



Instant Alert Manager Installation Guide

Summer, 2014

Copyright and Disclaimer

This document, as well as the software described in it, is furnished under license of the Instant Technologies Software Evaluation Agreement and may be used or copied only in accordance with the terms of such license. The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Instant Technologies. Instant Technologies assumes no responsibility or liability for any errors or inaccuracies that may appear in this document. All information in this document is confidential and proprietary.

Except as permitted by the Software Evaluation Agreement, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Instant Technologies .

Copyright © 2005 - 2014 Instant Technologies, All rights reserved.

Trademarks

All other trademarks are the property of their respective owners.

Contact Information

See our Web site for Customer Support information.

<http://www.instant-tech.com/>

TABLE OF CONTENTS

System Requirements.....	4
Environment	4
Optional Requirements for Email-to-IM Gateway	4
Software Prerequisites	4
Enable Required Role Services	4
Enable Role services in Windows Server 2008R2:	5
Enable Role services in Windows Server 2012:.....	8
Add Server Features	12
Windows Server 2008 R2	12
Windows Server 2012.....	14
Install Prerequisites.....	15
Install these components in the following order:.....	16
Alert Manager Installation	17
Active Directory Setup.....	18
SQL Setup.....	19
Server Login:	19
Database:	20
Create New Database.....	20
Use Existing Database.....	21
License Key.....	22
Enter a License Key	22
One-Month Trial License	22
AM Lync User.....	23
Select Dispatch Account.....	24
Select Group to Send Alerts	24
SMTP Config.....	24
IM Gateway SMTP Settings	25

Outgoing SMTP Settings	25
Configure IIS	26
Configure Gateway for Use	27
Create .IM Subdomain	27
Configure Exchange Send Connector (Exchange Server 2013)	28
Enabling Persistent Chat Rooms for use with Instant Alert Manager	34
Using the Gateway	37
Sending an Email to a Chat Room	37
Sending Email with Importance to Chat Room.....	40
Sending Email with Attachments.....	40
Sending Emails with URL Link(s)	41
Sending an IM to a User by Email.....	44
Sending an IM to a Group of Users	45
Sending IM Messages on Behalf of the Sender	Error! Bookmark not defined.
Email Response to Sender.....	45
Configuration Complete	48

ALERT MANAGER INSTALLATION GUIDE

SYSTEM REQUIREMENTS

Alert Manager is designed to operate on Windows Server 2008 R2® and Windows Server 2012®.

NOTE: Alert Manager should not be installed on the same server as Lync®. There are configuration issues when trying to host this application where Lync® is hosted.

ENVIRONMENT

- Active Lync 2010 environment
- SQL Server 2008 R2 -or – SQL Server 2012
- Access to Active Directory
- Desktop Experience (for Server 2008 R2) – or – Media Foundation (for Server 2012)

OPTIONAL REQUIREMENTS FOR EMAIL-TO-IM GATEWAY

- SMTP or Exchange Server
- Ability to modify MX records

SOFTWARE PREREQUISITES

- .NET Framework 4.5
- PowerShell 3.0
- UCMA 3.0 Runtime API [UcmaRuntime.msi]
- Microsoft System CLR Types for SQL Server 2012 (x64) [SQLSysClrTypes.msi]
- Microsoft SQL Server 2012 Shared Management Objects (x64) [SharedManagementObjects.msi]

ENABLE REQUIRED ROLE SERVICES

Alert manager requires some role services to be installed before the installation of the application can proceed. We require:

- IIS6 Management Compatibility Mode
- Security > Windows Authentication
- Application Development > ASP.NET; .NET Extensibility; ISAPI Extensions; ISAPI Filters
 - In addition, Windows Server 2012 requires: .NET Extensibility 3.5; .NET Extensibility 4.5; ASP.NET 3.5; ASP.NET 4.5; CGI

We have provided the appropriate PowerShell commands to quickly enable these roles services. They can be found in the PS_Commands folder provided in the download. Or if you prefer, you can enable these services through the GUI using the following steps:

ENABLE ROLE SERVICES IN WINDOWS SERVER 2008R2:

1. Start the Server Manager application as an administrator.
2. Select Roles from the directory tree.
3. Select Web Server, and scroll down to Role Services.

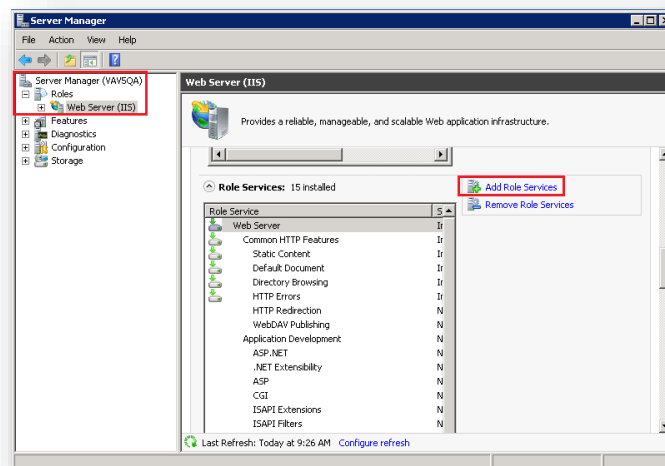


Figure 1: Add Role Services (Web Server (IIS))

4. Click on the option to “Add role services”
 - 4.1. Scroll to Application Development and select the following services:
 - **ASP.NET**
 - **.NET Extensibility**
 - **ISAPI Extensions**
 - **ISAPI Filters**

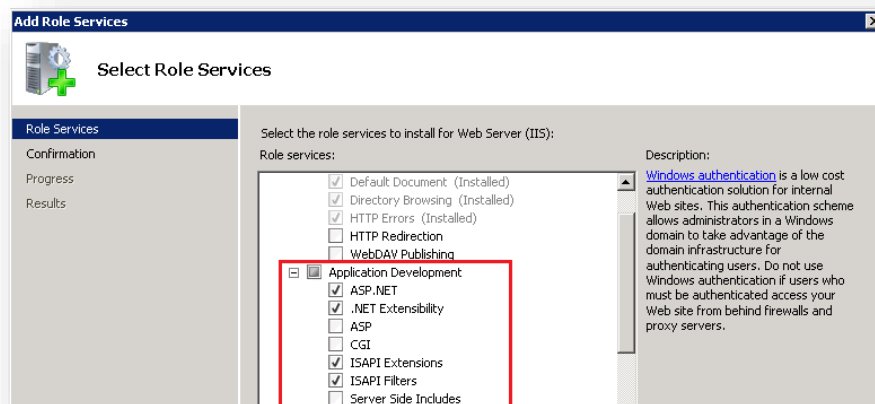


Figure 2: Select **Application Development** services

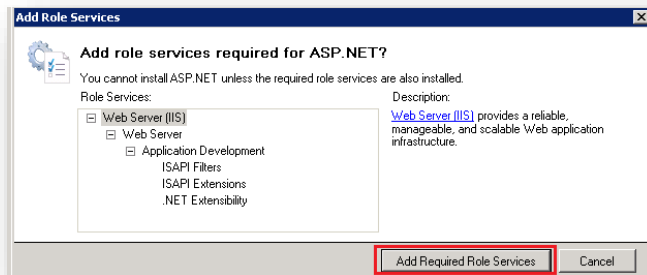


Figure 3: Select required role services for **ASP.NET**

4.2. Scroll to **Security** and select **Windows Authentication**.

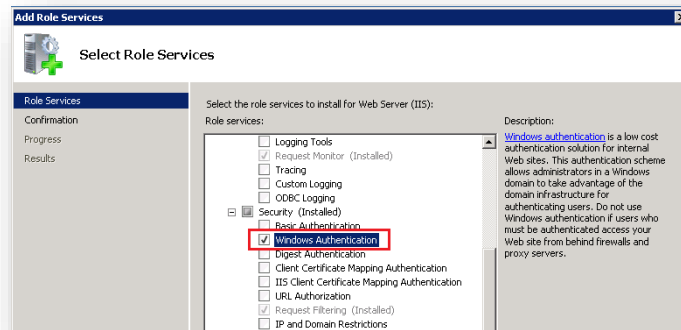


Figure 4: Select **Windows Authentication**

4.3. Scroll down until you find IIS6 Compatibility Mode, and select all the services in the **IIS6 Compatibility Mode** tree.

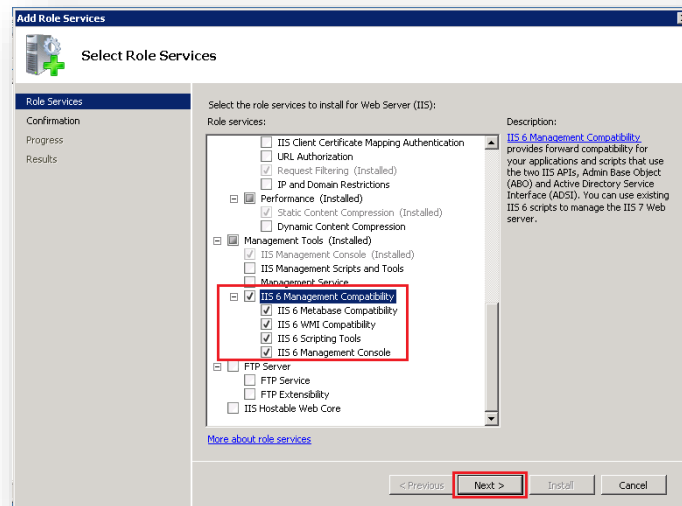


Figure 5: Select IIS 6 Management Compatibility

5. Click **Next** in the bottom right corner once all necessary services have been selected.
6. Click **Install** to install these services to the server.

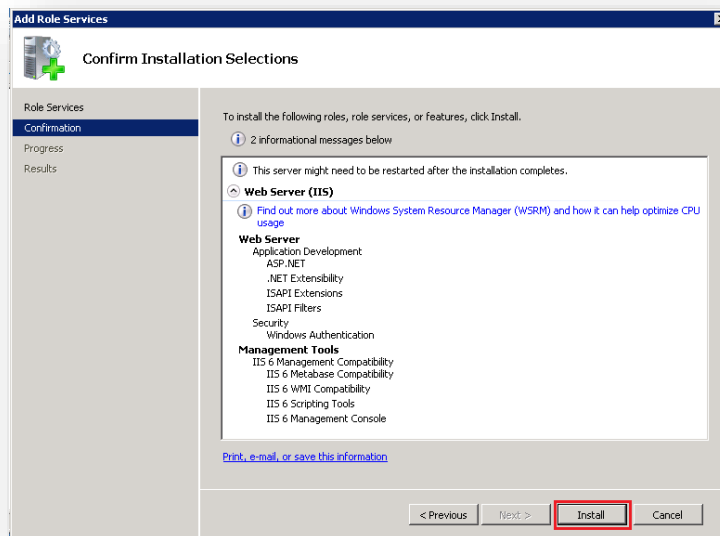


Figure 6: Install selected role services

- Click **Close** once installation of the selected services is completed.

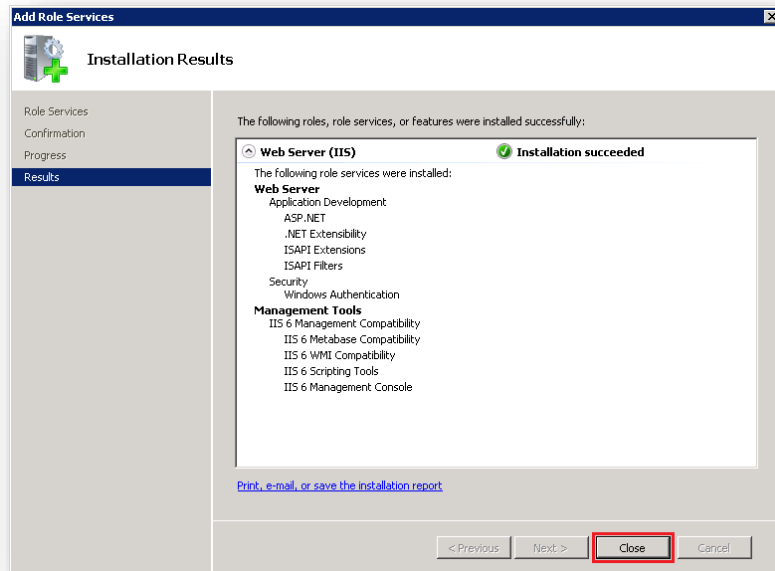


Figure 7: Installation of role services complete

ENABLE ROLE SERVICES IN WINDOWS SERVER 2012:

- Open the Server Manager application.
- Select **Add Roles and Features** from the **Manage** option.

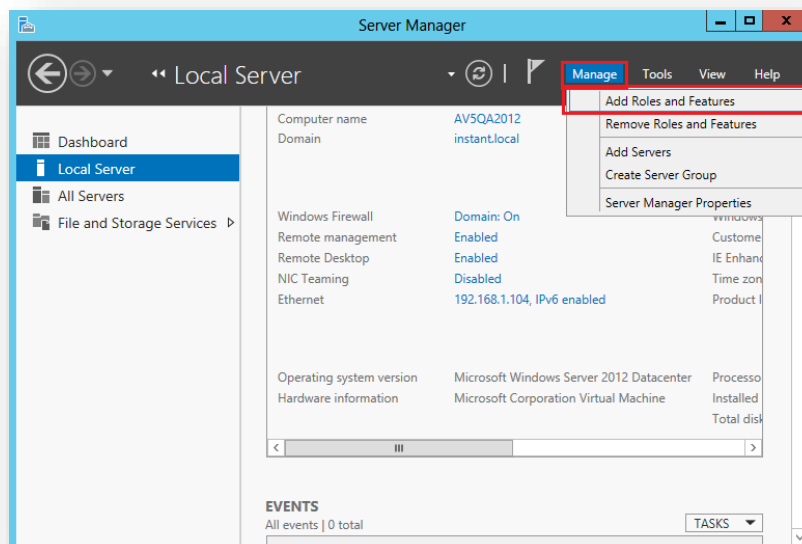


Figure 8: Add Roles and Features

- Select the option for **Role-based or feature-based installation** and click **Next**.

4. Select the appropriate server and click **Next**.
5. Add Web Server (IIS), and accept the Roles and Features prompted by the wizard. Click **Next**.

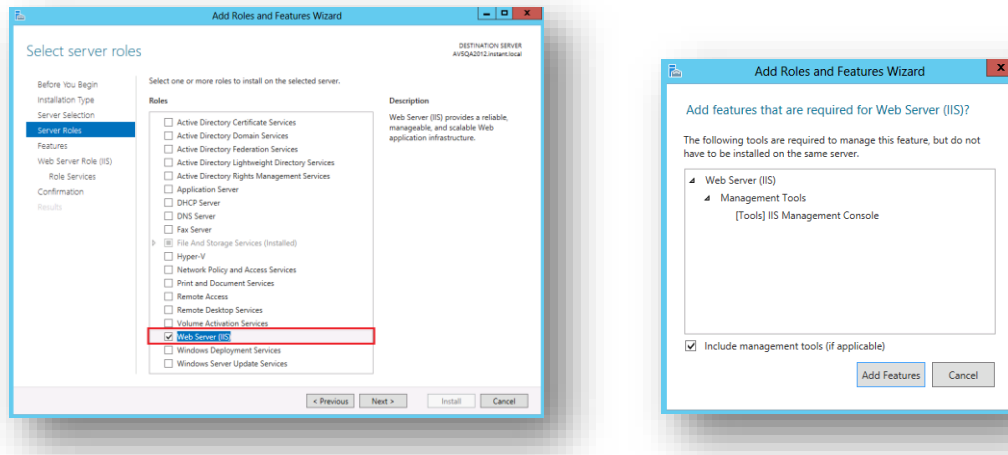


Figure 9: Add Web Server (IIS)

6. Do not select any features, and click **Next**.
7. Add Web Server (IIS) Role Services
 - a. Under **Security**, select the option for **Windows Authentication**.
 - b. Under **Application Development**, select the following services:
 - **.NET Extensibility 3.5**
 - **.NET Extensibility 4.5**
 - **ASP**
 - **ASP.NET 3.5**
 - **ASP.NET 4.5**
 - **CGI**
 - **ISAPI Extensions**
 - **ISAPI Filters**

By manually selecting **ASP.NET**, **ASP.NET 3.5**, and **ASP.NET 4.5**, the wizard will prompt you to accept the others, as they are required to for these services to run.

- c. Under **Management Tools**, select **IIS 6 Management Compatibility**, and then select the four additional services:
 - **IIS 6 Metabase Compatibility**
 - **IIS6 Management Console**
 - **IIS 6 Scripting Tools**
 - **IIS 6 WMI Compatibility**

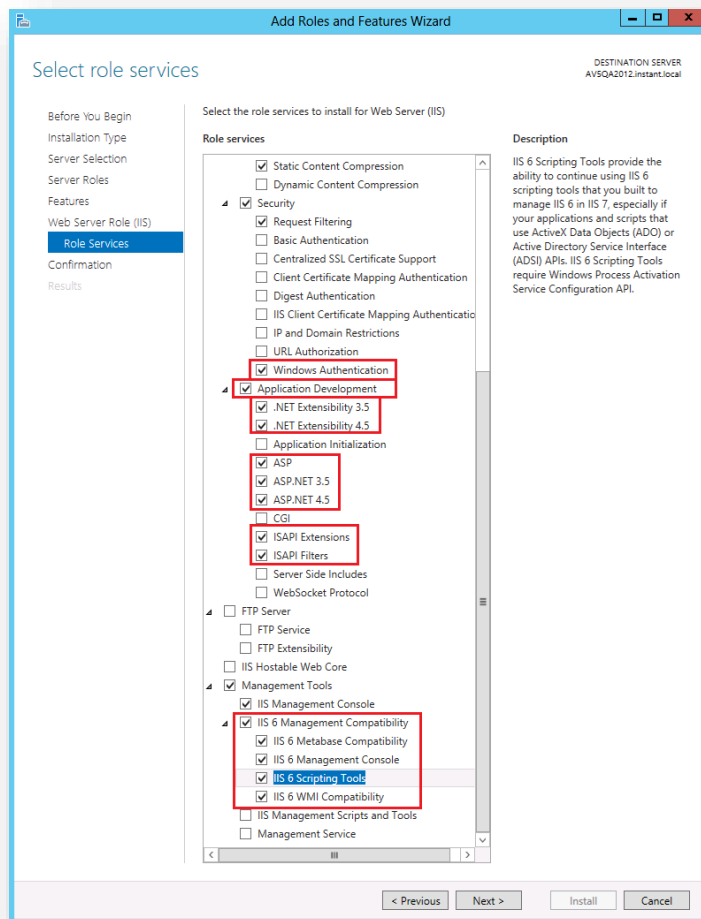


Figure 10: Add require role services

8. Click **Next** once these services have been selected.

9. Click **Install** to install the required services to your server.

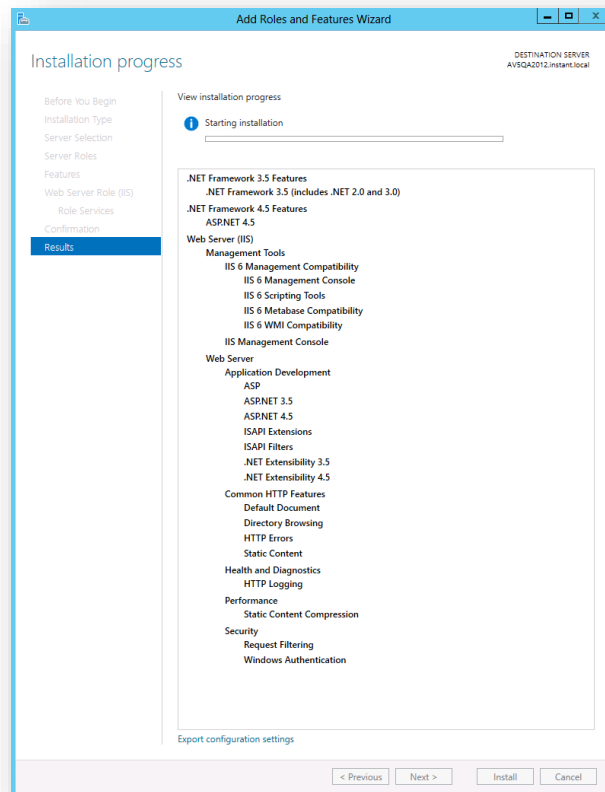


Figure 11: Installing required services

10. Installation of these services may take several minutes. Once complete, you are ready to begin installing Alert Manager.

ADD SERVER FEATURES

To install some of the prerequisites, it will be necessary to enable some additional features on the server.

WINDOWS SERVER 2008 R2

For Windows Server 2008 R2, it will be necessary to add the **Desktop Experience** feature. To do so, complete the following steps.

1. Start the Server Manager, and select **Add Features** in the Features Summary area.

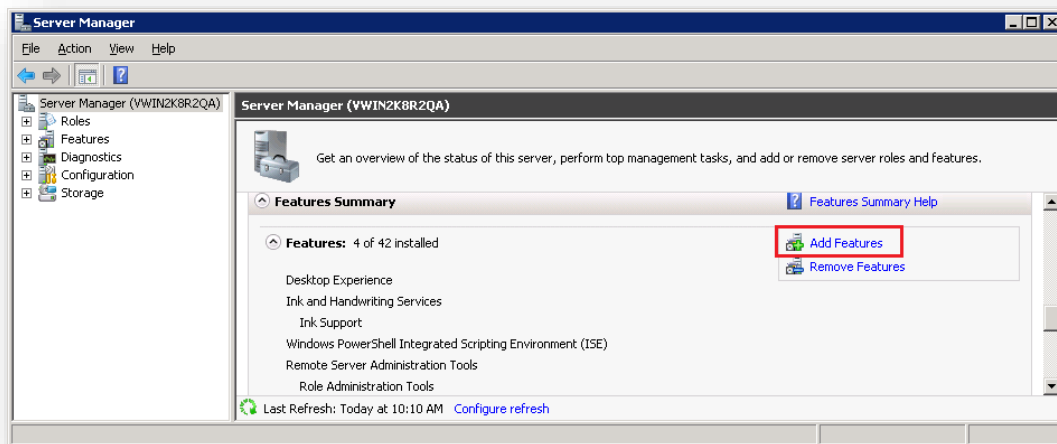


Figure 12: Add Features

2. Select **Desktop Experience**, and click **Next**.

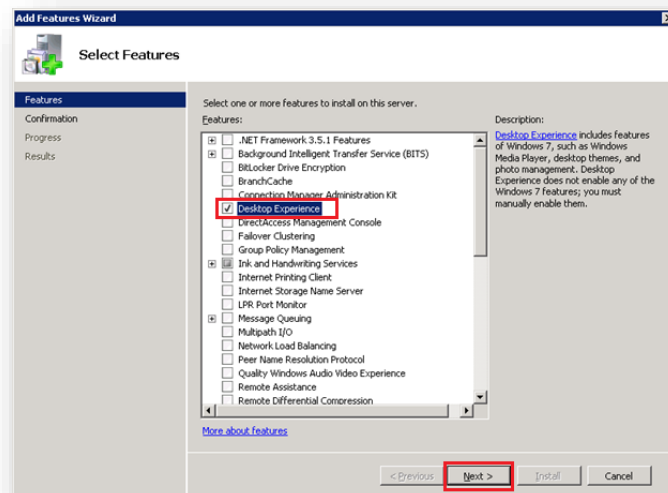


Figure 13: Select Desktop Experience

3. Accept the additional features required for Desktop Experience.

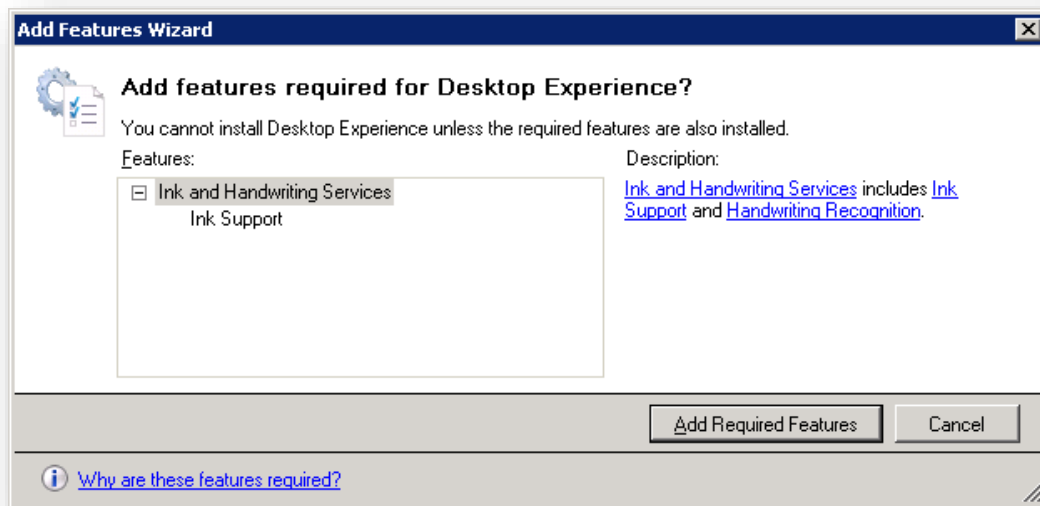


Figure 14: Accept required features

4. Restart the server when prompted once the installation is complete.

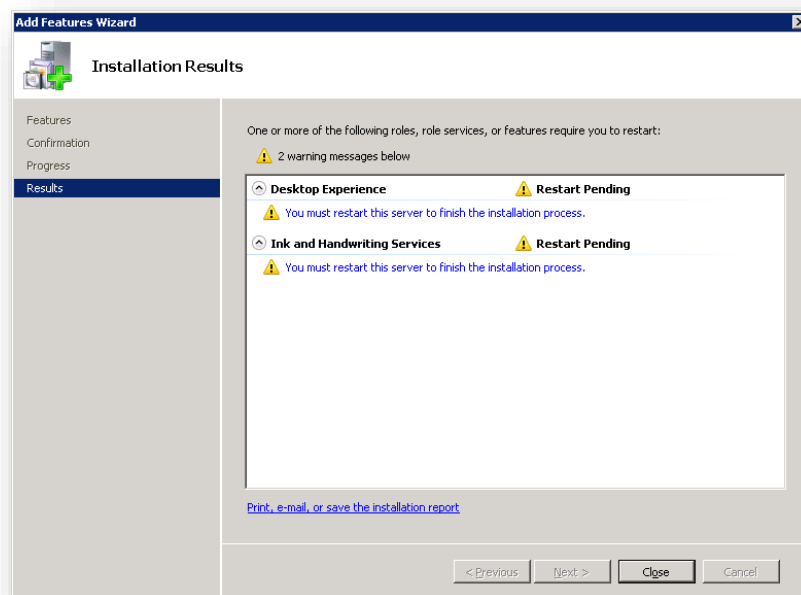


Figure 15: Installation of feature complete

WINDOWS SERVER 2012

For Windows Server 2012, it will be necessary to add the **Media Foundation** feature. To do so, complete the following steps:

1. Start the Server Manager.
2. Click **Manage > Add Roles and Features**.
3. Select the **Media Foundation** feature, and click **Next**.

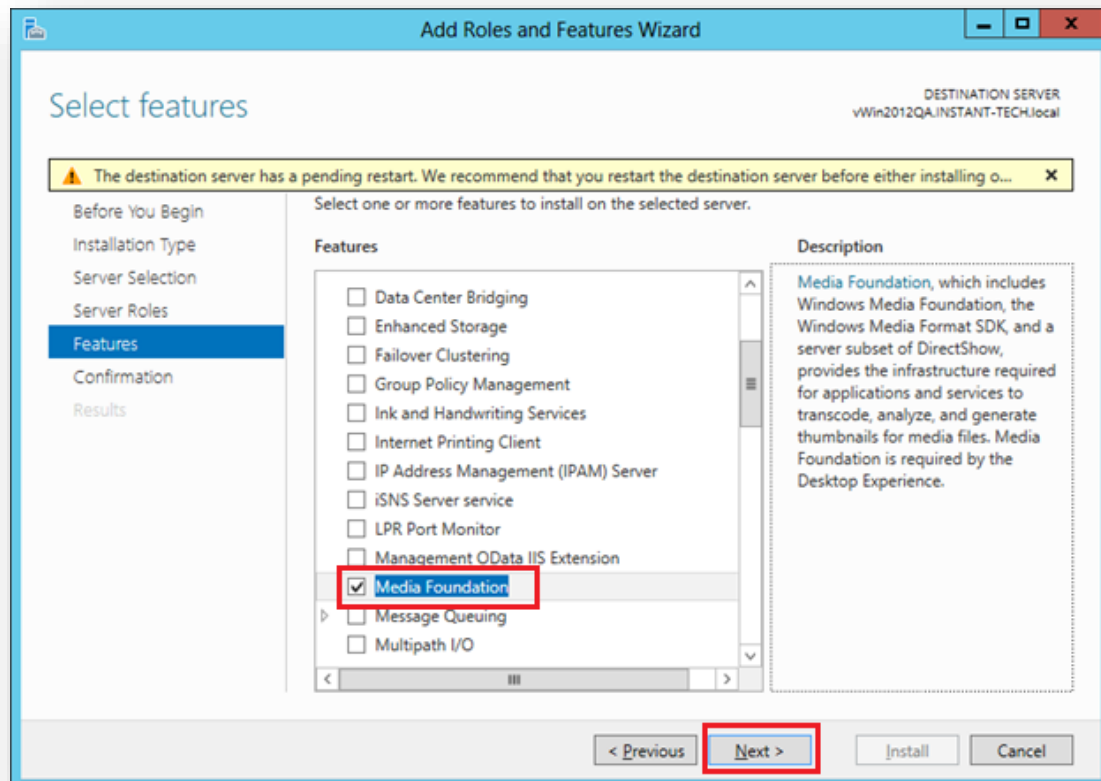


Figure 16: Add Media Foundation

4. Click **Install** to begin the installation of the feature to the server.

INSTALL PREREQUISITES

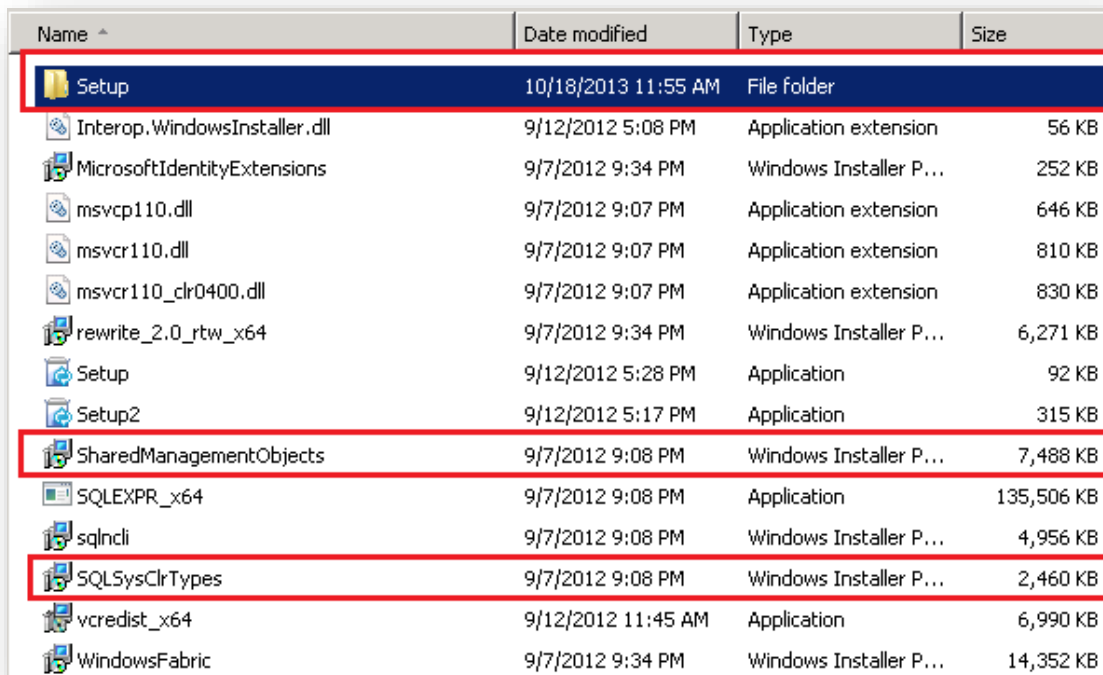
Alert Manager requires a number of features included on Lync servers to be installed on the server hosting the application. Most of these features can be found on your Lync Server 2010 Installation disc. Before you can install them, you will need to be sure that you have .NET4.0 and PowerShell 3.0 installed.

The UCMA 3.0 Runtime can be downloaded from:

<http://www.microsoft.com/en-us/download/details.aspx?id=20958>

The .msi files are located in the following directory:

..\LyncServerStandard\Setup\amd64



Name ^	Date modified	Type	Size
Setup	10/18/2013 11:55 AM	File folder	
Interop.WindowsInstaller.dll	9/12/2012 5:08 PM	Application extension	56 KB
MicrosoftIdentityExtensions	9/7/2012 9:34 PM	Windows Installer P...	252 KB
msvcp110.dll	9/7/2012 9:07 PM	Application extension	646 KB
msvcr110.dll	9/7/2012 9:07 PM	Application extension	810 KB
msvcr110_clr0400.dll	9/7/2012 9:07 PM	Application extension	830 KB
rewrite_2.0_rtw_x64	9/7/2012 9:34 PM	Windows Installer P...	6,271 KB
Setup	9/12/2012 5:28 PM	Application	92 KB
Setup2	9/12/2012 5:17 PM	Application	315 KB
SharedManagementObjects	9/7/2012 9:08 PM	Windows Installer P...	7,488 KB
SQLEXPR_x64	9/7/2012 9:08 PM	Application	135,506 KB
sqlncli	9/7/2012 9:08 PM	Windows Installer P...	4,956 KB
SQLSysClrTypes	9/7/2012 9:08 PM	Windows Installer P...	2,460 KB
vcredist_x64	9/12/2012 11:45 AM	Application	6,990 KB
WindowsFabric	9/7/2012 9:34 PM	Windows Installer P...	14,352 KB

Figure 17: Lync Server Prerequisite Components

..\LyncServerStandard\Setup\amd64\Setup

Name ^	Date modified	Type	Size
Speech	10/18/2013 11:58 AM	File folder	
admintools	9/12/2012 5:26 PM	Windows Installer P...	1,796 KB
appserver	9/12/2012 5:51 PM	Windows Installer P...	1,048 KB
ats	9/12/2012 5:21 PM	Windows Installer P...	4,608 KB
backupservice	9/12/2012 5:29 PM	Windows Installer P...	1,556 KB
caa	9/12/2012 5:53 PM	Windows Installer P...	36,992 KB
cas	9/12/2012 7:14 PM	Windows Installer P...	43,240 KB
cps	9/12/2012 5:23 PM	Windows Installer P...	2,160 KB
datamcu	9/12/2012 5:31 PM	Windows Installer P...	1,948 KB
deploy_topology_node	9/12/2012 2:42 PM	XML Document	8 KB
mediationserver	9/12/2012 5:35 PM	Windows Installer P...	1,820 KB
mgcserver	9/12/2012 5:31 PM	Windows Installer P...	2,248 KB
mgmtserver	9/12/2012 5:53 PM	Windows Installer P...	1,692 KB
ocscore	9/12/2012 5:51 PM	Windows Installer P...	30,392 KB
OCSMCU	9/12/2012 5:32 PM	Windows Installer P...	4,528 KB
OCSWMIBC	9/12/2012 5:28 PM	Windows Installer P...	1,172 KB
Pdp	9/12/2012 5:42 PM	Windows Installer P...	1,572 KB
ReachFonts	9/12/2012 6:05 PM	Windows Installer P...	100,436 KB
rgs	9/12/2012 5:26 PM	Windows Installer P...	4,888 KB
Server	9/12/2012 5:54 PM	Windows Installer P...	10,588 KB
setuphome	9/12/2012 2:42 PM	XML Document	9 KB
UcmaRuntime	9/12/2012 5:52 PM	Windows Installer P...	5,412 KB
ucmaworkflowruntime	9/12/2012 5:41 PM	Windows Installer P...	336 KB
webcomponents	9/12/2012 8:20 PM	Windows Installer P...	71,564 KB

Figure 18: Lync Server Prerequisite Components

INSTALL THESE COMPONENTS IN THE FOLLOWING ORDER:

1. UCMA 3.0 Runtime API [UcmaRuntime.msi]
2. Microsoft System CLR Types for SQL Server 2012 (x64) [SQLSysClrTypes.msi]
3. Microsoft SQL Server 2012 Shared Management Objects (x64) [SharedManagementObjects.msi]

ALERT MANAGER INSTALLATION

Once the required services, features, and prerequisites are installed, you are ready to begin installation of the Alert Manager application.

Run the **setup.exe** file provided in the Alert Manager download.

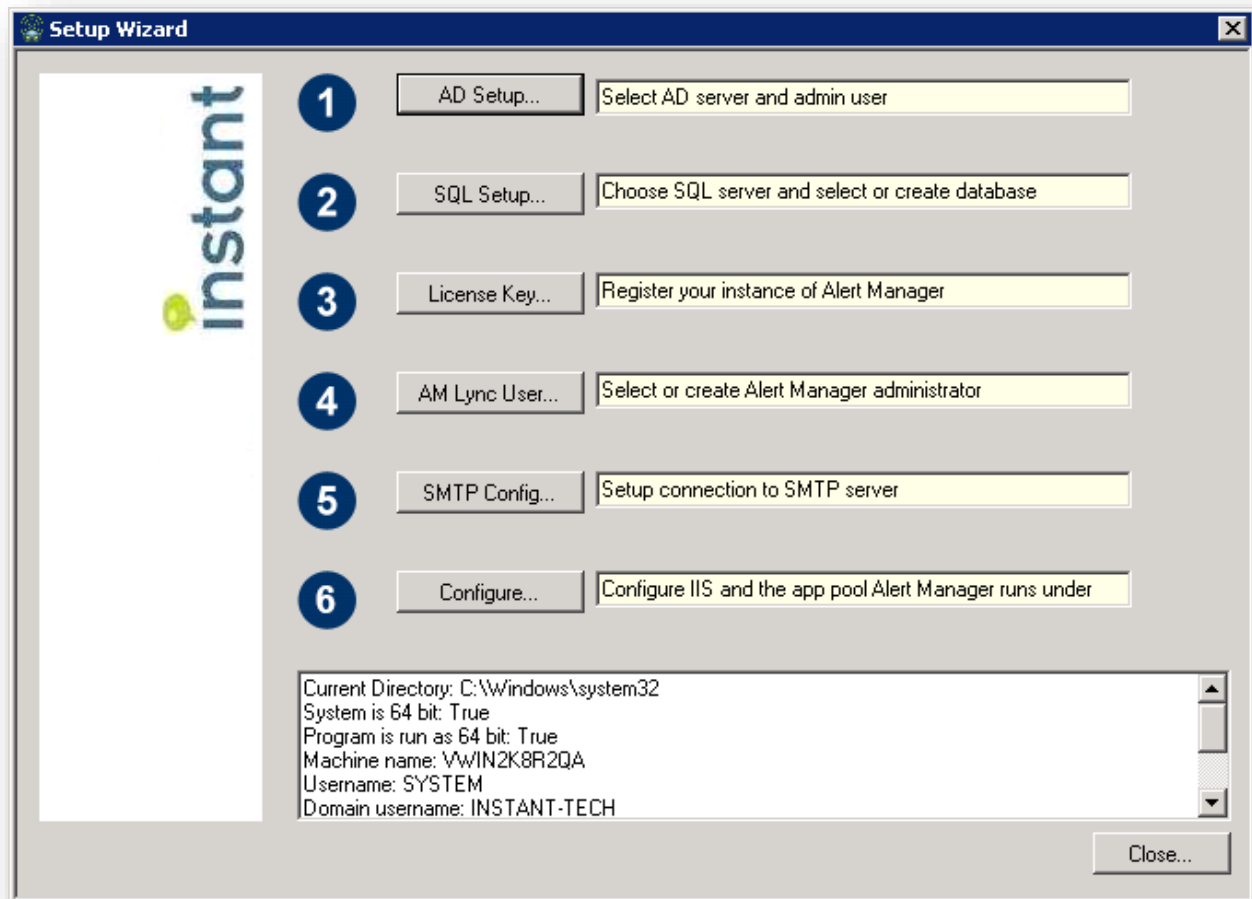
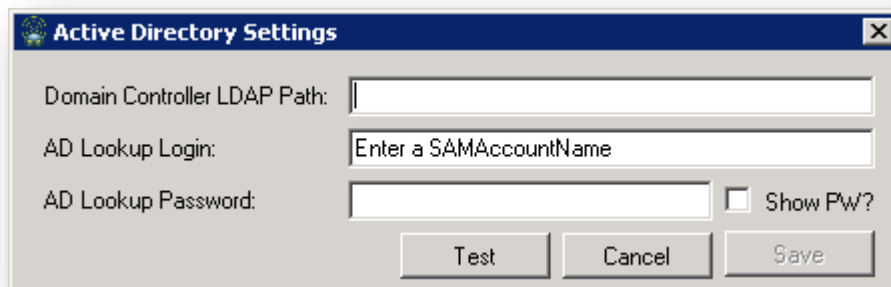


Figure 19: Alert Manager Installation Wizard

ACTIVE DIRECTORY SETUP

1. Enter Domain Controller LDAP Path.
Ex: MachineName.Domain
Note: You do not need to enter the **LDAP://** prefix, we will enter that automatically when testing the connection
2. Provide an account for AD Lookup Login. This account is used to query Active Directory when searching for users or groups to send alerts to.
3. Provide the password for the account provided in the previous step.
4. Click **Test** to verify that the values provided will successfully connect. If the test passes, click **Save**. If the test fails, verify the values provided and retest.



The 'Active Directory Settings' dialog box contains three input fields: 'Domain Controller LDAP Path:', 'AD Lookup Login:', and 'AD Lookup Password:'. The 'AD Lookup Login' field has a placeholder text 'Enter a SAMAccountName'. To the right of the password field is a checkbox labeled 'Show PW?'. At the bottom are three buttons: 'Test', 'Cancel', and 'Save'.

Figure 20: Active Directory Settings

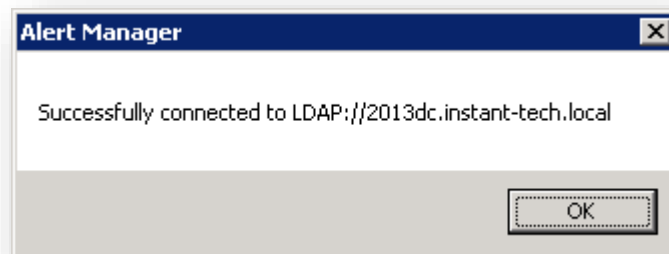
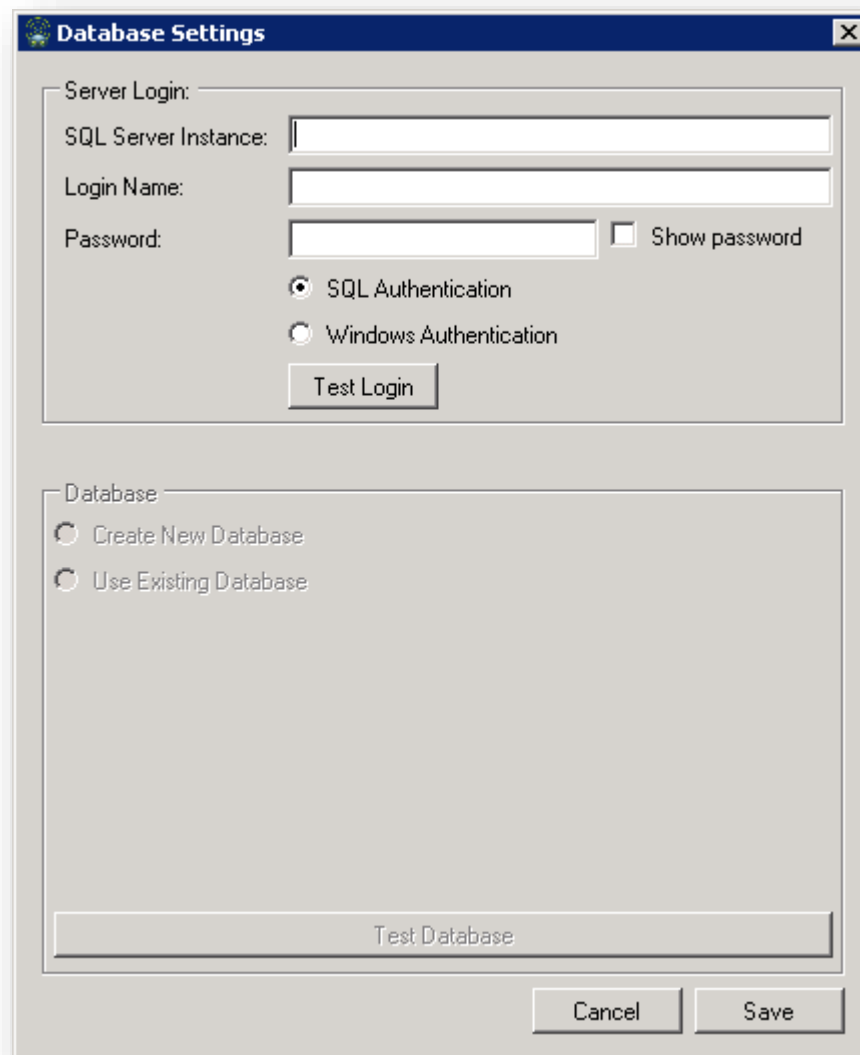


Figure 21: Successfully connected.

SQL SETUP

SERVER LOGIN:

1. Specify address for the SQL server to use.
 - a. Enter FQDN (Ex: **MachineName.Domain**)
2. Provide an account to login to the SQL server.
3. Provide password for the account provided in the previous step.
4. Click **Test Login** to verify that the values provided will successfully connect. If the test fails, verify the values provided. If the test passes, continue to the next step.



The screenshot shows a 'Database Settings' dialog box with a blue title bar and a close button. It is divided into two main sections: 'Server Login' and 'Database'. The 'Server Login' section contains fields for 'SQL Server Instance', 'Login Name', and 'Password', along with a 'Show password' checkbox. Below these fields are two radio buttons for 'SQL Authentication' (selected) and 'Windows Authentication', and a 'Test Login' button. The 'Database' section contains two radio buttons for 'Create New Database' and 'Use Existing Database', and a 'Test Database' button. At the bottom right are 'Cancel' and 'Save' buttons.

Database Settings

Server Login:

SQL Server Instance:

Login Name:

Password: ☐ Show password

☒ SQL Authentication

☐ Windows Authentication

Test Login

Database

☐ Create New Database

☐ Use Existing Database

Test Database

Cancel Save

Figure 22: Connect to SQL

DATABASE:

You have two options when configuring the database. You can choose to create a new database, or use an existing database created during a previous installation.

CREATE NEW DATABASE

1. Click the radio button for **Create New Database**.
2. Specify the location of the SQL instance that will be used for the new database.
3. Enter a name for the new database into the input field.
4. Click **Create Database**.

The screenshot shows the 'Database Settings' dialog box. It has two main sections: 'Server Login' and 'Database'. In the 'Server Login' section, the 'SQL Server Instance' is set to '2013sql.instant-tech.local', the 'Login Name' is 'sa', and the 'Password' is masked with dots. The 'SQL Authentication' radio button is selected. There is a 'Test Login' button. In the 'Database' section, the 'Create New Database' radio button is selected. The path 'C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA\' is entered in the text field. There is a 'Create Database' button. The 'Use Existing Database' radio button is unselected. At the bottom of the dialog, there is a 'Test Database' button and 'Cancel' and 'Save' buttons.

Figure 23: Creating a new database

USE EXISTING DATABASE

1. Click the radio button for **Use Existing Database**.
2. Click on the name of the database you wish to use.
3. Click **Test Database**. The wizard will verify that the application can successfully connect to the specified database.
4. Click **Save**.

Database Settings

Server Login:

SQL Server Instance: 2013sql.instant-tech.local

Login Name: sa

Password: •••••• ☐ Show password

☒ SQL Authentication
☐ Windows Authentication

Test Login

Database

☐ Create New Database
☒ Use Existing Database

AlertManager
am1
michaelAMtest
foo
potato
AlertManagerTesting
AlertManager1

Test Database

Cancel Save

Figure 24: Using an existing database

LICENSE KEY

During configuration, you have the option to either enter a license key manually, or generate a one-month trial license.

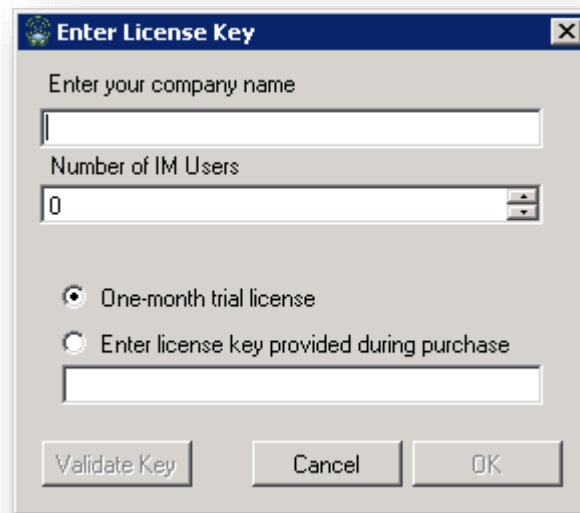


Figure 25: Enter a license key

ENTER A LICENSE KEY

1. Click the first radio button.
2. Enter the license key that has been provided to you into the input field.
3. Click **Validate Key**. The wizard will verify that the key you have entered is valid.
4. Click **OK**.

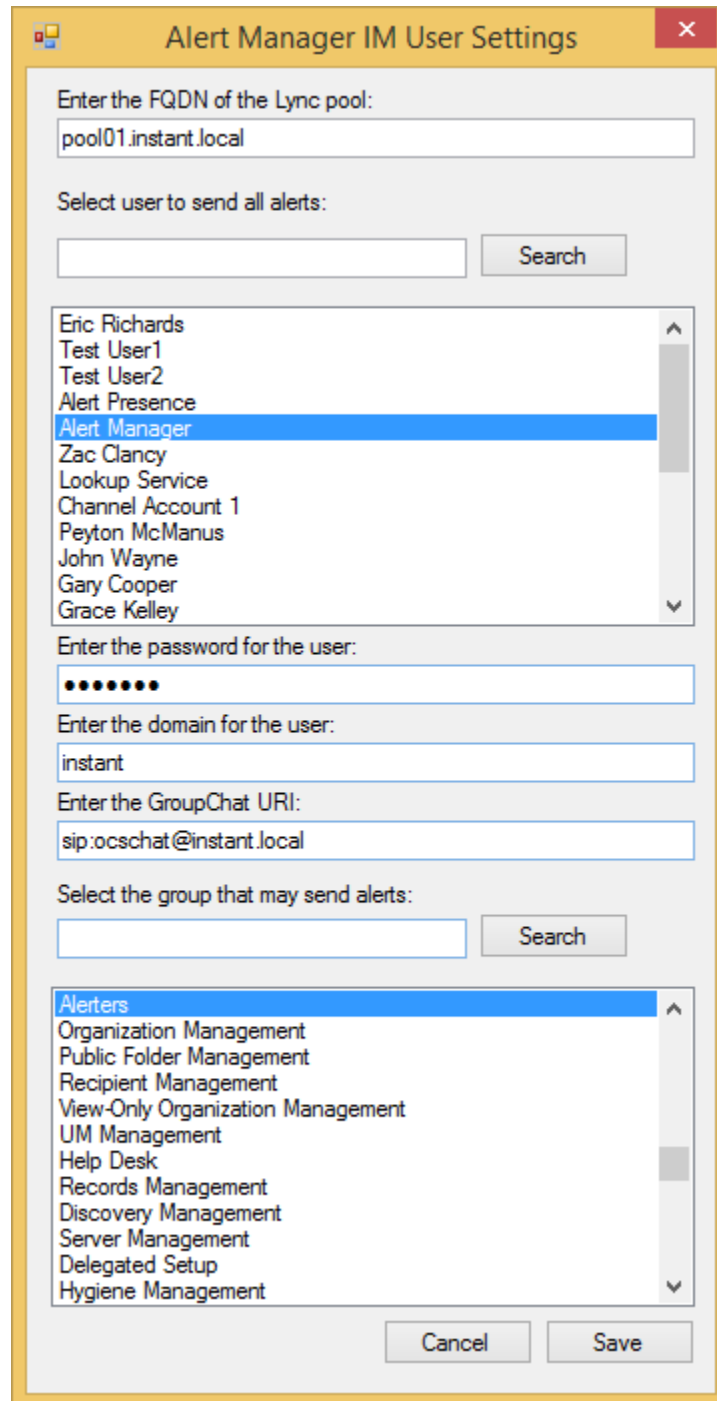
ONE-MONTH TRIAL LICENSE

1. Click the radio button for **One-month trial license**.
2. Enter your company name into the appropriately labeled input field.
3. Enter the number of IM users you will need to dispatch to.
4. Click **Validate Key**. The wizard will verify that the key is valid.
5. Click **OK**.

AM LYNC USER

You will need to assign a user account that the application can use to dispatch messages. It is recommended that you create a new account for this purpose.

You can later configure your message settings to inform the user who dispatched the message if desired.



The image shows a Windows-style dialog box titled "Alert Manager IM User Settings". It contains several input fields and two list boxes. The first list box, titled "Select user to send all alerts:", has "Alert Manager" selected. The second list box, titled "Select the group that may send alerts:", has "Alerters" selected. At the bottom are "Cancel" and "Save" buttons.

Enter the FQDN of the Lync pool:
pool01.instant.local

Select user to send all alerts:

Search

- Eric Richards
- Test User1
- Test User2
- Alert Presence
- Alert Manager**
- Zac Clancy
- Lookup Service
- Channel Account 1
- Peyton McManus
- John Wayne
- Gary Cooper
- Grace Kelley

Enter the password for the user:
●●●●●●

Enter the domain for the user:
instant

Enter the GroupChat URI:
sip:ocschat@instant.local

Select the group that may send alerts:

Search

- Alerters**
- Organization Management
- Public Folder Management
- Recipient Management
- View-Only Organization Management
- UM Management
- Help Desk
- Records Management
- Discovery Management
- Server Management
- Delegated Setup
- Hygiene Management

Cancel Save

Figure 26: Selecting IM User Settings

SELECT DISPATCH ACCOUNT

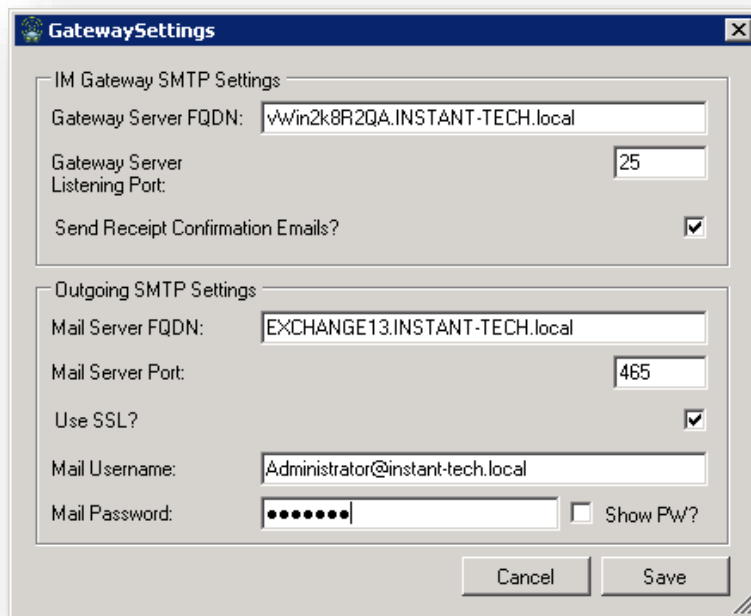
1. Enter the fully qualified domain name of the Lync pool
2. Enter the display name of the account you wish dispatch alerts.
3. Click **Search** to search the Active Directory for the account.
4. Click to select the account that you wish to use. The selected account will remain highlighted.
5. Enter the password for the chosen account
6. Enter the domain name for the chosen account
7. [Optional] Enter your Lync 2010 Group Chat URI. This is typically sip:ocschat@YourDomain.

SELECT GROUP TO SEND ALERTS

The application allows all members of a specified group to login to the service to send alerts. To control access, be sure that you have an Active Directory group appropriately setup to provide access to only the users who should be allowed to dispatch.

1. Enter the name of the Active Directory group in the input field.
2. Click **Search** to search the Active Directory for this group.
3. Click the name of the group you wish to use. The selected account will remain highlighted.
4. Click **Save** to save these settings.

SMTP CONFIG



The screenshot shows a Windows-style dialog box titled "GatewaySettings". It contains two main sections: "IM Gateway SMTP Settings" and "Outgoing SMTP Settings".

IM Gateway SMTP Settings:

- Gateway Server FQDN:
- Gateway Server Listening Port:
- Send Receipt Confirmation Emails? ☒

Outgoing SMTP Settings:

- Mail Server FQDN:
- Mail Server Port:
- Use SSL? ☒
- Mail Username:
- Mail Password: ☐ Show Pw?

At the bottom right, there are "Cancel" and "Save" buttons.

Figure 27: Email Gateway Settings

IM GATEWAY SMTP SETTINGS

This sets up the listening service for the Email-to-IM Gateway. These fields should automatically populate with the default settings. You will also need to create a new **.im** subdomain in order for the gateway to work.

1. Enter the Gateway (Alert Manager) Server FQDN into the appropriate field.
2. Specify the Gateway (Alert Manager) Server listening port.
3. Check or uncheck the checkbox to send receipt confirmation emails. If this box is checked, you must complete the next section of the form in order to dispatch the messages.

After completing the installation wizard, ensure that you have opened the gateway server listening port (default 25) on your server's firewall.

OUTGOING SMTP SETTINGS

These settings are used by the application to dispatch confirmation emails if you have selected to send the receipt confirmation emails.

The Outgoing SMTP Settings should be configured with the connection info for your current Exchange or SMTP server.

1. Enter the outgoing mail server FQDN into the appropriate field.
2. Specify the mail server port.
3. Check the box to use SSL if so desired.
4. Specify a username for the
5. Specify a password.
6. Click **Save** to apply the settings.

CONFIGURE IIS

This step ensures that the IIS settings for this application are correct.

1. Click **Test Settings** to perform a check of the current IIS settings.
2. Click **Autoconfigure** to have the application configure the settings to be correct, or manually change the settings using the Server Manager.
3. Click **OK** to complete this step.

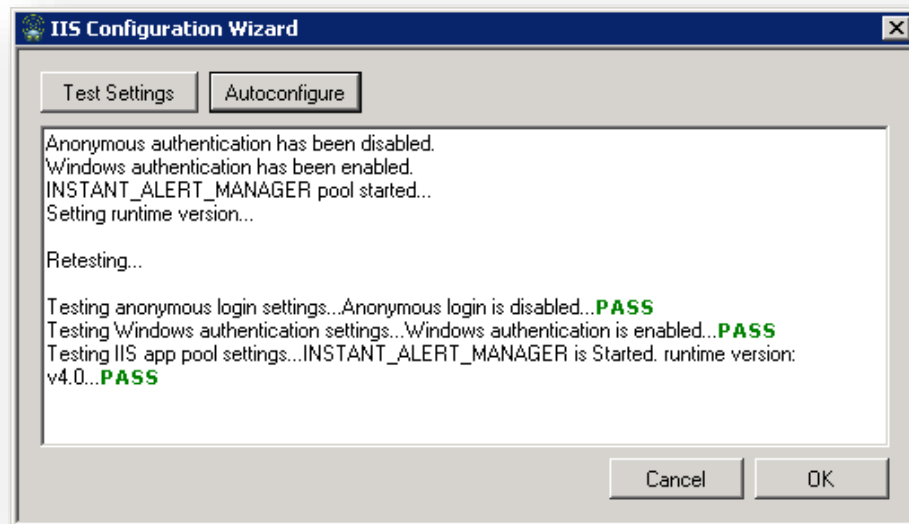


Figure 28: IIS Configuration Wizard

CONFIGURE GATEWAY FOR USE

You can configure the Email-to-IM Gateway for use with Microsoft Exchange, or any other SMTP server your organization is using.

For an SMTP server, follow the **Create .IM Subdomain** instructions.

For a Microsoft Exchange server, follow the **Configure Exchange Send Connector** instructions.

CREATE .IM SUBDOMAIN

In order for email messages to be correctly dispatched to Lync users, it is necessary to create an MX Record for the IM Gateway.

1. Login to the Domain Controller.
2. Open the **DNS Manager**.
3. Expand the proper domain controller node. Underneath there should be a node name **Forward Lookup Zones**. Underneath this you will find a list of domains. Select the domain corresponding to the email domain that you would like to use the IM Gateway to IM-enable.

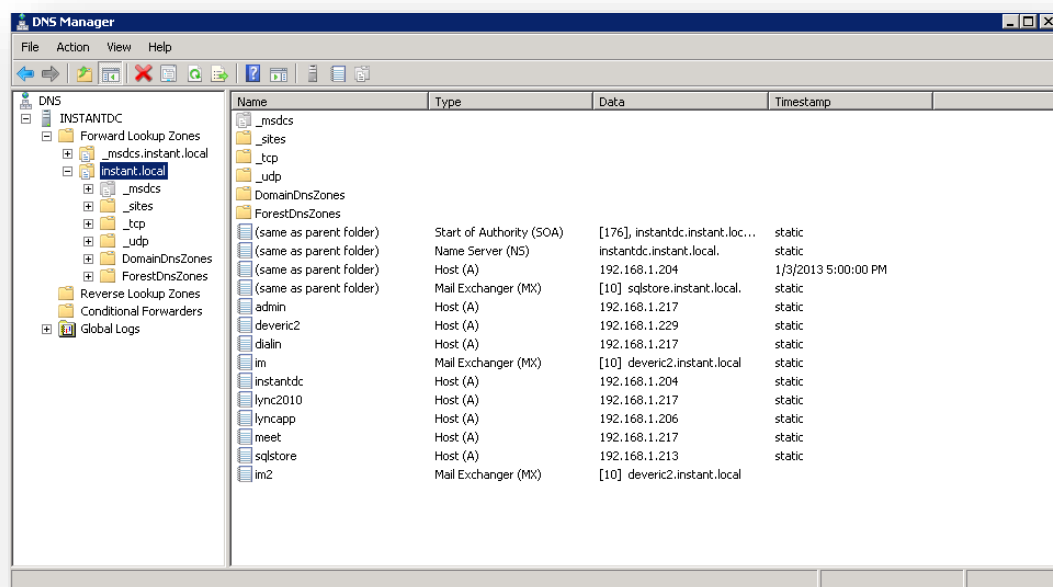


Figure 32: DNS Manager

4. Right-click in the main pane and select **New Mail Exchanger (MX)...** In the child domain input, enter **im**. Thus, if the parent domain is **contoso.com**, the second input should then read **im.contoso.com**. Enter the FQDN of the server which will run the IM Gateway in the third input (the Alert Manager server). Leave the priority field at the default.

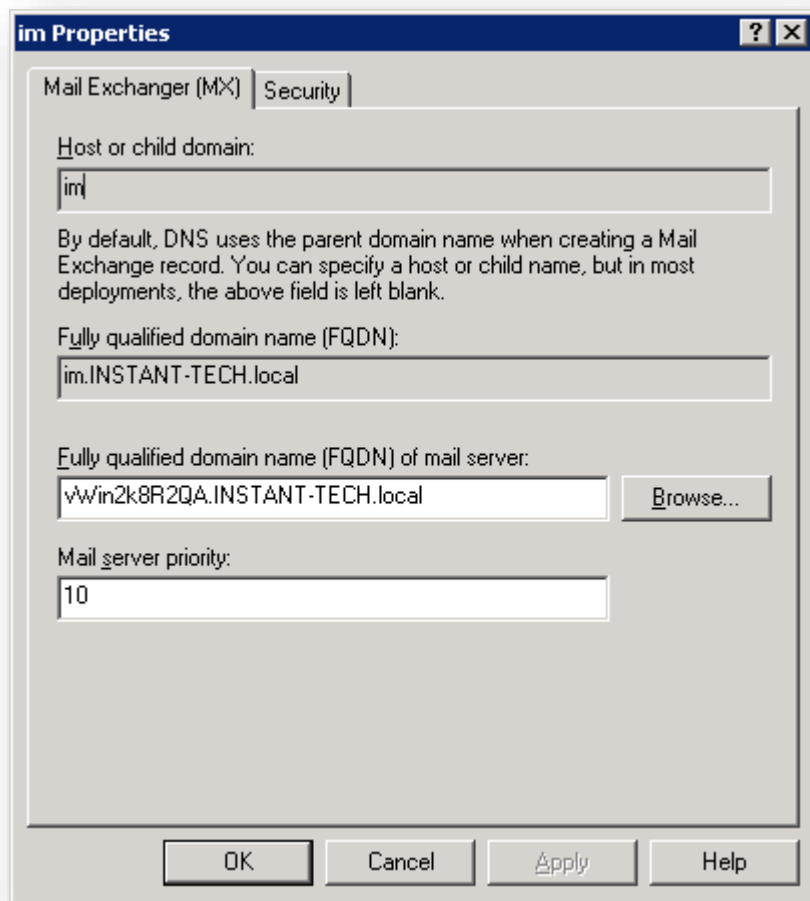


Figure 33: IM Subdomain Record

With the new MX record in place, emails addressed to the new **im.domain** will now be routed to the IM Gateway server.

CONFIGURE EXCHANGE SEND CONNECTOR (EXCHANGE SERVER 2013)

1. Access the Exchange Server Management Console using a supported browser (<SERVERADDRESS>/ecp).
2. Click on the **mail flow** option on the left side of the screen.
3. Click **accepted domains**.
4. Click the **+** icon to add a new accepted domain.

ADDING AN ACCEPTED DOMAIN

The new accepted domain will serve as a subdomain to route email messages to IM users. We recommend creating an **IM** subdomain. Prepending this new subdomain to email messages will allow these messages to be routed through the Alert Manager system.

Ex: user@im.domain.com

1. Provide a display name for the new domain
2. Create a new accepted domain (EX: **im.instant-tech.local**)
3. Choose the option for an **Internal relay domain**.
4. Click **save** to save the new settings.

Accepted Domain - Windows Internet Explorer

https://192.168.1.213/ecp/AcceptedDomain/NewAcceptedDomain.aspx?pwdcid=6&ReturnObjectType=1 Certificate error

new accepted domain [Help](#)

Accepted domains are used to define which domains will be accepted for inbound email routing.

*Name:
IM Gateway

*Accepted domain:
im.instant-tech.local

This accepted domain is:

☒ Authoritative domain. Email is delivered to a recipient in this Exchange organization.

☐ Internal relay domain. Email is delivered to recipients in this Exchange organization or relayed to an email server outside this organization.

☐ External Relay Domain. Email is relayed to an email server outside this Exchange organization.

save cancel

105%

Figure 34: Create a new accepted domain

CONFIGURE SEND CONNECTOR

1. Click **send connectors**.
2. Click the **+** to create a new send connector.
3. Enter a descriptive name for the new connector (Ex: IM Gateway).
4. Choose the option for **Custom**.

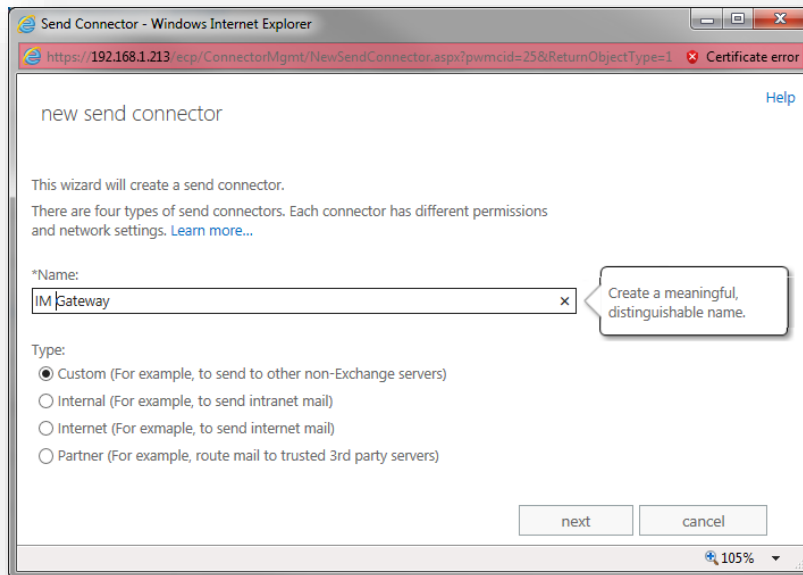


Figure 35: Name the new send connector

5. Click **next**.
6. Choose the option to **Route mail through smart hosts**.
7. Click **+** to add a new smart host.
8. Enter the FQDN of the server hosting Alert Manager in the field.

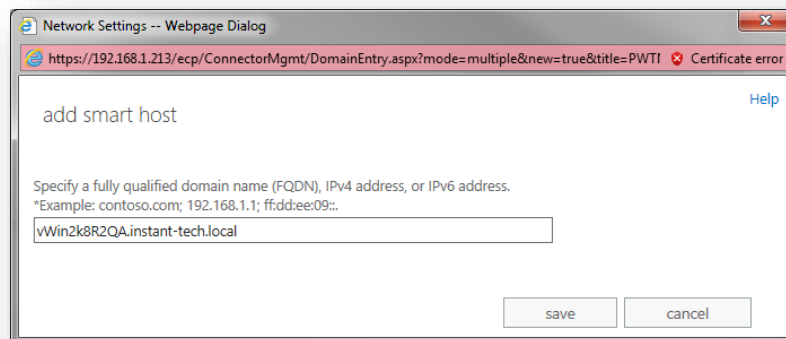


Figure 36: Add a smart host

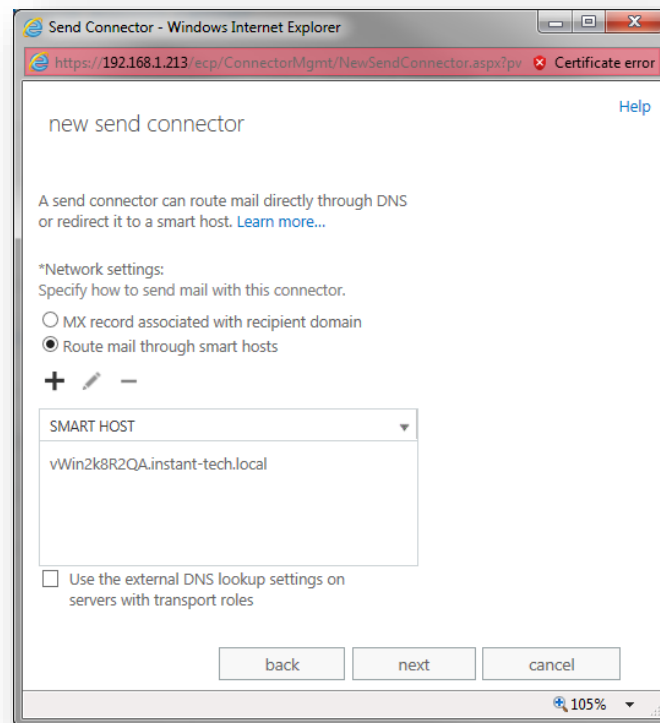


Figure 37: Send mail through a smart host

9. Click **next**.
10. Leave the default option of **none** selected for Smart host authentication.
11. Click **next**.
12. Click the **+** to specify an address space to use for this connector.
13. Leave the default type of **SMTP**.
14. Enter the FQDN of the new accepted domain created earlier (EX: im.instant-tech.local).
15. Leave the default cost **1**.
16. Click **save**.

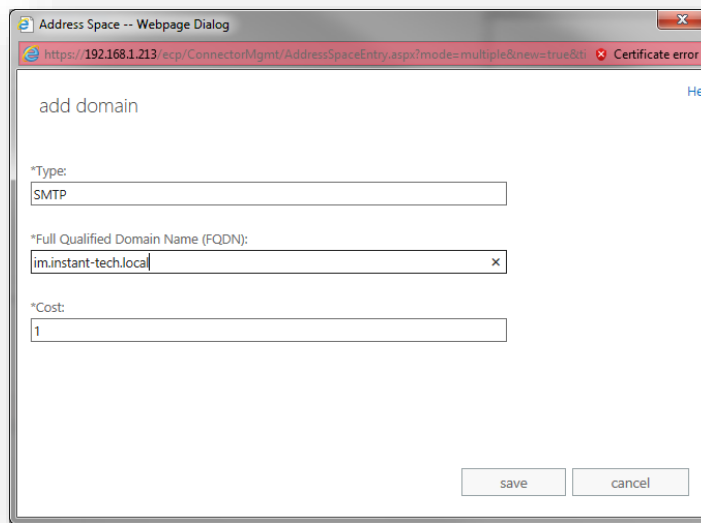


Figure 38: Add an address space

17. Click **next**.

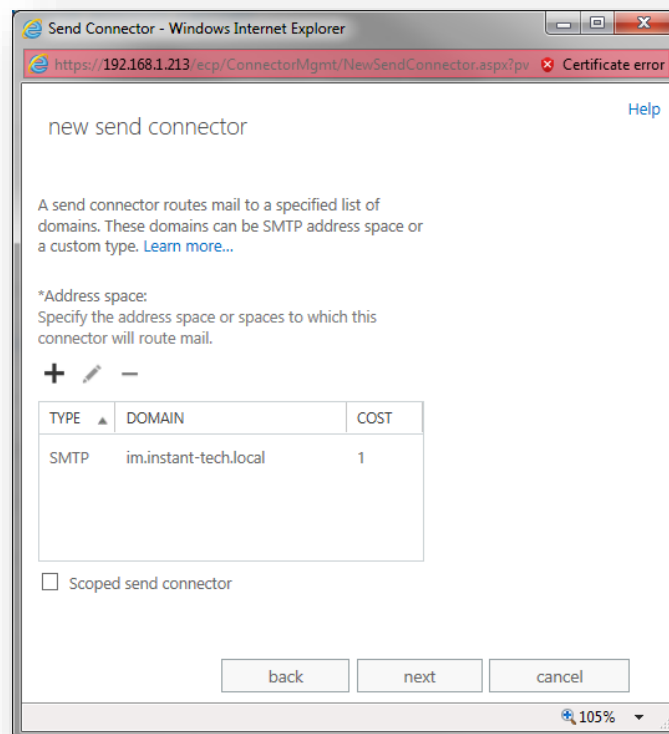


Figure 39: Address space specified

18. Click the **+** to associate a source server.

19. Select the appropriate exchange server, and click the **add** button.

20. Click **ok** to save the selection.

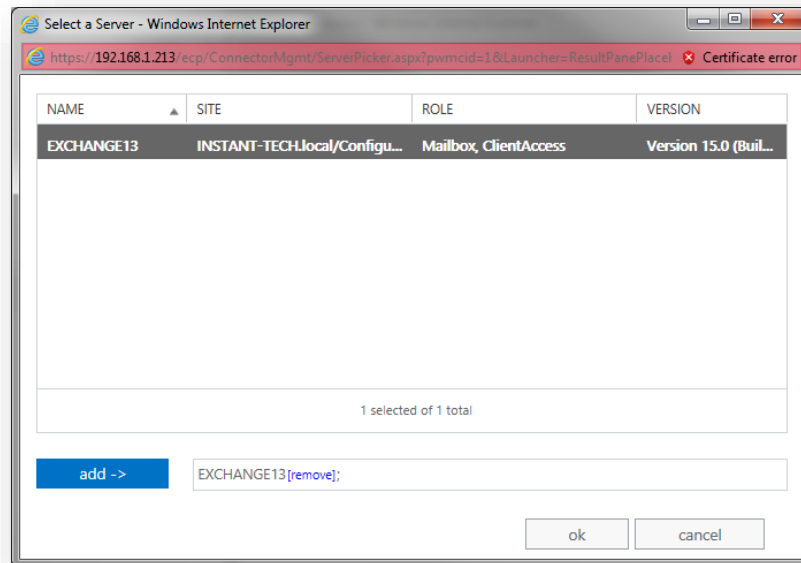


Figure 40: Select a mail server

21. Click **finish** to complete the creation of the new send connector.

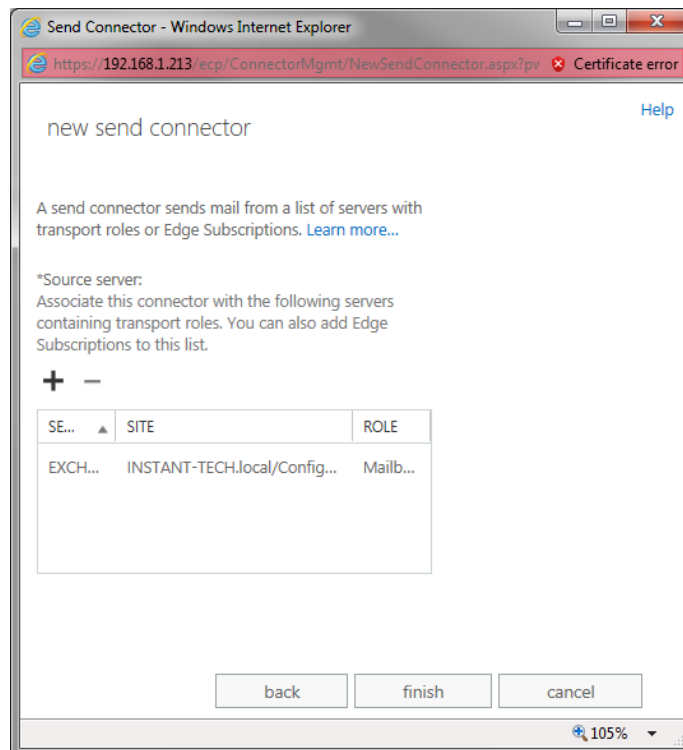


Figure 41: Finish send connector setup

ENABLING PERSISTENT CHAT ROOMS FOR USE WITH INSTANT ALERT MANAGER

To enable a Lync persistent chat room for receiving alerts from Instant Alert Manager, it is necessary to create an Active Directory Contact object for the chat room on your domain controller.

1. On your domain controller, open **Active Directory Users and Computers**, and navigate to the OU that you would like to add the chat room in. If you do not have specific OUs, then you will want to navigate to **Users**.

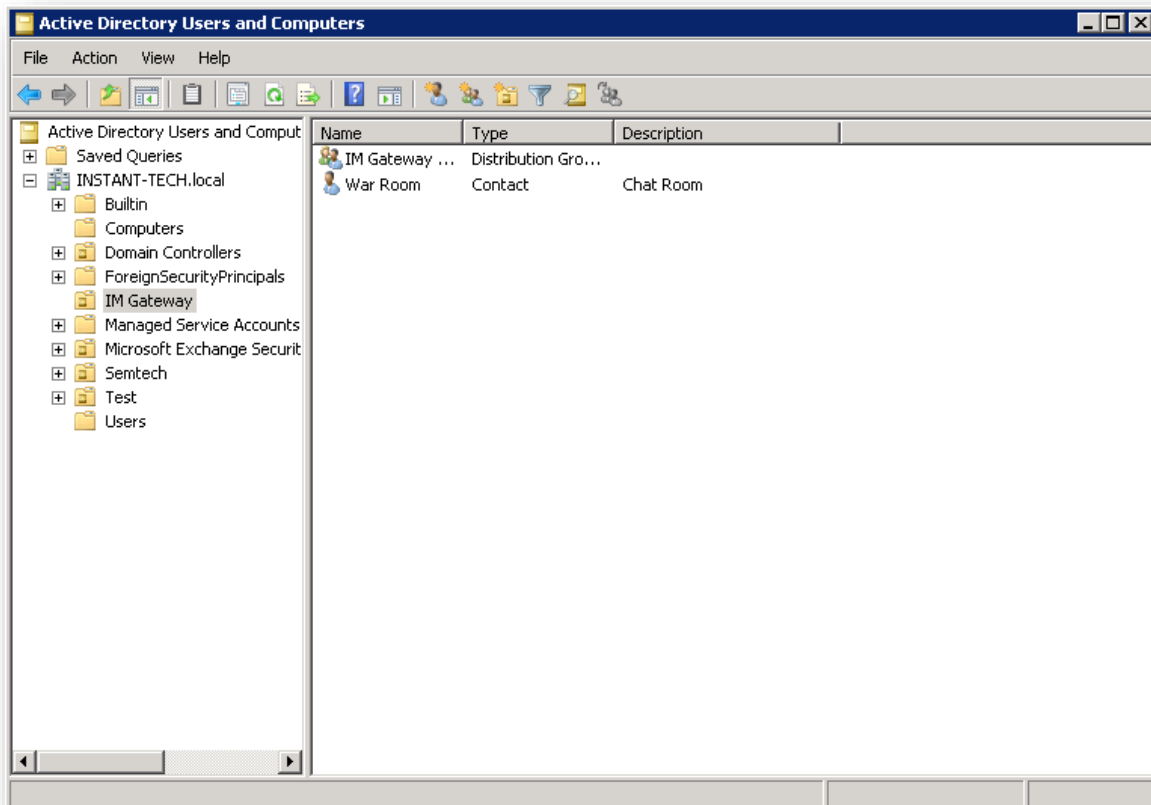
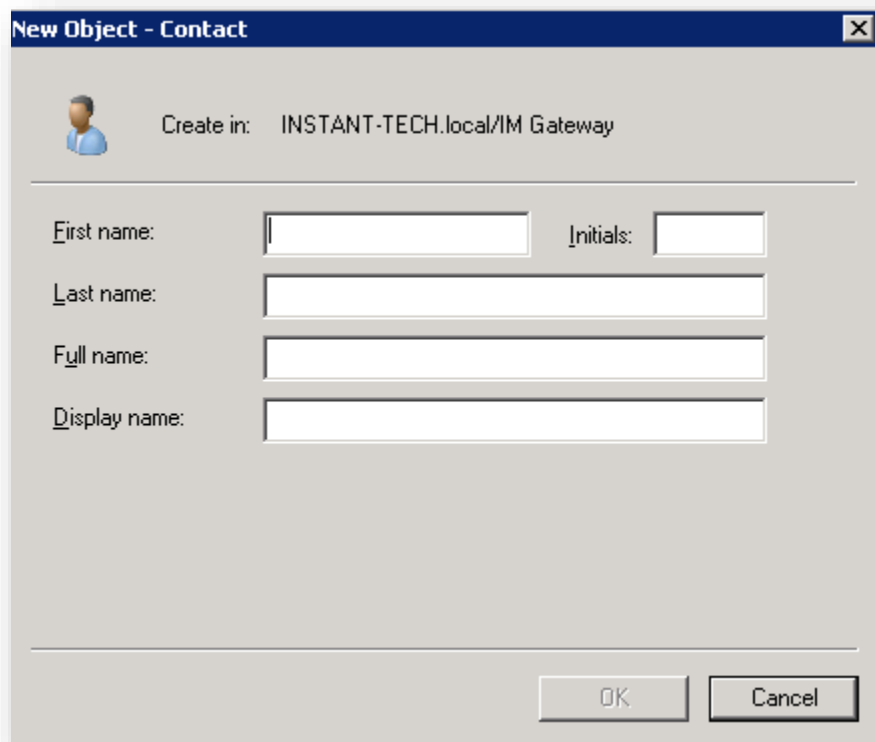


Figure 42: Active Directory

2. Right-click in the right panel, and from the context menu that appears select **New->Contact**. You should see the dialog below pop up.



New Object - Contact

Create in: INSTANT-TECH.local/IM Gateway

First name: Initials:

Last name:

Full name:

Display name:

OK Cancel

Figure 43: Create a new contact

3. Under **Display Name**, enter the name of the persistent chat room, as it is displayed in the Lync Client. Enter the same value, or any identification of your choice for the **Full Name** (This value is not used by AlertManager, but must be filled out to create the AD object). Click **OK** to create the new contact object.

4. Double-click on the newly created contact object in the right pane of the **Active Directories Users and Computers** dialog. This will open the properties dialog for the new contact object.

The screenshot shows a Windows-style dialog box titled "War Room Properties". It has several tabs: "General", "Address", "Telephones", "Organization", and "Member Of". The "General" tab is active. At the top left of the tab is a small icon of a person and the text "War Room". Below this are several text input fields: "First name:" with "War", "Initials:" (empty), "Last name:" with "Room", "Display name:" with "War Room", "Description:" with "Chat Room", and "Office:" (empty). Below these are three more fields: "Telephone number:" (empty) with an "Other..." button, "E-mail:" with "war_room@instant-tech.local", and "Web page:" (empty) with an "Other..." button. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

Figure 44: Chat Room Properties

5. In the **Description** field, enter the words "**Chat Room**". This indicates to the AlertManager service that this contact object represents a chat room; if you have other Contact objects without this description, AlertManager will not consider them when searching for Chat rooms or resolving addresses.
6. If you would like to enable the chat room for dispatching via email using the Email-to-IM Gateway feature, provide an email address for the contact object in the **E-mail** field. This email address does not need to have an actual Exchange mailbox associated with it.
7. Click **OK** to save the contact object. You should now be able to lookup the newly enabled chat room when sending an alert via the AlertManager web UI, or by sending an email to chatEmailName@im.chatRoomEmailDomain via the IM Gateway. (In this example, *chatRoomEmailName* would be **war_room** and *chatRoomEmailDomain* would be **instant-tech.local**, thus to send to this chat room, you would email **war_room@im.instant-tech.local**.)

USING THE GATEWAY

SENDING AN EMAIL TO A CHAT ROOM

To send a message to a chat room using the Instant IM Gateway, simply compose an email to the address defined for the chat room, with the (**im.**) subdomain prepended to the domain. For instance, in the screen shot below, a message is being sent to the Microsoft Development chat room, which is defined in AD as microsoft_development@instant.local. The (**im.**) subdomain is essential to ensure that the message is correctly routed to the IM Gateway server, rather than the normal mail server. In the following example, the 'To' address of the email is: microsoft_development@im.instant.local.

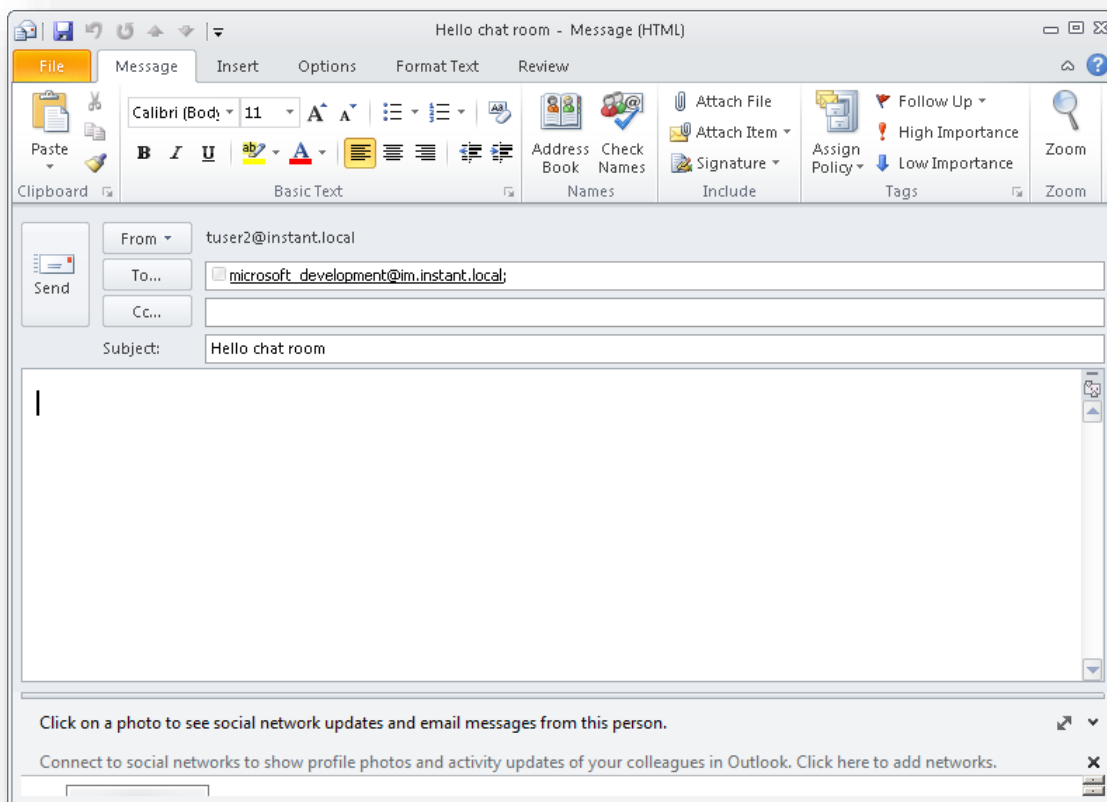


Figure 45: Sending an email through the Gateway

You have three options when sending a message to a chat room through the IM Gateway.

- 1.) A message with a subject, but no body, will appear in the chat room as a single line of text.
- 2.) A message with a body and no subject will also appear as a single line of text, unless the body text exceeds the max length limit of the chat client. If this limit is exceeded, the chat will be converted to a story.

- 3.) A message with subject and body will be displayed as a story, with the subject of the mail as the subject of the story.

NOTE: When possible, emails should be sent as plain-text, not as HTML. The IM Gateway currently supports HTML formatted email, but HTML is not rendered with the Lync 2010 Group Chat room. Therefore, the IM Gateway will attempt parse the HTML contained within an email into a format suitable for the Lync 2010 Chat Room.

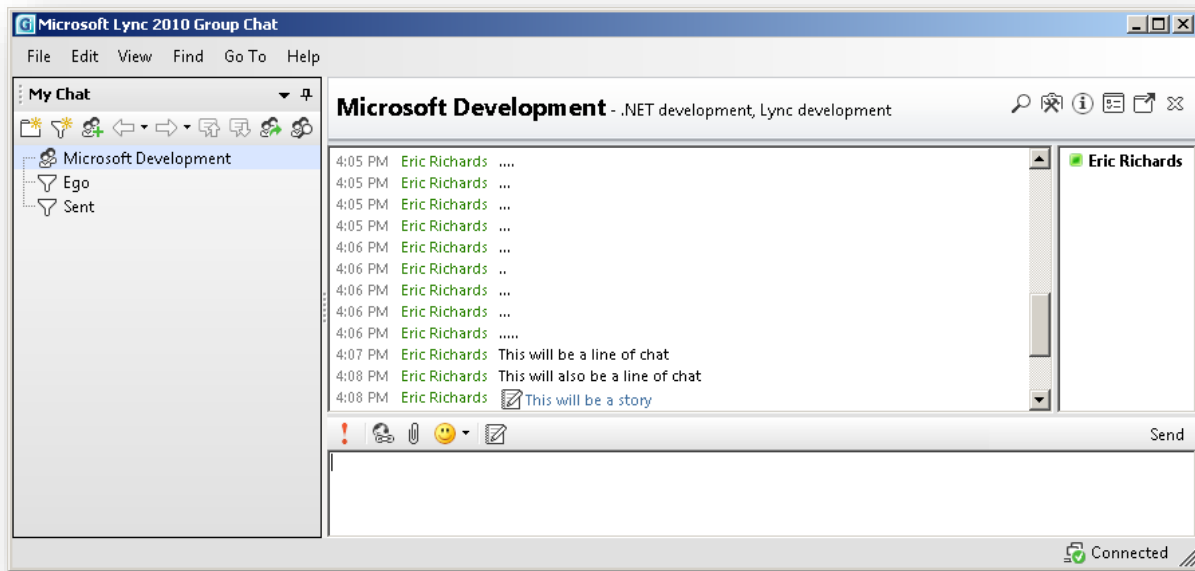


Figure 46: Message delivered to group chat room

The following screen shot demonstrates how a message will be displayed in the Group Chat room when the message is consolidated to a Group Chat story:

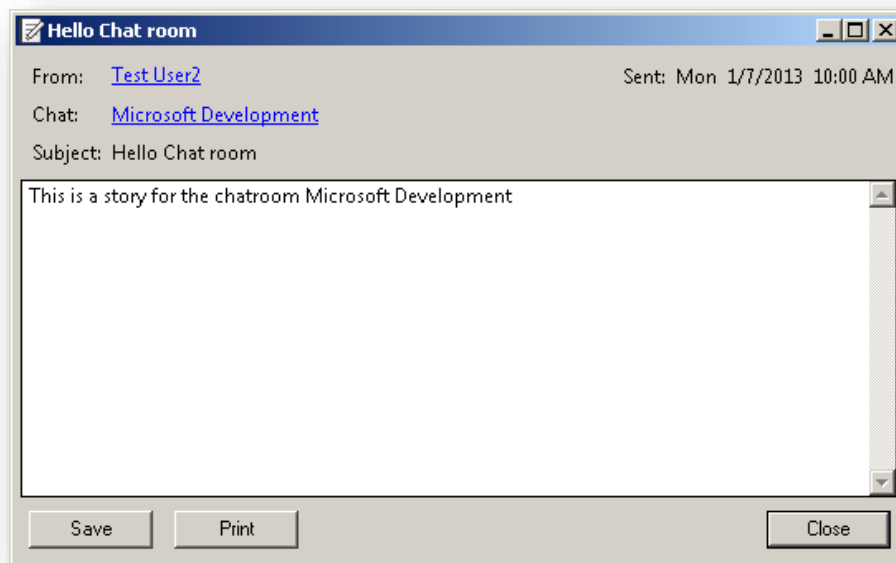


Figure 47: Message displayed as a story

In the event that an email contains a significant amount of information, then the email message will automatically be split into different 'stories' and placed into the Lync Group Chat room as a collection of 'parts'. For example, the following screen shot demonstrates several emails that have been submitted to the chat room and they have been split across a collection of story segments:

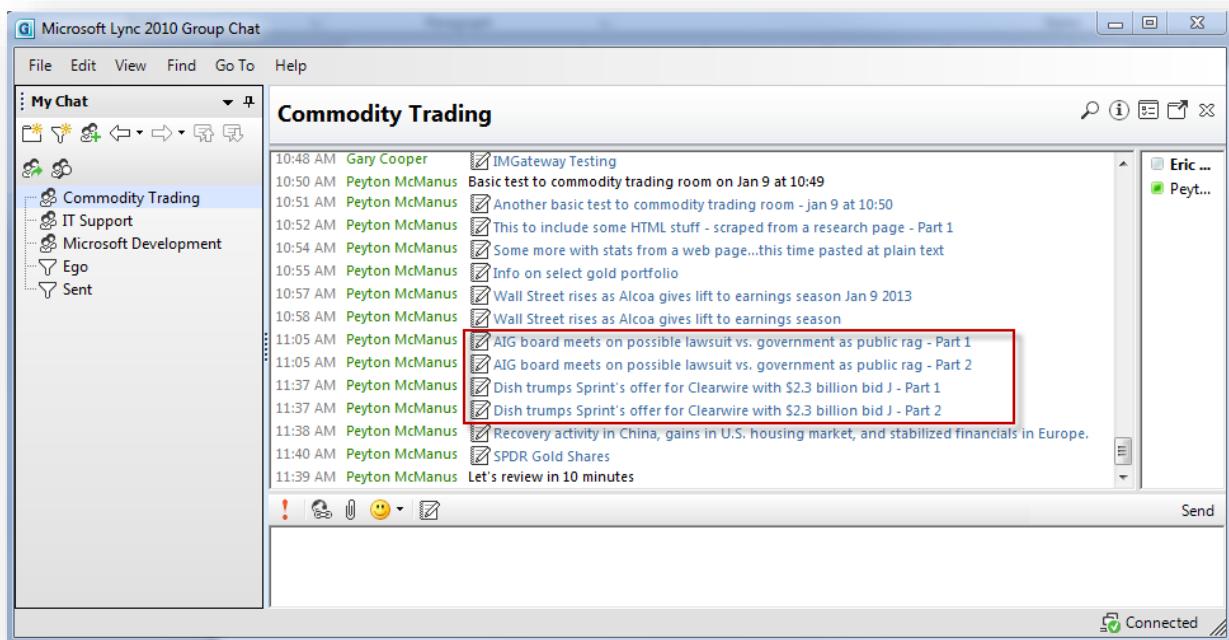


Figure 48: Large message split up into multiple stories

SENDING EMAIL WITH IMPORTANCE TO CHAT ROOM

By default, the gateway supports the ability to convert emails marked with 'importance' to a similar message in the Lync Group Chat room. So, if an email is marked as important, the message will be dispatched to the chat room and flagged as important.

SENDING EMAIL WITH ATTACHMENTS

The gateway supports the ability to receive emails with attachments and the application will automatically post attachments to the designated Microsoft Lync Group Chat room. Currently the gateway does not support the ability to distribute attachments to individuals via the Lync IM protocol.

The following screen shots demonstrate sending an email with either one, or multiple attachments, to a Group Chat room.

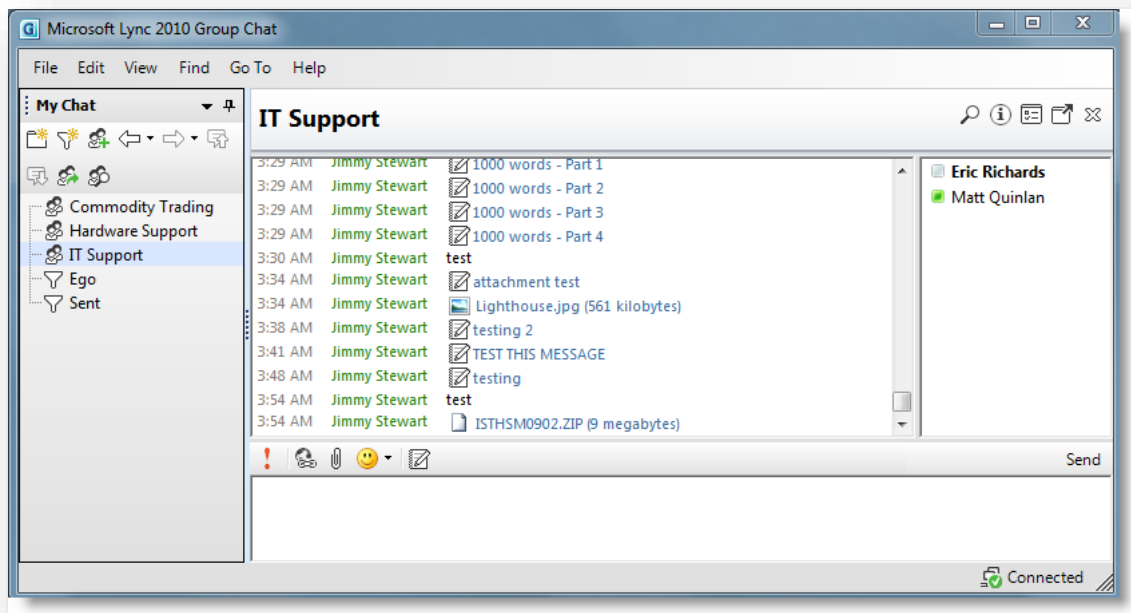


Figure 49: Attachments delivered to the chat room

By default, the Lync Group Chat room may provide specific 'hover' behavior for certain types of files. For example, the following screen shot demonstrates how an image might be rendered via a hover action:

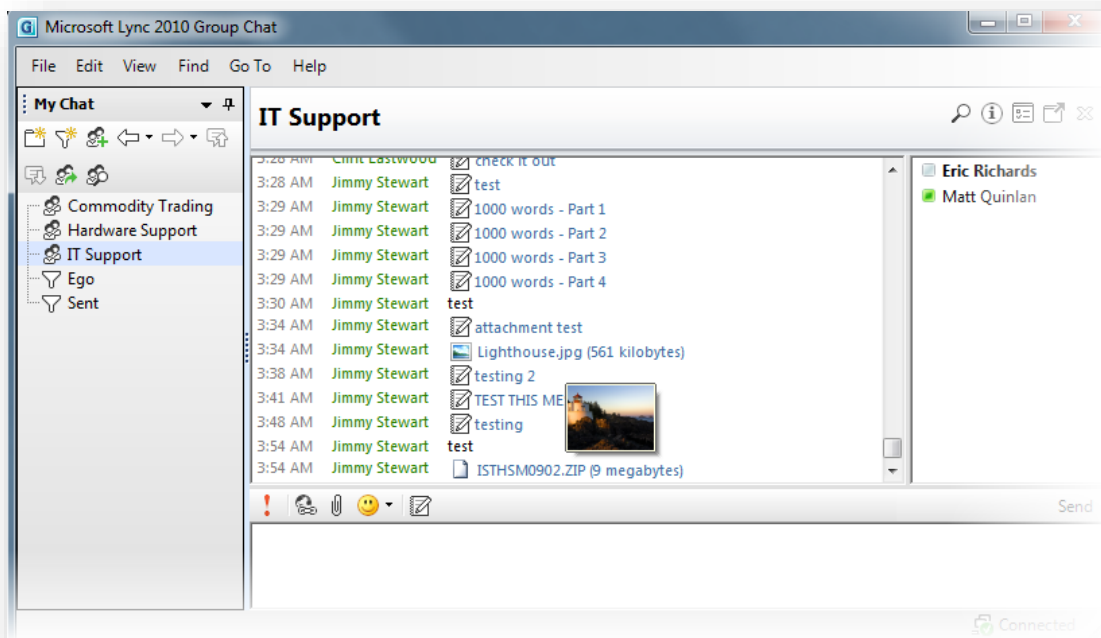


Figure 50: Pictures delivered to a chat room

SENDING EMAILS WITH URL LINK(S)

It is also possible to send an email to a chat room that contains hyperlinks. In many cases, the IM Gateway server will attempt to map hyperlinks to the appropriate structure within the Lync Group Chat room. The Lync Group Chat room will display the link as 'clickable' and the link will be represented with a story structure. In many cases, the IM Gateway will attempt to parse the email message and identify the various 'link' references. In order to explicitly indicate a link, please surround the link with the <> characters.

The following screen shot demonstrates how to send a clickable link to the chat room – this is accomplished by enclosing the link URL with <> characters.

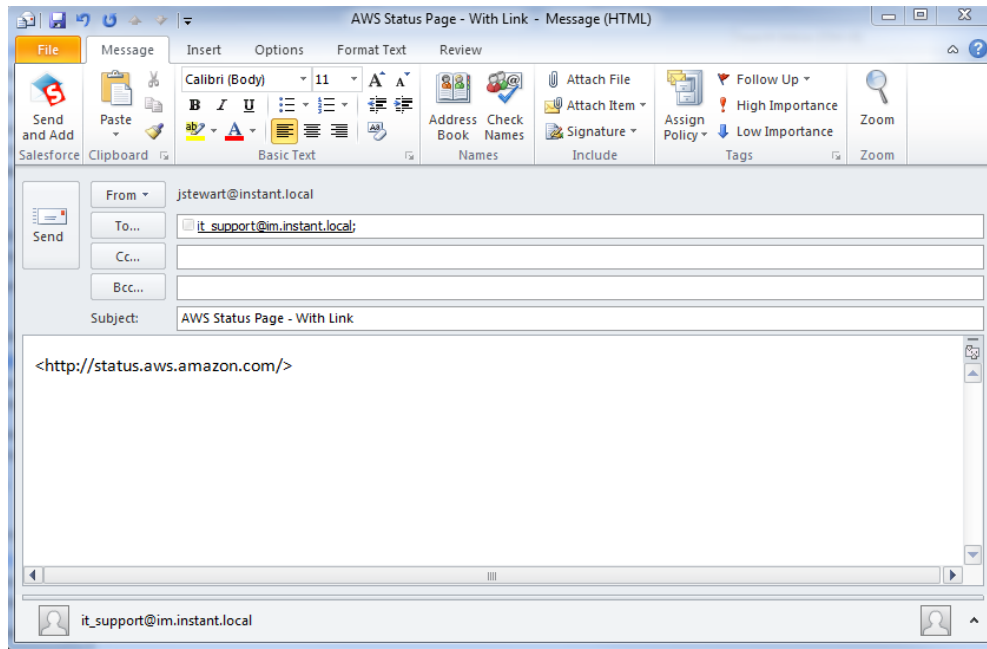


Figure 51: Sending a link in a message

The following screen shot demonstrates how the message will be displayed in the IT Support group chat room:

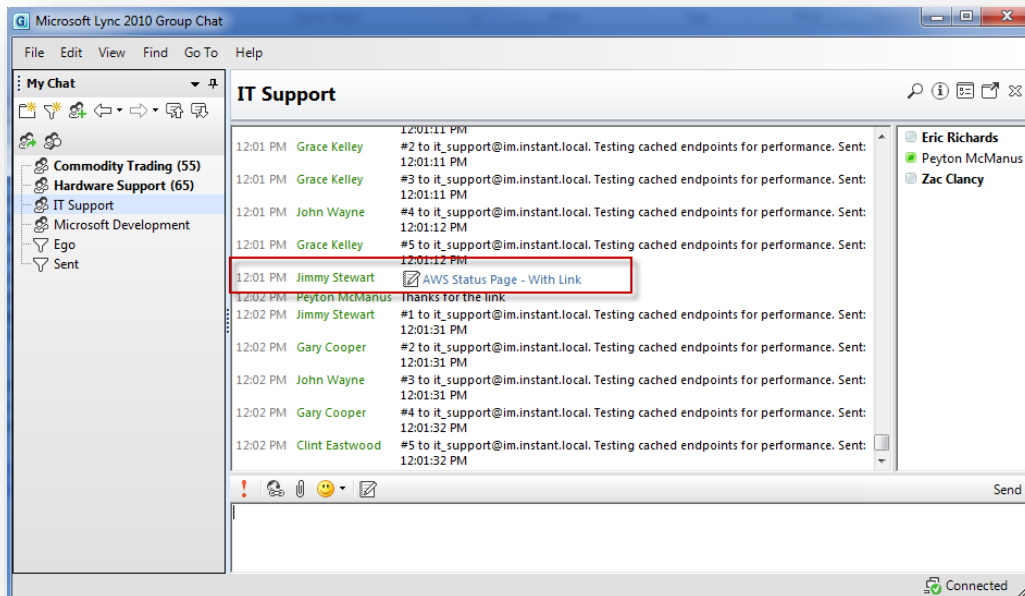


Figure 52: Link formatted in chat

When the story is expanded, or read, then the link will appear as a clickable entity:

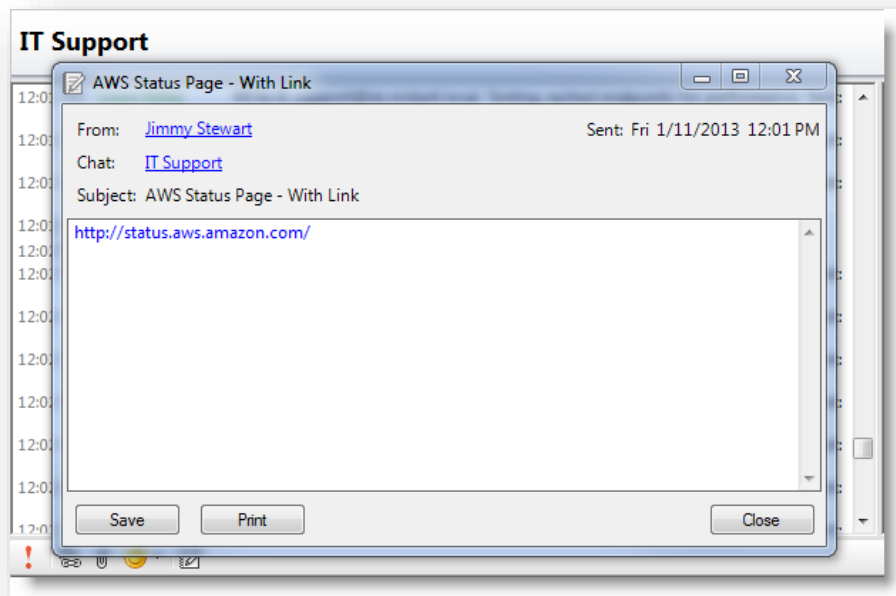


Figure 53: Link displayed in a story

SENDING AN IM TO A USER BY EMAIL

You may send an IM to a user via email with the IM Gateway by composing an email to the user's normal email address, and then prepending the (**im.**) subdomain to the domain portion of the address.

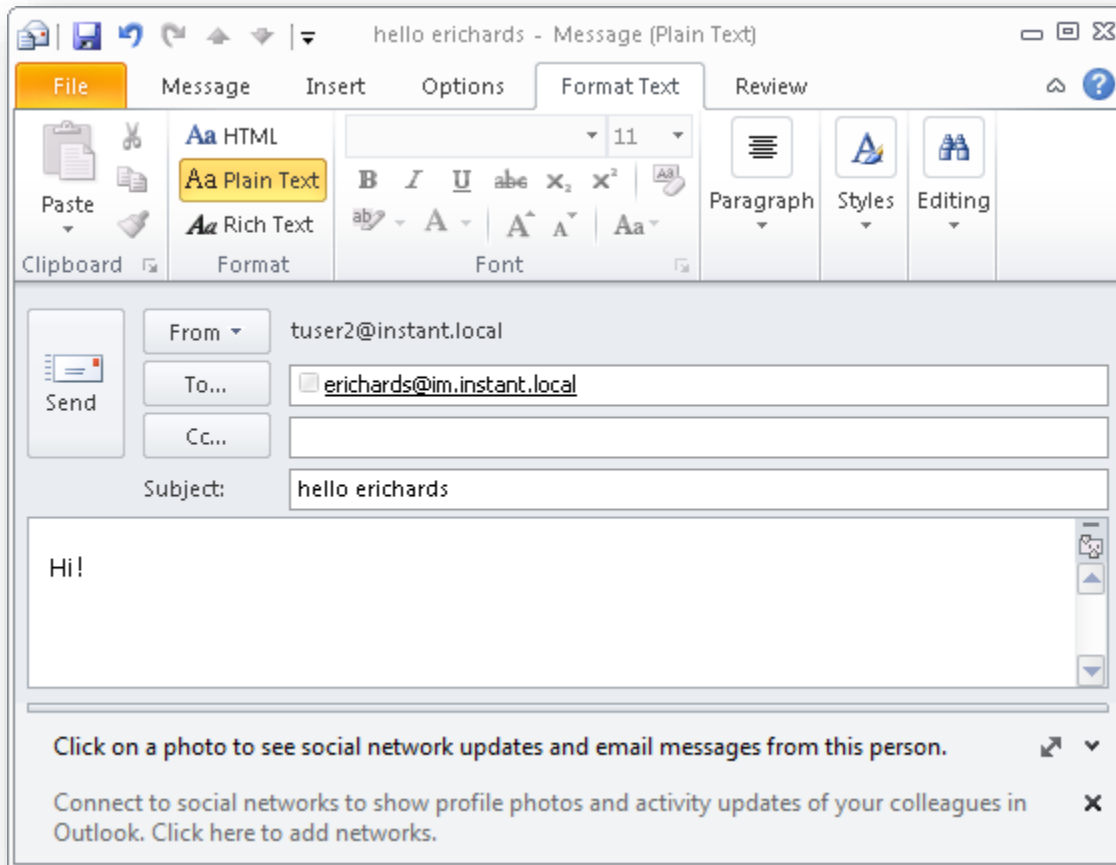


Figure 54: Sending an message to a user

In this example, the following IM will be sent to the user with the email address: erichards@instant.local. In this example, the IM Gateway server will receive the email (since the subdomain im.instant.local was provided) and then the email will be converted to an IM message and dispatched, using the user's SIPURI, to the user in Active Directory who matches the user erichards@instant.local.

These IM alerts are entirely one-way; responses to the messages will not be delivered to the sender of the alert, and if a recipient attempts to reply, they will receive notification that their response will not be delivered.

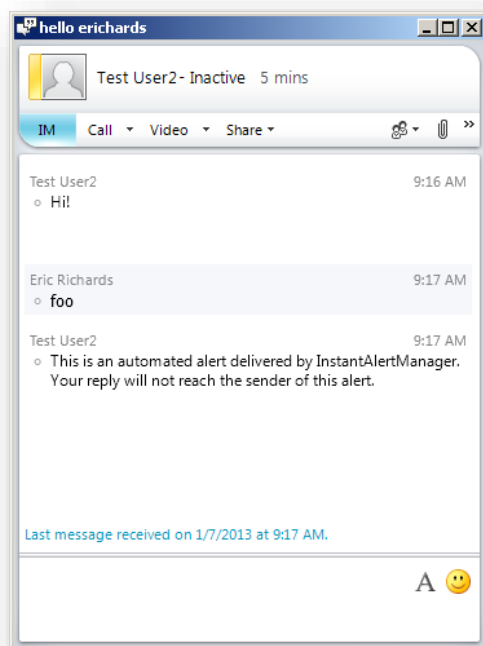


Figure 55: Message delivered to user

SENDING AN IM TO A GROUP OF USERS

In addition to sending an email, and thus an IM, to an individual user, the Instant IM Gateway has the ability to dispatch messages to standard Microsoft Exchange distribution groups. So, the Instant IM Gateway will expand the distribution list, stage the IM messages, and distribute the IM messages to all users within the distribution group.

Distribution lists composed of Lync Group Chat rooms are not supported. In order to send a message to multiple Lync Group Chat rooms, the rooms should be specified as unique email addresses in the email message.

EMAIL RESPONSE TO SENDER

The IM Gateway will automatically acknowledge each email request by providing a return email notification to the original email sender. This email acknowledgement will include information on the status of the request and whether or not the user's SIPURI was located.

The following return receipt indicates that the participant of the original message was located:

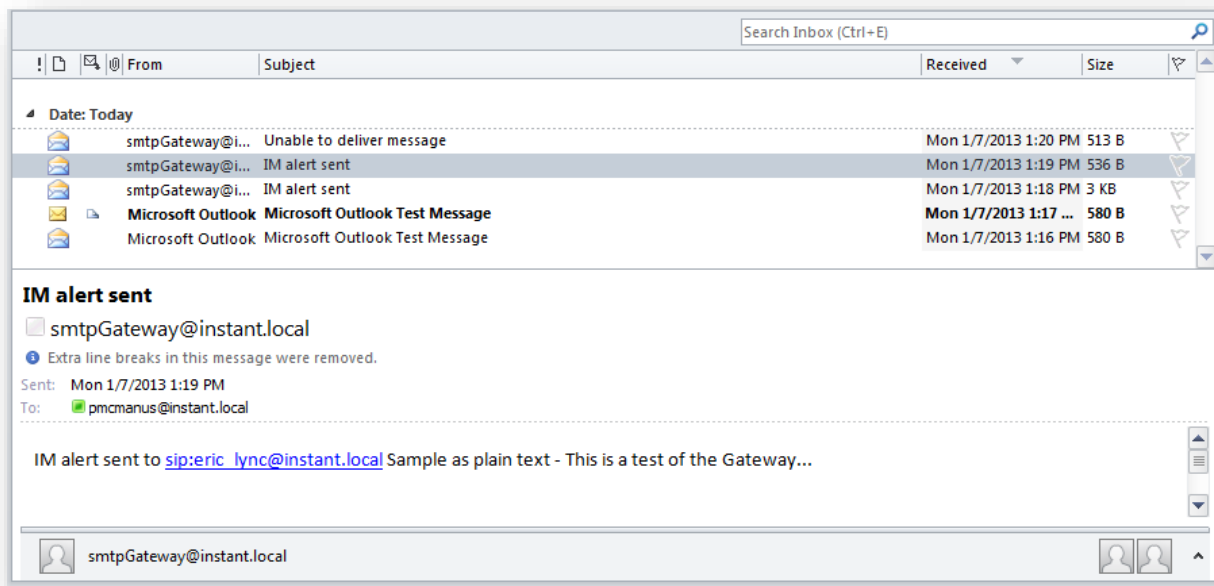


Figure 56: Delivery receipt dispatched by the gateway

If the designated person was not located (i.e. their email address did not resolve against a user in Active Directory and the system was not able to determine a SIPURI in Active Directory), then an email message will be returned indicating that the user was not located in the directory.

For example, the following screen shot demonstrates an email message that is returned from the IM Gateway server if the recipient is not located (i.e. their SIPURI was not located in Active Directory):

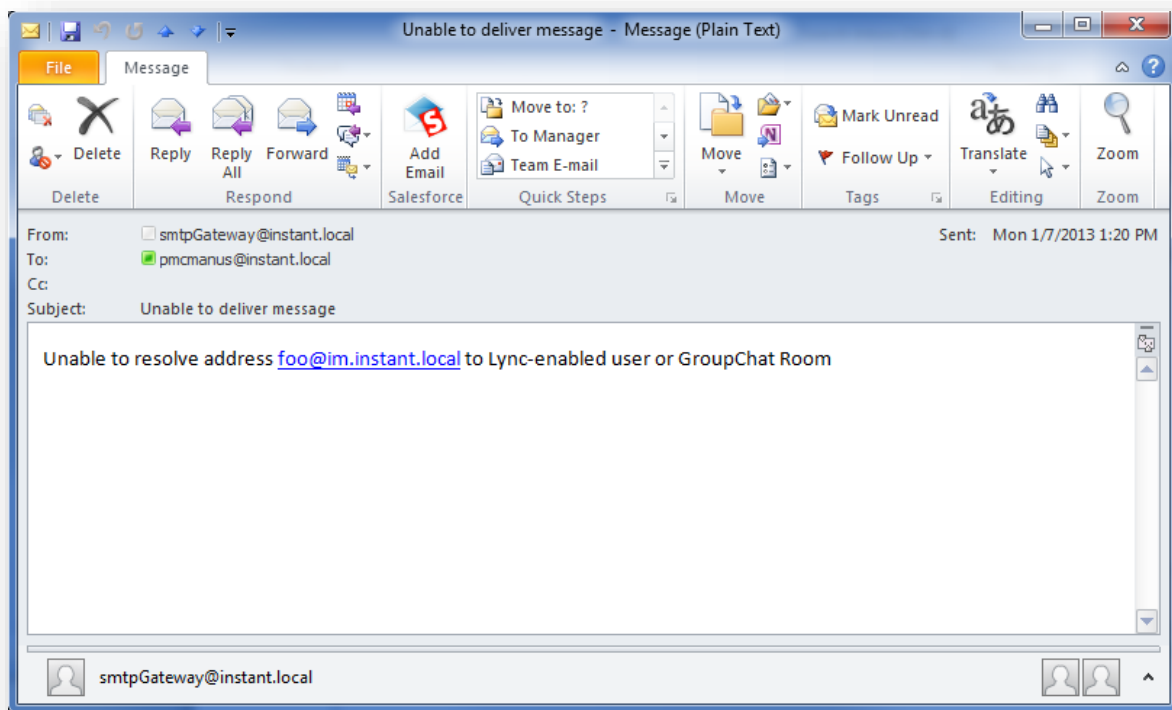


Figure 57: Failed delivery message

CONFIGURATION COMPLETE

The application should now be successfully installed and configured. To access the application, enter
< <http://ServerAddress/alertmanager> > into a web browser.

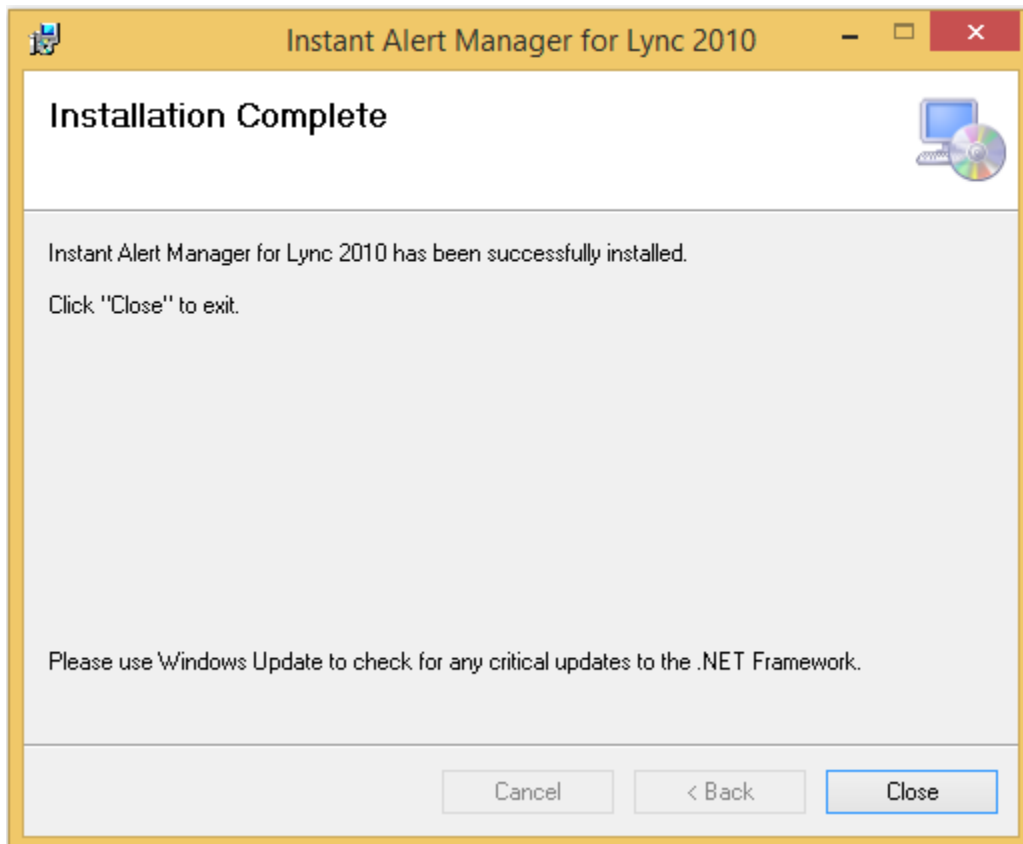


Figure 58: Installation Complete

If you are experiencing any troubles installing, configuring, or accessing the application, contact the Instant Technologies support team:

Support@instant-tech.com

Phone: 1 (800) 884-0443

Intl: +1 (603) 397-3344