HP Enterprise Collaboration

Software Version: 1.0

Enterprise Collaboration Installation and Configuration Guide

Document Release Date: December 2011

Software Release Date: December 2011

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

Introduction

Enterprise Collaboration (EC) is a collaboration platform that enhances and facilitates the collaboration that takes place in almost any flow in the IT organization using HP products. It does this by connecting the structured data managed in various applications in the IT workspace with the unstructured collaboration that supports it.

This guide explains how to install and configure Enterprise Collaboration.

Enterprise Collaboration is installed and configured in the following stages:

1. " Install and Configure Enterprise Collaboration" (on page 9)
2. "Configure the User Repository and User Roles" (on page 21)
3. "Set Up the Integration with Office Communicator Server (OCS)" (on page 24) Perform this procedure if you want to use EC with Office Communicator.
4. "Update EC Configuration" (on page 47) Perform this procedure if you want to make changes to database or OCS settings that were defined during the initial installation, or to configure EC for Office Communicator Server (if you performed the OCS integration setup).
5. "Set Up the Adapter" (on page 50) Perform this procedure if you want EC to support integrations with other applications, for example bringing context objects to conversations or showing facets on an existing context object .
6. "Perform Additional Configuration Steps" (on page 51): Depending on your system setup, you may need to perform some additional configuration steps. See this section if your system meets one or more of the following criteria:
   - Your mail server is accessed using a secure connection and its certificate is self-signed
   - You work with a standalone web application network configuration
   - You work in a reverse proxy network configuration
   - You want to disable redirection to https for authentication (for security reasons, this is not recommended)

HP Enterprise Collaboration Documentation Library

HP Enterprise Collaboration includes the following guides and references available in PDF format. For the latest copies of the HP Enterprise Collaboration documentation, go the HP Software Manuals website: http://h20230.www2.hp.com/selfsolve/manuals. This site requires that you register for an HP Passport and sign in.

Guide	Description
HP Enterprise Collaboration Installation and Configuration Guide	Describes how to install and configure HP Enterprise Collaboration.
HP Enterprise Collaboration Concepts Guide	Provides a detailed overview of HP Enterprise Collaborationi concepts, components, and the conversation workflow.
HP Enterprise Collaboration Integration Guide	Describes how to develop adapters for adding customized

Guide	Description
	application content and how to integrate Enterprise Collaboration into third-party applications.
HP Enterprise Collaboration Developers Guide	Describes how to integrate HP Enterprise Collaborationi into individual customer applications.
HP Enterprise Collaboration Release Notes	Provides last-minute news and information about HP Enterprise Collaborationi.
HP Enterprise Collaboration Support Matrix	Details the HP EC system requirements and lists the HP products and versions which currently come with HP Enterprise Collaboration.
HP Enterprise Collaboration Open Sources and Third-Party Software Agreements	Lists the licenses for open source and third-party components included in HP Enterprise Collaboration.

In addition, you can access the HP Enterprise Collaboration movie from the following location on the DVD:

Documentation\Movies\HPEC_1.wmv

Chapter 1

Install and Configure Enterprise Collaboration

This section includes instructions for the initial installation and configuration of Enterprise Collaboration (EC). If you have already installed EC and want to update the configuration, see the section "Update EC Configuration" (on page 47).

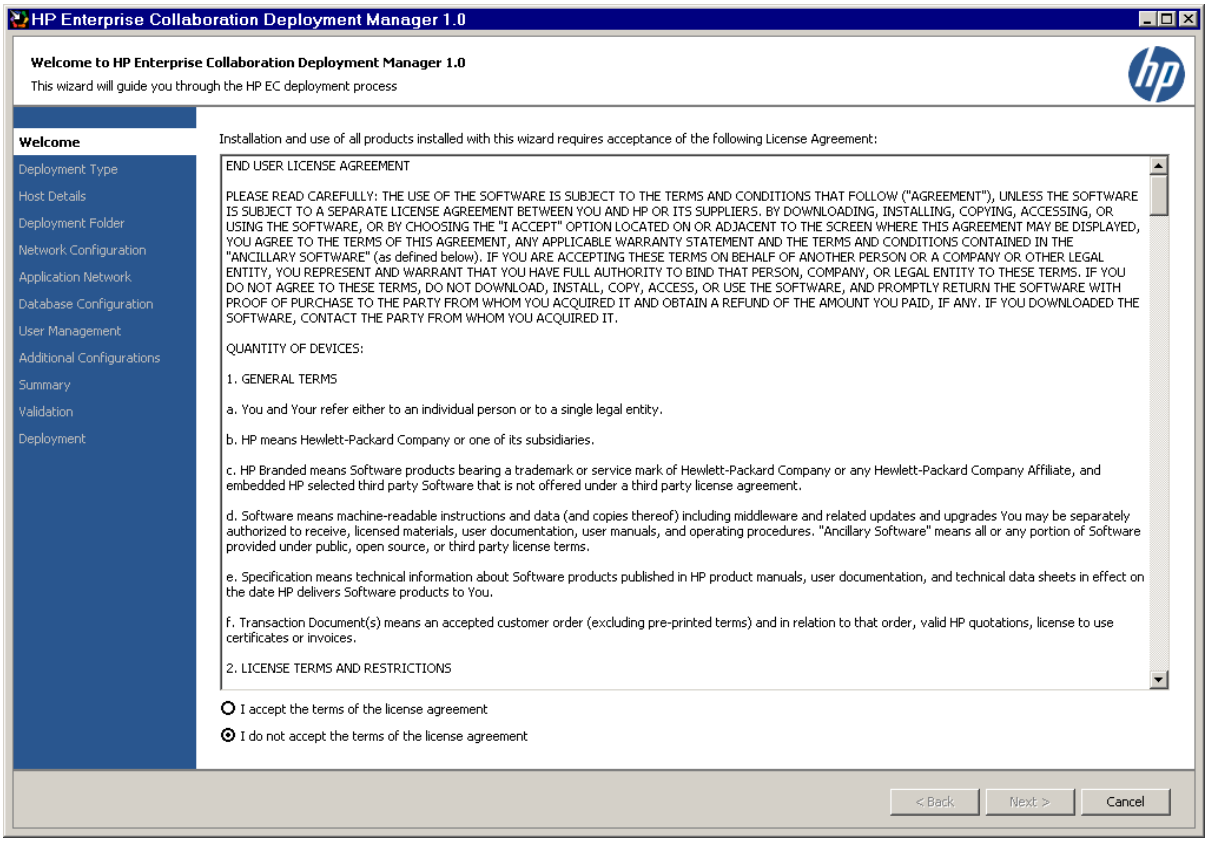
To install Enterprise Collaboration:

1. **If you are downloading the EC installation .zip file from the HP website:** Extract the contents of the EC installation **.zip** file to any location that has access to all EC topology entities(such as MSSQL or optional entities such as the mail server or OCS) that EC communicates with.

   If you are installing from a DVD: Copy the entire contents of the DVD to a directory on your hard drive.

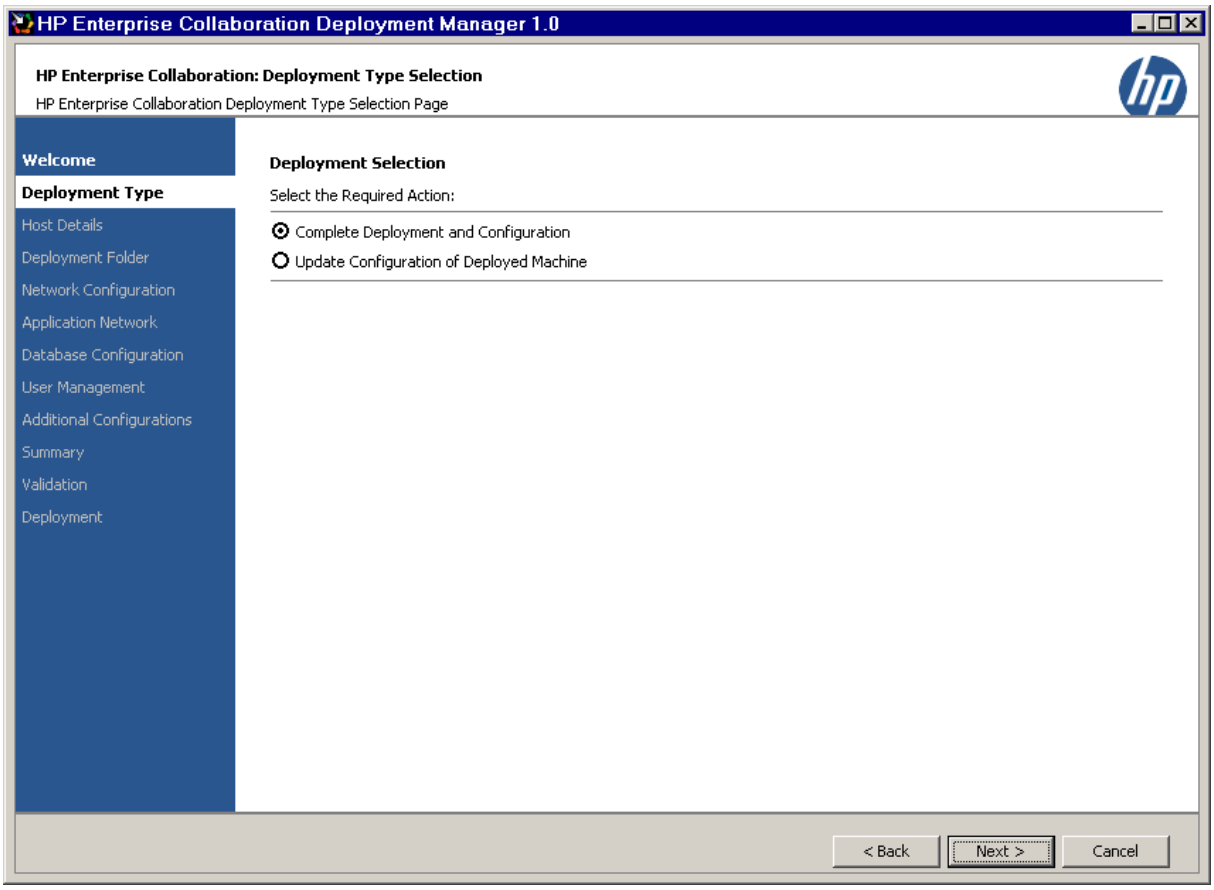
2. Open the folder **Windows_Setup** and double-click **EC.exe**.

3. The Enterprise Collaboration Deployment Manager wizard opens.



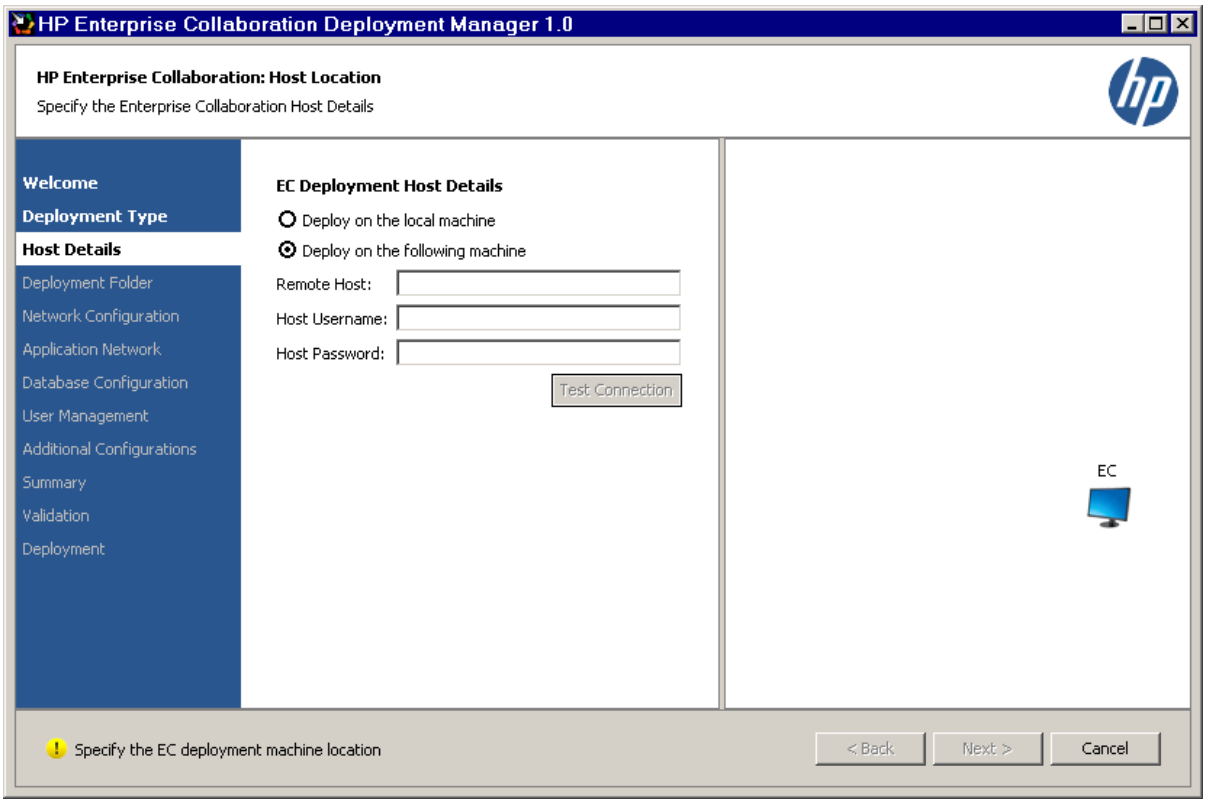
   Read the license agreement. Select “I accept the terms of the license agreement”. Click Next.

4. The Deployment Type Selection page opens.



Select “Complete Deployment and Configuration”. Click **Next**.

5. The EC Deployment Host Details page opens.



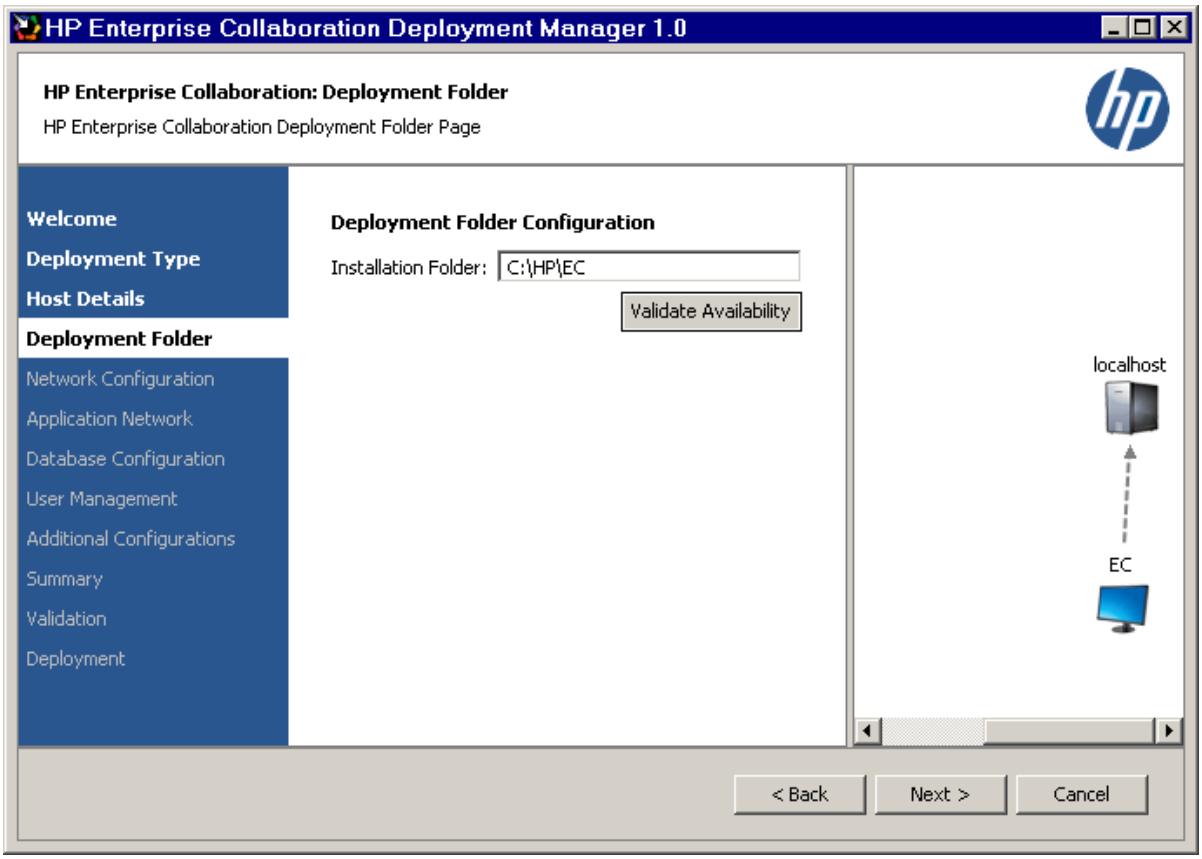
Select either “Deploy on the local machine” or “Deploy on the following machine”.

- If you choose “Deploy on the local machine”. Click **Next**.
- If you choose “Deploy on the following machine”, enter details for the Remote Host location, Host Username, and (optional) Host Password. Click **Next**.

Note:

- If you deploy on a Remote Host Location, you can click the Test Connection button at this point to test the connection between your PC and the Remote Host Location. This test is not required, but is recommended.
- Once you have chosen a machine for deployment, from this stage on you can hover over the server machine icon on each wizard page with the mouse arrow to display a pop-up of validation information (such as memory requirements, available ports, etc). If during the configuration process you enter data that affects these validations (for example selecting port that is already in use on the machine), then a red ‘X’ will be displayed on the server machine, and the pop-up shows the conflicted port.

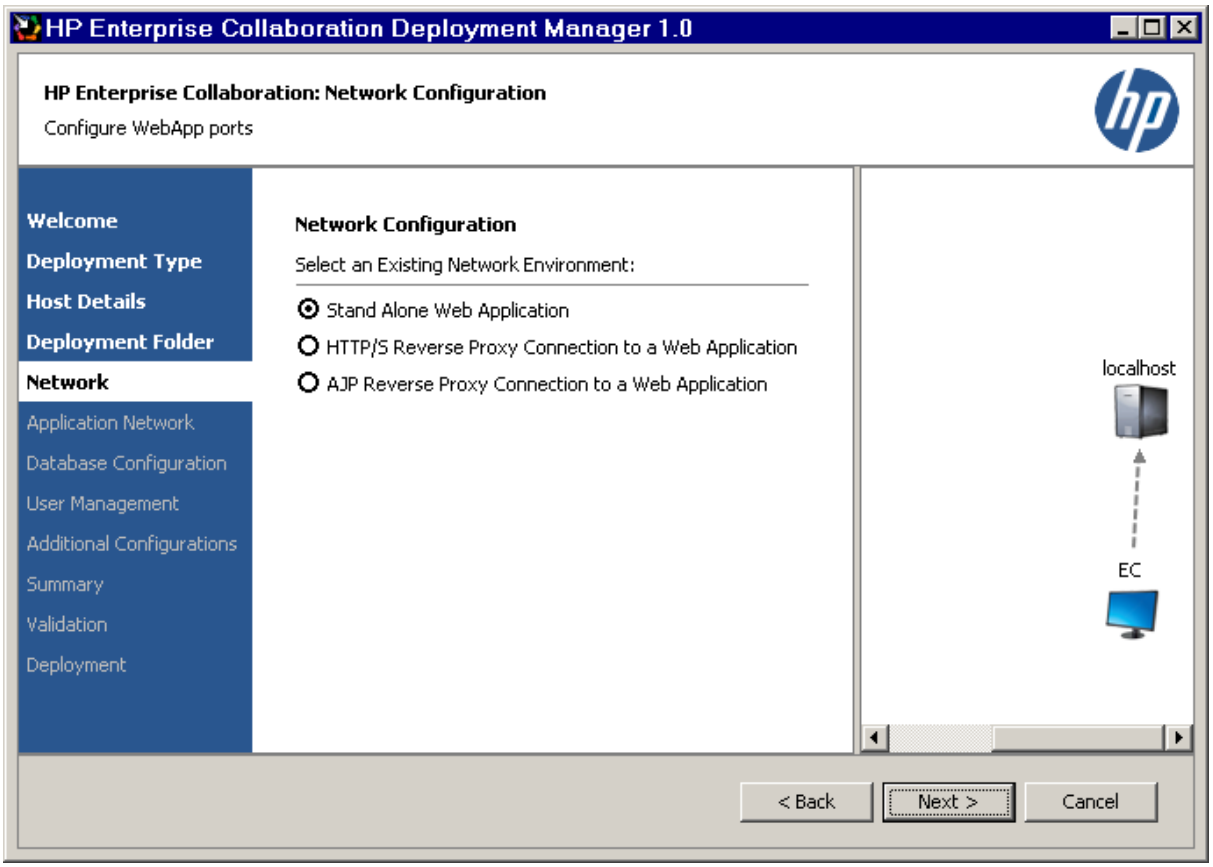
6. The Deployment Folder Configuration page opens.



Enter a path for the installation folder or use the default path. Click **Next**.

> **Note:** To check if the installation folder path is valid, click the Validate Availability button. This checks if the folder path already exists and can prevent content override. This check is optional, but recommended.

7. The Network Configuration page opens.



a. Select one of the following Network Environments:

- Stand Alone Web Application
- HTTP/S Reverse Proxy Connection to a Web Application
- AJP Reverse Proxy Connection to a Web Application

> **Note:** For more information regarding the possible network environment configurations, see the diagrams in "Appendix A: Network Configuration Schemas for HP Enterprise Collaboration" (on page 53).

b. Click **Next**.

8. Depending on the network environment you chose, one of the following pages opens:

- Stand Alone Application Configuration
- HTTP/S Reverse Proxy Configuration
- AJP Reverse Proxy Configuration

a. If you want to allow only a secure connection to the web application even after the login authentication stage, select **Use a Secure Connection to connect to the Web Application.** By default, a secure connection is used for login authentication. After login authentication, the client will continue with the same level of security it uses to access the

web application.

> **Note:** Using a secure connection to connect to the web application may affect performance due to use of SSL for all connections.

b. Enter the following information in the relevant network configuration page:

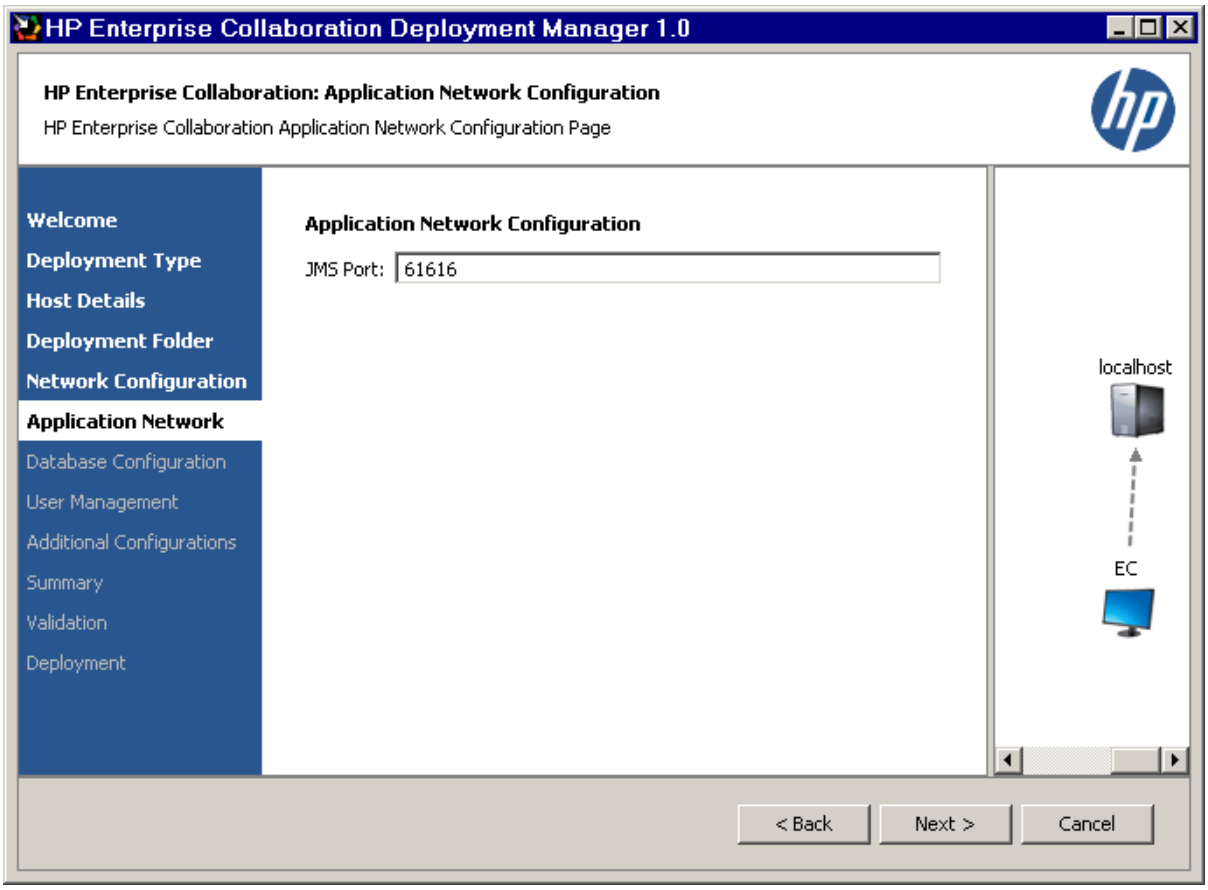
- **FQDN:** Enter the FQDN of the web application or reverse proxy. If you are performing the Stand Alone Application configuration, the a default value is the FQDN of the deployed machine.

  > **Note:** After entering the FQDN, you can have the wizard automatically enter the IP Address and Domain Name by clicking the **Fill IP/Domain** button.

- **IP Address:** Enter the IP address of the web application or reverse proxy. If you are performing the Stand Alone Application configuration, the default value is the IP address of the deployed machine.
- **Domain Name:** Enter the Domain name of the web application or reverse proxy. If you are performing the Stand Alone Application configuration, the default value is the Domain name of the deployed machine.
- **HTTP Port (for Web Application):** The default value is 8080.
- **HTTPS Port (for Web Application):** The default value is 8443 (this port is not relevant for the AJP Reverse Proxy).
- **HTTP Port (for Reverse Proxy):** The default value is 8080.
- **HTTPS Port (for Reverse Proxy):** The default value is 8443.
- **AJP Port (non-secure connection):** For AJP Reverse Proxy only. The default value is 8009.
- **AJP Port (secure connection):** For AJP Reverse Proxy only. The default value is 8109.

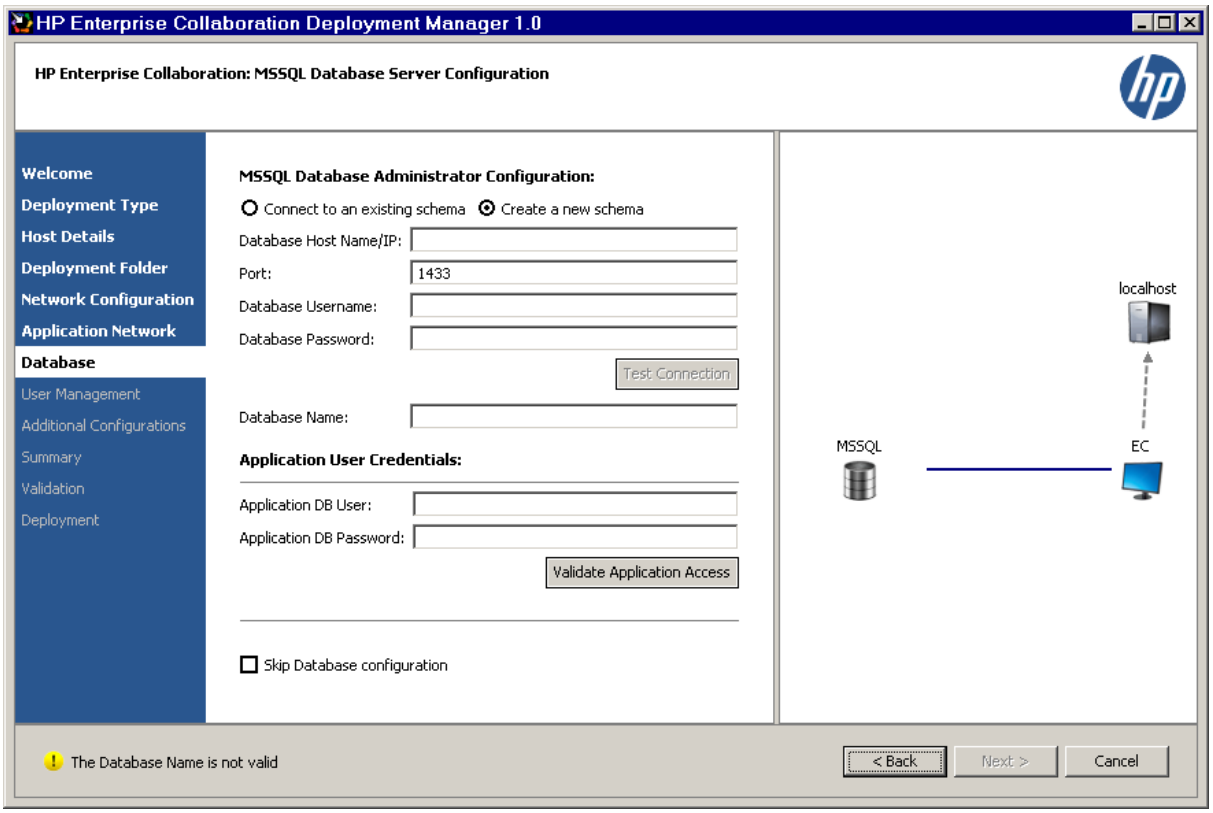
c. Click **Next**.

9. The Application Network Configuration page opens.



Enter a value for JMS Port or use the default value of 61616. Click **Next**.

10. The MSSQL Database Server Configuration page opens.



a. Configure the MSSQL Database Administrator:
   - Select either **Connect to an existing schema** or **Create a new schema**.
   - Enter the following information:
     - **Database Host Name/IP**
     - **Port:** A default value of 1433 appears.

       Note: Supported database credentials are in SQL Authentication format.

     - **Database Username:** Select a user name with administrator permissions, including create permission.
     - **Database Password**
   - Click the **Test Connection** button after entering the information above.

     Note: If the test fails, you must modify the information you entered on this page, or select 'Skip Database configuration'.

   - **Database Name**: If you selected c**Connect to an existing schema**, enter the name of the database to connect to. If you chose **Create a new schema**, enter the name of the new database.

b. Enter Application User Credentials:

Application DB User: This user name is used by the application to communicate with the database.

Application DB Password: This password is used by the application to communicate with the database.

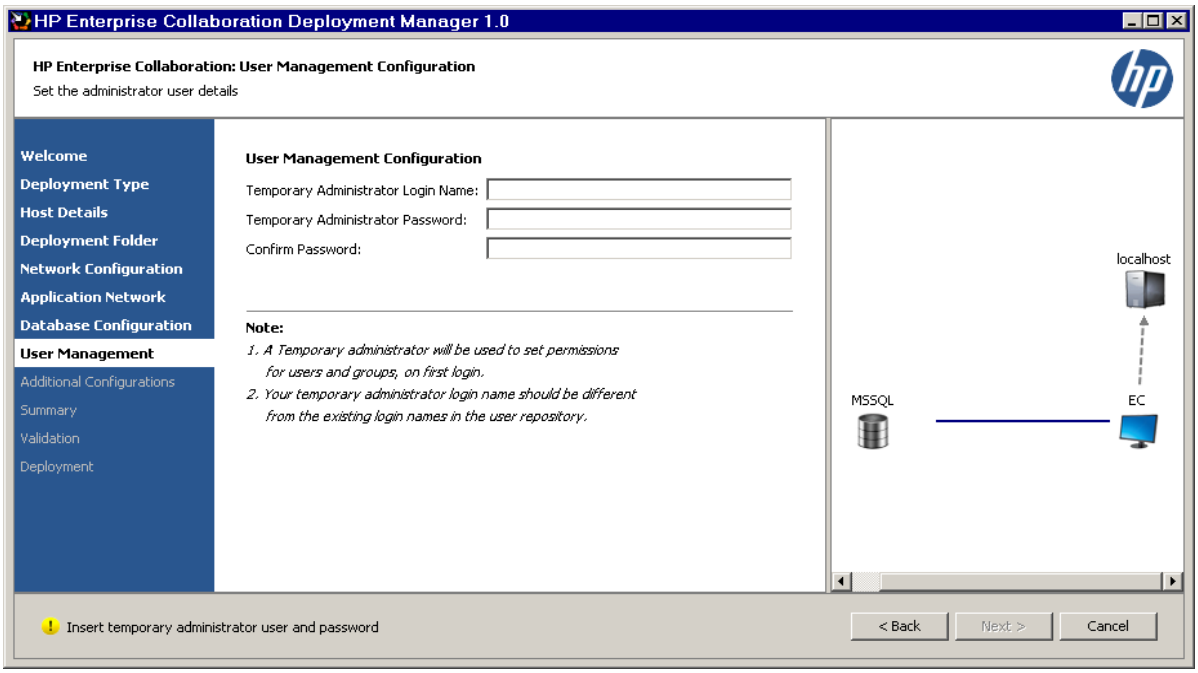
c. Click the **Validate Application Access** button.

> **Note:** If this validation fails, you must validate your user credentials.

d. Click **Next.**

11. The User Management Configuration page opens.

> **Note:** If you skip database configuration, the User Management Configuration page is automatically skipped.

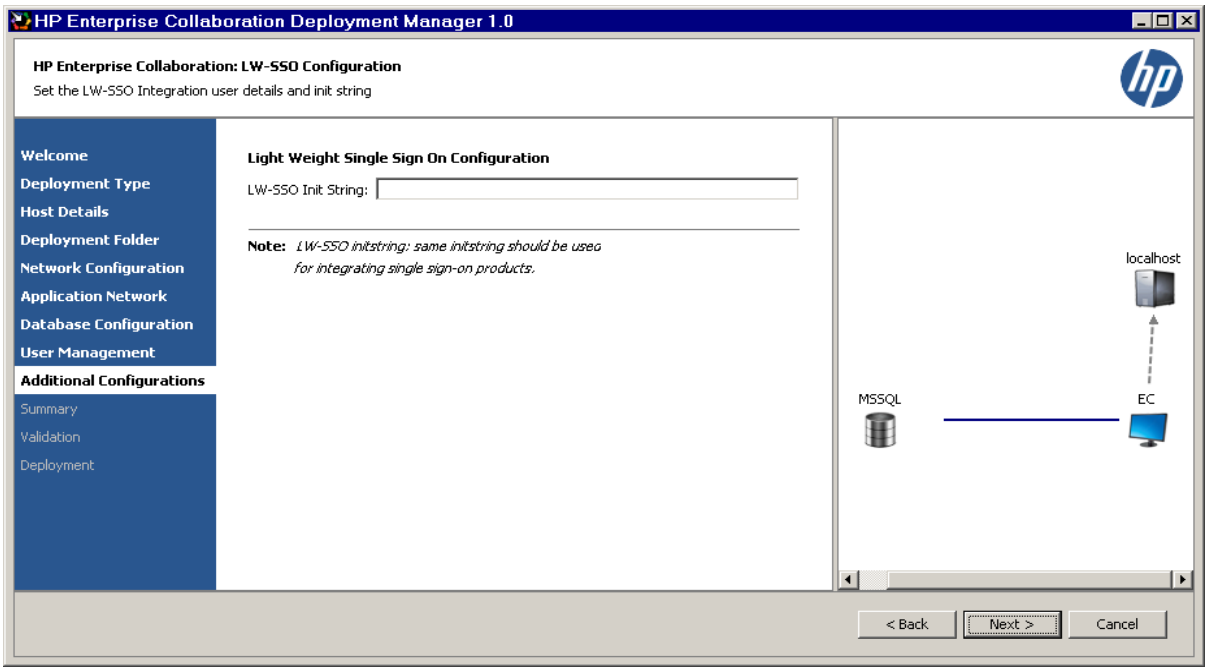


a. Enter the following information:

- **Temporary Administrator Login Name:** This login name should not exist in your existing user repository.
- **Temporary Administrator Password**
- **Confirm Password**

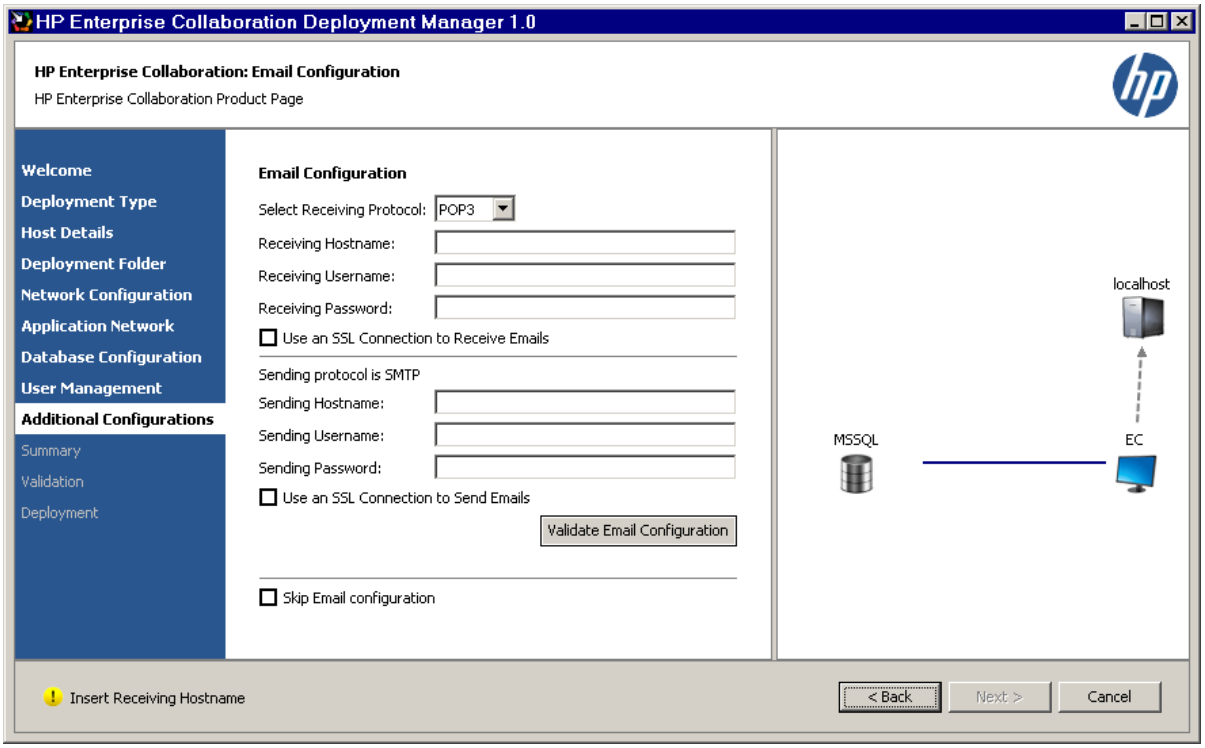
b. Click **Next**.

12. The Light Weight Single Sign On (LW-SSO) configuration page appears.



Enter the LW-SSO Init String and click **Next**.

13. The Email Configuration page opens.



a. Enter the following information:
   - **Select Receiving Protocol:** From the drop down list, choose either POP3 or IMAP4.
   - **Receiving Hostname**
   - **Receiving Username**
   - **Receiving Password**
   - **Sending Hostname**
   - **Sending Username**
   - **Sending Password**

   Note: The supported Sending Protocol is SMTP.

b. If your receiving protocol is secured, select 'Use an SSL Connection to Receive Emails'.

c. If your sending protocol is secured, select 'Use an SSL Connection to Send Emails'.

d. **Optional:** Test the Email configuration by clicking the "Validate Email Configuration" button after entering all the configuration settings.

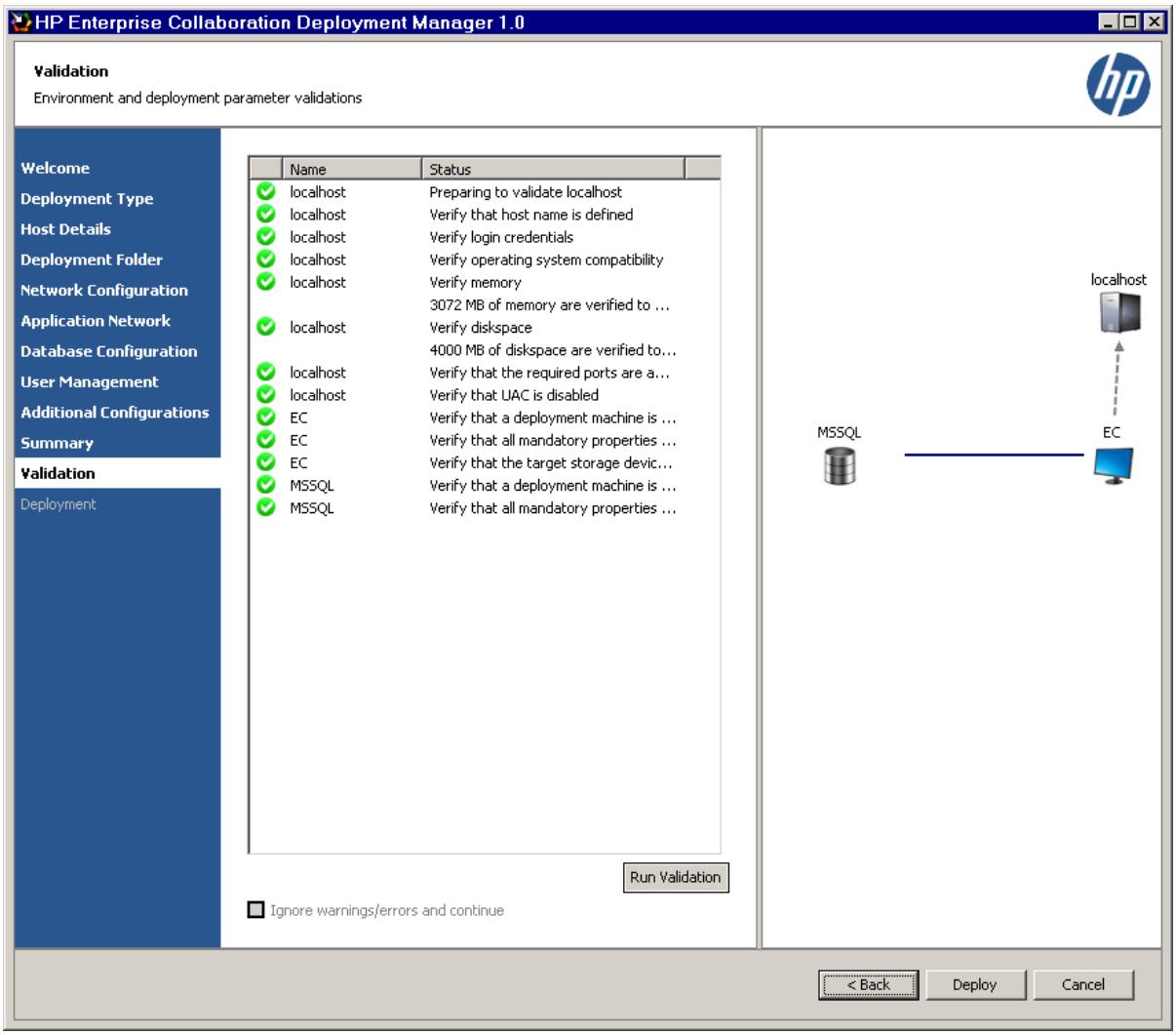
e. Click **Next**.

Note: All the information you enter in the Email Configuration page is optional. You can skip this page by selecting "Skip Email configuration".

14. The Summary page opens.

    In the Summary page, review all the information that you entered. If you want to change anything, click the **Back** button to return to the page where you want to make the change. If all the information is correct, click **Next**.

15. The Validation page opens.



Validation occurs automatically when clicking **Next** in the Summary page.

- If all icons are green, validation was successful.
- If one or more icons are red, there is a problem with the configuration or you skipped the database setup. You can choose to ignore the warning by selecting "Ignore warnings/errors and continue", or fix the problem and then click the **Run Validation** button in order to test if the configuration problem was properly fixed.

16. Click **Deploy**.
17. Wait for deployment to finish (follow the progress bar), and click **Finish**.

    After successful deployment, the following shortcuts appear in the Programs menu, under the HP EC folder:

    - Start HP EC
    - Stop HP EC
    - Uninstall HP EC

Chapter 2

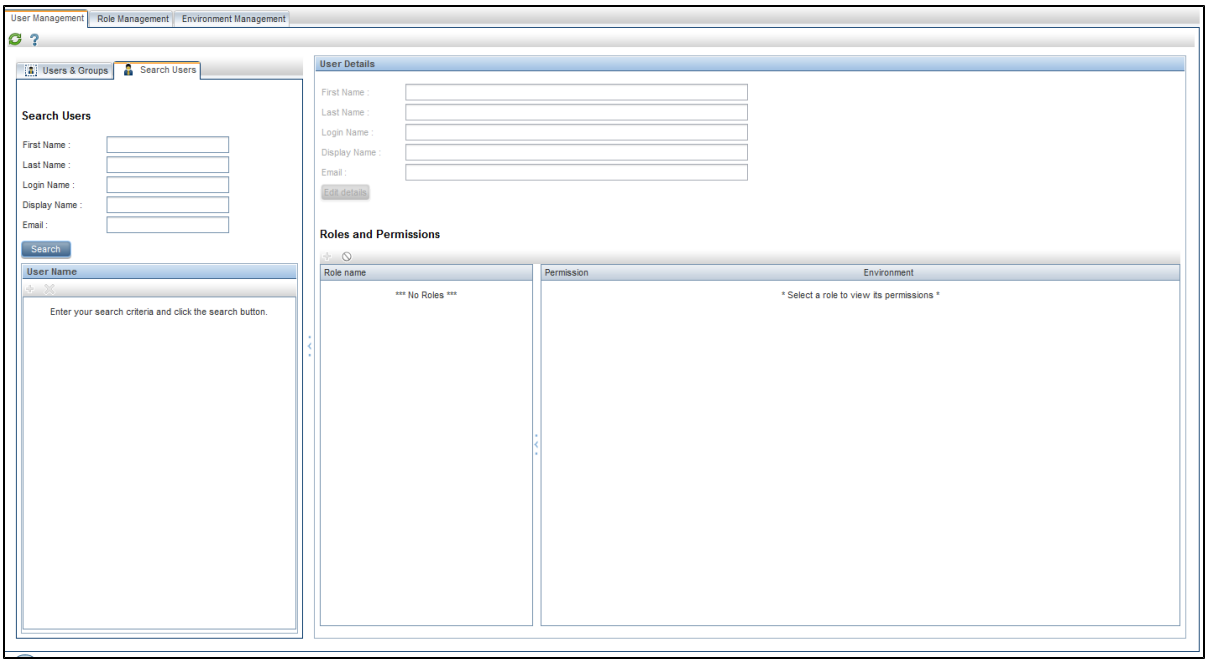
Configure the User Repository and User Roles

After completing installation, you must configure the user repository and user roles. Without completing these steps, you will not be able to login to EC.

To configure the user repository and user roles, perform the following steps:

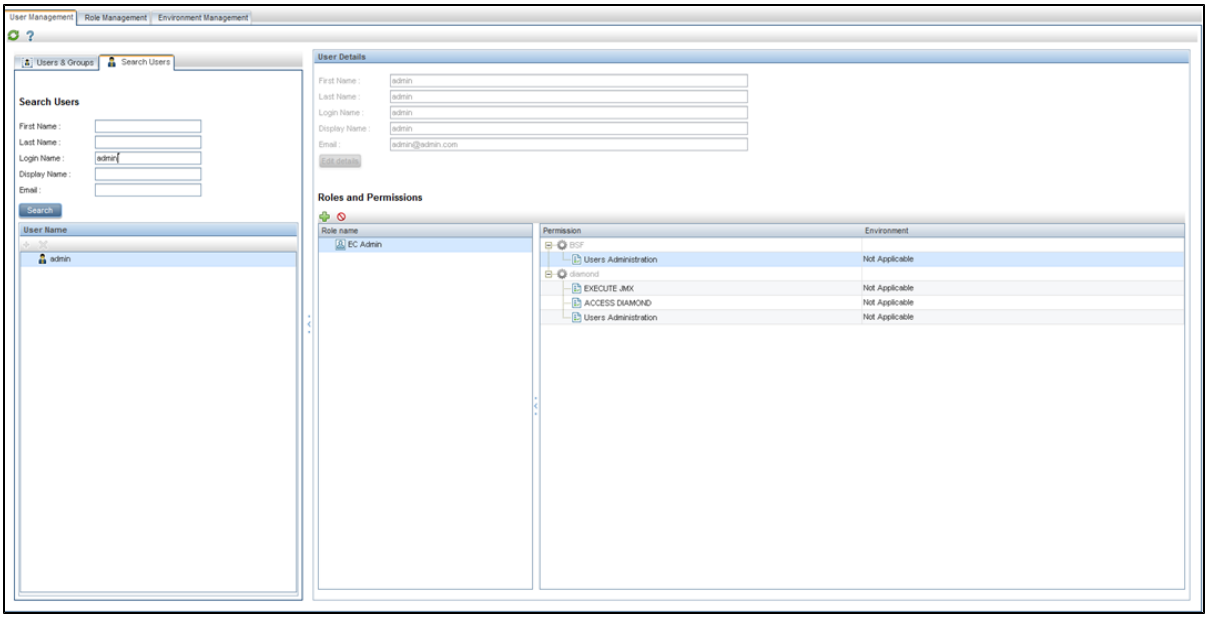
1. Update the external-ldap.properties file located in the /conf directory, according to the instructions in "Appendix B: Updating the external-ldap.properties File" (on page 54).
2. **Optional:** If you are using LDAP over SSL, import your LDAP server certificate to the keystore by executing the following batch file:

   C:\HP\EC\diamond-deploy\set-ldap-certificate.bat <path_of_certificate_file>
3. In the **bsf.properties** file located in the **\conf** folder, set the following properties with the values listed below and save the changes:
   - authentication.provider=SHARED
   - personalization.provider=SHARED
   - users.provider=EXTERNAL
   - groups.provider=EXTERNAL
   - roles.provider=SHARED
   - roles.relations.provider=SHARED
4. Start EC by going to **Program Menu->HP EC-> Start HP EC icon**.
5. Open the User Management UI located at: **http://<Server FQDN>:<port>/bsf**
6. Log in using your temporary administrator user credentials as you defined during the installation process.
7. The User Management UI opens.



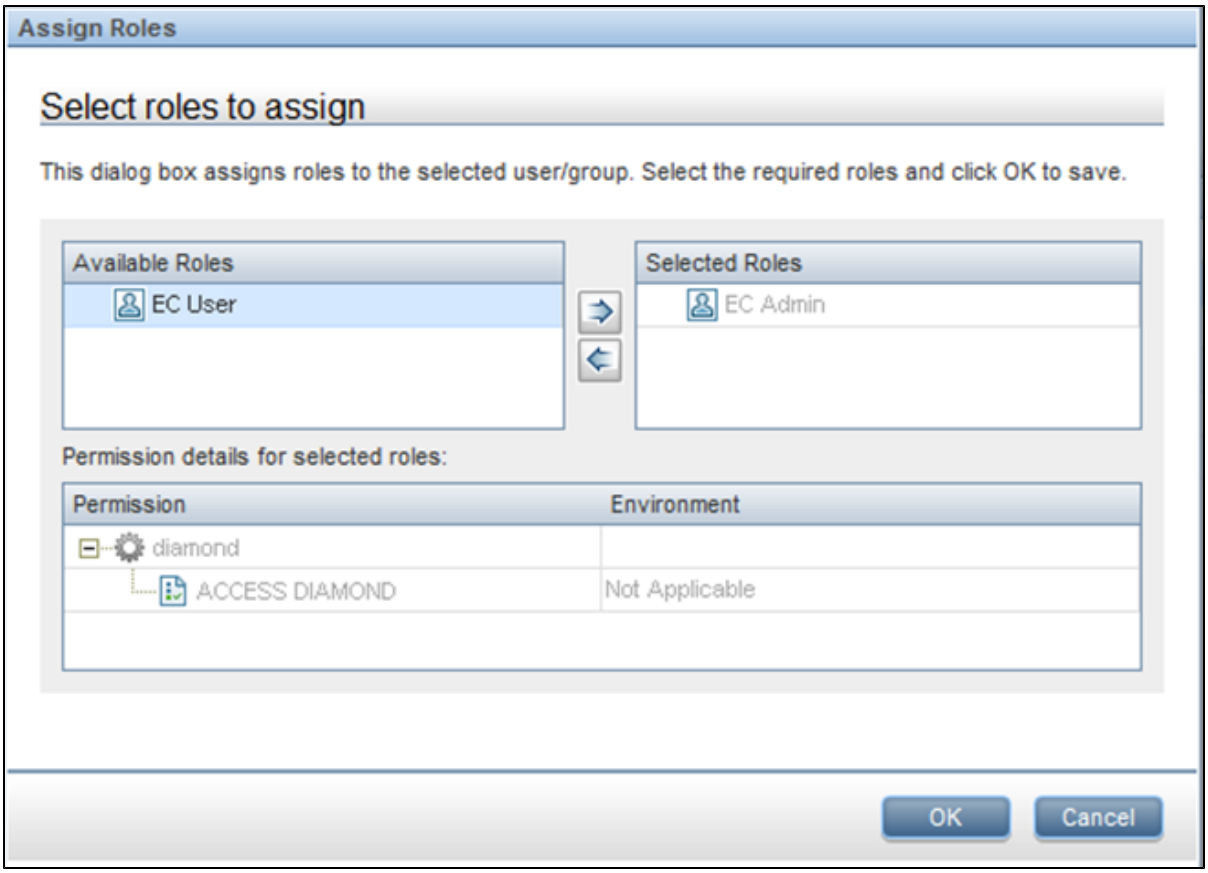
In the User Management section, find the relevant users and/or groups. For example, to find a user click on the Search Users tab, enter the search details. Click the **Search** button.

8. A list of users and/or groups matching the search details appears in the Roles and Permissions section.



Select the relevant user. Click on the Add Role icon ( ).

9. The Assign Roles dialog box opens.



Add the following roles to the user:

- EC Admin: For permission to access EC, JMX, and User Management
- EC User: For permission to access EC

> **Note:** It is important to set at least one EC Admin user to have access to the User Management UI and the JMX.

10. Stop EC by going to **Program Menu->HP EC-> Stop HP EC icon**.
11. Update the **bsf.properties** file as follows:
    - authentication.provider=EXTERNAL
    - personalization.provider=SHARED
    - users.provider=EXTERNAL
    - groups.provider=EXTERNAL
    - roles.provider=SHARED
    - roles.relations.provider=SHARED
12. Restart EC by going to **Program Menu->HP EC-> Start HP EC icon**.

Chapter 3

Set Up the Integration with Office Communicator Server (OCS)

Preconditions

- The OCS Server port should be open for communication from OCS agent machine.
- The domain user performing OCS agent setup should be a member of the RTCUniversalServerAdmins group and a member of the Local/Administrators group on the OCS agent machine.

Install the UCMA SDK

To install the Microsoft UCMA 2.0 SDK:

1. Go to the MSDN Download Center at **http://go.microsoft.com/fwlink/?LinkID=139195**.
2. Download and run the **UcmaSdkWebDownload.msi** file. This installs the component SDKs and other supporting resources on your local drive. By default, all of the files are installed in the **<C:\Microsoft Unified Communications Managed API 2.0 SDK Installer Package>** folder.
3. Go to the Installer Package folder on the local drive and navigate to the **SetupUCMASdk.exe** file. Double-click this file to start the SDK installation. In the last step of the installation, follow the Language Pack Download link to install at least one speech language package. The language pack is required by the UCMA Workflow application.

Install the Root Certificate Authority (CA) Certificate

Note: The instructions in this section are written for the Microsoft CA Issuer. If you are using a different issuing system, these instructions can serve as a basis for installing the Root CA Certificate, but are not exact.

There are two stages in installing the Root CA Certificate, which are:

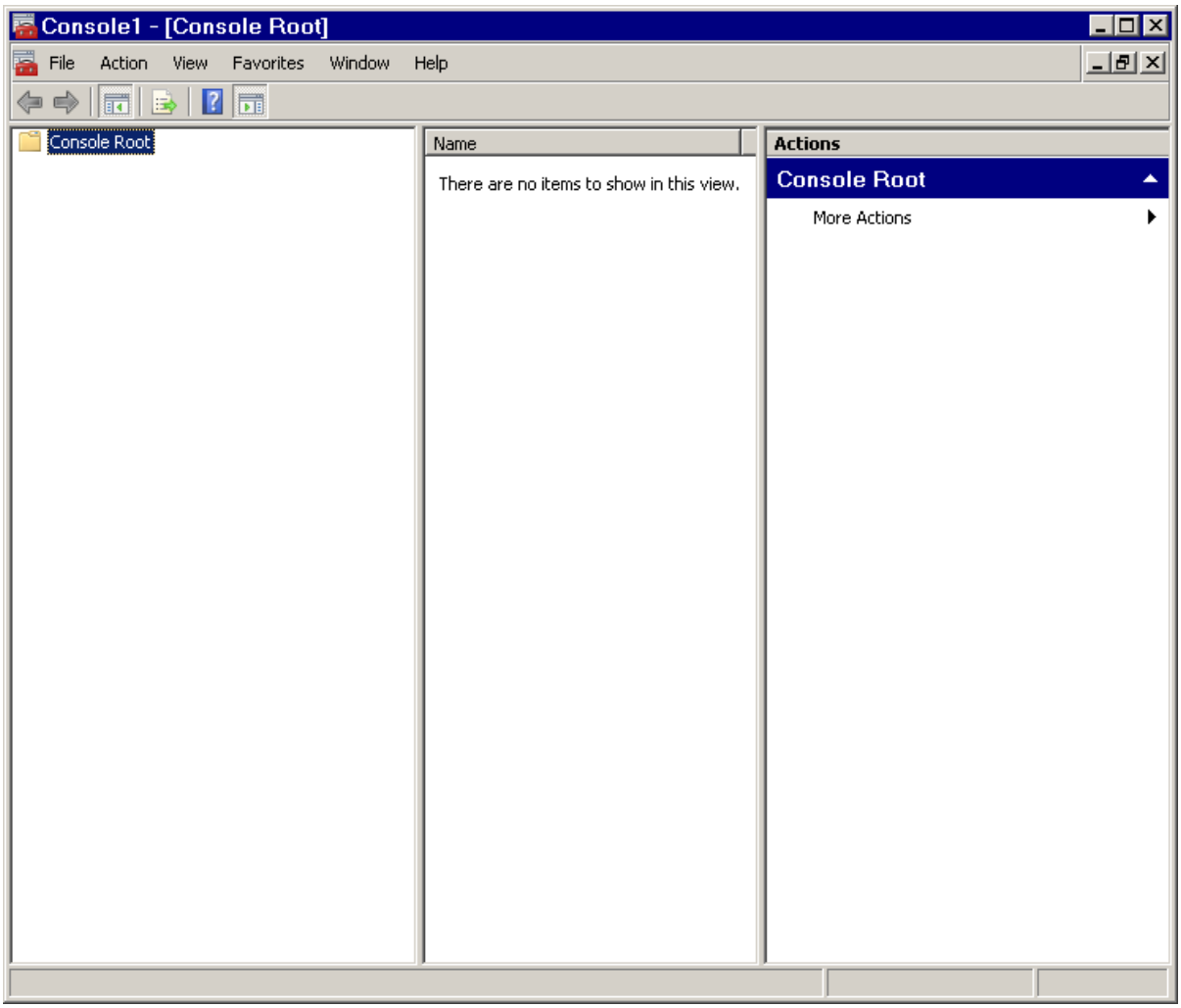
- "Check Which CA Is Used by the OCS" (on page 24)
- "Download and Install the Root CA Certificate" (on page 29)

If you already know the URL of the CA, you can skip the first stage and go directly to the second stage.

Check Which CA Is Used by the OCS

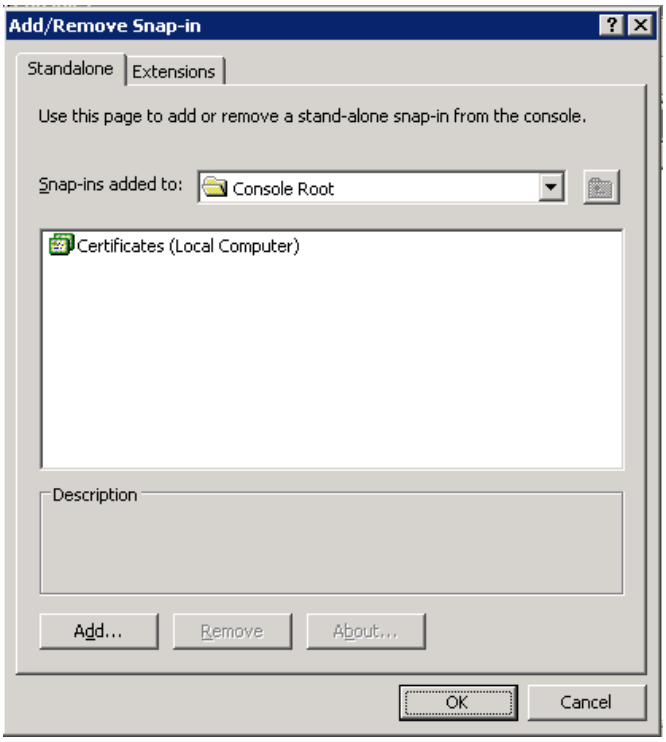
To check which CA is used by the OCS:

1. Login to the OCS server and run **mmc.exe**.
2. The Console Root opens.



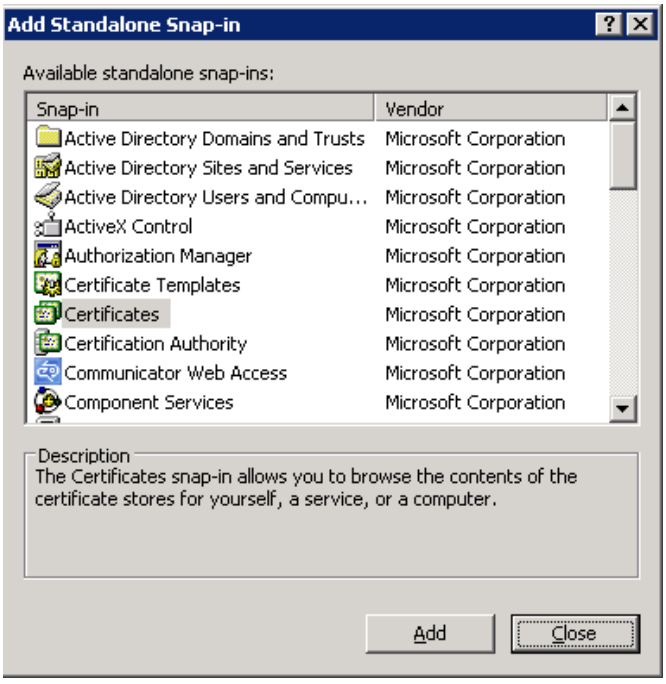
In the **Console Root**, go to **File>Add/Remove Snap-in**.

3. The **Add/Remove Snap-In** dialog opens.

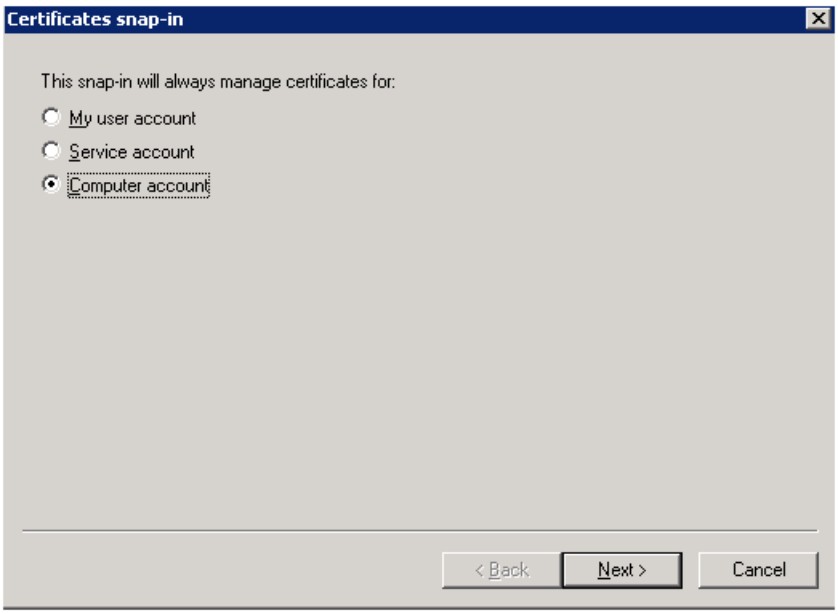


Select **Certificates**. Click **Add**.

4. The **Add Standalone Snap-In** dialog opens. Click **Add**.

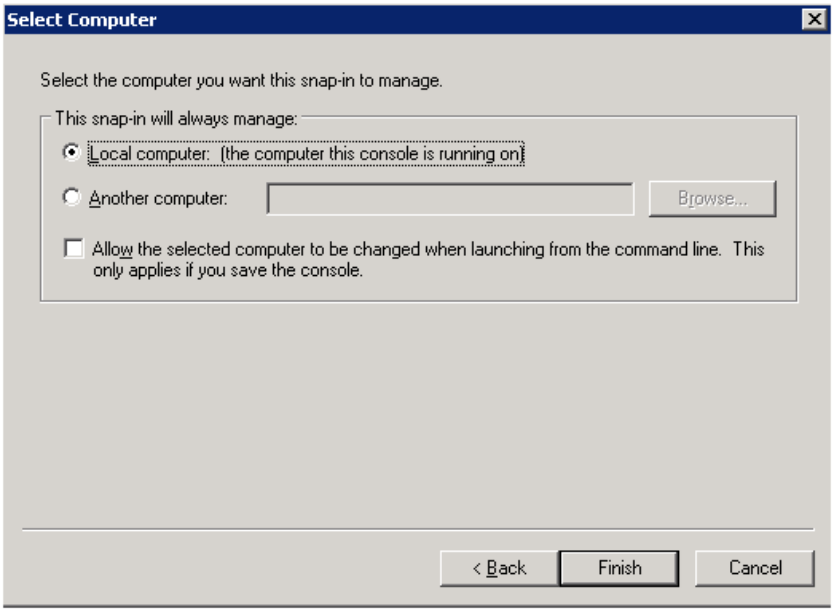


5. The **Certificates snap-in** dialog opens.



Select **Computer Account**. Click **Next**

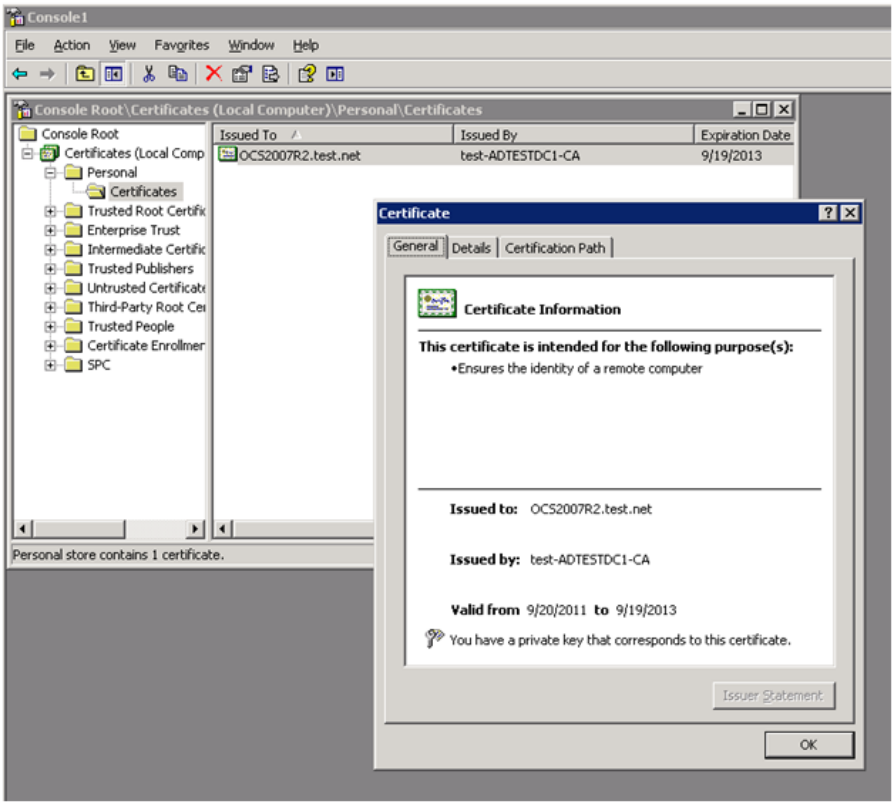
6. The **Select Computer** dialog opens.



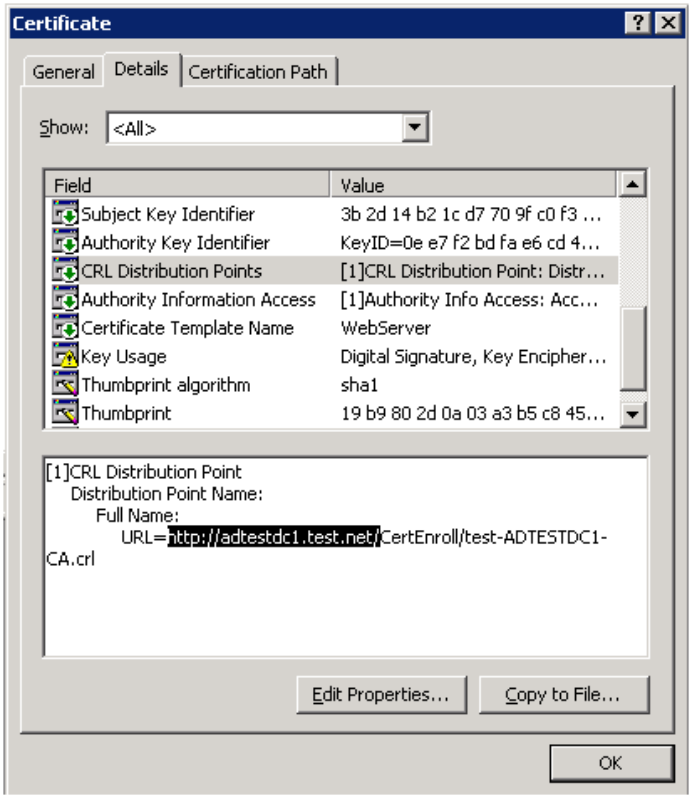
Select **Local Computer**. Click **Finish**.

7. The **Add Standalone Snap-In** dialog opens again. Click **Close**.
8. The **Add/Remove Snap-In** dialog opens again. Click **OK**.
9. The **Console Root** opens again.

   Go to **Personal>Certificates** (see below) to see the Root CA certificate and which CA issued it.



10. Go to the **Details** tab.

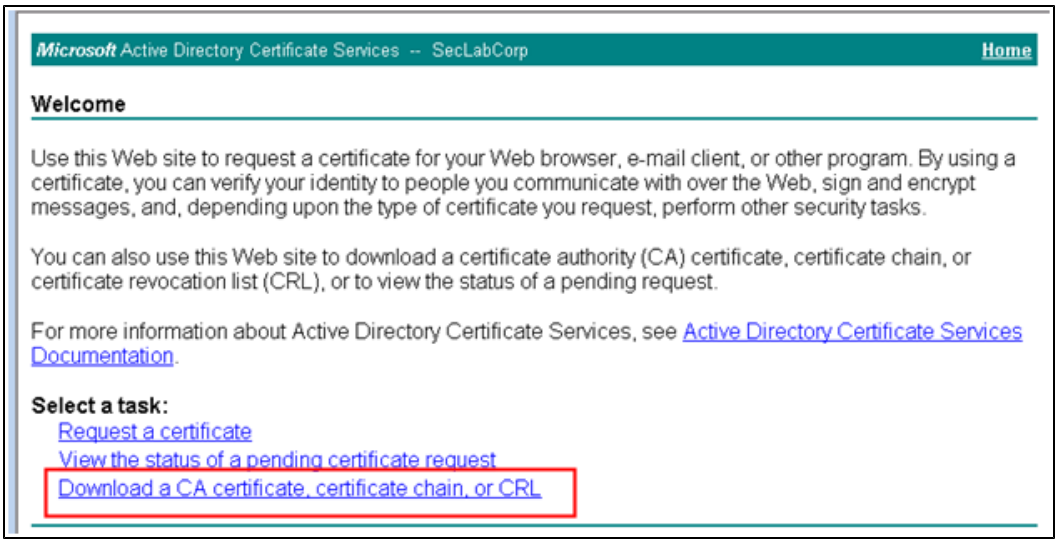


11. Use the Authority Name in the URL to download the Root CA certificate in the next step. The Authority Name appears in the URL from the '=' to the first single '/'. For example, in the picture above the Authority name is **http://adtestdc1.test.net.**

Download and Install the Root CA Certificate

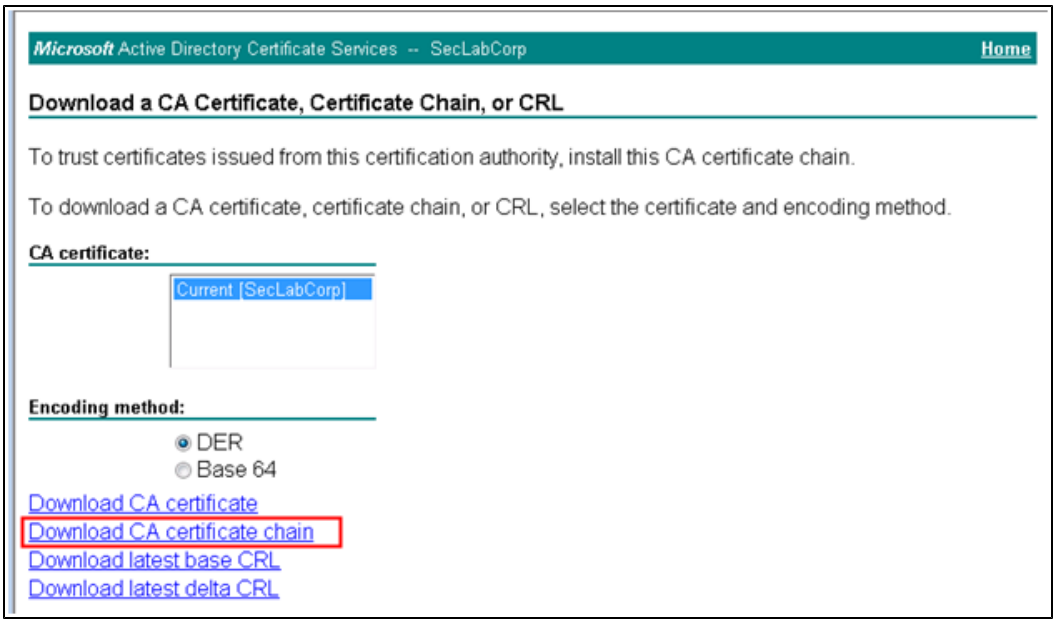
To download and install the Root CA certificate:

1. Login to the OCS agent machine.
2. Browse to the Certificate Authority web server with the Certificate's Authority Name from the URL you received above in the **Details** tab. You must use the Authority Name and append to it **/certsrv**. For example, in the Details tab above, the Authority Name is **http://adtestdc1.test.net.**. Therefore, you would browse to the Certificate Authority web server with the URL **http://adtestdc1.test.net/certsrv**.
3. The Welcome page opens.



In the Welcome page, click **Download a CA certificate, certificate chain, or CRL**.

4. The following page opens.



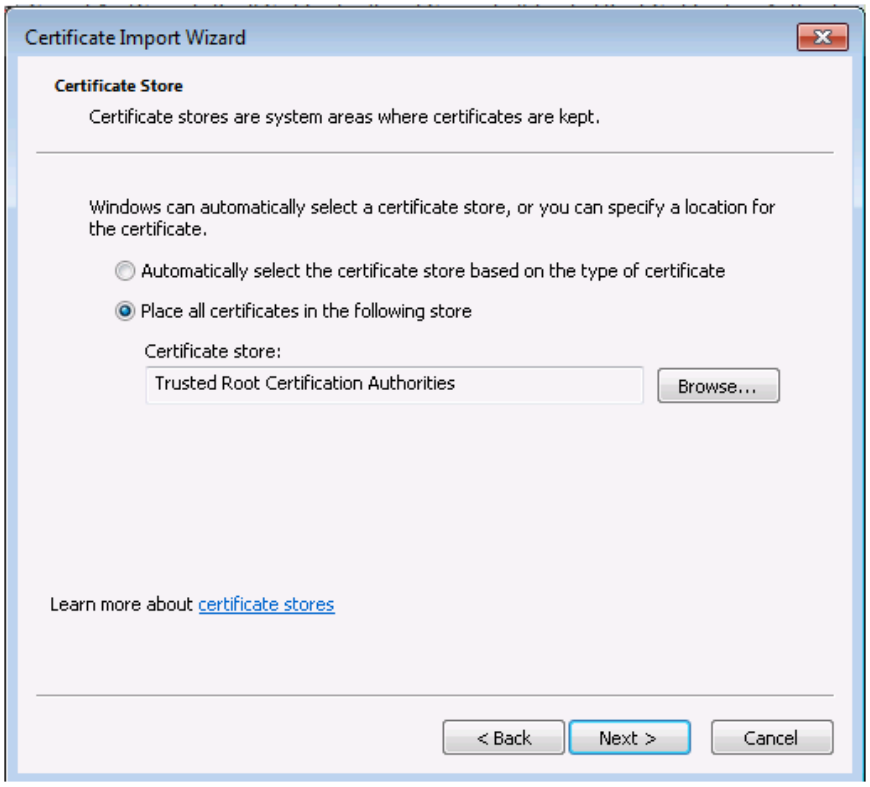
Click **Download CA certificate chain**.

5. A File Download prompt opens, asking if you want to save the Root CA Certificate (***.p7b** file).

   Save the Root CA certificate anywhere on the file system.
6. Run **mmc.exe**.
7. In the **Console Root**, go to **File>Add/Remove Snap-in**.
8. In the **Add/Remove Snap-In** dialog, click **Add**.
9. In the **Add Standalone Snap-In** dialog, select **Certificates** from the list. Click **Add**.
10. In the **Certificates snap-in** dialog, select **Computer Account**. Click **Next**.
11. In the **Select Computer** dialog, select **Local Computer**. Click **Finish**.
12. In the **Add Standalone Snap-In** dialog, click **Close**.
13. In the **Add/Remove Snap-In** dialog, click **OK**.

    The Certificate Import Wizard is launched.

14. Click **Next** in the wizard.
15. In the **Certificate Store** screen, select **Place all certificates in the following store** (see below). Click **Next**.

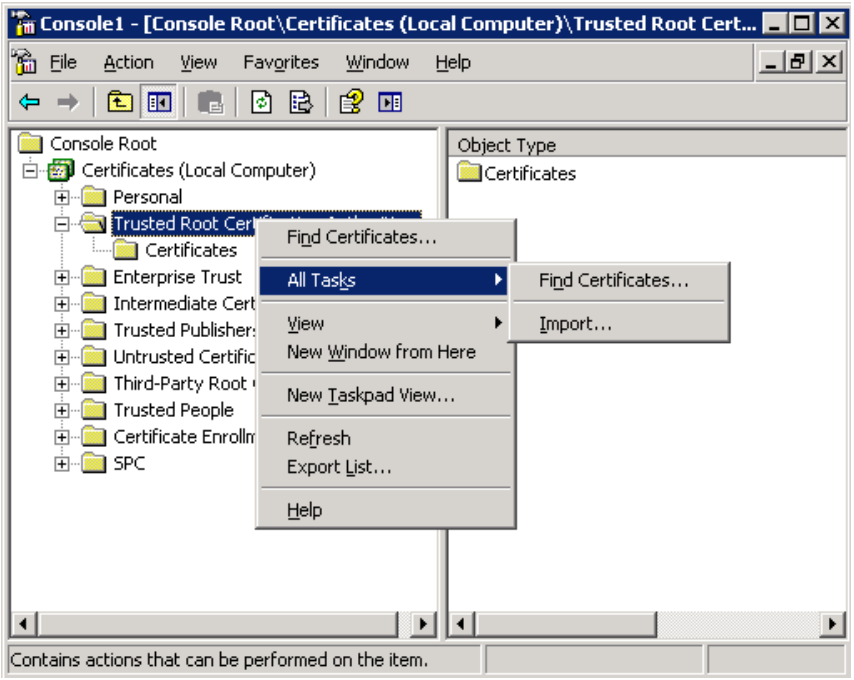


16. When the wizard finishes, go to the **Console Root** and right-click the **Trusted Root**

Certification Authorities folder.

17. A pop-up menu appears.

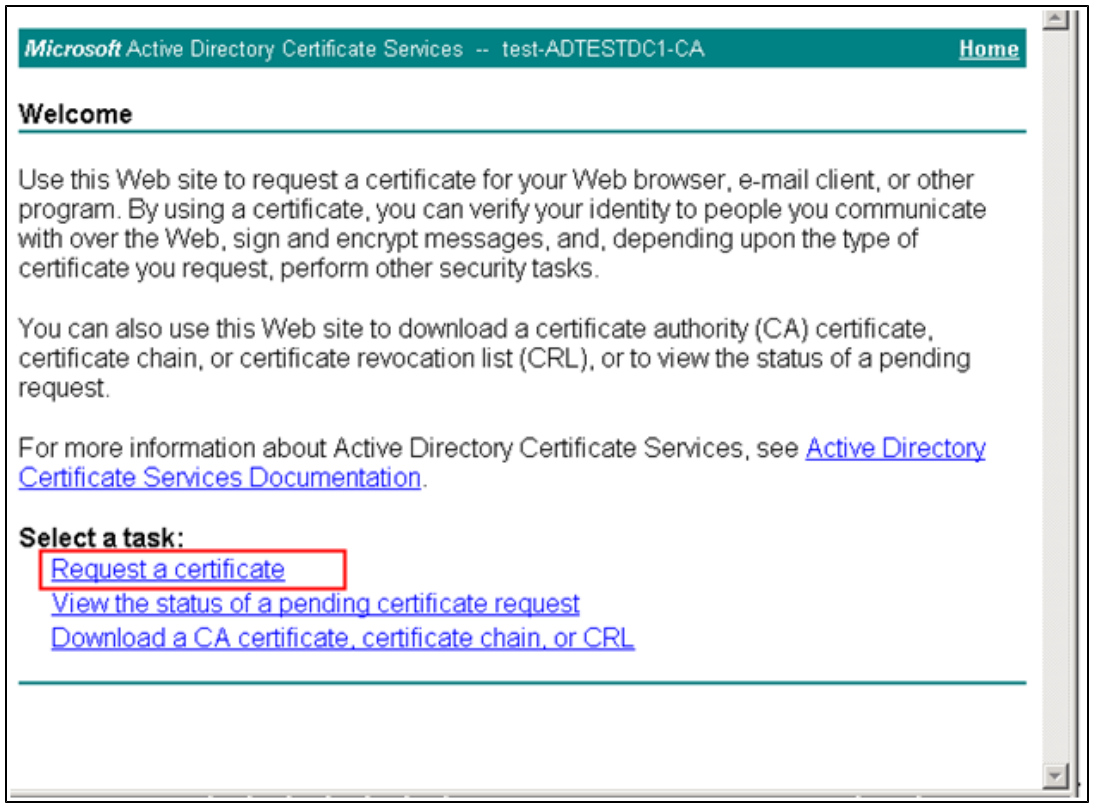
    Go to **All Tasks>Import** (see below) to import the Root CA certificate.



Install the Server Certificate on the OCS Agent Machine

To issue the Server Certificate and install it on the OCS agent machine:

1. From the OCS agent machine (important), browse to the CA web site with the Certificate's Authority Name. You must use the Authority Name and append to it **/certsrv**. For example, if the Authority Name is **http://adtestdc1.test.net.**, you would browse to the Certificate Authority web server with the URL **http://adtestdc1.test.net/certsrv**.
2. A Welcome screen opens. Select **Request a certificate**.



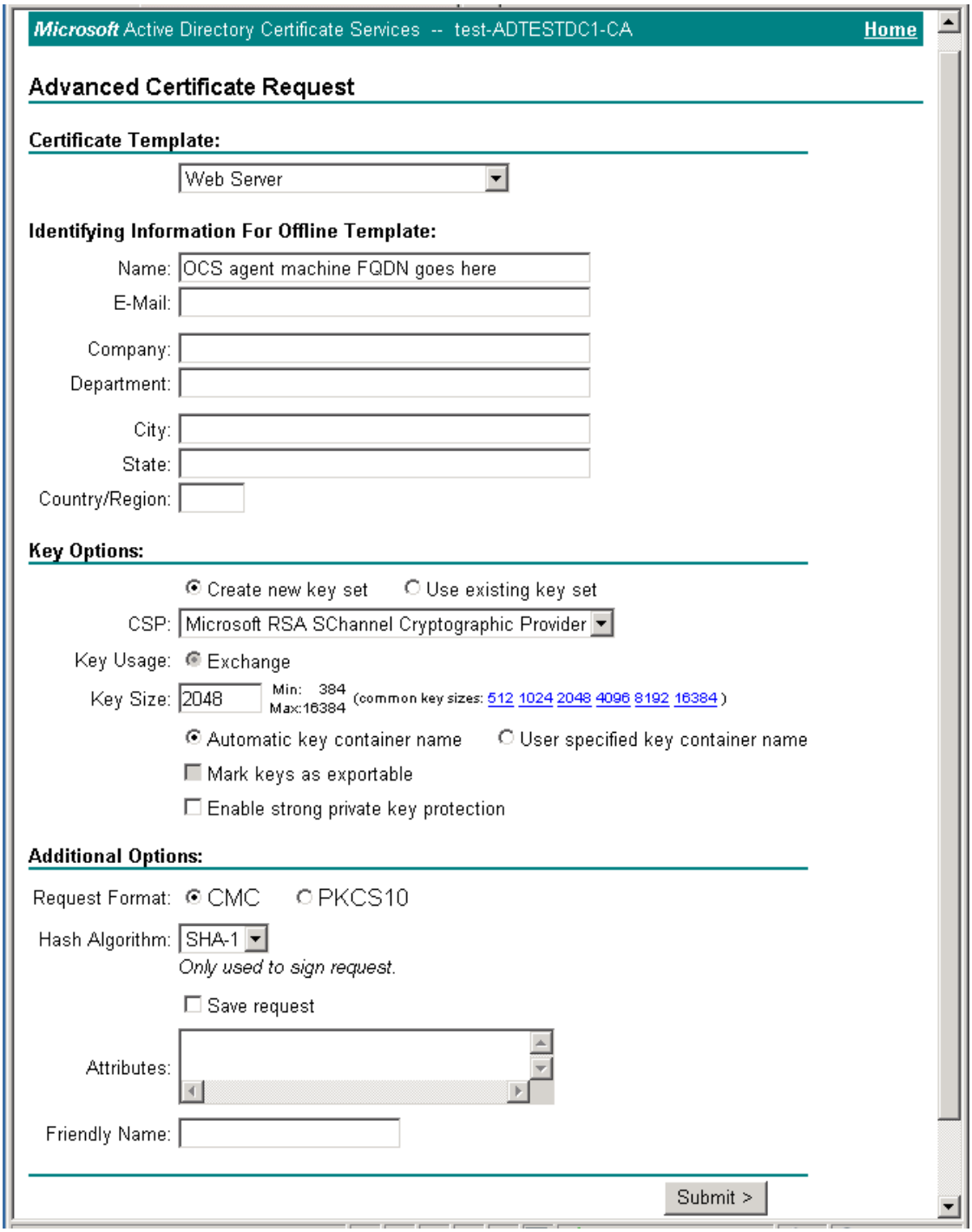
3. The **Request a Certificate** screen opens.

Select **advanced certificate request.**

4. The **Advanced Certificate Request** screen opens.

Select **Create and submit a request to this CA**.

5. The **Advanced Certificate Request** form opens.

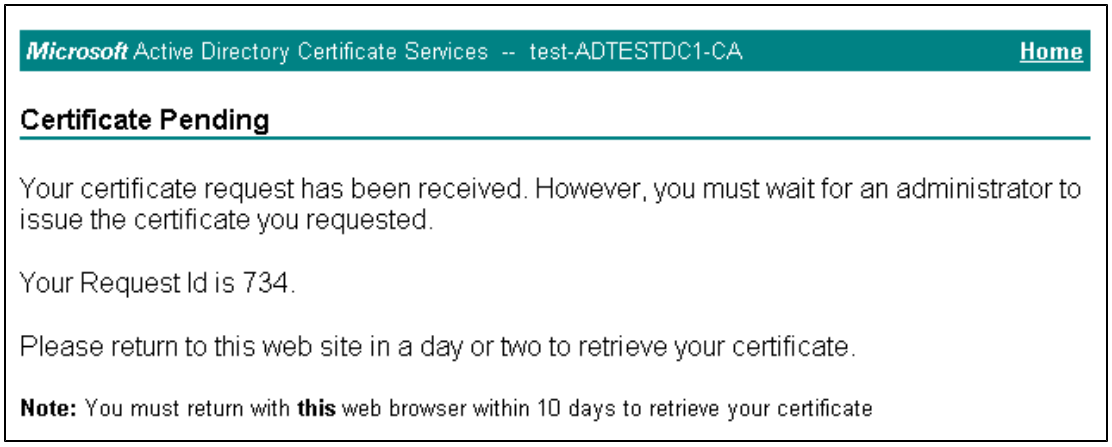


Fill in the form. Note that “Mark keys as exportable” checkbox may be disabled, but if you browsed from the OCS agent machine it does not need to be enabled.

6. Click the **Submit** button when you are finished filling out the form.
   - If your Certificate Authority Service is configured to automatically issue the certificate, the **Certificate Issued** screen appears (see below). Click **Install this certificate** and continue

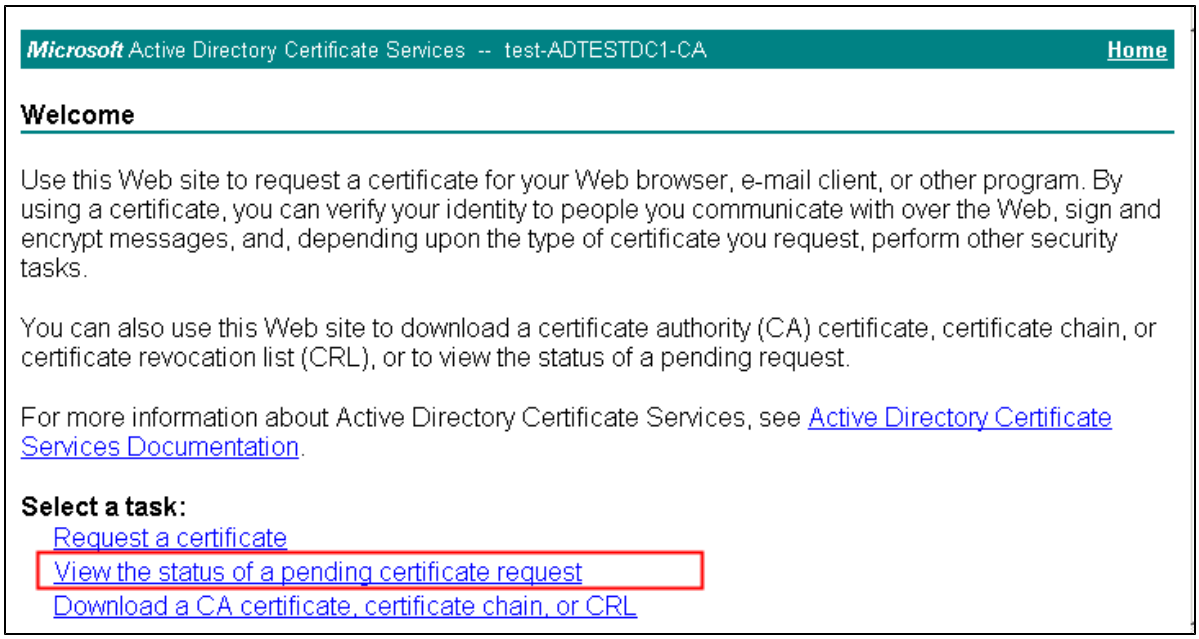
to the next step.

- If your Certificate Authority Service is not configured to automatically issue the certificate, you must ask your CA Administrator to issue the specific certificate request. In this case, instead of the **Certificate Issued** screen above, a **Certificate Pending** screen appears.



  i. Once you get a message that the certificate was issued, browse to the CA web site with the Certificate's Authority Name from the OCS agent machine (important) in the same manner as you did in the first step in this section.

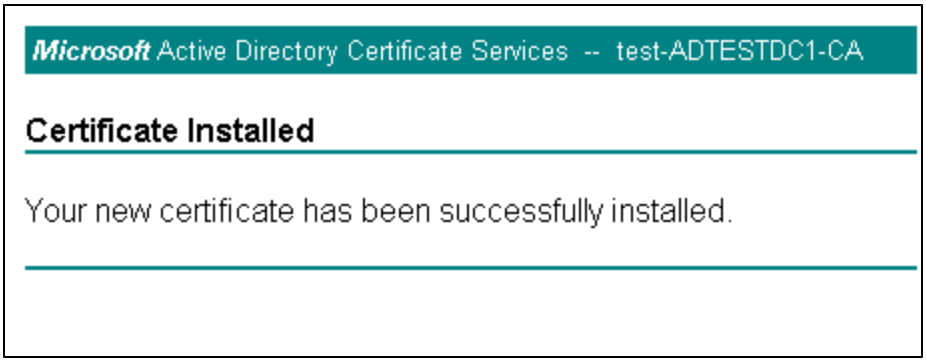
  ii. In the Welcome screen that appears, click **View the status of a pending certificate request**.



iii. The following screen opens. Select the issued certificate.

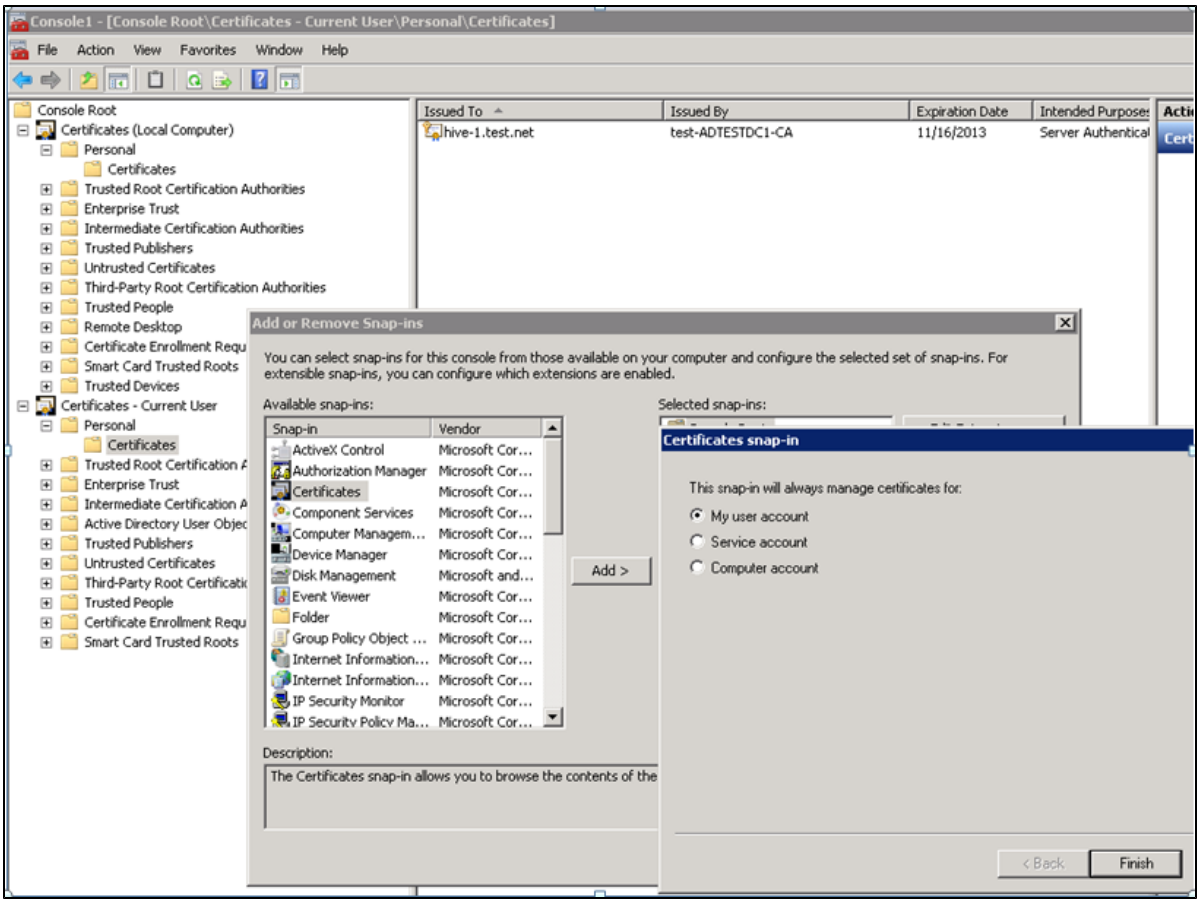
iv. The **Certificate Issued** screen appears. Select **Install this certificate**.

7. Verify that you get the following message.

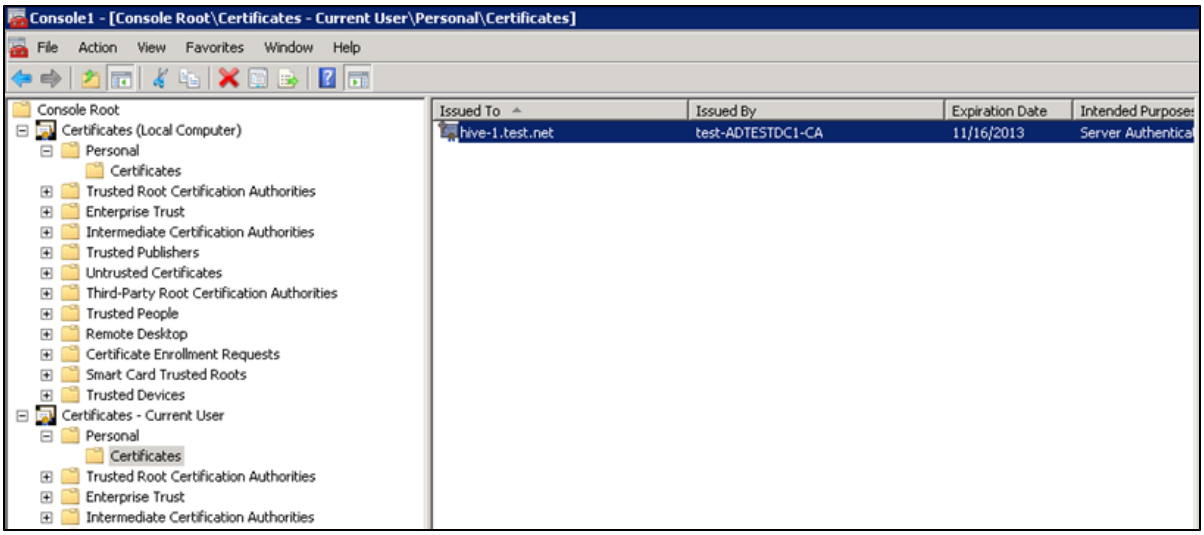


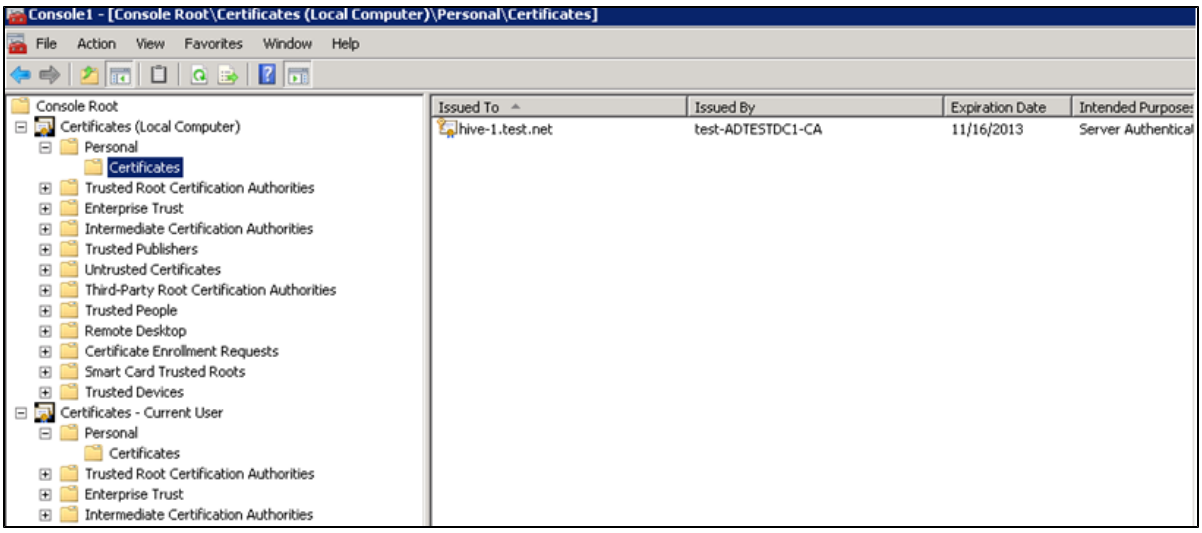
8. Login to the OCS server and run **mmc.exe**.
9. The Console Root opens. Go to **File>Add/Remove Snap-in**.
10. The **Add/Remove Snap-In** dialog opens. Select **Certificates**. Click **Add**.

11. The **Add Standalone Snap-In** dialog opens. Click **Add**.
12. The **Certificates snap-in** dialog opens. Select **My user account** (see below) to add the **User account Certificates Snap-In**. Click **Finish**.



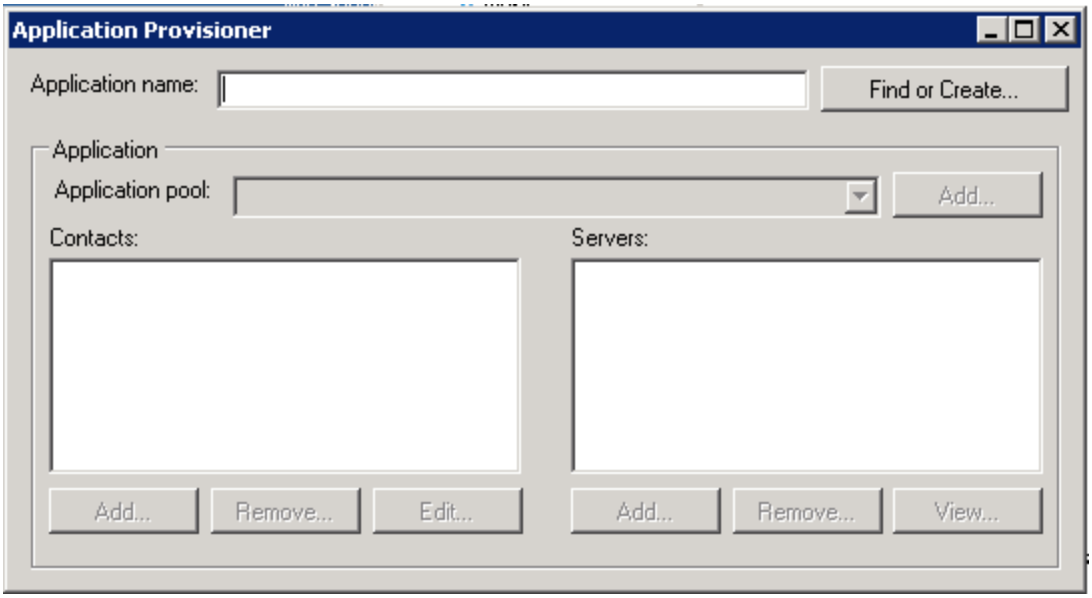
13. If you need to run the OCS agent process from different user accounts, drag the issued certificate from
Certificates - Current User>Personal>Certificates (see the first figure below) to the **Certificates (Local Computer)/Personal/Certificates** (see the second figure below).





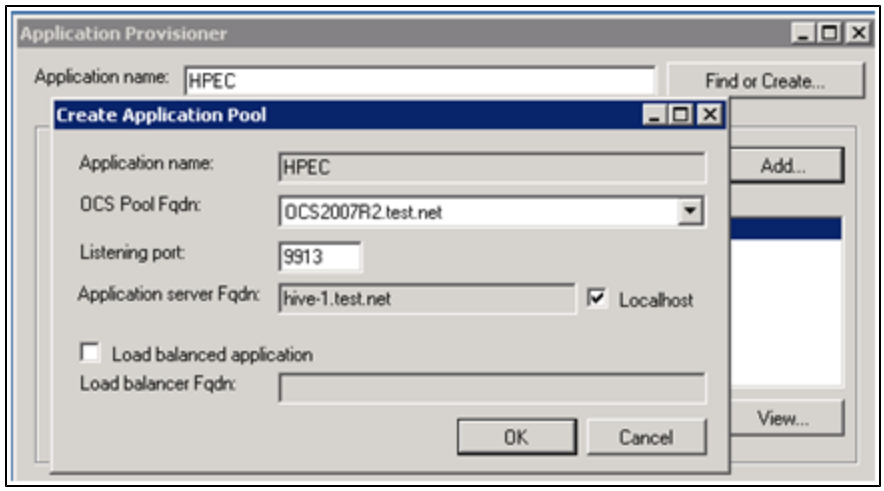
OCS Agent Provisioning

1. Login to the OCS agent machine as a user who is a member of the RTCUniversalServerAdmins group.
2. Double-click the Microsoft utility **ApplicationProvisioner.exe** in the folder **ocs-agent** (deployed as part of Enterprise Collaboration).
3. The **Application Provisioner** dialog box opens.



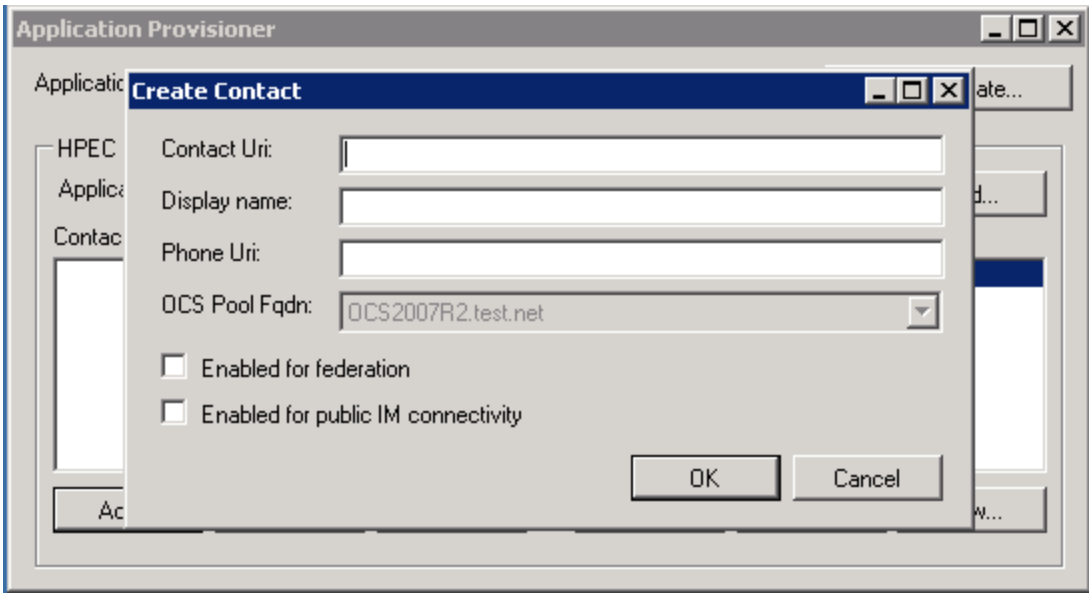
For **Application Name**, enter **HPEC**. Click **Find or Create…**

4. The **Create Application Pool** dialog box opens.



   a. Enter the following information:
      - Choose the **FQDN** of your OCS server from the **OCS Pool Fqdn:** drop-down list.
      - Enter a value for the Listening port, or use the default value.
      - Check the **Localhost** checkbox.
   b. Click **OK**.
5. The **Application Provisioner** dialog box opens.

   Create a Contact object by clicking **Add…** under the Contacts section.
6. The **Create Contact** dialog box opens.



a. Enter the following Contact information:

- **Contact Uri:** Enter here the SIP address of the HPEC OCS agent. The format is **sip:<name>@<domain name>**. For example, **sip:HPEC@hp.com**.

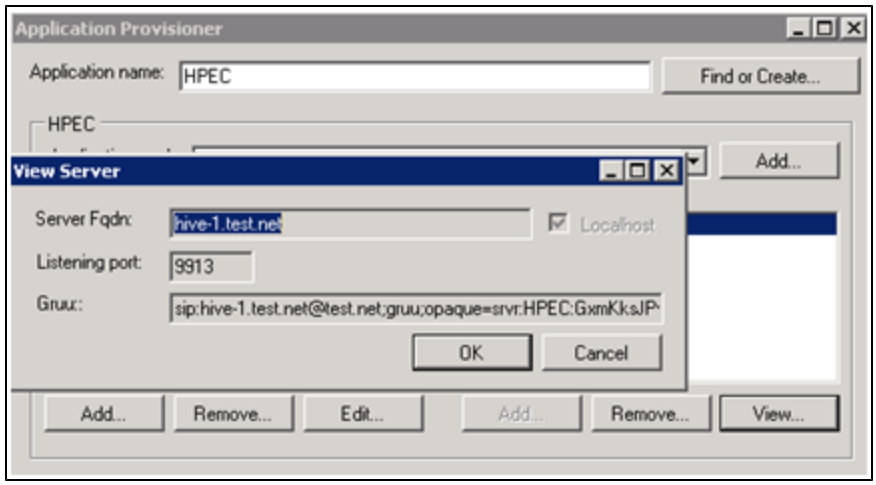
  Note: The <name> in the Contact Uri should be a user that exists in the active directory, with email and OCS permissions.

- **Display name:** The name you enter here will be the name that OC users see as the sender display name when receiving OC messages from EC. For example, **HPEC**.

  Note: Phone Uri should remain empty, and the two checkboxes in the dialog box should be unchecked.

b. Click **OK**.

7. In the **Application Provisioner**, select the Contact. Click **View…** under the Servers section.
8. The **View Server** dialog box opens.



In the **View Server** dialog box, save the GRUU for further configuration of the OCS agent.

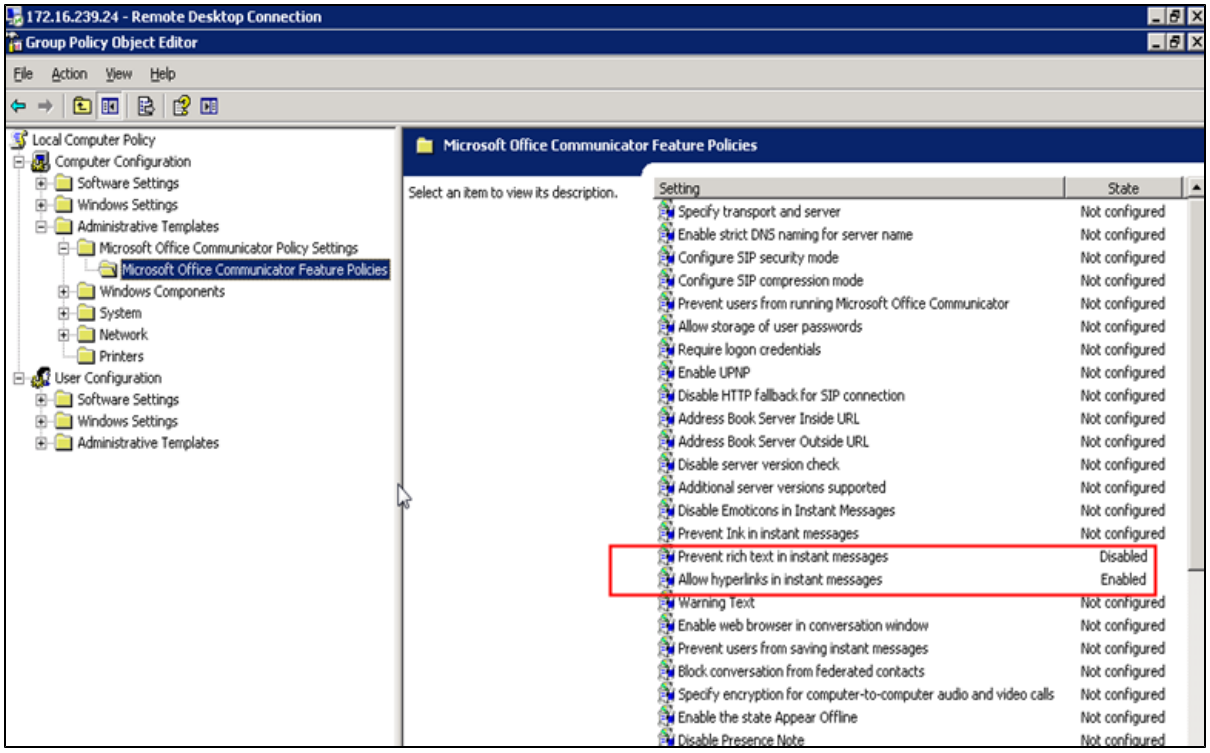
OCS Setup to Support Rich Content

Note: OCS setup to support Rich Content is optional. If you have already setup the OCS to support Rich Content, or you do not need Rich Content support, you can skip this section.

To setup OCS to support Rich Content:

1. Copy the file **Communicator.adm** that is located in the folder where you installed Enterprise Collaboration to the OCS machine.
2. Run **gpedit.msc** as follows:
   a. Go to **Computer Configuration**. Right-click **Administrative Templates** and choose **Add/Remove Templates…**
   b. In the dialog, click **Add…** and specify the path where the Communicator **.adm** file is located.
   c. Go to **Computer Configuration>Administrative Templates>Microsoft Office Communicator Policy Settings>Microsoft Office Communicator Feature Policies**.
   d. Change the setting of **Prevent rich text in instant messages** to **Disabled**, and the setting

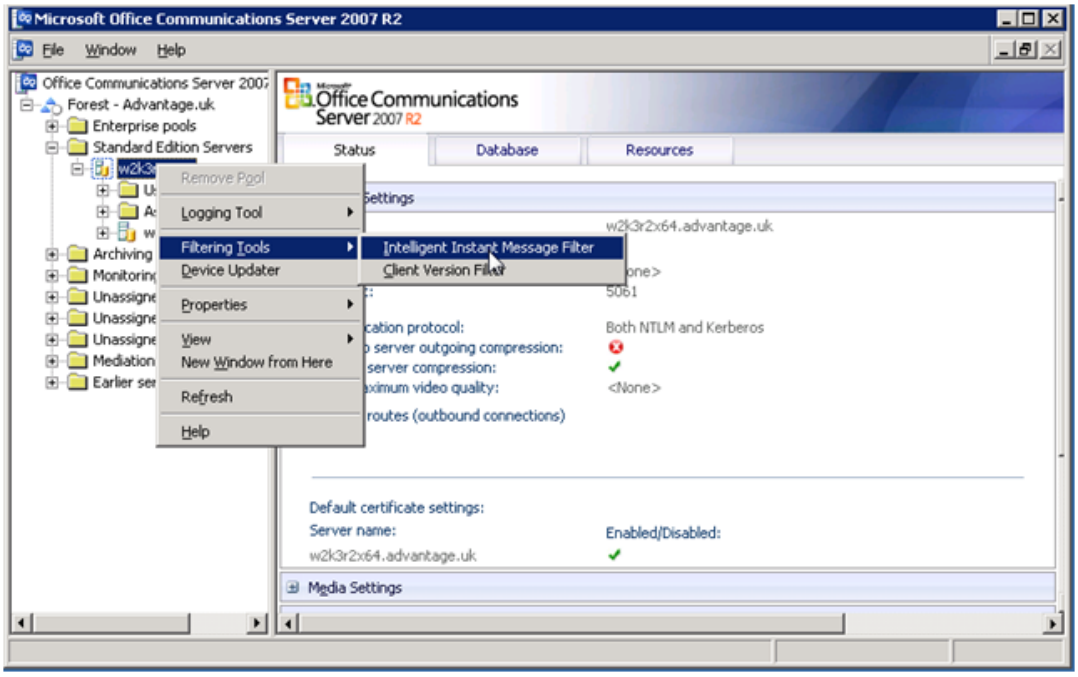
of **Allow hyperlinks in instant messages** to **Enabled**, as shown below.



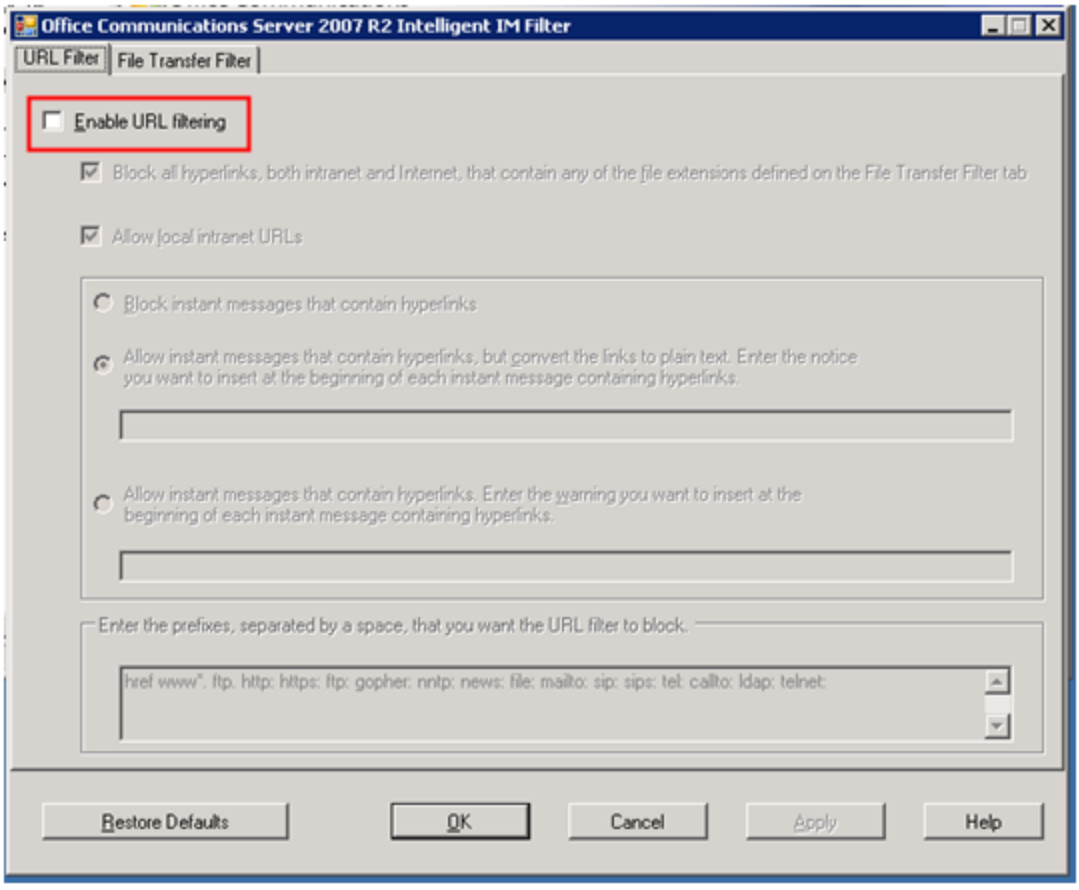
3. Run the Microsoft Management Console by running **C:\Program Files\Common Files\Microsoft Office Communications Server 2007 R2\WRTCSnap2.msc**.

   a. Go to **Forest - …>Standard Edition Servers** and right-click the poll with the OCS server host name.

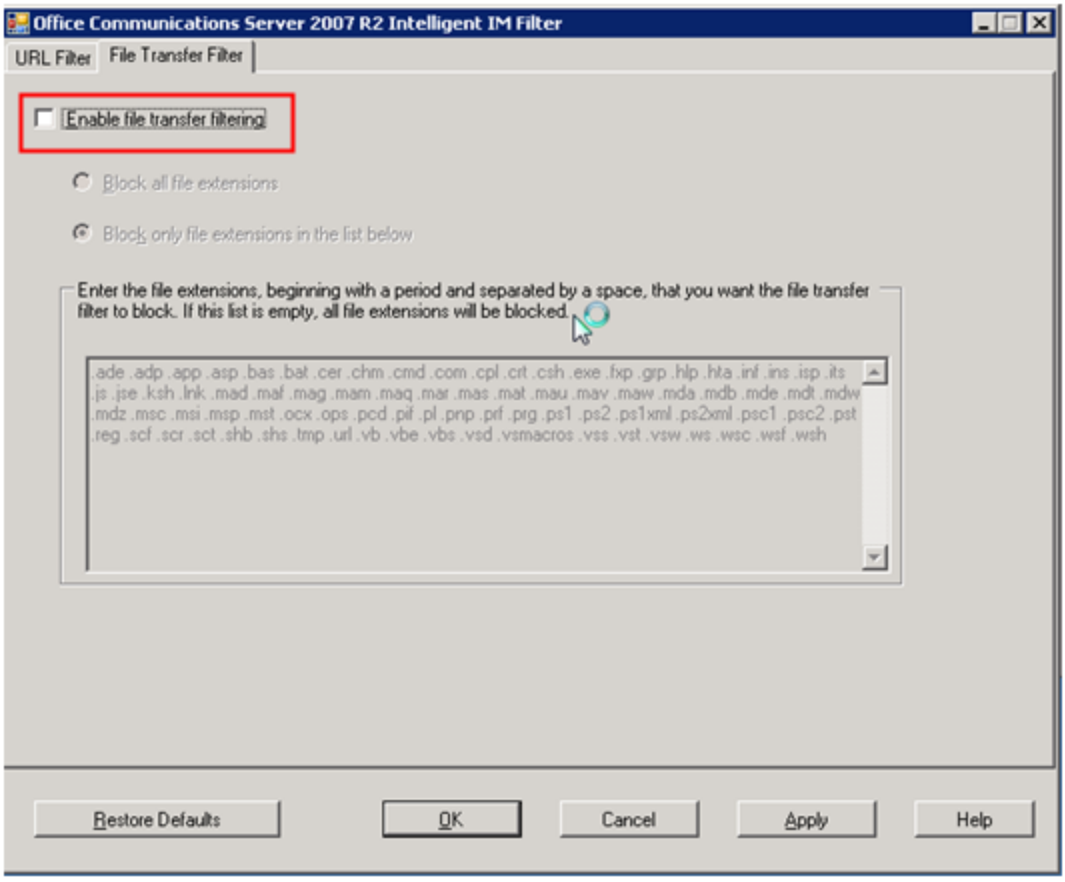
   b. From the pop-up menu, choose **Filtering Tools>Intelligent Instant Message Filter**, as shown below.



c. On the **URL Filter** tab, uncheck the **Enable URL filtering** checkbox, as shown below.



d. On the **File Transfer Filter** tab, uncheck **Enable file transfer filtering**, as shown below.



4. Restart the OCS server machine.

OC Client Setup to Support Rich Content

Note: OC client setup to support Rich Content is optional. If you have already setup the OC client to support Rich Content, or you do not need Rich Content support, you can skip this section.

1. Copy the file **OCSClient.reg** that is located in the folder where you installed Enterprise Collaboration to the machine where the OC client is installed.
2. On the client machine (where the OC client is installed), run the file **OCSClient.reg** and restart the OC client application.

Sanity Test of EC and OCS Integration

1. Start the HP EC server on the server machine.
2. Start the OCS agent on the server machine.
3. Start the OC client on the client machine. Login as user2.
4. Start the browser, go to the HP EC site. Login as user1.

5. Create a new conversation. Add user2 to the conversation.
6. Mark user2 as required (urgent) in the conversation. User2 should receive notification in the OC client.
7. Send a reply from OC client. The reply from user2 should be added to the conversation.

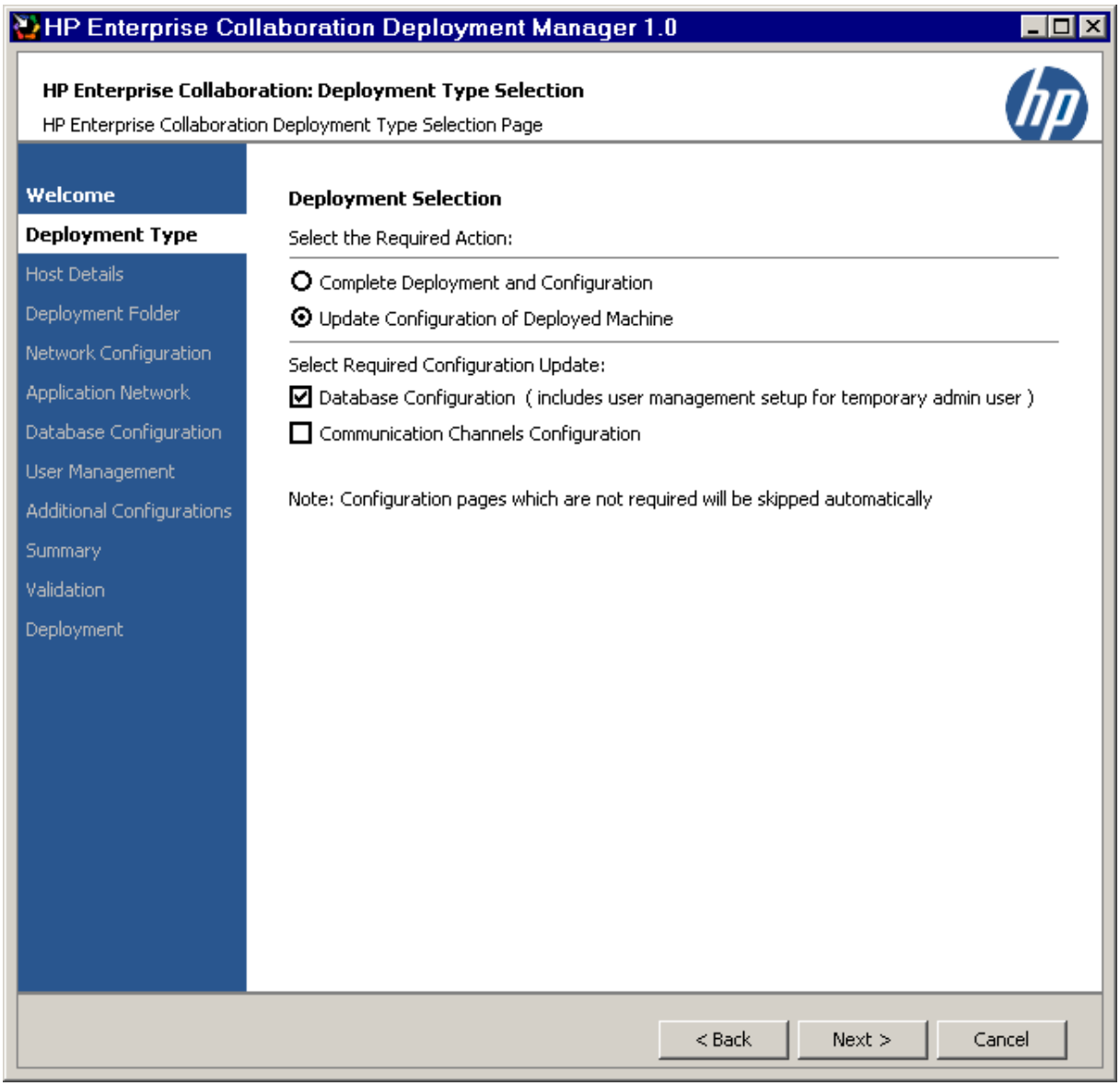
Chapter 4

Update EC Configuration

1. In the EC-Deployment Manager folder, double-click **EC.exe**.
2. The Enterprise Collaboration Deployment Manager wizard opens.

   In the Welcome page, check “I accept the terms of the license agreement”. Click **Next**.
3. The Deployment Selection page opens.

   Check **Update Configuration of Deployed Machine**.
4. Additional options appear for selecting the type of configuration update.



The configuration options are:

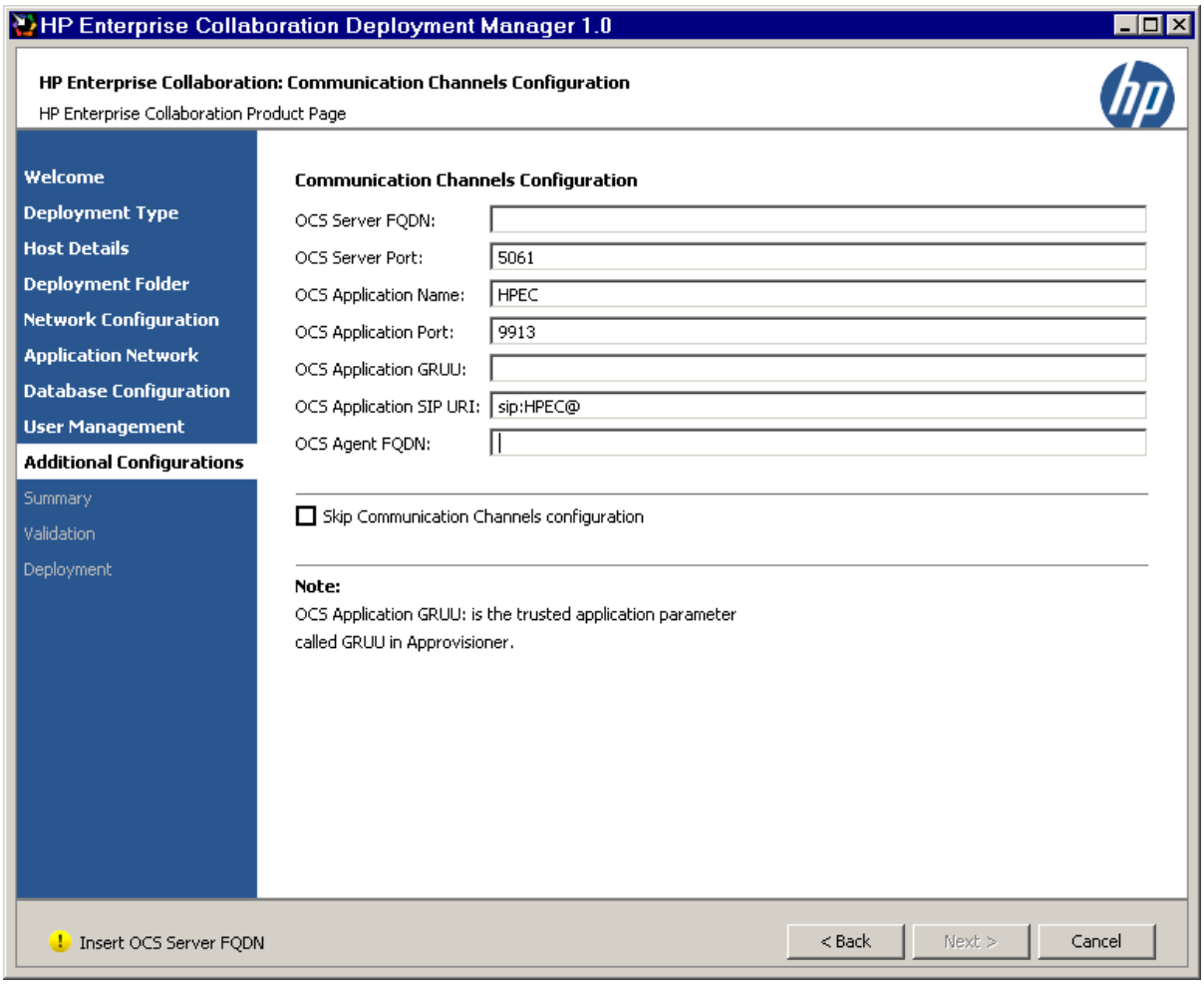
- **Database Configuration:** If you choose this configuration, the update wizard takes you through the following pages: EC Deployment Host Details, Deployment Folder Configuration, MSSQL Database Server Configuration, User Management Configuration, Summary, and Validation. The pages not presented, that were part of the installation procedure, are Network Configuration, Application Network Configuration, Lightweight Single Sign On Configuration, and Email Configuration.
- **Communication Channels Configuration:** This configuration should be performed only if you intend to use Enterprise Collaboration with Office Communicator and only after you have performed the Office Communicator Setup as described in "Set Up the Integration with Office Communicator Server (OCS)" (on page 24).

It is possible to select both configuration options and perform them at the same time.

5. Choose the type of configuration update you want to perform. Click **Next**.
6. If you chose **Database Configuration** in the previous step, the configuration wizard takes you through the pages mentioned in step 4 and you can modify settings in these pages according to your needs.

   If you chose **Communication Channels Configuration** in the previous step, the configuration wizard takes you through the pages EC Deployment Host Details, Deployment Folder Configuration, and Communication Channels Configuration. EC Deployment Host Details and Deployment Folder Configuration were already presented during installation and you can modify settings in these pages according to your needs.

   The Communication Channels Configuration page is shown below.



7. In the Communication Channels Configuration page, enter the following information:
   - **OCS Server FQDN**: Enter here the **OCS Pool Fqdn** that you entered during the "OCS Agent Provisioning" (on page 39) process.
   - **OCS Server Port:** The default value is 5061. Consult your system administrator for this port number.
   - **OCS Application Name:** The default name is **HPEC**. Enter here the **Display Name** that you entered during the "OCS Agent Provisioning" (on page 39) process. .
   - **OCS Application Port:** The default value is 9913. Enter here the Listening Port number that you entered during the "OCS Agent Provisioning" (on page 39) process.
   - **OCS Application GRUU:** Enter here the string that you obtained during the "OCS Agent Provisioning" (on page 39) process.
   - **OCS Application SIP URI:** The default value is **sip:HPEC@**. Enter here the **Contact Uri** that you entered during the "OCS Agent Provisioning" (on page 39) process.
   - **OCS Agent FQDN:** This value should be the FQDN of the EC server.

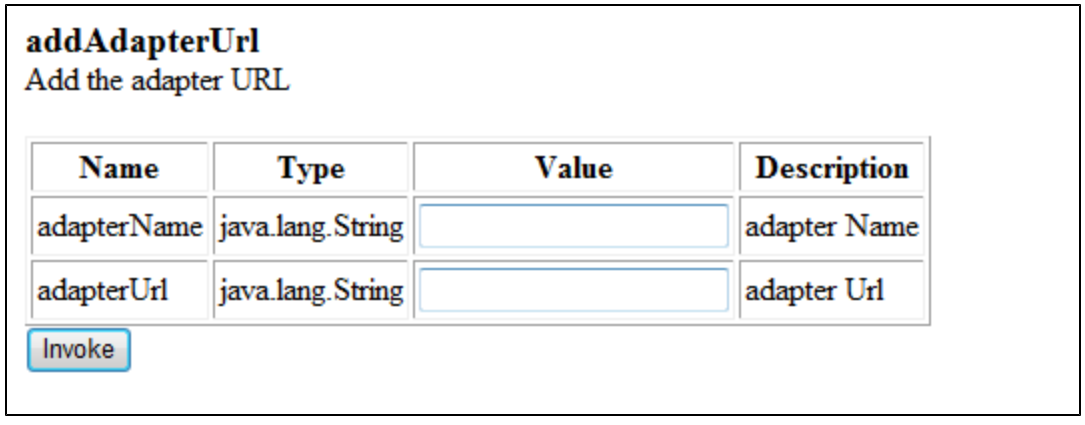
Chapter 5

Set Up the Adapter

1. Download the adapter **.war** file from: www.hp.com/go/livenetwork
2. Put the adapter **.war** file in the directory **<EC_Installation_Folder>/servers/server-0/webapps**. The name of the adapter **.war** file should be the same as the adapter name.

   If you want to deploy the adapter remotely, you can use the Tomcat manager application to do this, according to the following instructions:
   http://tomcat.apache.org/tomcat-7.0-doc/manager-howto.html

   Note: In order to prevent network speed issues, copy the adapter **war** file to the temporary directory in the target server. Then after the deployment, move it from the temporary directory to the directory **<EC_Installation_Folder>/servers/server-0/webapps**.
3. Add the basic adapter URL using JMX as follows:
   a. Go to **<EC_application_url>/diamond/jmx-console** (for example, **http://my_host:8080/diamond/jmx-console**).
   b. Select **Diamond > Diamond adapter config jmx service**.
   c. In the method **addAdapterUrl** (see the figure below) add the following parameters:
      - **adapterName:** This name should be identical to the **adapter.war** filename For example, if the filename is **sm.war**, enter here **sm**.
      - **adapterUrl:** For local deployment, the adapter URL should be **{local}/adapter_name**.



   d. Click **Invoke**.
4. If your adapter uses LWSSO, check that the **initString** defined in the LWSSO configuration file in adapter **.war** is the same value that you defined for **initString** in the Lightweight Single Sign On configuration page during EC installation.

Chapter 6

Perform Additional Configuration Steps

Install a Certificate for the Mail Client

This installation is required if the mail server is accessed using a secure connection and its certificate is self-signed.

To install a certificate for the mail client:

1. Verify that EC is not running.
2. Open CMD.
3. Run the following command to import your certificate:

   <EC FOLDER>\java\windows\x86_64\bin\keytool.exe -import -alias <YOUR CERTIFICATE ALIAS> -file <ROOT CA CERTIFICATE PATH> -keystore <EC FOLDER>\java\windows\x86_64\lib\security\cacerts

Install Customer Certificates

At the end of the installation process, the Tomcat server is set with a self-signed temporary certificate.

If you work with a standalone web application network configuration, you can work with the self-signed certificate generated during the EC installation without performing the steps below. However, it is recommended to import your Server Certificate to the keystore as described below.

If you work in a reverse proxy network configuration, you should import your Root CA certificate and Server Certificate to the EC server keystore by performing the steps below.

To install a certificate for Tomcat:

1. Verify that EC is not running.
2. Open CMD.
3. Run the following command to delete the temp certificate from keystore:

   <EC FOLDER>\java\windows\x86_64\bin\keytool.exe -delete -alias tomcat -keystore <EC FOLDER>\servers\server-0\ec-keystore.jks

4. Perform one of the following commands:
   - To import your keystore to the EC keystore:

     <EC FOLDER>\java\windows\x86_64\bin\keytool.exe -importkeystore -srckeystore <YOUR KEYSTORE PATH> -destkeystore <EC FOLDER>\servers\server-0\ec-keystore.jks -srcstoretype <YOUR KEYSTORE TYPE>

   - To import your certificate to the EC keystore:

<EC FOLDER>\java\windows\x86_64\bin\keytool.exe -import -alias <YOUR CERTIFICATE ALIAS> -file <YOUR CERTIFICATE PATH> -keystore <EC FOLDER>\servers\server-0\ec-keystore.jks

Note: For reverse proxy certificates, this command should be performed for both Root CA and Server Certificates.

Disabling Default Secure Authentication (optional)

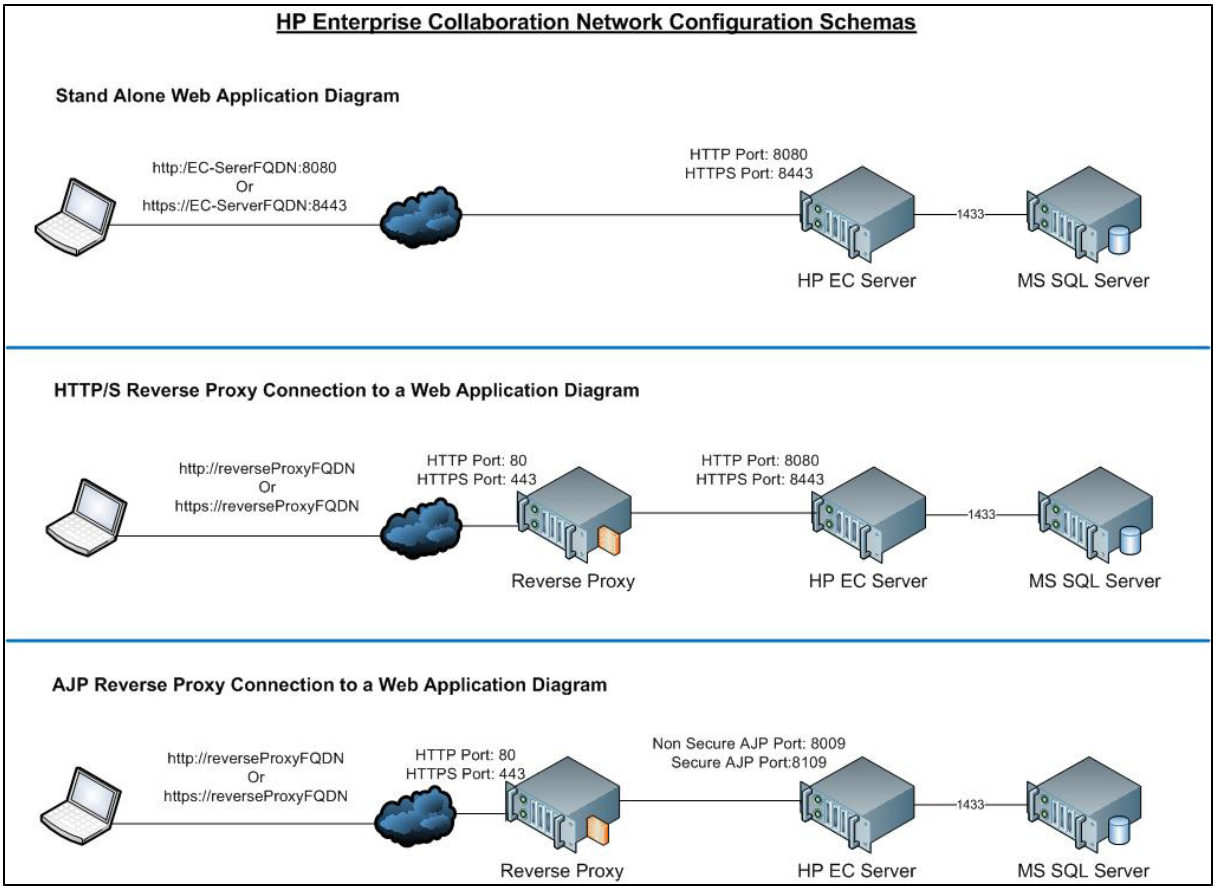
Perform this step only if you want to disable redirection to https for authentication.

Note: For security reasons, this is not recommended.

1. Verify that EC is not running.
2. Open CMD.
3. Run **C:\HP\EC\diamond-deploy\disable-secure-authentication.bat**.
4. Start EC.

Appendix A: Network Configuration Schemas for HP Enterprise Collaboration

The following diagrams show the possible network configuration schemas for HP Enterprise Collaboration.



Appendix B: Updating the external-ldap.properties File

Before making changes in the **external-ldap.properties** file, you should be familiar with the relevant LDAP properties required for your User Repository. If you are unfamiliar with the LDAP configuration, you can use tools such as the Apache Directory Studio LDAP browser in order to detect the relevant LDAP properties required for your User Repository. For instruction on how to login to LDAP using the Apache Directory Studio LDAP Browser, see the section "Logging into LDAP using the Apache Directory Studio LDAP Browser" (on page 58) at the end of this appendix.

Basic LDAP Properties

The following table lists the basic LDAP properties that you need to configure in **external-ldap.properties** in order for EC to logon to LDAP.

Attribute	Description
ldapHost	LDAP host name
ldapPort	LDAP port number
enableSSL	True/False—use SSL connection to LDAP
useAdministrator	True/False—use this user to connect to LDAP
ldapAdministrator	LDAP user DN (defined if useAdministrator=True)
ldapAdministratorPassword	LDAP user password (defined if useAdministrator=True)

Configure the User Providers

Update the **external-ldap.properties** file with the following attributes according to the customer's organizational LDAP properties.

Attribute	Description
usersBase	LDAP Base Distinguished Name (DN) for the users search. Only users under this DN in the LDAP hierarchy are returned from the search.
usersScope	LDAP search scope for users search. Defines how exactly the search under the usersBase location should be performed. SCOPE_BASE search space contains a single entry pointed by the userBase; SCOPE_ONE - search space contains the userBase and its direct children only; SCOPE_SUB - search space contains the userBase and its whole sub tree.
usersFilter	LDAP filter for users search

Configuring Users Object Class

The following properties are used to define the LDAP vendor or customized implementation-specific objects that represent the user objects.

To map the user configuration properties to the LDAP server configuration properties of the organization, update the **external-ldap.properties** file with following attributes according to the organization's LDAP properties.

Attribute	Description
usersObjectClass	LDAP object class representing the user's object.
usersUniqueIDAttribute	The user's unique ID LDAP attribute name.
usersLoginNameAttribute	The user's login name LDAP attribute name.

The following attributes are optional:

Attribute	Description
usersDisplayNameAttribute	Users display name LDAP attribute name.
usersFirstNameAttribute	Users first name LDAP attribute name.
usersLastNameAttribute	Users last name LDAP attribute name.
usersEmailAttribute	Users email LDAP attribute name.
usersPreferredLanguageAttribute	Users preferred language LDAP attribute name.
usersPreferredLocationAttribute	Users preferred location LDAP attribute name.
usersTimeZoneAttribute	Users time zone LDAP attribute name.
usersDateFormatAttribute	Users date format LDAP attribute name.
usersNumberFormatAttribute	Users number format LDAP attribute name.
usersWorkWeekAttribute	Users work week LDAP attribute name.
usersTenantIDAttribute	Users tenant ID LDAP attribute name.
usersPasswordAttribute	Users password LDAP attribute name.

Groups Search

The following properties define the search mechanism that is implemented on LDAP groups. There are two sets of properties, one for regular groups and one for root groups.

In order to display only a limited number of groups, restrict the root groups search criteria appropriately. The same search criteria for both root and non-root groups can be used. This configuration is recommended when the overall number of groups is small.

To map the groups configuration properties to the LDAP server configuration properties, update the **external-ldap.properties** file with the following attributes according to the organization's LDAP.

Attribute	Description
groupsBase	LDAP Base Distinguished Name (DN) for groups search. Only groups under this DN in the LDAP hierarchy are returned from the search.
groupsScope	LDAP scope for groups search. • SCOPE_BASE search space contains a single entry pointed to the groupsBase; • SCOPE_ONE - search space contains the groupsBase and its direct children; • SCOPE_SUB - search space contains the groupsBase and its whole sub tree
groupsFilter	LDAP filter for groups search. The only valid values are rootGroupsBase, rootGroupsScope, or rootGroupsFilter.
rootGroupsBase	LDAP Base Distinguished Name (DN) for groups search. Only groups under this DN in LDAP hierarchy are returned from the search.
rootGroupsScope	LDAP search scope for groups search. Specifies how the search under the gropusBase location should be performed. • SCOPE_BASE - search space contains a single entry pointed to the rootGroupsBase; • SCOPE_ONE - search space contains the rootGroupsBase and its direct children only; • SCOPE_SUB - search space contains the rootGroupsBase and its whole sub tree
rootGroupsFilter	LDAP filter for groups search

Groups Object Class (LDAP Vendor Dependent)

The following properties are used to define the LDAP vendor or custom implementation-specific objects representing static groups. More than one comma-separated object class is supported. In this scenario, the user can define the appropriate corresponding comma-separated attribute names.

To map the groups configuration properties to the LDAP server configuration properties, update the **external-ldap.properties** file with the following attributes according to the organization's LDAP properties.

Attribute	Description
groupsObjectClass	LDAP object class representing group object.
groupsMembersAttribute	Groups members LDAP attribute name. This multi-value attribute contains the full distinguished names (DNs) of static group members.

The following attributes are optional:

Attribute	Description
groupsNameAttribute	Groups unique name LDAP attribute name. In most default LDAP implementations, this attribute is usually the same as groupsDisplayNameAttribute.
groupsDisplayNameAttribute	Groups display name LDAP attribute name. In most default LDAP implementations, this attribute is usually the same as groupsNameAttribute.
groupsDescriptionAttribute	Groups description LDAP attribute name. The attribute contains the groups' description.
enableDynamicGroups	Boolean attribute for enabling dynamic groups. If the value of this attribute is true, dynamic groups are searched. Note that enumerating members of very large dynamic groups may be time consuming.
dynamicGroupsClass	LDAP object class representing dynamic group object.
dynamicGroupsMemberAttribute	Dynamic groups members LDAP attribute name. This attribute contains the LDAP search URL. The values returned by this LDAP search URL are considered dynamic group members.
dynamicGroupsNameAttribute	Dynamic groups unique name LDAP attribute name. In most default LDAP implementations, this attribute is usually the same as dynamicGroupsDisplayNameAttribute.
dynamicGroupsDisplayNameAttribute	Dynamic groups display name LDAP attribute name. In most default LDAP implementations, this attribute is usually the same as dynamicGroupsNameAttribute.
dynamicGroupsDescriptionAttribute	Dynamic groups description LDAP attribute name. This attribute contains the groups description.

Groups Hierarchy

The Groups Hierarchy attributes defines whether HP Enterprise Collaboration relates to LDAP server groups hierarchy information.

Attribute	Description
enableNestedGroups	Enable support of nested groups. If support of nested groups is disabled, subgroups of a group are not searched.
maximalAllowedGroupsHierarchyDepth	Maximal allowed depth of groups hierarchy. No groups are searched beneath this level.

Advanced Configuration

The advanced configuration attributes are used for fine-tuning the LDAP connection.

Attribute	Description
ldapVersion	LDAP protocol version. Possible values are: • 3 (default) • 2 (for old versions of LDAP)
baseDistinguishNameDelimiter	Base DN delimiter. Symbol used in configuration when putting multiple base DNs for users or groups or users search. Note that this symbol must not appear as part of the base DN used in this configuration. If it appears in the base DNs, change the default value to some other symbol.
scopeDelimiter	Scope delimiter. Symbol used in configuration when putting multiple scopes for users or groups search. This symbol must not appear as part of the scope name used in this configuration. If it appears in the scope name, change the default value to some other symbol.
attributeValuesDelimiter	Symbol used in configuration when putting in multiple attribute names of users or group. Pay attention that this symbol must not appear as part of attributes used in this configuration. If it appears in attribute names, then change the default value to some other symbol.

Logging into LDAP using the Apache Directory Studio LDAP Browser

The following instructions explain how to log into LDAP using the Apache Directory Studio LDAP Browser.

To connect to the LDAP server, perform the following steps:

1. Download and Install the Apache Directory Studio LDAP browser from:

   http://directory.apache.org/studio/

2. Open the LDAP browser and select the New Connection button from the Connections tab located in the bottom left side of the application window.
3. Enter the LDAP Host name (ldapHost) and Port number (ldapPort).
4. Select the appropriate encryption level (enableSSL).
5. Click the **Check Network Parameters** button.
6. Click the **Next** button.
7. Select one of the following Authentication methods:
   - No Authentication: useAdministrator=false
   - Simple Authentication: useAdministrator=true
8. Click the **Finish** button (this automatically tests the connection).