HP Enterprise Collaboration

For the Windows ® operating system

Software Version: 1.1

Installation and Configuration Guide

Document Release Date: August 2012 Software Release Date: August 2012



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

© Copyright 2012 Hewlett-Packard Development Company, L.P.

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

Installation and Configuration Guide	1
Contents	5
Introduction	7
HP Enterprise Collaboration Documentation Library	7
Prerequisites	9
Database and Tablespace Authorizations	9
Email Configuration	9
Install and Configure Enterprise Collaboration	10
Install Enterprise Collaboration	10
Configure the User Repository and User Roles	24
Configuration for Secure Login when Using Reverse Proxy	27
Set Up Integration with Office Communicator Server and MS Lync Server	29
Install the Root Certificate Authority (CA) Certificate	29
Install the Server Certificate on the OCS Agent Machine	37
Agent Provisioning	44
Agent Provisioning for OCS 2007	44
Agent Provisioning for Lync 2010	47
OCS Setup to Support Rich Content	48
OC Client Setup to Support Rich Content	51
Sanity Testing of EC and OCS Integration	51
Perform Additional Configuration Steps	53
Install a Certificate for the Mail Client	53
Install Customer Certificates	53
Disabling Default Secure Authentication (optional)	54
Update Configuration in the Deployment Manager	55
Set Up the Adapter	. 59
Upgrade EC Configuration from 1.0 to 1.1	60

Desktop Client Installation	62
Appendix A: Network Configuration Schemas for HP Enterprise Collaboration	67
Appendix B: Updating the external-Idap.properties File	68
Basic LDAP Properties	68
Configure the User Providers	
Configuring Users Object Class	69
Groups Search	
Groups Object Class (LDAP Vendor Dependent)	71
Groups Hierarchy	72
Advanced Configuration	72
Logging into LDAP using the Apache Directory Studio LDAP Browser	73

Chapter 1

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 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 10)
- 2. "Configure the User Repository and User Roles" (on page 24)
- 3. <u>"Set Up Integration with Office Communicator Server and MS Lync Server" (on page 29)</u> Perform this procedure if you want to use EC with Office Communicator.
- <u>"Update Configuration in the Deployment Manager" (on page 55)</u> 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 in stage 3).
- <u>"Set Up the Adapter" (on page 59)</u> 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. <u>"Perform Additional Configuration Steps" (on page 53)</u>: Depending on your system setup, you may need to perform additional configuration steps. Refer to 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: <u>http://h20230.www2.hp.com/selfsolve/manuals</u>. 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.

Chapter 1: Introduction

Guide	Description
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 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 Collaboration.
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

Prerequisites

Before installing Enterprise Collaboration, Windows UAC (User Account Control) must be disabled. If UAC is enabled, an error message will appear on the validation page during the installation process.

To disable UAC:

- 1. From the Start menu, select Run and type msconfig.
- 2. In the System Configuration window, select the **Tools** tab.
- 3. From the Tools list, select Change UAC Settings and click Launch.
- 4. In the User Accounts Control window, scroll the bar to Never Notify and click OK.

Database and Tablespace Authorizations

A regular user (with special permissions) can install and configure the Enterprise Collaboration database. There is no need for a DBA user.

When you create the installer user <username>, assign them the following permissions:

GRANT CREATE USER TO <username> WITH ADMIN OPTION;

GRANT CONNECT TO <username> WITH ADMIN OPTION;

GRANT UNLIMITED TABLESPACE TO <username> WITH ADMIN OPTION;

GRANT CREATE VIEW TO <username> WITH ADMIN OPTION;

GRANT RESOURCE TO <username> WITH ADMIN OPTION;

GRANT CREATE JOB TO <username> WITH ADMIN OPTION;

As the installation checks that the tablespace exists, the installer needs the following additional permissions:

GRANT SELECT ON DBA TABLESPACES TO <username>;

Email Configuration

During the course of a conversation Enterprise Collaboration sends mails using the users email addresses.

Not all mail servers allow this as the **EmailGeneralFromName** parameter is set to False by default, preventing emails from being sent.

In this case, change the value of the **EmailGeneralFromName** parameter to **True** manually in the JMX Console.

Install and Configure Enterprise Collaboration

This section contains detailed instructions on how to install and configure Enterprise Collaboration. Before installing check that you have the correct prerequisites and authorizations as described in Prerequisites and Database and Tablespace Authorizations.

Install Enterprise Collaboration

This section includes instructions for the initial installation of Enterprise Collaboration (EC). If you have already installed EC and want to update the configuration, see the section <u>"Update</u> Configuration in the Deployment Manager" (on page 55).

To install Enterprise Collaboration:

 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.

🙀 HP Enterprise Collaboration	n Deployment Manager 1.1	_ 🗆 🗵
Welcome to HP Enterprise Collaboration Deployment Manager 1.1 This wizard will guide you through the HP EC deployment process		
Welcome Installation and use of all products installed with this wizard requires acceptance of the following License Agreement:		
Deployment Type	END USER LICENSE AGREEMENT	-
Host Details PLEASE READ CAREFULLY: THE USE OF THE SOFTWARE IS SUBJECT TO THE TERMS AND CONDITIONS THAT FOLLOW ("AGREEMENT"), UNLESS THE SOFTWARE Deployment Folder Deployment Folder USING THE SOFTWARE (SEGREMENT BETWEEN YOU AND HO PR. ITS SUPPLIERS. BY DOWNLOADING, INSTALLING, COPTING, ACCESSING, OR USING THE SOFTWARE, OR BY CHOOSING THE "IA COEPT' OPTION LOCATED ON OR ADJACENT TO THE SCREEN WHERE THIS ARBEEMENT MAY BE DISPLAYED, YOU AGREE TO THE TERMS OF THIS AGREEMENT, ANY APPLICABLE WARRANTY STATEMENT AND THE TERMS AND CONDITIONS CONTAINED IN THE "ANCILLARY SOFTWARE" (sa defined below). IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER RESON, COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BUTCH THESE TERMS, ICHON TO RE ADJACENT, OR LEGAL ENTITY TO THESE TERMS.		E
Application Network Database Configuration	DO NOT AGREE TO THESE TERMS, DO NOT DOWILOAD, INSTALL, COPY, ACCESS, OR USE THE SOFTWARE, AND PROMPTLY RETURN THE SOFTWARE WITH PROOF OF PURCHASE TO THE PARTY FROM WHOM YOU ACQUIRED IT AND OBTAIN A REFUND OF THE AMOUNT YOU PAID, IF ANY. IF YOU DOWILOADED TH SOFTWARE, CONTACT THE PARTY FROM WHOM YOU ACQUIRED IT.	E
- User Management	QUANTITY OF DEVICES:	
Additional Configurations	1. GENERAL TERMS	
Summary	a. You and Your refer either to an individual person or to a single legal entity.	
Validation	b. HP means Hewlett-Packard Company or one of its subsidiaries.	
Deployment	c. HP Branded means Software products bearing a trademark or service mark of Hewlett-Packard Company or any Hewlett-Packard Company Affiliate, and embedded HP selected third party Software that is not offered under a third party license agreement.	
	d. Software means machine-readable instructions and data (and copies thereof) including middleware and related updates and upgrades You may be separately authorized to receive, licensed materials, user documentation, user manuals, and operating procedures. "Ancillary Software" means all or any portion of Software provided under public, oper source, or third party license terms.	re
	e. Specification means technical information about Software products published in HP product manuals, user documentation, and technical data sheets in effect the date HP delivers Software products to You.	on
	f. Transaction Document(s) means an accepted customer order (excluding pre-printed terms) and in relation to that order, valid HP quotations, license to use certificates or invoices.	
	2. LICENSE TERMS AND RESTRICTIONS	T
	O I accept the terms of the license agreement	
	O I do not accept the terms of the license agreement	
	< Beck Next > Can	cel

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

4. The Deployment Type Selection page opens.

🙀 HP Enterprise Collaboratio	Collaboration Deployment Hanager 1.1	
Deployment Type Selection HP Enterprise Collaboration De	Interprise Collaboration Deployment Manager 1.1 Interprise Collaboration Deployment Manager 1.1 Interprise Collaboration Deployment Type Selection Page Interprise Collaboration Deployment Type Selection Page Interprise Collaboration Deployment Type Selection Page Interprise Collaboration Deployment Selection Select the Required Action: Select the Required Act	
Welcome	Deployment Selection	
Deployment Type	Select the Required Action:	
Host Details	O Complete Deployment and Configuration	
Deployment Folder	O Update Configuration of Deployed Machine	
Network Configuration		
Certificate Configuration		
Application Network		
Database Configuration		
User Management		
Additional Configurations		
Summary		
Validation		
Deployment		
	< Back Next >	Cancel

Select "Complete Deployment and Configuration". Click Next.

5. The EC Deployment Host Details page opens.

🕌 HP Enterprise Collabora	tion Deployment Manager 1.1	
Host Location Specify the Enterprise Collab	poration Host Details	
Welcome Deployment Type Host Details Deployment Folder Network Configuration Certificate Configuration Application Network Database Configuration User Management Additional Configurations Summary Validation Deployment	EC Deployment Host Details O Deploy on the local machine O Deploy on the following machine Remote Host Host Username: Host Username: Host Password: Test: Connection	EC
Specify the EC deployr	nent machine location	<back next=""> Cancel</back>

Select either "Deploy on the local machine" or "Deploy on the following machine".

 If you choose "Deploy on the local machine", the Deployment Folder Configuration page opens.

HP Enterprise Collaborat	ion Deployment Manager 1.1	
Deployment Folder HP Enterprise Collaboration (Deployment Folder Page	(D)
Welcome Deployment Type Host Details Deployment Folder Network Configuration Certificate Configuration Application Network Database Configurations User Management Additional Configurations Summary Validation Deployment	Deployment Folder Configuration Installation Folder: [::\HP\EC Validate Availability Validate Availability	Iccahost EC
		< Back Next > Cancel

Use the **Browse** button to select an 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.

 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 optional, but 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 validation information (such as memory requirements, available ports, etc). If during the configuration process you enter data that affects the validation (e.g. selecting a port that is already in use on the machine), a red 'X' is displayed on the server machine, and the pop-up shows the conflicted port.
- 6. The Network Configuration page opens.

HP Enterprise Collaboration Deployment Manager 1.1			
Network Configuration Configure WebApp ports			2
Welcome Deployment Type Host Details Deployment Folder Network Configuration Application Network. Database Configuration User Management Additional Configurations Summary Validation Deployment	Network Configuration Select an Existing Network Environment: Stand Alone Web Application MTTP/S Reverse Proxy Connection to a Web Application AJP Reverse Proxy Connection to a Web Application 	EC EC	
		< Back Next > Cancel]

- 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 about the possible network environment configurations, see the diagrams in <u>"Appendix A: Network Configuration Schemas for HP Enterprise</u> Collaboration" (on page 67).

- b. Click Next.
- 7. Depending on the network environment selected, one of the following pages opens:
 - Stand Alone Application Configuration

🕌 HP Enterprise Collaborat	ion Deployment Manager 1.1	
Network Configuration Configure Stand Alone Applic	ation	(hp
Welcome Deployment Type Host Details Deployment Folder Network Configuration Application Network Database Configuration User Management Additional Configurations Summary Validation Deployment	Stand Alone Application Configuration Note: Authentication uses a secure connection by default. To block incoming HTTP traffic to the web application, Additional frewall configuration is required. Selecting the following option may affect performance. Use a Secure Connection to connect to the Web Application Web Application Details: FQDN: HAKIPU1.emea.hpgcorp.net FIII IP/Domain IP Address: 16.60.206.137 Domain Name: emea.hpgcorp.net HTTP Port: 8080 HTTPS Port: 8443	localhost
		Back Next > Cancel

HTTP/S Reverse Proxy Configuration

🔁 HP Enterprise Collaborati	on Deployment Manager 1.1	
Network Configuration Configure Reverse Proxy		
Welcome Deployment Type Host Details Deployment Folder Hetwork Configuration Application Network Database Configuration User Management Additional Configurations Summary Validation Deployment	HTTP/S Reverse Proxy Configuration Mote: Authentication uses a secure connection by default.	Iccahost I EC
🤳 Insert FQDN		Kext > Cancel

AJP Reverse Proxy Configuration

没 HP Enterprise Collaborat	ion Deployment Manager 1.1	
Network Configuration Configure AJP Proxy		
Welcome Deployment Type Host Details Deployment Folder Hetwork Configuration Certificate Configuration Application Network Database Configuration Liser Management Additional Configurations Summary Validation Deployment	AP Reverse Proxy Configuration Note: Authentication uses a secure connection by default. To block incoming HTTP traffic to the web application, Additional frewal configuration is required. Selecting the following option may affect performance. Use a Secure Connection to connect to the Web Application Reverse Proxy Details: FQDN: PAddress: Domain Name: Reverse Proxy HTTP Port: 8080 Reverse Proxy HTTP Port: 8080 Reverse Proxy HTTP Port: 8080 To connect to a web application using a non-secure connection: AJP Port: 8009 To connect to a web application using a secure connection: AJP Port: 8109	localhost EC
1 Insert FQDN		< Back Mext > Cancel

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.

To block incoming HTTP traffic to the web application additional firewall configuration is required.

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 default value is the FQDN of the deployed machine.

Note: After entering the FQDN, click **Fill IP/Domain** to make the wizard automatically enter the IP Address and Domain Name.

- 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.
- 8. The Certificate page opens:

HP Enterprise Collaborati	on Deployment Manager 1.1	
Certificate Configuration HP Enterprise Collaboration C	ertificate Configuration Page	пр пр
Welcome	Certificate Configuration	
Deployment Type	 Use temporary certificate 	
Host Details	O Use custom certificate	
Deployment Folder	Keystore file path: Browse	
Network Configuration	Keystore type JKS 💌	localhost
Certificate Configuration	Keystore Password	
Application Network	Key alias	<u>₽</u>
Database Configuration	Key Bacquord	
User Management	KGY Fassword	
Additional Configurations		EC
Summary		
Validation		
Deployment		
		< Back Cancel

The certificate page is used to add a server certificate to EC in order to work with a secure connection to the web application. If the customer wants to import their own certificate from an existing keystore, they must enter the keystore path, keystore type, keystore password.

In the key alias field, they should enter the alias of the certificate they want to add to EC as it appears in their own keystore.

In the key password field, they should enter the password of the certificate in the keystore. If the certificate does not have a different password, the keystore password should be entered.

By default, EC generates a temporary self-signed certificate.

9. Click Next.

The Application Network Configuration page opens.

HP Enterprise Collaborat	ion Deployment Manager 1.1	
Application Network Con HP Enterprise Collaboration A	figuration pplication Network Configuration Page	
Welcome Deployment Type Host Details Deployment Folder Network Configuration Certificate Configuration Application Network Database Configuration User Management Additional Configurations Summary Validation Deployment	Application Network Configuration JMS Port: 61616	Iccalhost EC
		< Back Next > Carrel

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

10. The Database Server Configuration page opens.

🙀 HP Enterprise Collaboratio	on Deployment Manager 1.1		>
Database Server Configu	ration		(p)
Welcome Deployment Type Host Details Deployment Folder Network Configuration Certificate Configuration Application Network User Management Additional Configurations Summary Validation Deployment	Database Administrator Configuration: Orade	Database I	localhost
🧜 Enter a database host n	ame or IP address for Database		< Back Next > Cancel

11. Select Oracle or MSSQL.

Configure the Oracle Database Administrator:

没 HP Enterprise Collaborati	on Deployment Manager 1.1		
Database Server Configu	ration		Ø
Welcome Deployment Type Host Details Deployment Folder Network Configuration Application Network Database Configuration User Management Additional Configurations Summary Validation Deployment	Database Administrator Configuration: Oracle MSQL Connect to an existing schema Create a new schema Database Host Name/IP:	Database	iocalhost
! Enter a database host r	ame or IP address for Database		<back next=""> Cancel</back>

Schema:

Select either Connect to an existing schema or Create a new schema.

- 12. Enter the following information:
 - Database Host Name/IP
 - **Port:** A default value of 1521 is shown.
 - SID/Service: System ID.
 - Admin Username
 - Admin Password
 - **Application Username:**The name of the schema that the application uses to connect to the database.
 - Application User Password
 - Confirm Password
 - **Default Tablespace:** The tablespace of the schema. If the schema does not have a tablespace, enter **System** in this field.

13. Configure the MSSQL Database Administrator:

🙀 HP Enterprise Collaborat	ion Deployment Manager 1.1		
Database Server Configu	ration	1	Ø
Welcome Deployment Type Host Details Deployment Folder Network Configuration Application Network Database Configuration User Management Additional Configurations Summary Validation Deployment	Database Administrator Configuration: O Cracle O MSQU Connect to an existing schema O Create a new schema Database Host Name/IP: Port: 1433 Database Username: Database Varname: Database Name: Database Name: Application User Credentials: Application DB User: Application DB Password: Validate Application Access Skip Database configuration	Database	Iccahost
			< Back Next > Cancel

- 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 Connect to an existing schema, enter the name of the database to connect to. If you selected Create a new schema, enter the name of the new database.
- 14. Enter Application User Credentials:

Application DB User: The name of the user used by the application to communicate with the database.

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

15. Click the Validate Application Access button.

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

- 16. Click Next.
- 17. The User Management Configuration page opens.

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

HP Enterprise Collaboratio	n Deployment Manager 1.1		
HP Enterprise Collaboratic User Management Config Set the administrator user Welcome Deployment Type Host Details Deployment Folder Network Configuration	n Deployment Manager 1.1 uration details User Management Configuration Temporary Administrator Login Name: Temporary Administrator Password: Confirm Password:		Iccalhost
Certificate Configuration Application Network Database Configuration User Management Additional Configurations Summary Validation Deployment	Note: 1. A Temporary administrator will be used to set permissions for users and groups, on first login. 2. Your temporary administrator login name should be different from the existing login names in the user repository.	Database	EC
! Insert temporary adm	inistrator user and password]]	< Back Next > Cancel

- a. Enter the following information:
 - Temporary Administrator Login Name: This login name should not exist in your existing user repository and must not have been used in previous installations when selecting "Connect to existing schema" in "Schema:" (on page 19).
 - Temporary Administrator Password
 - Confirm Password
- b. Click Next.
- 18. The Lightweight Single Sign-On (LW-SSO) configuration page appears.

🙀 HP Enterprise Collaborati	on Deployment Manager 1.1		_0
LW-SSO Configuration Set the LW-SSO Integration u	iser details and init string		(p)
Welcome Deployment Type Host Details Deployment Folder Network Configuration Certificate Configuration Application Network Database Configuration User Management Additional Configurations Summary Validation Deployment	Lightweight Single Sign On Configuration UW-SSO Init String: Confirm Init String: Note: UW-SSO initstring: same initstring should be usea for integrating single sign-on products.	Database	Iocahost
			< Back Cancel

Enter the LW-SSO Init String, confirm the string and click Next.

19. The Email Configuration page opens.

HP Enterprise Collaborati	on Deployment Man	ager 1.1				_ 🗆 ×
Email Configuration HP Enterprise Collaboration P	roduct Page			4		(III)
Welcome Deployment Type Host Details Deployment Folder Network Configuration Certificate Configuration Application Network Database Configuration User Management Additional Configurations Summary Validation Deployment	Email Configural Protocol: Hostname: Port: User Name: Password: Encryption Type: Trust Server: Secure Port: Secure Port: Skip Note: EC automa	tion Sending Email Info SMTP 465 5SL Approve 465 tically detects the authential	Receiving Email Info POP3 Info Info Info Receiving Email Info POP3 Info Info Receive Pops Validate Kabion method used.	Database	Iccalhost Internet Sector EC	
! Insert Receiving Hostna	me				< Back Next > Can	cel

The information on this page is divided into Sending Email and Receiving Email information. For each type of email, fill in the following:

- a. **Protocol:** Select a protocol to use to send/receive data. For sending data, use SMTP. For receiving data, select either POP3 or IMAP4.
- b. Hostname: The hostname of the incoming/outgoing mail server.
- c. **Port:** The port number of the incoming/outgoing data.
- d. Username: The EC mailbox username for receiving/sending emails.
- e. **Password:** The password for the EC mailbox.
- f. **Encryption Type** Select the encryption to be used for the email server. If your protocol is secured, select SSL or TLS according to the email server configuration:
 - SSL: For SSL encryption, the **Secure Port** field is filled in automatically with the port number and cannot be changed
 - TLS Trust Server. Enter the port number manually in the Secure Port field.

For each encryption type, select **Approve** to add the secure port.

These definitions are used for validating and installing certificates for EC to work against.

Optional: Test the Email configuration by clicking the "Validate" button after entering all the configuration settings. After clicking this button, the EC installer checks if the Email server uses a server certificate and if necessary automatically adds it to the EC keystore.

Click Next.

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

20. 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**.

21. The Validation page opens.

🕌 HP Enterprise Collaboratio	n Deployment Manag	er 1.1			_ 🗆 ×
Validation Environment and deployment p	parameter validations		1		(III)
Welcome Deployment Type Host Details Deployment Folder Network Configuration Certificate Configuration Application Network Database Configurations User Management Additional Configurations Summary Validation Deployment	Name Localhost Localhost Localhost Localhost Localhost Localhost Localhost EC EC EC Database Database	Status Preparing to validate localhost Verfy that host name is defined Verfy operating system compatibility Verfy operating system compatibility Verfy operating system compatibility Verfy diskspace 4000 MB of diskspace are verified to Verfy that the required ports are a Verfy that a deployment machine is Verfy that all mandatory properties Verfy that all mandatory properties	Database	localhost	
				< Back Deploy	Cancel

Validation occurs automatically when clicking Next in the Summary page.

- If all icons are green, validation is 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 has been fixed.
- 22. Click **Deploy**.
- 23. Wait for deployment to finish 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

Configure the User Repository and User Roles

After completing the 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:

1. Update the external-Idap.properties file located in the /conf directory, according to the instructions in "Appendix B: Updating the external-Idap.properties File" (on page 68).

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-Idap-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 **Start > All Programs > 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 defined during the installation process.
- 7. The User Management UI opens.

User Management Role Management Environment Management				
Ø?				_
1 Users & Groups	User Details			
	Firet Name :			
	Last Name :			
Search Users	Losi Name :			
First Name :	Display Name :			
Last Name :	Emeil:			
Login Name :	Eritäria.			
Display Name :	[Lun dottina]			
Email :	Datas and Demissions			
Search	Roles and Permissions			
User Name	Role name	Permission	Environment	
+ X	tit No Dolog tit		# Colort a role to view ite permissions #	
Enter your search criteria and click the search button.	Ho Roles			
	3			
	<			
		L		

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.

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

User Management Role Management Environment Management			
0 ?			
	liser Dataile		
👗 Users & Groups 🔒 Search Users	User Details		
	First Name : admin		
Carbonard Exceptional Exception Exceptio			
Search Users	Login Name : admin		
First Name :	Display Name : admin		
Last Name :			
Login Name : admin	Crit desize		
Display Name :	(Loss Messel)		
Entel			
	Roles and Permissions		
Search			
User Name	Role name	Permission	Environment
* X	EC Admin	₽- Q BSF	
🛔 admin		Users Administration	Not Applicable
		E-Q damond	
		- E EXECUTE JMX	Not Applicable
		- CESS DIAMOND	Not Applicable
		Users Administration	Not Applicable
	1		
		<	
L.			
<u></u>			

9. The Assign Roles dialog box opens.

Available Roles EC User Image: C Admin Permission details for selected roles: Permission Environment Image: C Admin Image: Access DIAMOND Not Applicable	ect the re	the r	e requ	uired	I roles	s and c	click 0)K to s	save.
Permission Environment Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. Image: Comparison of the selected roles. <	ected Rol	EC	Role: C Ad	es Amin					
diamond ACCESS DIAMOND Not Applicable	nment	ent							
ACCESS DIAMOND Not Applicable									
	plicable	able	e						
					1	OK	\sim	С	ancel

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 give at least one EC Admin user 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**.

Configuration for Secure Login when Using Reverse Proxy

When using Secure Login (HTTPS) with Reverse Proxy, perform the following steps after the installation has completed and before starting the server:

- 1. Open the bsf.war package using 7zip, WinRAR or any suitable extraction program to edit its internal content.
- 2. Open the file C:\HP\EC\servers\server-0\webapps\bsf.war\WEB-INF\applicationContextsecurity.xml.
- 3. Update the forceHttps value to true as follows (marked in bold):

```
<bean id="authenticationProcessingFilterEntryPoint"
class="com.hp.sw.bto.security.springsecurity.
BSFAuthenticationProcessingFilterEntryPoint">
<property name="loginFormUrl">
<value>/login.form</value>
</property>
<value>true</value>
</property>
</bean>
```

 Update the file C:\HP\EC\servers\server-0\webapps\diamond\WEB-INF\classes\diamondlwssofmconf.xml by adding the lines in bold to the webui section:

```
<nonsecureURLs>
    <url>.*/images/.*</url>
    <url>.*/desktopClient/.*</url>
</nonsecureURLs>
</reverseProxy enabled="true">
<full-
ServerURL>https://your.reverse.proxy.fqdn:8443/</fullServerURL>
</reverseProxy>
```

 Validate that the authentication point is pointing at the reverseProxy. To do so, edit the file C:\HP\EC\conf\client-config.properties and check the marked value (it should have the reverseProxy FQDN).

bsf.server.url=https://your.reverse.proxy.fqdn:8443/bsf

Chapter 3

Set Up Integration with Office Communicator Server and MS Lync Server

Enterprise Collaboration can integrate with the following versions of MS Communicator Servers:

- Office Communicator Server 2007 (OCS)
- MS Lync 2010 Server

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 29)
- "Download and Install the Root CA Certificate" (on page 34)

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.

Chapter 3: Set Up Integration with Office Communicator Server and MS Lync Server

🚟 Console1 - [Console Root]		
🚟 File Action View Favorites Window H	Help	_B×
Console Root	Name	Actions
	There are no items to show in this view.	Console Root 🔹
		More Actions
,	,	,

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

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

Chapter 3: Set Up Integration with Office Communicator Server and MS Lync Server

Add/Remove Snap-in 🔹 😵 🗙
Standalone Extensions
Use this page to add or remove a stand-alone snap-in from the console.
Snap-ins added to: Gonsole Root
Certificates (Local Computer)
Description
Add Remove About
Cancel

Select Certificates. Click Add.

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

A	dd Standalone Snap-in		?	×
	Available standalone snap-ins:			
	Snap-in	Vendor		
	Active Directory Domains and Trusts	Microsoft Corporation		
	📓 Active Directory Sites and Services	Microsoft Corporation		
	Active Directory Users and Compu	Microsoft Corporation		
	al ActiveX Control	Microsoft Corporation		
	🛺 Authorization Manager	Microsoft Corporation		
	🔯 Certificate Templates	Microsoft Corporation		
	Certificates	Microsoft Corporation		
	Certification Authority	Microsoft Corporation		
	🔄 Communicator Web Access	Microsoft Corporation		
	Discomponent Services	Microsoft Corporation	-	l.
	Description The Certificates snap-in allows you to bro certificate stores for yourself, a service,	wse the contents of the or a computer.		
	[<u>A</u> dd	e)]

5. The Certificates snap-in dialog opens.

Chapter 3: Set Up Integration with Office Communicator Server and MS Lync Server

Certificates snap-in	×
This shap in will always manage certificates for	
This shaphin will always manage certificates for.	
O <u>My</u> user account	
Service account	
Computer account	
	< <u>B</u> ack <u>N</u> ext > Cancel

Select Computer Account. Click Next

6. The Select Computer dialog opens.

Select Computer	X
Select the computer you want this snap-in to manage. This snap-in will always manage:	
< <u>B</u> ack Finish Cancel	

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 the CA that issued it.

Chapter 3: Set Up Integration with Office Communicator Server and MS Lync Server

Tonsole1	
Eile Action View Favorites Window Help	
Console Root Cons	Onol/Certificates Issued By Expiration Date test-ADTESTDC1-CA 9/19/2013 Certificate ? × General Details Details Certification Path Emeral Details Certificate Information This certificate is intended for the following purpose(s): •Ensures the identity of a remote computer
• » •	Issued to: OCS2007R2.test.net
Personal store contains 1 certificate.	Issued by: test-ADTESTDC1-CA
	Valid from 9/20/2011 to 9/19/2013
	\mathscr{P} You have a private key that corresponds to this certificate.
	Issuer Statement
	ОК

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

Certificate	? ×
General Details Certification P	ath
Show: <all></all>	V
Field	Value 🔺
Subject Key Identifier Authority Key Identifier CRL Distribution Points Authority Information Acces Certificate Template Name Key Usage Thumbprint algorithm	3b 2d 14 b2 1c d7 70 9f c0 f3 KeyID=0e e7 f2 bd fa e6 cd 4 [1]CRL Distribution Point: Distr ss [1]Authority Info Access: Acc WebServer Digital Signature, Key Encipher sha1 19 b9 80 2d 0a 03 a3 b5 c8 45 ▼
[1]CRL Distribution Point Distribution Point Name: Full Name: URL= <u>http://adtestdc1</u> CA.crl	.test.net/CertEnroll/test-ADTESTDC1- Edit Properties Copy to File

11. Use the Authority Name in the URL line 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 image 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.
- 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.

Welcome Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Active Directory Certificate Services, see <u>Active Directory Certificate Services</u> <u>Documentation</u> .
Select a task:
Request a certificate
View the status of a bending certificate request
Dowinioad a CA certificate certificate chain, of CRL

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

4. The following page opens.

Chapter 3: Set Up Integration with Office Communicator Server and MS Lync Server

Microsoft Active Directory Certificate Services SecLabCorp Hom	ne
Download a CA Certificate, Certificate Chain, or CRL	_
To trust certificates issued from this certification authority, install this CA certificate chain.	
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.	
CA certificate:	
Encoding method:	
● DER ◎ Base 64	
Download CA certificate Download CA certificate chain Download latest base CRL Download latest delta CRL	

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 window, click Add.
- 9. In the Add Standalone Snap-In window, select Certificates from the list. Click Add.
- 10. In the Certificates snap-in window, select Computer Account. Click Next.
- 11. In the Select Computer window, select Local Computer. Click Finish.
- 12. In the Add Standalone Snap-In window, click Close.
- 13. In the Add/Remove Snap-In window, click OK.

The Certificate Import Wizard is launched.

Chapter 3: Set Up Integration with Office Communicator Server and MS Lync Server



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

Certificate Import Wizard
Certificate Store Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
O Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities Browse
Learn more about <u>certificate stores</u>
< Back Next > Cancel

16. When the wizard finishes, go to the **Console Root** and right-click on the **Trusted Root Certification Authorities** folder.
17. A pop-up menu opens.

Go to **All Tasks > Import** to import the Root CA certificate.

🚡 Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Cert 💶 🗙				
🚡 Eile Action View Fa	vorites Window Help			
	1 🗈 🛛 🕄 💷			
Console Root	puter) Object Type			
Certificates Enterprise Trust	All Tas <u>k</u> s Find Certificates			
Trusted Publisher: Trusted Certific	View Import			
	New <u>T</u> askpad View			
⊕ Certificate Enrollm ⊕ in SPC	Refresh Export <u>Li</u> st			
	Help			
Contains actions that can be performed on the item.				

Install the Server Certificate on the OCS Agent Machine

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

- 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.

Chapter 3: Set Up Integration with Office Communicator Server and MS Lync Server

	-
Microsoft Active Directory Certificate Services test-ADTESTDC1-CA	
Welcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.	
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.	
For more information about Active Directory Certificate Services, see <u>Active Directory</u> Certificate Services Documentation.	
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	
	-

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

Microsoft Active Directory Certificate Services test-ADTESTDC1-CA				
Request a Certificate				
Select the certificate type: User Certificate				
Or, submit an advanced certificate request.				

Select advanced certificate request.

4. The Advanced Certificate Request screen opens.

Chapter 3: Set Up Integration with Office Communicator Server and MS Lync Server

Microsoft Active Directory Certificate Services test-ADTESTDC1-CA	<u>Home</u>
Advanced Certificate Request	
The policy of the CA determines the types of certificates you can request. Click one following options to:	of the
Create and submit a request to this CA.	
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file submit a renewal request by using a base-64-encoded PKCS #7 file.	<u>ə, or</u>

Select Create and submit a request to this CA.

5. The Advanced Certificate Request form opens.

Chapter 3: Set Up Integration with Office Communicator Server and MS Lync Server

Microsoft Active	Directory Certificate Services test-ADTESTDC1-CA	<u>Home</u>	
Advanced Ce	rtificate Request		
Certificate Temp	olate:		
	Web Server		
Identifying Infor	mation For Offline Template:		
Name:	OCS agent machine FQDN goes here		
E-Mail:			
Company:			
Department:			
City:			
State:			
Country/Region:			
Key Options:			
	O Create new key set		
CSP:	Microsoft RSA SChannel Cryptographic Provider		
Key Usage:	Exchange		
Key Size:	2048 Min: 384 (common key sizes: <u>512 1024 2048 4096 8192 16384</u>) Max: 16384		
	Automatic key container name O User specified key container name		
	☐ Mark keys as exportable		
	Enable strong private key protection		
Additional Optio	ins:		
Request Format:	©CMC ○PKCS10		
Hash Algorithm:	SHA-1 V		
	Only used to sign request.		
	🗖 Save request		
A ++ -: [A		
Attroutes:	<u>۲</u>		
Friendly Name:			
	Submit >		Î

Fill in the form. Note that the "Mark keys as exportable" check box may appear disabled. If you browsed from the OCS agent machine this check box 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.

Chapter 3: Set Up Integration with Office Communicator Server and MS Lync Server

<i>Microsoft</i> Active Directory Certificate Services test-ADTESTDC1-CA	<u>Home</u>
Certificate Issued	
The certificate you requested was issued to you.	
Install this certificate	
□ Save response	

 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.

Microsoft Active Directory Certificate Services test-ADTESTDC1-CA	<u>lome</u>
Certificate Pending	
Your certificate request has been received. However, you must wait for an administrate issue the certificate you requested.	or to
Your Request Id is 734.	
Please return to this web site in a day or two to retrieve your certificate.	
Note: You must return with this web browser within 10 days to retrieve your certificate	
i. After you get a message that the certificate was issued, browse to the CA web site	

- i. After 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) as you did in Step 1.
- ii. In the Welcome screen that appears, click View the status of a pending certificate request.

Chapter 3: Set Up Integration with Office Communicator Server and MS Lync Server



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

Microsoft Active Directory Certificate Services test-ADTESTDC1-CA	<u>Home</u>
View the Status of a Pending Certificate Request	
Select the certificate request you want to view:	
(Sunday December 04 2011 2:17:20 PM)	

- iv. The Certificate Issued screen appears. Select Install this certificate.
- 7. Verify that you get the following message.

Microsoft Active Directory Certificate Services -- test-ADTESTDC1-CA

Certificate Installed

Your new certificate has been successfully installed.

- 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 (shown in the first image below) to the Certificates (Local Computer)/Personal/Certificates (shown in the second image below).



Chapter 3: Set Up Integration with Office Communicator Server and MS Lync Server

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]						
🚘 File Action View Favorites Window Help						
🗢 🔿 🗾 🖬 📋 💁 📴 🖬	🗢 🔿 📶 📋 🕰 💀 📓 🖬					
Console Root	Issued To 🔺	Issued By	Expiration Date	Intended Purpose:		
Certificates (Local Computer)	🕼 hive-1.test.net	test-ADTESTDC1-CA	11/16/2013	Server Authentical		
Personal	-					
Certificates						
Trusted Root Certification Authorities						
Enterprise Trust						
Intermediate Certification Authorities						
Trusted Publishers						
Untrusted Certificates						
Third-Party Root Certification Authorities						
Trusted People						
Remote Desktop						
E Certificate Enrolment Requests						
E Smart Card Trusted Roots						
Trusted Devices						
🖃 🔜 Certificates - Current User						
🖃 🚞 Personal						
Certificates						
🗄 🧮 Trusted Root Certification Authorities						
Emerprise Trust						
Intermediate Certification Authorities						

Agent Provisioning

This section describes how to set up Agent Provisioning for Office Communicator Server 2007 and Lync Server 2010.

Agent Provisioning for OCS 2007

Prerequisites

- 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.

To set up agent provisioning for Office Communicator Server 2007:

- 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.

Chapter 3: Set Up Integration with Office Communicator Server and MS Lync Server

Application Provisioner		
Application name:	Fin	d or Create
Application Application pool:		Add
Contacts:	Servers:	
Add Ren	ove Edit Add Remove	View

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

4. The Create Application Pool dialog box opens.

Application Provisioner	_ 🗆 ×
Application name: HPEC	Find or Create
Create Application Pool	
Application name: HPEC	Add
OCS Pool Fqdn: OCS2007R2.test.net	
Listening port. 9913	
Application server Fqdn: hive-1.test.net	ost
Load balanced application	_
OK Cance	View

- 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.
 - Select the Localhost check box.
- 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.

Chapter 3: Set Up Integration with Office Communicator Server and MS Lync Server

Application	n Provisioner			
Applicatic	Create Contact			_ 🗆 🗙 ate
HPEC	Contact Uri:			
Applica	Display name:			<u>t</u>
Contac	Phone Uri:			
	OCS Pool Fqdn:	OCS2007R2.test.net		T
	Enabled for fe	deration		
	Enabled for p	ublic IM connectivity		
			ОК	Cancel
Ac				w

- 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.

Application Provi	sioner	_ 🗆 ×
Application name:	HPEC	Find or Create
HPEC		
View Server		
Server Figdn:	hive-1.test.net	
Listening port:	9913	
Gruu:	sip:hive-1.test.net@test.net;gruu;opaque=srvr:HPEC:GxmKksJP	
	OK Cancel	1
Add	Remove Edit Add Remov	ve View

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

Agent Provisioning for Lync 2010

1. On the Lync Server machine, run:

```
Start > Microsoft Lync Server 2010 > Lync Server Management
Shell
```

2. Create a trusted application by running the following command:

```
New-CsTrustedApplication -ApplicationId <application-id> -Port <application-port> -TrustedApplicationPoolFqdn <ocs-agent-fqdn>
```

For example:

```
New-CsTrustedApplication -ApplicationId EeApplicationId -Port 6000
-TrustedApplicationPoolFqdn exum.fabrikam.com
```

No errors should occur:

🐺 Administrator: Lync Server Manag	jement Shell	٧×
PS C:\Users\Administrator.l applicationpoolfqdn exum.f WARNING: The following char Enable-CsTopology must stil	FABRIKAM> new-cstrustedapplication -applicationid EeApplicationId -truste abrikam.com -port 6000 nges must be made in order for the operation to be complete. 11 be run for all changes to take effect.	.d 🛌
Identity	: exum.fabrikam.com∕urn:application:eeapplicationid	
ComputerGruus	: {exum.fabrikam.com sip:exum.fabrikam.com@fabrikam.com;gruu;opaque=srvr :eeapplicationid:hr10ogJNF10kKB9UaWsC7AAA>	
ServiceGruu	: sip:exum.fabrikam.com@fabrikam.com;gruu;opaque=srvr:eeapplicationid:hr 10ogJNF10kKB9UaWsC7AAA	
Protocol	: Mtls	
ApplicationId	: urn:application:eeapplicationid	
TrustedApplicationPoolFqdn	: exun.fabrikam.com	
Port	: 6000	
LegacyApplicationName	: eeapplicationid	

- 3. Save the ServiceGruu value for further configuration of the OCS agent.
- 4. Enable topology by running the following command:

Enable-CsTopology

5. Create trusted application endpoint by running the following command:

```
New-CsTrustedApplicationEndpoint -SipAddress <app-sip>
-DisplayName <app-display-name> -TrustedApplicationPoolFqdn <ocs-
agent-fqdn> -ApplicationId <app-id>
```

For example:

```
New-CsTrustedApplicationEndpoint -SipAddress sip:ee@fabrikam.com -
DisplayName EE
-TrustedApplicationPoolFqdn exum.fabrikam.com -ApplicationId
```

EeApplicationId

😹 Administrator: Lync Server M	anagement Shell	_ 8 ×
PS C:\Users\Administrat com -displayname "EEApp d	or.FABRIKAM> new-cstrustedapplicationendpoint -sipaddress sip:eeapp@fabri " -trustedapplicationpoolfqdn exum.fabrikam.com -applicationid EeApplicat	kan. ionI
Identity	: CN={a6b170dd-03d8-47aa-bd40-bd91f89c83b6>,CN=Application Contacts,CN=RI ervice,CN=Services,CN=Configuration,DC=fabrikam,DC=con	C S
RegistrarPool	: 912668696	
HomeServer	: CN=Lc Services, CN=Microsoft, CN=fabrikan.con:1, CN=Pools, CN=RTC Service, C ervices, CN=Configuration, DC=fabrikan, DC=con	IN=S
OwnerUrn	: urn:application:EeApplicationId	
SipAddress	: sip:eeapp@fabrikan.com	
DisplayNane	: EEApp	
DisplayNumber		
LineURI		
PrimaryLanguage	= 0	
SecondaryLanguages	= <u>O</u>	
EnterpriseVoiceEnabled	: Irue	
Enabled	: True	

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

a 172.16.239.24 - Remote Desktop Connection _ 8 × Group Policy Object Editor _ 8 × Elle Action View Help ⇔ → 🗈 🗷 🗟 😭 🖬 💕 Local Computer Policy Microsoft Office Communicator Feature Policies 🖻 🛃 Computer Configuration 🖲 📄 Software Settings State Select an item to view its description. Setting 🔄 🦲 Windows Settings 🕃 Specify transport and server Not configured 😑 🚞 Administrative Templates 🗿 Enable strict DNS naming for server name Not configured E Microsoft Office Communicator Policy Settings 😫 Configure SIP security mode Not configured Microsoft Office Communicator Feature Policies Configure SIP compression mode Not configured E - Windows Components 🖇 Prevent users from running Microsoft Office Communicator Not configured E System Allow storage of user passwords Not configured 🧰 Network 🕅 Require logon credentials Not configured Printers 🖥 Enable UPNP Not configured 🖃 🚮 User Configuration Not configured 🖇 Disable HTTP fallback for SIP connection - Software Settings Address Book Server Inside URL Not configured Windows Settings
 Address Book Server Outside URL Administrative Templates Not configured Disable server version check Not configured Additional server versions supported Not configured Disable Emoticons in Instant Messages Not configured 🛐 Prevent Ink in instant messages Not configured 🖗 Prevent rich text in instant messages Disabled 🗿 Allow hyperlinks in instant messages Enabled Warning Text Not configured Enable web browser in conversation window Not configured Prevent users from saving instant messages Not configured Block conversation from federated contacts Not configured Specify encryption for computer-to-computer audio and video calls Not configured Enable the state Appear Offline Not configured Disable Presence Note Not configured

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.
 - 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.

Chapter 3: Set Up Integration with Office Communicator Server and MS Lync Server

Microsoft Office Communication	is Server 2007 R2			
📴 Eile <u>W</u> indow <u>H</u> elp				_8×
Office Communications Server 2007 Forest - Advantage.uk	Coffice Commun Server 2007 R2	ications		
Standard Edition Servers	Status	Database	Resources	
Remove Pool				
E A Logging Tool	Settings		ustanut advantana uk	
E- W Filtering <u>I</u> cols	 Intelligent 	Instant Message Filte	wzkorzkowiauvankageluk	
Monitoring Device Updab	er <u>C</u> lient Vers	ion Filles	one>	
Unassigne Properties	•		5061	
Unassigne View	cation protoco	ol:	Both NTLM and Kerberos	
Mediation New Window	from Here server compr	ession:	2	
Earlier ser Refresh	sximum video	quality:	<none></none>	
Help	routes (outbo	ound connections)		
				-
	Default certificate sett Server name: w2k3r2x64.advantage @ Mgdia Settings	tings: e.uk	Enabled/Disabled:	
× >	•			

c. In the URL Filter tab, clear the Enable URL filtering check box, as shown below.

fice Filter	Communications Server 2007 R2 Intelligent IM Filter
En	able URL filtering
V	Block all hyperlinks, both intranet and Internet, that contain any of the file extensions defined on the File Transfer Filter t
V	Allow Jocal intranet URLs
(C Block instant messages that contain hyperinks
(Allow instant messages that contain hyperlinks, but gonvert the links to plain text. Enter the notice you want to insert at the beginning of each instant message containing hyperlinks.
	Allow instant messages that contain hyperlinks. Enter the warning you want to insert at the beginning of each instant message containing hyperlinks.
Γ	Enter the prefixes, separated by a space, that you want the URL filter to block.
	href www", ftp. http:://ttp:/
	Bestore Defaults DK Cancel Apply Help
	Towne concert

d. In the File Transfer Filter tab, clear the Enable file transfer filtering check box, as

shown below.

File Transfer Filter	
able file transfer filtering	
Block all file extensions	
Block only file extensions in	the list below
nter the file extensions, begin	ning with a period and separated by a space, that you want the file transfer
ter to block. If this list is empty	y, all file extensions will be blocked.
ade .adp .app .asp .bas .bat js .jse .ksh .lnk .mad .maf .ma	t.cer.chm.cmd.com.cpl.crt.csh.exe.fxp.grp.hlp.hta.inf.ins.isp.its 🖉 👘
mdz .msc .msi .msp .mst .ocx reg .scf .scr .sct .shb .shs .tm	k.ops.pod.pif.pl.pnp.pf.prg.ps1.ps2.ps1xml.ps2xml.psc1.psc2.pst mp.url.vb.vbe.vbs.vsd.vsmacros.vss.vst.vsw.ws.wsc.wsf.wsh
	×.
	×
	×
	<u>v</u>
	Y

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 Testing 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.

Chapter 3: Set Up Integration with Office Communicator Server and MS Lync Server

- 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

Perform Additional Configuration Steps

This section presents two manual processes that should be used if the automatic process during the installation has failed.

Install a Certificate for the Mail Client

There are two ways to 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.

Method 1

- 1. Complete the EC installation providing Email configuration data, but without running Email configuration validation.
- 2. Discover with IT which ports of the email server are secure.
- 3. On the EC server, run **diamond-deploy/add-email-certificates.bat** with the following parameters:

add-email-certificates.bat <email-sending-host>:<email-sending-secure-port> <email-receiving-host>:<email-receiving-secure-port>

For example:

add-email-certificates.bat exch14.net:466 exch14.net:996

4. Restart the EC server.

Method 2

- 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 selfsigned 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\eckeystore.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.

Chapter 5

Update Configuration in the Deployment Manager

You can update the configuration from the **Deployment Type** tab of the Deployment Manager.

- 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.

Select Update Configuration of Deployed Machine.

4. Additional options appear for selecting the type of configuration update.

Deployment Type Selecti HP Enterprise Collaboratio	on n Deployment Type Selection Page
Welcome	Deployment Selection
Host Details Deployment Folder Network Configuration Certificate Configuration Application Network Database Configuration User Management Additional Configurations Summary Validation Deployment	Complete Deployment and Configuration Update Configuration of Deployed Machine Select Required Configuration Update: Database Configuration (includes user management setup for temporary admin user) Communication Channels Configuration Update custom certificate Note: Configuration pages which are not required will be skipped automatically.
	< Back Next > Cancel

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
- Validation
- 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 <u>"Set Up Integration with</u> Office Communicator Server and MS Lync Server" (on page 29).
 - **Upload Custom Certificate:** Select this configuration to upload a customized security certificate at the end of the installation. See Step 8 for details.

It is possible to select all configuration options.

- 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.

Chapter 5: Update Configuration in the Deployment Manager

HP Enterprise Collaboration Deployment Manager 1.0		
Welcome Deployment Type Host Details Deployment Folder Network Configuration Application Network Database Configuration User Management Summary Validation Deployment	Communication Channels Configuration OCS Server PQDN: OCS Application Name: IPEC OCS Application Port: 9913 OCS Application GRUU: OCS Application SIP URI: sip:HPEC@ OCS Application SIP URI: sip:HPEC@ OCS Application Channels configuration Image: Skip Communication Channels configuration Note: OCS Application GRUU: is the trusted application parameter called GRUU in Approvisioner.	
Insert OCS Server FQDN	N Can	tel

- 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 <u>"Set Up</u> Integration with Office Communicator Server and MS Lync Server" (on page 29) process.
 - OCS Server Port: The default value is 5061. Consult your system administrator for this port number.
 - OCS Application Name: The default name is EE. Enter here the Display Name that you entered during the "Set Up Integration with Office Communicator Server and MS Lync Server" (on page 29) process.
 - OCS Application Port: The default value is 6000. Enter here the Listening Port number that you entered during the <u>"Set Up Integration with Office Communicator Server and</u> MS Lync Server" (on page 29) process.
 - OCS Application GRUU: Enter here the string that you obtained during the <u>"Set Up</u> Integration with Office Communicator Server and MS Lync Server" (on page 29) process.
 - OCS Application SIP URI: The default value is sip:EE@. Enter here the Contact Uri that you entered during the <u>"Set Up Integration with Office Communicator Server and MS Lync</u> Server" (on page 29) process.
 - OCS Agent FQDN: This value should be the FQDN of the EE server.

- 8. If you choose **Upload Custom Certificate**, select to **Use temporary certificate** or to use a customized certificate **Use custom certificate**.
- 9. If you select **Use custom certificate**, enter the keystore details in the relevant fields.

HP Enterprise Collaboration	on Deployment Manager 1.01		
Certificate Configuration HP Enterprise Collaboration Certificate Configuration Page			
Welcome Deployment Type Host Details Deployment Folder Network Configuration Certificate Configuration Application Network Database Configuration User Management Additional Configurations Summary Validation Deployment	Certificate Configuration Use temporary certificate Use custom certificate Keystore file path: Keystore type IKS Keystore Password Key alias Key Password	Iocalhost EC	
keystore file path can	1 keystore file path can not be empty Cancel		

Two types of keystores supported.- JKS and PKC.

The certificate is imported according to the Key alias entered.

Chapter 6

Set Up the Adapter

- 1. Download the adapter .war file from: www.hp.com/go/livenetwork
- 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

- 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 addAdapterUrI (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 sm here.
 - adapterUrl: For local deployment, the adapter URL should be {local}/adapter_name.

Name	Туре	Value	Description
adapterName	java.lang.String		adapter Name
dapterUrl	java.lang.String		adapter Url

- 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 the EC installation.

Chapter 7

Upgrade EC Configuration from 1.0 to 1.1

This section describes how to upgrade Enterprise Collaboration from version 1.0 to version 1.1.

If you have a previous version of Enterprise Collaboration installed and need to use the same data in the EC 1.1 installation, before upgrading, perform the following steps:

Note: EC 1.1 must be installed on the machine on which the previous EC version was installed.

- 1. Backup the external-ldap.properties and ldap certificate file (if they exist) from the previous installation to a temporary directory.
- 2. Backup all existing adapters from C:\HP\EC\servers\server-0\webapps to temp directory.
- 3. Backup the database schema.
- 4. Uninstall EC (1.00 or 1.01), so the EC service and all shortcuts will be removed.

Next, install Enterprise Collaboration 1.1:

- 1. Install EC 1.1 as described in <u>Install Enterprise Collaboration</u> using the **Connect to Existing Schema** option (See "Configure the MSSQL Database Administrator:" (on page 20)).
- During installation, enter all the configuration details as in the previous installation (init-string, email, OCS).

Note: The temporary administrator that you add at this stage must be different from the previous temporary administrator and must not exist in the user repository.

- After the installation has completed successfully, copy the external-Idap.properties file from the C:\temp directory to C:\HP\EC\conf (overwriting the existing file).
- 4. Place the backup Idap certificate (if one exists) in diamond-deploy and then run:

set-ldap-certificate.bat certificate-file-name

5. Update bsf.properties to:

```
authentication.provider=EXTERNAL
```

```
personalization.provider=SHARED
```

users.provider=EXTERNAL

groups.provider=EXTERNAL

roles.provider=SHARED

roles.relations.provider=SHARED

- 6. Move the backup adapters from the temp directory into C:\HP\EC\servers\server-0\webapps
- 7. Start the EC server.

- 8. To allow all existing conversations to be reindexed for searches, reset the elastic search as follows:
 - a. Gotohttp://diamond_host:<http_port>/diamond/jmx-console.
 - b. Login with the administrator user (temporary administrator user created in the User Management Configuration page during the installation of version 1.1).
 - c. Select Diamond > Diamond search JMX service.
 - d. Invoke the resetExperienceLastIndexRunTime method.

Note: After completing the Upgrade procedure, there is *no need* to enter BSF user management as all the role definitions already exist in the database.

Chapter 8

Desktop Client Installation

The Desktop Client application is an additional tool for viewing notifications about changes made in EC conversations. It provides information about current conversations in Enterprise Collaboration in which you are a participant.

This task explains how to install the Desktop Client on your system and provides a detailed description of the Installation wizard steps.

To install the Enterprise Collaboration Desktop Client from within Enterprise Collaboration:

1. Click on the user name in the upper right corner of the EC window:



2. The User Profile window opens:

User Profile		×
First Name:	Leah	
Last Name:	Hakim	
Email:	leah.hakim@hp.com	
Job Title:		
Image:	Browse	
	Delete	
	Download Desktop Clien	nt
	Ok Cancel	
	Galicer	-

- 3. Click on the **Download Desktop Client** link at the bottom of the window.
- 4. If the Open File warning window opens, click **Run** in this window.
- 5. Select Save or Open to download and extract the Desktop Client zip file.

- 6. Then run hpec_dc.exe.
- 7. The HP EC Desktop Client Installation begins.



8. In the Introduction dialog box, click Next.

🐙 HP EC Desktop Client 1.5.2.0	
	Install Folder
 Introduction Install Folder Server Info When to Start Pre-Installation Summary Installing Install Complete 	Please choose a destination folder for this installation. Where Would You Like to Install: C:\Program Files (x86)\HP EC Desktop Client Restore Default Folder Choose
InstallAnywhere Cancel	Previous Next

9. In the **Choose Install Folder** dialog box, click **Choose** to browse to the installation folder and then click **Next**.

Chapter 8: Desktop Client Installation

🖫 HP EC Desktop Client 1.4.8	
	Choose server host and port
 Introduction Choose Install Folder Choose Shortcut Folder Choose server host and Automatic start Pre-Installation Summary Installing Start HP EC Desktop Client Install Complete 	Please enter server host name and port (you can always change it later in Settings) Server host name vmcncdev26 Server port number 8080
InstallAnywhere Cancel	Previous <u>N</u> ext

10. In the **Choose server host and port** dialog box, enter the EC Server host name and port number and click **Next**.

🖫 HP EC Desktop Client 1.5.2.0		
	When to S	Start
 Introduction Install Folder Server Info When to Start Pre-Installation Summary Installing Install Complete 	When would you like to start the application: Image: Start the application when you log on to Windows Image: Start the application after installation	
Cancel	Previous Next	

11. In the When to Start dialog box, select Start the application when you log on to Windows to automatically run the EC Desktop Client each time you log in to Windows. Select Start the

application after installation to run the EC Desktop Client immediately after the installation procedure.



12. A summary of the installation details is presented. Review the summary and then click Install.



13. Click Done. The HP EC Desktop Client Settings window opens.

Chapter 8: Desktop Client Installation

HP EC De	esktop Client 1.5.2	×
	HP EC host:	
6	hpechost1	
	HP EC port:	
	8080	
	User name:	
	bob.smith@hp.com	
	Password:	
	🔽 Enable logs	
	🔽 Run on startup	
	OK Cancel	

- 14. In the Password field, type in the user's password and then click OK.
- 15. The Desktop Client begins running and is shown minimized on the status bar.
- 16. If you did not select Start the application after installation in the When to Start dialog box you can run the Desktop Client at any time by selecting Start > All Programs
 > HP EC Desktop Client.

For details on using the EC Desktop Client, see the Enterprise Collaboration Concepts Guide.

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-Idap.properties File

Before making changes in the **external-Idap.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 instructions on how to login to LDAP using the Apache Directory Studio LDAP Browser, see "Logging into LDAP using the Apache Directory Studio LDAP Browser" (on page 73).

Basic LDAP Properties

Attribute	Description
IdapHost	LDAP host name
IdapPort	LDAP port number
enableSSL	True/False—use SSL connection to LDAP
useAdministrator	True/False—use this user to connect to LDAP
IdapAdministrator	LDAP user DN
	(defined if useAdministrator=True)
IdapAdministratorPassword	LDAP user password
	(defined if useAdministrator=True)
	Note: The password for the LDAP user is not encrypted in the external-ldap.properties file.

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

Configure the User Providers

Update the **external-Idap.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

Attribute	Description
	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-Idap.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.
usersSipAttribute	Users SIP 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-Idap.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

Appendix B: Updating the external-Idap.properties File

Attribute	Description
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-Idap.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.

Installation and Configuration Guide Appendix B: Updating the external-Idap.properties File

Attribute	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
IdapVersion	LDAP protocol version. Possible values are:
	• 3 (default)
	• 2 (for old versions of LDAP)
baseDistinguishNameDelimiter	Base DN delimiter. Symbol used in configuration when putting
Attribute	Description
--------------------------	---
	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

This section explains 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 (IdapHost) and Port number (IdapPort).
- 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).