



Enterprise Chat and Email Installation and Configuration Guide, Release 11.5(1)

For Packaged Contact Center Enterprise

First Published: August 2016
Last Modified: November 2018

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCBs public domain version of the UNIX operating system. All rights reserved. Copyright 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Enterprise Chat and Email Installation and Configuration Guide: For Packaged Contact Center Enterprise. November 1, 2018

Copyright © 2006–2017, Cisco Systems, Inc. All rights reserved.

Contents

- Preface7**
 - Audience 8
 - Obtaining Documentation and Submitting a Service Request 8
 - Documentation Feedback 8
 - Field Alerts and Field Notices 9
 - Document Conventions..... 9
 - Other Learning Resources..... 9
 - Online Help 9
 - Document Set 10

- Chapter 1: Pre-Installation Tasks.....11**
 - Deployment Model for ECE 12
 - Preparing Virtual Machine 12
 - Obtain Installation Media 12
 - Download OVA for ECE 12
 - Create Virtual Machines from the OVA 13
 - Install Microsoft Windows Server 13
 - Install VMware Tools 13
 - Install Microsoft SQL Server 13
 - Mounting and Unmounting ISO Files..... 13
 - Disabling Loopback Adapter Configuration..... 14
 - Verifying Network Configuration..... 14
 - Configuring Port Numbers Between Components 15
 - Setting Up User Accounts and Permissions 16
 - Setting Up Domain Account..... 16
 - Preparing ECE Server Machine 16
 - Verifying Microsoft SQL Server Features 16
 - Verifying Collation Settings 17
 - Choosing Authentication Method for Database Connectivity 17
 - Creating SQL User for Installing ECE Databases 17
 - Running SQL Server Services..... 17
 - Preparing Web Server Machine 19

Configuring Roles and Features	19
Installing IIS Rewrite Module on Web Servers	21
Configuring Permissions on IIS Config Folder.	21
Running the World Wide Web Publishing Service.	21
Configuring Virus Scanners	21
Configuring SMTP Port in Virus Scanners.	21
Configuring Virus Scanning Exclusions	22
Verifying Packaged CCE Configuration.	22
Chapter 2: Prepare Packaged CCE for the Integration	23
Relationship Between Objects in Packaged CCE and ECE	24
Adding MR PIM for ECE.	25
Adding ECE to Packaged CCE Inventory	26
Configuring Packaged CCE	26
Planning MRDs and Skill Groups.	28
Recommended Configuration	28
Enabling Sharing of Work Across MRDs.	29
Configuring Call Types.	30
Configuring Application Path	31
Configuring Agents	32
Configuring Skill Groups	34
Configuring Dialed Number	35
Creating Scripts	36
Configuring Precision Routing	41
Creating Attributes	41
Assigning Attributes to Agents	42
Creating Precision Queues	43
Adding Precision Queue Node to the Scripts	44
Configuring Finesse	44
Chapter 3: Installation Process	45
Installing ECE Server	46
Installing Web Server	49
Chapter 4: Post-Installation Tasks	51
Configuring Permissions on IIS Config Folder	52

Configuring SSL for Secure Connections.	52
Configuring SMTP Server Relay Address List.	52
Configuring Finesse	52
Copying Files from ECE Server	52
Configuring Finesse Files	53
Enabling 3rdpartygadget Account and Deploying the Gadget	53
Configuring Finesse Settings and Layout	53
Starting Finesse Services.	54
Configuring Active Directory Federation Services for Single Sign-On.	55
Starting ECE	55
Troubleshooting Application Start-Up Issues.	55
Stopping ECE	56
Signing in to ECE	56
Signing in to Agent Console	56
Signing in to All Other Consoles	56
Configuring Important Settings	57
Mandatory Settings	57
Optional Settings	57
Uninstalling ECE	58
Preparing to Uninstall	58
Stopping the Application.	58
Stopping IIS.	58
Uninstalling ECE.	58
Performing Post Uninstallation tasks	59
Starting IIS.	59

Chapter 5: Single Sign-On Configuration 60

Configuring Single AD FS Deployment.	61
Configuring Relying Party Trust for ECE.	61
Configuring Split AD FS Deployment	69
Adding Security Certificates for the AD FS Domains	69
Configuring Relying Party Trust for Shared AD FS in Customer AD FS	70
Configuring Claims Provider Trust for Customer AD FS in Shared AD FS	74
Configuring Relying Party Trust for ECE in Shared AD FS	78
Configuring Single Sign-On in ECE.	85

Chapter 6: SSL Configuration	86
Installing a Security Certificate.	87
Generating a Certificate Signing Request	87
Submitting the Certificate Request	89
Installing the Certificate on the Web Server	89
Binding the Certificate to the Application Website	91
Testing SSL Access	92
Configuring SSL or TLS for Retriever and Dispatcher Services	92
On the Services Server	93
Installing Certificates.	93
Deleting Certificates	94
In the Administration Console	94

Preface

- ▶ [Audience](#)
- ▶ [Obtaining Documentation and Submitting a Service Request](#)
- ▶ [Documentation Feedback](#)
- ▶ [Field Alerts and Field Notices](#)
- ▶ [Document Conventions](#)
- ▶ [Other Learning Resources](#)

Welcome to the Enterprise Chat and Email (ECE) feature, which provides multichannel interaction software used by businesses all over the world as a core component to the Unified Contact Center Enterprise product line. ECE offers a unified suite of the industry's best applications for chat and email interaction management to enable a blended agent for handling of web chat, email and voice interactions.

Audience

Enterprise Chat and Email Installation and Configuration Guide is intended for installation engineers, system administrators, database administrators, and others who are responsible for installing and maintaining Enterprise Chat and Email (ECE) installations that are integrated with Cisco Packaged Contact Center Enterprise (PCCE).

The best way to use the installation guide is to print it, read the entire guide, and then start at the beginning and complete each pre-installation, installation, and post-installation task, in sequence.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: <http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

Documentation Feedback

To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.

Field Alerts and Field Notices

Cisco products may be modified or key processes may be determined to be important. These are announced through use of the Cisco Field Alerts and Cisco Field Notices. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest.

Log into www.cisco.com and then access the tool at <http://www.cisco.com/cisco/support/notifications.html>

Document Conventions

This guide uses the following typographical conventions.

Convention	Indicates
<i>Italic</i>	Emphasis. Or the title of a published document.
Bold	Labels of items on the user interface, such as buttons, boxes, and lists. Or text that must be typed by the user.
Monospace	The name of a file or folder, a database table column or value, or a command.
<i>Variable</i>	User-specific text; varies from one user or installation to another.


Document conventions

Other Learning Resources

Various learning tools are available within the product, as well as on the product CD, and our web site. You can also request formal end-user or technical training.

Online Help

The product includes topic-based as well as context-sensitive help.

Use	To view
 Help button	Topics in <i>Enterprise Chat and Email Help</i> ; the Help button appears in the console toolbar on every screen.
F1 keypad button	Context-sensitive information about the item selected on the screen.

Online help options

Document Set

The latest versions of all Cisco documentation can be found online at <http://www.cisco.com>

- ▶ For general access to Cisco Voice and Unified Communications documentation, go to http://www.cisco.com/en/US/products/sw/voicesw/tsd_products_support_category_home.html

The ECE document set contains the following guides:

- ▶ *System Requirements for Enterprise Chat and Email*
- ▶ *Enterprise Chat and Email Installation Guide*
- ▶ *Enterprise Chat and Email Browser Settings Guide*

User guides for agents and supervisors

- ▶ *Enterprise Chat and Email Agent's Guide*
- ▶ *Enterprise Chat and Email Supervisor's Guide*

User guides for administrators

- ▶ *Enterprise Chat and Email Administrator's Guide to Administration Console*
- ▶ *Enterprise Chat and Email Administrator's Guide to Routing and Workflows*
- ▶ *Enterprise Chat and Email Administrator's Guide to Chat and Collaboration Resources*
- ▶ *Enterprise Chat and Email Administrator's Guide to Email Resources*
- ▶ *Enterprise Chat and Email Administrator's Guide to Reports Console*
- ▶ *Enterprise Chat and Email Administrator's Guide to System Console*
- ▶ *Enterprise Chat and Email Administrator's Guide to Tools Console*

1 Pre-Installation Tasks

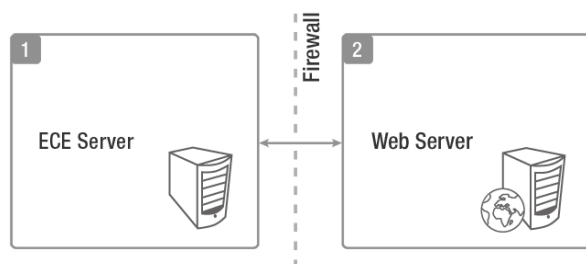
- ▶ [Deployment Model for ECE](#)
- ▶ [Preparing Virtual Machine](#)
- ▶ [Disabling Loopback Adapter Configuration](#)
- ▶ [Verifying Network Configuration](#)
- ▶ [Configuring Port Numbers Between Components](#)
- ▶ [Setting Up User Accounts and Permissions](#)
- ▶ [Preparing ECE Server Machine](#)
- ▶ [Preparing Web Server Machine](#)
- ▶ [Configuring Virus Scanners](#)
- ▶ [Verifying Packaged CCE Configuration](#)

This chapter describes pre-installation procedures that need to be completed before beginning the installation process. As you need to prepare the installation environment in advance, read this installation guide and the following documents before planning and implementing the installation:

- ▶ *System Requirements for Enterprise Chat and Email*
- ▶ *Enterprise Chat and Email Design Guide*

Deployment Model for ECE

The deployment has two servers - the ECE server (contains the file, database, application, services, and messaging server components) and the web server. The ECE server is installed on one machine and the web server is installed on a separate machine outside the firewall.



Deployment model for ECE

Preparing Virtual Machine

Obtain Installation Media

- ▶ Obtain the ECE installation media from a partner or by ordering from Cisco Systems, Inc.

Download OVA for ECE

1. Go to the Packaged Contact Center Enterprise Download Software page:
<https://software.cisco.com/download/type.html?mdfid=284360381&catid=null>
2. Click **Packaged Contact Center Enterprise Virtual Machine Templates**.
3. Download the Virtual Machine Templates zip file for the release.
4. Extract the file and save the OVAs to your local drive.

Create Virtual Machines from the OVA

- ▶ Follow the VMWare documentation to create virtual machines from the OVA. To determine the datastore on which to deploy the new virtual machine, see the *Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide*.

Install Microsoft Windows Server

- ▶ Follow the Microsoft documentation to install Microsoft Windows Server 2012 R2. While installing, make sure you select the **Custom: Install Windows only (advanced)** option, and select Drive 0 to install Microsoft Windows Server.

Install VMware Tools

- ▶ Follow the VMWare documentation to install the VMWare tools from the VMware vSphere Client. While installing, make sure you choose the Typical installation option.

Install Microsoft SQL Server

- ▶ Follow the Microsoft documentation to install Microsoft SQL Server 2014 Standard Edition. Make sure the required features for Microsoft SQL ([page 16](#)) are installed on the VM and the collation settings ([page 17](#)) are configured properly.

Mounting and Unmounting ISO Files

To upload ISO image to data store:

1. Select the host in the vSphere client and click **Configuration**. Then click **Storage** in the left panel.
2. Select the datastore that will hold the ISO file.
3. Click **Browse this datastore**.
4. Click the **Upload** icon and select **Upload file**.
5. Browse to the location on your local drive where you saved the ISO file, and upload the ISO to the datastore.

To mount the ISO image:

1. Right-click the VM in the vSphere client and select **Edit virtual machine settings**.
2. Click **Hardware** and select **CD|DVD Drive 1**.
3. Check **Connect at power on** (Device status panel upper right).
4. Click the **Datastore ISO File** radio button and then click **Browse**.
5. Navigate to the data store where you uploaded the file.
6. Select the ISO.

To unmount the ISO image:

1. Right-click the VM in the vSphere client and select **Edit virtual machine settings**.
2. Click **Hardware** and select **CD|DVD Drive 1**.
3. In the Device status panel, uncheck **Connect at power on**.

Disabling Loopback Adapter Configuration

ECE cannot be installed on machines where Microsoft Loopback Adapter is configured. Before you proceed with the installation, disable Loopback Adapter configuration on all machines in the deployment.

Skip this section if the machines in the configuration do not use the Loopback Adapter.

To disable Loopback Adapter:

1. Go to **Start > Control Panel**.
2. In the Control Panel window, click **Hardware**.
3. In the Devices and Printers section, click the **Device Manager** link.
4. In the Device Manager window, go to Network adapters and locate Microsoft Loopback Adapter.
5. Right-click Microsoft Loopback Adapter and select **Disable**.

Verifying Network Configuration

These tasks must be completed in all configurations in which components are installed on more than one physical machine.

To verify network configuration:

1. Ensure that both the machines are either assigned static IP addresses, or in cases where the IP address is assigned dynamically, are set to renew the same IP address upon lease expiration.
2. Ensure that all the required inbound and outbound ports that need to be opened for the flow of requests between the various components have been opened before you begin the installation. For details, see the [“Configuring Port Numbers Between Components”](#) on page 15.
3. For ECE server, the `nslookup` of the IP addresses should map to the fully qualified domain names of the servers. Similarly, the `nslookup` of the fully qualified domain names should map to the IP addresses of those servers.
4. Ensure that the system clocks of all the machines are synchronized.

Configuring Port Numbers Between Components

The following table lists the inbound and outbound ports that need to be opened for the flow of requests between the various components. The default port numbers are listed here. Ports that can be modified at the time of installation, or by editing property files are identified with an asterisk (*).

From Server	To Server	Default Destination Ports and Protocols
Agent Workstation	Web Server	<ul style="list-style-type: none"> ▶ 80 [Protocol: HTTP] ▶ 443 [Protocol: HTTPS]
Finesse Server	Web Server	<ul style="list-style-type: none"> ▶ 80 [Protocol: HTTP] ▶ 443 [Protocol: HTTPS]
ECE Server	SMTP Server	25 [Protocol: SMTP]
ECE Server	SMTP or ESMTP Server (with SSL enabled)	587 [Protocol: SMTP or ESMTP]
ECE Server	IMAP Server	143 [Protocol: IMAP]
ECE Server	IMAP Server (with SSL enabled)	993 [Protocol: IMAP]
Web Server	ECE Server	15006 [Protocol: TCP] *
ECE Server	SMTP or ESMTP Server	25 [Protocol: SMTP or ESMTP]
ECE Server	SMTP or ESMTP Server (with SSL enabled)	587 [Protocol: SMTP or ESMTP]
ECE Server	POP3 Server	110 [Protocol: POP3]
ECE Server	POP3 Server (with SSL enabled)	995 [Protocol: POP3]
ECE Server	IMAP Server	143 [Protocol: IMAP]
ECE Server	IMAP Server (with SSL enabled)	993 [Protocol: IMAP]
ECE Server	Primary CTI Server	42027*
ECE Server	Secondary CTI Server	42028*
ECE Server	Media Routing Peripheral Gateway	38002*
ECE Server	Primary Administration Workstation Database	1433 [Protocol: TCP]*
ECE Server	Primary Administration Workstation Database	1433 [Protocol: TCP]*

Setting Up User Accounts and Permissions

You will need administrator privileges on the local system to perform the installation and run the ECE services after installing the application. A *localUsername*, with administrator privileges, can be used or you can create a domain account to install the ECE server and the web server.



Important: You must use the same domain account to install the software environment and ECE. This account is also used to run the ECE services after installing the application ([page 55](#)).

Setting Up Domain Account

- ▶ Request your IT department to create a domain user account, for example, *InstallTeam* for exclusive use by ECE. The domain user account needs the **Log on as a Service** and **Local Administrator** privileges on each of the servers used in the deployment.

You will use this account to install and configure the software environment as well as ECE. This account is also used to run the ECE services after installing the application.



Caution: The recommendation is that you do not change the password of the domain account after the application is installed. If you must change it, make sure that you update the IIS directory security settings on web servers, and the login information for all Windows and MSSQL services that use that domain account.

Preparing ECE Server Machine

Verifying Microsoft SQL Server Features

- ▶ Ensure that the following Microsoft SQL Server features are installed.
 - Instance Feature:
 - Database Engine Services > Full Text and Semantic Extraction for Search
 - Shared Features
 - Client Tools Connectivity
 - Integration Services
 - Client Tools SDK
 - Management Tools - Basic > Management Tools - Advanced
 - SQL Client Connectivity SDK

Verifying Collation Settings

- ▶ Collation settings are typically chosen while installing SQL Server 2014. Since collations specify the rules for how strings of character data are sorted and compared, based on particular languages, a particular type of collation is required for the application to process and present information accurately.

On the Collation settings screen, choose SQL Collations and select the following option: **Dictionary order, case-insensitive, for use with 1252 Character Set**. For example, SQL_Latin1_General_CP1_CI_AS. Although this is the recommended collation, it is not mandatory. Any ASCII, case insensitive collation can be used. If you have already installed SQL Server 2014, consult your DBA and verify that the collation setting chosen is ASCII (case insensitive). The application databases will be installed using the collation that is configured for MSSQL Server.

Choosing Authentication Method for Database Connectivity

- ▶ The application supports two methods of authentication for connecting to the database.
 - SQL Server authentication
 - Windows authentication
- ▶ As part of the installation process, you will be asked to select the authentication method. Your selection will depend on the security policies of your organization, and should be consistent with the authentication method configured in SQL Server.

If you choose Windows authentication, certain additional steps must be completed before you begin installing the application. These steps are outlined in the [“Setting Up User Accounts and Permissions” on page 16](#). Also refer to [“Running SQL Server Services” on page 17](#).

Creating SQL User for Installing ECE Databases

Skip this section if you want to use the default SA user to install the ECE databases.

- ▶ Create a user for installing the ECE databases and make sure the following roles are assigned to the user:
`dbcreator, securityadmin, sysadmin`

Running SQL Server Services

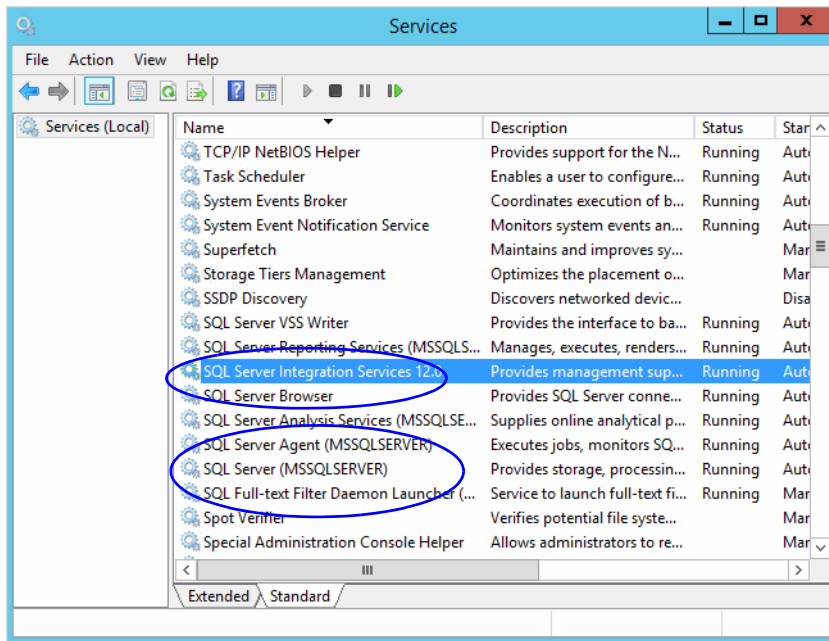
Make sure the following SQL services are running. These services should be started using the same domain account that you have created for installing the ECE application. You can also use a local account with administrative privileges.([page 16](#)).

- ▶ **SQL Server Service**
- ▶ **SQL Full-text Filter Daemon Launcher Service:** This service is required for text searches.
- ▶ **SQL Server Agent Service:** This service is used by the Reports module.
- ▶ **SQL Server Integration Service:** This service is used by the Reports module.

- ▶ **SQL Server Browser Service:** In configurations where database servers are configured to run on named instances, and no listener port is configured, the SQL Server Browser service needs to be running when you run the installer. This service does not have to be running if the database servers are configured to run on the default instance. It is also not required if the database servers are configured to run on named instances, and specific, static listener ports are configured for the named instances.

To start the services:

1. Go to **Start > Programs > Administrative Tools > Services**.
2. For the SQL Full-text Filter Daemon Launcher, SQL Server Agent, SQL Server, and SQL Server Browser services check if the right domain account is used for starting the services.
 - a. Select a service and right-click to open the menu.
 - b. From the menu select **Properties**.
 - c. In the Properties window, go to Log On tab and ensure the service is started using the same domain account that you have created for installing the ECE application (page 16).
3. Ensure that the SQL Full-text Filter Daemon Launcher, SQL Server Agent, SQL Server, SQL Server Integration Service, and SQL Server Browser services are running.
4. If they are not running, select the services one by one, and click **Start** to start the service.



Start the SQL services

Preparing Web Server Machine

Configuring Roles and Features

This task is performed automatically by the installation program. You can choose to do it manually before running the installation program.

Ensure that the following Roles and Features are installed for IIS.

- ▶ NET Extensibility 4.5
- ▶ ASP
- ▶ CGI
- ▶ ISAPI Extensions
- ▶ ISAPI Filters
- ▶ Server Side Includes
- ▶ Static Content
- ▶ Static Content Compression
- ▶ Dynamic Content Compression
- ▶ Directory Browsing
- ▶ Default Document

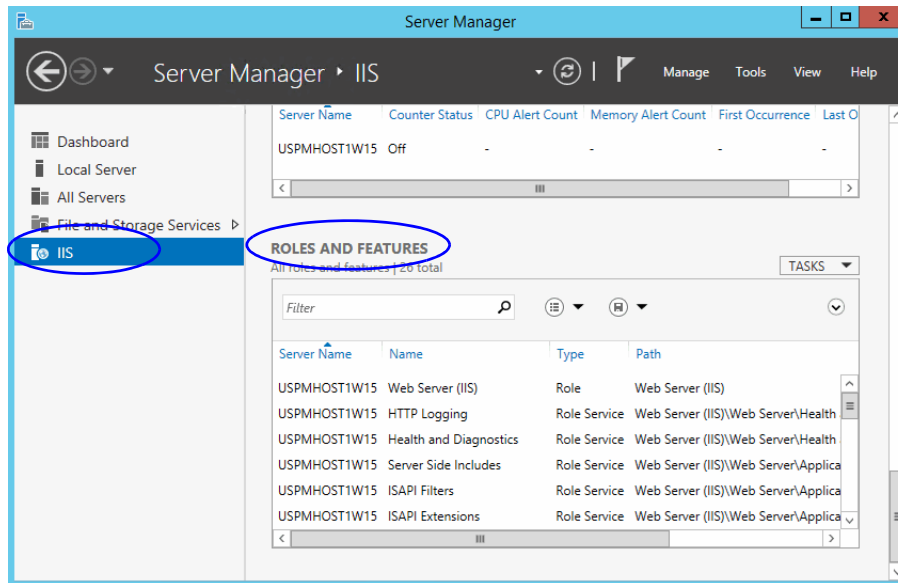
Ensure that the following feature is *not* installed for IIS.

- ▶ WebDAV Publishing

To install the roles and features:

1. Go to **Start > Control Panel > Administrative Tools > Server Manager**.

2. In the Server Manager window, Go to IIS section. In the IIS section, locate the Roles and Features section.



Go to Roles and Features section

3. In the Role and Features section, check if the required role services are installed.
4. If any of the roles and features are not installed, from the Tasks menu, click the **Add Roles and Features** button and run through the wizard to install the missing services. In the Server Roles section, expand the **Web Server (IIS)** list, and select the following:
 - In the Common HTTP Features list, select:
 - Default Document
 - Directory Browsing
 - Static Content
 - In the Performance list, select:
 - Static Content Compression
 - Dynamic Content Compression
 - In the Application Development list, select:
 - NET Extensibility 4.5
 - ASP
 - CGI
 - ISAPI Extensions
 - ISAPI Filters
 - Server Side Includes
5. In the Role and Features section, check if the **WebDAV Publishing** feature is installed. If the feature is installed, you need to uninstall it. From the Tasks menu, click the **Remove Roles and Features** button and run through the wizard to uninstall the feature.

Installing IIS Rewrite Module on Web Servers

This task is performed automatically by the installation program. You can choose to do it manually before running the installation program.

- ▶ The IIS rewrite module is required to be installed on the web server. Install the module using the installation program available in the `Environment\Web Server\URL Rewrite` folder of the installation package.

Configuring Permissions on IIS Config Folder

- ▶ Ensure that the user account you are going to use for installing the application ([page 16](#)) has read permissions on the following folder: `%systemroot%\system32\inet_srv\config`

Running the World Wide Web Publishing Service

- ▶ On the machine where the web server is to be installed, ensure that the World Wide Web Publishing Service is running.

Configuring Virus Scanners

Configuring SMTP Port in Virus Scanners

- ▶ Ensure that the virus scanner is configured to allow emails to be sent through the SMTP port (Port 25). In a distributed installation, configure this setting on the services server and all application servers.

Configuring Virus Scanning Exclusions

To ensure that virus and malware scanning software on the servers do not interfere with the performance of the application, certain folders and files must be excluded from continuous virus scanning. Since no files are downloaded to these locations from the internet, it is safe to exclude these directories from virus scanning.

Item	Exclude Subfolders?	Permissions
Windows File Protection	--	Read, Write
All files of type LOG	--	Read, Write
Pagefile.sys	No	Read, Write
<i>Drive\ECE_Home\</i>	Yes [other than Storage]	Read, Write
*.mdf	No	Read, Write
*.ldf	No	Read, Write
*.ndf	No	Read, Write
*.dat	No	Read, Write
*.rll	No	Read, Write

Verifying Packaged CCE Configuration

- ▶ Verify that Packaged CCE and Microsoft Active Directory (AD) have been installed on separate servers. Refer to Unified CCE documentation for more details.
- ▶ Verify that the Packaged CCE and AD servers are in the same network as the ECE servers and are accessible from the ECE servers.
- ▶ ECE uses the application instance, Multichannel, and the CUCM type of Agent PG. MRDs that are Application Path members on the Multichannel application instance are automatically imported during installation. Agents and skill groups, which belong to the CUCM type of Agent PG are imported during installation.
- ▶ In Packaged CCE, configure the items to be used in ECE. These include:
 - Peripherals
 - Network Voice Response Units (Network VRUs)
 - Call Type
 - Script Selector
 - Application Paths and Path Members
 - Agents
 - Skill Groups
 - ICM Scripts

For details, see [“Prepare Packaged CCE for the Integration”](#) on page 23.



Prepare Packaged CCE for the Integration

- ▶ [Relationship Between Objects in Packaged CCE and ECE](#)
- ▶ [Adding MR PIM for ECE](#)
- ▶ [Adding ECE to Packaged CCE Inventory](#)
- ▶ [Configuring Packaged CCE](#)
- ▶ [Configuring Finesse](#)

This chapter provides an overview of the process of setting up Packaged CCE for integration with ECE. It includes a note about the relationship between objects in the two systems.

Relationship Between Objects in Packaged CCE and ECE

This section provides a brief introduction to the relationship or “mapping” between objects that are used in both Packaged CCE and ECE.

The following table provides a high-level view of the relationship between various objects.

Packaged CCE object	Mapped in ECE to	Notes
Agent Supervisor Administrator	User	<ul style="list-style-type: none">▶ An agent belongs to a peripheral.▶ A peripheral belongs to an agent peripheral gateway (PG).
Skill group	User group	<ul style="list-style-type: none">▶ A skill group belongs to a peripheral.▶ A peripheral belongs to an agent PG.
Media routing domain (MRD)	Queue	<ul style="list-style-type: none">▶ Multiple queues can belong to a single MRD.
Script selector	Queue	<ul style="list-style-type: none">▶ A script selector can belong to only one queue.

Typically, the mapping between these objects is set up by using the import feature available in the ECE Administration Console. Once imported, these objects can be viewed from the department level nodes for these objects (Queues, Users, and User Groups) in the Administration Console in ECE.



Important: If you are planning to have multiple departments in ECE, then ensure that you create department specific MRDs, skill groups, and script selectors.

Adding MR PIM for ECE

To add MR PIM:

1. Sign into Unified CCE Administration and navigate to **System > General > Peripheral Gateways**. Open the Peripheral Gateways tab to determine the Peripheral ID for a Multichannel peripheral that is not in use. The **Routing Type** field should have the value **Unused Multichannel**.

Name	MR_PG				
Logical Controller ID	5001				
Peripherals	Name	Peripheral ID	Routing Client ID	Client Type	Routing Type
	Multichannel	5004	5004	MediaRouting	Unused Multichannel
	Multichannel2	5005	5005	MediaRouting	Unused Multichannel
	Multichannel3	5006	5006	MediaRouting	Unused Multichannel
	Outbound	5003	5003	MediaRouting	Outbound Voice

Identify an unused multichannel peripheral

2. Access the CCE PG on Side A.
3. From Cisco Unified CCE Tools, select **Peripheral Gateway Setup**.
4. On the Components Setup screen, in the Instance Components panel, select the PG2A Instance component for Side A. (Select PG2B for Side B.) Then click **Edit**.
5. In the Peripheral Gateways Properties screen, click **Media Routing**. Then click **Next**.
6. Click **Yes** at the prompt to stop the service.
7. In the Peripheral Interface Manager pane of the Peripheral Gateway Component Properties dialog box, click **Add**, select the next available PIM number, and configure with the Client Type of Media Routing as follows:
 - a. Check **Enabled**.
 - b. In the Peripheral name field, enter **MR**.
 - c. In the Peripheral ID field, enter the Peripheral ID for the unused Multichannel peripheral that you identified in Step 1.
 - d. In the Application Hostname (1), field, enter the hostname or the IP address of the ECE services server machine.
 - e. In the Application Connection Port (1), field, enter the port number on the ECE services server machine that the PIM will use to communicate with the application. The default port is 38001.
 - f. In the Application Hostname (2), field, leave the field blank.
 - g. In the Application connection port (2), field, leave the field blank.
 - h. In the Heartbeat interval (sec) field, enter **5**.
 - i. In the Reconnect interval (sec) field, enter **10**.
 - j. Click **OK**.
8. Accept defaults and click **Next** until the Setup Complete screen opens.
9. At the Setup Complete screen, check **Yes** to start the service. Then click **Finish**.
10. Click **Exit Setup**.
11. Repeat from Step 1 for the CCE PG on Side B.

Adding ECE to Packaged CCE Inventory

Deployments using ECE with Packaged CCE must add ECE to the system inventory as an external machine.

To add ECE to Packaged CCE inventory:

1. Sign in to Unified CCE Administration and navigate to **Web Administration > System > General > Deployment**.
2. Click **Add Machine**.
3. Select **Enterprise Chat and Email** from the drop-down list.
4. Add the hostname or IP address of the ECE Server.
5. Click **Save**.

Configuring Packaged CCE

This section describes the process of configuring Packaged CCE objects that are required for the integration with ECE. These objects must be configured in the order in which they are presented here. For details of these objects refer to the Online Help and printed documentation for Unified CCE. The specific objects that have to be configured will depend on the activities (email, chat etc.) supported by the integrated installation. This section describes the objects required for each activity type—inbound email, outbound email, chat, callback, and delayed callback.

For Packaged CCE, ECE uses the application instance, **Multichannel**, and the **CUCM** type of Agent PG. MRDs that are Application Path members on the **Multichannel** application instance are automatically imported during installation. Agents and skill groups, which belong to the **CUCM** type of Agent PG are imported during installation. In addition to this, objects listed in this section should be configured in Packaged CCE.

Packaged CCE customers who intend to use ECE must access Peripheral Gateway Setup on both CCE PGs to set up a Multichannel PIM that associates ECE with the MR PG (PG2). See [“Adding MR PIM for ECE” on page 25](#).

The following objects are part of the Packaged CCE base configuration and are automatically configured by the Packaged CCE installation.

▶ **Application Instance**

- ▶ **Media Classes:** A media class defines the type of requests you want to set up for routing on Unified CCE. A media class is created for each media supported by the ECE deployment. Media classes are required for creating MRDs and categorize the MRDs based on media type (email, for example).

The following media classes are created automatically. No action is required from you.

- ECE_Email (for inbound email)
- ECE_Outbound (for outbound email)
- ECE_Chat (for chat)
- Callback and Delayed callback use the existing `Cisco_Voice` media class, which is already created by the system.

- ▶ **Media routing domain:** An MRD is a collection of skill groups and services that are associated with a common communication medium. Packaged CCE uses an MRD to route tasks to agents who are associated with a skill group and a particular medium. A media routing domain is created in Packaged CCE for mapping to queues in ECE.

The following media routing domains are created automatically. No action is required from you:

- ECE_Email
- ECE_Outbound
- ECE_Chat
- For callback and delayed callback, use the existing voice media routing domain (`Cisco_Voice`) created by the system.

- ▶ **Network VRU:** Network VRU scripts are used to display dynamic content to chat customers (for example, wait time, activity ID, etc) while chat requests are being processed by the system. This is an optional feature. The dynamic messages are configured in ECE. For details, see *Enterprise Chat and Email Administrator's Guide to Chat and Collaboration Resources*.

- ▶ **Media Routing Peripheral Gateways (MR PGs)**

- ▶ **Agent Desk Settings**

- ▶ **Agent Peripheral Gateway (Agent PG)**

- ▶ **Agent Targeting Rule**

- ▶ **Expanded Call Context (ECC) variables:** ECC variables are used in Unified CCE scripts to facilitate and influence routing. ECC variables have a maximum length of 256 characters. Both Scalar and Array ECC variables are supported.

ECC variables are required for inbound email, outbound email, chat, callback, and delayed callback activities. The following ECC variables are created automatically:

- For chat, inbound and outbound email activities: `user.ece.activity.id`
- For callback and delayed callback activities: `user.ece.activity.id`, `user.ece.customer.name`

The following table indicates the necessary objects that need to be configured by the user. These objects must be configured in the order in which they are presented here.

Object	Details
Call type	Configured using the Unified CCE Administration page. (page 30)
Application path	Configured using the Configuration Manager tool. (page 31)
Agents	Configured using the Unified CCE Administration page. (page 32)
Skill groups	Configured using the Unified CCE Administration page. (page 34)
Dialed Number/Script Selectors	Configured using the Unified CCE Administration page. (page 35)
Scripts	Configured using the Script Editor. (page 36)
Precision Routing	Configured using the Unified CCE Administration page. (page 41)

Planning MRDs and Skill Groups

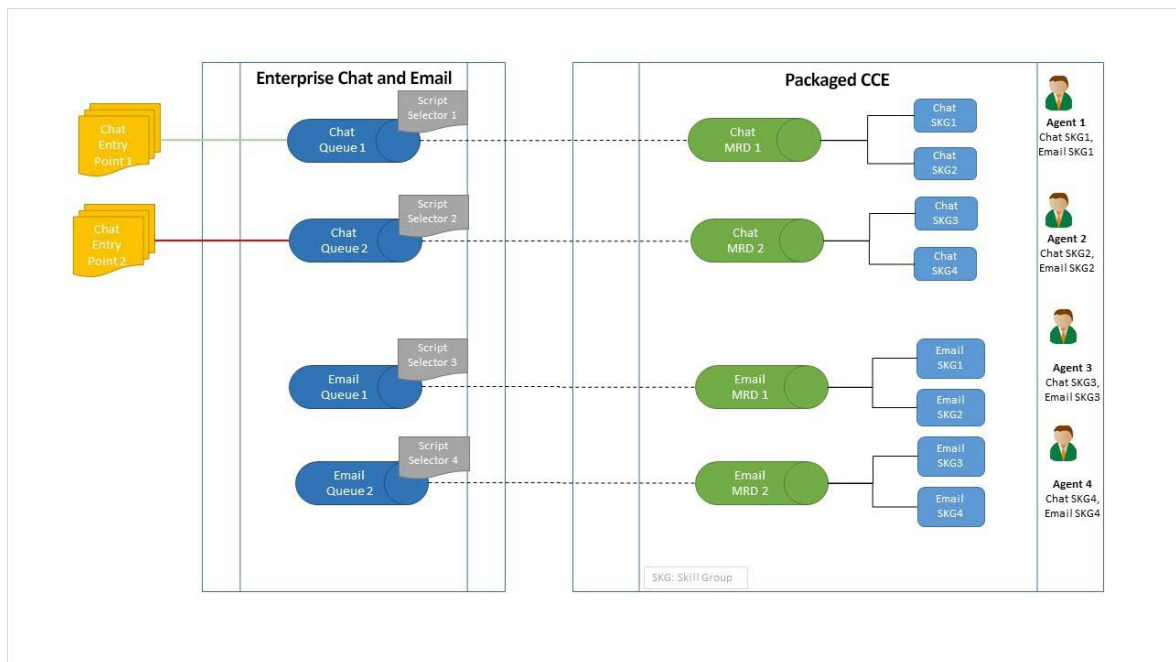
While deciding the MRDs and skill groups required in the system, it is important to understand a few things about how availability of agents is checked for chat interactions and how work is shared across MRDs and skill groups.

- ▶ If any agent belonging to an MRD is available, Agent Availability returns true and hence the chat entry point mapped to that queue (and hence MRD) gets enabled and allows customer to enter details to engage with an agent. However, the routing may not succeed if the agent with the right skill is not actually available.
- ▶ Work is shared by all agents who belong to the same MRD, i.e. you can transfer and pull work from queues and agents that belong to the same MRD.

Recommended Configuration

It is recommended to create separate MRDs and map homogeneous skill groups to each MRD, on which agents can perform tasks. It provides following benefits:

- ▶ **Right Task to Right Agent:** Only suitable agents can work on specific tasks
- ▶ **Encapsulation:** Agents with skill groups of one MRD cannot see the tasks of agents belonging to skill groups of other MRDs
- ▶ **Right Agent Availability:** Assures that a suitably skilled agent is available to pick and respond to an activity.

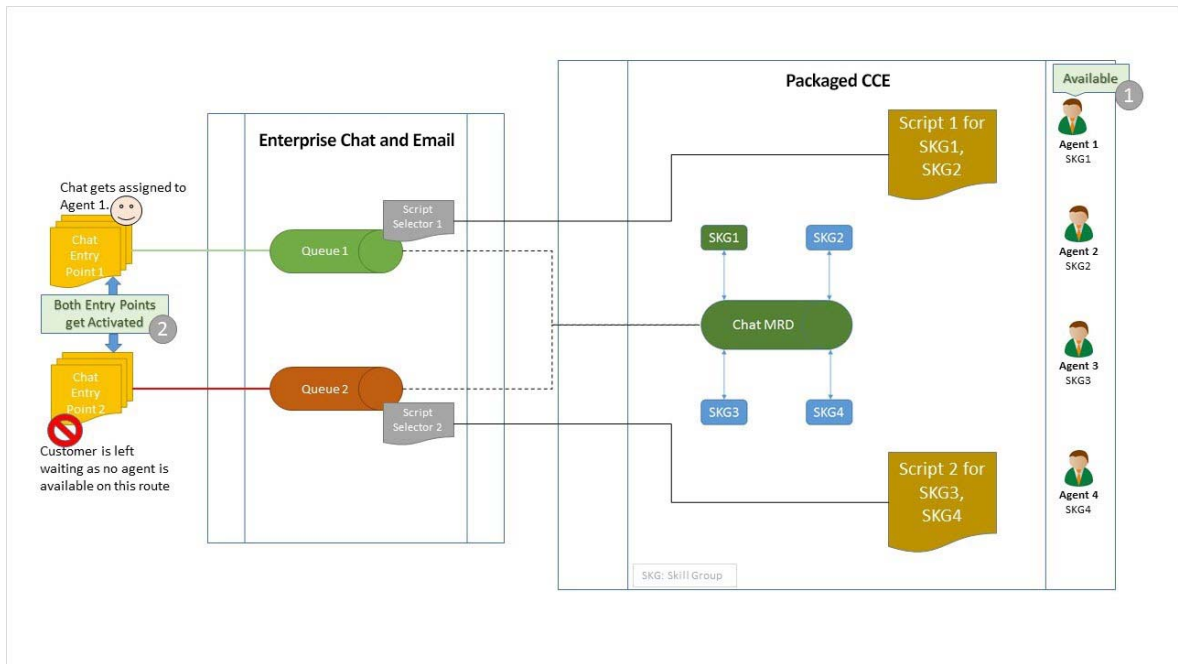


Recommended configuration

It is not recommended to have a single MRD and have all objects mapped to the same MRD. Reasons are:

- ▶ **No permission control:** All agents can share work with each other and they have visibility to all activities

- ▶ **Agent availability issues:** Availability of any agent enables the customer to access entry point and engage in chat, however, the routing may not succeed if the agent with the right skill is not actually available, as depicted in the following figure.

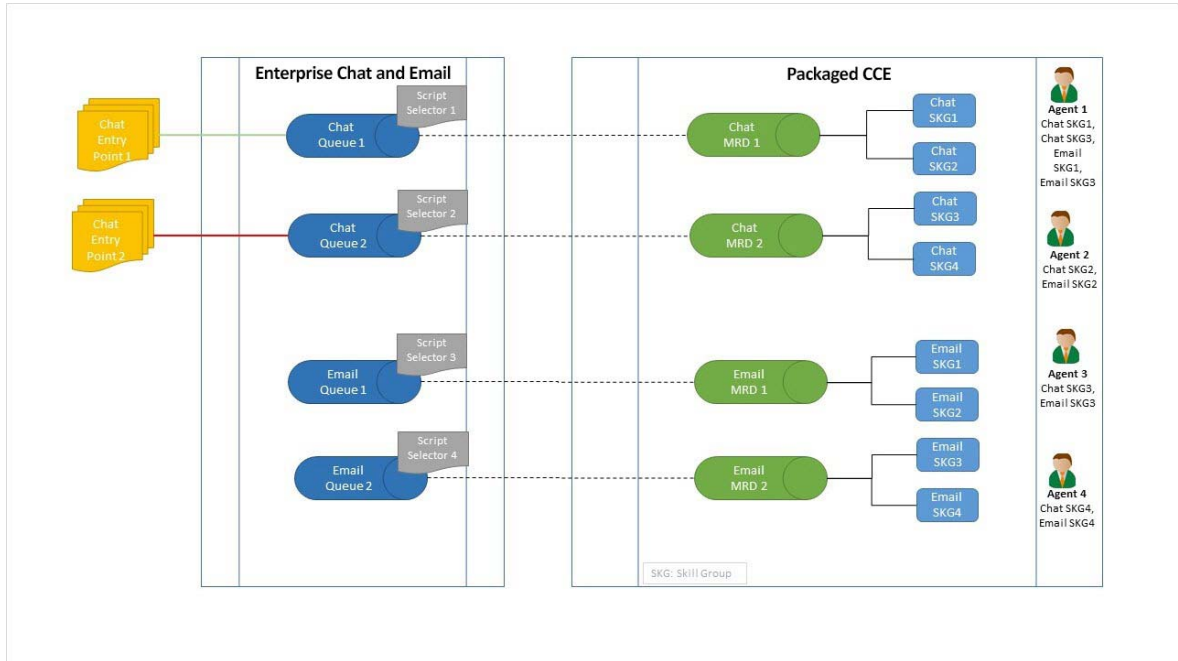


Not recommended configuration

For the same reasons, when you plan to have multiple departments in ECE, you must ensure that you create department specific MRDs and skill groups and not share them across departments.

Enabling Sharing of Work Across MRDs

- ▶ When there is a need to share work (pick, pull, and transfer capability) across MRDs, it is recommended to have a limited number of ‘Expert’ Agents, who have skill groups panning across MRDs where the transfers are intended. Such ‘Expert’ Agents can then communicate across MRDs. In the following figure, Agent 1 is the ‘Expert’ agent, who belongs to Skill Groups Chat SKG1, Chat SKG-3, Email SKG1 and Email SKG3, which allows him to transfer chats across Chat MRD1 and Chat MRD2 and transfer, pick, pull emails across Email MRD 1 and Email MRD 2.



Share work across MRDs with expert agents

Configuring Call Types

A call type is required to categorize a dialed number (for voice) or a script selector (for email). Call types are used in configuring routing scripts.

Individual call types are required for the following activities: inbound email, outbound email, chat, callback, and delayed callback activities. Make sure you complete these steps for each type of activity.

To configure a call type:

1. Launch the CCE Web Administration page, using the URL: https://Server_Name/cceadmin/
2. Login using the administrator credentials.
3. Go to **Manage > Call Types**.
4. On the List of Call Types page, Click **New**.
5. In the **Name** field, provide a name for the call type.
6. Click **Save**.

The screenshot shows the 'Unified CCE Administration' web interface. At the top, there are navigation tabs for 'Home', 'Manage', and 'System'. Below this is a sub-header 'Manage Call Types'. The main content area is titled 'New Call Type' and contains several form fields:

- Department:** A dropdown menu with 'Global' selected.
- Name:** A text input field containing 'Call Type Name'.
- Description:** An empty text area.
- Service Level Threshold:** A dropdown menu with 'System Default (20)' selected, followed by the unit 'seconds'.
- Service Level Type:** A dropdown menu with 'System Default (Ignore Abandoned Calls)' selected.
- Bucket Interval:** A dropdown menu with 'System Default (BuiltIn)' selected.

 At the bottom of the form are two buttons: 'Save' and 'Cancel'.

Provide the name of the call type

Configuring Application Path

An application path is required to open a communication channel with a CTI server associated with an Agent PG. It is used for agent and task status reporting. For each Agent PG, create an application path that ECE will use to connect to the Agent PG.

Create a single application path and add all the MRD-peripheral combinations for the Agent PG to the application path member list. The application path is used for inbound email, outbound email, chat, callback, and delayed callback activities.

Access to the application object filter is restricted. Log in as a super user to enable or disable the application object filter. For details about the super user password, see the *Configuration Guide* for Cisco Unified ICM/Contact Center Enterprise and Hosted available at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_installation_and_configuration_guides_list.html

Create a single application path and add all the peripheral-MRD combinations for the Agent PG (CUCM_PG) to the application path member list. You do not need to add the voice MRD (Cisco_Voice) to this list.

To configure an application path:

1. Access CCE AW in Side A or B and run Configuration Manager from the desktop shortcut **Unified CCE Administration Tools**.
2. In the Configuration Manager window, browse to **Tools > List Tools > Application Path List**.
3. Double-click Application Path List.
4. In the Name field, click **Retrieve**. Then click **Add** to display the Attributes panel.
5. In the Application Instance field, select **MultiChannel**.

- In the Peripheral Gateway field, select **CUCM_PG**. The Name field will auto-populate as **Generic_PG_MultiChannel**.

Attributes

Application instance * MultiChannel

Peripheral gateway * CUCM_PG

Name * CUCM_PG.MultiChannel

Description

Application Path Members

	Peripheral	Media routing domain
1	CUCM_PG_1	ECE_Email
2	CUCM_PG_1	ECE_Outbound
3	CUCM_PG_1	ECE_Chat

Add Remove

Select the Peripheral Gateway

- In the Application Path Members section, click Add and set the following:
 - From the Peripheral drop-down list, select CUCM_PG1. In the Media Routing Domain field, enter ECE_Email.
 - From the Peripheral drop-down list, select CUCM_PG1. In the Media Routing Domain field, enter ECE_Outbound.
 - From the Peripheral drop-down list, select CUCM_PG1. In the Media Routing Domain field, enter ECE_Chat.
- Click **Save**.

Configuring Agents

An agent is created in Unified CCE for mapping to users in ECE. Create all agents for whom routing or reporting is done in Unified CCE. If you plan to use Precision Routing, you need to assign attributes to agents. For details, see [“Assigning Attributes to Agents” on page 42](#).

Create agents for handling inbound email, outbound email, chat, callback, and delayed callback activities.

To configure an agent:

- Launch the CCE Web Administration page, using the URL: `https://Server_Name/cceadmin/`
- Login using the administrator credentials.
- Go to **Manage > Agents**.
- On the List of Agents page, Click **New**.

The New Agent window opens. This window has four tabs: General, Attributes, Skill Groups, and Supervisor. You cannot save the agent until you have entered all required fields on the General tab. You can complete other tabs as needed and in any order.

5. On the General tab, set the following details:
 - **Login Enabled:** Select the option.
 - **Single Sign-on (SSO):** Select this option if you want to use single sign-on for the agent. Password fields are disabled if you select this option.
 - **Username:** Provide the login name for the agent. For callback and delayed callback agents, the login name should match the User ID provided while configuring End users from the Cisco Unified Communication Manager Administration user interface.
 - **First name:** Provide the first name.
 - **Last name:** Provide the last name.
 - **Password:** Provide the password for the agent. Make sure the password does not contain the following characters: = (equal to) and ; (semicolon) as ECE does not allow the users to login if these characters are present in the passwords. Password fields are disabled if single sign-on option is selected for the agent.
6. Click **Save**.

The screenshot shows the 'Unified CCE Administration' interface. The 'Manage Agents' section is active, and the 'New Agent' form is displayed. The 'General' tab is selected, showing various configuration options. The 'Login Enabled' checkbox is checked, and the 'Single Sign-on (SSO)' checkbox is unchecked. The 'Is Supervisor' checkbox is also unchecked. The 'Department' dropdown is set to 'Global'. The 'Username' field contains 'Jane_Doe', 'First Name' contains 'Jane', and 'Last Name' contains 'Doe'. The 'Agent ID' field is empty, with a note 'Value will be created if left blank'. The 'Description' field is empty. The 'Desk Settings' dropdown is set to 'System Default (Default_Agent_Desk_Settings)'. The 'Team' dropdown is set to 'None'. The 'Set Password' checkbox is checked, and the 'Enter Password' and 'Re-enter Password' fields are masked with dots. The 'Save' and 'Cancel' buttons are visible at the bottom of the form.

Configure an agent

Configuring Skill Groups



Important: If you are planning to have multiple departments in ECE, then ensure that you create department specific skill groups.

A skill group is created in Unified CCE for mapping to user groups in ECE. The skill group members (agents) are administered and managed in Unified CCE. A skill group (with associated skill group members) is used in scripts to facilitate routing through Unified CCE to the skill group. This is used for inbound email, outbound email, chat, callback, and delayed callback activities.

To configure a skill group:

1. Launch the CCE Web Administration page, using the URL: `https://Server_Name/cceadmin/`
2. Login using the administrator credentials.
3. Go to **Manage > Skill Groups**.
4. On the List of Skill Groups page, Click **New**.

The New Skill Group window opens and has two tabs: General and Members. You can complete the tabs in any order, but you cannot save the skill group until you have entered all required fields on the General tab.

5. On the General tab, provide the following details:
 - **Name:** Provide a name for the skill group.
 - **Media routing domain:** From the dropdown list, select an MRD configured for ECE.

The screenshot shows the 'Unified CCE Administration' web interface. The top navigation bar includes 'Home', 'Manage' (highlighted), and 'System'. Below the navigation bar, the page title is 'Manage Skill Groups' and the current page is 'Edit Email_skill_group'. The 'General' tab is active, and the 'Members' tab is also visible. The form contains the following fields:

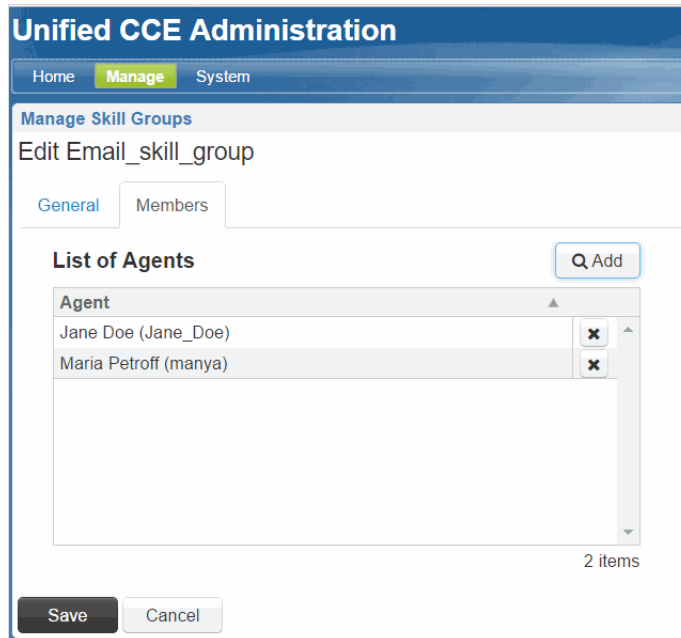
- Department: Global
- Name: Email_skill_group
- Description: (empty text area)
- Media Routing Domain: ECE_EMail
- Bucket Interval: System Default (BuiltIn)
- Service Level Threshold: System Default (30) seconds
- Service Level Type: Ignore Abandoned Calls
- Peripheral Number: 14270886

At the bottom of the form, there are 'Save' and 'Cancel' buttons.

Configure the properties of a skill group

6. On the Members tab, do the following:
 - a. Click the **Add** button.

- b. From the Add Agents pop-up window, select the agents to be added in the skill group.



Add agents to the skill group

Configuring Dialed Number

A script selector is a keyword that identifies the routing script for an activity request from ECE to Unified CCE. Script selectors are used in routing scripts as part of the **Dialed Number** node.

Individual script selectors are required for the following activities: inbound email, outbound email, chat, callback, and delayed callback activities. Make sure to complete these steps for each type of activity.



Important: If you are planning to have multiple departments in ECE, then ensure that you create department specific dialed numbers.

Before you begin:

- ▶ Configure the MR PIM for ECE ([page 25](#)) and add ECE as an External Machine in the System Inventory ([page 26](#)). The configuration must pass validation.

To configure a dialed number:

1. Launch the CCE Web Administration page, using the URL: `https://Server_Name/cceadmin/`
2. Login using the administrator credentials.
3. Go to **Manage > Dialed Number**.
4. Click the **New** button.
5. On the New Dialed Number page, provide the following details:
 - **Dialed Number String:** Provide a name for the dialer number.
 - **Routing Type:** Select the routing type and **Enterprise Chat and Email**.

- **Media routing domain:** From the dropdown list, select the MRD configured for ECE.
- **Call Type:** Select the Call Type created for ECE.

The screenshot shows the 'Unified CCE Administration' interface. The top navigation bar includes 'Home', 'Manage', and 'System'. The main content area is titled 'Manage Dialed Numbers' and contains a 'New Dialed Number' form. The form fields are:

- Department: Global
- * Dialed Number String: ECE_Chat_SS
- Description: (empty text area)
- * Routing Type: Email and Web Manager
- Media Routing Domain: ECE_Chat
- Call Type: ECE_Chat_CT

 At the bottom of the form are 'Save' and 'Cancel' buttons.

Configure Dialed Number

6. Click **Save**.

Creating Scripts

A routing script determines the path and target object for an activity routed from ECE to Packaged CCE. Individual routing scripts are required for the following activities: inbound email, chat, callback, and delayed callback activities. Make sure to complete these steps for all these activities. You do not need routing scripts for outbound email activities.

Universal queues and Precision queues can be used in the scripts configured for ECE.

For details about creating universal queues, see the *Scripting and Media Routing Guide* for Unified CCE available at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_user_guide_list.html. Make sure to use the guide that matches the version of the product that you are using. To find the right version, refer to the *Cisco Unified Contact Center Enterprise (Unified CCE) Software Compatibility Guide* available at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_device_support_tables_list.html.

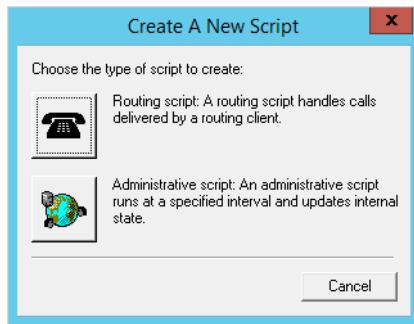
For details about configuring Precision Routing, see “[Configuring Precision Routing](#)” on page 41.

The following procedure shows how to set up a particular script. To find out more about setting up different types of scripts to meet your routing requirements, see the *Scripting and Media Routing Guide* for Unified CCE.

To create a script:

1. Go to **Start > All Programs > Cisco Unified CCE Tools > Administration Tools > Script Editor**.
2. In the Script Editor window, click the **New** button.

- In the Create A New Script window, select the **Routing script** option.



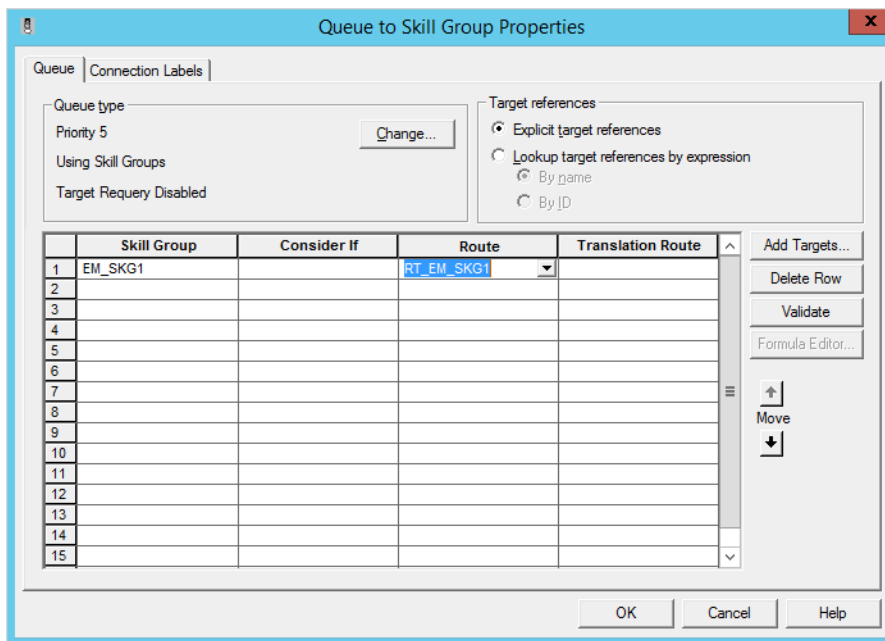
Select the **Routing Script** option

A new script editor opens. The Start node is added by default to the script editor.

- In the Script Editor window, go to **View > Palette**.

The Palette window opens.

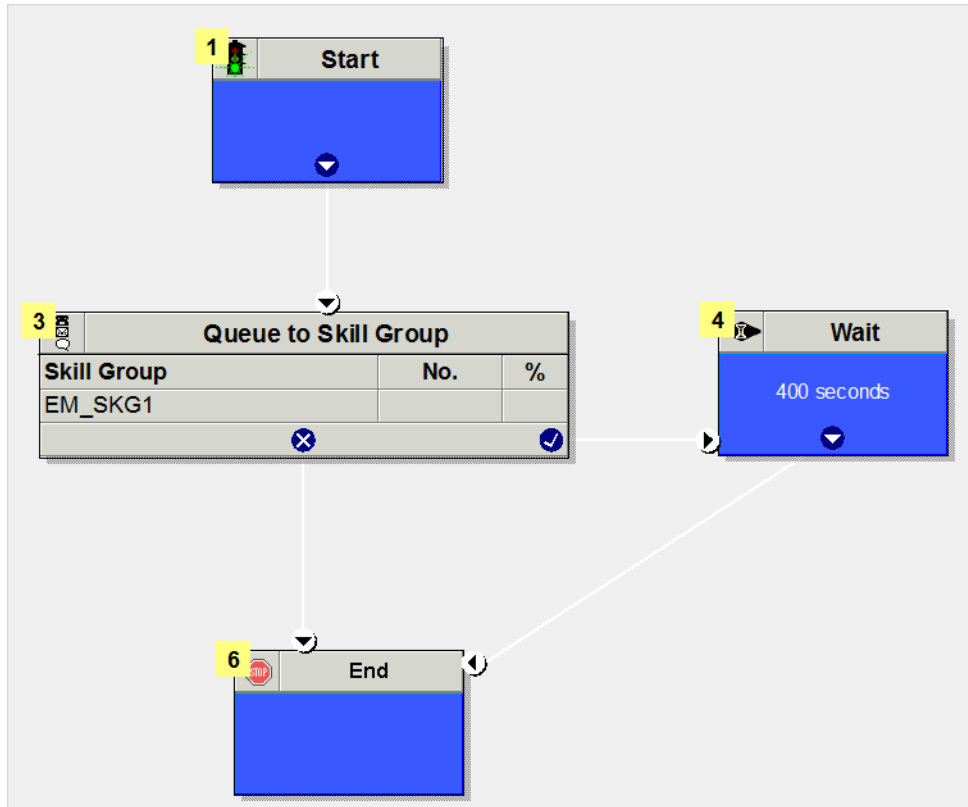
- In the Palette window, on the Queue tab, click the **Queue** button, and click in the script editor. The Queue to Skill Group node is added to the script editor.
- Double-click the Queue to Skill Group node to open the Queue to Skill Group Properties window.
- In the Queue to Skill Group Properties window, on the Queue tab, in the Skill Group column, select a skill group.



Select a skill group

- Next, in the Palette window, on the General tab, click the **Line Connector** button and configure the success and error paths for each node. This creates the routing path of the script.
- Click the **Validate Script** button to check if the script is created properly. If there are any errors, fix them.

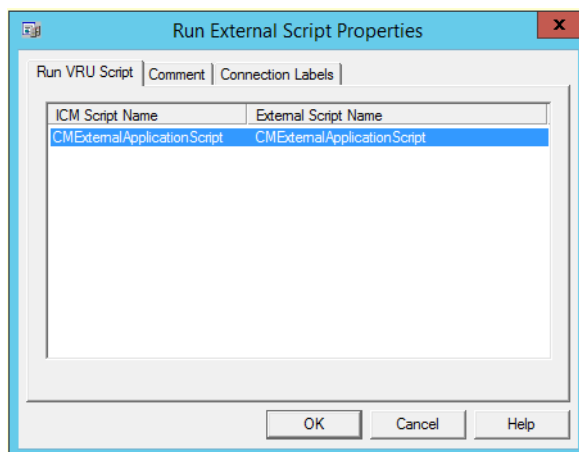
10. Click the **Save** button to save the script.



A sample script

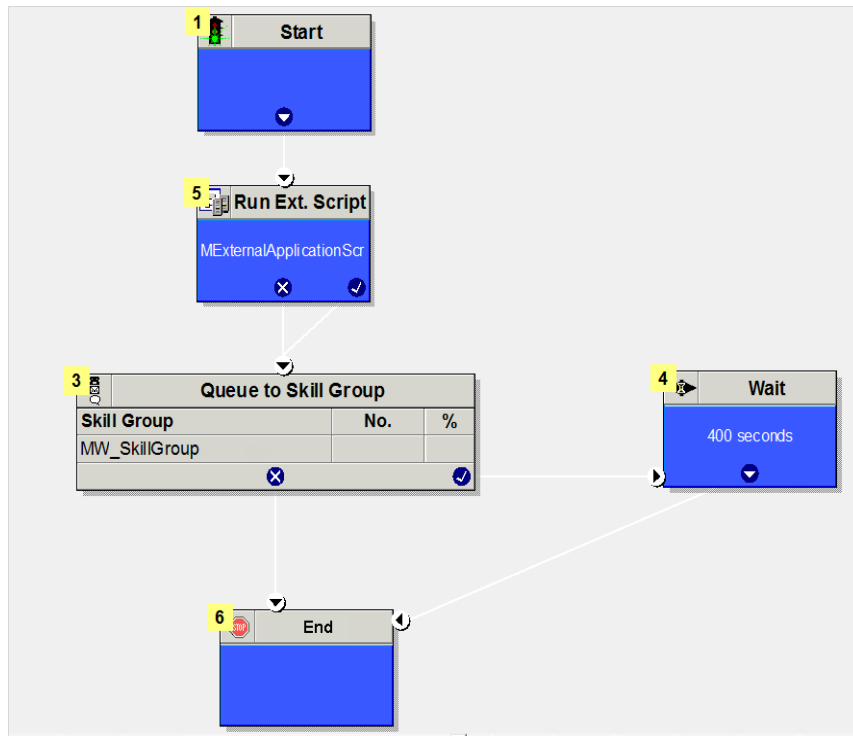
To display dynamic content to chat customers (for example, wait time, activity ID, etc.) while chat requests are being processed by the system, ensure that the Run External Script node is configured.

11. In the ICM script, add the Run External Script node and select the Network VRU script created for ECE.



Select the Network VRU script

The script will look like this.

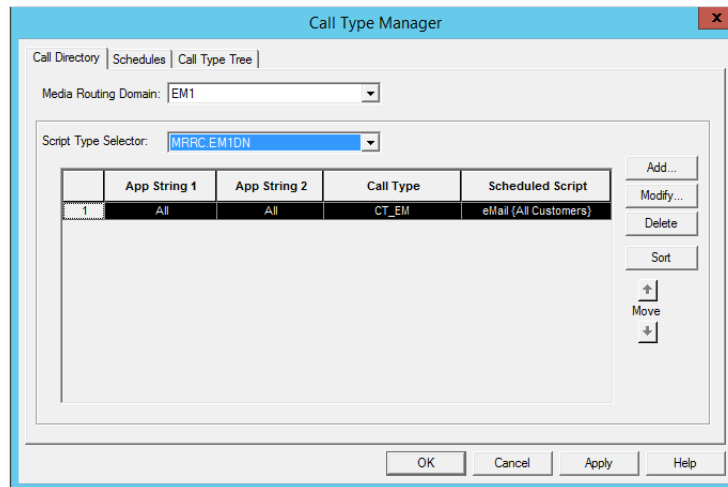


A sample script

After creating a script, map the script to a call type, MRD, and script selector. Also set the run schedule for the script.

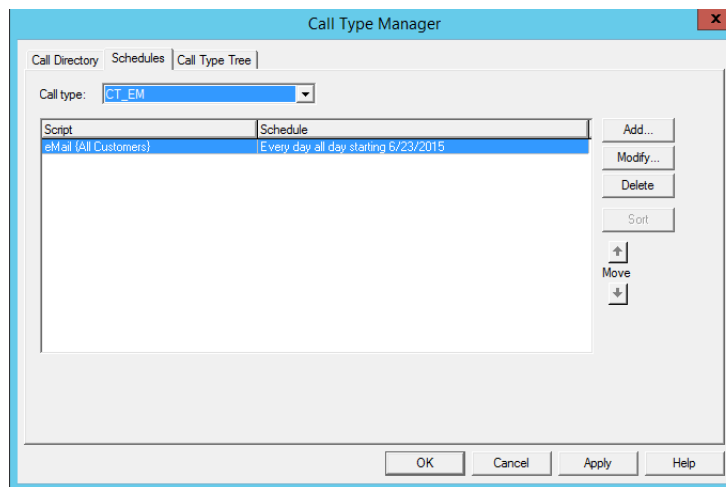
12. In the Script Editor window, go to **Script > Call Type Manager**.
13. In the Call Type Manager window, in the Call Directory tab, do the following:
 - a. In the Media Routing Domain field, from the dropdown list, select the MRD configured for ECE.
 - b. In the Script Type Selector field, from the dropdown list, select the script selector created for the MRD (page 35).

- c. Next, click the **Add** button. The Add Call Type Selector Entry window appears. In the Call type field, select the call type configured for ECE (page 30). Click **OK**.



Map the script to a call type, MRD, and script selector

14. In the Call Type Manager window, in the Schedule tab, do the following:
 - a. In the Call type field, from the dropdown list, select the same call type you selected in Step 13.
 - b. Next, click the **Add** button. In the Add Call Type Schedule window that appears, do the following:
 - i. In the Script tab, select the script configured for ECE (page 36).
 - ii. In the Period tab, set a schedule for the script.
 - iii. Click **OK**.



Set a schedule for the script

15. Click **OK** to close the Call Type Manager window.

Configuring Precision Routing

Precision Routing provides multidimensional routing with simple configuration, scripting, and reporting. For details about Precision Routing, see http://docwiki.cisco.com/wiki/Precision_Routing_Documentation



Important: Precision Queue feature is available only for installations integrated with version 11.5 of Packaged CCE.

To configure precision routing, create the following objects:

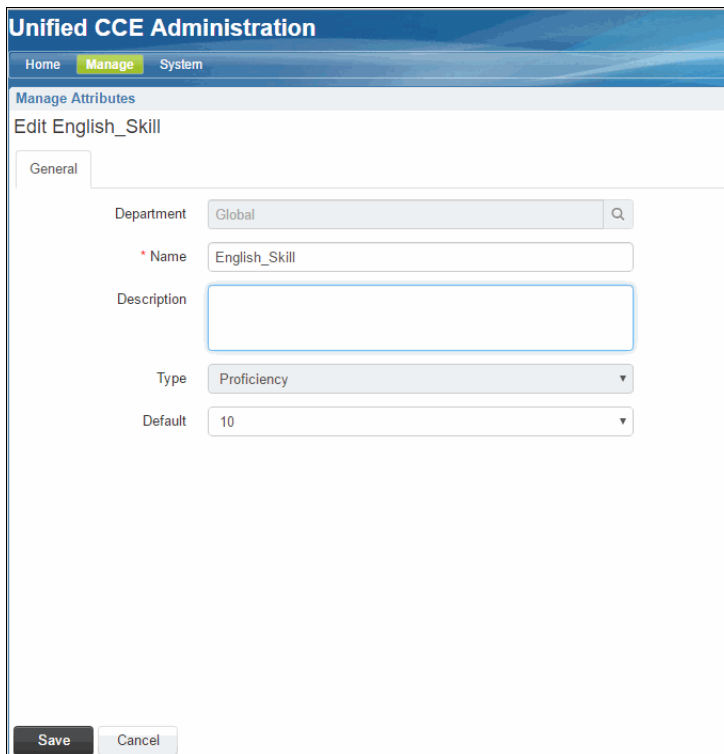
1. Create attributes ([page 41](#))
2. Assign attributes to agents ([page 42](#))
3. Create precision queues ([page 43](#))
4. Add precision queue node to the scripts ([page 44](#))

Creating Attributes

To create an attribute:

1. Launch the CCE Web Administration page, using the URL: `https://Server_Name/cceadmin/`
2. Login using the administrator credentials.
3. Go to **Manage > Attributes**.
4. On the Manage Attributes page, Click **New**.
5. In the **Name** field, type a unique attribute name.
6. From the **Type** dropdown list, select the type of attribute, which can be **Boolean** or **Proficiency**.
7. From the **Default** dropdown list, select from **True** or **False** for **Boolean** or a number between 1-10 for **Proficiency**.

8. Click **Save**.



The screenshot shows the 'Unified CCE Administration' web interface. At the top, there are navigation tabs for 'Home', 'Manage', and 'System'. Below this is a breadcrumb trail 'Manage Attributes' and the page title 'Edit English_Skill'. A 'General' tab is selected. The form contains the following fields:

- Department: A dropdown menu with 'Global' selected and a search icon.
- Name: A text input field containing 'English_Skill'.
- Description: A large empty text area.
- Type: A dropdown menu with 'Proficiency' selected.
- Default: A dropdown menu with '10' selected.

At the bottom of the form are two buttons: 'Save' and 'Cancel'.

Create attributes

Assigning Attributes to Agents

To assign attributes to agents:

1. Launch the CCE Web Administration page, using the URL: `https://Server_Name/cceadmin/`
2. Login using the administrator credentials.
3. Go to **Manage > Agents**.
4. In the list of agents, select an agent to assign attributes.

5. On the Attributes tab add the required attributes to agent and set the values for the attributes. click **Save**.

The screenshot shows the 'Unified CCE Administration' web interface. At the top, there are navigation tabs for 'Home', 'Manage', and 'System'. Below this, the page title is 'Manage Agents' and the agent name is 'Edit Maria Petroff (manya)'. There are four sub-tabs: 'General', 'Attributes', 'Skill Groups', and 'Supervised Teams'. The 'Attributes' tab is active. It features a 'List of Attributes' section with a search and add button. A table below shows one attribute: 'English_Skill' with a value of '10'. At the bottom of the interface are 'Save', 'Copy', and 'Cancel' buttons.

Name	Value
English_Skill	10

Assign attributes to agents

Creating Precision Queues

To create a precision queue:

1. Launch the CCE Web Administration page, using the URL: `https://Server_Name/cceadmin/`
2. Login using the administrator credentials.
3. Go to **Manage > Precision Queues**.
4. On the New Precision Queue page, provide the following details:
 - a. Provide a name for the queue.
 - b. Select a Media Routing Domain created for ECE.
 - c. Set the values for Service Level Type, Service Level Threshold, Agent Order, Bucket Interval to meet your business needs.

- d. Create the steps for the precision queue and in the expressions use the attributes created for ECE.

The screenshot shows the 'Unified CCE Administration' interface. The main content area is titled 'Manage Precision Queues' and 'Edit ECE_Email_Attribute'. The configuration fields are as follows:

- Name: ECE_Email_Attribute
- Description: (empty)
- Media Routing Domain: ECE_Email
- Service Level Type: Ignore Abandoned Calls
- Service Level Threshold: 500 seconds
- Agent Order: Longest Available Agent
- Bucket Interval: System Default (BuiltIn)
- ID: 5000

Below the configuration fields is a 'Steps' table with the following data:

Name	Criteria	# Agents (Config)	Wait Time	
Step 1	(Email_Content_Attribute == true)	3	0	✕
Step 2	(English_skill == 6)	3	n/a	✕

At the bottom of the form are 'Save' and 'Cancel' buttons. An 'Add Step' button is located to the right of the 'Steps' table.

Sample precision queue

Adding Precision Queue Node to the Scripts

- ▶ In the scripts for ECE, add the precision Queue node. For details about doing this task see the Precision Routing Documentation available at: http://docwiki.cisco.com/wiki/Precision_Routing_Documentation

Configuring Finesse

- ▶ Agents always access ECE through Finesse. After installing ECE, configure Finesse to add the ECE gadget. For details about doing this task, “[Configuring Finesse](#)” on page 52.

3 Installation Process

- ▶ [Installing ECE Server](#)
- ▶ [Installing Web Server](#)

Before beginning the installation, ensure that you have complied with all the prerequisites listed in “Pre-Installation Tasks” on page 11.

Installing ECE Server

The installation program automatically installs and configures JDK and WildFly as part of the installation.

To install the ECE server:

1. Start the installation by using the physical installation media or a mounted ISO file. Run `setup_wsjb.exe` to launch the installation program.

Alternatively, you can create a temporary directory on any drive on your server. For example, `C:\Temp`. Copy the contents of the installation package to the `Temp` folder on your local machine where you are running the installer. Run `setup_wsjb.exe` from the `C:\Temp\Application` directory.

2. When the Introduction window appears, read the installation instructions. Click **Next**.
3. In the License Agreement window, review the licensing terms and select the **I accept the terms of the License Agreement** option. Click **Next**.
4. In the Installation Options window, select the **ECE Server** option. The following ECE components are installed on this server: **File, Database, Messaging, Services, Application Servers**. Click **Next**.
5. In the Enterprise Chat and Email Home Directory window provide the path of the directory where you would like to install ECE. For example, `C:\Cisco`, or `\\SharedSpace\Cisco`, if the file server is installed on a NAS device. Click **Next**.

The installation program also installs WildFly and JDK at the same location.



Important: Make sure that the path and folder name do not contain any of the following characters: `*?<>|+^!'"%`,`@`

6. In the WildFly Parameters window, provide the following details and click **Next**.
 - **WildFly HTTP port:** Port number used by WildFly. Default value is 9001.
 - **WildFly HTTP SSL Port:** Secure Sockets Layer port number used by WildFly. Default value is 9002.
7. In the RMI and RMID Parameters window, provide the following details and click **Next**.
 - **RMI registry port:** Port number used by the Remote Method Invocation (RMI) registry naming service. Default value is 15099.
 - **RMI activation port:** Port number used by the RMI Daemon Process. Default value is 15098.
8. In the Cisco Application Context Root window, provide the name used to identify the document root of the Web Server. The context root of a web application determines which URLs are delegated to the web application. Default value is `system`. Click **Next**.



Important: Make sure there are no spaces or special characters in the name of the context root.

9. In the Cisco System Administrator Account window, provide the following details and click **Next**.

- **User name:** User name for the system administrator. This is the first user that gets created for accessing the system partition. Default value is `sa`.
- **Password:** Password for the system administrator. Note: The password should have at least eight characters and should be a mix of numbers and letters. For example, `password@123`.



Important: Do not use the following characters in the password: < (less than), > (greater than), ; (semi colon), : (colon), = (equal to), \ (back slash).

10. In the Cisco Partition Administrator Account and Partition Details window, provide the following details and click **Next**.
 - **User name:** User name for the partition administrator. This is the first user that gets created for accessing the business partition. Default value is `pa`.
 - **Password:** Password for the system administrator. Note: The password should have at least eight characters and should be a mix of numbers and letters. For example, `password@123`.



Important: Do not use the following characters in the password: < (less than), > (greater than), ; (semi colon), : (colon), = (equal to), \ (back slash).

- **Partition name:** Name for the business partition. Make sure that the name does not contain any spaces or special characters. Also, the partition name should be different than the context root name.
 - **Description of partition:** A brief description for the partition.
11. In the Knowledge Base Primary Language window, select the default language for the Knowledge Base. Default value is `English (US)`. Click **Next**.
 12. In the Default Notification Parameters window, set the following details and click **Next**.
 - **Default SMTP server:** The SMTP server to be used to send email notifications.
 - **Notification mail redirection from address:** All notification emails are sent from this email address.
 - **Notification mail redirection to address:** All notification emails are sent to this email address.
 13. In the SQL Server Database Authentication window, select the authentication type to be used while connecting to the database. Set the value as **SQL Server Authentication mode** or **Windows Authentication mode**. If you selected **Windows Authentication** as the only mode of authentication while installing SQL Server, you must set the value as **Windows Authentication mode**. Click **Next**.
 14. In the Master Database Parameters window, provide the following details and click **Next**. The instance name and port number provided in this screen are also used for active and archive databases.
 - **Server instance name:** Name of the MSSQL Server instance to be used while creating the database. Set this value only if you are using a named instance, and not the default instance.
 - **Database listener port:** Port number of the MSSQL Server. Default value is 1433.
 - **Datafile path:** Path to the folder where you want to create the data file.



Important: You *must* create the datafile on a different drive than the ECE home directory. For example, if ECE home is on C drive (`C:\ECE_Home`), create the datafile path on the D drive (`D:\MSSQL\Data`).

The following properties appear only if you selected the SQL Server Authentication mode.

- **Database administrator username:** User name of the database administrator for MSSQL Server.

- **Database administrator password:** Password of the database administrator.
 - **Cisco Database username:** User name required to connect to the master database. The installation program creates the database and its user.
 - **Cisco Database password:** Password for the master database user.
15. In the Active Database Parameters window, provide the following details and click **Next**.
- **Server instance name:** This is a read only field.
 - **Database listener port:** This is a read only field.
 - **Datafile path:** Path to the folder where you want to create the data file. For example, D:\MSSQL\Data.



Important: You *must* create the datafile on a different drive than the ECE home directory. For example, if ECE home is on C drive (C:\ECE_Home), create the datafile path on the D drive (D:\MSSQL\Data).

The following properties appear only if you selected the SQL Server Authentication mode.

- **Database administrator username:** This is a read only field.
 - **Database administrator password:** This is a read only field.
 - **Cisco Database username:** User name required to connect to the master database. The installation program creates the database and its user.
 - **Cisco Database password:** Password for the active database user.
16. In the Archive Database Parameters window, provide the following details and click **Next**.
- **Server instance name:** This is a read only field.
 - **Database listener port:** This is a read only field.
 - **Datafile path:** Path to the folder where you want to create the data file. For example, D:\MSSQL\Data.



Important: You *must* create the datafile on a different drive than the ECE home directory. For example, if ECE home is on C drive (C:\ECE_Home), create the datafile path on the D drive (D:\MSSQL\Data).

The following properties appear only if you selected the SQL Server Authentication mode.

- **Database administrator username:** This is a read only field.
 - **Database administrator password:** This is a read only field.
 - **Cisco Database username:** User name required to connect to the archive database. The installation program creates the database and its user.
 - **Cisco Database password:** Password for the archive database user.
17. In the Packaged CCE Primary AWDB Details window, provide the following details and click **Next**.
- **Authentication:** Select from **SQL Server Authentication** or **Windows Authentication**.
 - **Host name:** The server name or IP address of the host where AWDB is installed for the Packaged CCE deployment.
 - **SQL server database name:** The name of the AWDB database.

- **Port number:** Set the value to match the port configured in Unified CCE. By default the value is set to 1433.

The following properties are enabled only when you are using SQL Authentication.

- **Database administrator login name:** The database administrator's user name.
- **Database administrator login password:** The database administrator password.

18. In the Packaged CCE Secondary AWDB Details window, provide the following details and click **Next**.

- **Configure Secondary AWDB details:** Select **Yes** if you want to add a secondary AWDB details.
- **Authentication:** Select from **SQL Server Authentication** or **Windows Authentication**.
- **Host name:** The server name or IP address of the host where AWDB is installed for the Packaged CCE deployment.
- **SQL server database name:** The name of the AWDB database.
- **Port number:** Set the value to match the port configured in Unified CCE. By default the value is set to 1433.

The following properties are enabled only when you are using SQL Authentication.

- **Database administrator login name:** The database administrator's user name.
- **Database administrator login password:** The database administrator password.

19. In the Organization Information window, provide the name, business unit, location, and country of your organization. Note that special characters are not allowed in any of the fields. Click **Next**.

20. In the Domain User Account Parameters window, provide the following details and click **Next**.

- **Domain User name:** User name of the domain user account you created for use by the application. For more information, refer to [“Setting Up User Accounts and Permissions” on page 16](#). If you are using a local account with administrative privileges, provide the value as `Machine_Name\Username`. For example, `ECE11\Jane`.
- **Domain User Password:** Password for the domain user.

21. Review the information displayed in the Summary window, and click **Install**.

22. In the Install Complete window, click the **Finish** button to complete the installation process.

A summary of the installation is saved in

`Cisco_Home\eservice\installation\logs\installation_summary_Server_Name.txt`.

Installing Web Server

The installation program automatically installs and configures IIS on the web server. If IIS is already installed, it will be used by the application. The installation program will check to see if all the required components and extensions are available. If not, it will prompt for confirmation to make changes to IIS. If you prefer to make these changes manually, follow instructions in [“Preparing Web Server Machine” on page 19](#).

To install the web server:

1. Start the installation by using the physical installation media or a mounted ISO file. Run `setup_wsjb.exe` to launch the installation program.

Alternatively, you can create a temporary directory on any drive on your server. For example, *C:\Temp*. Copy the contents of the installation package to the *Temp* folder on your local machine where you are running the installer. Run *setup_wsjb.exe* from the *C:\Temp\Application* directory.

2. When the Introduction window appears, read the installation instructions. Click **Next**.
3. In the License Agreement window, review the licensing terms and select the **I accept the terms of the License Agreement** option. Click **Next**.
4. In the Installation Options window, select the **Web Server** option. Click **Next**.
5. The installation program checks and sees if all the required IIS components are configured on the server. If not, it will prompt for confirmation to install the components. Click **Yes** to install the components and continue with the installation.
6. In the ECE Server Parameters window, provide the name of the server where ECE server is installed. Make sure you provide the DNS host name and not the IP address of the server. Click **Next**.
7. In the Enterprise Chat and Email Home Directory window provide the path of the directory where you would like to install ECE. For example, *C:\Cisco*, or *\\SharedSpace\Cisco*, if the file server is installed on a NAS device. Click **Next**.



Important: Make sure that the path and folder name do not contain any of the following characters: `*?<>|+^'"%`,`@`

8. In the IIS Web Site Parameters window, provide the name of the IIS Web Site on which the application is to be configured. Default value is Default Web Site. Click **Next**.
9. In the Cisco Application Context Root window, provide the same context root name which was provided at the time of installing the ECE server ([page 46](#)). Click **Next**.
10. In the Cisco Partition Name window, provide the name for the business partition. Make sure you provide the same name which was provided at the time of installing the ECE server ([page 47](#)).
11. In the Domain User Account Parameters window, provide the following details and click **Next**.
 - **Domain User name:** User name of the domain user account you created for use by the application. For more information, refer to “[Setting Up User Accounts and Permissions](#)” on [page 16](#). If you are using a local account with administrative privileges, provide the value as `Machine_Name\Username`. For example, *ECE11\Jane*.
 - **Domain User Password:** Password for the domain user.
12. Review the information displayed in the Summary window, and click **Install**.
13. In the Install Complete window, click the **Finish** button to complete the installation process.

A summary of the installation is saved in

Cisco_Home\eservice\installation\logs\installation_summary_Server_Name.txt.

After the installation is completed, perform the post-installation tasks ([page 51](#)).



Post-Installation Tasks

- ▶ [Configuring Permissions on IIS Config Folder](#)
- ▶ [Configuring SSL for Secure Connections](#)
- ▶ [Configuring SMTP Server Relay Address List](#)
- ▶ [Configuring Finesse](#)
- ▶ [Configuring Active Directory Federation Services for Single Sign-On](#)
- ▶ [Starting ECE](#)
- ▶ [Stopping ECE](#)
- ▶ [Signing in to ECE](#)
- ▶ [Configuring Important Settings](#)
- ▶ [Uninstalling ECE](#)

This chapter guides you through the tasks to be performed after installing the system. It also describes the process of uninstalling ECE.

Configuring Permissions on IIS Config Folder

- ▶ Skip this task if it was done as part of the pre-installation tasks ([page 21](#)). Ensure that the user account that you used for installing the application ([page 16](#)) has read permissions on the following folder on the web server: `%systemroot%\system32\inet_srv\config`.

Configuring SSL for Secure Connections

- ▶ You must set up Secure Sockets Layer (SSL) for more secure connections between browsers and the servers in your installation. This is a required step. See “[SSL Configuration](#)” on [page 86](#) for details.

Configuring SMTP Server Relay Address List

- ▶ The default SMTP server configured during the installation process is used to send notifications. To allow the system to successfully send such emails, verify that the IP addresses of all the application servers in the configuration are added to the relay address list of the SMTP server.

Configuring Finesse

Perform these tasks after installing ECE. Cisco Finesse enables the use of custom gadgets for Voice & Multichannel (ECE), facilitating the ECE user interface to be embedded within a gadget to provide contact center agents a unified desktop experience.



Important: Before you begin the configuration, ensure that the Finesse VM and software are installed and ready for use. Also, ensure that ECE is installed.

Copying Files from ECE Server

- ▶ From the ECE server, copy the contents of the `ECE_Home\Utilities\finesse_gadget` folder to a temporary directory, *Temp*, on your local machine.

Configuring Finesse Files

Perform these tasks from any local machine.

To configure the `ece_config.js` file:

1. From the `Temp\Finesse_gadget\agent` folder created on the local machine (page 52) open the `ece_config.js` file in a text editor.
2. Locate the following text in the file:

```
var web_server_name = "<Load_Balancer_or_Web_Server_Host_Name>";
```
3. Replace `<Load_Balancer_or_Web_Server_Host_Name>` with the host name of the ECE web server. If the deployment uses a load balancer, provide the host name of the load balancer.

Enabling 3rdpartygadget Account and Deploying the Gadget

Perform these tasks on the Finesse server.

To enable the 3rdpartygadget account and deploy the Gadget:

1. Using the Finesse Console, login as an administrator and enable the **3rdpartygadget** account on the Finesse server.

When you enable the **3rdpartygadget** account, a **files** folder gets created automatically.
2. Create a new folder called **ECE** under the **files** folder.
3. Deploy the gadget files from the `Temp\Finesse_gadget\agent` folder and the `Temp\Finesse_gadget\solve` folder on your local machine (page 53) to the Finesse server using a secure FTP client.

Configuring Finesse Settings and Layout

Perform these tasks from any local machine.

To configure the Finesse settings and layout:

1. Launch the URL: `http://Finesse_Server_Name/cfadmin`. Login as a finesse administrator.

2. Configure the Contact Center CTI Server Settings and Contact Center Enterprise Administration & Data Server Settings.

The screenshot shows the Cisco Finesse Administration interface. The top navigation bar includes 'Settings', 'Call Variables Layouts', 'Desktop Layout', 'Phone Books', 'Reasons', 'Team Resources', and 'Workflows'. The main content area is divided into two sections:

Contact Center Enterprise CTI Server Settings

Note: Any changes made to the settings on this gadget require a restart of Cisco Finesse Tomcat to take effect.

Fields for configuration:

- *A Side HostIP Address: 10.19.19.70
- B Side HostIP Address: []
- *A Side Port: 42027
- B Side Port: []
- *Peripheral ID: 5000

*Indicates required fields

Buttons: Save, Revert

Contact Center Enterprise Administration & Data Server Settings

Note: Any changes made to the settings on this gadget require a restart of Cisco Finesse Tomcat to take effect.

Fields for configuration:

- *Primary HostIP Address: 10.19.19.70
- Domain: training
- Backup HostIP Address: []
- *Username: administrator
- *Database Port: 1433
- *Password: []
- *AW Database Name: na_awdb

*Indicates required fields

Buttons: Save, Revert

Configure the settings

3. From Desktops Layout section, configure the layout for the ECE and Solve gadgets. XML contents for the ECE and Solve gadget tabs are available in the following files copied from the ECE server (page 52):

- Temp\ finesse_gadget\layout\agent.xml
- Temp\ finesse_gadget\layout\solve.xml

While configuring the gadgets, make sure that the path to the `ece.xml` file in the `<gadget>` tag is correct.

Refer the Finesse documentation to see how gadgets are added in Finesse.

Starting Finesse Services

To start the Finesse services:

On the Finesse server, restart Finesse Services by doing the following:

1. Connect to the Finesse Server using a remote client tool. For example, putty.
2. Login using the Finesse Administrator account.
3. Restart Cisco Tomcat service.

```
utils service restart Cisco Tomcat
```

4. Restart Cisco Finesse Tomcat service.

```
utils service restart Cisco Finesse Tomcat
```

Configuring Active Directory Federation Services for Single Sign-On

- ▶ Single Sign-On with Cisco IDS requires that ECE is connected to Active Directory Federation Services (AD FS). If you are planning to use single sign-on, see [“Single Sign-On Configuration” on page 60](#) for details about configuring AD FS.

Starting ECE



Important: Run the application using the same domain account that was used for installing the application ([page 16](#)).

To start ECE:

- ▶ On the ECE server, start the Cisco service from the Windows Services panel. If you get the following error while starting the Cisco service, see [“Troubleshooting Application Start-Up Issues” on page 55](#): Error 1069: The service did not start due to login failure.

Troubleshooting Application Start-Up Issues

Perform these tasks if you get the following error while starting the service: Error 1069: The service did not start due to login failure.

To troubleshoot:

1. In the Windows service panel, right-click the Cisco Service and from the menu select **Properties**.
2. In the Properties window, go to the Log On tab and provide the password of the domain user account ([page 16](#)) and click **Apply**.
3. Start the Cisco Service.

Stopping ECE

If you need to stop the application at any point during the post-installation tasks, follow the steps in this section.

To stop ECE:

- ▶ On the ECE server, stop the Cisco service from the Windows Services panel.

Signing in to ECE

Signing in to Agent Console

To sign in to the Agent Console:

1. Ensure that the desktops meet the requirements outlined in *System Requirements for Enterprise Chat and Email*.
2. Access the Finesse URL from a browser and sign in to Finesse: `https://Finesse_Server_Name/desktop`
3. Click on the Manage Chat and Email tab. If Single Sign-On is enabled, then the agent will be logged in automatically. If not, enter the username and password and click **Sign In**.

Signing in to All Other Consoles

A system partition and a business partition are created during the installation. To begin using the application, you log in to the business partition.

To sign in to the business partition:

1. Ensure that you have followed the instructions in the *Enterprise Chat and Email Browser Settings Guide* document to configure your browser, and that the desktops meet the requirements outlined in *System Requirements for Enterprise Chat and Email*.
2. Type the URL `http://Web_server.company.com/Partition_name` in your browser, where *Web_server.company.com* is the fully qualified domain name of your web server and *Partition_name* is the virtual directory created for this partition. During the installation, you are prompted to provide the partition name in the Partition Administrator Account and Partition window. This is used to create the virtual directory. If you have configured the web server to use SSL, then the URL is `https://Web_Server.company.com/Partition_name`.

Always use the fully qualified domain name of the web server when you type the URL to access ECE.

3. In the Sign In window, type the user name and password you had set up for the partition administrator in the Partition Administrator Login Parameters window during the installation. Click the **Log In** button.

Configuring Important Settings

This section introduces the main settings that allow you to configure various aspects of the application. Some settings are configured at the partition level, while others have to be set up for each department.

These settings are of two types:

1. **Mandatory settings:** These settings are configured during installation, and must be verified before using the application. Settings related to ESMTP protocol, must be configured manually if you are using ESMTP protocol for email notifications.
2. **Optional settings:** Although it is not mandatory to change these settings, you are likely to feel the need to configure them for your business.

Mandatory Settings

At the partition level

The following setting must be configured if you are using Single Sign-on or reports notifications:

- ▶ Web server URL or Load Balancer URL

The following settings are updated during installation, but we recommend that you log in to the application as a partition administrator, and verify and update them from the Administration Console, if required. The application starts using this information as soon as the installation is complete.

- ▶ Default SMTP server
- ▶ Notifications mail SMTP Server
- ▶ From: address for notification from Service
- ▶ To: address for notification from Service

At the department level

This setting is automatically updated for the first department created by the installation program. For all subsequent departments, the administrator must configure it.

- ▶ From email address for alarm

Optional Settings

Although it is not mandatory to change these settings, you are likely to feel the need to configure them for your business.

At the partition level

- ▶ Customer departmentalization
- ▶ Session time out
- ▶ Inactive time out
- ▶ Exception email SMTP

- ▶ Exception mail redirection to address
- ▶ Exception mail redirection from address
- ▶ Autopushback time (minutes after logout)
- ▶ Chat auto-pushback settings

At the department level

- ▶ Business calendar time zone

For a complete list of all available settings, refer to the *Enterprise Chat and Email Administrator's Guide to Administration Console*.

Uninstalling ECE

The application needs to be uninstalled from the following servers. The uninstallation program can be run in any order on these servers.

- ▶ ECE Server
- ▶ Web Server

To ensure that critical data is not lost, the program does not uninstall the following components:

- ▶ The databases
- ▶ The following folders on the ECE server:
 - *Cisco_Home\eService\storage*
 - *Cisco_Home\eService\logs*

Preparing to Uninstall

Stopping the Application

- ▶ Before you begin the uninstallation process, make sure you stop ECE. For details, refer to [“Stopping ECE” on page 56](#).

Stopping IIS

- ▶ Stop IIS (World Wide Web Publishing Service) on the web server in the installation.

Uninstalling ECE

To uninstall in graphical mode:

1. Go to **Start > Settings > Control Panel**.

2. Click **Programs** in the Control Panel window.
3. Click **Programs and Features** in the Programs window.
4. From the list of currently installed programs, right-click Enterprise Chat and Email and select **Uninstall/Change**.
5. In the Uninstall Enterprise Chat and Email window, click the **Uninstall** button.
6. When the uninstallation is complete, you are given a choice of restarting the server right away, or doing it later.
7. On the database server, go to the SQL Server Management Studio and delete the following, if required.
 - Go to **Databases** and delete the databases.
 - Go to **Security > Logins** and delete the logins created for the databases.
 - Go to **SQL Server Agent > Jobs** and delete the SQL Jobs for the databases. The jobs related to your databases will have the database name in the end. For example, `populatesmmy_eGReportsDB`.

Performing Post Uninstallation tasks

Starting IIS

- ▶ Start IIS (World Wide Web Publishing Service) on all web servers in the installation.



Single Sign-On Configuration

- ▶ [Configuring Single AD FS Deployment](#)
- ▶ [Configuring Split AD FS Deployment](#)
- ▶ [Configuring Single Sign-On in ECE](#)

Single Sign-On with Cisco IDS requires that ECE is connected to Active Directory Federation Services (AD FS). You can use one of the following options for AD FS:

- ▶ **Single AD FS:** In a single AD FS deployment, Resource Federation Server and Account Federation Server are installed on the same machine (page 61).
- ▶ **Split AD FS:** In a split AD FS deployment, Resource Federation Server and Account Federation Server are installed on separate machines (page 69).

Configuring Single AD FS Deployment

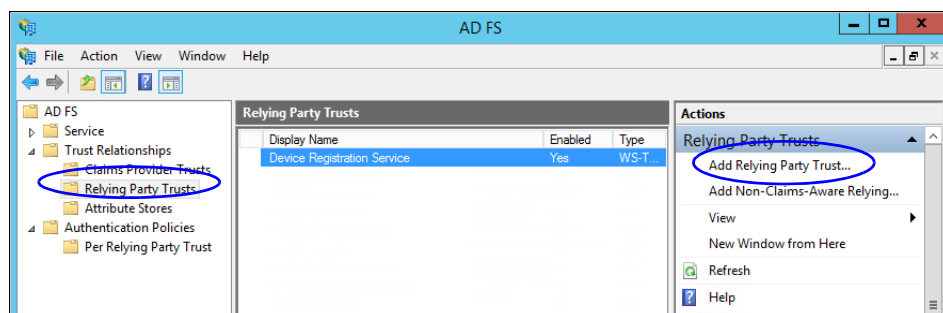
In a single AD FS deployment, Resource Federation Server and Account Federation Server are installed on the same machine.

Configuring Relying Party Trust for ECE

Perform these tasks on the server where Resource Federation Server and Account Federation Server are installed.

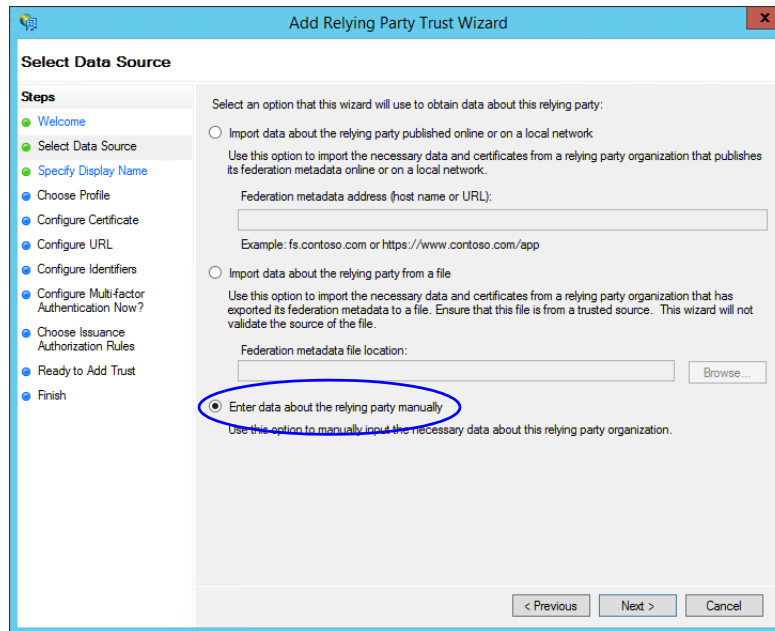
To configure relying party trust for ECE in single AD FS:

1. Go to the Start menu and open AD FS Management console.
2. In the AD FS Management console, navigate to **AD FS > Trust Relationships > Relying Party Trust**.
3. In the Actions section, go to Relying Party Trust, and click **Add Relying Party Trust...**



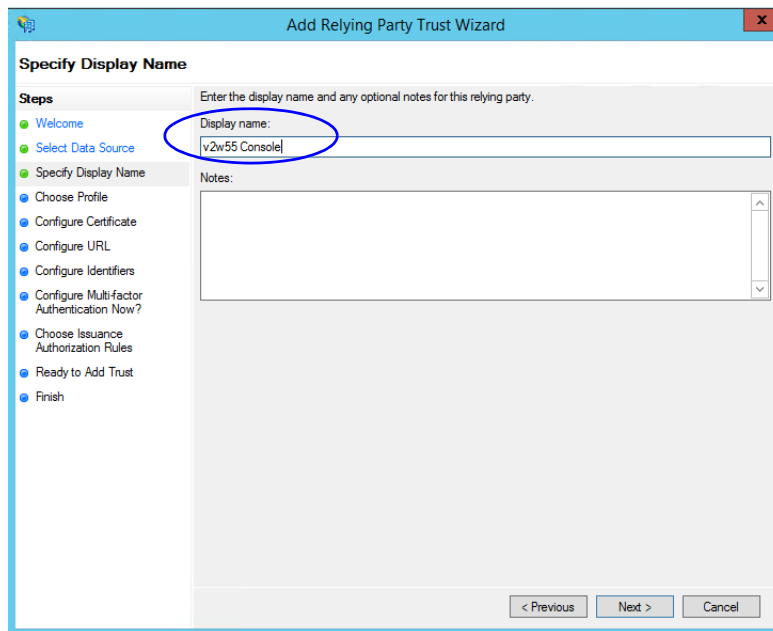
4. In the Add Relying Party Trust Wizard that appears, do the following:
 - a. On the Welcome screen, click **Start**.

- b. On the Select Data Source screen, select the **Enter data about the reply party manually** option and click **Next**.



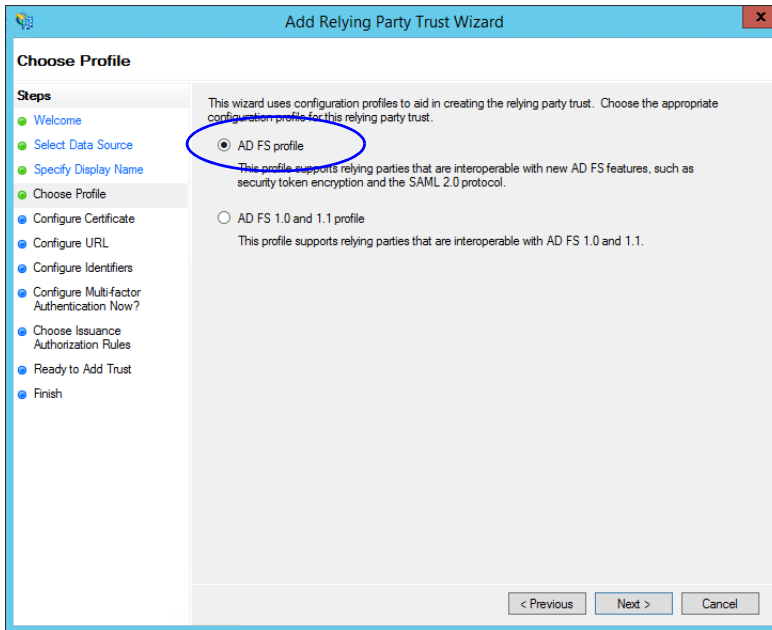
Select the *Enter data about the reply party manually* option

- c. On the Specify Display Name screen, provide a **Display name** for the relying party. Click **Next**.



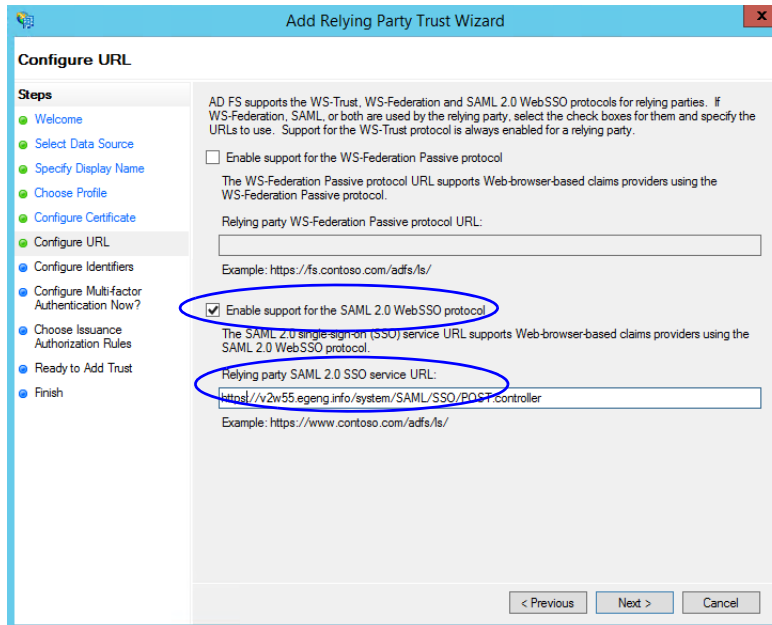
Provide a *display name*

- d. On the Choose Profile screen, select **AD FS profile** and click **Next**.



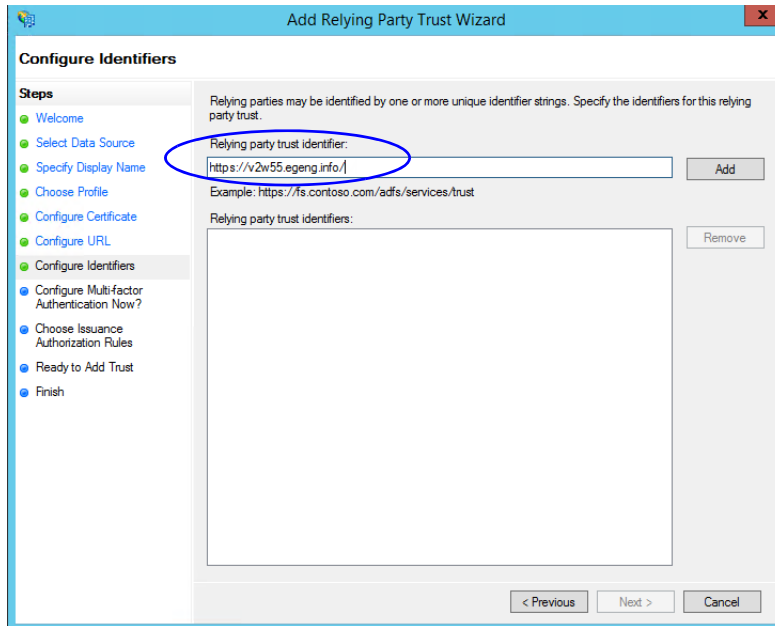
Select AD FS profile

- e. On the configure Certificate screen, click **Next**.
- f. On the Configure URL screen, set the following:
- Select the **Enable support for the SAML 2.0 Web SSO protocol** option.
 - In the **Relying Party SAML 2.0 SSO server URL** field provide the URL in the format: `https://Web_Server_Or_Load_Balancer_Server/system/SAML/SSO/POST.controller`. Replace `Web_Server_Or_Load_Balancer_Server` with the ECE web server name or the Load balancer server name.



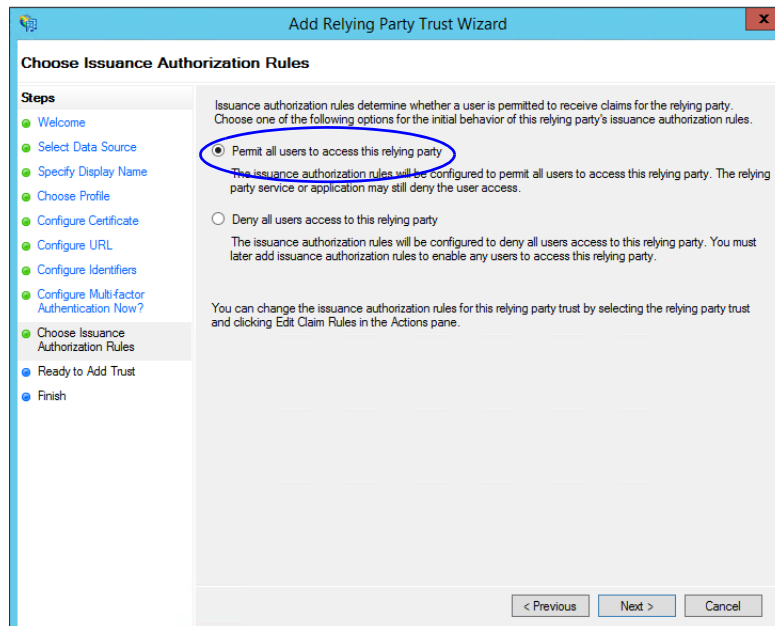
Configure the URL

- g. On the Configure Identifiers screen, provide the Relying party trust identifier and click **Add**. Value should be in the format: `https://Web_Server_Or_Load_Balancer_Server/`. Replace `Web_Server_Or_Load_Balancer_Server` with the ECE web server name or the Load balancer server name. Click **Next**.



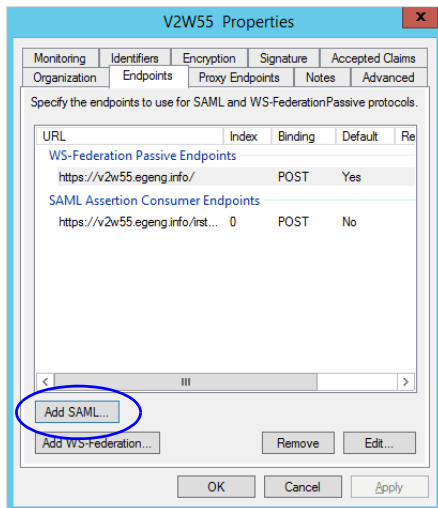
Configure the identifiers

- h. On the next screen, select the **I do not want to configure multi-factor authentication settings for the relying party trust at this time** option.
- i. On the Choose Issuance Authorization Rules screen, select the **Permit all users to access this relying party** option.



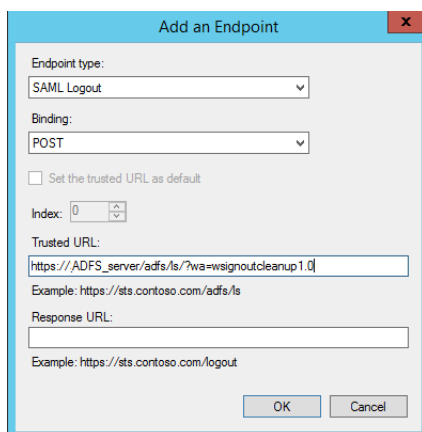
Select the Permit all users to access this relying party option

- j. On the Ready to add trust screen, click **Next**.
 - k. Uncheck the **Open the Edit Claim Rules dialogue for this relying party trust when the wizard closes** option and click **Close**. At the end, an entry is created in the Relying Provider Trusts list.
5. In the Relying Provider Trusts list, select the trust created for ECE, and in the actions section click **Properties**.
 6. In the Properties window, go to the Endpoints tab and click the **Add SAML..** button.



Click Add SAML

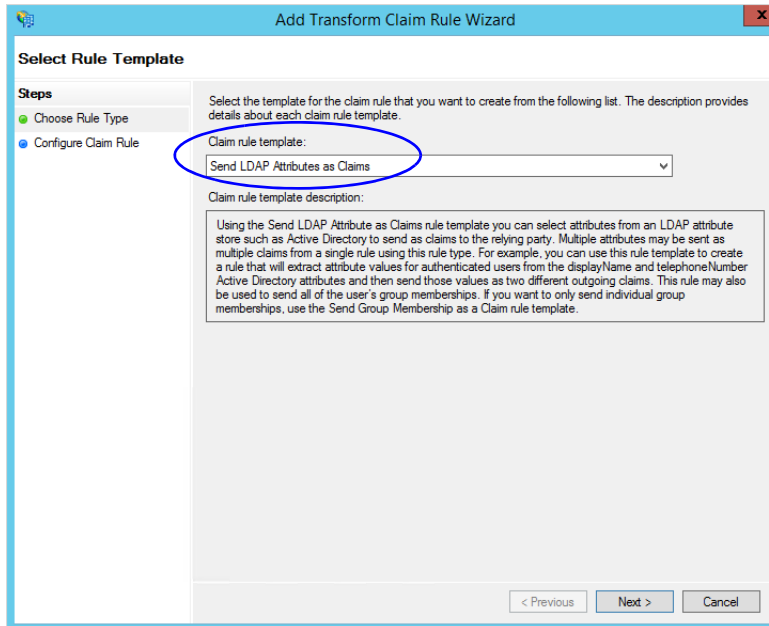
7. In the Add an Endpoint window, set the following:
 - a. Select the **Endpoint type** as **SAML Logout**.
 - b. Specify the **Trusted URL** as `https://ADFS_server/adfs/ls/?wa=wsignoutcleanup1.0`. Replace *ADFS_server* with the single AD FS server name.
 - c. Click **OK**.



Create an end point

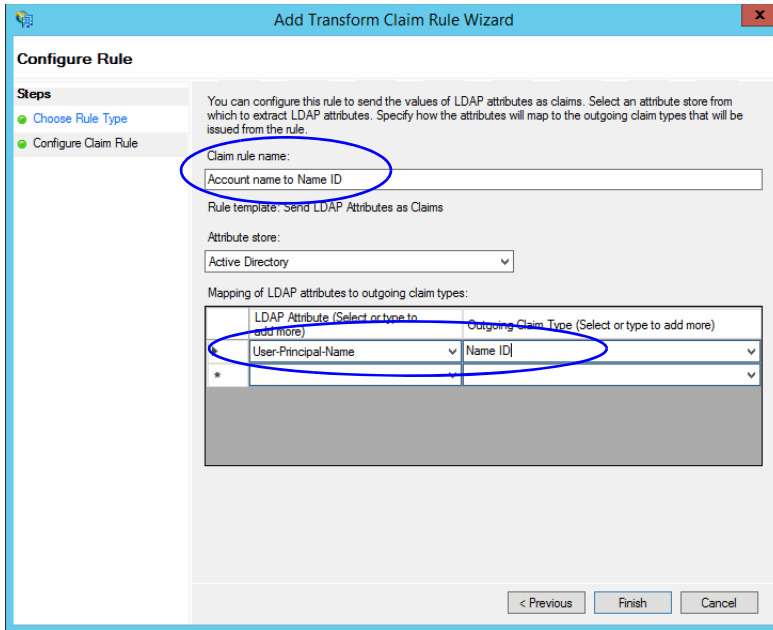
8. In the Relying Provider Trusts list, select the trust created for ECE, and in the actions section click **Edit Claim Rules**.

9. In the Edit Claim Rules window, in the Issuance Transform Rules tab, click the **Add Rule...** button.
In the Add Transform Claim Rule wizard that opens, do the following:
 - a. On the Choose Rule Type screen, from the **Claim rule template** dropdown, select **Send LDAP Attributes as Claims**. Click **Next**.



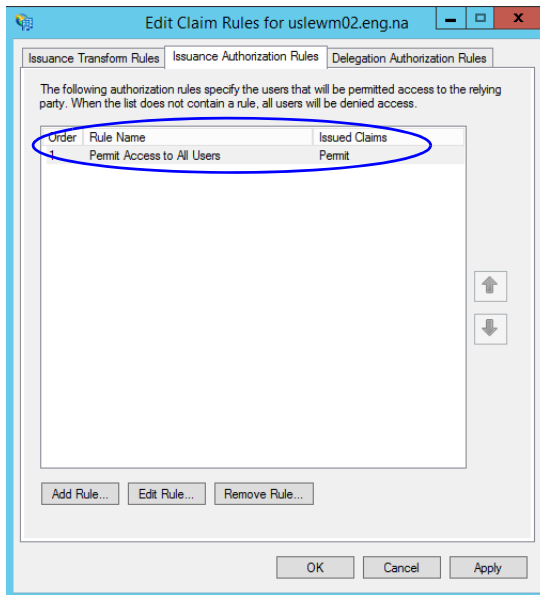
Select the claim rule template

- b. On the Configure Rule screen, set the following:
 - i. Provide the Claim rule name.
 - ii. Define mapping of LDAP attribute and the outgoing claim type. Select **Name ID** as the outgoing claim type name. Click **Finish** to go back to the Edit Claim Rules for single AD FS window.



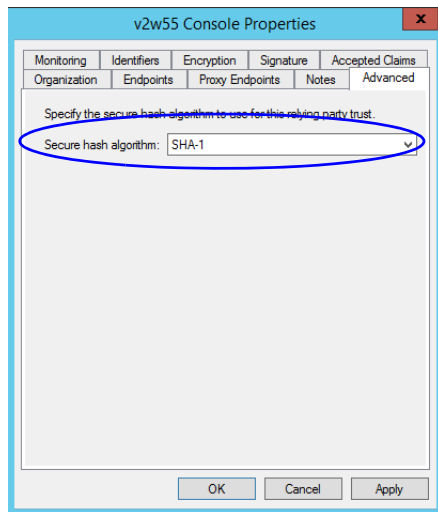
Configure the rule

- In the Edit Claim Rules window, in the Issuance Authorization Rules tab, ensure that the rule permits access to all users. Click **OK** to close the window.



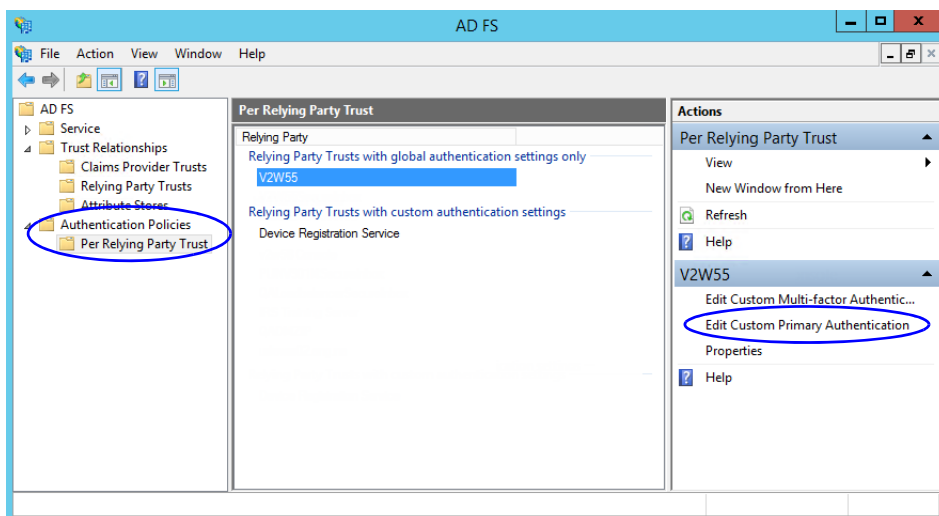
Check the authorization rules

11. In the Relying Provider Trusts list, double-click the relying party trust which you created. In the Properties window that opens, go to the Advanced tab and set the **Secure hash algorithm** to **SHA-1**. Click **OK** to close the window.



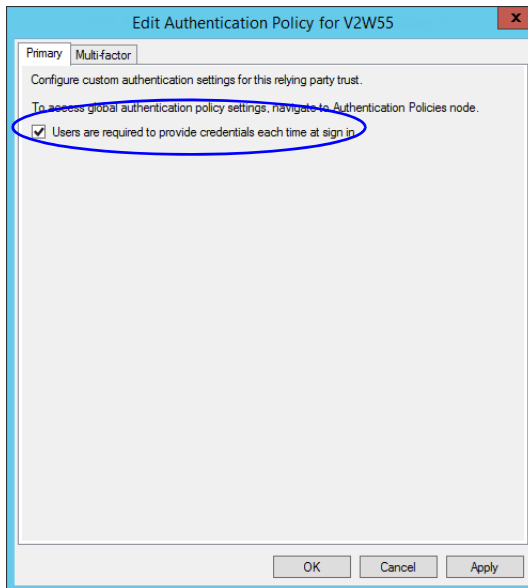
Set the secure hash algorithm

12. Next, in the AD FS Management console, go to the **Authentication Policy > Per Relying Party Trust**. Locate the Relying Party Trust created for ECE, and in the Actions section click **Edit Custom Primary Authentication**.



Change the authentication policy for ECE

13. In the Edit Authentication Policy window, in the Primary tab, select the **Users are required to provide credentials each time at sign in** option. Click **OK** to close the window.



Edit the authentication policy

Configuring Split AD FS Deployment

In a split AD FS deployment, Resource Federation Server and Account Federation Server are installed on separate machines. Resource Federation Server acts as shared AD FS and Account Federation Server acts as customer AD FS.

Configuring split AD FS includes:

- ▶ [Adding Security Certificates for the AD FS Domains](#)
- ▶ [Configuring Relying Party Trust for Shared AD FS in Customer AD FS](#)
- ▶ [Configuring Claims Provider Trust for Customer AD FS in Shared AD FS](#)
- ▶ [Configuring Relying Party Trust for ECE in Shared AD FS](#)

Adding Security Certificates for the AD FS Domains

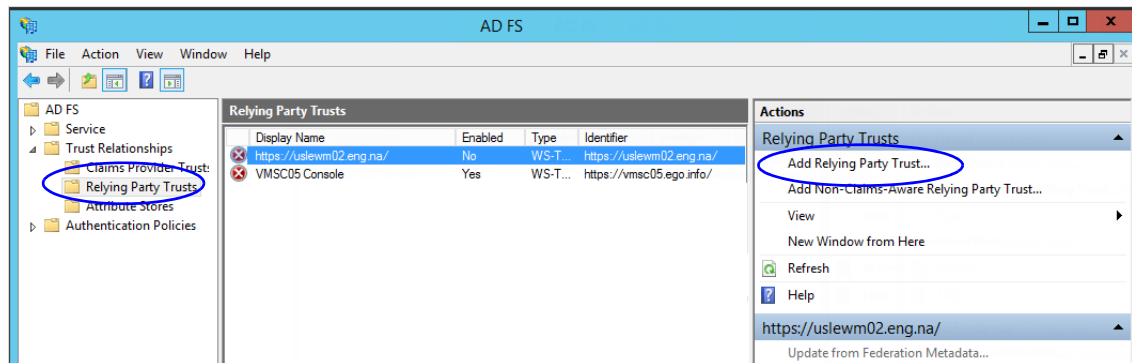
- ▶ If Customer AD FS and Shared AD FS are installed in different domain, you need to add certificates of the domains to the **Trusted Root Certification Authorities** store of the servers. On the Customer AD FS server, add the certificate of the Shared AD FS and vice versa. Contact your IT department to do this task.

Configuring Relying Party Trust for Shared AD FS in Customer AD FS

Perform these tasks on the server where customer AD FS is installed.

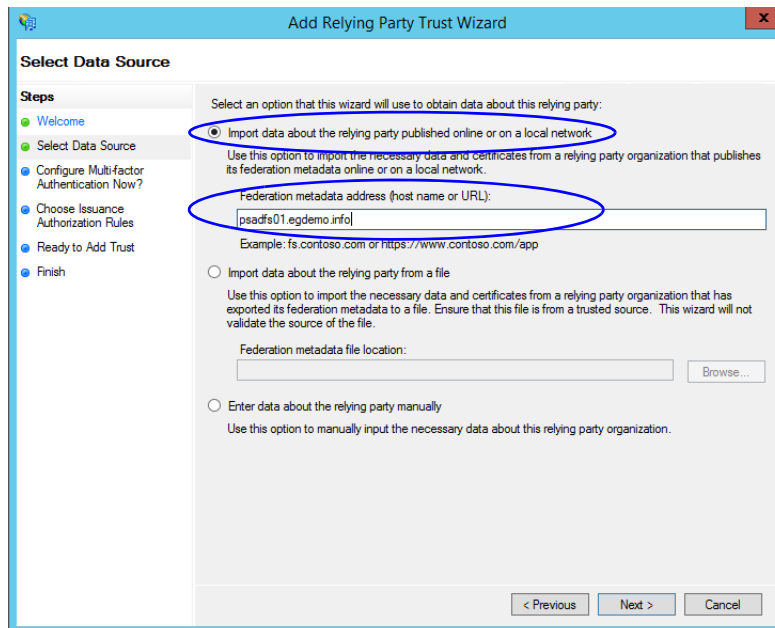
To configure relying party trust for shared AD FS in customer AD FS:

1. Go to the Start menu and open the AD FS Management console.
2. In the AD FS Management console, navigate to **AD FS > Trust Relationships > Relying Party Trust**.
3. In the Actions section, go to Relying Party Trust, and click **Add Relying Party Trust...**



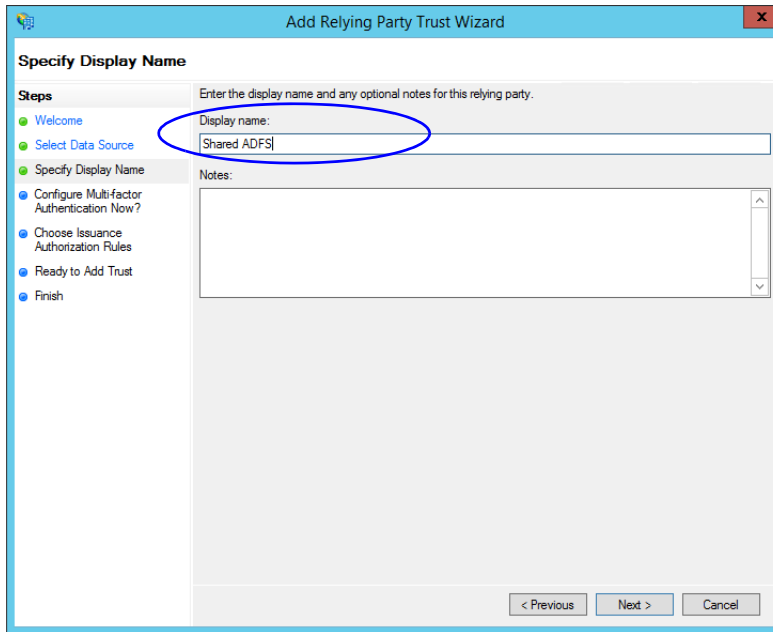
Click Add Relying Party Trust

4. In the Add Relying Party Trust Wizard that appears, do the following:
 - a. On the Select Data Source screen, set the following options:
 - i. Select the **Import data about the relying party published on online or on a local network** option.
 - ii. In the **Federation metadata address** field, provide the Shared AD FS server name.
 - iii. Click **Next**.



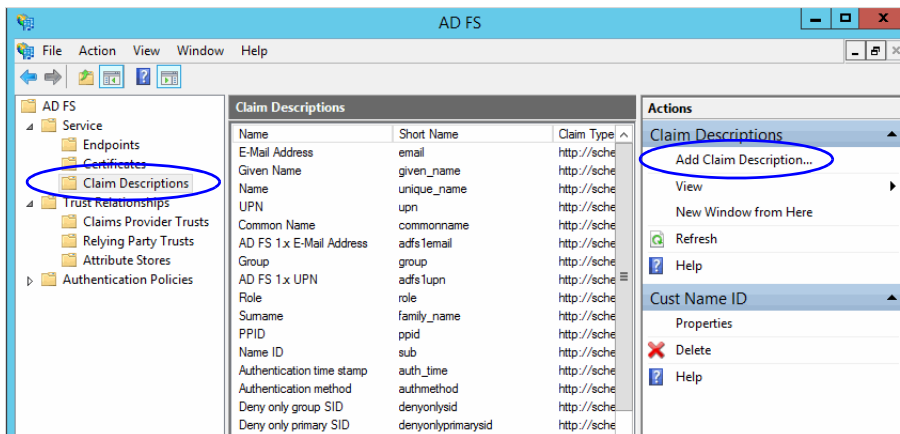
Select the data source options

- b. On the Specify Display Name screen, provide the **Display name**. Click **Next**.



Provide a display name

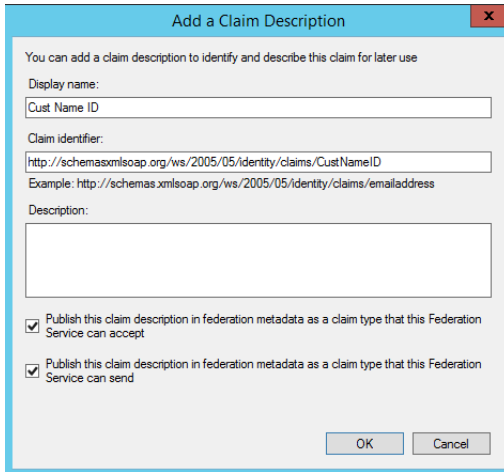
- c. In the screens that follow, do not alter the default values. Continue to click the **Next** button in the wizard until a trust is created. At the end, an entry is created in the Relying Party Trusts list.
5. In the AD FS Management console, navigate to **Services > Claim Descriptions**.
 6. In the Actions section, go to Claim Descriptions, and click **Add Claim Descriptions...**



Click Add Claim Description

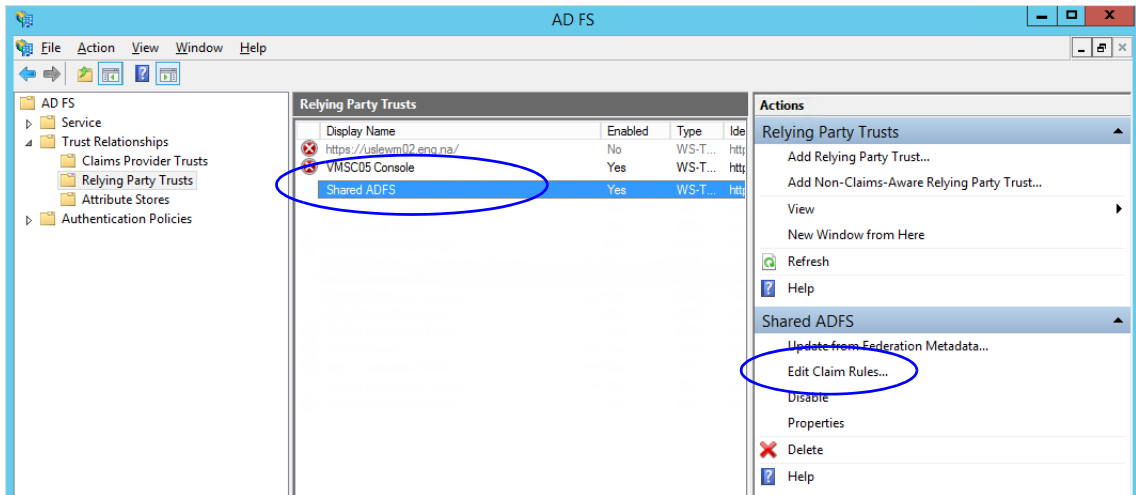
7. In the Add a Claim Description window, provide the following details:
 - a. Set the **Display name** as **Cust Name ID**.
 - b. Set the **Claim identifier** as **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/CustNameID**
 - c. Select the **Publish the claim description in federation metadata as a claim type that this Federation Service can accept** option.

- d. Select the **Publish the claim description in federation metadata as a claim type that this Federation Service can send** option.
- e. Click **OK** to close the window.



Provide the claim description

- 8. In the Relying Party Trusts list, select the Shared AD FS entry and in the Actions section, click **Edit Claims Rules**.

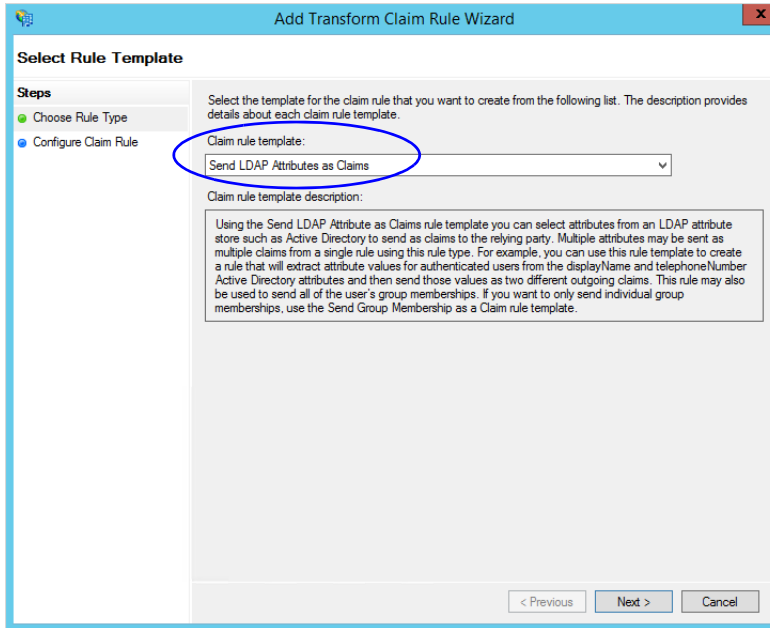


Click Edit Claims Rules

- 9. In the Edit Claim Rules for Shared AD FS window, in the Issuance Transform Rules tab, click the **Add Rule...** button.

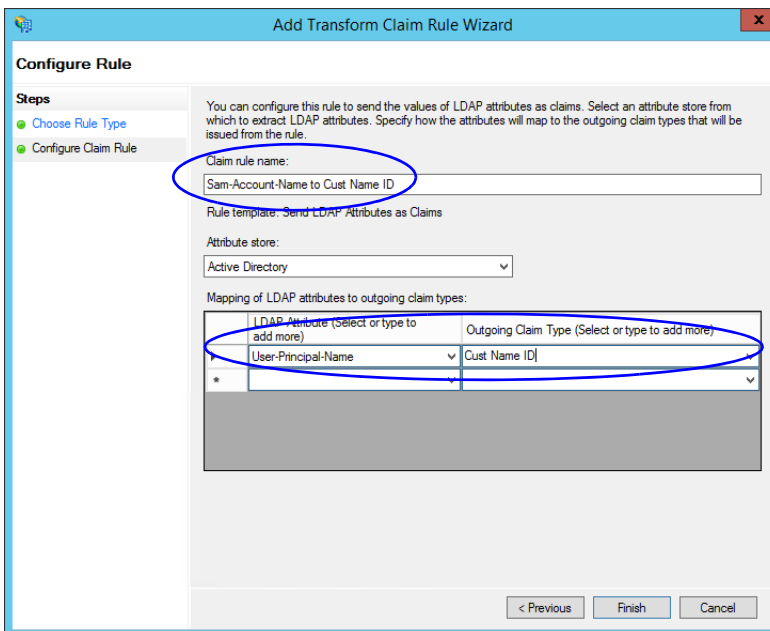
In the Add Transform Claim Rule wizard that opens, do the following:

- a. On the Choose Rule Type screen, from the **Claim rule template**, select **Send LDAP Attributes as Claims**. Click **Next**.



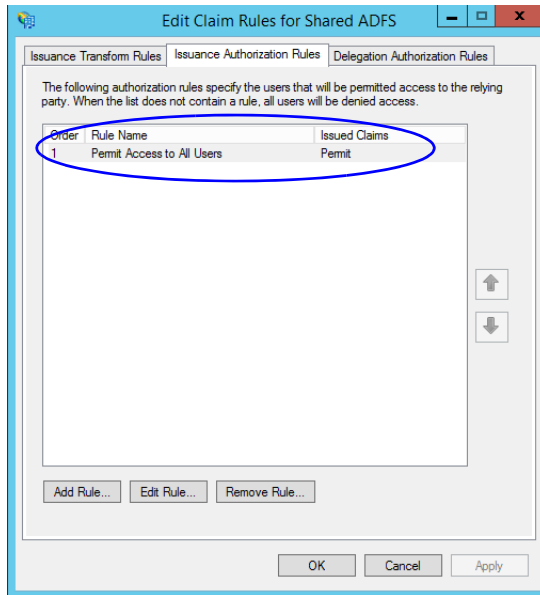
Select the claim rule template

- b. On the Configure Claim Rule screen, do the following:
 - i. Provide a claim rule name.
 - ii. Define mapping of LDAP attribute and the outgoing claim type. The outgoing claim type name must be unique across all the claims defined in all relying party trusts created on this AD FS server. Click **Finish** to go back to the Edit Claim Rules for Shared AD FS window.



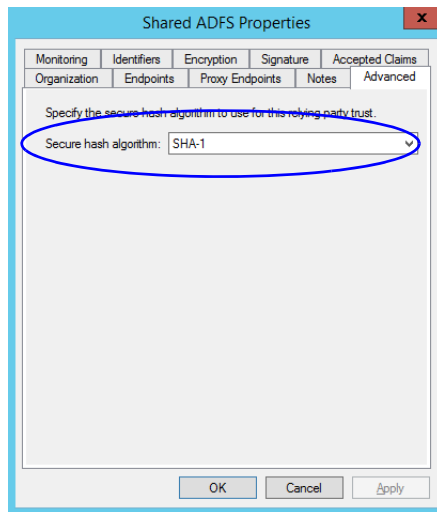
Configure the claim rule

10. In the Edit Claim Rules for Shared AD FS window, in the Issuance Authorization Rules tab, ensure that the rule permits access to all users. Click **OK** to close the window.



Check the authorization rules

11. In the Relying Party Trusts list, double-click the relying party trust which you created. In the Properties window that opens, go to the Advanced tab and set the **Secure hash algorithm** to **SHA-1**. Click **OK** to close the window.



Set the secure hash algorithm

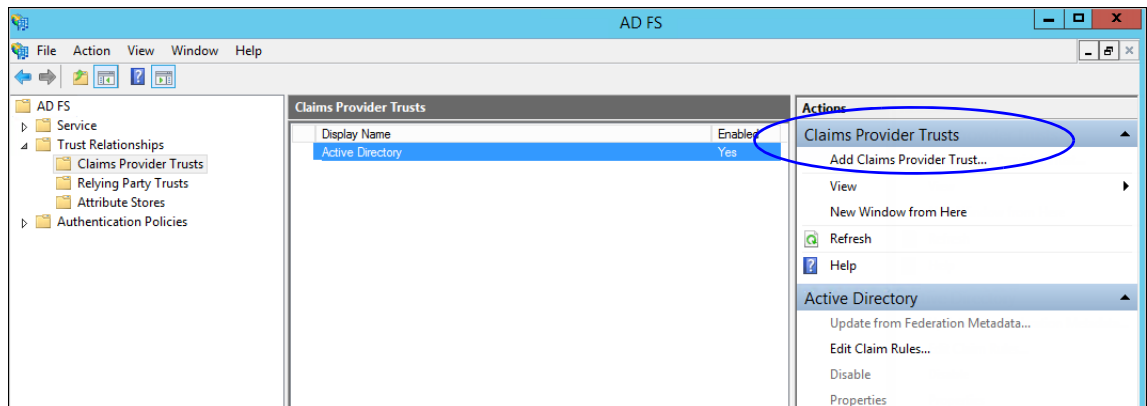
Configuring Claims Provider Trust for Customer AD FS in Shared AD FS

Perform these tasks on the server where shared AD FS is installed.

To configure claims provider trust for customer AD FS in shared AD FS:

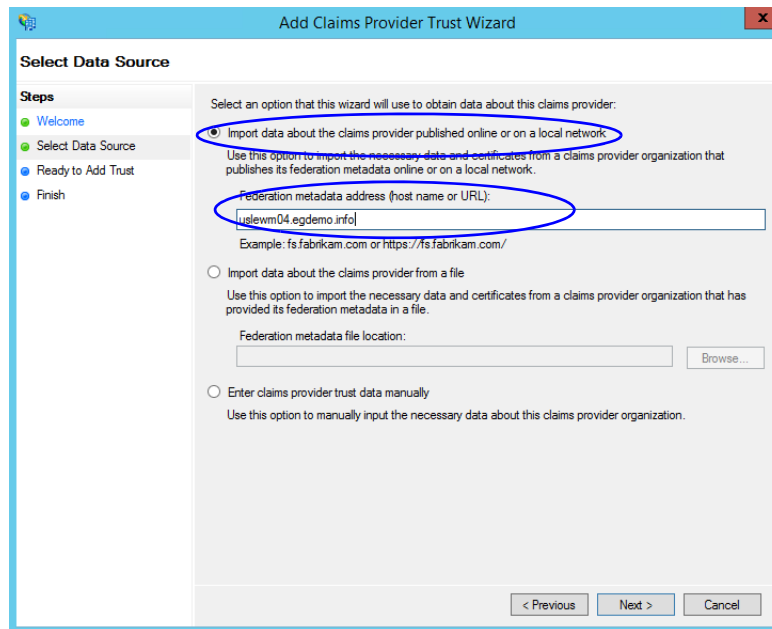
1. Go to the Start menu and open the AD FS Management console.

2. In the AD FS Management console, navigate to **AD FS > Trust Relationships > Claims Provider Trust**.
3. In the Actions section, go to Claim Provider Trusts, and click **Add Claims Provider Trust...**



Add claims provider trust

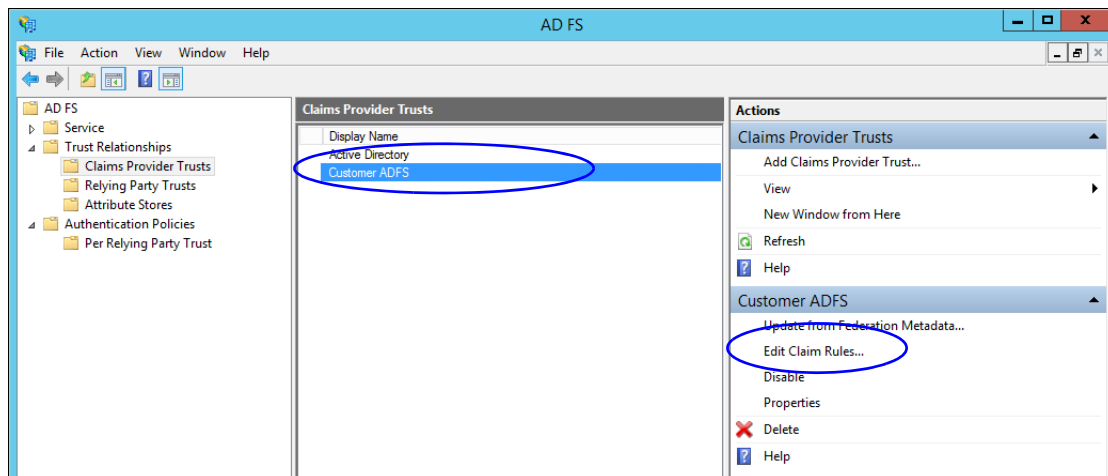
4. In the Add Claims Provider Trust Wizard that appears, do the following:
 - a. On the Select Data Source screen, set the following options:
 - i. Select the **Import data about the claims provider published on online or on a local network** option.
 - ii. In the **Federation metadata address** field, provide the Customer AD FS server name.
 - iii. Click **Next**.



Set the data source

- b. In the Specify Display Name screen, provide the **Display name**. Click **Next**.
- c. In the screens that follow, do not alter the default values. Continue to click the **Next** button in the wizard until a trust is created. At the end, an entry is created in the Claim Provider Trusts list.

5. In the Claim Provider Trusts list, select the Shared AD FS entry and click **Edit Claim Rules**.

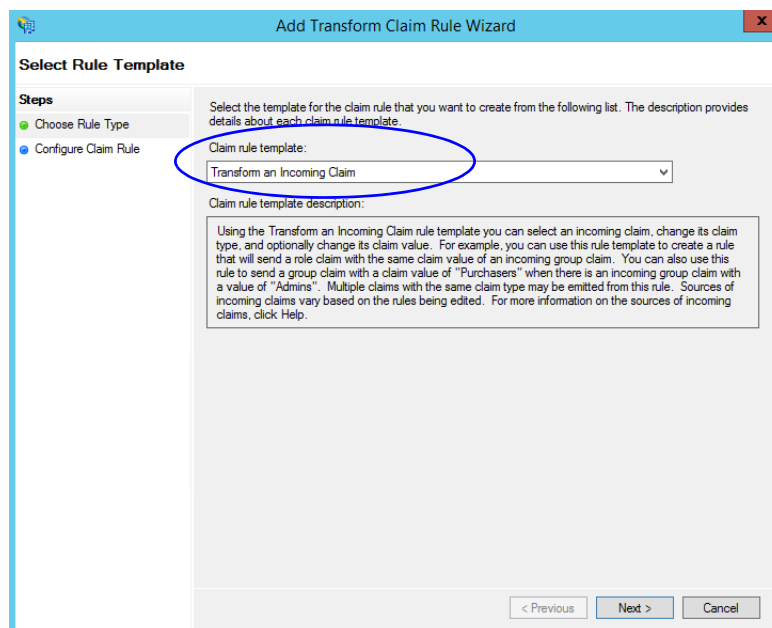


Edit the claim rules

6. In the Edit Claim Rules for Customer AD FS window, in the Acceptance Transform Rules tab, click the **Add Rule...** button.

In the Add Transform Claim Rule wizard that opens, do the following:

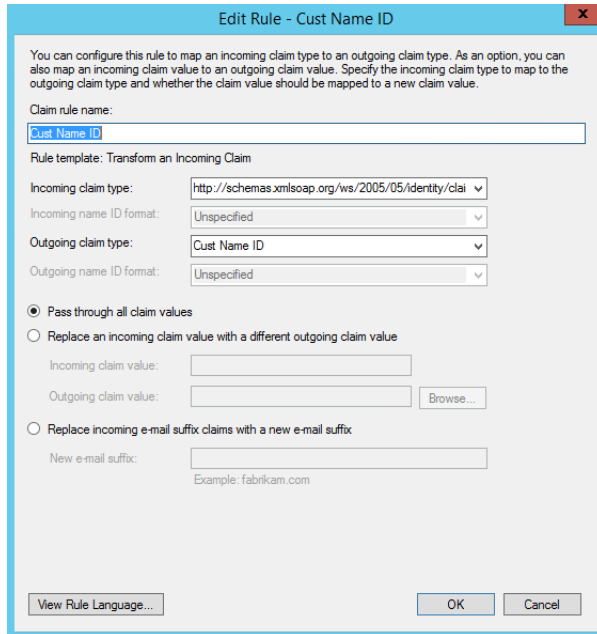
- a. On the Choose Rule Type screen, select **Transform an Incoming Claim** as the claim rule template. Click **Next**.



Choose the claim rule template

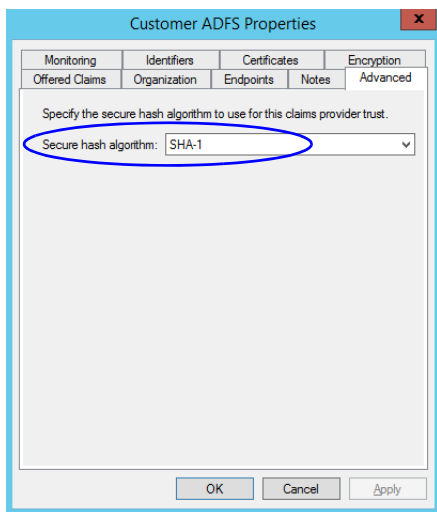
- b. On the Configure Claim Rule screen, set the following:
 - i. Provide the claim rule name as **Cust Name ID**.

- ii. In the **Incoming claim type** field provide the name as **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/CustNameID**. This is the same value as provided while creating the claim rule description (page 71).
- iii. Set the **Outgoing claim type** as **Cust Name ID**.
- iv. Select the **Pass through all claim values** option.



Configure the claim rule

- c. Click **Finish**. Claim is created and is displayed in the Edit Claim Rules for Customer AD FS window.
7. In the Claim Provider Trusts list, double-click the claim provider trust which you created. In the Properties window that opens, go to the Advanced tab and set the **Secure hash algorithm** to **SHA-1**. Click **OK** to close the window.



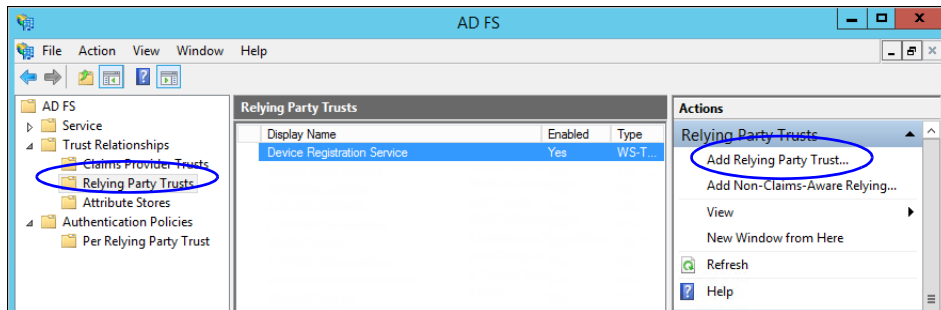
Set the secure hash algorithm

Configuring Relying Party Trust for ECE in Shared AD FS

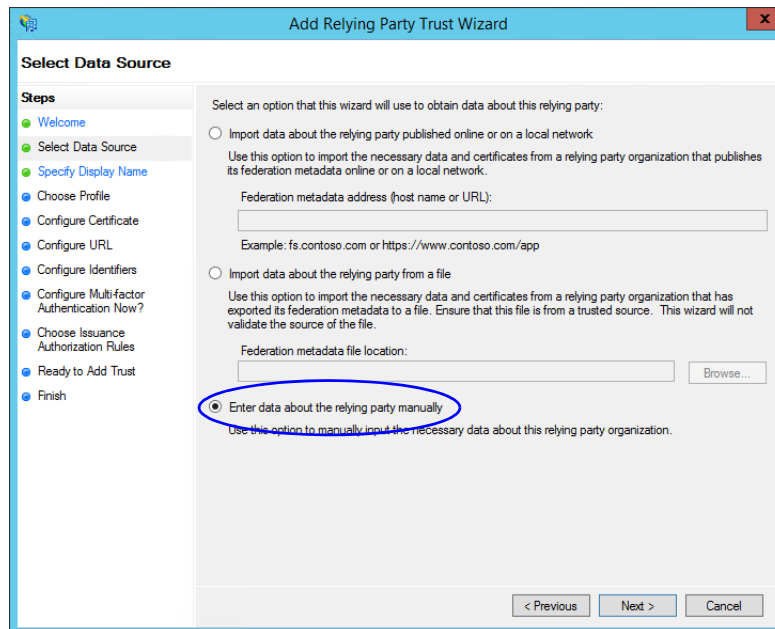
Perform these tasks on the server where shared AD FS is installed.

To configure relying party trust for ECE in shared AD FS:

1. Go to the Start menu and open AD FS Management console.
2. In the AD FS Management console, navigate to **AD FS > Trust Relationships > Relying Party Trust**.
3. In the Actions section, go to Relying Party Trust, and click **Add Relying Party Trust...**



4. In the Add Relying Party Trust Wizard that appears, do the following:
 - a. On the Welcome screen, click **Start**.
 - b. On the Select Data Source screen, select the **Enter data about the reply party manually** option and click **Next**.



Select the *Enter data about the reply party manually* option

- c. On the Specify Display Name screen, provide a **Display name** for the relying party. Click **Next**.

The screenshot shows the 'Specify Display Name' step of the 'Add Relying Party Trust Wizard'. The 'Display name' field is highlighted with a blue circle and contains the text 'v2w55 Console'. The 'Notes' field is empty. The 'Steps' list on the left includes: Welcome, Select Data Source, Specify Display Name (current), Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. Navigation buttons for '< Previous', 'Next >', and 'Cancel' are at the bottom.

Provide a display name

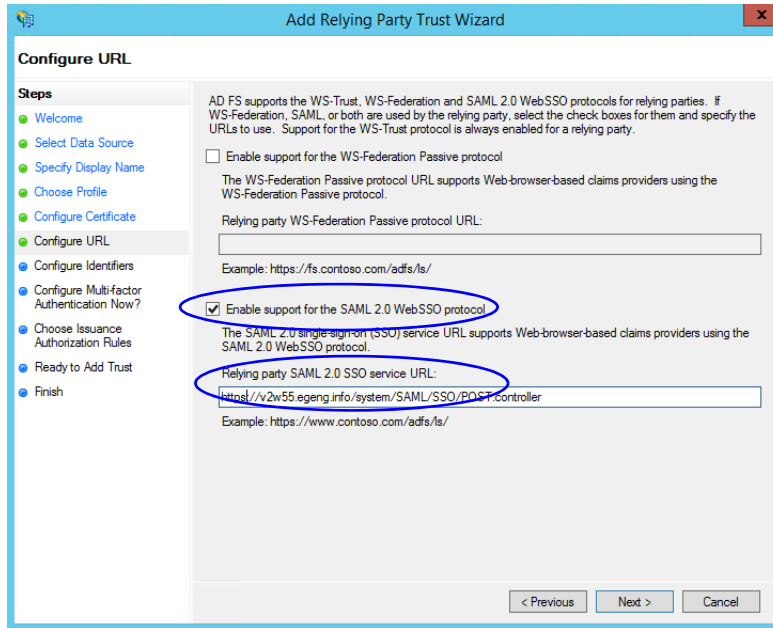
- d. On the Choose Profile screen, select **AD FS profile** and click **Next**.

The screenshot shows the 'Choose Profile' step of the 'Add Relying Party Trust Wizard'. The 'AD FS profile' radio button is selected and circled in blue. The 'AD FS 1.0 and 1.1 profile' radio button is unselected. The 'Steps' list on the left includes: Welcome, Select Data Source, Specify Display Name, Choose Profile (current), Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. Navigation buttons for '< Previous', 'Next >', and 'Cancel' are at the bottom.

Select AD FS profile

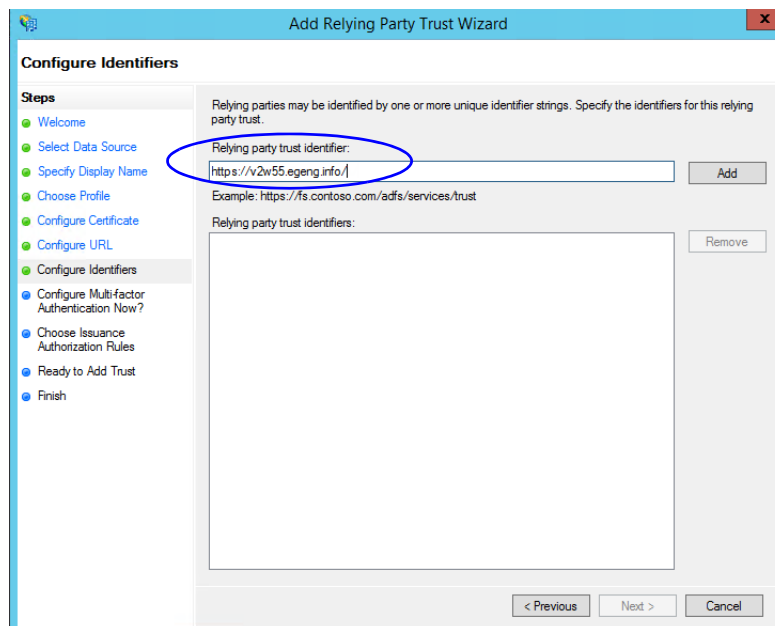
- e. On the configure Certificate screen, click **Next**.
- f. On the Configure URL screen, set the following:
- Select the **Enable support for the SAML 2.0 Web SSO protocol** option.

- ii. In the **Relying Party SAML 2.0 SSO server URL** field provide the URL in the format: `https://Web_Server_Or_Load_Balancer_Server/system/SAML/SSO/POST.controller`. Replace `Web_Server_Or_Load_Balancer_Server` with the ECE web server name or the Load balancer server name.



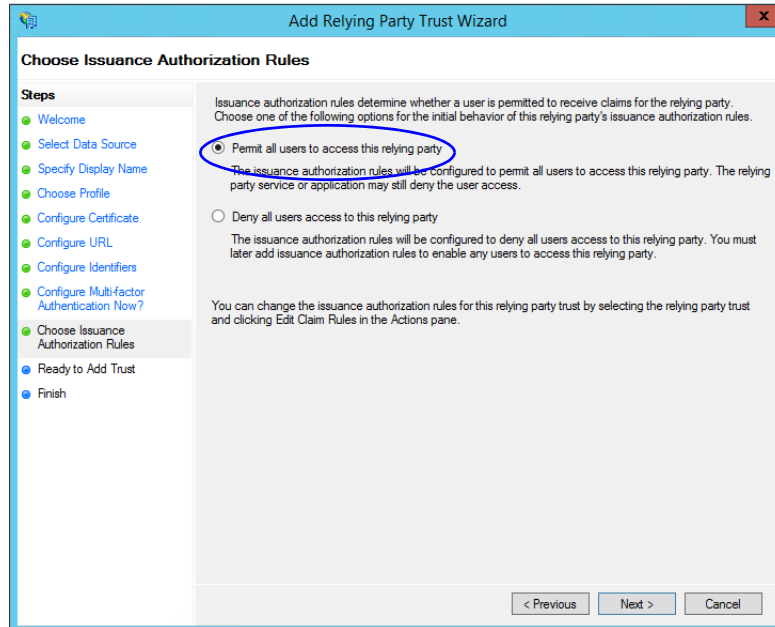
Configure the URL

- g. On the Configure Identifiers screen, provide the Relying party trust identifier and click **Add**. Value should be in the format: `https://Web_Server_Or_Load_Balancer_Server/`. Replace `Web_Server_Or_Load_Balancer_Server` with the ECE web server name or the Load balancer server name. Click **Next**.



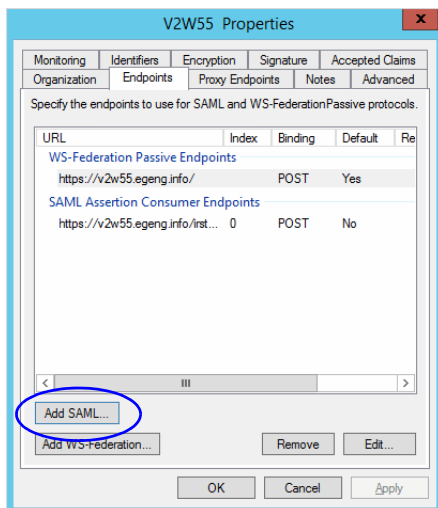
Configure the identifiers

- h. On the next screen, select the **I do not want to configure multi-factor authentication settings for the relying party trust at this time** option.
- i. On the Choose Issuance Authorization Rules screen, select the **Permit all users to access this relying party** option.



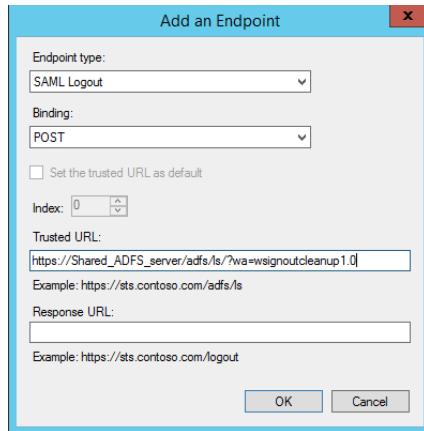
Select the *Permit all users to access this relying party* option

- j. On the Ready to add trust screen, click **Next**.
- k. Uncheck the **Open the Edit Claim Rules dialogue for this relying party trust when the wizard closes** option and click **Close**. At the end, an entry is created in the Relying Provider Trusts list.
5. In the Relying Provider Trusts list, select the trust created for ECE, and in the actions section click **Properties**.
6. In the Properties window, go to the Endpoints tab and click the **Add SAML..** button.



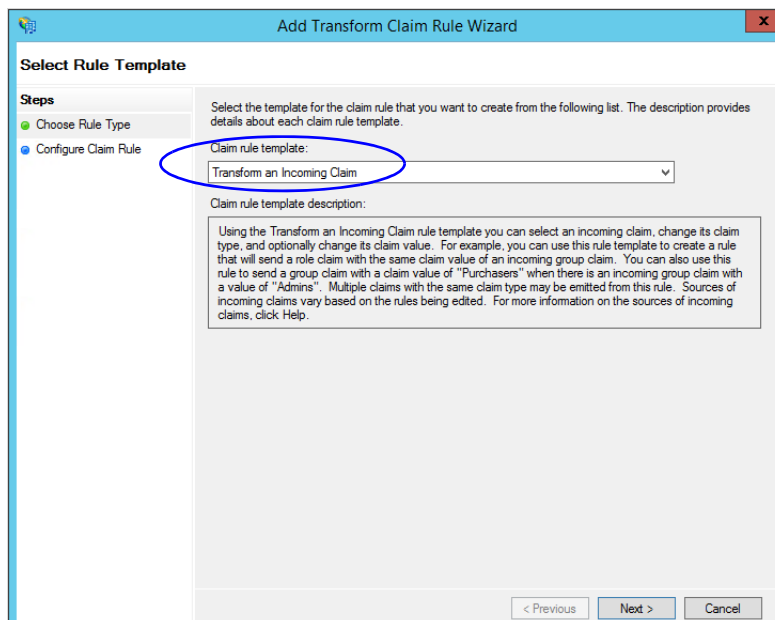
Click *Add SAML*

7. In the Add an Endpoint window, set the following:
 - a. Select the **Endpoint type** as **SAML Logout**.
 - b. Specify the **Trusted URL** as `https://Shared_ADFS_server/adfs/ls/?wa=wsignoutcleanup1.0`. Replace `shared_ADFS_server` with the Shared AD FS server name.
 - c. Click **OK**.



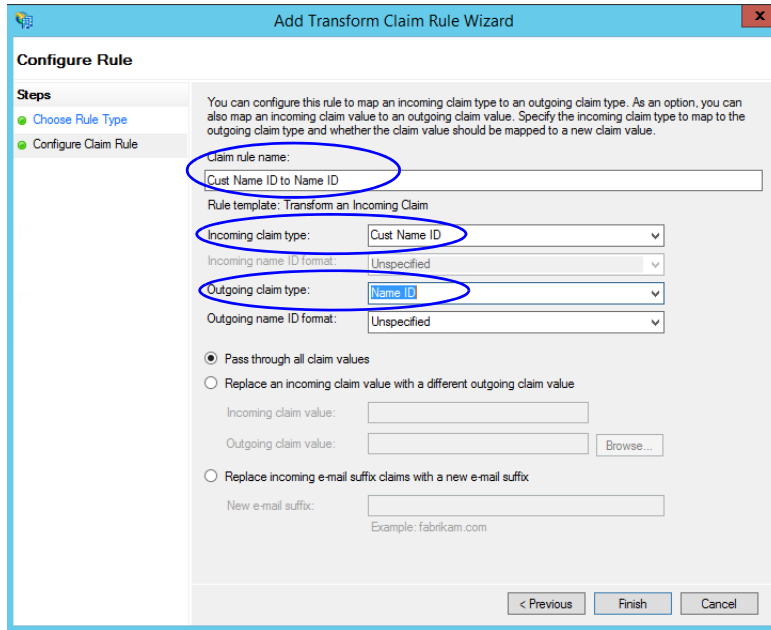
Create an end point

8. In the Relying Provider Trusts list, select the trust created for ECE, and in the actions section click **Edit Claim Rules**.
9. In the Edit Claim Rules window, in the Issuance Transform Rules tab, click the **Add Rule...** button. In the Add Transform Claim Rule wizard that opens, do the following:
 - a. On the Select Rule Template screen, from the **Claim rule template** dropdown, select **Transform an Incoming Claim**. Click **Next**.



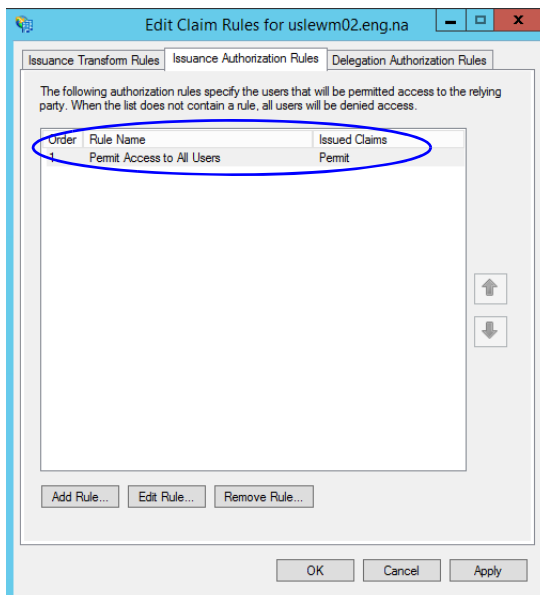
Select the claim rule template

- b. On the Configure Rule screen, set the following:
 - i. Provide the Claim rule name.
 - ii. In the **Incoming claim type** field provide the name of the outgoing claim specified in the Relying Party trust wizard (page 73).
 - iii. In the **Outgoing claim type** dropdown, select the **Name ID** option.



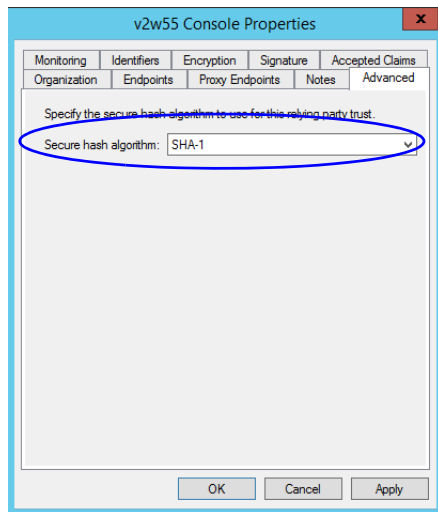
Configure the rule

- 10. In the Edit Claim Rules window, in the Issuance Authorization Rules tab, ensure that the rule permits access to all users. Click **OK** to close the window.



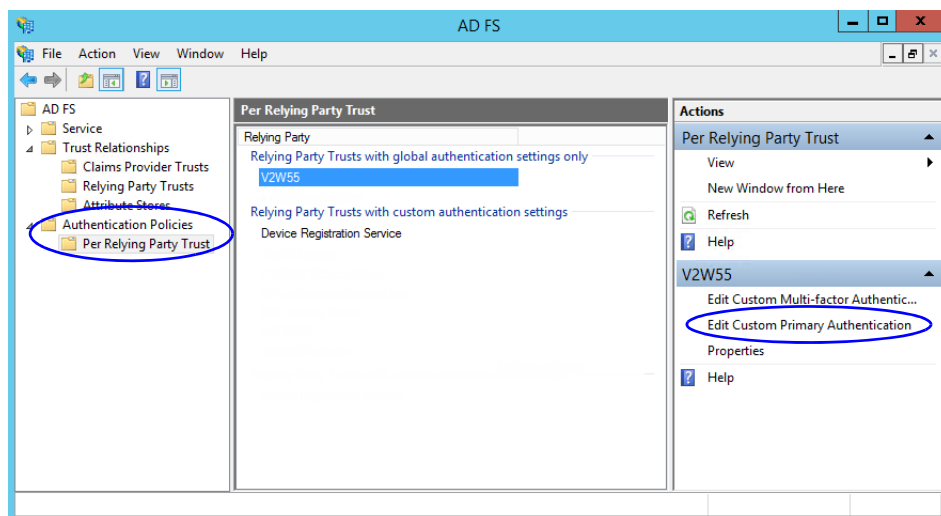
Check the authorization rules

11. In the Relying Provider Trusts list, double-click the relying party trust which you created. In the Properties window that opens, go to the Advanced tab and set the **Secure hash algorithm** to **SHA-1**. Click **OK** to close the window.



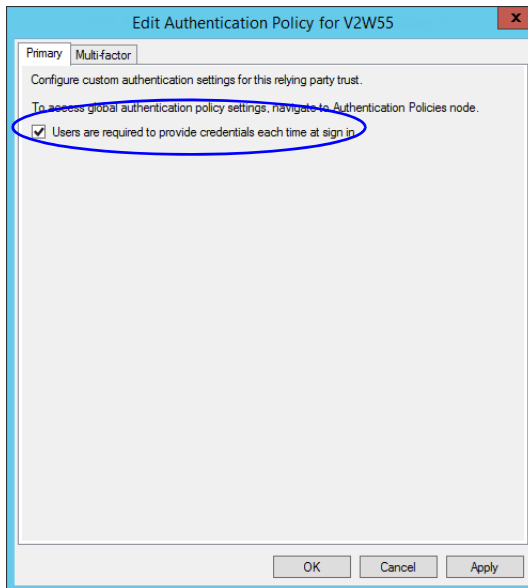
Set the secure hash algorithm

12. Next, in the AD FS Management console, go to the **Authentication Policy > Per Relying Party Trust**. Locate the Relying Party Trust created for ECE, and in the Actions section click **Edit Custom Primary Authentication**.



Change the authentication policy for ECE

13. In the Edit Authentication Policy window, in the Primary tab, select the **Users are required to provide credentials each time at sign in** option. Click **OK** to close the window.



Edit the authentication policy

Configuring Single Sign-On in ECE

- ▶ Follow instruction in the “Single Sign-On” chapter of the *Enterprise Chat and Email Administrator’s Guide to Administration Console* to complete the single sign-on configuration in ECE.

6 SSL Configuration

- ▶ [Installing a Security Certificate](#)
- ▶ [Binding the Certificate to the Application Website](#)
- ▶ [Testing SSL Access](#)
- ▶ [Configuring SSL or TLS for Retriever and Dispatcher Services](#)

Secure Sockets Layer (SSL) is widely used to create a secure communication channel between web browsers and servers. Set up SSL for more secure connections to your ECE installation by following the procedures described in this chapter.



Important: You must perform these tasks before using the application.

Installing a Security Certificate

This section explains the procedures that you must perform to acquire a certificate and install it on the web server. These include:

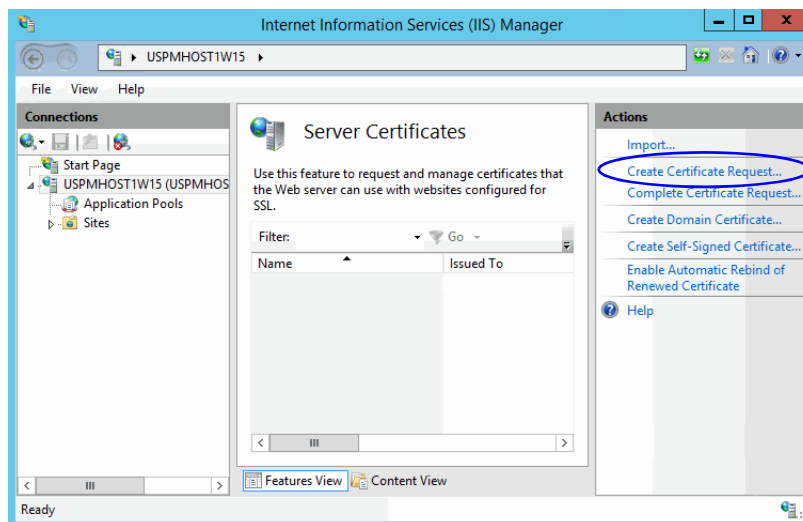
- ▶ [Generating a Certificate Signing Request](#)
- ▶ [Submitting the Certificate Request](#)
- ▶ [Installing the Certificate on the Web Server](#)

Generating a Certificate Signing Request

This procedure creates a new certificate request, which is then sent to a Certificate Authority (CA) for processing. If successful, the CA will send back a file containing a validated certificate.

To generate a certificate request:

1. Click the **Start** menu, go to **Control Panel > Administrative Tools**, and select **Internet Information Services (IIS) Manager**.
2. In the Connections pane, select the name of the server, and when the page is refreshed, double-click **Server Certificates**. The window is refreshed.
3. In the Actions pane on the right, click the **Create Certificate Request...** link.

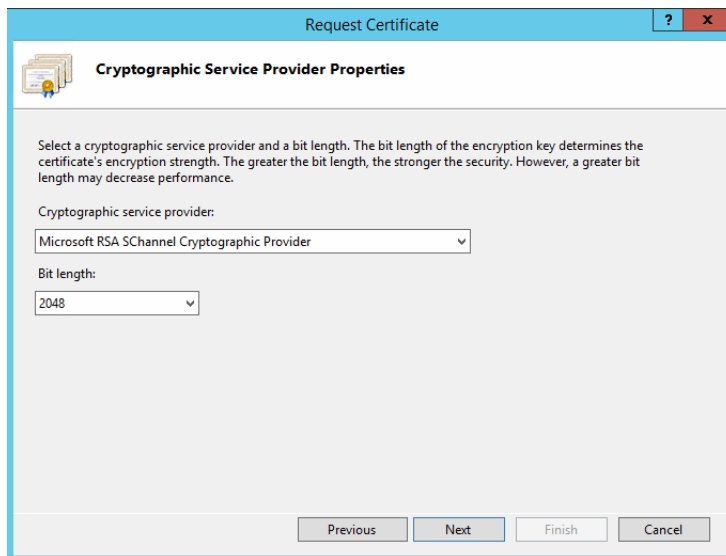


Click the *Create Certificate Request* link

4. In the Distinguished Name Properties window, enter information about the company and the site to be secured:
 - **Common Name:** The fully qualified domain name (FQDN) of your server. This must match exactly what users type in the web browser to get to the application.
 - **Organization:** The legal name of your organization. This should not be abbreviated and should include suffixes such as Inc, Corp, or LLC.
 - **Organizational Unit:** The division of your organization handling the certificate.
 - **City/locality:** The city where your organization is located.
 - **State/province:** The complete name of the state or region where your organization is located.
 - **Country/region:** The two-letter ISO code for the country where your organization is located.

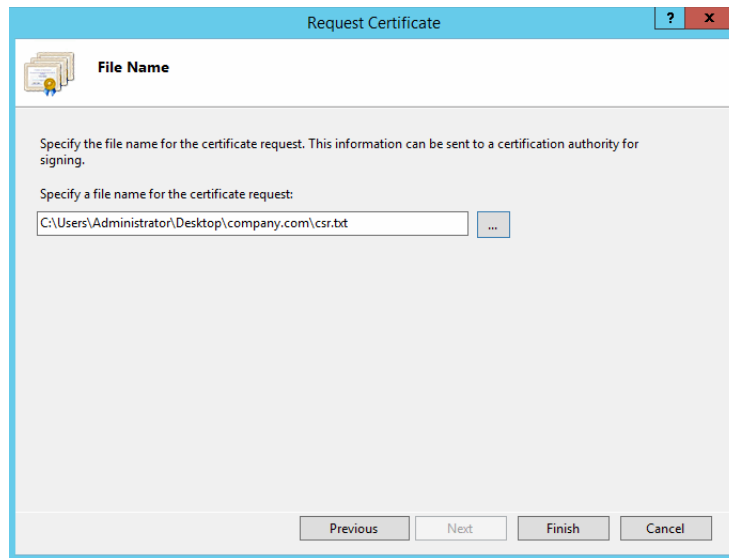
Click **Next**.

5. In the Cryptographic Service Provider window, select a cryptographic service provider and set the required bit length. The greater the bit length, the stronger the security. Click **Next**.



Select a cryptographic service provider and bit length

6. In the File Name window, click the **Assistance ...** button and browse to the location where you wish to save the certificate signing request file. Ensure that you enter a file name for the certificate signing request file. Click **Finish**.



Enter the location and file name

Once you have generated a certificate signing request, you can submit the certificate request to a certificate authority.

Submitting the Certificate Request

To submit the certificate request:

- ▶ Go to the website of the company that issues SSL certificates (such as VeriSign), and submit your certificate request. Make sure you provide the same information as you provided while generating the certificate signing request. To submit the request, you will need the certificate request file that you generated ([page 87](#)).

Once the request is processed, the vendor will generate the certificate and send it to you.

Installing the Certificate on the Web Server

Once you receive the certificate from your vendor, install it on the web server.

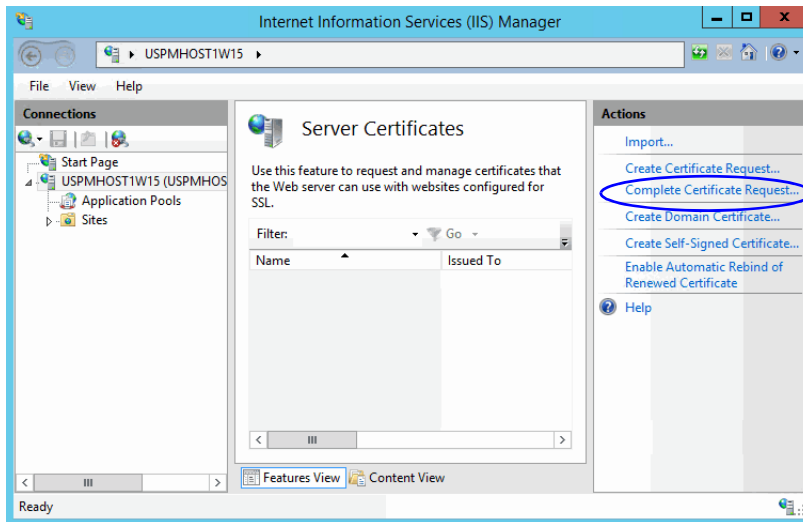


Important: You need to install the certificate for the website that was specified when the web server component was installed.

To install the certificate on the web server:

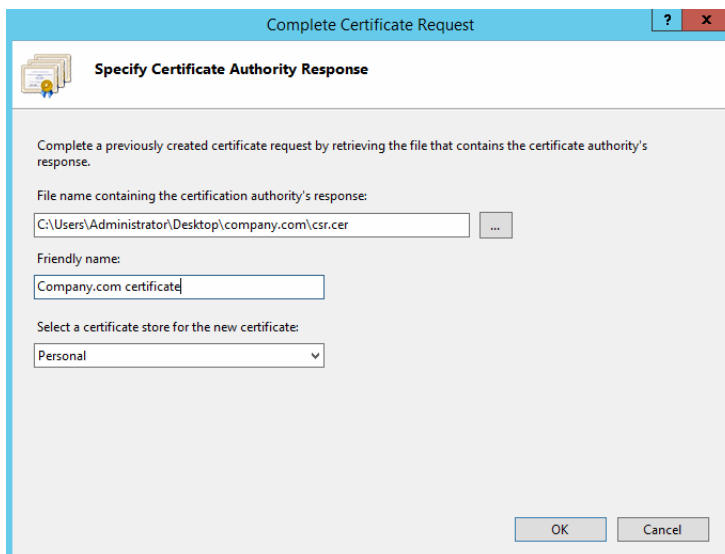
1. Click the **Start** menu, go to **Administrative Tools**, and select **Internet Information Services (IIS) Manager**.
2. In the Connections pane, select the name of the server, and when the page is refreshed, double-click **Server Certificates**. The window is refreshed.

3. In the Actions pane on the right, click the **Complete Certificate Request...** link.



Click the *Complete Certificate Request* link

4. In the Specify Certificate Authority Response window, complete these tasks:
 - Click the **Assistance ...** button and select the server certificate that you received from the certificate authority. If the certificate doesn't have a .cer file extension, select to view all types.
 - Enter a name for the certificate. Click **OK**.



Browse to the server certificate file

5. Verify that the certificate is added to the list of server certificates.

Binding the Certificate to the Application Website

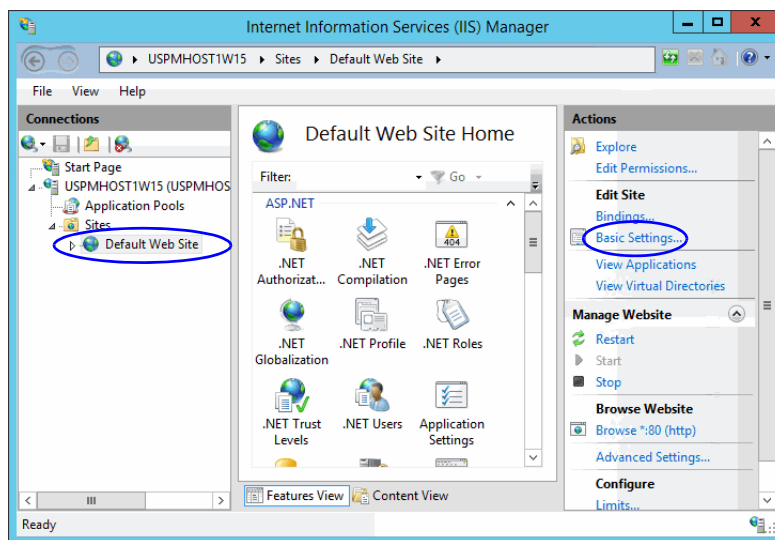
This procedure uses Internet Services Manager to configure the virtual directory to require SSL for access to the application URL.



Important: You need to configure the SSL access for the website that was selected when the web server component was selected.

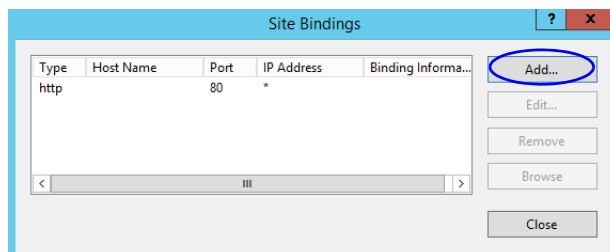
To bind the certificate to the application URL:

1. Click the **Start** menu, go to **Administrative Tools**, and select **Internet Information Services (IIS) Manager**.
2. In the Connections pane, select the name of the server and browse to **Sites** > *Web_Site_Name*.



Select the *Web_Site_Name*.

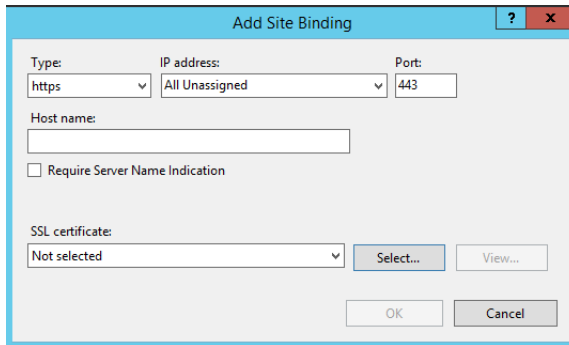
3. In the Actions pane on the right, from the Edit Site section, click the **Bindings...** link.
4. In the Site Bindings window, click the **Add...** button.



Click the **Add** button

5. In the Add Site Bindings window, complete these tasks:
 - **Type:** Select **https**.
 - **IP address:** Select **All Unassigned**.
 - **Port:** Default value is 443. If IIS is configured to use a different port for https, enter that port number.

- **SSL certificate:** Select the certificate that you installed. Click **OK**.



Select SSL certificate

6. The site binding for port 443 is displayed.
7. Restart the IIS Service. Make sure that both websites have started.
Clients browsing to this virtual directory must now use HTTPS.

Testing SSL Access

To test SSL access to ECE:

1. Open your web browser.
2. Use HTTP in the URL for the application. For example, `http://Web_server_FQDN/Partition_name`
You should see a message asking you to view the page over a secure channel.
3. Now use HTTPS in the URL for the application. For example, `https://Web_Server_FQDN/Partition_name`.
4. In the security message that appears, click the **View certificate** button.
5. After verifying the certificate information, click **OK**, then click **Yes** to proceed to the URL.
The ECE login window appears.

Configuring SSL or TLS for Retriever and Dispatcher Services



Important: This feature is available after you upgrade to ECE 11.6.

You need to perform these tasks only if you want to enable the retriever and dispatcher services to work with SSL or TLS enabled mail servers. POP3, IMAP, SMTP, and ESMTP protocols are supported.

To configure TLS and SSL, you must:

- Install the certificates on the services servers. (page 93)
- a. Modify the alias configuration (page 94)

On the Services Server

If your POP3, IMAP, SMTP, and ESMTP servers are installed on different machines, obtain the certificates for all the servers and install them on the services servers.

Installing Certificates

To configure SSL or TLS on the services server:

1. Obtain the certificate for the SSL or TLS enabled mail server on which the email alias is configured. If your POP3, IMAP, SMTP, and ESMTP servers are installed on different machines, obtain the certificates for all the servers.
2. Copy the certificates to a location in *Cisco_Home*.
3. Open the Command window and navigate to the `bin` folder in the `jre` folder in *JDK_Home*, the installation folder for JDK. For example, the command will look like:

```
cd C:\InstallFolder\Java\jdk1.8.0_60\jre\bin
```

4. Execute the following command to install the certificate:

```
keytool -import -trustcacerts -alias ALIAS_NAME -keystore  
"..\lib\security\cacerts" -file "CERTIFICATE_FILE_PATH"
```

where:

CERTIFICATE_FILE_PATH is the complete path to the certificate that you copied in [Step 2](#), including the name of the file.

Alias_Name is any name you want to assign to the certificate.

For example the command will look like:

```
keytool -import -trustcacerts -alias emailcertificate -keystore  
"..\lib\security\cacerts" -file "D:\eG\ms_exchange_certificate.cer"
```

5. When prompted, provide the keystore password. If you had changed the keystore password earlier, provide that password. If not, provide the default password, **changeit**.
6. Confirm the action when prompted.
7. To verify that the certificate is installed successfully, run the following command:

```
keytool -list -v -keystore "..\lib\security\cacerts" -alias ALIAS_NAME
```

where *Alias_Name* is the name you assigned to the certificate in [Step 4](#).

For example, the command will look like:

```
keytool -list -v -keystore "..\lib\security\cacerts" -alias emailcertificate
```

8. When prompted, provide the keystore password.

The output will list the installed certificate.

Deleting Certificates

Certificates generally have an expiry date. When your certificate expires, you might need to delete the old certificates and install new ones. The following section describes the steps for deleting the certificates. After deleting the certificates, repeat the steps in [“Installing Certificates” on page 93](#) to install new certificates.

To delete a certificate:

1. Open the Command window and navigate to the `bin` folder in the `jre` folder in `JDK_Home`, the installation folder for JDK. For example, the command will look like:

```
cd C:\InstallFolder\Java\jdk1.8_65\jre\bin
```

2. Execute the following command to delete the certificate:

```
keytool -delete -alias ALIAS_NAME -keystore "..\lib\security\cacerts"
```

where:

Alias_Name is the name you assigned to the certificate in [Step 4](#).

For example the command will look like:

```
keytool -delete -alias emailcertificate -keystore "..\lib\security\cacerts"
```

3. When prompted, provide the keystore password. If you had changed the keystore password earlier, provide that password. If not, provide the default password, `changeit`.

In the Administration Console



Important: These options in the Administration Console are available in systems upgraded to ECE 11.6.

To enable SSL for specific aliases:

1. Log into the application as an administrator who can modify the email alias configuration and go to the Administration Console.
2. In the Tree pane, browse to **Administration** > **Departments** > *Department_Name* > **Email** > **Aliases**.
3. In the List pane, select the appropriate email alias.
4. In the Properties pane, go to the Servers tab and edit the following fields.
 - **Connection type:** Set this to **SSL** or **TLS**.
 - **Port:** Enter the secure port number.

Properties: Marketing

General Servers

	Name	Value
Incoming	Server type	POP3
Outgoing	Server name *	EMS2K
	User name *	user@company
	Password *	*****
	Verify password *	*****
	Connection type	SSL
	Port *	995
	Folder *	inbox

Configure the alias properties

5. Repeat these steps for the Outgoing mail server, if required.
6. Save the changes.