Enterprise Chat and Email Installation and Configuration Guide, Release 15.0(1)

For Packaged Contact Center Enterprise

First Published: April, 2025
Last Updated: November, 2025

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
https://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 https://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 10, 2025

Copyright © 2016–2025, Cisco Systems, Inc. All rights reserved.

Contents

Preface **10**

About This Guide 11
Change History 11
Related Documents 12
Communications, Services, and Additional Information 12
Cisco Bug Search Tool 12
Field Alerts and Field Notices 12
Documentation Feedback 13
Document Conventions 13

Chapter 1: Planning **14**

Identifying Components 15
File Server Component 15
Database Server Component 15
Messaging Server Component 15
Application Server Component 16
Web Server Component 16
Services Server Component 17
Understanding Deployment Models for ECE 17
Collocated Deployment for ECE 17
Distributed-Server Deployment 17
Planning Components for Specific Configurations and High Availability 18
Disabling the TCP IP Offload Settings 18
Planning the File Server 19
Planning the Database Server 19
Installing the Application on a SQL Server 2022 Cluster 19
Planning Database Server Distribution 19
Planning Messaging Servers 19
Planning Services Servers 20
Planning Application Servers 20
Planning Web Servers 20
Load Balancing Considerations 20
Load Balancer Configuration Examples 21

Planning for High Availability Across Geographies. 23
For Collocated Deployments. 24
For Fully Distributed Deployments. 25
Installing ECE. 26

Chapter 2: Pre-Installation Tasks 27

Preparing Virtual Machine 28
Obtain Installation Media 28
Download OVA for ECE 28
Create Virtual Machines from the OVA 28
Install Microsoft Windows Server 28
Install VMware Tools 28
Mounting and Unmounting ISO Files. 29
Verifying Signature File for ISO. 29
Disabling Loopback Adapter Configuration. 30
Verifying Network Configuration. 30
Configuring Port Numbers Between Components 31
Setting Up User Accounts and Permissions 33
Setting Up Domain Account 34
Configuring Permissions on Active Directory Server. 34
Changing the Service Account Password 37
Changing the Password 37
Setting up Distributed File System (DFS) 38
Preparing Database Server VMs 38
Install Microsoft SQL Server 38
Verifying Microsoft SQL Server Features 38
Verifying Collation Settings 39
Choosing Authentication Method for Database Connectivity. 39
Setting up for Always On Availability Group Clustering. 39
Installing SQL Server Management Studio (SSMS). 39
Creating SQL User for Installing ECE Databases 40
Assigning Permissions to Domain User 40
Configuring Database Servers. 40
Configuring Memory Settings. 40
Configuring Microsoft DTC Settings 41
Running Services. 42

Preparing Web Server VMs 44
Configuring Roles and Features 44
Installing Modules on Web Servers 45
Configuring Permissions on IIS Config Folder. 45
Running the World Wide Web Publishing Service. 45
Configuring Virus Scanners 45
Configuring SMTP Port in Virus Scanners. 45
Configuring Virus Scanning Exclusions 46
Verifying Packaged CCE Configuration. 46

Chapter 3: Prepare Packaged CCE for the Integration 48

Relationship Between Objects in Packaged CCE and ECE 49
Adding ECE to Packaged CCE Inventory 49
For 2000 Agent Deployments 49
For 4000 & 12000 Agent Deployments 50
Configuring Packaged CCE 50
Configuring Call Types. 52
Configuring Application Path 52
Configuring Agents. 53
Configuring Skill Groups 54
Configuring Dialed Number 55
Creating Scripts. 55
Configuring Precision Routing 60
Creating Attributes 60
Assigning Attributes to Agents 61
Creating Precision Queues 61
Adding Precision Queue Node to the Scripts 61
Adding MR PIM for ECE. 62
Adding Agent PG PIM for ECE 63
Adding CTI for ECE. 63
Configuring Finesse 64

Chapter 4: Installation Process 65

Installation Overview 66
For 400 Agent Deployments 66
For 400 Agent Deployments (HA) 67

For 401-1500 Agent Deployments 67
For 401-1500 Agent Deployments (HA) 67
For 401-2500 Agent Deployments 68
For 401-2500 Agent Deployments (HA) 68
Installing ECE 69
Installation Details 71
File Server Details 71
Database Server Details 72
Web Server Details 77
Messaging Server Details 79
Application Server Details 80
Services Server Details 81

Chapter 5: Post-Installation Tasks 82

Configuring Permissions on IIS Config Folder 84
Assigning Permissions on ECE Home Directory 84
Configuring SSL for Secure Connections 84
Always On Availability Group Clustering Tasks 84
Creating an Encrypted SQL Server Database 85
Encrypting Primary Node 85
Encrypting Other Nodes 86
Configuring SMTP Server Relay Address List 87
Configuring Finesse 88
Configuring Finesse Files 88
Configuring Finesse Settings and Layout 88
For 4000 and 12000 Agent Deployments 88
For 2000 Agent Deployments 89
Configuring Single Sign-On 90
Starting ECE 91
Troubleshooting Application Start-Up Issues 91
Stopping ECE 92
Signing in to ECE 92
Signing in to Agent Console 92
Signing in to All Other Consoles 93
Integrating ECE with Packaged CCE 93

Configuring Important Settings 94
Mandatory Settings 94
Optional Settings 95
Configuring Clickjacking Protection 96
About Clickjacking Protection 96
Configuring Clickjacking Protection 96
Adding Data Source in CUIC for ECE Reports 96
Creating a Database User on ECE Reports Database 97
Adding Data Source in CUIC for ECE Reports 98
Uninstalling ECE 98
Preparing to Uninstall 98
Stopping the Application 98
Stopping IIS 99
Uninstalling ECE 99
Performing Post Uninstallation Tasks 99
Starting IIS 99

Chapter 6: Single Sign-On Configuration 100

About Single Sign-On with Cisco IDS 101
Configuring Single AD FS Deployment 101
Configuring Relying Party Trust for ECE 101
Configuring Split AD FS Deployment 109
Adding Security Certificates for the AD FS Domains 109
Configuring Relying Party Trust for Shared AD FS in Customer AD FS 110
Configuring Claims Provider Trust for Customer AD FS in Shared AD FS 114
Configuring Relying Party Trust for ECE in Shared AD FS 118
Configuring Single Sign-On in ECE 125

Chapter 7: SSL Configuration 126

Installing a Security Certificate 127
Generating a Certificate Signing Request 127
Submitting the Certificate Request 129
Installing the Certificate on the Web Server 129
Binding the Certificate to the Application Website 131
Testing SSL Access 132

Configuring SSL or TLS for Retriever and Dispatcher Services 133
On the File Server 133
Installing Certificates. 133
Deleting Certificates 134
Enable SSL for Specific Email Aliases. 134

Appendix A: Distributed File System Configuration 135

Installing DFS Management 136
Creating Shared Folders 136
Creating New Namespace. 136
Adding Namespace Server 137
Adding Folders and Configuring Replication. 138
For Two Server Installations. 138
Creating Folders on Side B 138
Adding Folders 138
For Distributed Server Installations 139

Appendix B: SQL Always-On Configuration 141

About Always On Availability Group Clustering. 142
Pre-Installation Tasks 142
Installing Failover Clustering Feature. 142
Creating Prestage Cluster Computer Objects in Active Directory Domain Services (AD DS) 142
Prestaging the CNO in AD DS 143
Granting User Permissions to Create Cluster 143
Granting the CNO Permissions to the OU 143
Creating Windows Failover Cluster 144
Configuring Permissions for the File Share Witness Folder. 144
Configure Cluster Quorum Settings 145
Verifying Cluster Settings. 145
Enabling Always On Availability Groups Feature on SQL 146
Configuring SQL Server Always On Availability Groups 146
Additional Configuration for Multi-subnet Availability Group 147
Install the Application. 148
Post-Installation Tasks 148
Verifying Recovery Model 148
Backing up ECE Databases. 148

Adding Databases to Availability Group 148
Run reports DB utility to configure secondary nodes 149
Running the Reports Database Utility 149
Run the UpdateDBIndexStats Utility 150
Running the UpdateDBIndexStats Utility 150
Creating Jobs to Take Log backups on All Nodes 151

Appendix C: Convert Existing Deployment to HA 152

Converting Existing Two Server Installation to HA 153
Converting Existing File Server to DFS 154
Setting up Distributed File System (DFS) 154
Installing Second Messaging, Services, and Application Server Components 154
Installing Second Web Server Component 154
Converting Databases to SQL Server to Always On Configuration 154
Stopping ECE Application and Disable SQL Jobs 155
Converting SQL Authentication to Windows Authentication 155
Backing up and Restoring Databases 156
Updating Files and Databases with New Listener Names 156
Starting the SQL Jobs and ECE Application 157
Updating Finesse Files 157
Converting Existing Distributed Server Installation to HA 157
Converting Existing File Server to DFS 158
Setting up Distributed File System (DFS) 158
Updating Files to Use DFS 158
Converting Databases to SQL Server Always On Configuration 158
Installing Second Messaging Server Component 159
Installing Second Services Server Component 159
Installing Additional Application Server Components 159
Installing Additional Web Server Components 159

Appendix D: Enhancements in ECE 15 161

Inter-component SSL Enabled by Default 162
Automated SSL Certificate Rotation 162
Centralized Log Collection for HA and Distributed Deployments 162

Preface

- About This Guide
- Change History
- Related Documents
- Communications, Services, and Additional Information
- Field Alerts and Field Notices
- Documentation Feedback
- Document Conventions

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 Packaged 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.

About This Guide

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 configuring 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.

Change History

This table lists changes made to this guide. Most recent changes appear at the top.

Change	See	Date
▶ Removed server features not supported by SQL 2022	"Verifying Microsoft SQL Server Features" on page 38	November, 2025
▶ Updated the step for obtaining the Active_DATBASE_URL.	"Running the UpdateDBIndex-Stats Utility" on page 150	
▶ Removed an obsolete step for converting SQL authentication to Windows authentication.	"Converting SQL Authentication to Windows Authentication" on page 155	
▶ Added information about setting connection timeout on loadbalancer	"Load Balancing Consider-ations" on page 20	August, 2025

Related Documents

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

Subject	Link
Complete documentation for Enterprise Chat and Email, for both Cisco Unified Contact Center Enterprise (UCCE) and Cisco Packaged Contact Center Enterprise (PCCE)	https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/tsd-products-support-series-home.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Field Alerts and Field Notices

Cisco can modify its products or determine key processes to be important. These changes 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.

Sign in www.cisco.com and then access the tool at https://www.cisco.com/c/en/us/support/web/tools-catalog.html.

Documentation Feedback

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

We appreciate your comments.

Document Conventions

This guide uses the following typographical conventions.

Convention	Indicates
Italic	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.
Variable	User-specific text; varies from one user or installation to another.

Document conventions

1 Planning

- Identifying Components
- Understanding Deployment Models for ECE
- Planning Components for Specific Configurations and High Availability
- Installing ECE

ECE can be installed in multiple configurations, ranging from a simple collocated installation, to many flavors of distributed installations. This chapter lists the components that make up ECE deployment and available configuration options. It also helps you plan your installation.

Identifying Components

All ECE installations have the following six components:

- File Server Component
- Database Server Component
- Messaging Server Component
- Application Server Component
- Web Server Component
- Services Server Component

File Server Component

The file server is used to store application files, reports templates, and reports output files. In non HA environment, there is only one file server in a deployment. HA deployments use DFS.

Database Server Component

All ECE databases are created on the database server. The installation program creates the following databases:

- A master database, that stores system configuration information to manage services.
- An active database, where all business and interaction data is stored. This is also referred to as the partition database.
- A reports database, where all data used by the reports module is stored.

The master and active databases are installed on the same instance. The reports database can be installed on a different instance.

Messaging Server Component

The messaging server provides a centralized location for the exchange of information asynchronously among various components of ECE application through the sending and receiving of messages.

For example,

- The application server publishes a message to the workflow cache process to refresh its cache when a user modifies a workflow in the Administration Console.

A deployment can have a cluster of messaging servers.

Components that use messaging are listed in the following table.

Component	Use
Email Workflow	▸ The Workflow Assignment Service publishes a message to application servers when a new email is assigned to a user. ▸ The application server publishes a message to Workflow Cache Service when any workflow is created or modified from the Administration Console. The Workflow Cache Service publishes a message to the Workflow Service after it rebuilds its cache.
Email Retriever and Dispatcher	The application server publishes a message to the Retriever and Dispatcher Services when an email alias is created or modified from the Administration Console.
Miscellaneous	▸ The Scheduler Service publishes a message to the Reports Service when the schedule for a report fires. ▸ The application server publishes a message to the Distributed Services Manager (DSM) whenever an agent logs in to or logs out of the application. ▸ The application server publishes a message to all other application servers and services when a Custom attribute is created from the Tools Console. ▸ The application server publishes a message to other application servers every time an article or topic is added, modified, or removed.

Application Server Component

The application server houses the business logic responsible for interactive responses to all user-interface requests–across all classes of users including customers, agents, administrators, knowledge authors, system administrators. It handles requests for operations from a user (the web client), interprets user requests and delivers responses as web pages, constructed dynamically using JSP (based on the user request).

A deployment can have more than one application server. The number of application servers in a deployment will depend on the amount of user load to be handled. For details about sizing, see the *Enterprise Chat and Email Design Guide*.

Web Server Component

The web server is used to serve static content to the browser.

It gets requests from, and serves static content such as images, java applets, and client-side JavaScript code to a web browser. All dynamic requests are routed to the application server for further processing and generation of dynamic content. The web server component is always installed on a separate VM.

Installing the web server does not need access to any other ECE component. The web server can be installed outside firewall. A deployment can have multiple web servers, with a one-to-one mapping between a web server and an application server. The web servers can be separated from their corresponding application servers across a firewall.

No user identification is required at the web server. Access to the application functionality is controlled at the application server layer.

Services Server Component

ECE has processes that perform specific business functions, such as fetching emails from a POP3 or IMAP server, sending emails through an SMTP server, processing workflows, assigning chats to agents, etc. All services run on the services server and are managed by the Distributed Service Manager (DSM). Framework services that manage these remote services also run on the services server.

A deployment can have two services servers.

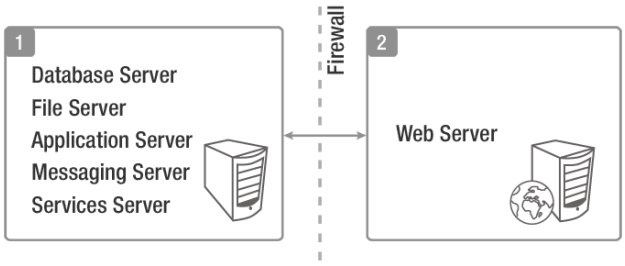
Understanding Deployment Models for ECE

With its modular, component-based architecture ECE caters effortlessly to the growing demands for increased concurrent user loads. To provide the flexibility to suit deployments of varied sizes, ECE supports components that may be distributed across various servers in a deployment. This section provides details of the possible deployment options.

- **Collocated Deployment for ECE:** The web server is installed on a separate VM and all other components are installed on one VM. The web server may be installed outside the firewall, if required.
- **Distributed-server deployment:** Components are distributed over two or more servers. A wide range of options are available for distributed-server deployment. The database is usually installed on a dedicated server, and the other components are installed on a separate server or spread over two or more servers.

Collocated Deployment for ECE

The web server is installed on a separate VM outside the firewall.

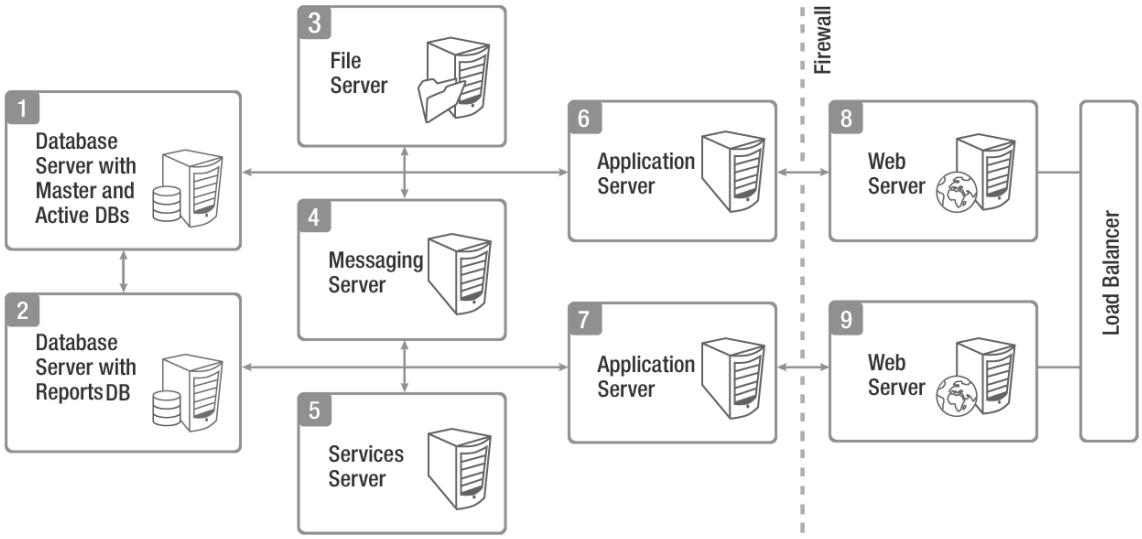


Collocated deployment for ECE

Distributed-Server Deployment

In this configuration, each component is on a separate VM, with the web servers installed outside the firewall. The application, messaging, services, and web servers in this configuration can be restarted without restarting any other servers.

- Multiple web-application server pairs are used with a load balancer.



Complex distributed-server configuration

Planning Components for Specific Configurations and High Availability

Disabling the TCP IP Offload Settings

Latency plays a critical role in the efficiency of contact center operations. To ensure optimal performance, it's essential to disable the Large Receive Offload (LRO) settings.

To disable the TCP IP Offload settings:

1. Ensure that the ECE network is in place and tested and verify that:
   - All LAN switches are configured for required subnets as per the System Design Specifications.
   - All IP Routers are configured as required.
   - There's IP connectivity between all subnets.
   - Required ethernet connections are in place between ECE software servers and LAN switches.
   - Required packet prioritization is configured on IP Routers.
2. To disable LRO, log in to the **ESXi** host or its vCenter with vSphere Client.
3. Select the host and choose **Configuration > Advanced Settings**.
4. Select **Net** and scroll down slightly to set the following parameters from 1 to 0:
   - `Net.VmxnetSwLROSL`
   - `Net.Vmxnet3SwLRO`
   - `Net.Vmxnet3HwLRO`

- `Net.Vmxnet2SwLRO`
- `Net.Vmxnet2HwLRO`

5. Reboot the **ESXi** host to activate the changes.

Planning the File Server

- Use Windows Distributed File System to achieve high availability for the File Server. For details about Windows Distributed File System, refer the Microsoft documentation: https://docs.microsoft.com/en-us/windows/desktop/dfs/distributed-file-system

Planning the Database Server

Installing the Application on a SQL Server 2022 Cluster

- ECE can be installed in a Microsoft SQL Server 2022 clustered environment using the **Always On Availability Group** cluster option to achieve high availability. To install and configure the SQL Server cluster, follow the instructions in the Microsoft SQL Server 2022 documentation.

  Things to note:

  - Clustering feature is available only for Enterprise Edition of MSSQL.
  - When using **Always On Availability Group** clustering, you must use the **Windows Authentication** mode.

Planning Database Server Distribution

- The master and active databases are installed on the same database server. The reports database can be installed on the same instance as the master and active databases or on a different instance.

  If the reports database is to be installed on a different instance, make sure that you complete the steps described in the "Configuring Database Servers" on page 40. You may also need to complete certain tasks described in "Setting Up User Accounts and Permissions" on page 33.

Planning Messaging Servers

- ECE can be installed with a cluster of messaging servers to achieve high availability. After deploying the cluster, when the application is started, it connects to one messaging server in the cluster. If at any time that messaging server goes down, the application connects to the next available messaging server in the cluster.
- For 400 Agent deployments, the messaging server component is collocated with other components. For 400+ agent deployments, the messaging server component is always installed on a dedicated VM.

  If the messaging server is on a separate VM, it can be restarted independently, without affecting application usage.

Planning Services Servers

- For high availability support, you can install two services servers. When the application starts, one server will become primary services server and other server will be secondary services server. The ECE application will need to be started on both the services servers, however, all the service processes (for example, retriever, dispatcher, etc.) will run only on the primary services server.
- All service processes will automatically failover to the secondary services server when the primary server is unavailable because of network connection failure or hardware issues. You can identify the primary services server from the System Console of the application. For details, see the *Enterprise Chat and Email Administrator's Guide to System Console*.

Important: **While initiating a failover when the connection to the database is down, the service processes will automatically run a retry mechanism every 10 seconds for an interval period of 30 seconds, thereby allowing the server to re-run the failover process for a maximum of three times. If the connection establishes within the defined interval period, services start successfully on the failed over services server.**

Planning Application Servers

- ECE can be installed with multiple application servers to achieve high availability. The number of application servers in your deployment depends on the total number of concurrent agents to be supported.

  If any of the application servers go down, a load balancer can help handle the failure through routing requests to alternate application servers through the web server.

Planning Web Servers

- ECE can be installed with multiple web servers. The number of web servers in a deployment depends on the number of application servers in the deployment.

  If any of the web servers go down, a load balancer can help handle the failure through routing requests to alternate web servers. The load balancer detects web server failure and redirects requests to another web server.

Load Balancing Considerations

- A load balancer may be used in a distributed installation of the application so that requests from agents and customers are either routed to the least-loaded web servers, or evenly distributed across all the available web servers. Please note that it is mandatory to use a load balancer for a VPN less ECE environment to ensure that agents working remotely without a VPN can seamlessly log into the system.

  While the application is agnostic to the particular brand of load balancer used in the configuration, it does require that the load balancer is configured to support "sticky sessions" with cookie-based persistence.

  Use the following URL to do the health check of the ECE web-app pair:
  `https://<WebServer_URL>/system/web/view/platform/common/login/root.jsp?partitionId=1`.

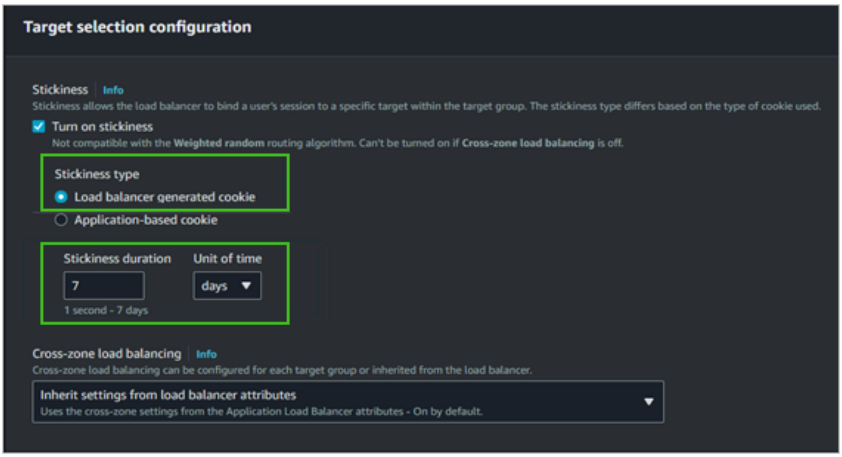
- The connection timeout on the load balancer must be set to 5 seconds.

Load Balancer Configuration Examples

Here are some essential configurations required on the load balancer. Please note that these are specific examples tied to a particular load balancer and are provided for reference purposes only. Similar configurations should be applied to the load balancer being used.

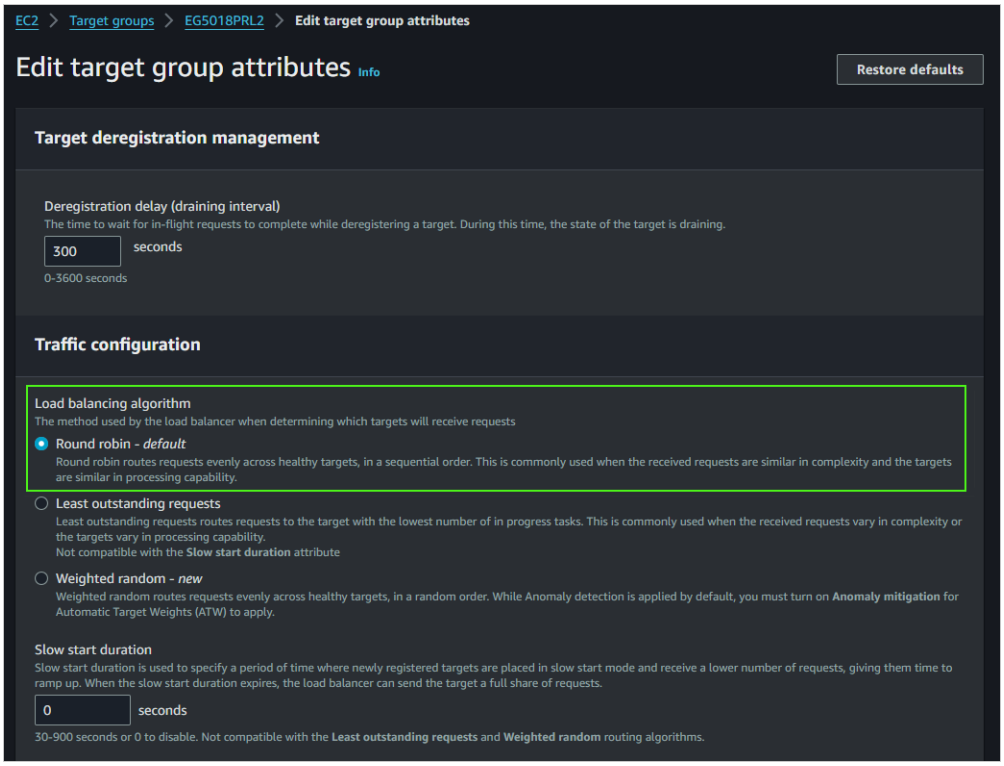
Cookie Persistence Configuration

This configuration enables the load balancer to generate cookies during the initial request and utilize them for session stickiness in subsequent requests.



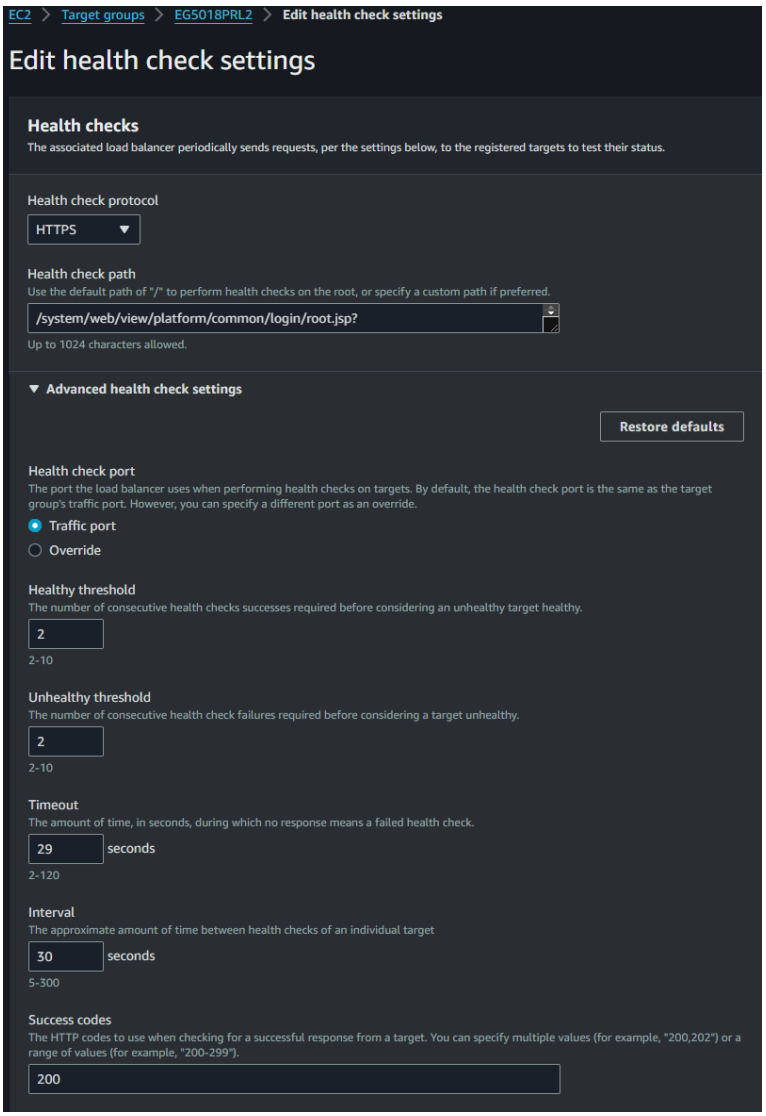
Request Routing Configuration

This configuration aims to distribute the session load evenly across available nodes (web servers), with round robin being the recommended method, though not the only option.



Health Check Configuration

This involves load balancer monitoring to detect the operational status of the nodes.

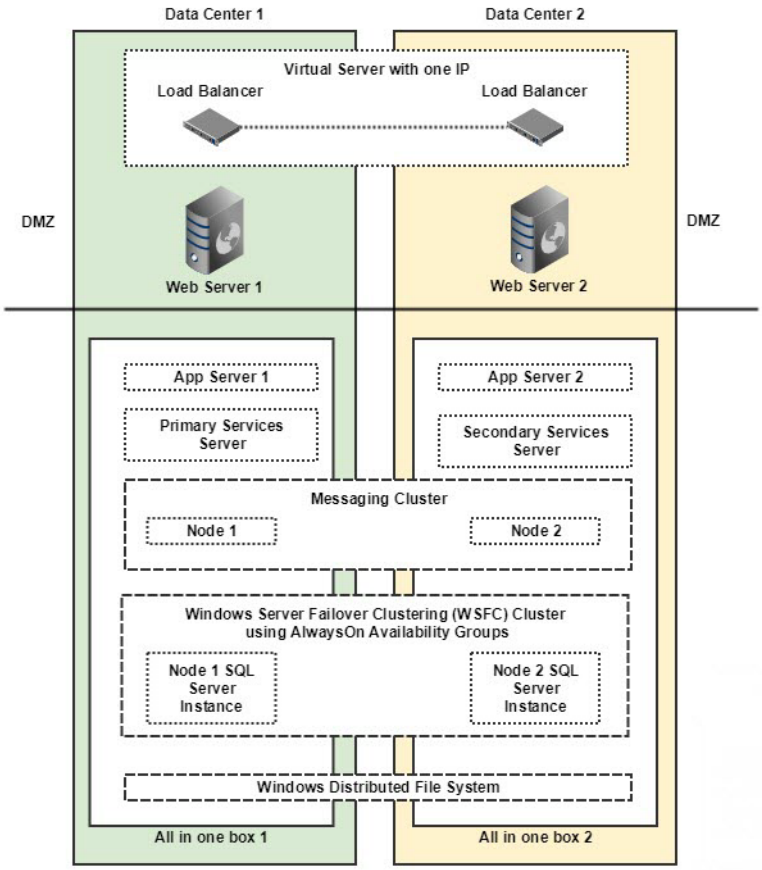


Planning for High Availability Across Geographies

- To achieve high availability across geographies, ECE can be deployed across two different geographical locations. The load balancer needs to be configured so that at any given point of time, all requests are redirected to web servers in one location.

For Collocated Deployments

For details about installing these servers, see "Installation Process" on page 65.



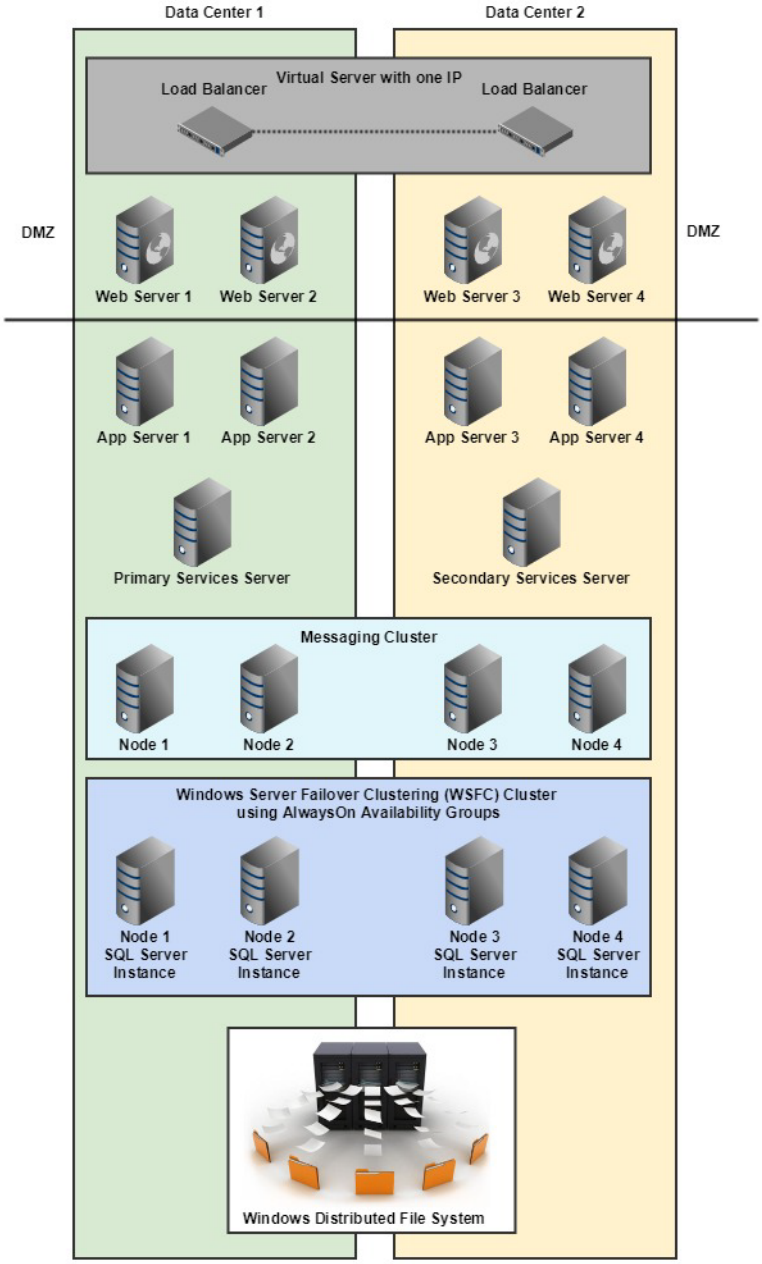
High Availability Across Geographies

In this deployment, the ECE components are installed on four VMs:

- **On Side A:**
  - **VM-1A:** File server (Windows Distributed File System Node1), Database server (Always On Availability Group), Messaging server, Application server, Services server
  - **VM-2A:** Web Server
- **On Side B:**
  - **VM-1B:** File server (Windows Distributed File System Node2), Database server (Always On Availability Group), Messaging server, Application server, Services server
  - **VM-2B:** Web Server

For Fully Distributed Deployments

For details about installing these servers, see "Installation Process" on page 65.



High Availability Across Geographies

In this deployment, following are the requirements to install the ECE components::

1. 30 VMs for 1500 Agents (No change in existing 15.0(1) OVAs)
2. 18 VMs for 1500 Agents (with new OVAs specifications as provided with ECE 12.6 ES3)
3. 22 VMs for 2500 Agents (with new OVAs specifications as provided with ECE 12.6 ES3)

- **On Side A:**
  - **VM-1A:** File server (Windows Distributed File System Node1)
  - **VM-2A:** Database server (active and master databases)
  - **VM-3A:** Database server (reports database)
  - **VM-4A:** Messaging server
  - **VM-5A:** Services server
  - **VM-6A to VM-10A:** Application server
  - **VMA-11A to VM-15A:** Web Server
- **On Side B:**
  - **VM-1B:** File server (Windows Distributed File System Node 2)
  - **VM-2B:** Database server (active and master databases)
  - **VM-3B:** Database server (reports database)
  - **VM-4B:** Messaging server
  - **VM-5B:** Services server
  - **VM-6B to VM-10B:** Application server
  - **VM-11B to VM-15B:** Web Server

Installing ECE

- Follow the pre-installation tasks (page 27), installation tasks (page 65), and post-installation tasks (page 82), to install ECE. To set up SSL, follow instructions in the "SSL Configuration" on page 126.

2 Pre-Installation Tasks

- Preparing Virtual Machine
- Disabling Loopback Adapter Configuration
- Verifying Network Configuration
- Configuring Port Numbers Between Components
- Setting Up User Accounts and Permissions
- Changing the Service Account Password
- Preparing Database Server VMs
- Preparing Web Server VMs
- 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*

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 **Enterprise Chat and Email - 12.6(1)** Software Download page.
2. Download the Virtual Machine Templates file for the release. You can download:
   - **For upto 400 agents:** ECE_15.0_400_Win2022_vmv18_v1.0.ova
   - **For 401-1500 agents:** ECE_15.0_1500_Win2022_vmv18_v1.0.ova
   - **For 401-2500 agents:** ECE_15.0_2500_Win2022_vmv18_v1.0.ova

     This is only available from ECE 12.6 ES3 onwards.
3. 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 2022. 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.

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**.

Verifying Signature File for ISO

To verify the signature file for ISO:

1. Download and install **openssl** from https://slproweb.com/products/Win32OpenSSL.html

   Any type of installer (either EXE or MSI) with any bit (32 or 64) can we downloaded from the link.
2. Install the download **openssl** using the instructions provided on the website. Have the **openssl** path added to the system path environment variable so that **openssl** command can be launched from any path.
3. Place the downloaded ISO image, ISO image signature file, and the public key.der from CCO in the same folder.
   - **ECE_15.0_Fresh.iso.signature**
   - **ECE_15.0_Fresh.iso**
   - **ReleaseCodeSign_publicKey.der**
4. Launch the command prompt by right-clicking and choosing **Run as administrator**.
5. Execute the **cli** command in the command prompt to verify the authenticity and integrity of the CCO downloaded ISO.

Syntax: `Openssl dgst -sha512 -keyform der -verify` *<public Key.der>* `-signature` *<ISO image.iso.signature> <ISO Image>*

For example: `Openssl dgst -sha512 -keyform der -verify ReleaseCodeSign_publicKey.der -signature ECE_15.0_Fresh.iso.signature ECE_15.0_Fresh.iso`

6. Upon successful verification output will be **Verified OK** and on failure **Verification failed**.

Disabling Loopback Adapter Configuration

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

Skip this section if the VMs 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 VM.

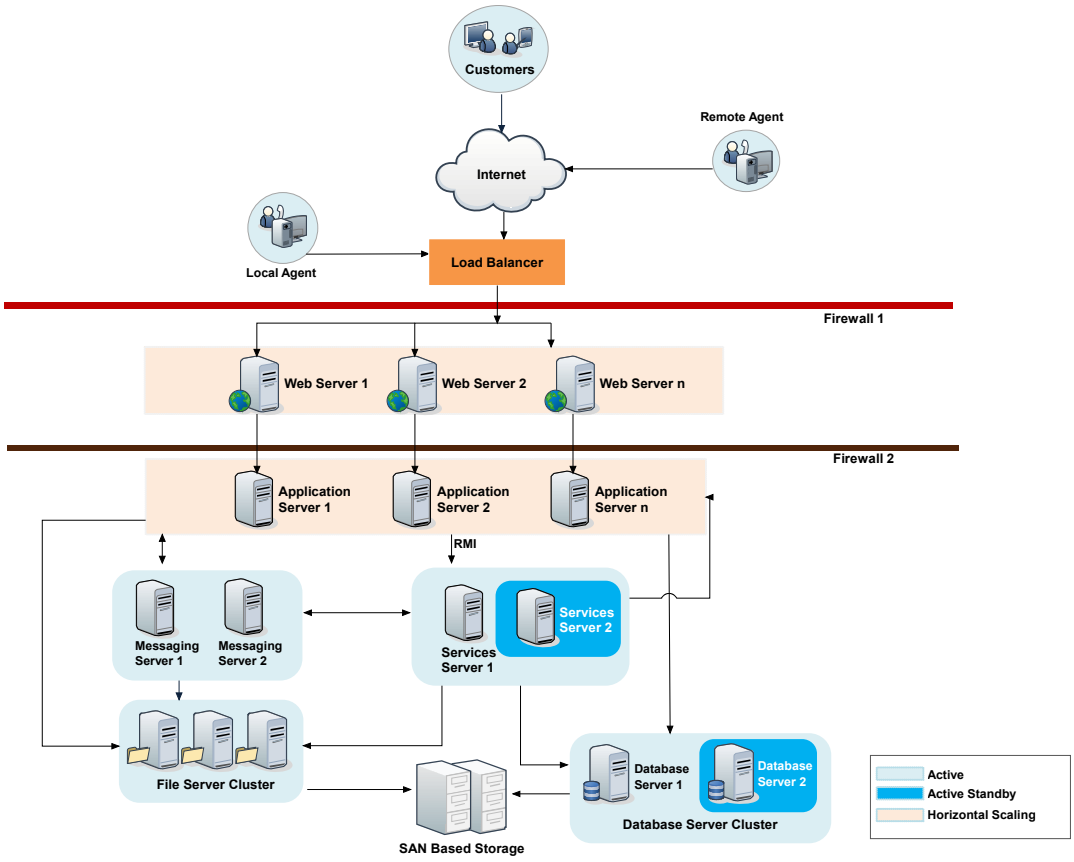
To verify network configuration:

1. Internet Protocol Version 6 (IPv6) must be disabled on all servers.
2. Ensure that all the VMs 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.
3. Ensure that all VMs other than the web servers, are in the same Active Directory domain. The web servers do not need to be installed in the same domain as other Enterprise Chat and Email components. They can be located anywhere, for example, in a DMZ. Note that the application cannot be installed in a workgroup.
4. 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 31.
5. For messaging, application, and services servers 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.
6. Ensure that all the VMs are in the same LAN.

7. Ensure that the system clocks of all the VMs are synchronized.
8. Ensure that all the servers, except the web server, are able to communicate with the database server at the time of installation.
9. If multiple NICs are configured on ECE servers, set NIC metrics for each NIC. The lowest (default) metric must be assigned to NIC that will be used for the ECE application.

Configuring Port Numbers Between Components

This section describes the ports that need to be opened for the flow of requests between the various components. The following diagram shows the ECE system architecture. This will help you understand the communication between the different components.



System architecture

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 (Internet)	Web Server	▸ 80 [Protocol: HTTP] ▸ 443 [Protocol: HTTPS]
Finesse Desktop (Internet)	Web Server	▸ 80 [Protocol: HTTP] ▸ 443 [Protocol: HTTPS]
Application Server	Services Server	▸ 15099 (RMI Registry port) [Protocol: RMI]* ▸ 49152 – 65535 (Dynamic port range used by RMI server objects) [Protocol: TCP]
Application Server	File Server	139 or 445 [Protocol: NETBIOS - TCP]
Application Server	Database Server	1433 [Protocol: TCP] *
Application Server	Messaging Server	15097 [Protocol: TCP] *
Application Server	Application Server	▸ 2434 [Protocol: TCP]* ▸ 6701 [Protocol: TCP]*
Application Server	SMTP Server	25 [Protocol: SMTP]
Application Server	SMTP or ESMTP Server (with SSL enabled)	587 [Protocol: SMTP or ESMTP]
Application Server	IMAP Server	143 [Protocol: IMAP]
Application Server	IMAP Server (with SSL enabled)	993 [Protocol: IMAP]
Web Server	Application Server	9001 [Protocol: TCP]*
Messaging Server	File Server	139 or 445 [Protocol: NETBIOS - TCP]
Messaging Server	Messaging Server	15097 [Protocol - TCP]*
Messaging Server	Database Server	1433 [Protocol: TCP]*
Services Server	Application Server	6701 [Protocol: TCP]
Services Server	File Server	139 or 445 [Protocol: NETBIOS - TCP]
Services Server	Database Server	1433 [Protocol: TCP] *
Services Server	Messaging Server	15097 [Protocol: TCP]*
Services Server	Services Server	47500 [Protocol: TCP]*
Services Server	SMTP or ESMTP Server	25 [Protocol: SMTP or ESMTP]
Services Server	SMTP or ESMTP Server (with SSL enabled)	587 [Protocol: SMTP or ESMTP]
Services Server	POP3 Server	110 [Protocol: POP3]
Services Server	POP3 Server (with SSL enabled)	995 [Protocol: POP3]

From Server	To Server	Default Destination Ports and Protocols
Services Server	IMAP Server	143 [Protocol: IMAP]
Services Server	IMAP Server (with SSL enabled)	993 [Protocol: IMAP]
Active Database Server	File Sever	Not applicable
Reports Database Server	Active Database Server	▸ 1433 [Protocol: TCP]* ▸ 135 [Port for Remote Procedure Call (RPC)] ▸ 5000-5020 (Port range for RPC ports required for MSDTC to work across firewall)
Services Server	Primary CTI Server	42027*
Services Server	Secondary CTI Server	42028*
Services Server	Media Routing Peripheral Gateway	38002*
Services Server	Primary Administration Workstation Database	1433 [Protocol: TCP]*
Application Server	Primary Administration Workstation Database	1433 [Protocol: TCP]*
Application Server	IdS Servers	443 & 8533
Application Server	IdP (ADFS) Servers	443

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.

Important: **For all servers other than the ECE web server, you must use the same domain account to install the software environment and ECE. ECE web server can be installed in DMZ and can have a different domain account. Use the service account to run the ECE services after installing the application (page 91).**

Setting Up Domain Account

- Request your IT department to create the following accounts. Make sure the passwords for these accounts are not more than 30 characters. You will not be able to install the application, if the passwords exceed this limit.

Caution: **The recommendation is that you do not change the password of the Service Account and SQL Services Account after the application is installed. If you must change it, make sure that you update the login information for: all Windows and MSSQL services that use these accounts and in IIS for: the Default and *Context Root* folders under IIS > Sites > *Site for ECE*.**

Account Type	Description	Privileges Required
Installation Account	You will use this account to install ECE. This can be an existing user with Administrator privileges on the server. This account, or any other account with **same privileges** can be used in future to install ECE updates and do version upgrades. **Note:** Password of this user account should not contain blank spaces, single quotes, and double quotes.	Administrator
Service Account	This account is used to run the ECE Windows service after installing the application. This is an exclusive user for use by the ECE application.	Log on as Service
SQL Services Account	Dedicated domain user account for configuring and running SQL server services. This is an optional account. You would create this account If you *do not* want the Service account to be used for running SQL services. This is an exclusive user for use by the ECE application.	Log on as Service
Manage Services Account	This account is used to start and stop the ECE service. This can be a local user or domain user. This can be an existing user with Manage Service privileges on the server.	Manage Service

Configuring Permissions on Active Directory Server

If you are using Windows authentication database connectivity, *or* the configuration includes more than one database server VMs, perform these additional tasks on the Active Directory server. You will need administrator privileges to complete these tasks. Contact your IT administrator for assistance if required.

To configure permissions:

1. Go to **Start > Run > Command** to launch the command window and run the following command. This sets the Service Principal Names (SPN) to the domain account for MSSQL service on the database servers.

   `setspn -A MSSQLSvc/`*HOST:PORT accountname*

   `setspn -A MSSQLSvc/`*HOST:instancename accountname*

   Run this command for both short and fully qualified host names for all database servers. Use the SQL Services Account for these tasks. If you did not create one, use the Service Account (page 33). For example,

if there are two database servers, `serv234` and `serv235`, with instance name as `MSSQLSERVER` and port as 1433, with the user account `SQLSERVICEUSER` in the domain1 domain, then run the following commands. If you are using **Always On Availability Group** clustering, then use the **Listener Name** (page 146) instead of the server name.

```
setspn -A MSSQLSvc/serv234.company.na:1433 domain1\SQLSERVICEUSER
setspn -A MSSQLSvc/serv234.company.na:MSSQLSERVER domain1\SQLSERVICEUSER
setspn -A MSSQLSvc/serv234:1433 domain1\SQLSERVICEUSER
setspn -A MSSQLSvc/serv234:MSSQLSERVER domain1\SQLSERVICEUSER
setspn -A MSSQLSvc/serv235.company.na:1433 domain1\SQLSERVICEUSER
setspn -A MSSQLSvc/serv235.company.na:MSSQLSERVER domain1\SQLSERVICEUSER
setspn -A MSSQLSvc/serv235:1433 domain1\SQLSERVICEUSER
setspn -A MSSQLSvc/serv235:MSSQLSERVER domain1\SQLSERVICEUSER
```

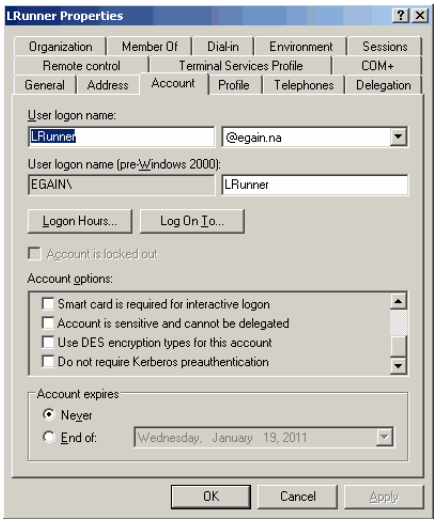
If you are using the Always On Availability Group clustering, then use the Listener Name (page 146) instead of the server name in the following format:

```
setspn -A MSSQLSvc/listener_hostname_FQDN:port_number SQL Service_Account.
```

For example, if there are two listeners with listener hostname FQDNs as `listener1.egeng.info` and `listener2.egeng.info` and port as 1444, with the SQL service accounts as `egeng\qeuser`, then run the following commands:

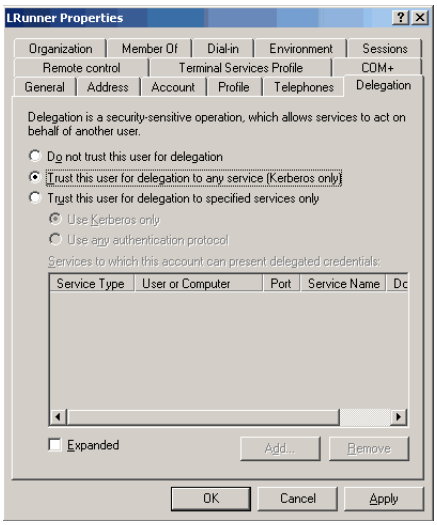
```
setspn -A MSSQLSvc/listener1.egeng.info:1444 egeng\qeuser
setspn -A MSSQLSvc/listener2.egeng.info:1444 egeng\qeuser
```

2. Go to **Start > Control Panel > Administrative Tools > Active Directory Users and Computers**.
3. Navigate to the domain user account used for MSSQL service on the database servers. Right-click and select **Properties**.
   a. In the Properties window, click the Account tab. Ensure that the following options are *not* selected:
      - **Account is sensitive and cannot be delegated**.
      - **Do not require Kerberos preauthentication**.



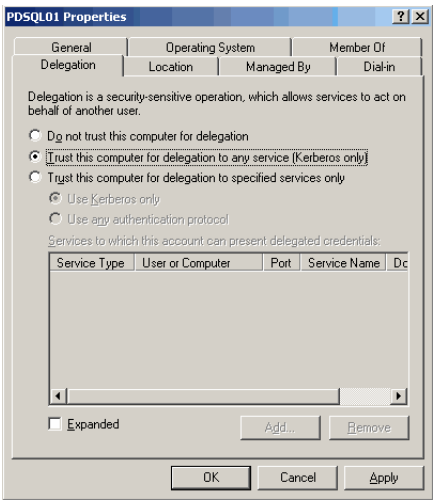
Set account properties for domain user account

b. Click the Delegation tab. Ensure that the domain user account is trusted for delegation. For a more secure configuration, you can select the **Trust the user for delegation to specified services only** option and specify the service added in Step 1.



Set delegation properties for domain user account

4. In the **Active Directory Users and Computers** tree, navigate to the database server. Ensure that it is trusted for delegation. Repeat this step for each database server. For a more secure configuration, you can select the **Trust the user for delegation to specified services only** option and specify the service added in Step 1.



Set delegation properties for database server

Changing the Service Account Password

To adhere to the organizational security policy, you must change the passwords at a periodic interval for the following:

- Application, Services and Messaging Server
- Web Server

Changing the Password

To change the password for the Application, Services and Messaging server:

1. From the Windows Services Manager, stop the Cisco services.
2. Right click on **Cisco Service** and go to **Properties**.
3. In the Properties window, go to the **Log On** tab.
4. Specify the new service account password and click **OK**.
5. Now, open the **File Explorer**.
6. If there exists a mapped network drive e.g. *g:*, which is mapped to the ECE File Server installation directory, disconnect it by right clicking on the drive.
7. Restart the Cisco Service.

To change the password for the Web server:

1. Open the **Internet Information Services (IIS) Manager**.

2. From the Connections pane, locate the website being used for ECE, for example, *Default Web Site*.
3. Expand the website to see following virtual directories:
   a. **default**
   b. **system**
4. Configure the basic settings on all the virtual directories:
   a. From the Actions pane, click the **Basic Settings...** button.
   b. In the Edit Site window, click the **Connect as...** button.
   c. In the Connect As window, select the **Specific user** option and click the **Set...** button.
   d. In the Set Credentials window, provide the **User name**, and the new password in the **Password** and **Confirm password** field.
5. Configure the advanced settings on all the virtual directories:
   a. From the Actions pane, click the **Advanced Settings** button.
   b. In the Advanced Settings window, select the **Physical Path Credentials** option.
   c. In the Connect As window, select the **Specific user** option and click the **Set...** button
   d. In the Set Credentials window, provide the **User name**, and the new password in the **Password** and **Confirm password** field.
6. Restart IIS.

Setting up Distributed File System (DFS)

You need to perform this task if you are planning an HA deployment. For details, see "Appendix A: Distributed File System Configuration" on page 135.

Preparing Database Server VMs

Install Microsoft SQL Server

Follow the Microsoft documentation to install Microsoft SQL Server 2022, Standard Edition or Enterprise Edition. Make sure the required features for Microsoft SQL are installed on the VM and the collation settings are configured properly.

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 Feature:
  - Integration Services

Verifying Collation Settings

- Collation settings are typically chosen while installing SQL Server 2022. 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 the SQL Collation as **SQL_Latin1_General_CP1_C1_AS** and select the following option: **Dictionary order, case-insensitive, for use with 1252 Character Set.** You must use this collation.

Choosing Authentication Method for Database Connectivity

Important: **If you are planning to use Always On Availability Group clustering (page 19), you must use Windows Authentication.**

- The application supports two methods of authentication for connecting to the database.
  - **SQL Server authentication:** Make sure you enable **mixed-mode** authentication if you plan to use SQL authentication for database connectivity.
  - **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 33.

Setting up for Always On Availability Group Clustering

You need to perform this task if you are planning an HA deployment. For details, see "Appendix B: SQL Always-On Configuration" on page 141.

Important: **The High Availability feature is available only for installations using Enterprise Edition of MSSQL.**

Installing SQL Server Management Studio (SSMS)

- Install SSMS tool on the database server. Install a version that is compatible with Microsoft SQL 2022. Refer the Microsoft documentation for details about doing this task.

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`

Assigning Permissions to Domain User

- Give `sysadmin` permission to the **Service Account** created for running the application. If you have created a separate **SQL Service Account** for the database services, then assign the permission to that user (page 33).

Configuring Database Servers

Skip this section if the reports database is on the same instance as the active and master databases. If any database is on a different instance, consult your administrator and verify that:

- All database server VMs used in the configuration are in the same domain as all the other Enterprise Chat and Email servers.
- All databases must be either on named instances or on default instances. For example, if you are using the **default** instance for the active and master databases, then use the **default** instance for the reports database as well.
- If you are using Windows authentication, also ensure that the steps outlined in the following section have been completed: "Configuring Permissions on Active Directory Server" on page 34. After you have completed these tasks, you should be able to run a linked server query on each database from a third machine acting as a SQL client.
- Enable mixed-mode authentication if you plan to use SQL authentication for database connectivity.

Configuring Memory Settings

To configure memory settings:

1. Connect to DB server.
2. Under the Object Explorer section, right-click a server and select **Properties**.
3. In the Server Properties window, under the Select a Page section, select **Memory**.
4. Under the Server memory options section, select the Maximum and Minimum server memory (in MB):
   - For ECE Lite Environment: Set the **Minimum server memory** value as **3072** MB and the **Maximum server memory** value as **10240** MB.
   - For ECE Fully Distributed Setup: Set the **Minimum server memory** value as **3072** MB and the **Maximum server memory** value as **14336** MB.
5. Click **OK**.

Alternatively, you can configure the memory settings by executing the following T-SQL script.

- For ECE Lite Environment:

```
USE master
GO
sp_configure 'show advanced options', 1;
GO
RECONFIGURE;
GO
sp_configure 'min server memory', 3072;
GO
RECONFIGURE;
GO
sp_configure 'max server memory', 10240;
GO
RECONFIGURE;
GO
```

- For ECE Fully Distributed Setup:

```
USE master
GO
sp_configure 'show advanced options', 1;
GO
RECONFIGURE;
GO
sp_configure 'min server memory', 3072;
GO
RECONFIGURE;
GO
sp_configure 'max server memory', 14436;
GO
RECONFIGURE;
GO
```

Configuring Microsoft DTC Settings

The Microsoft Distributed Transaction Coordinator (DTC) service, a component of Microsoft Windows, is responsible for coordinating transactions that span multiple resources like databases. MSDTC settings must be configured on all the database servers in a configuration.

Enable network DTC access on each database server VM.

To enable network DTC access:

1. Go to **Start > Control Panel > Administrative Tools > Component Services.**

2. In the console tree, browse **Component Services > Computers > My Computer > Distributed Transaction Coordinator > Local DTC.**
3. Right-click **Local DTC** and from the menu select **Properties.**
4. In the Local DTC Properties window, go to the Security tab and set the following:
   a. In the Security Settings section, select the following two options:
      - **Network DTC Access**
      - **Enable XA Transactions**
   b. Within the Network DTC Access section, select the following four options:
      - **Allow Remote Clients**
      - **Allow Remote Administration**
      - **Transaction Manager Communication - Allow Inbound**
      - **Transaction Manager Communication - Allow Outbound**
   c. In the DTC Logon Account section, set the value in the **Account** field to **NT Authority\NetworkService**.

   Click **OK**.
5. In the DTC Console Message box, click **Yes**.
6. Restart the machine.
7. Go to **Start > All Programs > Administrative Tools > Services**.
8. In the Services window, locate the following two services and stop them.
   - **Distributed Transaction Coordinator**
   - **SQL Server (MSSQLSERVER)** for Microsoft SQL 2022.
9. Now, start the two services in the following order:
   a. Distributed Transaction Coordinator
   b. **SQL Server (MSSQLSERVER)** for Microsoft SQL 2022.
10. Next, go to **Start > All Programs > Control Panel.**
11. Open Windows Firewall, and in the Windows Firewall window, click the **Allow an app or feature through Windows Firewall** link.
12. In the Allowed Programs window, click the **Change Settings** link and select the **Distributed Transaction Coordinator** option. Click **OK**.

Running Services

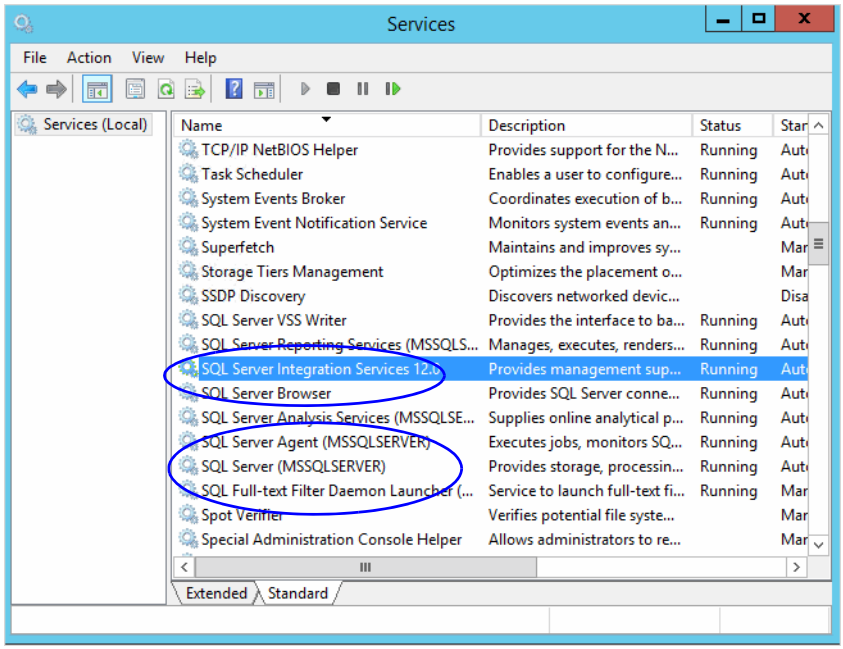
Make sure the following services are running. These services should be started using the **SQL Services Account** that you have created for the ECE application. If you didn't create a **SQL Services Account**, use the **Service Account** created for the ECE application (page 34).

- **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.
- **Windows Remote Management Service:** This service is required only on the reports database.

To start the services:

1. Go to **Start** > **Programs** > **Administrative Tools** > **Services**.
2. For all the services, do the following:
   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 correct domain account. These services should be started using the **SQL Services Account** that you have created for the ECE application. If you didn't create a **SQL Services Account**, use the **Service Account** created for the ECE application (page 34).
3. Ensure that the SQL Server Service, SQL Full-text Filter Daemon Launcher, SQL Server Agent, Windows Remote Management Service, 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 VMs

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 4.7
- 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.
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) > Web Server** 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 4.7

- 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 Modules 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 Application Request Routing and URL Rewrite modules are required to be installed on the web server. Download and install the modules from the Microsoft website. The installation programs are also available in the `Environment\Web Server` folder of the installation package. After installing the module, restart IIS.

Configuring Permissions on IIS Config Folder

- Ensure that the user account you are going to use for installing the application (page 34) has read permissions on the following folder: `%systemroot%\system32\inetsrv\config`

Running the World Wide Web Publishing Service

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

Configuring Virus Scanners

Important: **Any external application outside of ECE must not use the JDK utilized by the ECE application. The JDK path for the ECE application is located at <Installation_directory>\env\jdk and <Installation_directory>\eService\env\jdk.**

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.

On the File, Messaging, Services, Application, and Web Servers

Follow the instructions for your virus scanning software to exclude the following folders and file types. On a Windows 2022 Server machine, these exclusions must also be setup for **Windows Defender**.

Item	Exclude Subfolders?	Execute permissions
Windows File Protection	--	Read, Write
All files of type LOG	--	Read, Write
Pagefile.sys	No	Read, Write
Drive:\ECE_Home	Yes [other than **Storage**]	Read, Write
*.rll	No	Read, Write

On the Database Servers

Follow the instructions for your virus scanning software to exclude the following folders and file types. On a Windows 2022 Server machine, these exclusions must also be setup for the **Windows Defender**.

Item	Exclude Subfolders?	Permissions
Windows File Protection	--	Read, Write
All files of type LOG, if any	--	Read, Write
Pagefile.sys	No	Read, Write
Drive:\Path_to_datafile	Yes	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 Packaged 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.
- 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
  - Precision queues

  For details, see "Prepare Packaged CCE for the Integration" on page 48.

3 Prepare Packaged CCE for the Integration

- Relationship Between Objects in Packaged CCE and ECE
- Adding ECE to Packaged CCE Inventory
- Configuring Packaged CCE
- Adding MR PIM for ECE
- Adding Agent PG PIM for ECE
- Adding CTI for ECE
- 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	▸ An agent belongs to a peripheral. ▸ A peripheral belongs to an agent peripheral gateway (PG).
Skill group	User group	▸ A skill group belongs to a peripheral. ▸ A peripheral belongs to an agent PG.
Media routing domain (MRD)	Queues (Only selected skill groups and PQs of the MRD)	▸ Multiple queues can belong to a single MRD.
Script selector	Queue	▸ 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.

Adding ECE to Packaged CCE Inventory

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

For 2000 Agent Deployments

To Add ECE database server:

1. Sign in to Unified CCE Administration and navigate to **Infrastructure Settings > Inventory.**
2. Click **Add Machine**
3. Select **ECE Data Server.**
4. Add the hostname or IP address of the ECE Database Server.
5. Click **Save**.

To Add ECE web server:

1. Sign in to Unified CCE Administration and navigate to **Infrastructure Settings > Inventory.**
2. Click **Add Machine.**
3. Select **ECE Web Server.**
4. Add the hostname or IP address of the ECE Web Server.
5. Enter **Application Instance Name.**
6. Enter **Username** and **Password** for ECE Web Server Administration.

For 4000 & 12000 Agent Deployments

For 4000 and 12000 agent deployments, you can add to the inventory in two ways:

- By providing ECE servers details in **CSV** file while setting the initial deployment.
- By using **Import > Device** under **Infrastructure Settings > Inventory**.

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 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.

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 62.

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 52)
Application path	Configured using the Configuration Manager tool. (page 52)
Agents	Configured using the Unified CCE Administration page. (page 53)
Skill groups	Configured using the Unified CCE Administration page. (page 54)
Dialed Number/Script Selectors	Configured using the Unified CCE Administration page. (page 55)
Scripts	Configured using the Script Editor. (page 55)
Precision Routing	Configured using the Unified CCE Administration page. (page 60)

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. Navigate to **Call Settings > Route Setting**. Click the Call Types tab.
4. In the Call Types tab, click **New**. The New Call Type page opens.
5. In the **Name** field, provide a name for the call type.
6. Click **Save.**

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. You *must* create a new application path for ECE.

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.

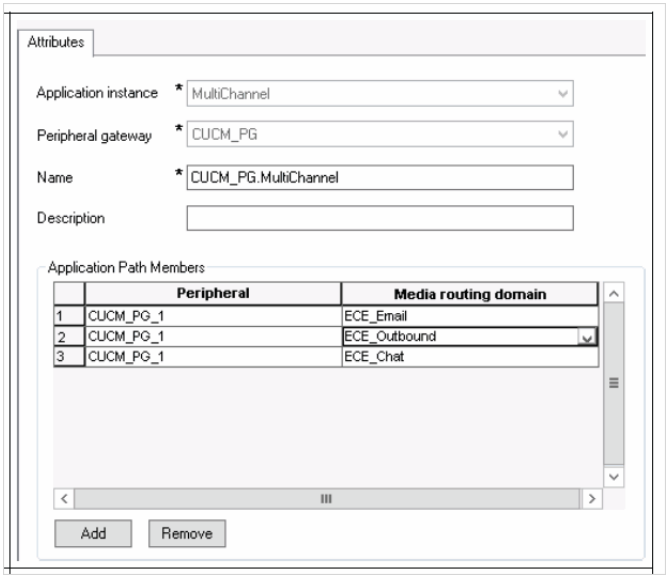
Access to the application object filter is restricted. Log in as a super user to enable or disable the application object filter. For details about the super user password, see the *Configuration Guide* for Cisco Unified ICM/Contact Center Enterprise available at https://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_installation_and_configuration_guid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

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



Select the Peripheral Gateway

7. 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`.
8. 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 61.

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

To configure an agent:

1. Launch the CCE Web Administration page, using the URL: `https://`*Server_Name*`/cceadmin/`
2. Login using the administrator credentials.
3. Navigate to **User Setup > Agents**.
4. On the List of Agents page, click **New**.

The New Agent page opens. This window has four tabs: General, Attributes, Skill Groups, and Supervised Teams. 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:
   - **Enable SSO:** Select this option if you want to use single sign-on for the agent. Password fields are disabled if you select this option.
   - **Login Enabled:** Select the option.
   - **Is Supervisor:** Select this option to make a user supervisor in ECE.
   - **Support Email & Chat:** Select this option to create the user automatically in ECE
   - **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.
   - **Department:** Select the ECE department in which the user should be created.
6. If you selected the **Support Email & Chat** option for the user, go to the Enable Email & Chat tab and provide the **Screen Name** (required) and **Email Address** (optional) for the user.
7. Click **Save.**

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. Navigate to **Organization Setup > Skills.** Click the Skill Groups tab.
4. In the Skill Groups tab, click **New**.

   The New Skill Group page 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.
6. On the Members tab, do the following:
   a. Click the **Add New** button.
   b. From the Add Agents pop-up window, select the agents to be added in 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 49) and add ECE as an External Machine in the System Inventory (page 49). 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. Navigate to **Call Settings > Route Setting.** Click the Dialed Number tab.
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 as **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.
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.

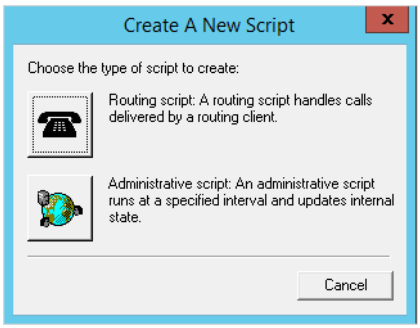
For details about creating universal queues, see the *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise* available at https://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_user_guide_list.html. Make sure to use the guide that matches the version of the product that you are using. To find the right version, refer to the Unified CCE Solution Compatibility Matrix available at https://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 60.

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 Cisco Unified ICM/Contact Center Enterprise*.

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



*Select the **Routing Script** option*

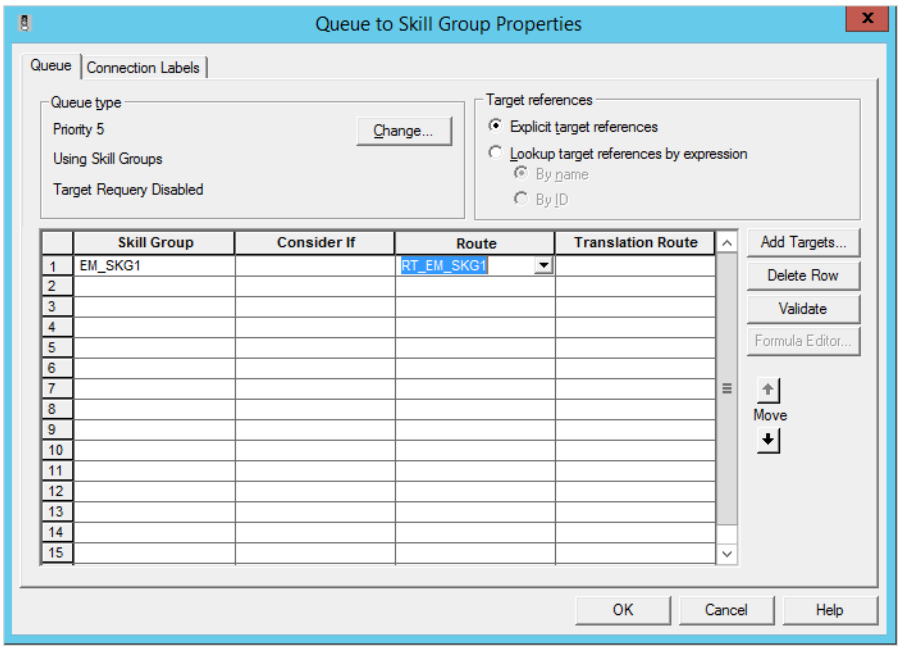
A new script editor opens. The Start node is added by default to the script editor.

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

   The Palette window opens.

5. 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.
6. Double-click the Queue to Skill Group node to open the Queue to Skill Group Properties window.

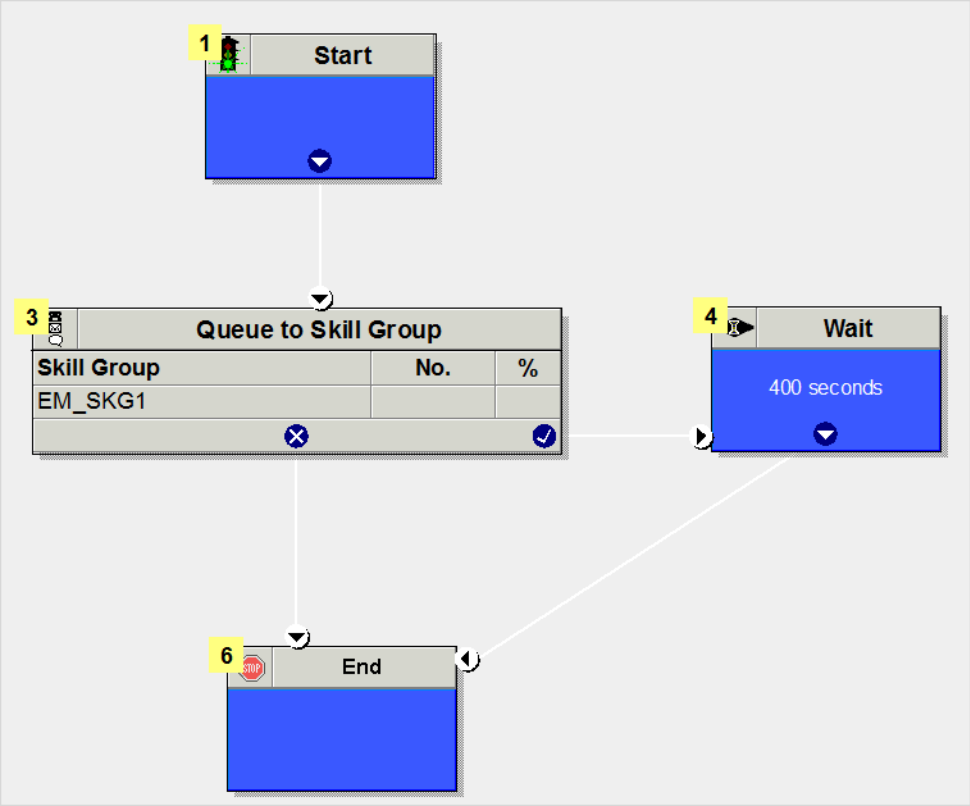
7. In the Queue to Skill Group Properties window, on the Queue tab, in the Skill Group column, select a skill group.



Select a skill group

8. 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.
9. Click the **Validate Script** button to check if the script is created properly. If there are any errors, fix them.

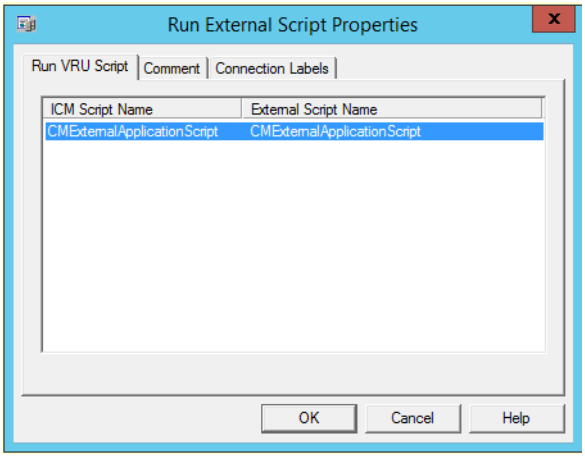
10. Click the **Save** button to save the script.



A sample script

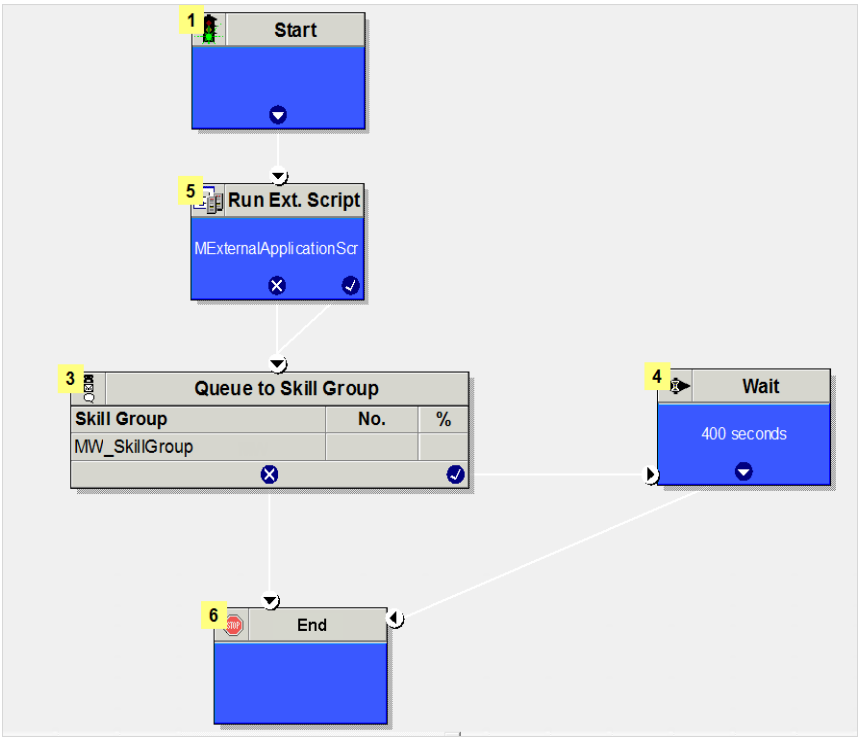
To display dynamic content to chat customers (for example, wait time, activity ID, etc.) while chat requests are being processed by the system, ensure that the Run External Script node is configured.

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.

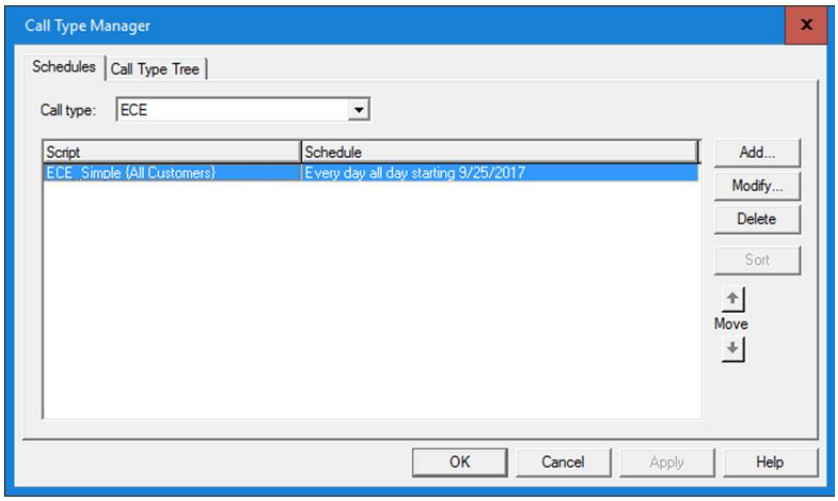


A sample script

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 Schedule tab, do the following:
    a. In the **Call type** field, from the dropdown list, select the call type created for ECE.
    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 55).
        ii. In the Period tab, set a schedule for the script.

iii. Click **OK**.



Set a schedule for the script

14. 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 the **Precision Queues** chapter in *Administration Guide for Cisco Unified Contact Center Enterprise*.

To configure precision routing, create the following objects:

1. Create attributes (page 60)
2. Assign attributes to agents (page 61)
3. Create precision queues (page 61)
4. Add precision queue node to the scripts (page 61)

Important: **If you are planning to have multiple departments in ECE, then ensure that you configure department specific precision queues.**

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. Navigate to **Organization Setup > Skills**. Click the Attributes tab.
4. In the Attributes tab, click **New**. The New Attribute page opens.
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.**

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. Navigate to **User Setup > Agents**.
4. In the list of agents, select an agent to assign attributes.
5. On the Attributes tab click the **Add New** button and add the required attributes to agent and set the values for the attributes. click **Save**.

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. Navigate to **Organization Setup > Skills**. Click the Precision Queues tab.
4. In the Precision Queues tab, click **New**. The Add New Precision Queue page opens.
5. On the Add 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.

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 Queues** chapter in *Administration Guide for Cisco Unified Contact Center Enterprise*.

Adding MR PIM for ECE

To add PG and PIM for MRPG:

1. On the CCE Peripheral Gateway on Side A, from Cisco Unified CCE Tools, click **Peripheral Gateway Setup**.
2. On the Components Setup screen, in the Instance Components panel, click the **Add** button.
3. On the Components Setup screen, in the Instance Components panel, click on peripheral gateway.
4. In the Peripheral Gateways Properties screen, slosh client type as **Media routing**. Then click **Next**.
5. In the Peripheral Interface Manager pane of the Peripheral Gateway Component Properties dialog box, click **Add**, select **PIM1**, 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 Media Routing Peripheral Gateway that you are not using for any other purpose.
   d. In the **Application Hostname (1)** field, enter the FQDN (Fully Qualified Domain Name) of ECE Services Server that matches how the ECE Dataserver has been resolved after it has been added to CCE Administration Inventory. If you have installed two services servers for high availability, provide the information for the primary services server on Side A.
   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, enter the FQDN (Fully Qualified Domain Name) of ECE Services Server that matches how the ECE Dataserver has been resolved after it has been added to CCE Administration Inventory on Side B. Set this value only if you have installed two services servers for high availability.
   g. In the **Application Connection Port (2)** 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. Set this value only if you have installed two services servers for high availability.
   h. In the **Heartbeat interval (sec)** field, enter **5.**
   i. In the **Reconnect interval (sec)** field, enter **10**.
   j. Select the **Enable Secured Connection** option if you want to use the secure PII feature. You will be prompted to update the Application connection ports. Check the *Port Utilization Guide for Cisco Unified Contact Center* to find the port number to be used for secure connection. If you select this option, you must configure the security options for the External Agent Assignment Service instance in ECE. For details, see the *Enterprise Chat and Email Administrator's Guide*.
   k. Click **OK**.
6. Accept defaults and click **Next** until the Setup Complete screen opens.
7. On the Setup Complete screen, check **Yes** to start the service. Then click **Finish**.
8. Click **Exit Setup**.

   Repeat these steps for the CCE Peripheral Gateway on Side B.

Adding Agent PG PIM for ECE

To add PG and PIM for Agent PG:

1. On the CCE Peripheral Gateway on Side A, from Cisco Unified CCE Tools, select the **Peripheral Gateway Setup** option.
2. On the Components Setup screen, in the Instance Components panel, click the **Add** button.
3. Select peripheral gateway and click it. PG1A will be created.
4. On the Components Setup screen, in the Instance Components panel, click on peripheral gateway.
5. In the Peripheral Gateways Properties screen, slosh client type as **CUCM**. Then click **Next**.
6. In the Peripheral Interface Manager pane of the Peripheral Gateway Component Properties dialog box, click **Add**, select **PIM1**, and configure with the **Client Type** of **CUCM** as follows:
   a. Check **Enabled**.
   b. In the **Peripheral name** field, enter **Agent PG**.
   c. In the **Peripheral ID** field, enter the Peripheral ID for the Agent PG that you are not using for any other purpose.
   d. In the CUCM section, provide the CUCM server details with username and password.
   e. Click the **OK** button.
7. Click **Next** until the Setup Complete screen opens.
8. On the Setup Complete screen, check **Yes** to start the service. Then click **Finish**.
9. Click **Exit Setup.**

   Repeat these steps for the CCE Peripheral Gateway on Side B.

Adding CTI for ECE

To add CTI for ECE:

1. On the CCE Peripheral Gateway on Side A, from Cisco Unified CCE Tools, click **Peripheral Gateway Setup**.
2. On the Components Setup screen, in the Instance Components panel, click the **Add** button.

   The Component selection screen opens.
3. Click on **CTI server.** In the CTI server component screen, select the check box for secure port, if you want to use secure port. Click the **Next** button.
4. Click **Next** until the Setup Complete screen opens.
5. On the Setup Complete screen, check **Yes** to start the service. Then click **Finish**.
6. Click **Exit Setup.**

   Repeat these steps for the CCE Peripheral Gateway on Side B.

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 88.

4 Installation Process

- Installation Overview
- Installing ECE
- Installation Details

This chapter provides an overview of how to install the application. Before beginning the installation, ensure that you have complied with all the prerequisites listed in "Pre-Installation Tasks" on page 27.

Installation Overview

You can do a collocated deployment, where all components, except for the web server, are installed on the same VM and the web server is installed on a separate VM. The web server may be installed outside the firewall, if required. Or, you can do a distributed-server installation, where each component is installed on a separate VM.

When each component is on a different VM, the installation program is run on each server separately. Make sure you install the file server first, followed by the database server. Note that the installer should always be launched from the machine meant to be File server as only the Database server can be installed remotely. Since the database is installed remotely when file server is being installed, select both the file server and the database components at the same time in the installation wizard. The program will ask you for the details of the database server as you work through the installation.

If you are installing two components, for example, application and services server components, on the same VM, make sure that you install both application server and services server at the same time. The installation program can only be run once per server.

The valid sequence for running the installation program is:

Install the following components first:

1. File server + Database server

The following components can be installed in any order:

2. Messaging server
3. Application server
4. Services server

The following server can only be installed after Application server has been installed:

5. Web server

If you plan to have multiple application and web servers, run the installer on all the VMs where these components need to be installed. If you plan to install a cluster of messaging servers, make sure you install all the messaging servers. Likewise, if you are planning to have two services server, then make sure you install both the services servers. You can add additional servers at any point after installing the application, but always make sure to run the installation program on the new servers to add them to the deployment.

For 400 Agent Deployments

Install the components on two VMs:

- **VM-1:** File server, Database server, Messaging server, Application server, Services server
- **VM-2:** Web Server

For 400 Agent Deployments (HA)

Install the components on four VMs:

- **On Side A:**
  - **VM-1A:** File server (Windows Distributed File System Node1), Database server (Always On Availability Group), Messaging server, Application server, Services server
  - **VM-2A:** Web Server
- **On Side B:**
  - **VM-1B:** Messaging server, Application server, Services server

    (Already configured while setting up **Side A** and should not be installed again: File server (Windows Distributed File System Node2), Database server (Always On Availability Group))
  - **VM-2B:** Web Server

For 401-1500 Agent Deployments

Install the components on following VMs:

- **VM-1:** File server
- **VM-2:** Database server (active and master databases)
- **VM-3:** Database server (Reports database)
- **VM-4:** Messaging server
- **VM-5:** Services Server
- **VM-6-VM10:** Application server
- **VM-11-15:** Web Server

For 401-1500 Agent Deployments (HA)

Install the components on following VMs:

- **On Side A:**
  - **VM-1A:** File server (Windows Distributed File System Node1)
  - **VM-2A:** Database server (active and master databases)
  - **VM-3A:** Database server (reports database)
  - **VM-4A:** Messaging server
  - **VM-5A:** Services server
  - **VM-6A to VM-10A:** Application server
  - **VMA-11A to VM-15A:** Web Server
- **On Side B:**
  - **VM-4B:** Messaging server
  - **VM-5B:** Services server

- **VM-6B to VM-10B:** Application server
- **VM-11B to VM-15B:** Web Server

  (Already configured while setting up **Side A** and should not be installed again: **VM-1B:** File server (Windows Distributed File System Node 2), **VM-2B:** Database server (active and master databases), **VM-3B:** Database server (reports database))

For 401-2500 Agent Deployments

Install the components on following VMs:

- **VM-1:** File server
- **VM-2:** Database server (active and master databases)
- **VM-3:** Database server (Reports database)
- **VM-4:** Messaging server
- **VM-5:** Services Server
- **VM-6-VM-8:** Application server
- **VM-9- VM-11:** Web Server

For 401-2500 Agent Deployments (HA)

Install the components on following VMs:

- **On Side A:**
  - **VM-1A:** File server (Windows Distributed File System Node1)
  - **VM-2A:** Database server (active and master databases)
  - **VM-3A:** Database server (reports database)
  - **VM-4A:** Messaging server
  - **VM-5A:** Services server
  - **VM-6A to VM-8A:** Application server
  - **VMA-9A to VM-11A:** Web Server
- **On Side B:**
  - **VM-4B:** Messaging server
  - **VM-5B:** Services server
  - **VM-6B to VM-8B:** Application server
  - **VM-9B to VM-11B:** Web Server

    (Already configured while setting up **Side A** and should not be installed again: **VM-1B:** File server (Windows Distributed File System Node 2), **VM-2B:** Database server (active and master databases), **VM-3B:** Database server (reports database))

Installing ECE

This section talks about installing the application. In a distributed-server installation, repeat these tasks on all VMs in your configuration.

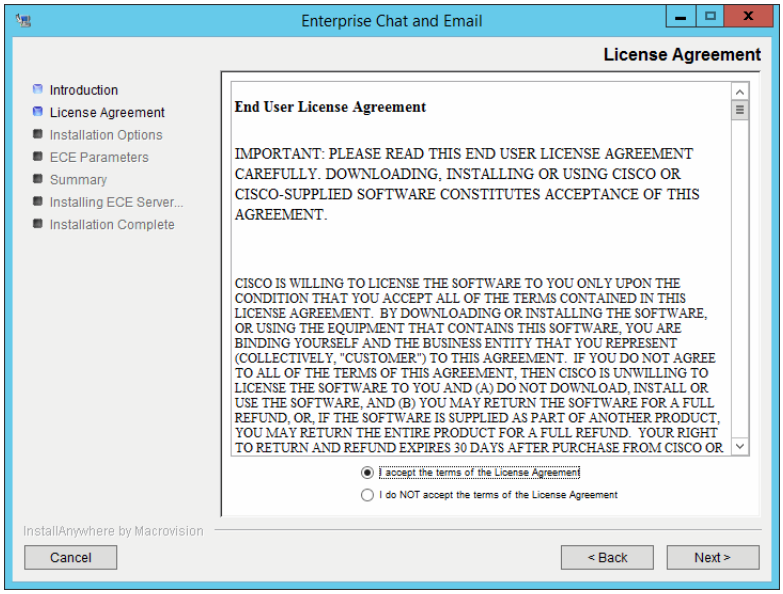
To install ECE:

1. Start the installation by using the physical installation media or a mounted ISO file. Run `setup.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.exe` from the *C:\Temp*`\Application` directory.

2. When the Introduction window appears, read the installation instructions. Click **Next**.

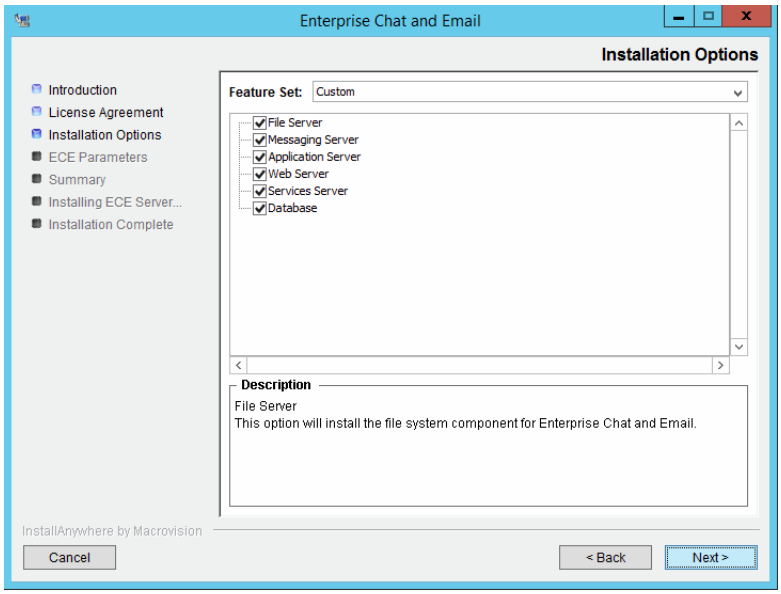
3. In the License Agreement window, review the licensing terms and select the **I accept the terms of the License Agreement** option. Click **Next**.



Read and accept the terms of the License Agreement

4. In the Installation Options window, select from the following components. Make sure you select all the components you wish to install. For details, see "Installation Overview" on page 66.
   - **File Server**
   - **Messaging Server**
   - **Application Server**
   - **Web Server**
   - **Services Server**
   - **Database**

Click **Next**.



Select installation options

Based on the components you choose to install, you will see a different set of screens. The installation program for ECE has on-screen help that describes the information that needs to be provided for each screen. If you need to refer to the fields that each screen displays, see the following sections.

- File Server Details on page 71
- Database Server Details on page 72
- Web Server Details on page 77
- Messaging Server Details on page 79
- Application Server Details on page 80
- Services Server Details on page 81

5. Review the information displayed in the Summary window, and click **Install.**
6. In the Install Complete window, click the **Finish** button to complete the installation process.

A summary of the installation is saved in *ECE_HOME*`\eService\installation\logs\installation_summary_`*Server_Name*`.txt`.

After the installation is completed, perform the post-installation tasks (page 82).

Installation Details

File Server Details

#	Field Name	Description	Value
Enterprise Chat and Email Home Directory			
1.	File Server Directory/NAS path/ DFS Path	Provide the path of the directory where you would like to install Enterprise Chat and Email. For example, *Install_Drive*`\Cisco`, or `\\SharedSpace\Cisco`, if the file server is installed on a NAS device or DFS. **Note:** NAS is supported on non-HA environment while DFS is supported on HA environment. Make sure that the path and folder name do not contain any of the following characters: *?<>|+^'"%`,@	
Domain User Account Parameters			
2.	Domain user name	User name of the domain user account created for use by the application. For more information, refer to "Setting Up User Accounts and Permissions" on page 33. User name should be provided in the format: `Domain\username`	
3.	Domain user password	Password for the domain user.	

File server details

Database Server Details

#	Field Name	Description	Value
File Sever Parameters			
1.	File Server Name/NAS Path/ DFS Path	The fully qualified domain name of the file server. If the file server is installed on a NAS device or DFS, provide the path to the shared folder. For example, \\SharedSpace\Cisco. **Note:** NAS is supported on non-HA environment while DFS is supported on HA environment. Make sure you provide the DNS host name and not the IP address of the server.	
Cisco Application Context Root			
2.	Context Root Name	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. **Note:** You should refrain from changing the value of the **Context Root Name** to a non-default value as it disallows users from accessing the ECE application URL and a 404 error is observed. Also, make sure there are no spaces or special characters in the name of the context root.	system
Cisco System Administrator Account			
3.	User name	User name for the system administrator. This is the first user that gets created for accessing the system partition.	sa
4.	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.` Do not use the following characters in the password: < (less than), > (greater than), ; (semi colon), : (colon), = (equal to), \ (back slash)	
Cisco Partition Administrator Account and Partition Details			
5.	User name	User name for the partition administrator. This is the first user that gets created for accessing the business partition.	pa
6.	Password	Password for the partition administrator. **Note:** The password should have at least eight characters and should be a mix of numbers and alphabets. For example, `password@123.` Do not use the following characters in the password: < (less than), > (greater than), ; (semi colon), : (colon), = (equal to), \ (back slash)	

#	Field Name	Description	Value
7.	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.	default
8.	Description of partition	Description for the partition.	
Installation Identifiers			
9.	Unique name for this installation	Provide a unique name for this installation. For example: PROD, PRD1, TEST, TST2, or DEMO. The length of the name must be between 1 and 4 characters long. The name must not contain any spaces or special characters.	
10.	4-digit identifier for this installation	Provide a 4-digit numerical value, between 2001 and 9998, that will be used internally as system ID.	
Knowledge Base Primary Language			
11.	Knowledge Base Primary Language	The default language for the Knowledge Base.	English (US)
Default Notification Parameters			
12.	Default SMTP server	The SMTP server to be used to send email notifications.	
13.	Notification mail redirection from address	All notification emails are sent from this email address.	
14.	Notification mail redirection to address	All notification emails are sent to this email address.	
SQL Server Database Authentication			
15.	Authentication	Authentication type to be used while connecting to the database. Set the value as **SQL Server Authentication mode** or **Windows Authentication mode.** If you are using MSSQL Server **Always On Availability Group** Clustering, select the authentication type as **Windows Authentication.** **Note:** If you selected Windows Authentication as the only mode of authentication while installing SQL Server, you must set the value as **Windows Authentication mode.**	
Master Database Parameters			
16.	Server name	Name of the local or remote server on which you want to install the master database. If you are using MSSQL Server **Always On Availability Group** clustering, specify the Listener name (page 146). **Note:** Make sure you provide the DNS host name and not the IP address.	
17.	Database name	Name of the master database. The installation program creates a database with the name you provide here.	

#	Field Name	Description	Value
18.	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. If you are using MSSQL Server **Always On Availability Group** clustering, provide the name of the Listener instance. **Note:** You can skip configuring this field when the value of the Server name field is set as the Listener name.	
19.	Database listener port	Port number of the MSSQL Server or the Listener name.	1433/1444
20.	Datafile path	Path to the folder on the database server, where you want to create the data file. For example, `D:\MSSQL\Data`.	
21.	Datafile initial size (MB)	Minimum size of the data file for the database.	100
22.	Datafile maximum size (MB)	Maximum size of the data file for the database.	Unlimited
23.	Datafile increment size (MB)	Additional file size limit that will be allocated to the database after the initial size is full.	10
24.	Logfile initial size (MB)	Minimum size of the log file.	25
25.	Logfile maximum size (MB)	Maximum size of the log file.	Unlimited
26.	Database administrator user name	User name of the database administrator for MSSQL Server. If you have created a separate user for installing Enterprise Chat and Email databases, provide the name of that user (page 40). **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
27.	Database administrator password	Password of the database administrator. **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
28.	Cisco Database user name	User name required to connect to the master database. The installation program creates the database and its user.	
29.	Cisco Database password	Password for the master database user.	
Active Database Parameters			
30.	Server name	Name of the local or remote server on which you want to install the active database. **Note:** It must be the same server on which the master database is installed.	
31.	Database name	Name of the active database. The installation program creates a database with the name you provide here.	
32.	Server instance name	Name of the MSSQL Server instance to be used while creating the database. This should match the value set for the master database instance name. **Note:** You can skip configuring this field when the value of the Server name field is set as the Listener name.	

#	Field Name	Description	Value
33.	Database listener port	Port number of MSSQL Server or the Listener Name. This should match the value set for the master database.	1433/1444
34.	Datafile path	Path to the folder on the database server, where you want to create the data file. For example, `C:\MSSQL\Data`.	
35.	Datafile initial size (MB)	Minimum size of the data file for the database.	2048
36.	Datafile maximum size (MB)	Maximum size of the data file for the database.	Unlimited
37.	Datafile increment size (MB)	Additional file size limit that will be allocated to the database after the initial size is full.	500
38.	Logfile initial size (MB)	Minimum size of the log file.	1024
39.	Logfile maximum size (MB)	Maximum size of the log file.	Unlimited
40.	Database administrator user name	User name of the database administrator for MSSQL Server. If you have created a separate user for installing Enterprise Chat and Email databases, provide the name of that user (page 40). **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
41.	Database administrator password	Password of the database administrator. **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
42.	Cisco Database user name	User name required to connect to the database. The installation program will create this user. **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
43.	Cisco Database password	Password for the database user. **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
Active Database Filegroup Parameters			
44.	Filegroup Datafile 1 Name	Provide the name of the first file group to be created for the active database.	
45.	Filegroup Datafile 1 Path	Provide the location for the first filegroup. Make sure you provide the path to the drive that is created for storing file groups.	
46.	Filegroup Datafile 2 Name	Provide the name of the second file group to be created for the active database.	
47.	Filegroup Datafile 2 Path	Provide the location for the second filegroup. Make sure you provide the path to the drive that is created for storing file groups.	
48.	Filegroup Datafile 3 Name	Provide the name of the third file group to be created for the active database.	
49.	Filegroup Datafile 3 Path	Provide the location for the third filegroup. Make sure you provide the path to the drive that is created for storing file groups.	

#	Field Name	Description	Value
50.	Filegroup Datafile 4 Name	Provide the name of the fourth file group to be created for the active database.	
51.	Filegroup Datafile 4 Path	Provide the location for the fourth filegroup. Make sure you provide the path to the drive that is created for storing file groups.	
Reports Database Parameters			
52.	Server name	Name of the local or remote server on which the reports database should be installed. If you are using MSSQL Server **Always On Availability Group** clustering, specify the Listener name for the reports database (page 146). **Note:** Make sure you provide the DNS host name and not the IP address of the server.	
53.	Database name	Name of the reports database. The installation program creates a database with the name you type here.	
54.	Database server instance	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. ▸ If you are using MSSQL Server **Always On Availability Group** clustering, provide the name of the Listener instance. ▸ **Note:** You can skip configuring this field when the value of the Server name field is set as the Listener name.	
55.	Database listener port	Port number of the MSSQL Server or the Listener Name.	1433/1444
56.	Datafile path	Path to the folder on the database server, where you want to create the data file. For example, `D:\MSSQL\Data`.	
57.	Datafile initial size (MB)	Minimum size of the data file for the database.	1024
58.	Datafile maximum size (MB)	Maximum size of the data file for the database.	Unlimited
59.	Datafile increment size (MB)	Additional file size limit that will be allocated to the database after the initial size is full.	500
60.	Logfile initial size (MB)	Minimum size of the log file.	512
61.	Logfile maximum size (MB)	Maximum size of the log file.	Unlimited
62.	Database administrator user name	User name of the database administrator for MSSQL Server. If you have created a separate user for installing Enterprise Chat and Email databases, provide the name of that user (page 40). **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
63.	Database administrator password	Password of the database administrator. **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	

#	Field Name	Description	Value
64.	Cisco Database user name	User name required to connect to the reports database. The installation program will create this user. **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
65.	Cisco Database password	Password for the database user. **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
Reports Database Filegroup Parameters			
66.	Filegroup Datafile 1 Name	Provide the name of the first file group to be created for the reports database.	
67.	Filegroup Datafile 1 Path	Provide the location for the first filegroup. Make sure you provide the path to the drive that is created for storing file groups.	
68.	Filegroup Datafile 2 Name	Provide the name of the second file group to be created for the reports database.	
69.	Filegroup Datafile 2 Path	Provide the location for the second filegroup. Make sure you provide the path to the drive that is created for storing file groups.	
70.	Filegroup Datafile 3 Name	Provide the name of the third file group to be created for the reports database.	
71.	Filegroup Datafile 3 Path	Provide the location for the third filegroup. Make sure you provide the path to the drive that is created for storing file groups.	
72.	Filegroup Datafile 4 Name	Provide the name of the fourth file group to be created for the reports database.	
73.	Filegroup Datafile 4 Path	Provide the location for the fourth filegroup. Make sure you provide the path to the drive that is created for storing file groups.	
Domain User Account Parameters			
74.	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 33. User name should be provided in the format: `Domain\username`	
75.	Domain user password	Password for the domain user.	

Database server details

Web Server Details

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 VMs" on page 44.

#	Field Name	Description	Value
Application Server Parameters			
1.	Application server name	Type the name of the application server for which you want to configure the web server. **Note:** Make sure you provide the DNS host name and not the IP address of the server.	
2.	Jetty HTTP Port	Jetty HTTP listener port of the application server where all the HTTP requests are handled. **Note:** This port should match the port number provided while installing the application server (page 80).	
Enterprise Chat and Email Directory			
3.	Enterprise Chat and Email Home Directory	Provide the path of the directory where you would like to install ECE. For example, *Install_Drive*`\Cisco.` **Note:** Make sure that the path and folder name do not contain any of the following characters: *?<>|+^'"%`,@	
IIS Web Site Parameters			
4.	IIS Web Site Name	Name of the IIS Web Site on which the application is to be configured.	Default Web Site
Cisco Application Context Root			
5.	Context Root Name	Provide the same context root name which was provided at the time of installing the Cisco database server (page 72).	
Cisco Partition Name			
6.	Partition Name	Provide the name for the business partition. Make sure you provide the same name which was provided at the time of installing the Cisco database server (page 72).	
Domain User Account Parameters			
7.	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 33. User name should be provided in the format: `Domain\username`	
8.	Domain user password	Password for the domain user.	

Web server details

Messaging Server Details

The installation program automatically installs and configures JDK and ActiveMQ as part of the installation. These software are installed in the *ECE Home* directory. For example, *Install_Drive*\Cisco\jdk.

#	Field Name	Description	Value
File Server Parameters			
1.	File Server name/NAS Path/ DFS Path	The fully qualified domain name of the file server. If the file server is installed on a NAS device or DFS, provide the path to the shared folder. For example, \\SharedSpace\Cisco. **Note:** NAS is supported on non-HA environment while DFS is supported on HA environment. Make sure you provide the DNS host name and not the IP address of the server.	
Enterprise Chat and Email Home Directory			
2.	Enterprise Chat and Email Home Directory	Provide the path of the directory where you would like to install Enterprise Chat and Email. For example, *Install_Drive*\Cisco. The installation program also installs ActiveMQ and JDK at the same location. **Note:** Make sure that the path and folder name do not contain any of the following characters: *?<>|+^'"%`,@	
ActiveMQ Parameters			
3.	ActiveMQ Port	ActiveMQ listener port used by JMS clients to connect to ActiveMQ messaging server. The port number can be between 1024-65535.	15097
4.	Admin ActiveMQ Port	ActiveMQ Admin listener port used for administering and monitoring resources on the server. The port number can be between 1024-65535.	15096
Domain User Account Parameters			
5.	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 33. User name should be provided in the format: Domain\username	
6.	Domain user password	Password for the domain user.	

Messaging server details

Application Server Details

The installation program automatically installs and configures JDK and Jetty as part of the installation. These software are installed in the *ECE Home* directory. For example, *Install_Drive*\Cisco\jdk.

#	Field Name	Description	Value
File Server Parameters			
1.	File Server name/ NAS Path/ DFS Path	The fully qualified domain name of the file server. If the file server is installed on a NAS device or DFS, provide the path to the shared folder. For example, \\SharedSpace\Cisco **Note:** NAS is supported on non-HA environment while DFS is supported on HA environment. Make sure you provide the DNS host name and not the IP address of the server.	
Enterprise Chat and Email Home Directory			
2.	Enterprise Chat and Email Home Directory	Provide the path of the directory where you would like to install ECE. For example, *Install_Drive*\Cisco. The installation program also installs Jetty and JDK at the same location. **Note:** Make sure that the path and folder name do not contain any of the following characters: *?<>|+^'"%`,@	
Jetty Parameters			
3.	Jetty HTTP port	Jetty HTTP listener port where all the HTTP requests are handled. The port number can be between 1024-65535.	9001
4.	Jetty HTTP SSL Port	Jetty HTTPS listener port where all the SSL requests are handled. The port number can be between 1024-65535.	9002
5.	Jetty Stop Port	Jetty shutdown command listener port. This port is used for issuing shutdown command to stop Jetty. The port number can be between 1024-65535.	15095
Domain User Account Parameters			
6.	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 33. User name should be provided in the format: Domain\username	
7.	Domain user password	Password for the domain user.	

Application server details

Services Server Details

The installation program automatically installs and configures JDK as part of the installation. JDK is installed in the *ECE Home* directory. For example, *Install_Drive*\Cisco\jdk.

#	Field Name	Description	Value
File Server Parameters			
1.	File Server name/NAS Path/ DFS Path	The fully qualified domain name of the file server. If the file server is installed on a NAS device or DFS, provide the path to the shared folder. For example, \\SharedSpace\Cisco **Note:** NAS is supported on non-HA environment while DFS is supported on HA environment. Make sure you provide the DNS host name and not the IP address of the server.	
Enterprise Chat and Email Home Directory			
2.	Enterprise Chat and Email Home Directory	Provide the path of the directory where you would like to install ECE. For example, *Install_Drive*\Cisco. The installation program also installs JDK at the same location. **Note:** Make sure that the path and folder name do not contain any of the following characters: *?<>|+^'"%`,@	
RMI and RMID Parameters			
3.	RMI registry port	Port number used by the Remote Method Invocation (RMI) registry naming service.	15099
4.	RMI activation port	Port number used by the RMI Daemon Process.	15098
Organization Information			
5.	Name	Provide the name of the organization. Make sure that the name does not contain any special characters.	
6.	Business Unit	Provide the business unit name. Make sure that the value does not contain any special characters.	
7.	Location	Provide the location of your organization. Make sure that the value does not contain any special characters.	
8.	Country	Select the country from the dropdown list.	
Domain User Account Parameters			
9.	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 33. User name should be provided in the format: Domain\username	
10.	Domain user password	Password for the domain user.	

Services server details

5 Post-Installation Tasks

- Configuring Permissions on IIS Config Folder
- Assigning Permissions on ECE Home Directory
- Configuring SSL for Secure Connections
- Always On Availability Group Clustering Tasks
- Creating an Encrypted SQL Server Database
- Configuring SMTP Server Relay Address List
- Configuring Finesse
- Configuring Single Sign-On
- Starting ECE
- Stopping ECE
- Signing in to ECE
- Integrating ECE with Packaged CCE
- Configuring Important Settings
- Configuring Clickjacking Protection

- Adding Data Source in CUIC for ECE Reports
- 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 45). Ensure that the user account that you used for installing the application (page 33) has **read** permissions on the following folder on the web server: `%systemroot%\system32\inetsrv\config.`

Assigning Permissions on ECE Home Directory

The **Service Account** created for running the ECE application needs **Full Control** permission on the ECE home directory. You must perform this task on the file server *before* starting the application.

To assign permissions on the ECE home directory:

1. Right-click the ECE home directory.
2. Select **Properties**.
3. In the Properties window, go to the Sharing tab and click **Advanced Sharing.**
4. In the Advanced Sharing window, click **Permissions**.
5. In the Permissions window, click the **Add** button and add the **Service Account** (page 33) created for ECE. Assign the **Full Control** permission to the user.

- Click **Apply**.

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 126 for details.

Always On Availability Group Clustering Tasks

- Perform all the tasks listed in "Post-Installation Tasks" on page 148.

Creating an Encrypted SQL Server Database

This is an optional task and you need to do it only if you want to encrypt the databases. This feature is available only for the Enterprise edition of MSSQL. You can do this task any time after installing the ECE application.

If you are using **Always On Availability Group** clustering, perform this task on all the nodes.

Encrypting Primary Node

Perform these tasks on the primary node.

To create an encrypted SQL server database:

1. Create a master key in the master database. This key is then used to create the server certificate that can be used to secure the database encryption key. Connect to the master database and run the following query.

```
USE master
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'company@123'
GO
```

2. Backup the master key. This creates a certificate in the master database.

```
BACKUP MASTER KEY TO FILE = 'c:\temp\masterkey'
    ENCRYPTION BY PASSWORD = 'company@123'
GO
```

3. Now create the server certificate database encryption key ("DEK").

```
USE master
GO
CREATE CERTIFICATE DEKCert WITH SUBJECT = 'DEK Certificate'
GO
```

4. Create a backup of the server certificate database encryption key (“DEK”).

```
BACKUP CERTIFICATE DEKCert TO FILE = 'c:\DEKCert'
WITH PRIVATE KEY ( FILE = 'c:\temp\DEKCertPrivKey' ,
ENCRYPTION BY PASSWORD = 'company@123' )
GO
```

5. Create database encryption key for the database where you wish to configure transparent data encryption. In the following query, *eGActiveDB_name* is the name of the active database.

```
USE eGActiveDB_name
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_128
ENCRYPTION BY SERVER CERTIFICATE DEKCert
```

```
GO
```

You now have all the prerequisites for enabling transparent data encryption, so database encryption can be enabled.

6. Enable database encryption. Run the following query where *eGActiveDB_name* is the name of the active database.

```
ALTER DATABASE eGActiveDB_name SET ENCRYPTION ON
```

By setting encryption on, a background task starts encrypting all the data pages and the log file. This can take a considerable amount of time, depending on the size of the database.

Database maintenance operations should not be performed when this encryption scan is running.

7. To query the status of the database encryption and its percentage completion, query the new `sys.dm_database_encryption_keys DMV`.

```
SELECT DB_NAME(e.database_id) AS DatabaseName,
       e.database_id,
       e.encryption_state,
   CASE e.encryption_state
        WHEN 0 THEN 'No database encryption key present, no encryption'
        WHEN 1 THEN 'Unencrypted'
        WHEN 2 THEN 'Encryption in progress'
        WHEN 3 THEN 'Encrypted'
        WHEN 4 THEN 'Key change in progress'
        WHEN 5 THEN 'Decryption in progress'
   END AS encryption_state_desc,
      c.name,
      e.percent_complete
   FROM sys.dm_database_encryption_keys AS e
   LEFT JOIN master.sys.certificates AS c
   ON e.encryptor_thumbprint = c.thumbprint
```

Encrypting Other Nodes

To encrypt other nodes:

1. Copy the `c:\temp` folder from the first node to the other nodes.
2. Create a master key in the master database. This key is then used to create the server certificate that can be used to secure the database encryption key. Connect to the master database and run the following query.

```
USE master
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'company@123'
GO
```

3. Now create the server certificate.

```
USE master
GO
CREATE CERTIFICATE TDE_Test_Cert FROM FILE = 'c:\temp\DEKCert'
WITH PRIVATE KEY (FILE = 'c:\temp\DEKCertPrivKey',
DECRYPTION BY PASSWORD = 'company@123'); GO
```

4. Enable database encryption. Run the following query where *eGActiveDB_name* is the name of the active database.

```
ALTER DATABASE eGActiveDB_name SET ENCRYPTION ON
```

   By setting encryption on, a background task starts encrypting all the data pages and the log file. This can take a considerable amount of time, depending on the size of the database.

   Database maintenance operations should not be performed when this encryption scan is running.

5. To query the status of the database encryption and its percentage completion, query the new `sys.dm_database_encryption_keys DMV`.

```
SELECT DB_NAME(e.database_id) AS DatabaseName,
       e.database_id,
       e.encryption_state,
   CASE e.encryption_state
        WHEN 0 THEN 'No database encryption key present, no encryption'
        WHEN 1 THEN 'Unencrypted'
        WHEN 2 THEN 'Encryption in progress'
        WHEN 3 THEN 'Encrypted'
        WHEN 4 THEN 'Key change in progress'
        WHEN 5 THEN 'Decryption in progress'
   END AS encryption_state_desc,
      c.name,
      e.percent_complete
   FROM sys.dm_database_encryption_keys AS e
   LEFT JOIN master.sys.certificates AS c
   ON e.encryptor_thumbprint = c.thumbprint
```

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.**

Configuring Finesse Files

You need to perform these tasks only if you are using a load balancer for the web servers.

To configure the ece_config.js file:

1. On the ECE web server, open the *ECE_Home*`\eService\templates\finesse\gadget\agent\ece_config.js` file in a text editor.
2. Locate the following property in the file: `var web_server_name =`
3. Replace the value of the property with the host name of the load balancer used for the installation.

Configuring Finesse Settings and Layout

Perform these tasks from any local machine. You will need access to the following `xml` files on the ECE web server:

- *ECE_Home*`\eService\templates\finesse\gadget\layout:`
  - `agent.xml`
  - `solve.xml`
  - `cobrowse.xml`

For 4000 and 12000 Agent Deployments

To configure the Finesse settings and layout:

1. Launch the CCE Web Administration page, using the URL: `https://`*Server_Name*`/cceadmin/`. Login using the administrator credentials.
2. Go to **Infrastructure Settings > Device Configuration.**
3. In the **Device Configuration** space, in the left menu, click **Finesse** and configure the following:
   - In the CTI server settings tab, configure the Contact Center CTI Server Settings.
   - In the Enterprise and database settings tab configure the Contact Center Enterprise Administration & Data Server Settings.
4. Go to **Desktop > Resources** to open the Resources space.

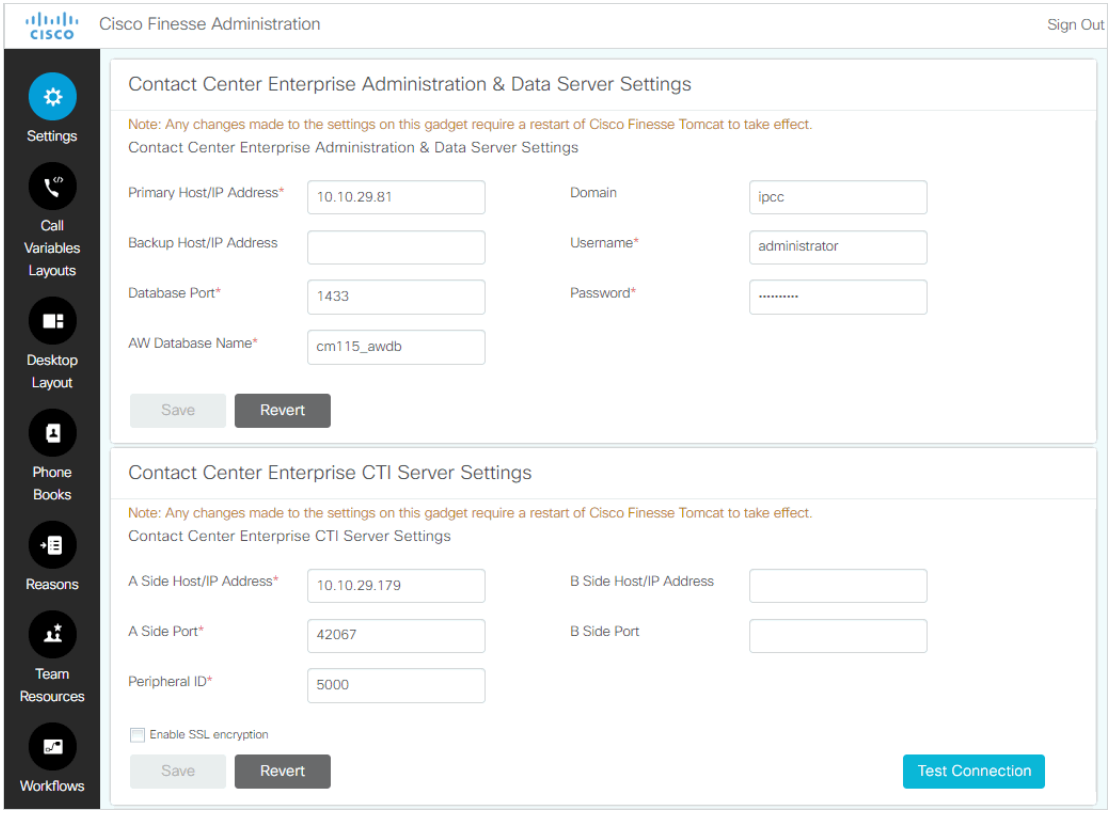
5. In the Desktops Layout tab, configure the layout for ECE, Solve, and Cobrowse gadgets. XML contents for the ECE, Solve, and Cobrowse gadget tabs are available in the following files on the ECE web server:
   - *ECE_Home*`\eService\templates\finesse\gadget\layout\agent.xml`: After copying the content of the `agent.xml` file, in the `gadget` tag, replace the web server name with the host name of the load balancer used for ECE web servers. This task needs to be performed only if you are using a load balancer for ECE web servers.
   - *ECE_Home*`\eService\templates\finesse\gadget\layout\solve.xml:` After copying the content of the `solve.xml` file, make the following changes in the `gadget` tag:
     i. Replace `EGAIN_WEBSERVER_OR_LOADBALANCER` with the eGain Solve for Cisco web server. If the installation has more than one web servers, provide the name of the load balancer.
     ii. Replace `CONTEXT_ROOT` with the context root of eGain Solve for Cisco.
   - *ECE_Home*`\eService\templates\finesse\gadget\layout\cobrowse.xml`: You need to configure this only if you are using the Cobrowse gadget in Finesse. After copying the content of the `cobrowse.xml` file, make the following changes in the in the `gadget` tag:
     i. Replace the `EGAIN_WEBSERVER_OR_LOADBALANCER` with the eGain Solve for Cisco web server. If the installation has more than one web servers, provide the name of the load balancer.
     ii. Replace the `CONTEXT_ROOT` with the context root of eGain Solve for Cisco.

For 2000 Agent Deployments

To configure the Finesse settings and layout:

1. Launch the URL: `https://`*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. To configure a secure connection, select the **Enable SSL encryption** option in the Contact Center CTI Server Settings section and provide the secure ports. For details about doing this configuration, see the *Cisco Finesse Administration Guide*.



Configure the settings

3. From the Desktops Layout section, configure the layout for ECE, Solve, and Cobrowse gadgets. For details, see Step 5 on page 89.

Configuring Single Sign-On

- Single sign-on is available for all users of the application. For details about doing this task, see the *Enterprise Chat and Email Administrator's Guide (For PCCE).*
  - Single sign-on must be configured for all partition users of the application.
  - If you are planning to use single sign-on while accessing any of the ECE consoles outside of Finesse, you must also complete the tasks in the section: "Single Sign-On Configuration" on page 100.

Starting ECE

There is no mandatory sequence that should be followed while starting ECE. All the VMs on which components are installed should be running and available on the network.

Important: **Run the application using the same domain account that was used for installing the application (page 33).**

To start ECE:

If you get the following error while starting the Cisco Service, see "Troubleshooting Application Start-Up Issues" on page 91: `Error 1069: The service did not start due to login failure.`

Important: **The CISCO service cannot be restarted via the Windows Service Manager. Instead, to restart the service, you can stop it and then start it again. Additionally, when stopping the services, please ensure all Java processes are terminated gracefully before restarting the services. This ensures that new processes are spawned without any issues when the ECE service is restarted, allowing the application to start successfully.**

- In collocated installation:
  - On the server where application, messaging, services, file, and database components are installed, start the Cisco Service from the Windows Services panel.
- In a distributed-server installation:

  Ensure that all the VMs in the configuration are available and connected to the network.

  a. Start Cisco Service on the messaging server by starting the Cisco Windows service from the Windows Services panel. If you have installed a cluster of messaging servers, you would need to start the application on all the servers in the cluster.

  b. On each services server, start the application by starting the Cisco Windows service from the Windows Services panel.

  c. On each application server, start the application by starting the Cisco Windows service from the Windows Services panel.

Troubleshooting Application Start-Up Issues

Perform these tasks if you get the following error while starting the Cisco 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 33) 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.

In a distributed environment, stop the application on the following servers. There is no mandatory sequence that should be followed while stopping the application.

- The application servers
- The messaging servers
- The services servers

To stop ECE:

- In a collocated installation:
  - On the server where application, web, messaging, services, file, and database components are installed, stop the Cisco Service from the Windows Services panel.
- In a distributed-server installation:
  a. On each application server VM, stop the Cisco Service from the Windows Services panel. Open the Windows Task Manager and verify that none of the `java` processes are running.
  b. On the messaging server VM, stop the Cisco Service from the Windows Services panel. If you have installed a cluster of messaging servers, you would need to stop the application on all the servers in the cluster. Open the Windows Task Manager and verify that none of the `java` processes are running.
  c. On each services server VM, stop the Cisco Service from the Windows Services panel. If you have installed two services servers, stop the application on both servers. Open the Windows Task Manager and verify that none of the `java` processes (the services) are running.

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.

Integrating ECE with Packaged CCE

Integration between ECE and Packaged CCE is enabled and configured through the Enterprise Chat and Email administration space in the Unified CCE Administration.

To integrate ECE with Packaged CCE:

1. In the global-level Top menu, click the **Integration** option.
1. In the Left menu, navigate to **Unified CCE > Unified CCE**.In the Unified CCE Details space, In Unified CCE Administration, in the Enterprise Chat and Email administration space, in the global-level Top menu, click the **Integration** option.
2. In the Left menu, navigate to **Unified CCE > Unified CCE.**
3. In the Unified CCE Details space, on the AWDB Details tab, provide information for the following fields under the Primary AWDB section. If any of these configurations change at a later point in Packaged CCE, you must update the details here as well.
   - **Authentication:** Select from **Windows Authentication** or **SQL Authentication.**
   - **Unified CCE administration host name:** The server name or IP address of the Packaged CCE host.
   - **Active:** Click this toggle to enable the configuration.
   - **SQL server database name:** The name of the AWDB database.
   - **Port number:** Set the value to match the port configured in Packaged CCE. By default the value is set to 1433.
   - **Database administrator login name:** The database administrator's user name. This value needs to be set only when using **SQL Authentication.**

- **Database administrator login password:** The database administrator password. This value needs to be set only when using **SQL Authentication.**
- **Maximum capacity:** The maximum number of allowed connections to be made to the AWDB. By default, this is set to 360.

4. If you have a secondary AWDB and wish to apply it to your integration, provide the necessary details in the Secondary AWDB section.
5. Click the **Save** button.

Note: For PCCE 2K deployment, application Instance with the name "MultiChannel" is created automatically and is required while integrating with ECE via Administration console.
For 4K/12K deployment, an application instance is created manually, and there is no restriction on the nomenclature for the application instance. The process is same as of integrating ECE with UCCE.

6. On the Configuration tab, set the following:
   - **Application Instance:** Select an instance from the dropdown field.
   - **Agent Peripheral Gateways:** Click the **Search and Add** button to add any desired gateways for agent peripherals.

Important: **When you save your changes, your system is permanently connected to your Packaged CCE installation. This cannot be undone.**

7. Click the **Save** button. Your system is now connected with Packaged CCE. To complete the integration, you must import the MRDs and users from the Packaged CCE system. For details about doing this task, see the *Enterprise Chat and Email Administrator's Guide.*

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 global 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 global level

Navigate to **Partition > Apps > General Settings** and configure the following setting:

- External URL of Application

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

- Default SMTP Server Settings

Note: When upgrading to ECE15 from ES9 or earlier versions, make sure you regenerate the authentication token if the Default SMTP Server Settings are configured to use OAuth authentication with a Microsoft Office 365 registered app. This step is not required if the Default SMTP Server Settings are configured with Basic Authentication or if you are using Gmail.

- 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 global level

- Customer departmentalization
- Session time out
- Inactive time out
- Chat auto-pushback settings

At the department level

- Business calendar time zone
- Autopushback time (minutes after logout)

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

Configuring Clickjacking Protection

About Clickjacking Protection

Clickjacking is a malicious technique of tricking a web user into performing an unwanted action unintentionally by rendering invisible page elements like hyperlinks underneath legitimate clickable content. These attacks are done to reveal confidential and sensitive information or to gain control of the victim's system.

The Clickjacking Protection is a self-service feature. It provides an option to configure the desired domains that are allowed to embed the applications like ECE Agent Console, in an iframe, in the Finesse Desktop.

Configuring Clickjacking Protection

In the Web Server, IIS Outbound rules can now be modified manually to allow framing for desired parent domains only.

To configure clickjacking protection:

1. On the web server, 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 browse to **Sites >** *Web_Site_Name*. Please note that the *Web_Site_Name* would be the IIS website used for ECE deployments.
3. In the Actions pane on the right, from the Edit Site section, click the **Basic Settings**... link.
4. In the Edit Site window, the Physical Path field defines the path for the **web.config** file.
5. Browse to the location on your local drive and open the **web.config** file in a text editor.
6. To allow domain1\.com and domain2\.com, replace all occurrences of following string: **wsname=((http[s]?)(:|%3A)(/|%2F)(/|%2F)([_0-9a-z-.@:%_\+~#=]*))** with the following string: **wsname=((http[s]?)(:|%3A)(/|%2F)(/|%2F)([a-z0-9.]+?)(domain1\.com|domain2\.com)(&|%26|$))**

   Note that the domains to be allowed are specified in simple brackets and are separated by the | character.
7. Save changes to the file.
8. Restart IIS.

In the IIS Manager, verify that for all the outbound rules that are applied to the headers or the content of the HTTP response, the **wsname** query parameter has been updated.

Adding Data Source in CUIC for ECE Reports

The following ECE reports can be accessed in the Cisco Unified Intelligence Center (CUIC) via historical templates:

- Chat Volume by Queue
- Email Volume By Queue

- Agent Work Summary

To access these reports from CUIC, you need to add the ECE Reports Database as a data source in CUIC.

Creating a Database User on ECE Reports Database

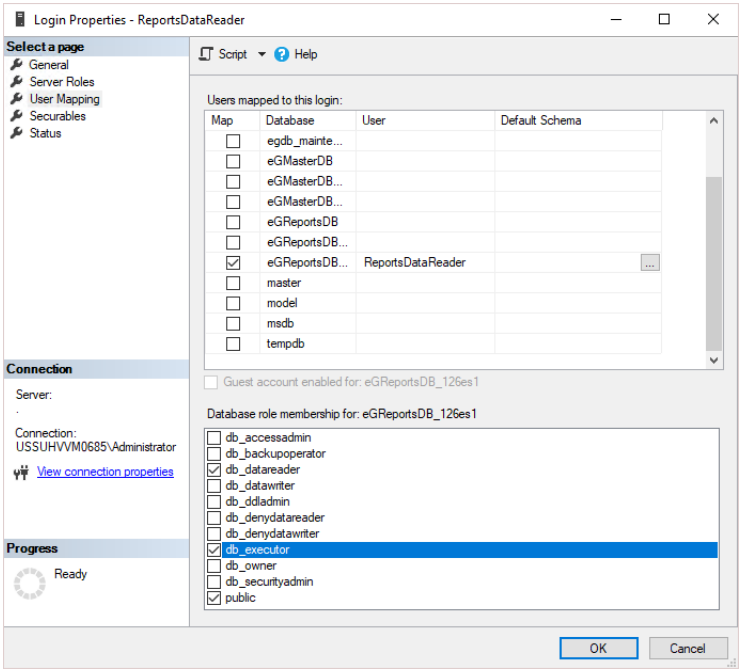
If the reports database is part of the always-on group, create the database login with the same name on all nodes of the cluster starting with the current primary node and map database login to reports database of each node. Refer to the Microsoft documentation for maintaining SQL logins and permissions for user databases in always on cluster.

To create a database user on ECE reports database:

1. Create a SQL login on the reports database server, for example, `ReportsDataReader`.
2. Create a new role on the reports database server:

```
CREATE ROLE db_executor;
GRANT EXECUTE TO db_executor;
```

3. Map the user to the ECE reports database and set the **Default Schema** as **dbo**.
4. Assign the following database role memberships to the database user `ReportsDataReader`:
   - `public`
   - `db_datareader`
   - `db_executor`



Create a database user

Adding Data Source in CUIC for ECE Reports

See the Cisco Unified Intelligence Center Report Customization Guide for steps on adding a data source in CUIC.

Make sure you set the following values on the data source details page:

- In the **Datasource Host** field, provide the name of the server where the ECE reports database is installed. In case of always on cluster for reports database, connect to the reports database using always on default cluster name or load balancer name.
- In the **Database name** field, provide the name of the ECE reports database.
- In the **Database User ID** field, provide the name of the SQL user created on the ECE reports database server (page 97).

Uninstalling ECE

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

- Application Server
- Messaging Server
- Services Server
- Web Server
- File Server

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

- The databases
- The following folders on the file server:
  - *ECE_HOME*`\eService\storage`
  - *ECE_HOME*`\eService\logs`

Important: **After the uninstaller runs on all the servers, you must delete these components manually to make the servers ready for the reinstallation of ECE on the same servers.**

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 92.

Stopping IIS

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

Uninstalling ECE

To uninstall ECE:

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, `populatesmy_`*eGReportsDB*.
8. On the file server, manually delete the following folders:
   - *ECE_HOME*`\eService\storage`
   - *ECE_HOME*`\eService\logs`

Performing Post Uninstallation Tasks

Starting IIS

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

6 Single Sign-On Configuration

- About Single Sign-On with Cisco IDS
- Configuring Single AD FS Deployment
- Configuring Split AD FS Deployment
- Configuring Single Sign-On in ECE

Important: **Perform these tasks only if you are planning to use single sign-on while accessing any of the ECE consoles outside of Finesse.**

About Single Sign-On with Cisco IDS

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 101).
- **Split AD FS:** In a split AD FS deployment, Resource Federation Server and Account Federation Server are installed on separate machines (page 109).

Configuring Single AD FS Deployment

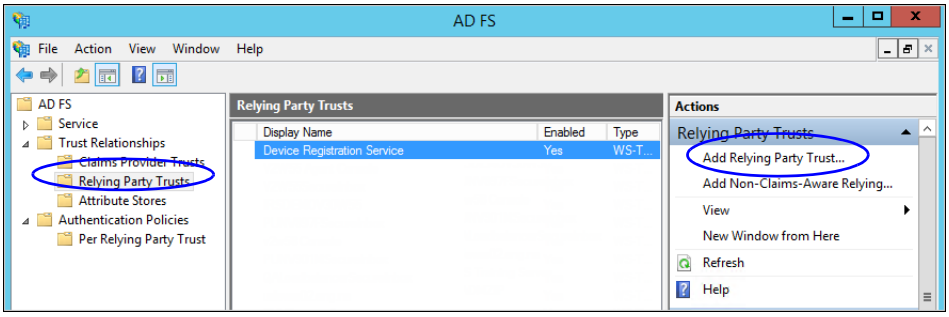
In a single AD FS deployment, Resource Federation Server and Account Federation Server are installed on the same machine.

Configuring Relying Party Trust for ECE

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

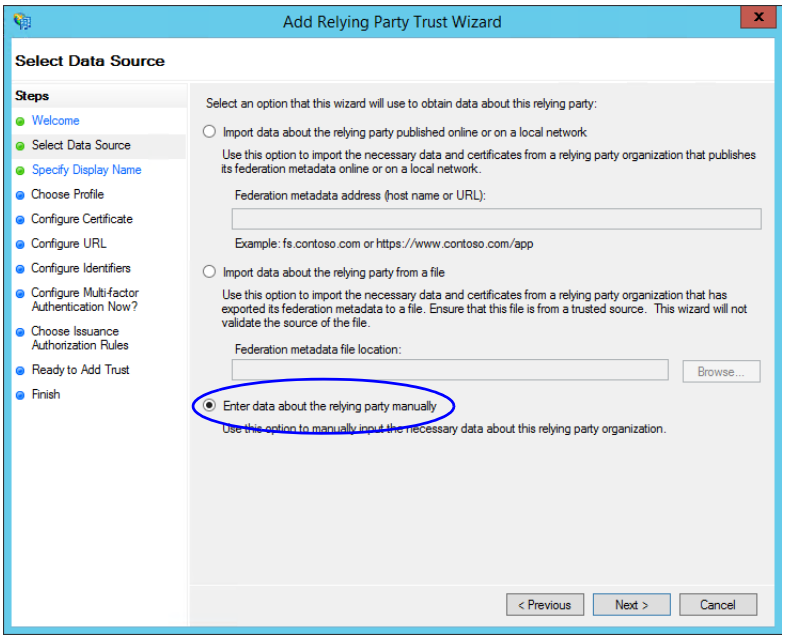
To configure relying party trust for ECE in single AD FS:

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...**



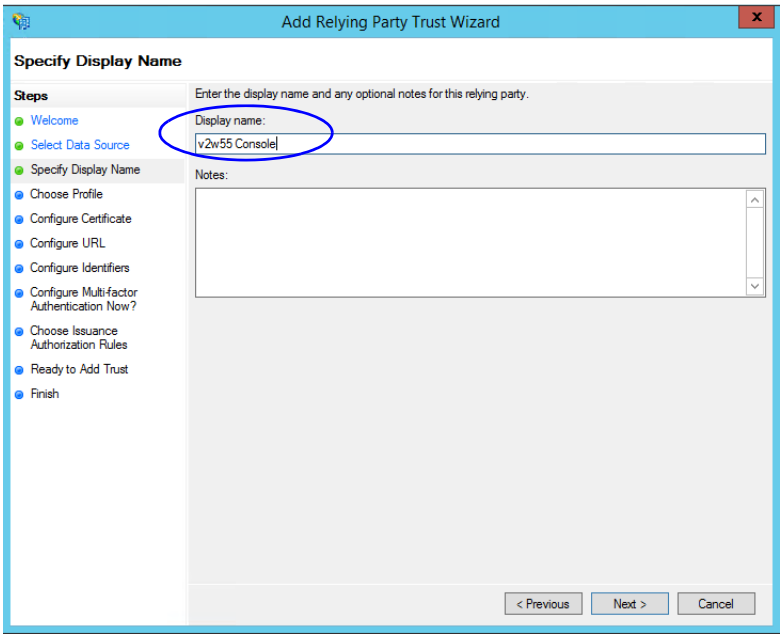
4. In the Add Relying Party Trust Wizard that appears, do the following:
   a. On the Welcome screen, click **Start.**

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



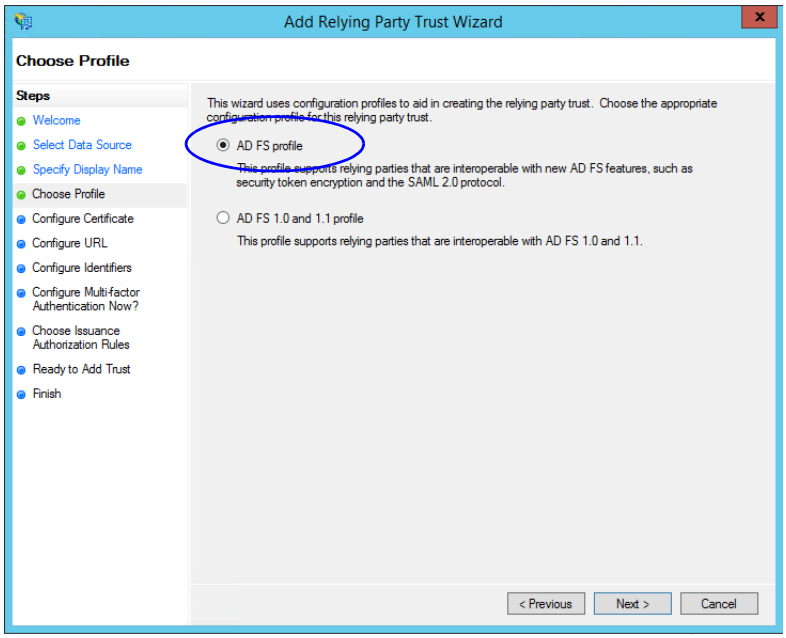
Select the Enter data about the reply party manually option

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**.



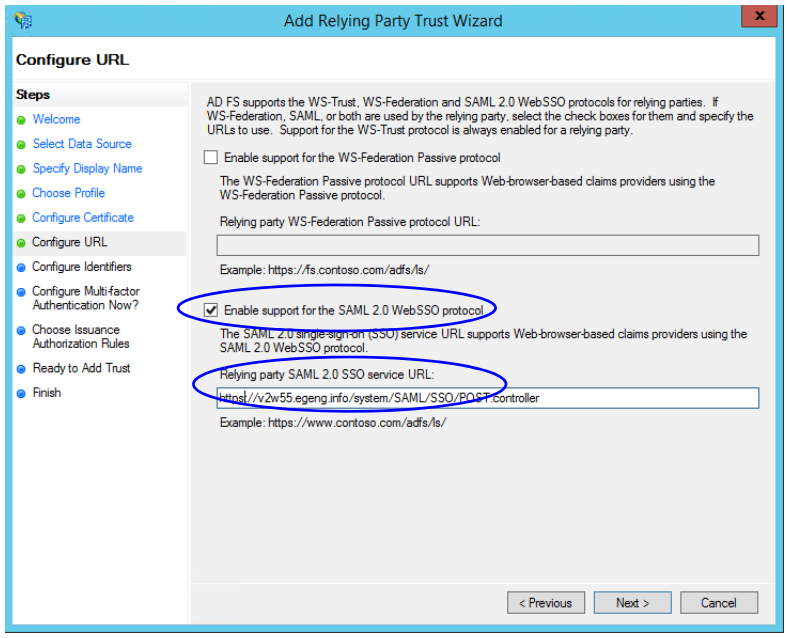
Select AD FS profile

e. On the Configure Certificate screen, click **Next.**

f. On the Configure URL screen, set the following:

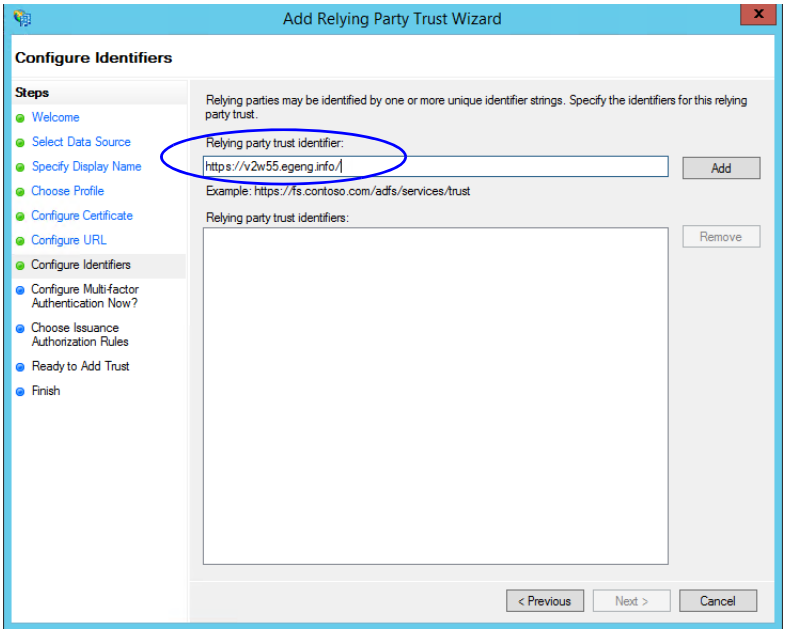
i. Select the **Enable support for the SAML 2.0 Web SSO protocol** option.

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

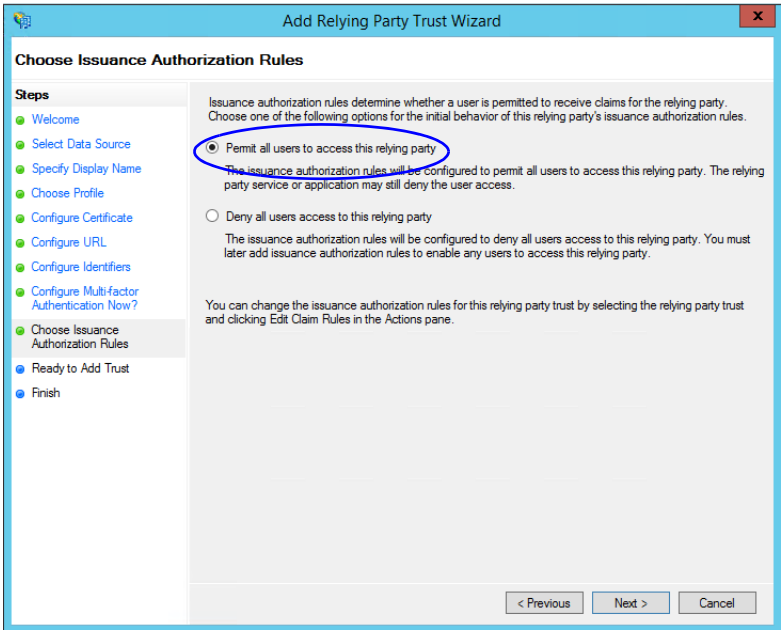
g. On the Configure Identifiers screen, provide the **Replying party trust identifier** and click **Add**. Value should be in the format: `https://`*Web_Server_Or_Load_Balancer_Server*`/`. Replace *Web_Server_Or_Load_Balancer_Server* with the ECE web server name or the Load balancer server name. Click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



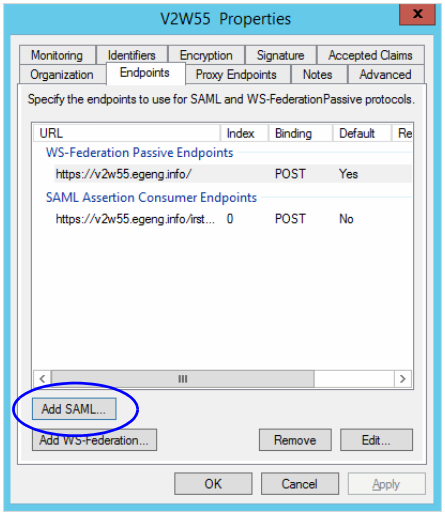
Select the Permit all users to access this relying party option

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.



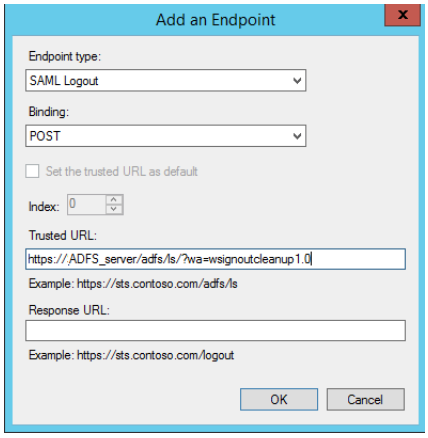
Click Add SAML

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.**



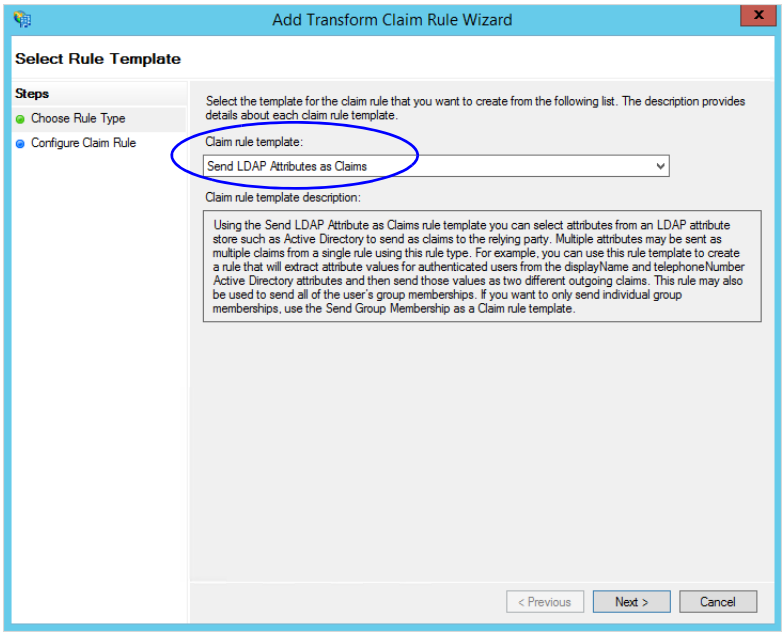
Create an end point

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**.

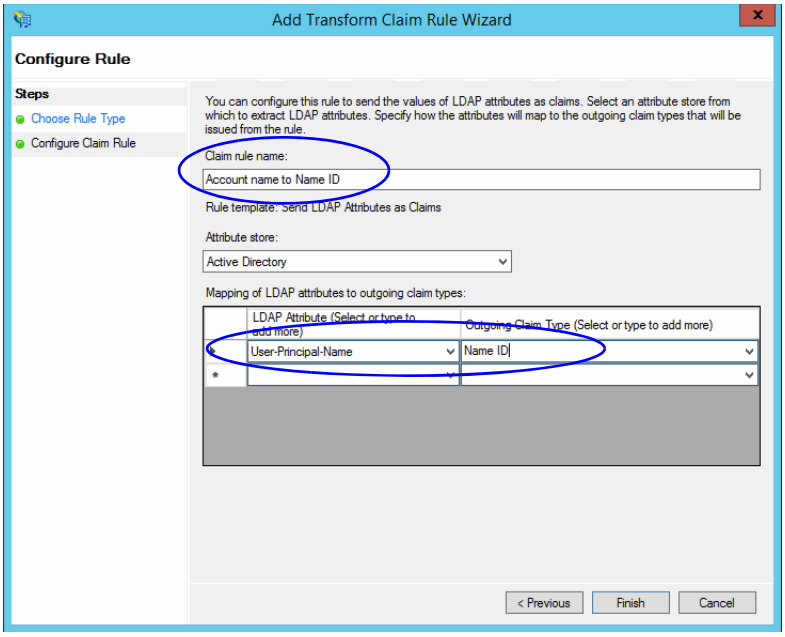


Select the claim rule template

   b. On the Configure Rule screen, set the following:

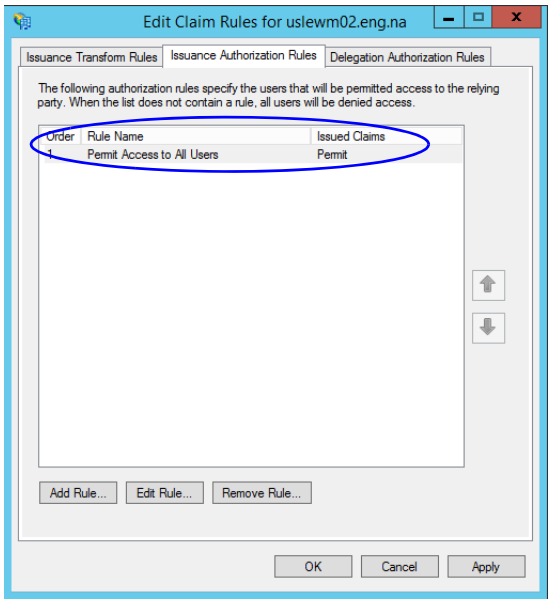
      i. Provide the Claim rule name.

      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.



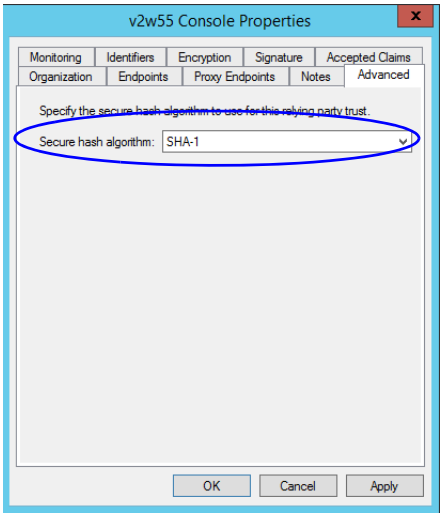
Configure the rule

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.



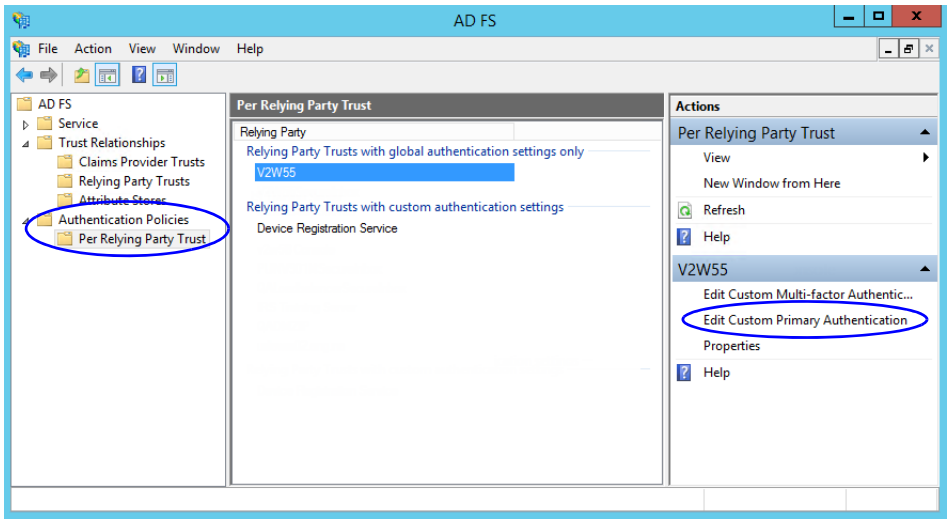
Check the authorization rules

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.



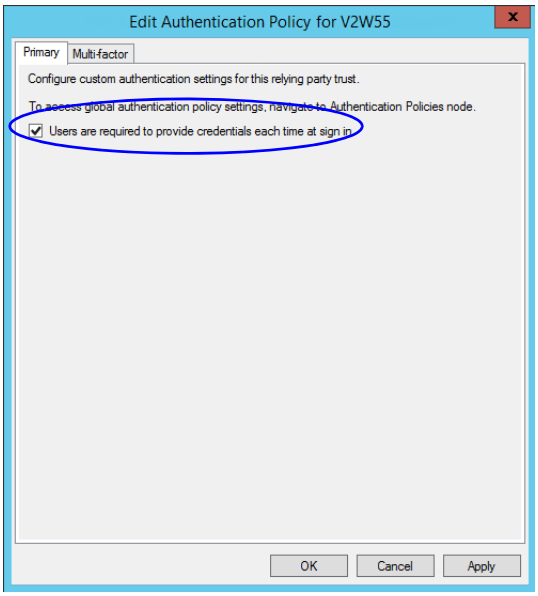
Set the secure hash algorithm

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 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

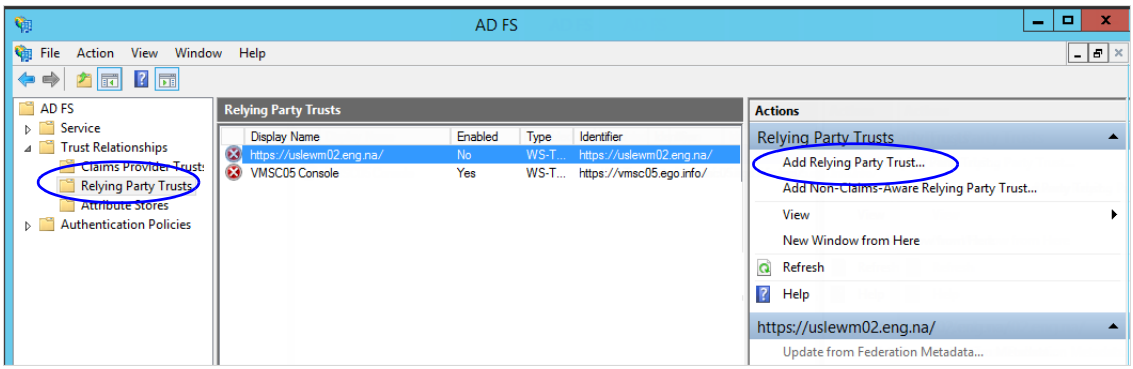
- If Customer AD FS and Shared AD FS are installed in different domain, you need to add certificates of the domains to the **Trusted Root Certification Authorities** store of the servers. On the Customer AD FS server, add the certificate of the Shared AD FS and vice versa. Contact your IT department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

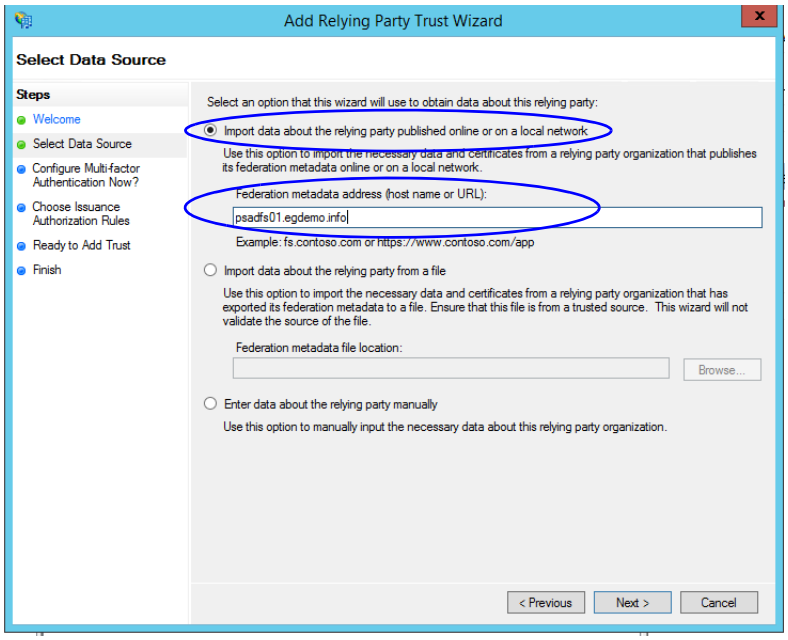
To configure replying party trust for shared AD FS in customer AD FS:

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...**



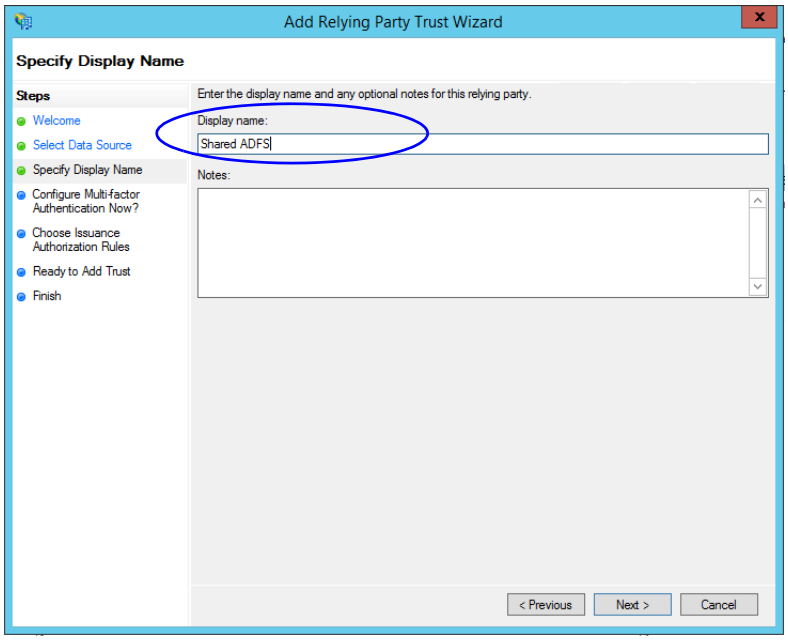
Click Add Relying Party Trust

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**.

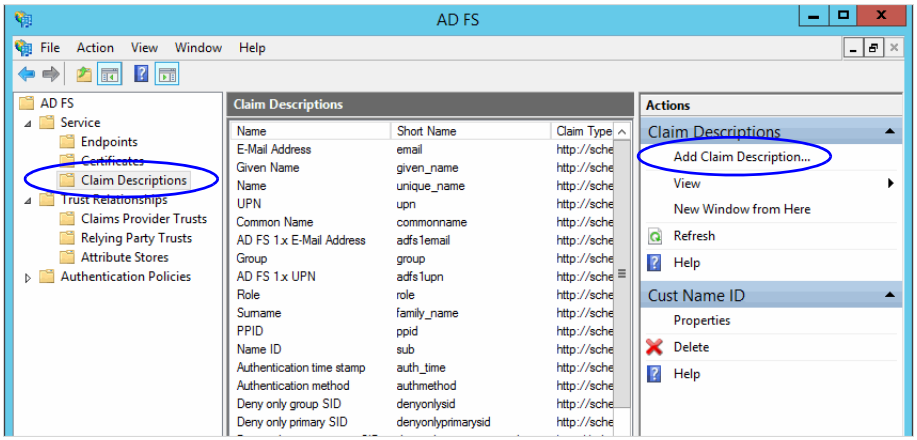


Provide a display name

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:

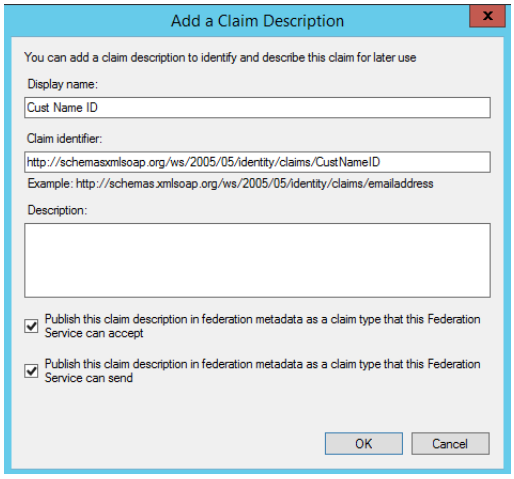
a. Set the **Display name** as **Cust Name ID**.

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.

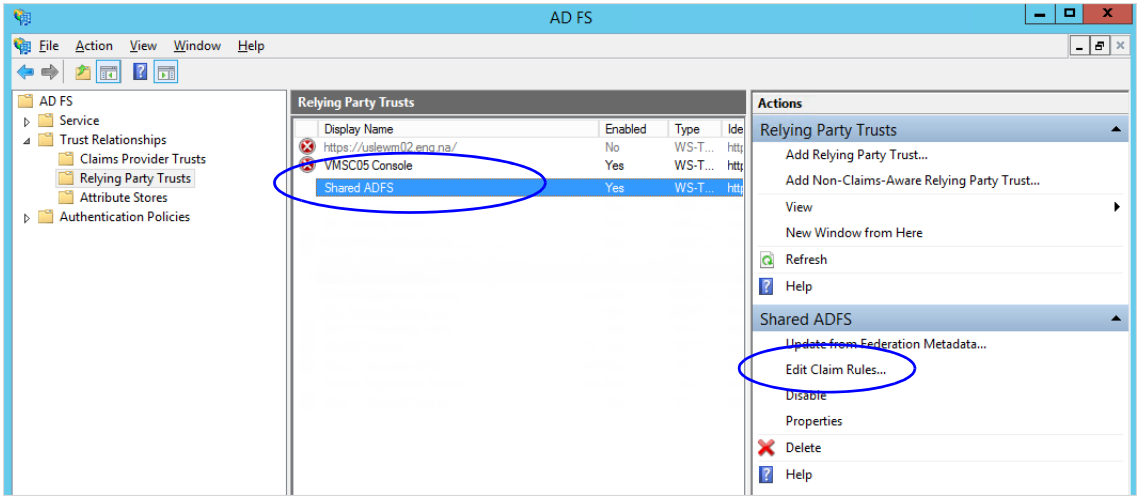
d. Select the **Publish the claim description in federation metadata as a claim type that this Federation Service can send** option.

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.**

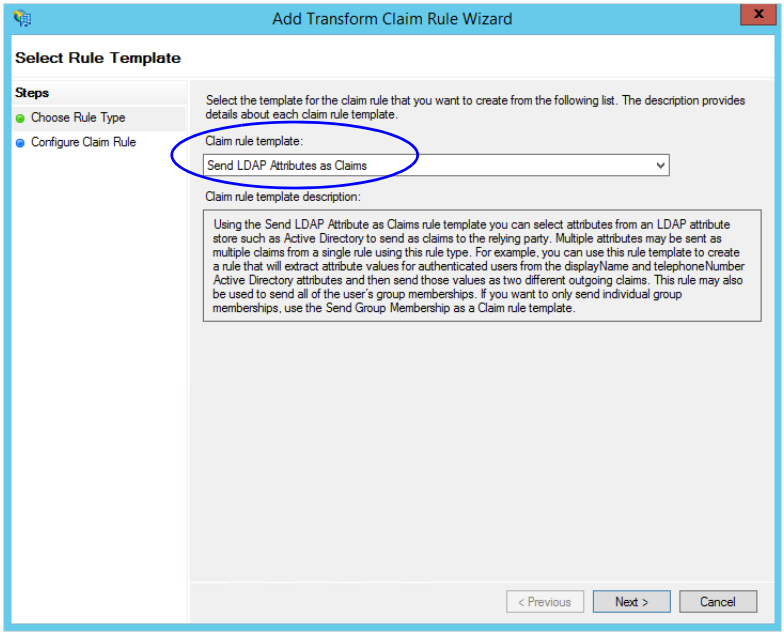


Click Edit Claims Rules

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**.

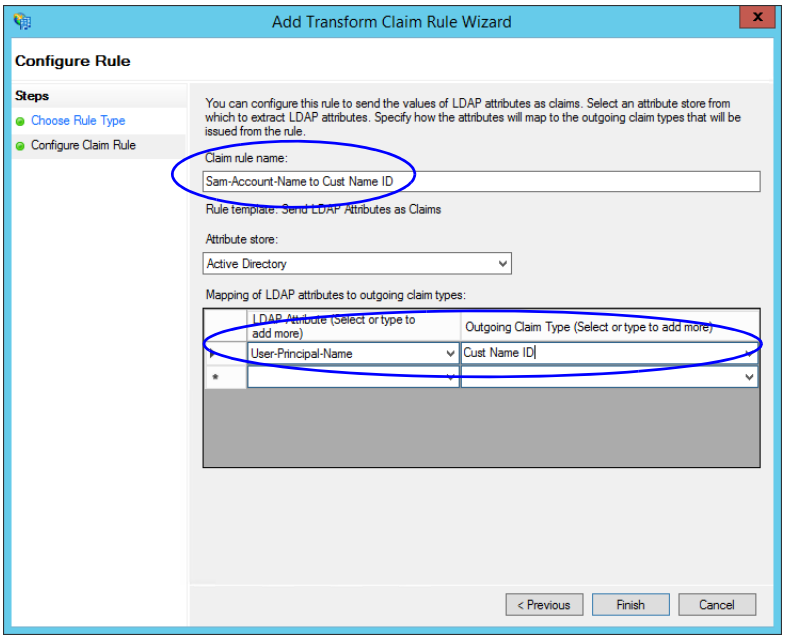


Select the claim rule template

b. On the Configure Claim Rule screen, do the following:

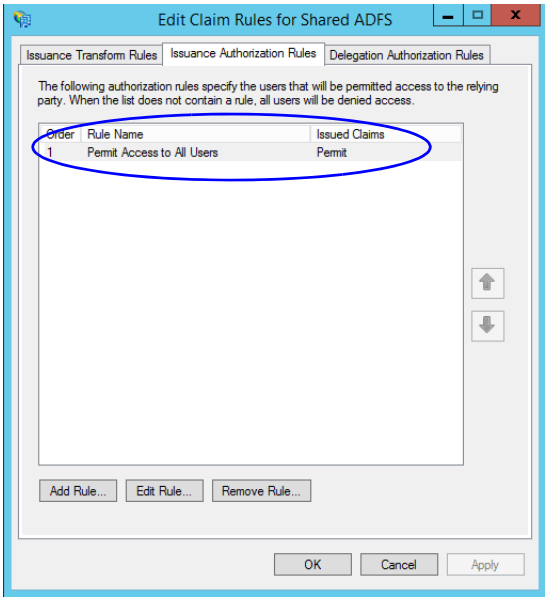
i. Provide a claim rule name.

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.



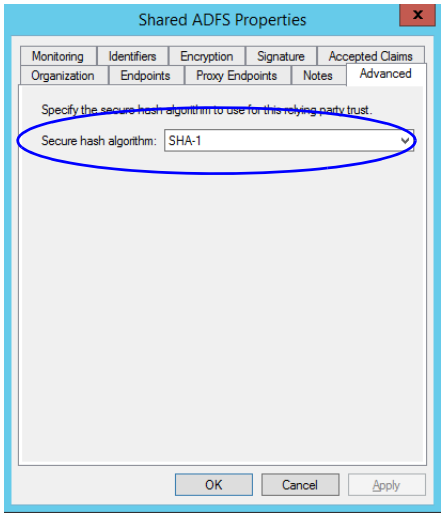
Configure the claim rule

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

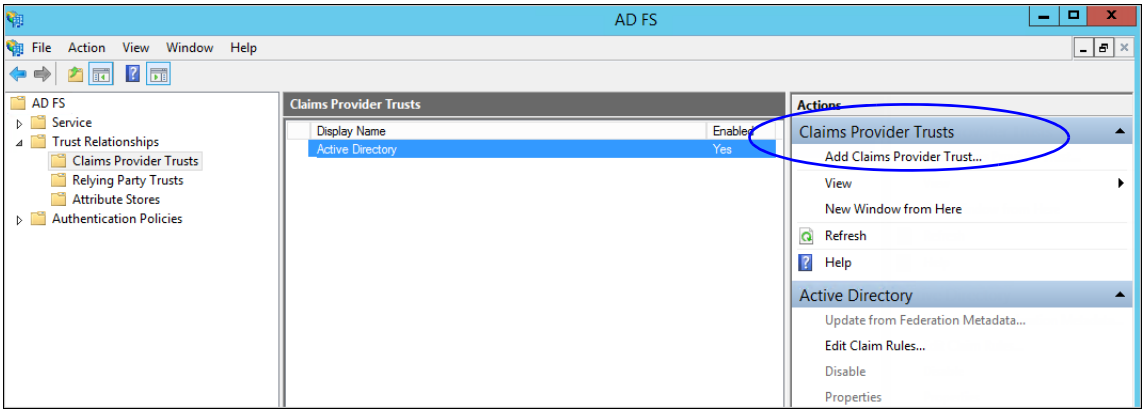
Configuring Claims Provider Trust for Customer AD FS in Shared AD FS

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:

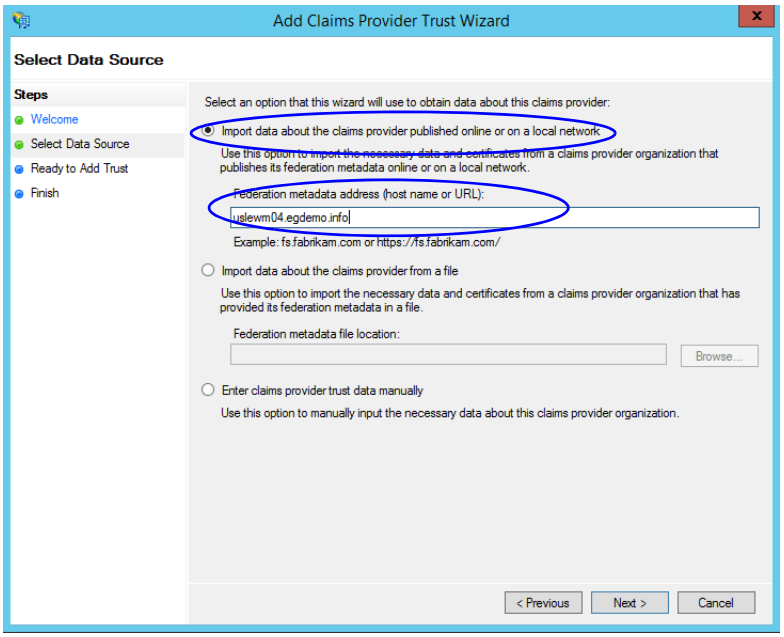
1. Go to the Start menu and open the AD FS Management console.

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

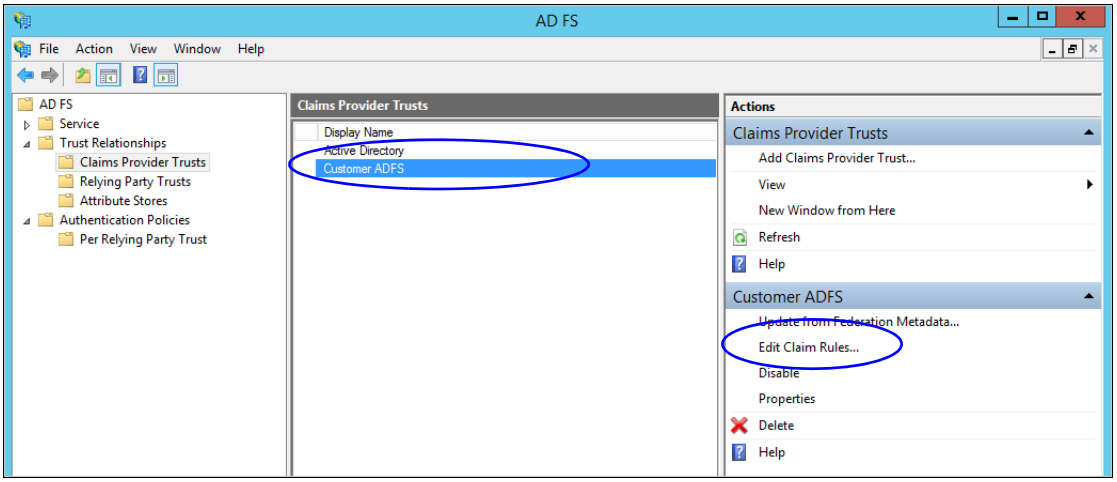
4. In the Add Claims Provider Trust Wizard that appears, do the following:
   a. On the Select Data Source screen, set the following options:
      i. Select the **Import data about the claims provider published on online or on a local network** option.
      ii. In the **Federation metadata address** 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.**

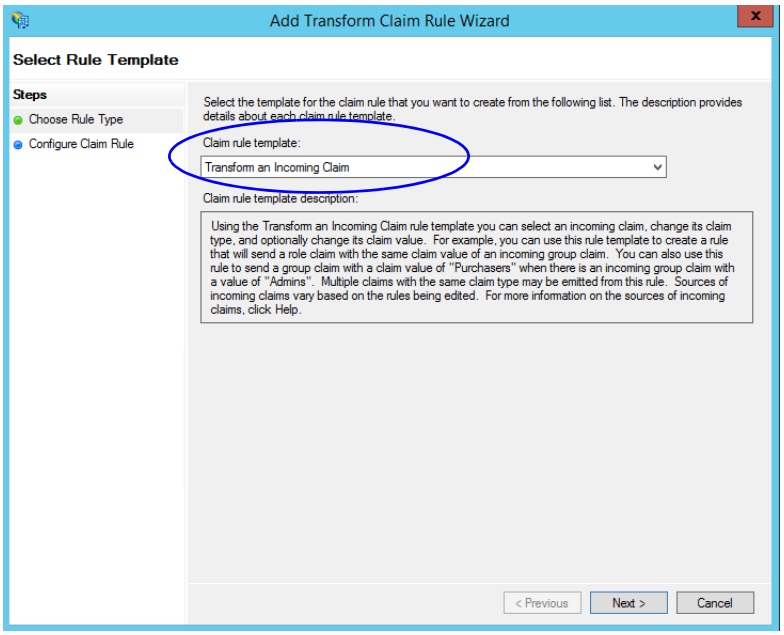


Edit the claim rules

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

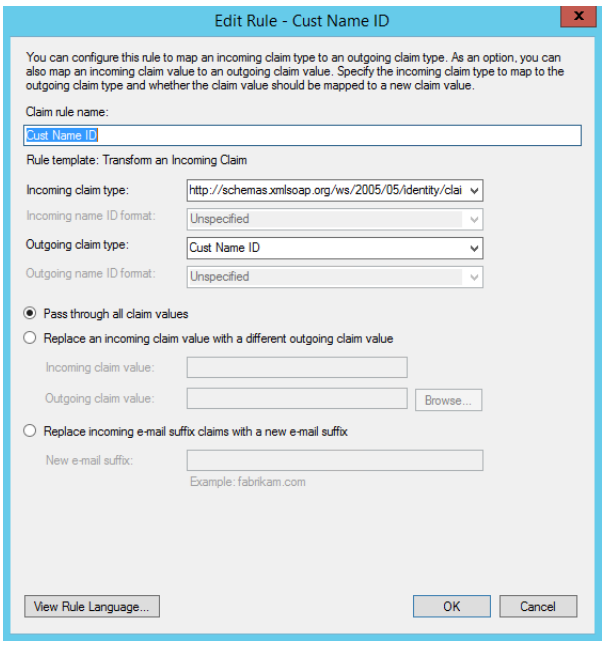
   b. On the Configure Claim Rule screen, set the following:

      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 111).

iii. Set the Outgoing claim type as **Cust Name ID.**

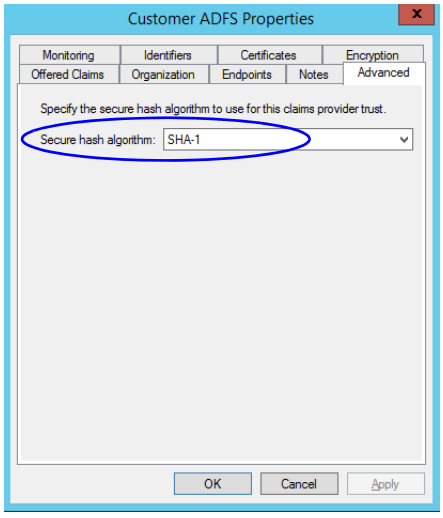
iv. Select the **Pass through all claim values** option.



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.



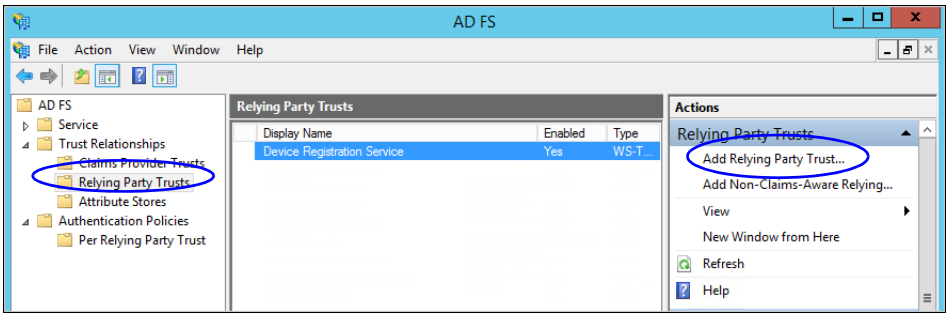
Set the secure hash algorithm

Configuring Relying Party Trust for ECE in Shared AD FS

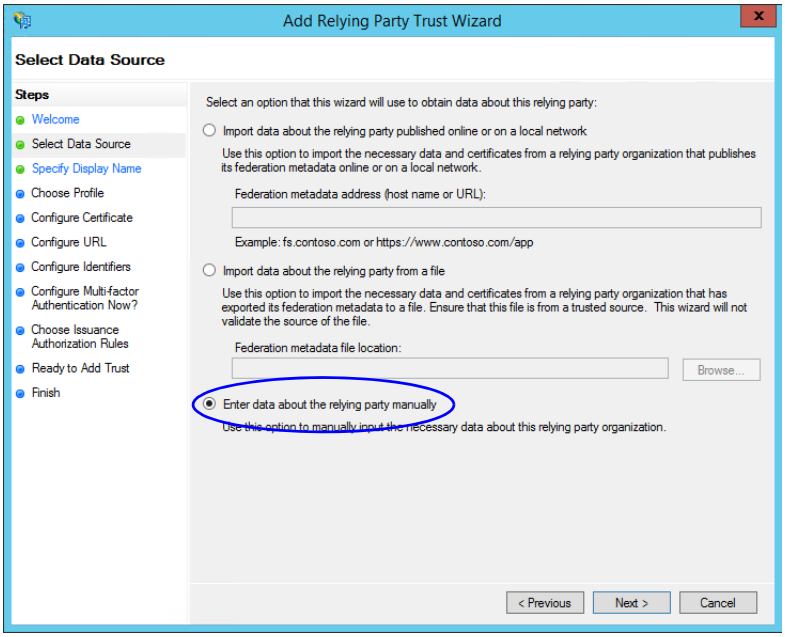
Perform these tasks on the server where shared AD FS is installed.

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...**

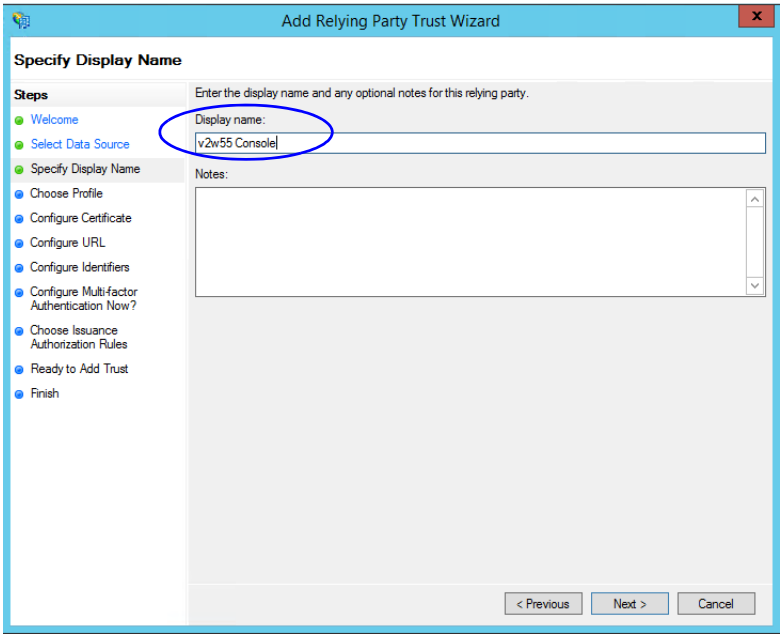


4. In the Add Relying Party Trust Wizard that appears, do the following:
   a. On the Welcome screen, click **Start.**
   b. On the Select Data Source screen, select the **Enter data about the reply party manually** option and click **Next**.



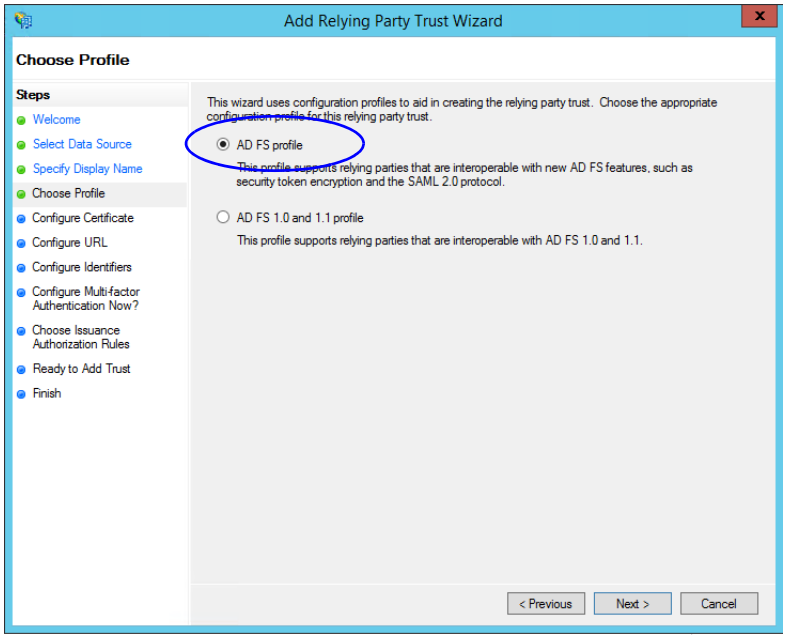
Select the Enter data about the reply party manually option

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



Provide a display name

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



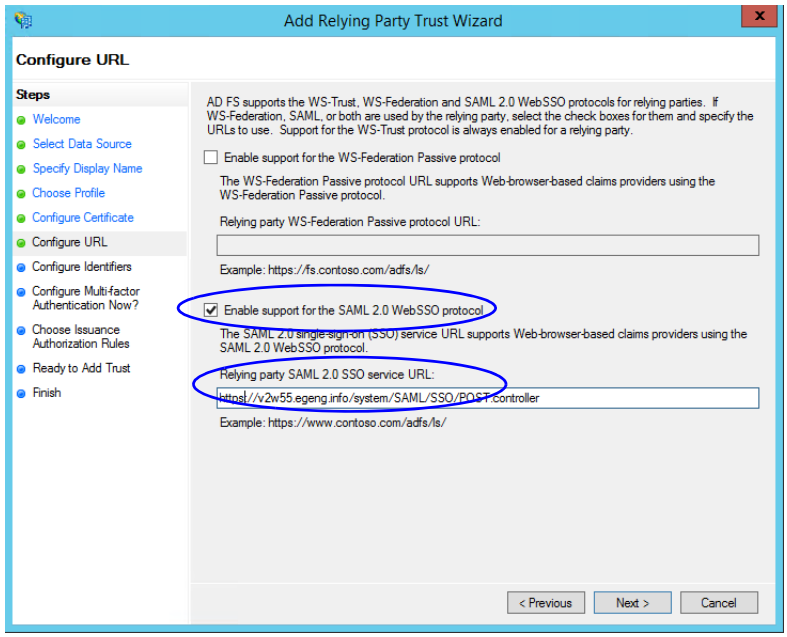
Select AD FS profile

e. On the configure Certificate screen, click **Next.**

f. On the Configure URL screen, set the following:

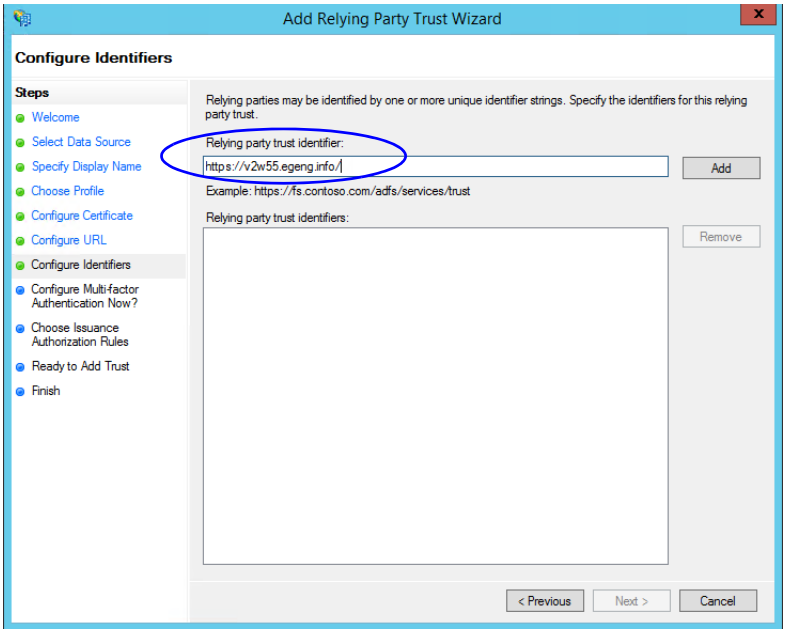
i. Select the **Enable support for the SAML 2.0 Web SSO protocol** option.

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

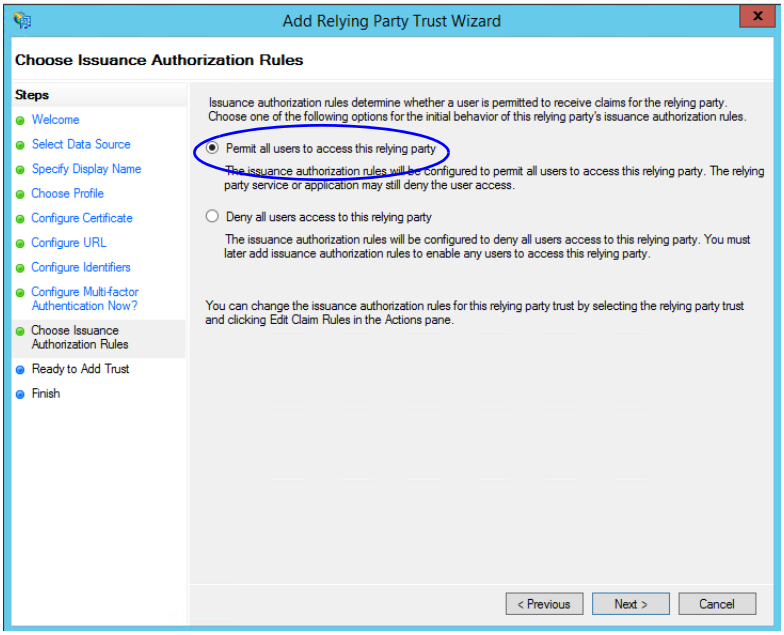
g. On the Configure Identifiers screen, provide the Replying party trust identifier and click **Add**. Value should be in the format: `https://`*Web_Server_Or_Load_Balancer_Server*`/`. Replace *Web_Server_Or_Load_Balancer_Server* with the ECE web server name or the Load balancer server name. Click **Next.**



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.



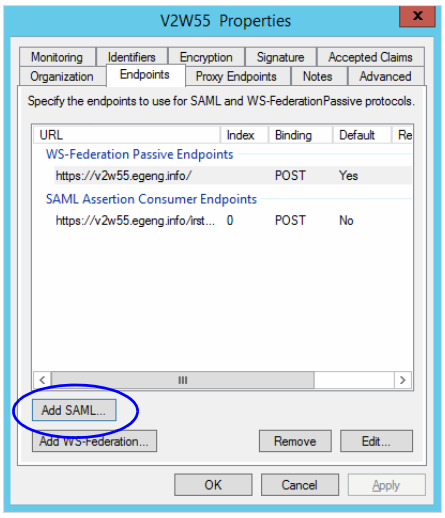
Select the Permit all users to access this relying party option

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.

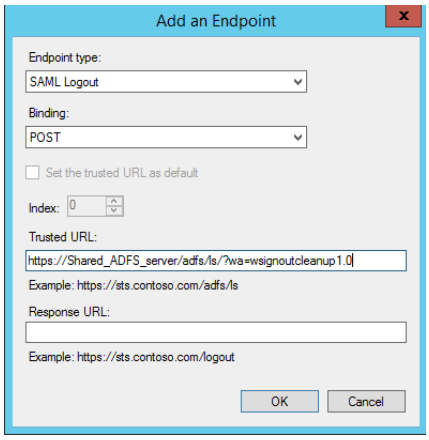
5. In the Relying Provider Trusts list, select the trust created for ECE, and in the actions section click **Properties**.

6. In the Properties window, go to the Endpoints tab and click the **Add SAML..** button.



Click Add SAML

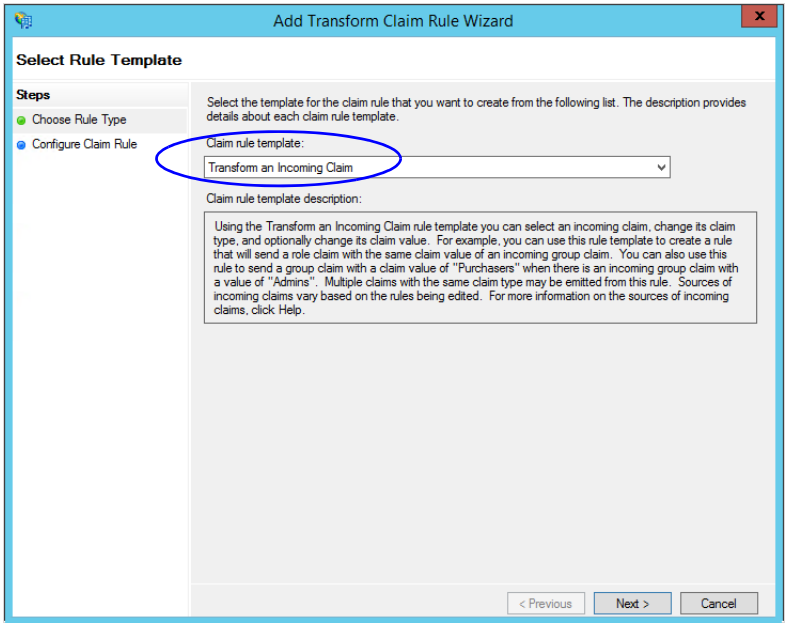
7. In the Add an Endpoint window, set the following:
   a. Select the **Endpoint type** as **SAML Logout**.
   b. Specify the **Trusted URL** as `https://`*Shared_ADFS_server*`/adfs/ls/?wa=wsignoutcleanup1.0`. Replace *Shared_ADFS_server* with the Shared AD FS server name.
   c. Click **OK.**



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**.



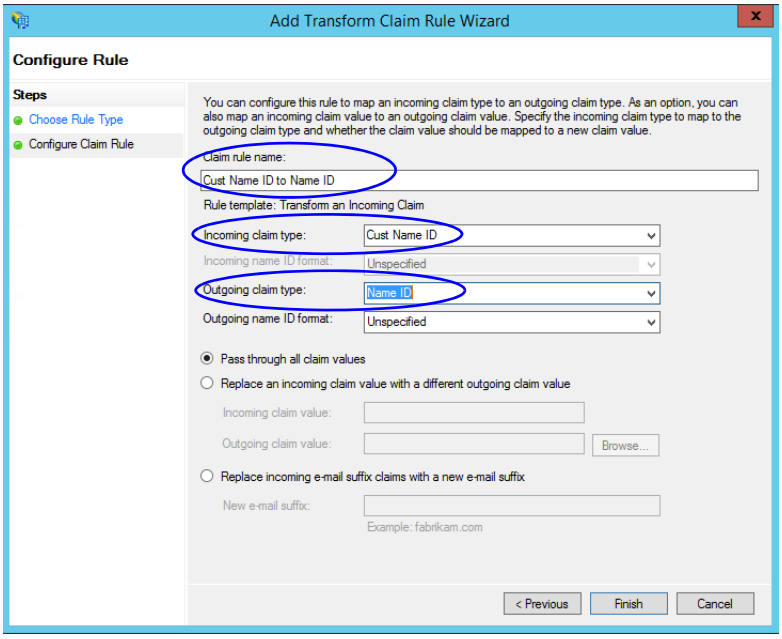
Select the claim rule template

b. On the Configure Rule screen, set the following:

i. Provide the Claim rule name.

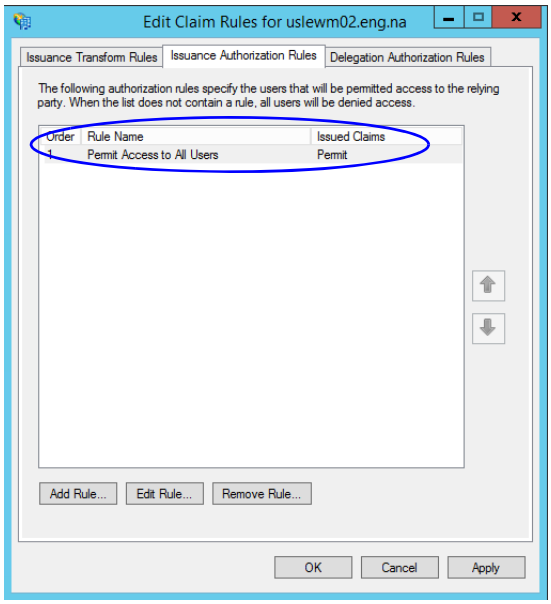
ii. In the **Incoming claim type** field provide the name of the outgoing claim specified in the Relying Party trust wizard (page 113).

iii. In the **Outgoing claim type** dropdown, select the **Name ID** option.



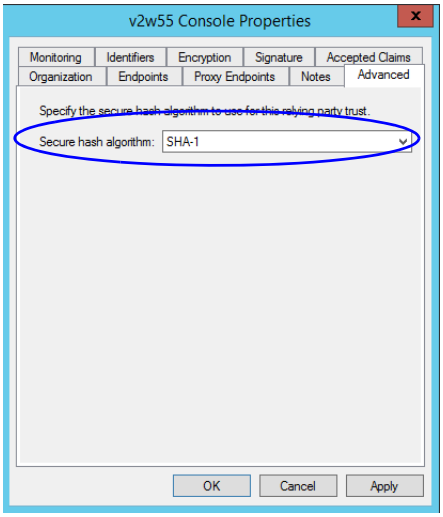
Configure the rule

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.



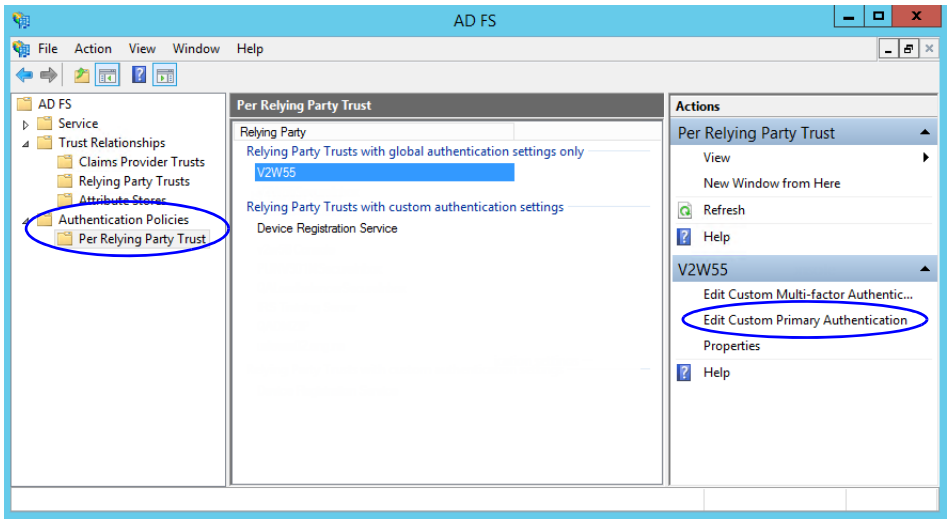
Check the authorization rules

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.



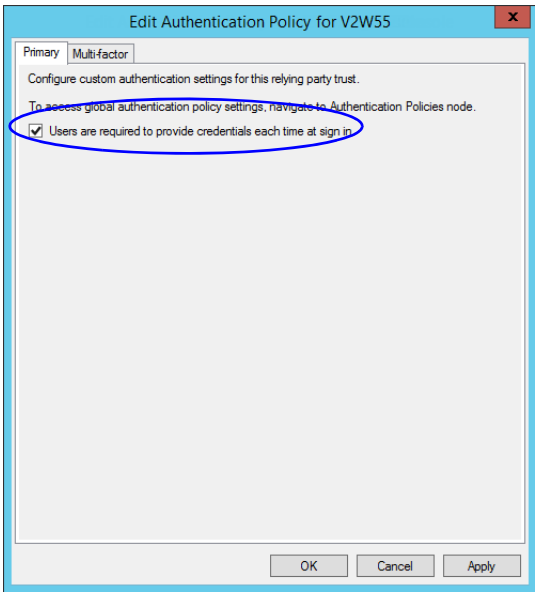
Set the secure hash algorithm

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.

7 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. If the configuration uses a load balancer, configure SSL on the load balancer.

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:

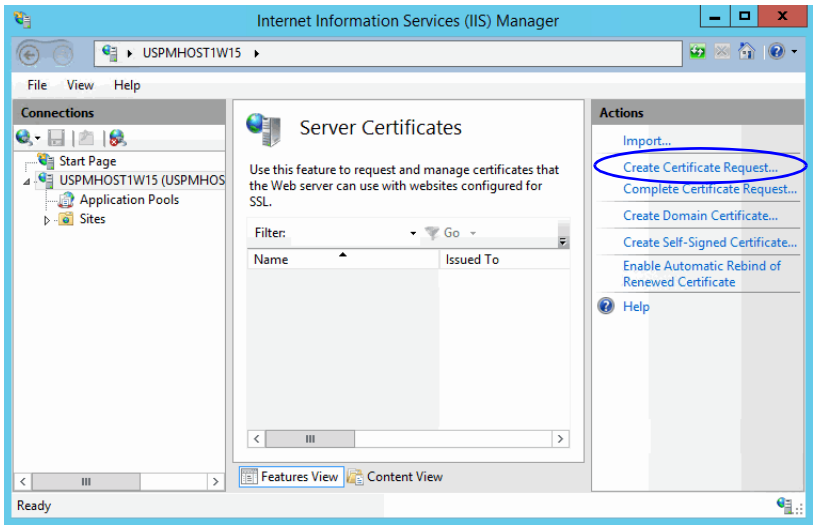
- Generating a Certificate Signing Request
- Submitting the Certificate Request
- Installing the Certificate on the Web Server

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:

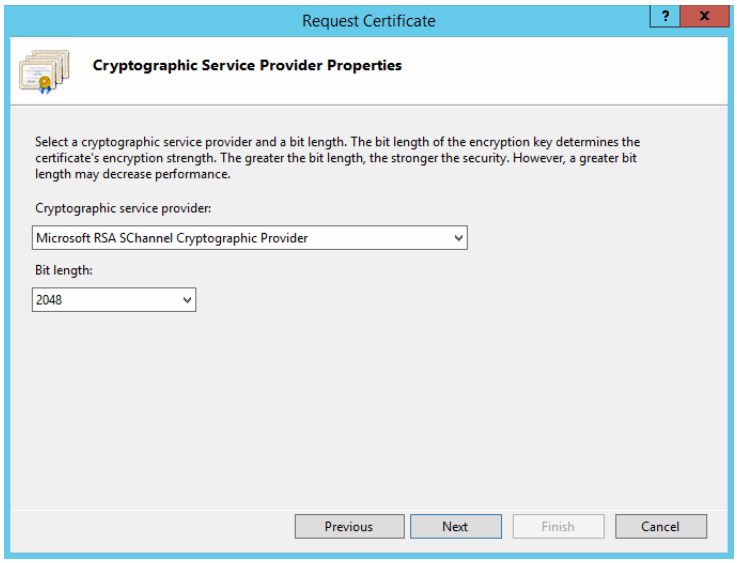
1. Click the **Start** menu, go to **Control Panel > Administrative Tools**, and select **Internet Information Services (IIS) Manager.**
2. In the Connections pane, select the name of the server, and when the page is refreshed, double-click **Server Certificates**. The window is refreshed.
3. In the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



*Click the **Create Certificate** Request link*

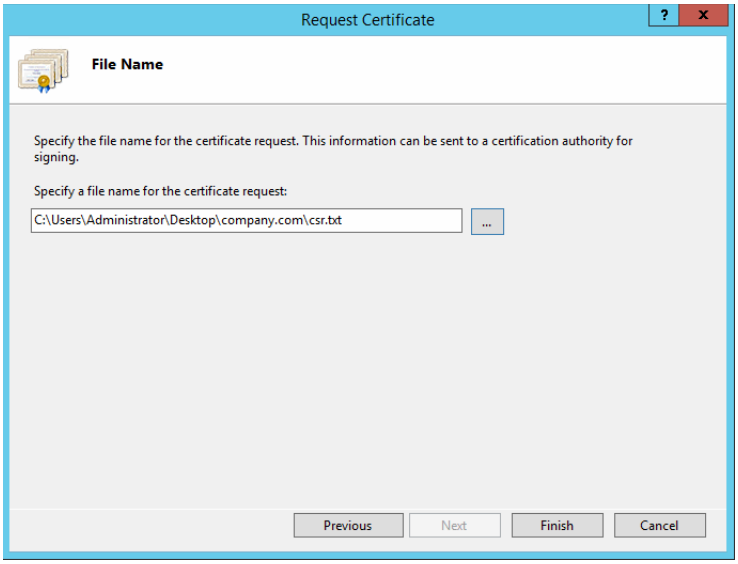
4. In the Distinguished Name Properties window, enter information about the company and the site to be secured:
   - **Common Name**: The fully qualified domain name (FQDN) of your server. This must match exactly what users type in the web browser to get to the application. If you are using a load balancer, enter the name of the server on which the load balancer is installed.
   - **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 127).

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

Installing the Certificate on the Web Server

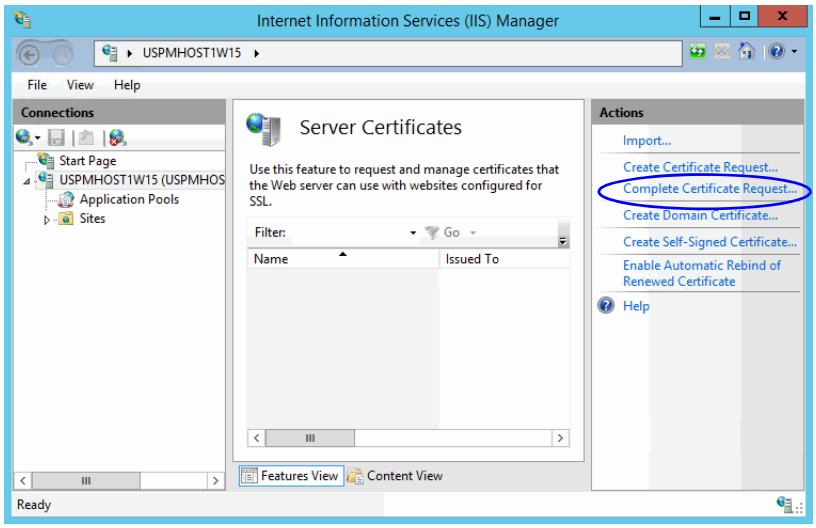
Once you receive the certificate from your vendor, install it on all web servers. If you are using load balancer, install it on the load balancer server.

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:

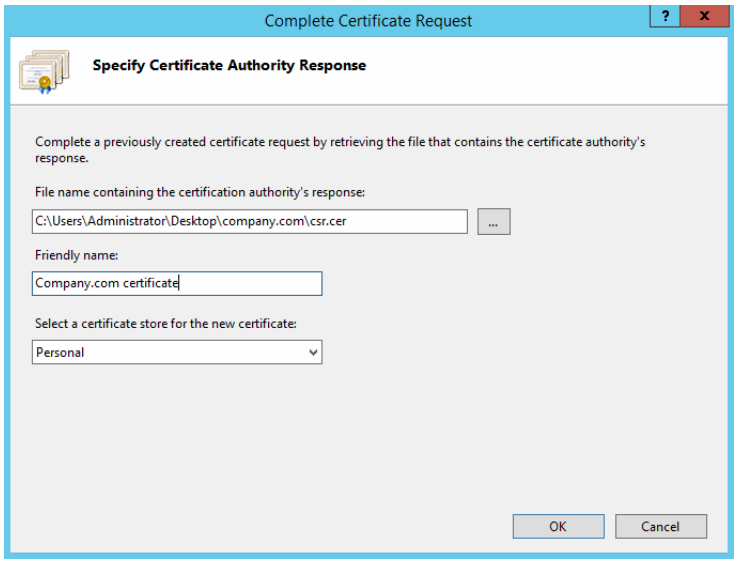
1. Click the **Start** menu, go to **Administrative Tools**, and select **Internet Information Services (IIS) Manager.**

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.

Repeat this process on all web servers.

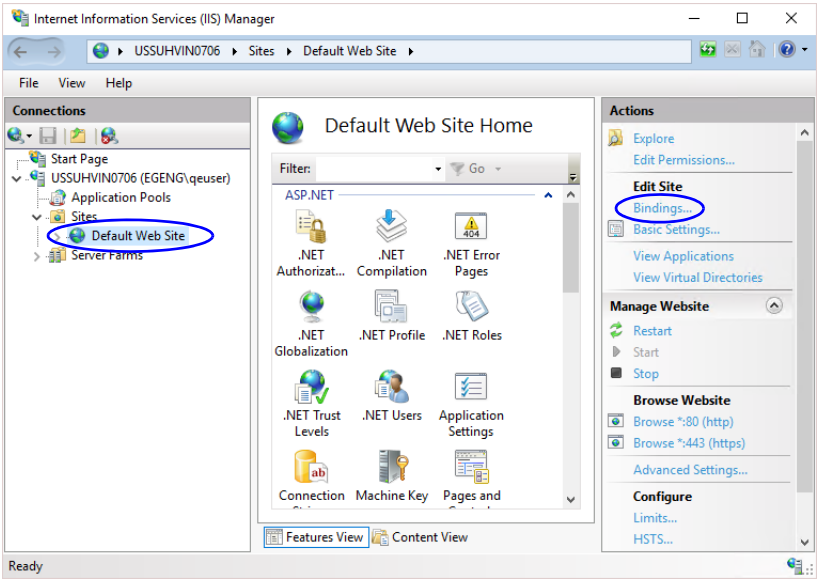
Binding the Certificate to the Application Website

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.**

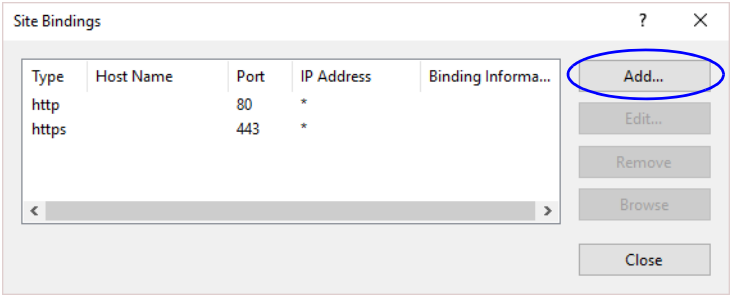
To bind the certificate to the application URL:

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



Select the Web_Site_Name.

4. In the Site Bindings window, click the **Add...** button.

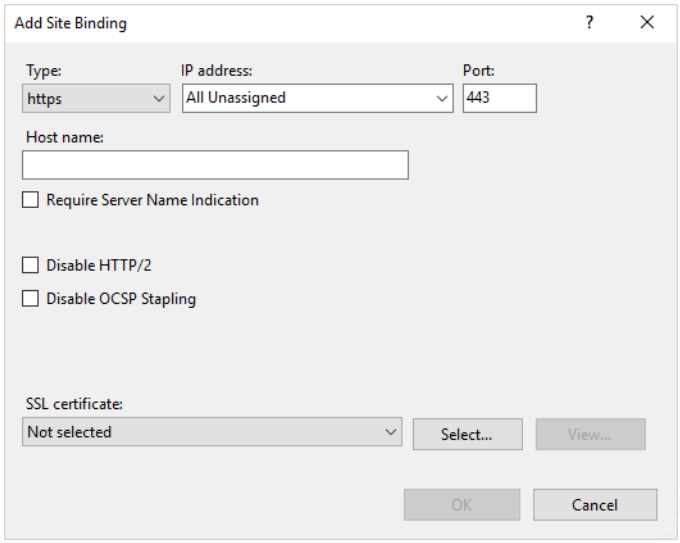


*Click the **Add** button*

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**.

Important: **When ECE is integrated with PCCE, while selecting the SSL certificate, ensure that the Host name field is left blank. If this is not done, the PCCE-ECE integration does not work as the API calls are made using the IP address and not the FQDN.**



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

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 file server. (page 133)

a. Modify the alias configuration (page 134)

On the File 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 file server.

Perform these tasks on the file server. In case of Distributed File Server, perform these tasks on the Active Node.

Installing Certificates

To configure SSL or TLS on the file 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 *ECE_HOME*.
3. Open the Command window and navigate to the `bin` folder in *JDK_Home*, the installation folder for JDK. For example, the command will look like:

   ```
   cd Install_Drive\ECE_Home\env\jdk\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 133 to install new certificates.

To delete a certificate:

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

   ```
   cd Install_Drive\ECE_Home\env\jdk\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`.

Enable SSL for Specific Email Aliases

To enable SSL for specific aliases:

- In Unified CCE Administration, in the Enterprise Chat and Email administration space, configure the email alias **Connection Type** as **SSL** or **TLS** and provide secure ports for the incoming and outgoing servers. For details, see the Aliases chapter in *Enterprise Chat and Email Administrator's Guide to Chat and Email Resources.*

Appendix A: Distributed File System Configuration

- Installing DFS Management
- Creating Shared Folders
- Creating New Namespace
- Adding Namespace Server
- Adding Folders and Configuring Replication

Installing DFS Management

Perform these tasks on both the servers where you want to store the ECE file share for DFS.

To install DFS by using Server Manager

1. Open Server Manager, click **Manage**, and then click **Add Roles and Features**. The Add Roles and Features Wizard appears.
2. On the Server Selection page, select the server on which you want to install DFS.
3. On the Server Roles page, in File and **Storage Services > File and iSCSI Services**, select **DFS Namespaces** and **DFS Replication**. Run through the wizard to complete the installation.

Creating Shared Folders

Perform these tasks on all the servers where you want to store the ECE file share for DFS.

To create a shared folder:

1. Create a folder on the server where you want to store the ECE file share for DFS.
2. Right-click the folder and select **Properties**. Set the following in the properties window:
   a. Go to the Security tab and click the **Edit** button. Add the **Service** account and assign the **Service** account **Modify** permissions on the folder. Click **Apply**.
   b. Go to the Sharing tab and click **Advanced Sharing** and select the **Share this folder** option in the Advanced Sharing window. Click the **Permissions** button and in the Permissions window, assign the Service account **Full Control** permission on the folder.
   c. From the Sharing tab, copy the Network Path of the shared folder and access it from the second server to make sure it is accessible. Create a test folder in the shared folder to test the permissions.

   Repeat these steps on the other servers.

Creating New Namespace

Perform these tasks on one of the file servers where you want to store the ECE file share for DFS.

To add new namespaces:

1. In the DFS Management window, browse to **DFS Management > Namespaces.**
2. Right-click **Namespaces** and select **New Namespaces** from the context-menu.
3. In the New Namespace Wizard, set the following:
   a. On the Namespace Server screen, click the **Browse** button and provide the name of the server where you created the shared folder. Click **Next**.

b. On the Namespace Name and Settings screen, provide a name for the namespace. Click the **Edit Settings** button. In the Edit Settings window, select the **Administrators have full access; other users have read-only permissions** option. Click **Next**.

c. On the Namespace Type screen, select **Domain-based namespace**. Select the **Enable Windows Server 2008 mode** option. Click **Next**.

d. On the Review Settings and Create Namespace screen, note down the **Namespace Name** (this is the UNC path where you access the share). Click **Create**.

4. Click **Close** to exit the wizard.

Adding Namespace Server

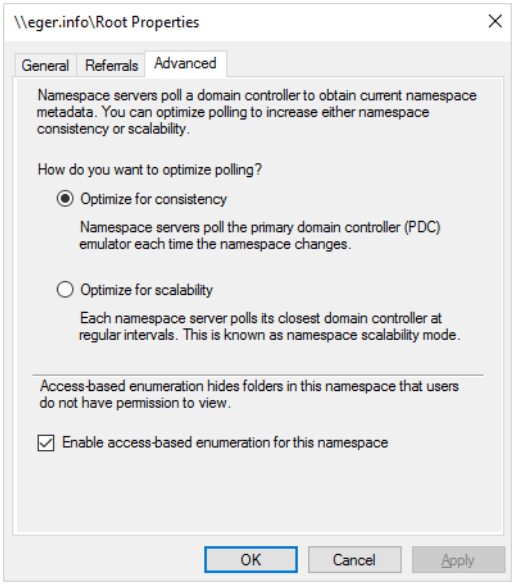
Perform these tasks on other file servers in the deployment.

To add the namespace server:

1. In the DFS Management window, browse to **DFS Management > Namespaces**.
2. Right-click the namespace you created on page 136 and select **Add Namespace Server** from the context-menu.
3. In the Add Namespace Server window, click **Browse** in the **Namespace server** field. In the Select Computer window provide the name of the **second server** where you created the shared folder. Click the **Edit Settings** button. In the Edit Settings window, select the **Administrators have full access; other users have read-only permissions** option. Click **OK**.
4. Select the Namespace Servers tab and check that both servers are listed.
5. Click on the **Properties** link of the Namespace.

   The Properties window opens.
6. In Properties window, go to the Advanced tab.

7. Select the **Enable access based enumeration for this namespace checkbox** and click OK.



Enable access based enumeration

Adding Folders and Configuring Replication

For Two Server Installations

Creating Folders on Side B

- Create the following directories on Side B.
  - *Drive_Name*\ECE_Files\env
  - *Drive_Name*\ECE_Files\eService
  - *Drive_Name*\ECE_Files\Uninstaller
  - *Drive_Name*\ECE_Files\Utilities

Adding Folders

To add folders and configure replication:

1. In the DFS Management window, browse to **DFS Management > Namespaces >** DFS created for ECE.
2. In the Actions section, click the **New Folder** button. Set the following in the New Folder window.
   - Provide a name for the folder. For example, ECE.
   - In the Folder targets, add the network path of both the shared folders created on the ECE servers.

3. When prompted to create a Replication group, click **No**.
4. In the DFS Management window, right-click the **Replication** folder and from the menu select **New Replication Group.**
5. Run through the New Replication Group Wizard to set up replication.
    a. On the Replication Group Type screen, select **Multipurpose Replication Group**. Click **Next.**
    b. On the Name and Domain screen, provide a **Name of replication group** and specify the **Domain**. Click **Next.**
    c. On the Replication Group member screen, add the servers to be the list. Click **Next.**
    d. On the Topology selection screen, select **Full mesh.** Click **Next**.
    e. On the Replication group Schedule and Bandwidth screen, select the **Replicate continuously with specific Bandwidth** option. Click **Next**.
    f. On the Primary Member screen, select any one server to be the primary server. Click **Next**.
    g. In the **Folders to Replicate** screen, add the following folders and click **Next**.
        - *Drive_Name\ECE_Home*`\env`
        - *Drive_Name\ECE_Home*`\eService`
        - *Drive_Name\ECE_Home*`\Uninstaller`
        - *Drive_Name\ECE_Home*`\Utilities`
    h. On the Local Path of env on other members screen, click the **Edit** button and in the Edit window, select **Enabled** and provide the Local path for **env** on side B (page 138). Click **OK** to close the window. Click **Next**.
    i. On the Local Path of eService on other members screen, click the **Edit** button and in the Edit window, select **Enabled** and provide the Local path for **eService** on side B (page 138). Click **OK** to close the window. Click **Next**.
    j. On the Local Path of Utilities on other members screen, click the **Edit** button and in the Edit window, select **Enabled** and provide the Local path for **Utilities** on side B. Click **OK** to close the window. Click **Next**.
    k. On the Local Path of Uninstaller on other members screen, click the **Edit** button and in the Edit window, select **Enabled** and provide the Local path for **Uninstaller** on side B (page 138). Click **OK** to close the window. Click **Next**.
    l. On the Review Settings and Create Replication Group screen, ensure the information provided is corrct and click **Create.**
6. Once replication is setup, set the Staging folder quota for the replication. You must set a number based on the available bandwidth and the size of the files to be replicated. Follow Microsoft documentation for guidelines for setting the quota numbers.

For Distributed Server Installations

To add folders and configure replication:

1. In the DFS Management window, browse to **DFS Management > Namespaces >** DFS created for ECE.

2. In the Actions section, click the **New Folder** button. Set the following in the New Folder window.
   - Provide a name for the folder. For example, `ECE`.
   - In the Folder targets, add the network path of both the shared folders created on the ECE servers.
3. When prompted to create a Replication group, click **Yes**.
4. Once replication is setup, set the Staging folder quota for the replication. You must set a number based on the available bandwidth and the size of the files to be replicated. Follow Microsoft documentation for guidelines for setting the quota numbers.

Appendix B: SQL Always-On Configuration

- About Always On Availability Group Clustering
- Pre-Installation Tasks
- Install the Application
- Post-Installation Tasks

About Always On Availability Group Clustering

Important: **ECE supports the clustering feature only for installations using the Enterprise Edition of MSSQL.**

This chapter talks about an Always On cluster configuration with two nodes. You can add more nodes, if required. The two deployment models supported are:

1. Reports database and active and master databases are on the same node with a common availability group for the databases.
2. Reports database is on one node and active and master databases are on a separate node with respective availability groups for each node.

Important: **Ensure that all the databases related pre-installation and post-installation tasks are performed on all nodes in the cluster.**

Pre-Installation Tasks

Installing Failover Clustering Feature

Perform this task on for all nodes of active and reports databases.

To install the failover cluster feature:

1. Open Server Manager, click **Manage**, and then click **Add Roles and Features**. The Add Roles and Features Wizard appears.
2. On the Server Selection page, select the server on which you want to install the Failover Clustering.
3. On the Features page, select **Failover Clustering**. Run through the wizard to complete the installation.

Creating Prestage Cluster Computer Objects in Active Directory Domain Services (AD DS)

To create the cluster name object (CNO) automatically, the user who creates the failover cluster must have the **Create Computer objects** permission to the organizational unit (OU) or the container where the servers that will form the cluster reside.

To enable a user or group to create a cluster without having this permission, a user with appropriate permissions in AD DS (typically a domain administrator) can prestage the CNO in AD DS.

These tasks are done by a network administrator.

Prestaging the CNO in AD DS

To prestage the CNO in AD DS:

1. On a computer that has the AD DS Tools installed from the Remote Server Administration Tools, or on a domain controller, open Active Directory Users and Computers. To do this on a server, open **Server Manager** and from the **Tools** menu, select **Active Directory Users and Computers**.
2. In Active Directory Users and Computers, on the **View** menu, make sure that **Advanced Features** is selected.
3. Create an OU, if it does not exists. For the cluster computer objects, right-click the domain name or an existing OU, and select **New > Organizational Unit**. In the **Name** box, enter the name of the OU, and then click **OK**.
4. In the console tree, right-click the OU where you want to create the CNO, point to **New**, and then select **Computer**.
5. In the **Computer name** box, enter the name that will be used for the failover cluster, and then select **OK**.
6. As a best practice, right-click the computer account that you just created, click **Properties**, and then click the Object tab. On the Object tab, select the **Protect object from accidental deletion** check box, and then click **OK**.
7. Right-click the computer account that you just created, and then select **Disable Account**. Select **Yes** to confirm, and then select **OK**. You must disable the account so that during cluster creation, the cluster creation process can confirm that the account is not currently in use by an existing computer or cluster in the domain.

Granting User Permissions to Create Cluster

To grant user permissions to create cluster:

1. In Active Directory Users and Computers, on the **View** menu, make sure that **Advanced Features** is selected.
2. Locate and then right-click the CNO, and then click **Properties**.
3. On the Security tab, click **Add**.
4. In the Select Users, Computers, or Groups dialog box, specify the user account or group that you want to grant permissions to, and then click **OK**.
5. Select the user account or group that you just added, and then next to **Full control**, select the **Allow** check box.
6. Select **OK**.

Granting the CNO Permissions to the OU

To grant the CNO permissions to the OU:

1. In Active Directory Users and Computers, on the **View** menu, make sure that **Advanced Features** is selected.

2. Right-click the OU where you created the CNO (page 143) and then select **Properties**.
3. On the Security tab, select **Advanced**.
4. In the Advanced Security Settings dialog box, select **Add**.
5. Next to Principal, select **Select a principal.**
6. In the Select User, Computer, Service Account, or Groups dialog box, select **Object Types**, select the **Computers** check box, and then select **OK**.
7. Under **Enter the object names to select**, enter the name of the CNO, select **Check Names**, and then select **OK**. In response to the warning message that says that you are about to add a disabled object, select **OK**.
8. In the Permission Entry dialog box, make sure that the **Type** list is set to **Allow**, and the **Applies to** list is set to **This object and all descendant objects.**
9. Under Permissions, select the **Create Computer objects** and **Delete Computer Object** check boxes.
10. Select **OK** until you return to the Active Directory Users and Computers snap-in.

Creating Windows Failover Cluster

Perform this task on one active server node and one reports database node.

To install Windows server failover cluster:

1. Open **Server Manager** and from the **Tools** menu, select **Failover Cluster Manager.**
2. In the Failover Cluster Manager, right-click **Failover Cluster Manager** and select **Create Cluster** from the menu.
3. In the Create Cluster Wizard, on the Select Servers screen, enter the **Server Name** for both active database servers to be added to the cluster and Click **Add**.
4. On the Validation Warning screen, select **Yes** to validate the cluster nodes. The program will run you through the validation process.
5. On the Access Point for Administering the Cluster screen, provide the **Cluster Name**. This is the name of the computer object created in the Active Directory. Enter the IP address reserved for the Windows Cluster Name Object. You will need two IPs for the Cluster if the target servers are at two different subnets. Click **Next.**
6. On the Confirmation screen, uncheck the **Add all eligible storage to the cluster** option. Click **Next.**
7. Click **Finish** on the Summary screen.

   Repeat this task for the reports database node. In Step 3, add the reports database servers.

Configuring Permissions for the File Share Witness Folder

To configure permissions for the file share witness folder:

1. Create folder on the VM which is used for file share witness (for example, Quorum126)
2. Give **Full** control permission to the CNO user on this (for example, collocatedHA which is the CNO in the organization unit (OU)). Perform the following tasks:

a. Right click on the folder created in Step1 and select **Properties > Security> Edit > Add.**

b. Under the **Select Users, Computers, Service Accounts or group** dialogue box, click the **Object Types** button.

c. Search for the CNO user created for the failover cluster (for example, CollocatedHA).

3. Give Full control permission to the recently created user.
4. Go to Sharing tab and ensure that the user is added to list with **Read/ Write** permission.
5. Click on the **Share** button for path sharing.
6. Follow the quorum setting configuration available in "Configure Cluster Quorum Settings" on page 145.

Configure Cluster Quorum Settings

Quorum is a configuration database for the cluster and is stored on a shared location, accessible to all of the nodes in a cluster.

In case of even number of nodes (but not a multi-site cluster) **Node and Disk Majority Quorum** configuration is recommended. If you don't have a shared storage, **Node and File Share Majority** is recommended. Here it will be configuring a **FileShare Witness** quorum.

It is recommended that you configure the quorum size to be 500 MB. This size is the minimum required for an efficient NTFS partition. Larger sizes are allowable but are not currently needed.

Perform this task on one active server node and one reports database node.

To configure cluster quorum settings:

1. In the Failover Cluster Manager, right-click the cluster you added. From the context-menu, go to **More Actions > Configure Cluster Quorum Settings...**.
2. In the Configure Cluster Quorum Wizard, on the Before You Begin screen, click **Next**.
3. On the Select Quorum Configuration Option screen, select the **Select the quorum witness** option.
4. On the Select Quorum Witness screen, select the **Configure a file share witness** option.
5. On the Configure File Share Witness screen, click the **Browse** button next to the **File Share Path** field. In the Browse for Shared Folders window that opens, select the shared folder that you want to use and click **OK**. Now Click **Next**.

   It is recommended to have the share folder on a different node than the participating nodes on cluster.
6. Run through the rest of the wizard to complete the configuration.

Verifying Cluster Settings

1. Right-click the cluster, and select **Validate Cluster**.
2. Review **Cluster At this point**. The cluster should be fully setup and confirmed to work properly.

3. Review the Failover Cluster Manager for any errors. In the Cluster Events node, you can find Windows Events which are directly related to the cluster. Since the IP address that matches the subnet of the non-primary server is not accessible until the cluster switches sides, you can ignore the errors related to the dual-subnet. If you see other errors, investigate and resolve each error.

Enabling Always On Availability Groups Feature on SQL

Perform this task on one active server node and one reports database node.

To enable always-on availability groups feature:

1. Open the SQL Server Configuration Manager and browse to SQL Server Services.
2. In the list pane, right-click **SQL Server** service and select **Properties**.
3. In the Properties window, go to the AlwaysOn High Availability tab and select the **Enable AlwaysOn Availability Groups** option. You will be prompt to restart the SQL Server service. Click **OK.**

   Perform this task on both servers (primary and secondary).
4. Change the service account of all SQL server services to the **SQL Services Account** that you have created for the ECE application. If you didn't create a **SQL Services Account**, use the **Service Account** created for the ECE application (page 33).
5. Restart the SQL Server services.

Configuring SQL Server Always On Availability Groups

Before configuring the SQL Server Always On Availability Groups, perform the following tasks:

- Adhering to the Microsoft recommendations for SQL Always-On configuration, configure the system in the **Automatic** mode.
- Verify the stability of the Failover Cluster instance using a Fileshare witness ensuring that it is consistently online and in a healthy state. This should be supported by a minimum of two upvotes to reinforce robust high-availability and failover capabilities.
- For efficient and automatic synchronization of database replicas within the Always On availability group, set the **Automatic Seeding** setting to **Yes**.

Perform this task on one active server node and one reports database node.

To configure SQL server always on availability group:

1. First, create a temporary database. This database is required only for creating the availability group. The database should be in fully recovery model and at least one full backup of the database must be performed.

   Important: **Ensure that a new endpoint is created for the named instance before setting up a new availability group.**
2. Go to Management Studio, right click **AlwaysOn High Availability** and select **New Availability Group Wizard.**
3. In the Specify Availability Group Name screen, provide a name for the group. Click **Next**.

4. In the Select Database screen, select the temporary database created in Step 1. Ensure that th **Status** is **Meets prerequisites**. Click **Next**.
5. In the Replica screen, set the following:
   - On the Replicas tab, click the **Add Replica** button to add all the nodes. Select the **Synchronous Commit** option for both nodes. For secondary replicas, select the **Yes** option under the **Readable Secondary** column.
   - On the Endpoints tab, verify the server names and endpoint URLs.
   - On the Backup Preferences tab, select the **Any Replica** option to allow backup operation at both primary and secondary servers.
6. On the Listener tab, provide a fully qualified listener name, which is registered with the DNS, port (default 1433), and select the Static IP option. Click the **Add** button. In the Add IP Address window, add a static IP address. Like cluster creation, you need two IPs if the target servers are on two different subnets. Select the respective subnet from the dropdown and add the respective IP address for that.
7. On the Summary screen, verify the choices made in the wizard. Click **Finish** to start the process.
8. On the Select Initial Data Synchronization page, select the **Full** option. Click **Next**.
9. The Results screen shows if all the tasks are completed successfully. Click **Close**.

Additional Configuration for Multi-subnet Availability Group

There are two parameters that affect how the AGL is registered with DNS. By modifying these parameters on the server we can transparently change the experience of the client OS in its name resolution caching.

1. Open Power Shell as Administrator from the Primary node and import the **FailoverCluster** module using the following command:

   ```
   Import-Module FailoverClusters
   ```

2. To get the Get cluster and the listener name, use the following command:

   ```
   Get-ClusterResource
   ```

3. Change the value of the **RegisterAllProvidersIP** and **HostRecordTTL** parameters for both cluster (for windows failover) and listener (for SQL Server failover).

   Please note that you need to replace *<Cluster Name>* with the cluster name and *<Listener Name>* with the cluster listener name in the script below.

   ```
   Get-ClusterResource "<Cluster Name>" | Set-ClusterParameter RegisterAllProvidersIP
   0
   ```

   ```
   Get-ClusterResource "<Cluster Name>" |Set-ClusterParameter HostRecordTTL 60
   ```

   ```
   Get-ClusterResource "<Listener Name>" | Set-ClusterParameter
   RegisterAllProvidersIP 0
   ```

   ```
   Get-ClusterResource "<Listener Name>" | Set-ClusterParameter HostRecordTTL 60]
   ```

4. Restart the Cluster and the listener. Replace *<Cluster Name>* with the cluster name and *<Listener Name>* with the cluster listener name in the script below.

   ```
   Stop-ClusterResource "<Cluster Name>"
   ```

   ```
   Start-ClusterResource "<Cluster Name>"
   ```

   ```
   Stop-ClusterResource "<Listener Name>"
   ```

```
Start-ClusterResource "<Listener Name>"
```

Install the Application

- Install the ECE application. See “Installation Process” on page 65.

Post-Installation Tasks

Verifying Recovery Model

Verify that the recover model for ECE databases is set to `full`.

To view or change the recovery model:

1. In the SQL Server Management Studio, browse to the ECE databases.
2. Right-click the database, and from the context menu select **Properties**.
3. In the Database Properties window, go to the **Options** section and set the **Recovery model** to **Full**.
4. Click **OK**.

Backing up ECE Databases

- Take a full backup of all ECE databases - Active database, Master database and Reports database. As per availability group requirements, the database *must be* backed up once in full recovery mode.

Adding Databases to Availability Group

To add databases to the availability group:

1. Open SQL Server Management Studio and connect with the primary database server or Listener.
2. Go to **AlwaysOn High Availability > Availability Groups >** *Your Availability Group*.
3. Right-click the availability group and from the context menu select **Add database.**
4. On the Select Databases page, select the databases from the list of available databases and click **Next**.
5. On the Select Data Synchronization page, select the **Join Only** option. Click **Next**.
6. In the next window click **Connect** to check the connection with the secondary server then click on **Next**.
7. You will be notified if the connection is successful.

Run reports DB utility to configure secondary nodes

Running the Reports Database Utility

This utility needs to be run to complete the reports database configurations on the secondary nodes. Perform this task on the services server.

Note: The Reports Database utility should only be run for fresh installations and major version upgrades and not for minor upgrades.

To run the utility:

1. From the installation package, copy the **ReportsDB Utility (SQL Server Always On)** folder on the services server.
2. Open the `reportsdb_utility.properties` file in a text editor and set the following properties:
   - EGAIN_HOME_DIR: Provide the location of the ECE home directory.
   - IS_WINDOWS_AUTHENTICATION: Set the value to `true`.
   - CREATE_DBLINK_FROM_CONNPOOLMAP: Value is set to `true` and should not be changed.
   - REPORTS_DB_SERVER_NAME: Server name of the secondary node for the reports database.
   - REPORTS_DB_LST_PORT: Provide the port number.
   - REPORTS_DB_INSTANCE_NAME: Provide the instance name.
   - REPORTS_DB_NAME: Provide the name of the reports database.
   - ACT_DB_SERVER_NAME: Server name of the secondary node for the active database.
   - ACT_DB_LST_PORT: Provide the port number.
   - ACT_DB_INSTANCE_NAME: Provide the instance name.
   - ACT_DB_NAME: Provide the name of the active database.
3. Open the command prompt as an administrator and navigate to the utility folder.
4. Run the following command:

   Utility_Location`\reportsdb_utility.bat createDBObjects`

   For example, `D:\utility\reportsdb_utility.bat createDBObjects`
5. The following log files are created at the same location from where the utility is run:
   - `reportsdb_validation.log:` Check this file to verify that no errors are logged in the file.
   - `eg_log_serv234_ReportsDBUtil.log`: Check the file to see the status of the utility. You will see the following message when all the tasks are completed - `ReportsDB utility is executed successfully`

Run the UpdateDBIndexStats Utility

Running the UpdateDBIndexStats Utility

The **UpdateDBIndexStats** Utility can be used for updating index statistics for ECE active and reports database specifically after a major upgrade.

To run the utility:

1. On the Services Server, open the **input.properties** file in a text editor.
2. Provide values for following properties in **input.properties** file:
   - ACTIVE_DATABASE_URL: Specify the JDBC URL for the Active DB. To obtain this URL, browse to the *ECE_HOME*`\eService\lib\deployment.zip` file, extract the `dataaccess\egpl_ds_connpool_map.xml` file, and perform the following steps:
     - Open `egpl_ds_connpool_map.xml` in a text editor.
     - Locate the `<connpool>` XML node definition having the name as **Platform_MSSQL_Pool**.
     - Locate the child node with the name **Url** in it. The content of this node is the JDBC URL for Active DB. (For example: `jdbc:sqlserver://<DB server name>:1433;integratedSecurity=true;databaseName=<`*Database Name*`>`)
   - ACTIVE_USER: If SQL authentication is used to connect to the Active DB, specify the user name that is used to connect to the Active DB. If Windows Authentication is used to connect to the Active DB, then keep this blank.
   - ACTIVE_PASS: If SQL authentication is used to connect to the Active DB, specify the password for the user name mentioned above. If Windows Authentication is used to connect to the Active DB, then keep this blank.
   - REPORTS_DATABASE_URL: Specify the JDBC URL for the Reports DB. To obtain this URL, browse to the *ECE_HOME*`\eService\lib\deployment.zip` file, extract the `dataaccess\egpl_ds_connpool_map.xml` file, and perform the following steps:
     - Open `egpl_ds_connpool_map.xml` in a text editor.
     - Locate the `<connpool>` XML node definition having the name as **ReportsDB_MSSQL_Pool**.
     - Locate the child node with the name **Url** in it. The content of this node is the JDBC URL for the Active DB. (For example: `jdbc:sqlserver://<DB server name>:1433;integratedSecurity=true;databaseName=<`*Database Name*`>`)
   - REPORTS_USER: If SQL authentication is used to connect to the Reports DB, specify the user name that is used to connect to the Reports DB. If Windows Authentication is used to connect to the Reports DB, then keep this field as blank.
   - REPORTS_PASS: If SQL authentication is used to connect to the Reports DB, specify the password for the user name mentioned above. If Windows Authentication is used to connect to the Reports DB, then keep this field as blank.
3. Save the changes.
4. Open `UpdateDBIndexStats.bat` in a text editor.
5. Replace `<JAVA_HOME>` with the JDK home directory. For example, `C:\ECE\jdk`.
6. Save the changes.

7. Run `UpdateDBIndexStats.bat file` in the command prompt.
8. After running the utility, check `UpdateDBIndexStats.log` (generated in the same folder) for details about the last execution of the utility.

Creating Jobs to Take Log backups on All Nodes

Perform this task on all active server nodes and all reports database nodes. Create jobs on all databases to take backups of logs every **30 minutes.** This is required as the database log grows rapidly when the Always On Availability feature is enabled.

You can use the following script to create jobs for log backups:

- `BACKUP LOG [`*eGActiveDB*`] TO DISK = '`*Path*`\eGActiveDB_LOG_backup.trn' WITH INIT`
- `BACKUP LOG [`*eGMasterDB*`] TO DISK = '`*Path*`\eGMasterDB_LOG_backup.trn' WITH INIT`
- `BACKUP LOG [`*eReportsDB*`] TO DISK = '`*Path*`\eGReportsDB_LOG_backup.trn' WITH INIT`

  Replace, *eGActiveDB*, *eGMasterDB*, and *eReportsDB* with the database names.

  Replace *Path* with the backup folder path.

Appendix C: Convert Existing Deployment to HA

- Converting Existing Two Server Installation to HA
- Converting Existing Distributed Server Installation to HA

Converting Existing Two Server Installation to HA

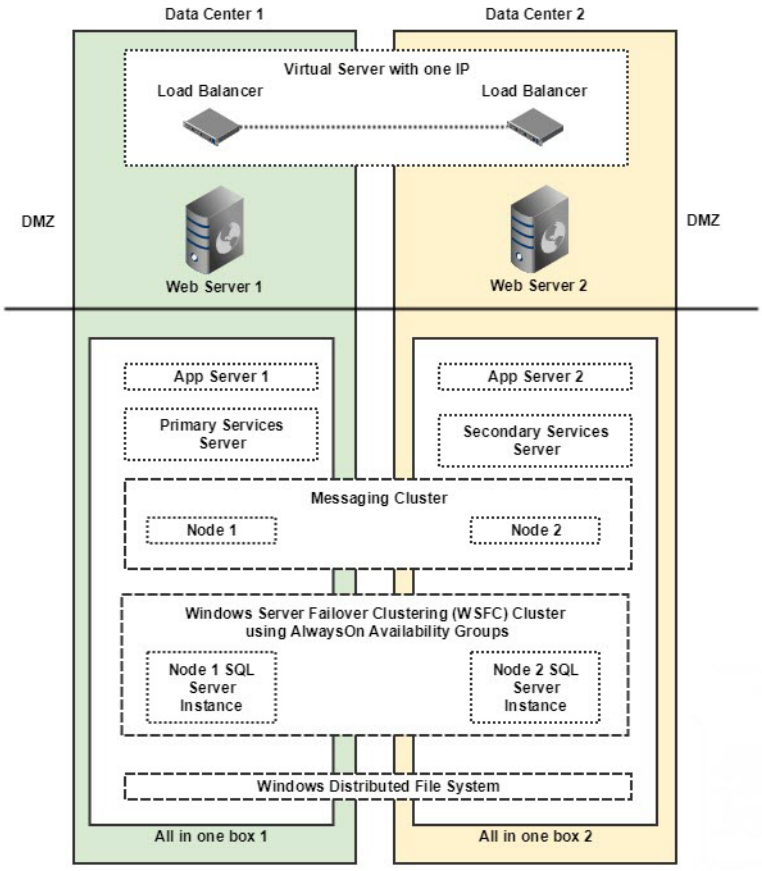
This section helps you convert your existing two server installation into an HA installation. Please ensure that the SQL is upgraded to the Enterprise version.

Existing installation and VMs:

- **VM-A:** ECE All-in-One server (file, messaging, application, services and database components are installed on this server). Please create a new home directory for the installation, for example, ECE_ALL. This will become the Windows Distributed File System Node1 for file server.
- **VM-B:** ECE Web server component

Acquire New VMs for Side B (Windows 2022):

- **VM-C:** For installing the second Messaging, Services, and Application server components, please create a new home directory, for example, ECE_AMS and another home directory to install the file server, for example, ECE_FILE. This will become the Windows Distributed File System Node2 for file server. For more information on the creation of the ECE_FILE folder and its sub folders for file server replication, see "Appendix A: Distributed File System Configuration" on page 135.
- **VM-D:** For second web server component



Converting Existing File Server to DFS

Setting up Distributed File System (DFS)

- Install and Enable DFS Namespace and DFS Replication roles and features on **VM-A** and **VM-C**. For details, see "Appendix A: Distributed File System Configuration" on page 135.

Installing Second Messaging, Services, and Application Server Components

- Install the new components on **VM-C**. While installing:
  - In the Installation Options window, select Messaging Server, Services Server, and Application Server.
  - In the File Server Parameters window, provide the new DFS location.

Installing Second Web Server Component

- Install the new component on **VM-D**. While installing:
  - In the Installation Options window, select Web Server.

Converting Databases to SQL Server to Always On Configuration

Perform all the tasks listed in the following table in the order defined.

Task	Notes
Perform all the required pre-installation tasks on the new database servers. "Pre-Installation Tasks" on page 27	
"Stopping ECE Application and Disable SQL Jobs." on page 155	
If your existing database uses SQL Authentication, convert SQL Authentication to Windows Authentication. "Converting SQL Authentication to Windows Authentication" on page 155	
"Installing Failover Clustering Feature" on page 142	
"Creating Prestage Cluster Computer Objects in Active Directory Domain Services (AD DS)" on page 142	
"Creating Windows Failover Cluster" on page 144	
"Configure Cluster Quorum Settings" on page 145	
"Enabling Always On Availability Groups Feature on SQL" on page 146	
"Configuring SQL Server Always On Availability Groups" on page 146 ▸ In Step 4, select existing ECE active, master, and reports databases. ▸ In Step 6, select **Join** option.	
"Verifying Recovery Model" on page 148	

Task	Notes
"Backing up and Restoring Databases" on page 156	
"Adding Databases to Availability Group" on page 148	
"Updating Files and Databases with New Listener Names" on page 156	
Ensure that the load balancer URL is being used as the External URL of Application. For more information, refer to"Mandatory Settings" on page 94	
"Run reports DB utility to configure secondary nodes" on page 149	
"Creating Jobs to Take Log backups on All Nodes" on page 151	
"Creating an Encrypted SQL Server Database" on page 85	
"Starting the SQL Jobs and ECE Application" on page 157	

Stopping ECE Application and Disable SQL Jobs.

1. Stop the ECE application. See "Stopping ECE" on page 92.
2. Disable the following jobs on ECE database machines.
   - **EG_OFFERS_SUMMARIZATION**_*Active_Database_Name*
   - **egicm_data_cleanup_job**_*Active_Database_Name*
   - **egicm_reindex_active_job**_*Active_Database_Name*
   - **egicm_reindex_reports_job**_*Reports_Database_Name*
   - **egut_async_index_create**_*Active_Database_Name*
   - **egut_async_index_create**_*Reports_Database_Name*
   - **populatesmy**_*Reports_Database_Name*

Converting SQL Authentication to Windows Authentication

Important: **Windows Authentication is required for setting Always On. You need to perform this task only if your existing installation does not use Windows Authentication.**

To convert SQL authentication to Windows authentication:

1. Stop the ECE application.
2. Follow steps to configure Windows Authentication on MSSQL Server as mentioned in the installation guide.
3. On the file server, go to the ECE installation folder.
4. Browse to *ECE_HOME*`\eService\lib\deployment.zip`, extract the `\dataaccess\egpl_ds_connpool_map.xml` file, and make the following changes:
   a. Locate **<conn_pool_list**.
   b. In all **connpool** nodes in the list, remove the values of **User** and **Password** nodes.

c. In all **connpool** nodes in the list, for the **Url** node, change all references of `integratedSecurity=false` to `integratedSecurity=true`

For example, change:

```
<User egid="3026">eGActiveDB</User>
<Password egid="3027">36423441363</Password>
<Url
egid="3028">jdbc:sqlserver://ussuh23:1433;integratedSecurity=false;databaseN
ame=eGActiveDB</Url>
```

to

```
<User egid="3026"></User>
<Password egid="3027"></Password>
<Url
egid="3028">jdbc:sqlserver://ussuh23:1433;integratedSecurity=true;databaseNa
me=eGActiveDB</Url>
```

d. Add the updated file in `deployment.zip`.

Backing up and Restoring Databases

To backup and restore databases:

1. Take Full backups of active, master, and reports database in the primary server location.
2. Now, move the backup in a temporary location in the new secondary database server.
3. Take Transaction Log backup of active, master, and reports database in primary server location (same folder path where full backup was saved).
4. Restore all three full backups and transaction log backups with **NORECOVERY** at the secondary database server.

Updating Files and Databases with New Listener Names

Modifying Master Database

Perform this task on the primary node.

To modify the database server name for master database:

- Run the following query on the ECE master database:

```
UPDATE [dbo].[EGPL_DSM_HOST]
SET [HOST_NAME] = '<Listener Name>'
WHERE [DESCRIPTION] = 'Database Server'
```

Replace *<Listener Name>* with the cluster listener name.

Starting the SQL Jobs and ECE Application

1. Enable the following jobs on ECE database machines.
   - **EG_OFFERS_SUMMARIZATION_***Active_Database_Name*
   - **egicm_data_cleanup_job_***Active_Database_Name*
   - **egicm_reindex_active_job_***Active_Database_Name*
   - **egicm_reindex_reports_job_***Reports_Database_Name*
   - **egut_async_index_create_***Active_Database_Name*
   - **egut_async_index_create_***Reports_Database_Name*
   - **populatesmy_***Reports_Database_Name*
2. Start the ECE application. See "Starting ECE" on page 91.

Updating Finesse Files

The Desktop Layout gadget in Finesse points to the ECE web server in the installation. If you are using a load balancer, after converting the deployment to HA, you must update the layout to point to the load balancer.

To update the Finesse layout settings:

1. Launch the URL: `https://`*Finesse_Server_Name*`/cfadmin`. Login as a finesse administrator.
2. In the **Desktops Layout** section, locate the node for `ece.xml`. In the value, replace the web server name with the host name of the load balancer used for ECE web servers.

   For example, change:

   ```
   <gadgets>
   <gadget>https://ECEWebServer.domain.com/system/templates/finesse/gadget/agent/ece.xml</gadget>
   </gadgets>
   ```

   to

   ```
   <gadgets>
   <gadget>https://ECELoadBalancer.domain.com/system/templates/finesse/gadget/agent/ece.xml</gadget>
   </gadgets>
   ```
3. Save the changes.

Converting Existing Distributed Server Installation to HA

This section helps you convert your existing distributed server installation into an HA installation.

Existing installation and VMs:

- **VM-1A:** File server

- **VM-2A:** Database server (active and master databases)
- **VM-3A:** Database server (Reports database)
- **VM-4A:** Messaging server
- **VM-5A:** Services Server
- **VM-6A to VM-10A:** Application server
- **VM-11A to VM-15A:** Web Server

Acquire New VMs for Side B:

- **VM-1B:** File server (Windows Distributed File System Node 2)
- **VM-2B:** Database server (active and master databases)
- **VM-3B:** Database server (reports database)
- **VM-4B:** Messaging server
- **VM-5B:** Services server
- **VM-6B to VM-10B:** Application server
- **VM-11B to VM-15B:** Web Server

Converting Existing File Server to DFS

Setting up Distributed File System (DFS)

- Install and Enable DFS Namespace and DFS Replication roles and features on **VM-1A** and **VM1-B**. For details, see "Appendix A: Distributed File System Configuration" on page 135.

Updating Files to Use DFS

To update files on original ECE server (VM-1A) to use new DFS location:

1. Browse to *ECE_HOME*`\eService\bin\platform\windows`
2. Open the following files in a text editor: `egainstart.bat` and `egainstop.bat` files.
3. Locate the property `env.fs.shared.location` in both the files and change the value to point to the new DFS location. For example, the property will look like `SET env.fs.shared.location=\\egeng.info\DFS1\ECE\eService`

Converting Databases to SQL Server Always On Configuration

- Perform all the tasks listed in this section: "Converting Databases to SQL Server to Always On Configuration" on page 154.

Installing Second Messaging Server Component

- Install the new messaging server component on **VM-4B**. While installing:
  - In the Installation Options window, select Messaging Server.
  - In the File Server Parameters window, provide the new DFS location.

Installing Second Services Server Component

- Install the new services server component on **VM-5B**. While installing:
  - In the Installation Options window, select Services Server.
  - In the File Server Parameters window, provide the new DFS location.

Installing Additional Application Server Components

- Install the new application server component on **VM-6B** to **VM10B**. While installing:
  - In the Installation Options window, select Application Server.
  - In the File Server Parameters window, provide the new DFS location.

Installing Additional Web Server Components

- Install the new web server component on **VM-11B** to **VM-15B**. While installing:
  - In the Installation Options window, select Web Server.
  - In the Application Server Parameters window, provide the Application Server name.

Appendix D: Enhancements in ECE 15

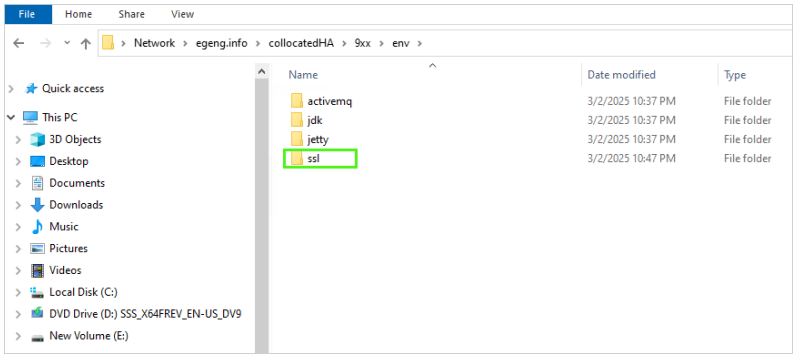
- Inter-component SSL Enabled by Default
- Automated SSL Certificate Rotation
- Centralized Log Collection for HA and Distributed Deployments

This appendix outlines key enhancements introduced in the latest ECE 15 release, including updates to SSL certificate management and centralized log collection for high availability (HA) and distributed deployments.

Inter-component SSL Enabled by Default

- With ECE 15, inter-component SSL is now enabled by default to enhance security across all application components. As a result, the following components will communicate securely using SSL:
  - Application Server
  - Services Server
  - Messaging Server
- The generated SSL certificates are stored at the following location:

  <*File_Server_Installation_Directory*>\env\ssl



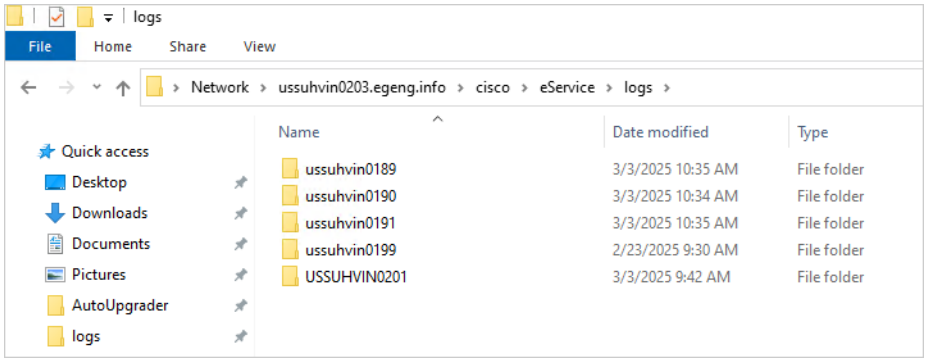
Automated SSL Certificate Rotation

- To ensure security compliance, SSL certificates will now be automatically rotated by the installer as part of major releases. The default expiration period for these certificates is five years, after which they will be replaced during an upgrade.

Centralized Log Collection for HA and Distributed Deployments

- A new centralized log collection method has been introduced to improve log management in high availability (HA) and fully distributed deployments. With this enhancement, all Java process logs from different servers are now available in a single, centralized location on the `FILE_SERVER`. The logs are stored in the following directory: <*FILE_SERVER_INSTALLATION_DIR*>\eService\logs\<*SERVERNAME*>. Here, *SERVERNAME* represents the specific server type, such as
  - Application Server

- Services Server
- Messaging Server



- This enhancement simplifies log retrieval and troubleshooting by providing a unified location for monitoring logs across all servers.