## 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  
    - Planning the File Server ........................................ 18  
      - Installing the Application on a SQL Server 2016 Cluster .............................. 18  
      - Planning Database Server Distribution .............................................. 19  
      - Choosing Authentication Method for Database Connectivity ..................... 19  
    - Planning Messaging Servers ................................. 19  
    - Planning Services Servers ................................... 19  
    - Planning Application Servers ................................ 20  
    - Planning Web Servers ......................................... 20  
    - Load Balancing Considerations ................................ 20  
    - Planning for High Availability Across Geographies ....................................... 20
Chapter 2: Pre-Installation Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparing Virtual Machine</td>
<td>25</td>
</tr>
<tr>
<td>Obtain Installation Media</td>
<td>25</td>
</tr>
<tr>
<td>Download OVA for ECE</td>
<td>25</td>
</tr>
<tr>
<td>Create Virtual Machines from the OVA</td>
<td>25</td>
</tr>
<tr>
<td>Install Microsoft Windows Server</td>
<td>25</td>
</tr>
<tr>
<td>Install VMware Tools</td>
<td>25</td>
</tr>
<tr>
<td>Install Microsoft SQL Server</td>
<td>26</td>
</tr>
<tr>
<td>Mounting and Unmounting ISO Files</td>
<td>26</td>
</tr>
<tr>
<td>Disabling Loopback Adapter Configuration</td>
<td>26</td>
</tr>
<tr>
<td>Verifying Network Configuration</td>
<td>27</td>
</tr>
<tr>
<td>Configuring Port Numbers Between Components</td>
<td>28</td>
</tr>
<tr>
<td>Setting Up User Accounts and Permissions</td>
<td>30</td>
</tr>
<tr>
<td>Setting Up Domain Account</td>
<td>30</td>
</tr>
<tr>
<td>Configuring Permissions on Active Directory Server</td>
<td>31</td>
</tr>
<tr>
<td>Setting up Distributed File System (DFS)</td>
<td>33</td>
</tr>
<tr>
<td>Enabling PowerShell Remote Commands</td>
<td>33</td>
</tr>
<tr>
<td>Preparing Database Server VMs</td>
<td>34</td>
</tr>
<tr>
<td>Setting up for Always On Availability Group Clustering</td>
<td>34</td>
</tr>
<tr>
<td>Installing SQL Server Management Studio (SSMS)</td>
<td>34</td>
</tr>
<tr>
<td>Verifying Microsoft SQL Server Features</td>
<td>34</td>
</tr>
<tr>
<td>Verifying Collation Settings</td>
<td>34</td>
</tr>
<tr>
<td>Creating SQL User for Installing ECE Databases</td>
<td>35</td>
</tr>
<tr>
<td>Assigning Permissions to Domain User</td>
<td>35</td>
</tr>
<tr>
<td>Configuring Database Servers</td>
<td>35</td>
</tr>
<tr>
<td>Configuring Microsoft DTC Settings</td>
<td>35</td>
</tr>
<tr>
<td>Configuring SQL Server Integration Service on the Reports Database</td>
<td>36</td>
</tr>
<tr>
<td>Configuring Permissions for User Accounts</td>
<td>37</td>
</tr>
<tr>
<td>Verifying Server Privileges</td>
<td>37</td>
</tr>
<tr>
<td>Creating Directory for Data Files</td>
<td>37</td>
</tr>
<tr>
<td>Running Services</td>
<td>37</td>
</tr>
<tr>
<td>Preparing Web Server VMs</td>
<td>39</td>
</tr>
</tbody>
</table>
Configuring Roles and Features .................................................. 39
Installing Modules on Web Servers ............................................. 40
Configuring Permissions on IIS Config Folder. ............................. 40
Running the World Wide Web Publishing Service. ...................... 40
Configuring Virus Scanners ..................................................... 40
Configuring SMTP Port in Virus Scanners. ................................. 40
Configuring Virus Scanning Exclusions ..................................... 40
Verifying Packaged CCE Configuration ..................................... 41

Chapter 3: Prepare Packaged CCE for the Integration ....................... 43

Relationship Between Objects in Packaged CCE and ECE .................. 44
Adding ECE to Packaged CCE Inventory ..................................... 44
For 2000 Agent Deployments .................................................. 44
For 400 & 12000 Agent Deployments ........................................ 45
Configuring Packaged CCE ..................................................... 45
Configuring Call Types ......................................................... 47
Configuring Application Path .................................................. 47
Configuring Agents .............................................................. 48
Configuring Skill Groups ........................................................ 49
Configuring Dialed Number ..................................................... 50
Creating Scripts ................................................................. 50
Configuring Precision Routing ................................................ 55
Creating Attributes .............................................................. 55
Assigning Attributes to Agents ............................................... 56
Creating Precision Queues ..................................................... 56
Adding Precision Queue Node to the Scripts ............................... 56

Adding MR PIM for ECE ....................................................... 57
Adding Agent PG PIM for ECE .............................................. 58
Adding CTI for ECE ............................................................ 58
Configuring Finesse ............................................................ 59

Chapter 4: Installation Process .................................................... 60

Installation Overview .......................................................... 61
For 400 Agent Deployments .................................................. 61
For 400 Agent Deployments (HA) ............................................ 61
For 400+ Agent Deployments ................................................. 62
Chapter 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
- Encrypting Primary Node
- Encrypting Other Nodes
- Configuring SMTP Server Relay Address List
- Configuring Finesse
- Configuring Finesse Settings and Layout
- Configuring Single Sign-On
- Starting ECE
- Troubleshooting Application Start-Up Issues
- Stopping ECE
- Signing in to ECE
- Signing in to Agent Console
- Signing in to All Other Consoles
- Integrating ECE with Packaged CCE
- Configuring Important Settings
- Mandatory Settings
- Optional Settings
- Adding Data Source in CUIC for ECE Reports
- Creating a Database User on ECE Reports Database
Chapter 6: Single Sign-On Configuration ................................................................. 91

About Single Sign-On with Cisco IDS ............................................................... 92
Configuring Single AD FS Deployment ......................................................... 92
Configuring Relying Party Trust for ECE ..................................................... 92
Configuring Split AD FS Deployment ............................................................ 100
Adding Security Certificates for the AD FS Domains ............................... 100
Configuring Relying Party Trust for Shared AD FS in Customer AD FS .... 101
Configuring Claims Provider Trust for Customer AD FS in Shared AD FS .... 105
Configuring Relying Party Trust for ECE in Shared AD FS ....................... 109
Configuring Single Sign-On in ECE ....................................................... 116

Chapter 7: SSL Configuration .............................................................................. 117

Installing a Security Certificate ................................................................. 118
Generating a Certificate Signing Request .................................................... 118
Submitting the Certificate Request .......................................................... 120
Installing the Certificate on the Web Server ............................................. 120
Binding the Certificate to the Application Website ...................................... 122
Testing SSL Access .................................................................................. 123
Configuring SSL or TLS for Retriever and Dispatcher Services ............... 123
  On the File Server .................................................................................. 124
  Installing Certificates ............................................................................ 124
  Deleting Certificates ............................................................................ 125
  Enable SSL for Specific Email Aliases ................................................ 125

Appendix A: Distributed File System Configuration ...................................... 126

Installing DFS Management .................................................................... 127
Creating Shared Folders ................................................................. 127
Creating New Namespace ........................................................... 127
Adding Namespace Server ......................................................... 128
Adding Folders and Configuring Replication ............................... 128

Appendix B: SQL Always-On Configuration ...................................... 129

About Always On Availability Group Clustering .............................. 130
Pre-Installation Tasks ................................................................. 130
Installing Failover Clustering Feature ......................................... 130
Creating Prestage Cluster Computer Objects in Active Directory Domain Services (AD DS) ........................................................................ 130
Prestaging the CNO in AD DS ......................................................... 131
Granting User Permissions to Create Cluster ................................. 131
Granting the CNO Permissions to the OU ....................................... 131
Creating Windows Failover Cluster .............................................. 132
Configure Cluster Quorum Settings .............................................. 132
Enabling Always On Availability Groups Feature on SQL .............. 133
Configuring SQL Server Always On Availability Groups .............. 133
Install the Application ................................................................. 134
Post-Installation Tasks ................................................................. 134
Verifying Recovery Model ......................................................... 134
Backing up ECE Databases ......................................................... 134
Adding Databases to Availability Group ....................................... 135
Run reports DB utility to configure secondary nodes ....................... 135
Running the Reports Database Utility ......................................... 135
Creating Jobs to Take Log backups on All Nodes ......................... 136

Appendix C: Convert Existing Deployment to HA ................................. 137

Converting Existing Two Server Installation to HA (Windows 2016) ................................. 138
Converting Existing File Server to DFS ......................................... 139
Setting up Distributed File System (DFS) ..................................... 139
Updating Files to Use DFS ......................................................... 139
Installing Second Messaging, Services, and Application Server Components ................................................................. 139
Installing Second Web Server Component .................................. 139
Converting Databases to SQL Server to Always On Configuration ................................................................. 139
Stopping ECE Application and Disable SQL Jobs ......................... 140
Converting SQL Authentication to Windows Authentication ............ 140
Backing up and Restoring Databases ........................................... 141
Updating Files and Databases with New Listener Names .................. 141
Starting the SQL Jobs and ECE Application ................................. 143
Updating Finesse Files .............................................................. 143
Converting Existing Two Server Installation to HA (Windows 2012) ........ 144
Converting Existing File Server to DFS ........................................ 144
Installing Second Messaging and Application Server Components ........ 144
Installing Second Services Server Component ............................... 144
Installing Second Web Server Component .................................... 144
Converting Databases to SQL Server to Always On Configuration ........ 145
Updating Finesse Files .............................................................. 145
Converting Existing Distributed Server Installation to HA (Windows 2012 & 2016) . 145
Converting Existing File Server to DFS ........................................ 146
Setting up Distributed File System (DFS) .................................... 146
 Updating Files to Use DFS ......................................................... 146
Installing Second Messaging Server Component ............................ 146
Installing Second Services Server Component ............................... 146
Installing Additional Application Server Components ...................... 146
Installing Additional Web Server Components ............................... 146
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.

**Important:** New installations for ECE 12.0(1) are not supported on Windows Server 2012. If you need to access the archived documentation for the old platform, please contact Cisco Support.

Change History

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

<table>
<thead>
<tr>
<th>Change</th>
<th>See</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced the Planning Components for Specific Configurations and High Availability section with more details about High Availability options.</td>
<td>“Planning Components for Specific Configurations and High Availability” on page 18</td>
<td>October, 2019</td>
</tr>
<tr>
<td>Added information about number of VMs needed for installing the application.</td>
<td>“Installation Overview” on page 61</td>
<td></td>
</tr>
<tr>
<td>Added details about encrypting primary and secondary nodes.</td>
<td>“Creating an Encrypted SQL Server Database” on page 79</td>
<td></td>
</tr>
<tr>
<td>New chapter added: Distributed File System Configuration</td>
<td>“Appendix A: Distributed File System Configuration” on page 126</td>
<td></td>
</tr>
<tr>
<td>New chapter added: SQL Always-On Configuration</td>
<td>“Appendix B: SQL Always-On Configuration” on page 129</td>
<td></td>
</tr>
<tr>
<td>New chapter added: Convert Existing Deployment to HA</td>
<td>“Appendix C: Convert Existing Deployment to HA” on page 137</td>
<td></td>
</tr>
</tbody>
</table>
Related Documents

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

<table>
<thead>
<tr>
<th>Subject</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete documentation for Enterprise Chat and Email, for both Cisco Unified Contact Center Enterprise (UCCE) and Cisco Packaged Contact Center Enterprise (PCCE)</td>
<td><a href="https://www.cisco.com/c/en/us/support/contact-center/enterprise-chat-email-12-0-1/model.html">https://www.cisco.com/c/en/us/support/contact-center/enterprise-chat-email-12-0-1/model.html</a></td>
</tr>
</tbody>
</table>

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/?cisco/?support/?notifications.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.

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

(Document conventions)
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.

<table>
<thead>
<tr>
<th>Component</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Workflow</td>
<td>▶ The Workflow Assignment Service publishes a message to application servers when a new email is assigned to a user.</td>
</tr>
<tr>
<td></td>
<td>▶ 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.</td>
</tr>
<tr>
<td>Email Retriever and Dispatcher</td>
<td>The application server publishes a message to the Retriever and Dispatcher Services when an email alias is created or modified from the Administration Console.</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>▶ The Scheduler Service publishes a message to the Reports Service when the schedule for a report fires.</td>
</tr>
<tr>
<td></td>
<td>▶ The application server publishes a message to the Distributed Services Manager (DSM) whenever an agent logs in to or logs out of the application.</td>
</tr>
<tr>
<td></td>
<td>▶ The application server publishes a message to all other application servers and services when a Custom attribute is created from the Tools Console.</td>
</tr>
<tr>
<td></td>
<td>▶ The application server publishes a message to other application servers every time an article or topic is added, modified, or removed.</td>
</tr>
</tbody>
</table>

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](image)

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

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 2016 Cluster

- ECE can be installed in a Microsoft SQL Server 2016 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 2016 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 35. You may also need to complete certain tasks described in “Setting Up User Accounts and Permissions” on page 30.

Choosing Authentication Method for Database Connectivity

> Important: If you are planning to use Always On Availability Group clustering, you must use Windows Authentication.

- The application supports two methods of authentication for connecting to the database.
  - SQL Server authentication
  - Windows authentication

- As part of the installation process, you will be asked to select the authentication method. Your selection will depend on the security policies of your organization, and should be consistent with the authentication method configured in SQL Server.

If you choose Windows authentication, certain additional steps must be completed before you begin installing the application. These steps are outlined in the “Setting Up User Accounts and Permissions” on page 30. Also refer to “Configuring Database Servers” on page 35.

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.
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.

  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.

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 400 Agent Deployments

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 401 to 1500 Agent Deployments

In this deployment, the ECE components are installed on 30 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-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 24], installation tasks [page 60], and post-installation tasks [page 76], to install ECE. To set up SSL, follow instructions in the “SSL Configuration” on page 117.
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
- Enabling PowerShell Remote Commands
- 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 Packaged Contact Center Enterprise Download Software page: https://software.cisco.com/download/type.html?mdfid=284360381&catid=null
2. Click **Packaged Contact Center Enterprise Virtual Machine Templates**.
3. Download the Virtual Machine Templates zip file for the release.
4. Extract the file and save the OVAs to your local drive.

### Create Virtual Machines from the OVA

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

### Install Microsoft Windows Server

- Follow the Microsoft documentation to install Microsoft Windows Server 2016. While installing, make sure you select the **Custom: Install Windows only (advanced)** option, and select Drive 0 to install Microsoft Windows Server.

### Install VMWare Tools

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

- Follow the Microsoft documentation to install Microsoft SQL Server 2016 Service Pack 2, Cumulative Update 2 or higher, Standard Edition or Enterprise Edition. Make sure the required features for Microsoft SQL (page 34) are installed on the VM and the collation settings (page 34) are configured properly.

Mounting and Unmounting ISO Files

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

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

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

Disabling Loopback Adapter Configuration

ECE cannot be installed on 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 28.

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.
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 (*).

<table>
<thead>
<tr>
<th>From Server</th>
<th>To Server</th>
<th>Default Destination Ports and Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Workstation</td>
<td>Web Server</td>
<td>80 [Protocol: HTTP]</td>
</tr>
<tr>
<td>(Internet)</td>
<td></td>
<td>443 [Protocol: HTTPS]</td>
</tr>
<tr>
<td>Finesse Desktop</td>
<td>Web Server</td>
<td>80 [Protocol: HTTP]</td>
</tr>
<tr>
<td>(Internet)</td>
<td></td>
<td>443 [Protocol: HTTPS]</td>
</tr>
<tr>
<td>Application Server</td>
<td>Services Server</td>
<td>15099 (RMI Registry port) [Protocol: RMI]*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>49152 – 65535 (Dynamic port range used by RMI server objects) [Protocol: TCP]</td>
</tr>
<tr>
<td>From Server</td>
<td>To Server</td>
<td>Default Destination Ports and Protocols</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Application Server</td>
<td>File Server</td>
<td>139 or 445 [Protocol: NETBIOS - TCP]</td>
</tr>
<tr>
<td>Application Server</td>
<td>Database Server</td>
<td>1433 [Protocol: TCP] *</td>
</tr>
<tr>
<td>Application Server</td>
<td>Messaging Server</td>
<td>15097 [Protocol: TCP] *</td>
</tr>
<tr>
<td>Application Server</td>
<td>Application Server</td>
<td>2434 [Protocol: TCP]*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6701 [Protocol: TCP]*</td>
</tr>
<tr>
<td>Application Server</td>
<td>SMTP Server</td>
<td>25 [Protocol: SMTP]</td>
</tr>
<tr>
<td>Application Server</td>
<td>SMTP or ESMTP Server (with SSL enabled)</td>
<td>587 [Protocol: SMTP or ESMTP]</td>
</tr>
<tr>
<td>Application Server</td>
<td>IMAP Server</td>
<td>143 [Protocol: IMAP]</td>
</tr>
<tr>
<td>Application Server</td>
<td>IMAP Server (with SSL enabled)</td>
<td>993 [Protocol: IMAP]</td>
</tr>
<tr>
<td>Web Server</td>
<td>Application Server</td>
<td>9001 [Protocol: TCP]*</td>
</tr>
<tr>
<td>Messaging Server</td>
<td>File Server</td>
<td>139 or 445 [Protocol: NETBIOS - TCP]</td>
</tr>
<tr>
<td>Messaging Server</td>
<td>Database Server</td>
<td>1433 [Protocol: TCP] *</td>
</tr>
<tr>
<td>Services Server</td>
<td>File Server</td>
<td>139 or 445 [Protocol: NETBIOS - TCP]</td>
</tr>
<tr>
<td>Services Server</td>
<td>Database Server</td>
<td>1433 [Protocol: TCP] *</td>
</tr>
<tr>
<td>Services Server</td>
<td>Messaging Server</td>
<td>15097 [Protocol: TCP] *</td>
</tr>
<tr>
<td>Services Server</td>
<td>Services Server</td>
<td>47500 [Protocol: TCP] *</td>
</tr>
<tr>
<td>Services Server</td>
<td>SMTP or ESMTP Server</td>
<td>25 [Protocol: SMTP or ESMTP]</td>
</tr>
<tr>
<td>Services Server</td>
<td>SMTP or ESMTP Server (with SSL enabled)</td>
<td>587 [Protocol: SMTP or ESMTP]</td>
</tr>
<tr>
<td>Services Server</td>
<td>POP3 Server</td>
<td>110 [Protocol: POP3]</td>
</tr>
<tr>
<td>Services Server</td>
<td>POP3 Server (with SSL enabled)</td>
<td>995 [Protocol: POP3]</td>
</tr>
<tr>
<td>Services Server</td>
<td>IMAP Server</td>
<td>143 [Protocol: IMAP]</td>
</tr>
<tr>
<td>Services Server</td>
<td>IMAP Server (with SSL enabled)</td>
<td>993 [Protocol: IMAP]</td>
</tr>
<tr>
<td>Active Database Server</td>
<td>File Server</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Reports Database Server</td>
<td>Active Database Server</td>
<td>1433 [Protocol: TCP]*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>135 [Port for Remote Procedure Call (RPC)]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5000-5020 (Port range for RPC ports required for MSDTC to work across firewall)</td>
</tr>
<tr>
<td>Services Server</td>
<td>Primary CTI Server</td>
<td>42027*</td>
</tr>
<tr>
<td>Services Server</td>
<td>Secondary CTI Server</td>
<td>42028*</td>
</tr>
<tr>
<td>Services Server</td>
<td>Media Routing Peripheral Gateway</td>
<td>38002*</td>
</tr>
</tbody>
</table>
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. This account is also used to run the ECE services after installing the application (page 83). ECE web server can be installed in DMZ and can have a different domain account.

Setting Up Domain Account

- Request your IT department to create the following accounts.

**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.

<table>
<thead>
<tr>
<th>Account Type</th>
<th>Description</th>
<th>Privileges Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Account</td>
<td>You will use this account to install ECE. This account will also be used in future to install ECE updates and do version upgrades. This can be an existing user with Administrator privileges on the server.</td>
<td>Administrator</td>
</tr>
<tr>
<td>Service Account</td>
<td>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.</td>
<td>Log on as Service</td>
</tr>
</tbody>
</table>
Conifguring 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 30). 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 133) 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/serv235.company.na:1433 domain1\SQLSERVICEUSER
   setspn -A MSSQLSvc/serv235.company.na:MSSQLSERVER domain1\SQLSERVICEUSER
   ```


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.

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.

![Set delegation properties for database server](image.png)

**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 126.

**Enabling PowerShell Remote Commands**

Perform these tasks on the file server and reports database server.

**To enable PowerShell remote commands:**

1. On the file and reports database servers, ensure the Windows service **Windows Remote Management Service** is running. If file server is going to be installed on NAS or DFS, then run this service on the server from where you will install the file server and the databases.

2. On the reports database server, start **powershell** as an administrator. Run the following command **Enable-PSRemoting –Force**. This will enable the PowerShell Remoting (PSRemoting) Feature.

   The following two steps are required only when the file and databases servers are going to be installed on separate VMs.

3. On the file server, add the fully qualified domain name (FQDN) of the reports database server in the list of trusted hosts in **Windows Remote Management Service** (WinRM). If file server is going to be installed on NAS or DFS, then perform this task on the server from where you will install the file server and the databases. Sample powershell command: **winrm s winrm/config/client ' @{TrustedHosts="ReportsDB.company.com"}’**
4. On the reports database server, add the fully qualified domain name (FQDN) of the file server in the list of trusted hosts in Windows Remote Management Service (WinRM). If file server is going to be installed on NAS or DFS, then add the server from where you will install the file server and the databases. Sample powershell command:

```
winrm set winrm/config/client
@{TrustedHosts="FileServer.company.com"}
```

## Preparing Database Server VMs

### 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 129.

---

**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 2016. Refer the Microsoft documentation for details about doing this task.

### Verifying Microsoft SQL Server Features

Ensure that the following Microsoft SQL Server features are installed.

- **Instance Feature:**
  - Database Engine Services > Full Text and Semantic Extraction for Search

- **Shared Features**
  - Client Tools Connectivity
  - Integration Services
  - Client Tools SDK
  - SQL Client Connectivity SDK

### Verifying Collation Settings

- Collation settings are typically chosen while installing SQL Server 2016. Since collations specify the rules for how strings of character data are sorted and compared, based on particular languages, a particular type of collation is required for the application to process and present information accurately.

  On the Collation settings screen, choose SQL Collations and select the following option: **Dictionary order, case-insensitive, for use with 1252 Character Set.** For example, SQL_Latin1_General_CP1_C1_AS.

  Although this is the recommended collation, it is not mandatory. Any ASCII, case insensitive collation can
be used. If you have already installed SQL Server 2016, consult your DBA and verify that the collation setting chosen is ASCII (case insensitive). The application databases will be installed using the collation that is configured for MSSQL Server.

Creating SQL User for Installing ECE Databases

Skip this section if you want to use the default $A 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 30).

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 other databases 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 31. 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 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:**

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 Accounts 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 2016.

9. Now, start the two services in the following order:
   a. Distributed Transaction Coordinator
   b. SQL Server (MSSQLSERVER) for Microsoft SQL 2016.

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.

---

## Configuring SQL Server Integration Service on the Reports Database

The application uses the functionality provided by the SQL Server Integration Services (SSIS) to allow custom data to be available for inclusion in data extracts. Note that custom data is not available in the reports that are included out-of-the-box. There are three parts to completing this task:

1. Configuring permissions for user accounts. (page 37).
2. Verify Replace a process-level token privilege has been enabled for the server (page 37).
3. Finally, create a folder on the VM where all data files will be created by the application (page 37).
Configuring Permissions for User Accounts

This task is required while using Windows or SQL Authentication. Perform this task for the Install Account (page 30) created for installing the application.

To configure permissions:
1. From the SQL Management Studio, add the user account to Security > Logins. Assign the sysadmin role to this user.
2. From the Computer Management Console, add this user to the Remote Management Users Group.

Verifying Server Privileges

Ensure that the “Replace a process level token” privilege is enabled for the NT Service\MSSQL Server.

To verify server privileges:
1. On the database server where the Reports database is to be installed, open the command prompt and run gpedit.msc. The Local Group Policy Management Editor opens.
3. From the policy list, double-click Replace a process level token.
4. In the window that opens, click the Add User or Group... button.
5. Add the NT_SERVICE\DB_Instance_Name service account to the privilege.
   - If you are using the default instance name for the reports database, it will be NT_SERVICE\MSSQLSERVER.
   - If the reports database is installed with a named instance, add the service account NT_SERVICE\MSSQLDB_Instance_Name.
6. To apply your changes, restart the ECE server. If the privileges were already enabled on the service account, a reboot is not necessary.

Creating Directory for Data Files

Create a directory on the reports server VM, for example, D:\ssis_data and ensure that the SQL Services Account that you have created for the ECE application has write and modify permissions on this folder. If you didn’t create a SQL Services Account, check the permissions of the Service Account created for the ECE application (page 30).

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 30).

- 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.

Distributed Transaction Coordinator Service

To start the services:
1. Go to Start > Programs > Administrative Tools > Services.
2. For the SQL Full-text Filter Daemon Launcher, SQL Server Agent, SQL Server, and SQL Server Browser services check if the right domain account is used for starting the services.
   a. Select a service and right-click to open the menu.
   b. From the menu select Properties.
   c. In the Properties window, go to Log On tab and ensure the service is started using the same domain account that you have created for installing the ECE application (page 30).
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 4.6
- 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 4.6
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 30) 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

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 2016 Server machine, these exclusions must also be setup for Windows Defender.

<table>
<thead>
<tr>
<th>Item</th>
<th>Exclude Subfolders?</th>
<th>Execute permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows File Protection</td>
<td>--</td>
<td>Read, Write</td>
</tr>
<tr>
<td>All files of type LOG</td>
<td>--</td>
<td>Read, Write</td>
</tr>
<tr>
<td>Pagefile.sys</td>
<td>No</td>
<td>Read, Write</td>
</tr>
<tr>
<td>Drive:\ECE_Home\</td>
<td>Yes [other than Storage]</td>
<td>Read, Write</td>
</tr>
<tr>
<td>*.rll</td>
<td>No</td>
<td>Read, Write</td>
</tr>
</tbody>
</table>

On the Database Servers

Follow the instructions for your virus scanning software to exclude the following folders and file types. On a Windows 2016 Server machine, these exclusions must also be setup for the Windows Defender.

<table>
<thead>
<tr>
<th>Item</th>
<th>Exclude Subfolders?</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows File Protection</td>
<td>--</td>
<td>Read, Write</td>
</tr>
<tr>
<td>All files of type LOG, if any</td>
<td>--</td>
<td>Read, Write</td>
</tr>
<tr>
<td>Pagefile.sys</td>
<td>No</td>
<td>Read, Write</td>
</tr>
<tr>
<td>Drive:\Path_to_datafile</td>
<td>Yes</td>
<td>Read, Write</td>
</tr>
<tr>
<td>Drive:\Path_to_SSIS_ddatafile</td>
<td>Yes</td>
<td>Read, Write</td>
</tr>
<tr>
<td>*.mdf</td>
<td>No</td>
<td>Read, Write</td>
</tr>
<tr>
<td>*.ldf</td>
<td>No</td>
<td>Read, Write</td>
</tr>
<tr>
<td>*.ndf</td>
<td>No</td>
<td>Read, Write</td>
</tr>
<tr>
<td>*.dat</td>
<td>No</td>
<td>Read, Write</td>
</tr>
<tr>
<td>*.rll</td>
<td>No</td>
<td>Read, Write</td>
</tr>
</tbody>
</table>

Verifying Packaged CCE Configuration

- Verify that Packaged CCE and Microsoft Active Directory (AD) have been installed on separate servers. Refer to Unified CCE documentation for more details.
- Verify that the Packaged CCE and AD servers are in the same network as the ECE servers and are accessible from the ECE servers.
ECE uses the application instance, Multichannel, and the CUCM type of Agent PG. MRDs that are Application Path members on the Multichannel application instance are automatically imported during installation. Agents and skill groups, which belong to the CUCM type of Agent PG are imported during installation.

In Packaged CCE, configure the items to be used in ECE. These include:

- Peripherals
- Network Voice Response Units (Network VRUs)
- Call Type
- Script Selector
- Application Paths and Path Members
- Agents
- Skill Groups
- ICM Scripts

For details, see “Prepare Packaged CCE for the Integration” on page 43.
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.

<table>
<thead>
<tr>
<th>Packaged CCE object</th>
<th>Mapped in ECE to</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>User</td>
<td>An agent belongs to a peripheral.</td>
</tr>
<tr>
<td>Supervisor</td>
<td></td>
<td>A peripheral belongs to an agent peripheral gateway (PG).</td>
</tr>
<tr>
<td>Administrator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skill group</td>
<td>User group</td>
<td>A skill group belongs to a peripheral.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A peripheral belongs to an agent PG.</td>
</tr>
<tr>
<td>Media routing domain (MRD)</td>
<td>Queues (Only selected skill groups and PQs of the MRD)</td>
<td>Multiple queues can belong to a single MRD.</td>
</tr>
<tr>
<td>Script selector</td>
<td>Queue</td>
<td>A script selector can belong to only one queue.</td>
</tr>
</tbody>
</table>

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.

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

Packaged CCE customers who intend to use ECE must access Peripheral Gateway Setup on both CCE PGs to set up a Multichannel PIM that associates ECE with the MR PG (PG2). See “Adding ECE to Packaged CCE Inventory” on page 44.

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).

  - 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.

<table>
<thead>
<tr>
<th>Object</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call type</td>
<td>Configured using the Unified CCE Administration page.</td>
</tr>
<tr>
<td>Application path</td>
<td>Configured using the Configuration Manager tool.</td>
</tr>
<tr>
<td>Agents</td>
<td>Configured using the Unified CCE Administration page.</td>
</tr>
<tr>
<td>Skill groups</td>
<td>Configured using the Unified CCE Administration page.</td>
</tr>
<tr>
<td>Dialed Number/Script Selectors</td>
<td>Configured using the Unified CCE Administration page.</td>
</tr>
<tr>
<td>Scripts</td>
<td>Configured using the Script Editor.</td>
</tr>
<tr>
<td>Precision Routing</td>
<td>Configured using the Unified CCE Administration page.</td>
</tr>
</tbody>
</table>
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](image)

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 56.

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.
   - **Username**: Provide the login name for the agent. For callback and delayed callback agents, the login name should match the User ID provided while configuring End users from the Cisco Unified Communication Manager Administration user interface.
   - **First name**: Provide the first name.
   - **Last name**: Provide the last name.
   - **Password**: Provide the password for the agent. Make sure the password does not contain the following characters: = (equal to) and ; (semicolon) as ECE does not allow the users to login if these characters are present in the passwords. Password fields are disabled if single sign-on option is selected for the agent.

6. Click **Save**.

### 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 44) and add ECE as an External Machine in the System Inventory (page 44). 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](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
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.

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.

![Diagram of a sample script with nodes labeled Start, Queue to Skill Group, Wait, and End]

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.

![Image of Run External Script Properties window showing selected Network VRU script]

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 50).
      ii. In the Period tab, set a schedule for the script.
iii. Click **OK**.

![Call Type Manager window](image)

*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 55)
2. Assign attributes to agents (page 56)
3. Create precision queues (page 56)
4. Add precision queue node to the scripts (page 56)

---

**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 Call Server 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 hostname or the IP address of the ECE services server machine. 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 enter the hostname or the IP address of the secondary ECE services server machine 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.
   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 Call Server on Side B.
Adding Agent PG PIM for ECE

To add PG and PIM for Agent PG:
1. On the CCE Call Server on Side A, from Cisco Unified CCE Tools, click on Peripheral Gateway Setup.
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 Call Server on Side B.

Adding CTI for ECE

To add CTI for ECE:
1. On the CCE Call Server on Side A, from Cisco Unified CCE Tools, click on 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 Call Server on Side B.
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 82.
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 24.

**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. Since the database is installed remotely, you can install both the file server and the database components at the same time. 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:

1. File server + database server
2. Messaging server
3. Application server
4. Web Server
5. Services 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.

**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
For 400+ 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 400+ 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-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

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_wsjb.exe` to launch the installation program.

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

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

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

   ![Read and accept the terms of the License Agreement](image)

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 61.
   
   - 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 65
- Database Server Details on page 66
- Web Server Details on page 72
- Messaging Server Details on page 73
- Application Server Details on page 74
- Services Server Details on page 75

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

\[Cisco_Home\]eService\installation\logs\installation_summary_Server_Name.txt.

After the installation is completed, perform the post-installation tasks (page 76).
# Installation Details

## File Server Details

<table>
<thead>
<tr>
<th>#</th>
<th>Field Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>File Server Directory/NAS path</td>
<td>Provide the path of the directory where you would like to install Enterprise Chat and Email. For example, C:\Cisco, or \SharedSpace\Cisco, if the file server is installed on a NAS device or DFS. <strong>Note:</strong> Make sure that the path and folder name do not contain any of the following characters: `*?&lt;&gt;</td>
<td>+^,'%`,@</td>
</tr>
</tbody>
</table>

## 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 30. User name should be provided in the format: domain\username |
|----|---------------------------------|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| 3  | Domain user password            | Password for the domain user.                                               |-------------------------------------------------------------------------------------------------|
## Database Server Details

<table>
<thead>
<tr>
<th>#</th>
<th>Field Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File Server Parameters</strong></td>
<td><strong>1. File Server Name/NAS Path</strong></td>
<td>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. <strong>Note:</strong> Make sure you provide the DNS host name and not the IP address of the server.</td>
<td></td>
</tr>
<tr>
<td><strong>Cisco Application Context Root</strong></td>
<td><strong>2. Context Root Name</strong></td>
<td>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. <strong>Note:</strong> Make sure there are no spaces or special characters in the name of the context root.</td>
<td>system</td>
</tr>
<tr>
<td><strong>Cisco System Administrator Account</strong></td>
<td><strong>3. User name</strong></td>
<td>User name for the system administrator. This is the first user that gets created for accessing the system partition.</td>
<td>sa</td>
</tr>
<tr>
<td></td>
<td><strong>4. Password</strong></td>
<td>Password for the system administrator. <strong>Note:</strong> 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: &lt; (less than), &gt; (greater than), ; (semicolon), : (colon), = (equal to), \ (backslash)</td>
<td></td>
</tr>
<tr>
<td><strong>Cisco Partition Administrator Account and Partition Details</strong></td>
<td><strong>5. User name</strong></td>
<td>User name for the partition administrator. This is the first user that gets created for accessing the business partition.</td>
<td>pa</td>
</tr>
<tr>
<td></td>
<td><strong>6. Password</strong></td>
<td>Password for the partition administrator. <strong>Note:</strong> 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: &lt; (less than), &gt; (greater than), ; (semicolon), : (colon), = (equal to), \ (backslash)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>7. Partition name</strong></td>
<td>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.</td>
<td>default</td>
</tr>
<tr>
<td></td>
<td><strong>8. Description of partition</strong></td>
<td>Description for the partition.</td>
<td></td>
</tr>
</tbody>
</table>

### Installation Identifiers
<table>
<thead>
<tr>
<th>#</th>
<th>Field Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Unique name for this installation</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>4-digit identifier for this installation</td>
<td>Provide a 4-digit numerical value, between 2001 and 9998, that will be used internally as system ID.</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Knowledge Base Primary Language</td>
<td>The default language for the Knowledge Base.</td>
<td>English (US)</td>
</tr>
<tr>
<td>12</td>
<td>Default SMTP server</td>
<td>The SMTP server to be used to send email notifications.</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Notification mail redirection from address</td>
<td>All notification emails are sent from this email address.</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Notification mail redirection to address</td>
<td>All notification emails are sent to this email address.</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Authentication</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Server name</td>
<td>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 133). Note: Make sure you provide the DNS host name and not the IP address.</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Database name</td>
<td>Name of the master database. The installation program creates a database with the name you provide here.</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Server instance name</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Database listener port</td>
<td>Port number of the MSSQL Server.</td>
<td>1433</td>
</tr>
</tbody>
</table>
### Field Name

<table>
<thead>
<tr>
<th>#</th>
<th>Field Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>Datafile path</td>
<td>Path to the folder on the database server, where you want to create the data file. For example, D:\MSSQL\Data.</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Datafile initial size (MB)</td>
<td>Minimum size of the data file for the database.</td>
<td>100</td>
</tr>
<tr>
<td>22</td>
<td>Datafile maximum size (MB)</td>
<td>Maximum size of the data file for the database.</td>
<td>Unlimited</td>
</tr>
<tr>
<td>23</td>
<td>Datafile increment size (MB)</td>
<td>Additional file size limit that will be allocated to the database after the initial size is full.</td>
<td>10</td>
</tr>
<tr>
<td>24</td>
<td>Logfile initial size (MB)</td>
<td>Minimum size of the log file.</td>
<td>25</td>
</tr>
<tr>
<td>25</td>
<td>Logfile maximum size (MB)</td>
<td>Maximum size of the log file.</td>
<td>Unlimited</td>
</tr>
<tr>
<td>26</td>
<td>Database administrator user name</td>
<td>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 35).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> This property needs to be configured only if you are using the SQL Server Authentication mode.</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Database administrator password</td>
<td>Password of the database administrator.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> This property needs to be configured only if you are using the SQL Server Authentication mode.</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Cisco Database user name</td>
<td>User name required to connect to the master database. The installation program creates the database and its user.</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Cisco Database password</td>
<td>Password for the master database user.</td>
<td></td>
</tr>
</tbody>
</table>

### Active Database Parameters

<table>
<thead>
<tr>
<th>#</th>
<th>Field Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Server name</td>
<td>Name of the local or remote server on which you want to install the active database.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> It must be the same server on which the master database is installed.</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>Database name</td>
<td>Name of the active database. The installation program creates a database with the name you provide here.</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Server instance name</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>Database listener port</td>
<td>Port number of MSSQL Server. This should match the value set for the master database.</td>
<td>1433</td>
</tr>
<tr>
<td>34</td>
<td>Datafile path</td>
<td>Path to the folder on the database server, where you want to create the data file. For example, C:\MSSQL\Data.</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>Datafile initial size (MB)</td>
<td>Minimum size of the data file for the database.</td>
<td>2048</td>
</tr>
<tr>
<td>36</td>
<td>Datafile maximum size (MB)</td>
<td>Maximum size of the data file for the database.</td>
<td>Unlimited</td>
</tr>
<tr>
<td>37</td>
<td>Datafile increment size (MB)</td>
<td>Additional file size limit that will be allocated to the database after the initial size is full.</td>
<td>500</td>
</tr>
</tbody>
</table>
### Logfile Initial Size (MB)

- **Description**: Minimum size of the log file.
- **Value**: 1024

### Logfile Maximum Size (MB)

- **Description**: Maximum size of the log file.
- **Value**: Unlimited

### Database Administrator User Name

- **Description**: 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 35).
- **Note**: This property needs to be configured only if you are using the SQL Server Authentication mode.

### Database Administrator Password

- **Description**: Password of the database administrator.
- **Note**: This property needs to be configured only if you are using the SQL Server Authentication mode.

### Cisco Database User Name

- **Description**: 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.

### Cisco Database Password

- **Description**: 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

<table>
<thead>
<tr>
<th>#</th>
<th>Field Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>44</td>
<td>Filegroup Datafile 1 Name</td>
<td>Provide the name of the first file group to be created for the active database.</td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>Filegroup Datafile 1 Path</td>
<td>Provide the location for the first filegroup. Make sure you provide the path to the drive that is created for storing file groups.</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>Filegroup Datafile 2 Name</td>
<td>Provide the name of the second file group to be created for the active database.</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>Filegroup Datafile 2 Path</td>
<td>Provide the location for the second filegroup. Make sure you provide the path to the drive that is created for storing file groups.</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>Filegroup Datafile 3 Name</td>
<td>Provide the name of the third file group to be created for the active database.</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>Filegroup Datafile 3 Path</td>
<td>Provide the location for the third file group. Make sure you provide the path to the drive that is created for storing file groups.</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>Filegroup Datafile 4 Name</td>
<td>Provide the name of the fourth file group to be created for the active database.</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>Filegroup Datafile 4 Path</td>
<td>Provide the location for the fourth file group. Make sure you provide the path to the drive that is created for storing file groups.</td>
<td></td>
</tr>
</tbody>
</table>

### Reports Database Parameters
<table>
<thead>
<tr>
<th>#</th>
<th>Field Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>52.</td>
<td>Server name</td>
<td>Name of the local or remote server on which the reports database should be installed. If you are using MSSQL Server <strong>Always On Availability Group</strong> clustering, specify the Listener name for the reports database (page 133). <strong>Note:</strong> Make sure you provide the DNS host name and not the IP address of the server.</td>
<td></td>
</tr>
<tr>
<td>53.</td>
<td>Database name</td>
<td>Name of the reports database. The installation program creates a database with the name you type here.</td>
<td></td>
</tr>
<tr>
<td>54.</td>
<td>Database server instance</td>
<td>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. <strong>Note:</strong> The name of the instance should match the name given when you verify the server privileges while configuring the SQL Server Integration Service (page 37).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>▶ If you are using MSSQL Server <strong>Always On Availability Group</strong> clustering, provide the name of the Listener instance.</td>
<td></td>
</tr>
<tr>
<td>55.</td>
<td>Database listener port</td>
<td>Port number of the MSSQL Server.</td>
<td>1433</td>
</tr>
<tr>
<td>56.</td>
<td>Datafile path</td>
<td>Path to the folder on the database server, where you want to create the data file. For example, <code>D:\MSSQL\Data</code>.</td>
<td></td>
</tr>
<tr>
<td>57.</td>
<td>Datafile initial size (MB)</td>
<td>Minimum size of the data file for the database.</td>
<td>1024</td>
</tr>
<tr>
<td>58.</td>
<td>Datafile maximum size (MB)</td>
<td>Maximum size of the data file for the database.</td>
<td>Unlimited</td>
</tr>
<tr>
<td>59.</td>
<td>Datafile increment size (MB)</td>
<td>Additional file size limit that will be allocated to the database after the initial size is full.</td>
<td>500</td>
</tr>
<tr>
<td>60.</td>
<td>Logfile initial size (MB)</td>
<td>Minimum size of the log file.</td>
<td>512</td>
</tr>
<tr>
<td>61.</td>
<td>Logfile maximum size (MB)</td>
<td>Maximum size of the log file.</td>
<td>Unlimited</td>
</tr>
<tr>
<td>62.</td>
<td>Database administrator user name</td>
<td>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 35). <strong>Note:</strong> This property needs to be configured only if you are using the SQL Server Authentication mode.</td>
<td></td>
</tr>
<tr>
<td>63.</td>
<td>Database administrator password</td>
<td>Password of the database administrator. <strong>Note:</strong> This property needs to be configured only if you are using the SQL Server Authentication mode.</td>
<td></td>
</tr>
<tr>
<td>64.</td>
<td>Cisco Database user name</td>
<td>User name required to connect to the reports database. The installation program will create this user. <strong>Note:</strong> This property needs to be configured only if you are using the SQL Server Authentication mode.</td>
<td></td>
</tr>
<tr>
<td>65.</td>
<td>Cisco Database password</td>
<td>Password for the database user. <strong>Note:</strong> This property needs to be configured only if you are using the SQL Server Authentication mode.</td>
<td></td>
</tr>
</tbody>
</table>

**Reports Database Filegroup Parameters**
<table>
<thead>
<tr>
<th>#</th>
<th>Field Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>66.</td>
<td>Filegroup Datafile 1 Name</td>
<td>Provide the name of the first file group to be created for the reports database.</td>
<td></td>
</tr>
<tr>
<td>67.</td>
<td>Filegroup Datafile 1 Path</td>
<td>Provide the location for the first filegroup. Make sure you provide the path to the drive that is created for storing file groups.</td>
<td></td>
</tr>
<tr>
<td>68.</td>
<td>Filegroup Datafile 2 Name</td>
<td>Provide the name of the second file group to be created for the reports database.</td>
<td></td>
</tr>
<tr>
<td>69.</td>
<td>Filegroup Datafile 2 Path</td>
<td>Provide the location for the second filegroup. Make sure you provide the path to the drive that is created for storing file groups.</td>
<td></td>
</tr>
<tr>
<td>70.</td>
<td>Filegroup Datafile 3 Name</td>
<td>Provide the name of the third file group to be created for the reports database.</td>
<td></td>
</tr>
<tr>
<td>71.</td>
<td>Filegroup Datafile 3 Path</td>
<td>Provide the location for the third filegroup. Make sure you provide the path to the drive that is created for storing file groups.</td>
<td></td>
</tr>
<tr>
<td>72.</td>
<td>Filegroup Datafile 4 Name</td>
<td>Provide the name of the fourth file group to be created for the reports database.</td>
<td></td>
</tr>
<tr>
<td>73.</td>
<td>Filegroup Datafile 4 Path</td>
<td>Provide the location for the fourth filegroup. Make sure you provide the path to the drive that is created for storing file groups.</td>
<td></td>
</tr>
</tbody>
</table>

**Reports Database SSIS Parameters**

<table>
<thead>
<tr>
<th>#</th>
<th>Field Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>74.</td>
<td>SSIS Datafile Path</td>
<td>Provide the path of the SSIS Directory created on the reports database server (page 37). For example, D:\sis_data</td>
<td></td>
</tr>
<tr>
<td>75.</td>
<td>Domain User Name</td>
<td>User name of the <strong>Install Account</strong> created for use by the application. (page 30). User name should be provided in the format: Domain\username</td>
<td></td>
</tr>
<tr>
<td>76.</td>
<td>Domain User Password</td>
<td>Password of the domain user account.</td>
<td></td>
</tr>
</tbody>
</table>

**Reports Database SSIS Catalog Parameters**

<table>
<thead>
<tr>
<th>#</th>
<th>Field Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>77.</td>
<td>SSIS Catalog Encryption Password</td>
<td>Provide a password to encrypt the SSIS catalog.</td>
<td></td>
</tr>
<tr>
<td>78.</td>
<td>Verify SSIS Catalog Password</td>
<td>Verify SSIS catalog encryption password.</td>
<td></td>
</tr>
</tbody>
</table>

**Domain User Account Parameters**

<table>
<thead>
<tr>
<th>#</th>
<th>Field Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>79.</td>
<td>Domain user name</td>
<td>User name of the domain user account you created for use by the application. For more information, refer to “<strong>Setting Up User Accounts and Permissions</strong>” on page 30. User name should be provided in the format: Domain\username</td>
<td></td>
</tr>
<tr>
<td>80.</td>
<td>Domain user password</td>
<td>Password for the domain user.</td>
<td></td>
</tr>
</tbody>
</table>

*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 39.

<table>
<thead>
<tr>
<th>#</th>
<th>Field Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Application Server Parameters</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Application server name</td>
<td>Type the name of the application server for which you want to configure the web server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Make sure you provide the DNS host name and not the IP address of the server.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Jetty HTTP Port</td>
<td>Jetty HTTP listener port of the application server where all the HTTP requests are handled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> This port should match the port number provided while installing the application server (page 74).</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Enterprise Chat and Email Directory</strong></td>
<td>Provide the path of the directory where you would like to install ECE. For example, C:\Cisco.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Make sure that the path and folder name do not contain any of the following characters: *&lt;&gt;</td>
<td>+^&quot;%`,@</td>
</tr>
<tr>
<td></td>
<td><strong>IIS Web Site Parameters</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>IIS Web Site Name</td>
<td>Name of the IIS Web Site on which the application is to be configured.</td>
<td>Default Web Site</td>
</tr>
<tr>
<td></td>
<td><strong>Cisco Application Context Root</strong></td>
<td>Provide the same context root name which was provided at the time of installing the Cisco database server (page 66).</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Context Root Name</td>
<td>Provide the context root name which was provided at the time of installing the Cisco database server (page 66).</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco Partition Name</strong></td>
<td>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 66).</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Partition Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Domain User Account Parameters</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Domain user name</td>
<td>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 30. User name should be provided in the format: domain\username</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Domain user password</td>
<td>Password for the domain user.</td>
<td></td>
</tr>
</tbody>
</table>
**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, `C:\Cisco\jdk`.

<table>
<thead>
<tr>
<th>#</th>
<th>Field Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>File Server Parameters</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>File Server name/NAS Path</td>
<td>The fully qualified domain name of the file server. If the file server is</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>installed on a NAS device or DFS, provide the path to the shared folder.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, <code>\SharedSpace\Cisco</code>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Make sure you provide the DNS host name and not the IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>of the server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Enterprise Chat and Email Home</strong></td>
<td>Provide the path of the directory where you would like to install Enterprise</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Directory</td>
<td>Chat and Email. For example, <code>C:\Cisco</code>. The installation program also</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>installs ActiveMQ and JDK at the same location.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Make sure that the path and folder name do not contain any of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>following characters: `*&lt;&gt;</td>
<td>^%`,@.</td>
</tr>
<tr>
<td></td>
<td><strong>ActiveMQ Parameters</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>ActiveMQ Port</td>
<td>ActiveMQ listener port used by JMS clients to connect to ActiveMQ messaging</td>
<td>15097</td>
</tr>
<tr>
<td></td>
<td></td>
<td>server. The port number can be between 1024-65535.</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Admin ActiveMQ Port</td>
<td>ActiveMQ Admin listener port used for administering and monitoring</td>
<td>15096</td>
</tr>
<tr>
<td></td>
<td></td>
<td>resources on the server. The port number can be between 1024-65535.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Domain User Account Parameters</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Domain user name</td>
<td>User name of the domain user account you created for use by the application.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information, refer to &quot;Setting Up User Accounts and Permissions&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>on page 30. User name should be provided in the format: <code>Domain\username</code></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Domain user password</td>
<td>Password for the domain user.</td>
<td></td>
</tr>
</tbody>
</table>

**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, *C:\Cisco\jdk*.

<table>
<thead>
<tr>
<th>#</th>
<th>Field Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>File Server Parameters</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>File Server name/ NAS Path</td>
<td>The fully qualified domain name of the file server. If the file server is</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>installed on a NAS device or DFS, provide the path to the shared folder. For</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>example, \SharedSpace\Cisco</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Make sure you provide the DNS host name and not the IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>of the server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>**Enterprise Chat and Email Home</td>
<td>Provide the path of the directory where you would like to install ECE. For</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Directory</td>
<td>example, C:\Cisco. The installation program also installs Jetty and JDK at</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>the same location.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Make sure that the path and folder name do not contain any of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>following characters: *?&lt;&gt;</td>
<td>+=&quot;%'@</td>
</tr>
<tr>
<td></td>
<td><strong>Jetty Parameters</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Jetty HTTP port</td>
<td>Jetty HTTP listener port where all the HTTP requests are handled. The port</td>
<td>9001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>number can be between 1024-65535.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Jetty HTTP SSL Port</td>
<td>Jetty HTTPS listener port where all the SSL requests are handled. The port</td>
<td>9002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>number can be between 1024-65535.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Jetty Stop Port</td>
<td>Jetty shutdown command listener port. This port is used for issuing</td>
<td>15095</td>
</tr>
<tr>
<td></td>
<td></td>
<td>shutdown command to stop Jetty. The port number must be between 1024-65535.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Domain User Account Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Domain user name</td>
<td>User name of the domain user account you created for use by the application.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information, refer to “Setting Up User Accounts and Permissions”</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>on page 30. User name should be provided in the format: <strong>Domain\username</strong></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Domain user password</td>
<td>Password for the domain user.</td>
<td></td>
</tr>
</tbody>
</table>

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, C:\Cisco\jdk.

<table>
<thead>
<tr>
<th>#</th>
<th>Field Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>File Server name/NAS Path</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>Note: Make sure you provide the DNS host name and not the IP address of the server.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise Chat and Email Home Directory</td>
<td>Provide the path of the directory where you would like to install ECE. For example, C:\Cisco. The installation program also installs JDK at the same location.</td>
<td></td>
</tr>
<tr>
<td>Note: Make sure that the path and folder name do not contain any of the following characters: *?&lt;&gt;</td>
<td>+^'<code>%</code>,@</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RMI registry port</td>
<td>Port number used by the Remote Method Invocation (RMI) registry naming service.</td>
<td>15099</td>
</tr>
<tr>
<td></td>
<td>RMI activation port</td>
<td>Port number used by the RMI Daemon Process.</td>
<td>15098</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>Provide the name of the organization. Make sure that the name does not contain any special characters.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Business Unit</td>
<td>Provide the business unit name. Make sure that the value does not contain any special characters.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Location</td>
<td>Provide the location of your organization. Make sure that the value does not contain any special characters.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Country</td>
<td>Select the country from the dropdown list.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Domain user name</td>
<td>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 30. User name should be provided in the format: Domain\username</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Domain user password</td>
<td>Password for the domain user.</td>
<td></td>
</tr>
</tbody>
</table>

Services server details
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
- 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 40). Ensure that the user account that you used for installing the application (page 30) 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 30) 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 117 for details.

Always On Availability Group Clustering Tasks

- Perform all the tasks listed in “Post-Installation Tasks” on page 134.
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.

   ```sql
   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.

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

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

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

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

   ```sql
   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.

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

```sql
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.

```sql
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.

```sql
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 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

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.
5. In the Resources space, 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 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.

### 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 91.

### 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 30).

#### To start ECE:

If you get the following error while starting the Cisco Service, see “Troubleshooting Application Start-Up Issues” on page 84: **Error 1069: The service did not start due to login failure.**

- 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.
  - 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.
  - On each services server, start the application by starting the Cisco Windows service from the Windows Services panel.
  - 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 30) 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: \texttt{https://Finesse\_Server\_Name/des ttop}

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 \texttt{http://Web\_server\_company\_com/p a rtition\_name} in your browser, where \texttt{Web\_server\_company\_com} is the fully qualified domain name of your web server and \texttt{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 \texttt{https://Web\_server\_company\_com/p artition\_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 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.

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
The following setting must be configured:
- Web server URL or Load Balancer URL

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
- 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.

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

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:
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:
  - Cisco_Home\eService\storage
  - Cisco_Home\eService\logs

Preparing to Uninstall

Stopping the Application

Before you begin the uninstallation process, make sure you stop ECE. For details, refer to “Stopping ECE” on page 84.

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`.

### Performing Post Uninstallation Tasks

#### Starting IIS

- Start IIS (World Wide Web Publishing Service) on all web servers in the installation.
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
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 92).
- **Split AD FS**: In a split AD FS deployment, Resource Federation Server and Account Federation Server are installed on separate machines (page 100).

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**.

Important: Perform these tasks only if you are planning to use single sign-on while accessing any of the ECE consoles outside of Finesse.
b. On the Select Data Source screen, select the **Enter data about the reply party manually** option and click **Next**.

![Select Data Source](image1.png)

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**.

![Specify Display Name](image2.png)

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

![Choose Profile](image1)

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:

   ```
   ```

   Replace **Web_Server_Or_Load_Balancer_Server** with the ECE web server name or the Load balancer server name.

![Configure URL](image2)

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.

![Add SAML](image)

*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**.

![Add an Endpoint](image)

*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](image)

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.
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.
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](image)

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](image)
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](image)

**Configuring Split AD FS Deployment**

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

Configuring split AD FS includes:

- Adding Security Certificates for the AD FS Domains
- Configuring Relying Party Trust for Shared AD FS in Customer AD FS
- Configuring Claims Provider Trust for Customer AD FS in Shared AD FS
- Configuring Relying Party Trust for ECE in Shared AD FS

**Adding Security Certificates for the AD FS Domains**

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

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

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

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

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](Image)
b. On the Specify Display Name screen, provide the Display name, Click Next.

![Specify Display Name](image)

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...

![AD FS Management Console](image)

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.

![Add a Claim Description](image1.png)

*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**.

![AD FS](image2.png)

*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**.

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.
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](image1)

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](image2)

   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 Claim Rules](Image)

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](Image)

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 102).

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](image1.png)

**Select AD FS profile**

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

![Select AD FS profile](image2.png)

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**.
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**.

![Add an Endpoint window]

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**.

![Add Transform Claim Rule Wizard]

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 104).
   iii. In the **Outgoing claim type** dropdown, select the Name ID option.

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.
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](image1.png)

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](image2.png)
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](image)

**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.
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.
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 118).

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.

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**.

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.
4. In the Site Bindings window, 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.

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 124)
   a. Modify the alias configuration (page 125)
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 Cisco_Home.
3. Open the Command window and navigate to the bin folder in the jre folder in JDK_Home, the installation folder for JDK. For example, the command will look like:
   ```
   cd C:\InstallFolder\Java\jdk1.8.0_60\jre\bin
   ```
4. Execute the following command to install the certificate:
   ```
   keytool -import -trustcacerts -alias ALIAS_NAME -keystore "..\lib\security\cacerts" -file "CERTIFICATE_FILE_PATH"
   ```
   where:
   - `CERTIFICATE_FILE_PATH` is the complete path to the certificate that you copied in Step 2, including the name of the file.
   - `ALIAS_NAME` is any name you want to assign to the certificate.

   For example the command will look like:
   ```
   keytool -import -trustcacerts -alias emailcertificate -keystore "..\lib\security\cacerts" -file "D:\eG\ms_exchange_certificate.cer"
   ```
5. When prompted, provide the keystore password. If you had changed the keystore password earlier, provide that password. If not, provide the default password, changeit.
6. Confirm the action when prompted.
7. To verify that the certificate is installed successfully, run the following command:
   ```
   keytool -list -v -keystore "..\lib\security\cacerts" -alias ALIAS_NAME
   ```
   where `ALIAS_NAME` is the name you assigned to the certificate in Step 4.

   For example, the command will look like:
   ```
   keytool -list -v -keystore "..\lib\security\cacerts" -alias emailcertificate
   ```
8. When prompted, provide the keystore password.

   The output will list the installed certificate.
Deleting Certificates

Certificates generally have an expiry date. When your certificate expires, you might need to delete the old certificates and install new ones. The following section describes the steps for deleting the certificates. After deleting the certificates, repeat the steps in “Installing Certificates” on page 124 to install new certificates.

To delete a certificate:

1. Open the Command window and navigate to the bin folder in the jre folder in JDK_Home, the installation folder for JDK. For example, the command will look like:
   ```
   cd C:\InstallFolder\Java\jdk1.8_65\jre\bin
   ```
2. Execute the following command to delete the certificate:
   ```
   keytool -delete -alias ALIAS_NAME -keystore "..\lib\security\cacerts"
   ```
   where:
   - **ALIAS_NAME** is the name you assigned to the certificate in Step 4.
   For example the command will look like:
   ```
   keytool -delete -alias emailcertificate -keystore "..\lib\security\cacerts"
   ```
3. When prompted, provide the keystore password. If you had changed the keystore password earlier, provide that password. If not, provide the default password, changeit.

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.
   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.

If you are converting an exiting non-HA deployment to HA, you may see the following prompt: A shared folder Folder_Name already exists on the server. If the existing share folder is used, the security setting specified within the Edit Setting dialog box will not apply. Click Yes to continue.

c. On the Namespace Type screen, select Domain-based namespace. Click Next.

d. On the Review Settings and Create Namespace screen, 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 127 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.

### Adding Folders and Configuring Replication

**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. Run through the Replicate Folder Wizard to set up replication. When prompted to select the Primary Member, select any one server to be the primary server.
5. 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

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

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.


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 131) and then select Properties.


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.

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. Run through the Configure Cluster Quorum Wizard.
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, type the path of the shared folder that you want to use. 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.

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.
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 30).
5. Restart the SQL Server services.

Configuring SQL Server Always On Availability Groups

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.
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.
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.
   - 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.
   - 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, here also you will 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.

6. On the Select Initial Data Synchronization page, select the **Full** option. Click **Next**.

7. On the Validation screen, review the validations run by the wizard. Click **Next**.

8. On the Summary screen, verify the choices made in the wizard. Click **Finish** to start the process.

9. The Results screen shows if all the tasks are completed successfully. Click **Close**.

### Install the Application

- Install the ECE application. See “Installation Process” on page 60.

### 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 file server.

**Important:** If the file server is installed on a NAS device or DFS, run the utility from any other server like, services server, messaging server. The utility cannot be run from the web server.

To run the utility:
1. From the installation package, copy the ReportsDB Utility (SQL Server Always On) folder on the file server.
2. The file server needs to have JDK 1.8 Update 65 or higher installed on the machine. The installation package for JDK is available in the Environment\Server Side Java folder of the installation package.
3. Open the reportsdb_utility.bat file in a text editor.
4. Locate the SET JAVA_HOME property and set the value to the location where JDK 1.8 Update 65 or higher is installed on your machine. For example, C:\Java\jdk1.8.0_65.
5. 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: Value is set to true and should not be changed.
   - 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.
SSIS_INSTALL_PATH: Provide the path of the SSIS Directory created on the secondary node. For example, D:\ssis_data
SSIS_PKG_OVERWRITE: Set this to true.
SSIS_USER_ID: User name of the Install Account created for use by the application.
SSIS_USER_PASSWORD: Password of the user.
SSIS_CATALOG_PASSWORD: Provide a password to encrypt the SSIS catalog.

6. Open the command prompt as an administrator and navigate to the utility folder.

7. Run the following command:
   Utility_Location\reportsdb_utility.bat createDBObjects
   For example, D:\utility\reportsdb_utility.bat createDBObjects

8. 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

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\eReportsDB_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 (Windows 2016)
- Converting Existing Two Server Installation to HA (Windows 2012)
- Converting Existing Distributed Server Installation to HA (Windows 2012 & 2016)
Converting Existing Two Server Installation to HA (Windows 2016)

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

Existing installation and VMs:

- **VM-A:** ECE All-in-One server (file, messaging, application, services and database components are installed on this server). 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 2016):

- **VM-C:** For installing second Messaging, Services, and Application server components. This will become the Windows Distributed File System Node2 for file server.
- **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 126.

**Updating Files to Use DFS**

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

1. Browse to Cisco_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`

**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.
  - In the File Server Parameters window, provide the new DFS location.

**Converting Databases to SQL Server to Always On Configuration**

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform all the required pre-installation tasks on the new database servers. “Pre-Installation Tasks” on page 24</td>
<td></td>
</tr>
<tr>
<td>“Stopping ECE Application and Disable SQL Jobs.” on page 140</td>
<td></td>
</tr>
<tr>
<td>If your existing database uses SQL Authentication, convert SQL Authentication to Windows Authentication. “Converting SQL Authentication to Windows Authentication” on page 140</td>
<td></td>
</tr>
<tr>
<td>“Installing Failover Clustering Feature” on page 130</td>
<td></td>
</tr>
</tbody>
</table>
### Stopping ECE Application and Disable SQL Jobs.

1. Stop the ECE application. See “Stopping ECE” on page 84.

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
   - EGPL_rebuild_indexes_Active_Database_Name
   - EGPL_update_fulltext_Active_Database_Name
   - EGICM_reindex_reports_job_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. Make the following changes in the file:
   
   ```
   Cisco_Home\eService\installation\dataaccess\egpl_ds_connpool_map.xml
   ```

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

5. Browse to `Cisco_Home\eService\lib\deployment.zip` extract `dataaccess\egpl_ds_connpool_map.xml`. Make the changes listed in Step 4. 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 primary server location.

2. Share folder path with secondary 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 Reports Database**
Perform this task on the primary node.

To modify the database server names:

1. Connect to the SQL server with the listener name.
2. In the Microsoft SQL Server Management Studio, browse to Integration Services Catalogs > SSISDB > EG_Reports_DatabaseName > Environments > EG_eGReportsDB.
3. Right-click EG_eGReportsDB and from the context menu, select Properties.
4. In the Environment Properties window, go to the Variables section, and edit the values of the following variables.
   - **Destination_ConnectionString**: Replace the server name with the listener name of the reports database. If all databases are installed on same node, then it will be common listener name for both active and reports database.
   - **Destination_Server**: Replace the server name with the listener name of the reports database.
   - **Source_ConnectionString**: Replace server name with the listener name of the active database. If all databases are installed on same node, then it will be common listener name for both active and reports database.
   - **Source_Server**: Replace server name with the listener name of the active database.

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:
  ```sql
  UPDATE [dbo].[EGPL_DSM_HOST]
  SET [HOST_NAME] = '<Listener Name>'
  WHERE [DESCRIPTION] = 'Database Server'
  ``
  Replace `<Listener Name>` with the cluster listener name.

Modifying Connpool File

Perform this task on the file server.

To modify the connpool files:

1. Stop the ECE application.
2. On the file server, go to the ECE installation folder.
3. Make the following changes in the file:
   ```xml
   Cisco_Home\eService\installation\dataaccess\egpl_ds_connpool_map.xml
   ```
   a. Locate `<conn_pool_list`.
   b. In all `connpool` nodes in the list, locate the `URL` property and replace the database server name with the listener name.
      
      For example, change:
143

<Url
  egid="3018">jdbc:sqlserver://masterussuh50:1433;integratedSecurity=true;databaseName=eGMasterDB</Url>

to:

<Url
  egid="3018">jdbc:sqlserver://HAlistenerCluster:1433;integratedSecurity=false;databaseName=eGMasterDB</Url>

4. Browse to Cisco_Home\eService\lib\deployment.zip extract \dataaccess\egpl_ds_connpool_map.xml. Make the changes listed in Step 3. Add the updated file in deployment.zip.

**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
   - EGPL_rebuild_indexes_Active_Database_Name
   - EGPL_update_fulltext_Active_Database_Name
   - EGICM_reindex_reports_job_Reports_Database_Name
   - populatesmy_Reports_Database_Name

2. Start the ECE application. See “Starting ECE” on page 83.

**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>`
Converting Existing Two Server Installation to HA (Windows 2012)

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

Existing installation and VMs:
- **VM-A**: ECE All-in-One server (file, messaging, application, services and database components are installed on this server). This will become the Windows Distributed File System Node1 for file server.
- **VM-B**: ECE Web server component

Acquire New VMs for Side B:
- **VM-C**: For installing second Messaging and Application server components. This will become the Windows Distributed File System Node2 for file server.
- **VM-D**: For installing second services server component
- **VM-E**: For second web server component

Converting Existing File Server to DFS
- For details see “Converting Existing File Server to DFS” on page 139.

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

Installing Second Services Server Component
- Install the new component on **VM-D**. While installing:
  - In the Installation Options window, select Services Server.
  - In the File Server Parameters window, provide the new DFS location.

Installing Second Web Server Component
- Install the new component on **VM-E**. While installing:
  - In the Installation Options window, select Web Server.
In the File Server Parameters window, provide the new DFS location.

Converting Databases to SQL Server to Always On Configuration

- For details see “Converting Databases to SQL Server to Always On Configuration” on page 139.

Updating Finesse Files

- For details see “Updating Finesse Files” on page 143.

Converting Existing Distributed Server Installation to
HA (Windows 2012 & 2016)

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 126.

Updating Files to Use DFS

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

1. Browse to Cisco_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

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 Application Server.
  - In the File Server Parameters window, provide the new DFS location.