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

For Unified Contact Center Enterprise

First Published: August 2016
Last Modified: November 2018

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

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

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

Contents

Preface

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

Audience

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

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

Obtaining Documentation and Submitting a Service Request

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

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

Documentation Feedback

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

We appreciate your comments.

Field Alerts and Field Notices

Cisco products may be modified or key processes may be determined to be important. These are announced through use of the Cisco Field Alerts and Cisco Field Notices. You can register to receive Field Alerts and

Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest.

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

Document Conventions

This guide uses the following typographical conventions.

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

Document conventions

Other Learning Resources

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

Online Help

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

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

Online help options

Document Set

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

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

The ECE document set contains the following guides:

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

User guides for agents and supervisors

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

User guides for administrators

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

1 Planning

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 Servers Component
- Web Servers Component
- Services Server

File Server Component

The file server is used to store reports templates, reports output, license files, and startup scripts. There is only one file server in a configuration.

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.
- An archive database, where all archived data is stored. This database is created only in deployments that use the standard edition of MSSQL Server.
- A reports database, where all data used by the reports module is stored. This database is created only in deployments that use the enterprise edition of MSSQL Server.

The master and active databases are installed on the same machine. The archive or reports databases can be installed on different machines.

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 configuration can have only one messaging server.

Components that use messaging are listed in the following table.

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

Application Servers 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 configuration 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 Servers 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 often installed on the same machine as the application server, but can also be installed on a different physical machine.

Installing the web server does not need access to any other ECE component. The web server can be installed outside firewall. A configuration 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

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 configuration can have only one services server.

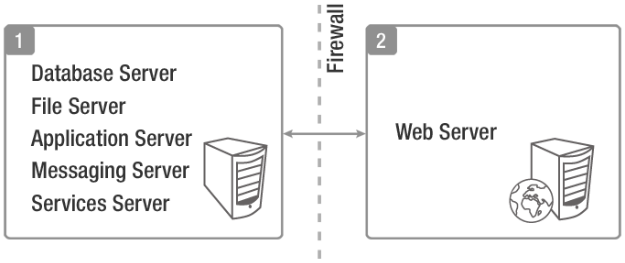
Understanding Deployment Models

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 machine and all other components are installed on one machine. 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 configurations. 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 machine outside the firewall.

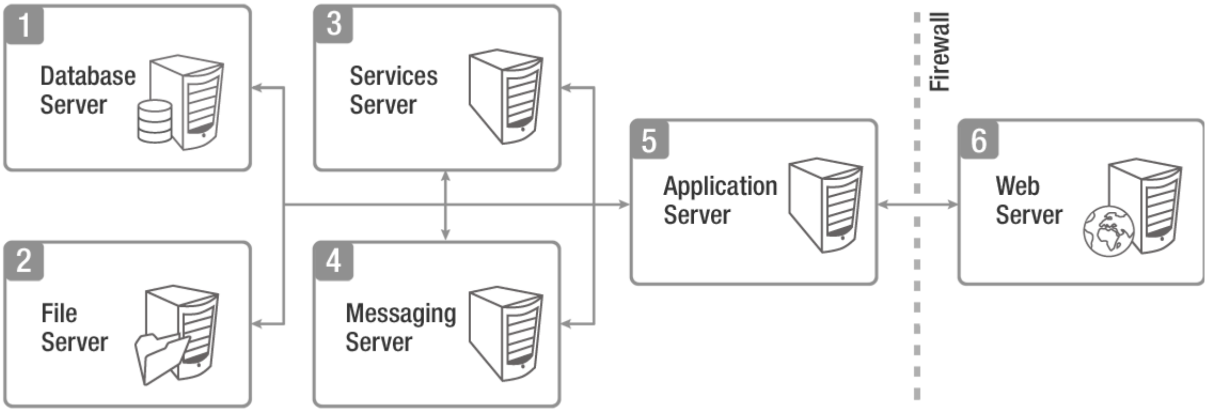


Collocated deployment for ECE

Distributed-Server Deployment

Distributed Configuration With Web Server Outside a Firewall

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

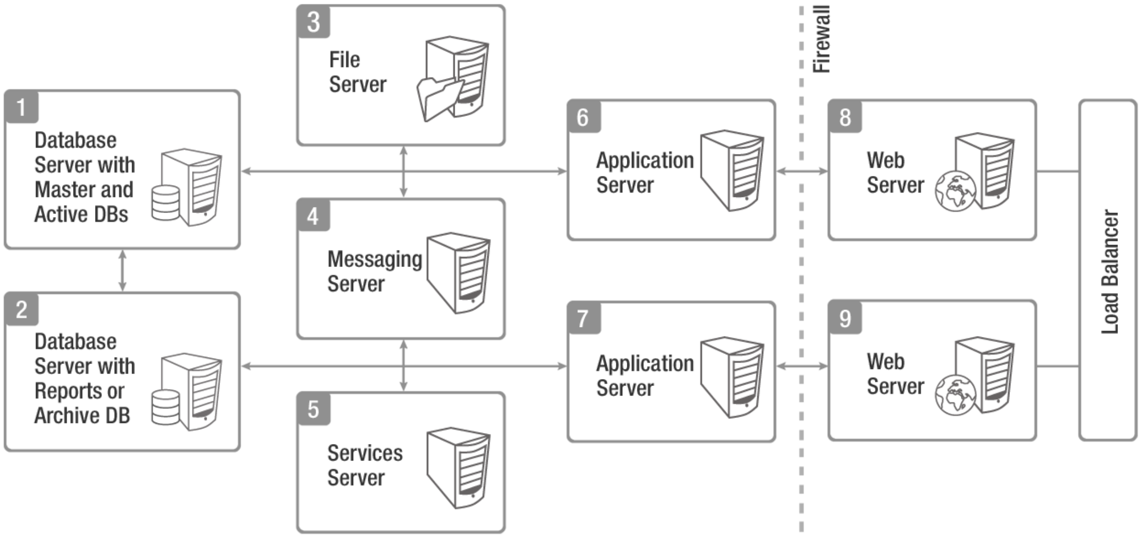


Distributed configuration with web server outside a firewall

Complex Distributed Configuration With Components on Different Machines

This configuration has each component on a different machine, with the following additional features:

- Reports and Archive DBs are installed on a separate machine.
- Multiple web-application server pairs are used with a load balancer.



Complex distributed-server configuration

Planning Components for Specific Configurations

The installation program creates the master and active databases.

Deployments that use the standard edition of MSSQL Server, get the following additional database:

- An archive database

Deployments that use the enterprise edition of MSSQL Server, get the following additional features:

- A reports database.
- The ability to distribute active and reports database tables among four different filegroups. For best performance, filegroups should be located on different physical volumes, each with a different disk controller, to maximize disk throughput. The following database tables are part of these file groups:
  - EGML_EMAIL_DATA
  - EGML_EMAIL_DATA_ALT
  - EGPL_EVENT_HISTORY_CASE_MGMT
  - EGML_EMAIL_ATTACHMENT
  - EGML_EMAIL_ATTACHMENT_LINK
  - EGOFR_SESSION
  - EGPS_SESSION_ATTR
  - EGPS_INTERACTION
  - EGPS_INTERACTION_ATTR
  - EGPS_EVENT
  - EGPS_EVENT_ATTR
  - EGSS_SESSION
  - EGSS_SESSION_ENTRY
  - EGLV_SURVEY

Planning Database Server Distribution

- The master and active databases are installed on the same database server. The reports databases can be installed on the same machine as the master and active databases or on different machines. Since the archive database can grow to be quite large, and operations performed on it can be slower, and can impact the overall performance of the system, it is typically installed on a different machine. This is optional, but it is the recommended practice.

  If the archive or reports database is to be installed on a different machine, make sure that you complete the steps described in the "Configuring Database Servers" on page 26. You may also need to complete certain tasks described in "Setting Up User Accounts and Permissions" on page 22.

Choosing Authentication Method for Database Connectivity

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

- ❍ Windows authentication

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

  If you choose Windows authentication, certain additional steps must be completed before you begin installing the application. These steps are outlined in the "Setting Up User Accounts and Permissions" on page 22. Also refer to "Configuring Database Servers" on page 26.

Planning the Messaging Server

- The messaging server can be installed on a separate machine, or on the same machine where the other components are installed, for example, install the messaging server along with the application server. To do this, select both the Application server and the Messaging server items in the Installation options screen while installing a distributed-server configuration.

  If the messaging server is on a separate machine, it can be restarted independently, without affecting any of the application servers in the configuration.

Planning Application and Web Servers

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

  If any of the web-application servers go down, a load balancer can help handle the failure through routing requests to alternate web-application servers. The load balancer detects application server failure and redirects requests to another application server. Users can log into the application without experiencing any significant loss of productivity.

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.

Installing ECE

- Follow the pre-installation tasks (page 18), installation tasks (page 40), and post-installation tasks (page 56), to install ECE.
- To set up SSL, follow the instructions in the "SSL Configuration" on page 93.

2

Pre-Installation Tasks

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*

Disabling Loopback Adapter Configuration

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

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

To disable Loopback Adapter:

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

Verifying Network Configuration

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

To verify network configuration:

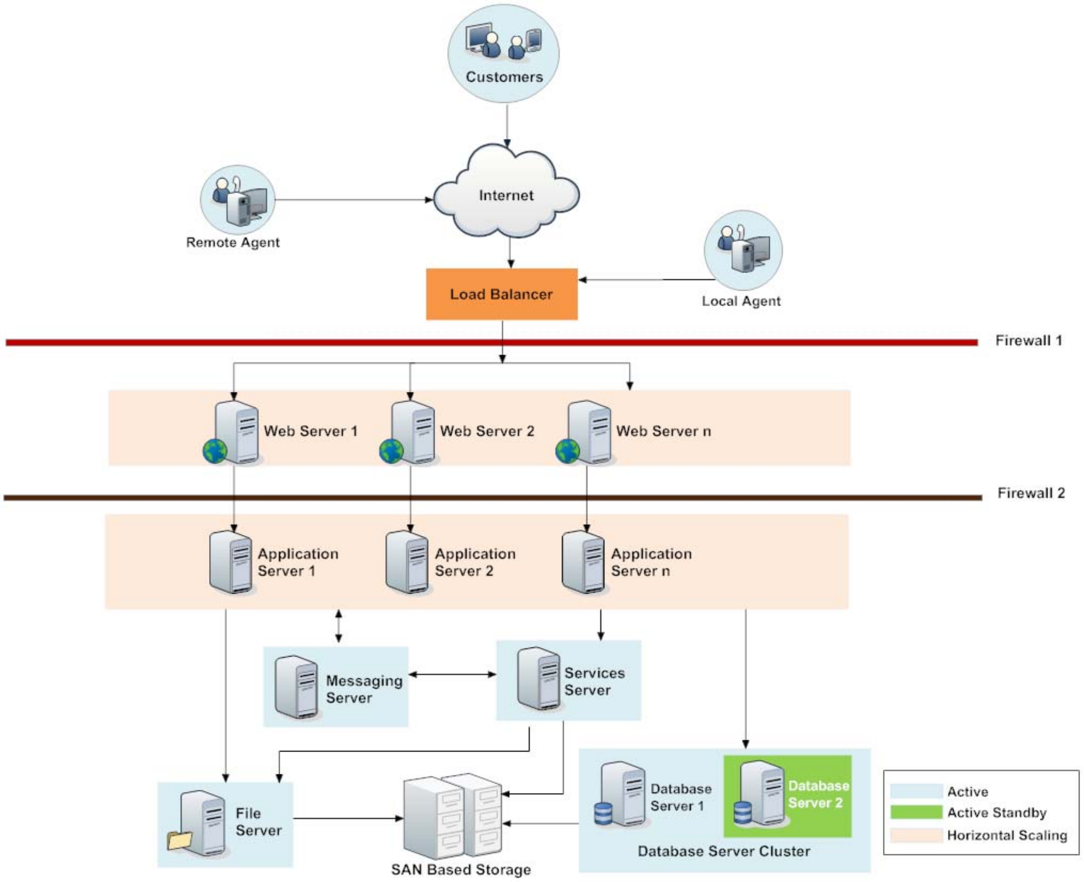
1. Ensure that all the machines are either assigned static IP addresses, or in cases where the IP address is assigned dynamically, are set to renew the same IP address upon lease expiration.
2. Ensure that all machines other than the web servers, are in the same Active Directory domain. The web servers 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.
3. 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 20.
4. 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.
5. Ensure that all the machines are in the same LAN.

6. Ensure that the system clocks of all the machines are synchronized.

7. 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 diagrams 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. The default port numbers are listed here. Ports that can be modified at the time of installation, or by editing property files are identified with an asterisk (*).

From Server	To Server	Default Destination Ports and Protocols
Agent Workstation	Web Server	▸ 80 [Protocol: HTTP] ▸ 443 [Protocol: HTTPS]
Finesse Server	Web Server	▸ 80 [Protocol: HTTP] ▸ 443 [Protocol: HTTPS]
Application Server	Services Server	▸ 15099 (RMI Registry port) [Protocol: RMI]* ▸ 49152 – 65535 (Dynamic port range used by RMI server objects) [Protocol: TCP]
Application Server	File Server	139 or 445 [Protocol: NETBIOS - TCP]
Application Server	Database Server	1433 [Protocol: TCP] *
Application Server	Messaging Server	5445, 9001 [Protocol: TCP] *
Application Server	SMTP Server	25 [Protocol: SMTP]
Application Server	SMTP or ESMTP Server (with SSL enabled)	587 [Protocol: SMTP or ESMTP]
Application Server	IMAP Server	143 [Protocol: IMAP]
Application Server	IMAP Server (with SSL enabled)	993 [Protocol: IMAP]
Web Server	Application Server	15006 [Protocol: TCP] *
Messaging Server	File Server	139 or 445 [Protocol: NETBIOS - TCP]
Services Server	File Server	139 or 445 [Protocol: NETBIOS - TCP]
Services Server	Database Server	1433 [Protocol: TCP] *
Services Server	Messaging Server	9001 [Protocol: TCP] *
Services Server	Application Server	9001 [Protocol: TCP] *
Services Server	SMTP or ESMTP Server	25 [Protocol: SMTP or ESMTP]
Services Server	SMTP or ESMTP Server (with SSL enabled)	587 [Protocol: SMTP or ESMTP]
Services Server	POP3 Server	110 [Protocol: POP3]
Services Server	POP3 Server (with SSL enabled)	995 [Protocol: POP3]
Services Server	IMAP Server	143 [Protocol: IMAP]
Services Server	IMAP Server (with SSL enabled)	993 [Protocol: IMAP]
Active Database Server	File Sever	Not applicable

From Server	To Server	Default Destination Ports and Protocols
Active Database Server	Archive Database Server	1433 [Protocol: TCP]* 135 [Port for Remote Procedure Call (RPC)] 5000-5020 (Port range for RPC ports required for MSDTC to work across firewall)
Reports Database Server	Active Database Server	1433 [Protocol: TCP]* 135 [Port for Remote Procedure Call (RPC)] 5000-5020 (Port range for RPC ports required for MSDTC to work across firewall)
Services Server	Primary CTI Server	42027*
Services Server	Secondary CTI Server	42028*
Services Server	Media Routing Peripheral Gateway	38002*
Services Server	Primary Administration Workstation Database	1433 [Protocol: TCP]*
Application Server	Primary Administration Workstation Database	1433 [Protocol: TCP]*

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: **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 59).**

Setting Up Domain Account

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

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

- If you do not want the same domain accounts to be used for running SQL services and the ECE application, you can optionally create an additional domain account for the database servers, for example, *SQLSERVICEUSER*. This account is used for running the SQL server services.

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

Configuring Permissions on Active Directory Server

If you are using Windows authentication database connectivity, *or* the configuration includes more than one database server machines, 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. For example, if there are two database servers, `tempv20w5` and `tempv20w6`, with instance name as `MSSQLSERVER` and port as `1433`, with the user account `InstallTeam` in the `domain1` domain, then run the following commands. If your MSQL Services are running with a different domain account, for example, `SQLSERVICEUSER` in the `domain1` domain, then use the `SQLSERVICEUSER` account to run these commands.

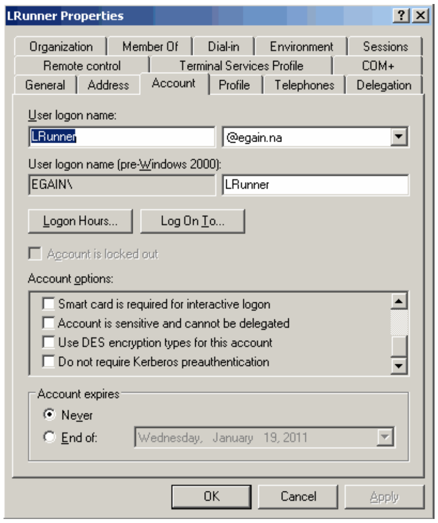
   ```
   setspn -A MSSQLSvc/tempv20w5.company.na:1433 domain1\InstallTeam
   setspn -A MSSQLSvc/tempv20w5.company.na:MSSQLSERVER domain1\InstallTeam
   setspn -A MSSQLSvc/tempv20w5:1433 domain1\InstallTeam
   setspn -A MSSQLSvc/tempv20w5:MSSQLSERVER domain1\InstallTeam
   setspn -A MSSQLSvc/tempv20w6.company.na:1433 domain1\InstallTeam
   setspn -A MSSQLSvc/tempv20w6.company.na:MSSQLSERVER domain1\InstallTeam
   setspn -A MSSQLSvc/tempv20w6:1433 domain1\InstallTeam
   setspn -A MSSQLSvc/tempv20w6:MSSQLSERVER domain1\InstallTeam
   ```

2. Go to **Start > Control Panel > Administrative Tools > Active Directory Users and Computers**.

3. Navigate to the domain user account used for MSSQL service on the database servers. Right-click and select **Properties**.

   a. In the Properties window, click the Account tab. Ensure that the following options are *not* selected:

      - **Account is sensitive and cannot be delegated**.
      - **Do not require Kerberos preauthentication**.



User logon name: LRunner @egain.na

User logon name (pre-Windows 2000): EGAIN\ LRunner

□ Account is locked out

Account options:

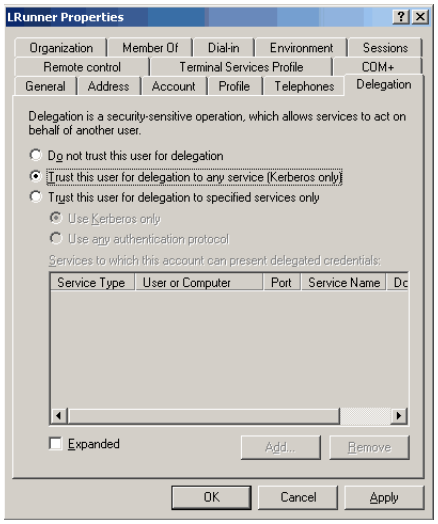
- □ Smart card is required for interactive logon
- □ Account is sensitive and cannot be delegated
- □ Use DES encryption types for this account
- □ Do not require Kerberos preauthentication

Account expires

- ● Never
- ○ End of: Wednesday, January 19, 2011

Set account properties for domain user account

b. Click the Delegation tab. Ensure that the domain user account is trusted for delegation.



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

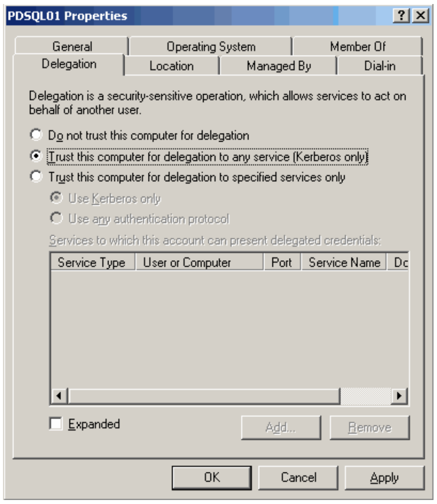
- ○ Do not trust this user for delegation
- ● Trust this user for delegation to any service (Kerberos only)
- ○ Trust this user for delegation to specified services only
  - ● Use Kerberos only
  - ○ Use any authentication protocol

Services to which this account can present delegated credentials:

□ Expanded

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.



PDSQL01 Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

● Trust this computer for delegation to any service (Kerberos only)

○ Trust this computer for delegation to specified services only

● Use Kerberos only

○ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service Name	Dc

□ Expanded

Set delegation properties for database server

Preparing Database Server Machines

Creating a New Drive for Partitioned File Groups

This section applies only to installations using MSSQL Enterprise Edition.

- It is recommended that you store the data files for the database partition groups on a separate drive than the drive where the ECE databases are installed. Create a new vDisk manually for this. For sizing of this drive, see the “Planning for Database Growth” section of the *Enterprise Chat and Email Design Guide*.

Verifying Microsoft SQL Server Features

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

Verifying Collation Settings

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

  On the Collation settings screen, choose SQL Collations and select the following option: **Dictionary order, case-insensitive, for use with 1252 Character Set.** For example, SQL_Latin1_General_CP1_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 2014, consult your DBA and verify that the collation setting chosen is ASCII (case insensitive). The application databases will be installed using the collation that is configured for MSSQL Server.

Creating SQL User for Installing ECE Databases

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

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

Assigning Permissions to Domain User

- Give `sysadmin` permission to the domain account created for installing and running the application. If you have created a separate account for the database services, then assign the permission to that user (page 22).

Configuring Database Servers

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

- All database server machines used in the configuration are in the same domain as all the other Enterprise Chat and Email servers.
- All databases are to 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 23. 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 machine.

To enable network DTC access:

1. Go to **Start > Control Panel > Administrative Tools > Component Services.**
2. In the console tree, browse **Component Services > Computers > My Computer > Distributed Transaction Coordinator > Local DTC.**
3. Right-click **Local DTC** and from the menu select **Properties.**
4. In the Local DTC Properties window, go to the Security tab and set the following:

   a. In the Security Settings section, select the following two options:

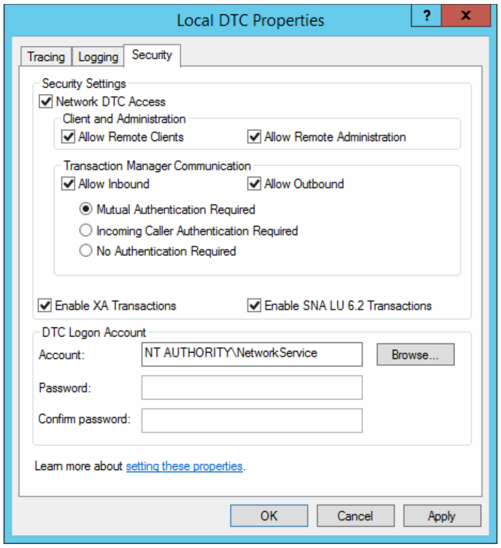
   - **Network DTC Access**
   - **Enable XA Transactions**

   b. Within the Network DTC Access section, select the following four options:

   - **Allow Remote Clients**
   - **Allow Remote Administration**
   - **Transaction Manager Communication - Allow Inbound**
   - **Transaction Manager Communication - Allow Outbound**

   c. In the DTC Logon Account section, set the value in the **Account** field to **NT Authority\NetworkService**.

   Click **OK**.



Security Settings

☑ Network DTC Access

Client and Administration

☑ Allow Remote Clients ☑ Allow Remote Administration

Transaction Manager Communication

☑ Allow Inbound ☑ Allow Outbound

● Mutual Authentication Required

○ Incoming Caller Authentication Required

○ No Authentication Required

☑ Enable XA Transactions ☑ Enable SNA LU 6.2 Transactions

DTC Logon Account

Account: NT AUTHORITY\NetworkService

Password:

Confirm password:

Learn more about setting these properties.

Enable network DTC settings

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 2014.

9. Now, start the two services in the following order:

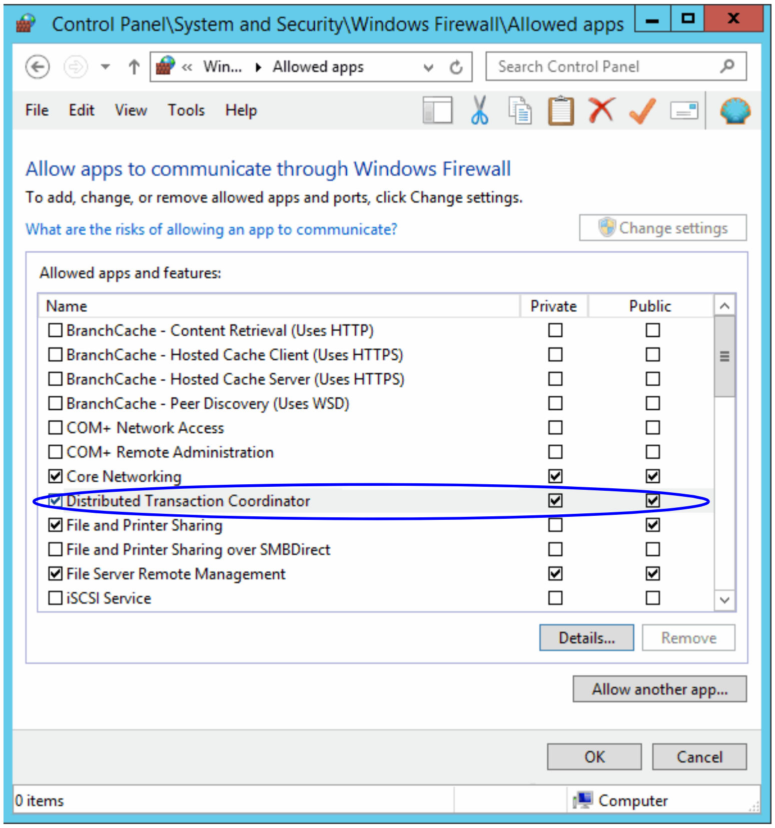
   a. **Distributed Transaction Coordinator**

   b. **SQL Server (MSSQLSERVER)** for Microsoft SQL 2014.

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**.



Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Private	Public
□ BranchCache - Content Retrieval (Uses HTTP)	□	□
□ BranchCache - Hosted Cache Client (Uses HTTPS)	□	□
□ BranchCache - Hosted Cache Server (Uses HTTPS)	□	□
□ BranchCache - Peer Discovery (Uses WSD)	□	□
□ COM+ Network Access	□	□
□ COM+ Remote Administration	□	□
☑ Core Networking	☑	☑
☑ Distributed Transaction Coordinator	☑	☑
☑ File and Printer Sharing	□	☑
□ File and Printer Sharing over SMBDirect	□	□
☑ File Server Remote Management	☑	☑
□ iSCSI Service	□	□

Select the Distributed Transaction Coordinator option

Configuring SQL Server Integration Service on the Reports Database

Important: **This task is required only in deployments that use the Enterprise Edition of MS SQL Server.**

There are six parts to completing this task:

1. First, install the SQL Server Integration service on the reports database server machine (page 29).

2. Then, create the SSISDB catalog (page 29).

3. Next, configure the recovery model for SSISDB (page 30).

4. Next, assign specific permissions to the domain user running the installer to allow them to make updates to this catalog and the schema (page 31).

5. Verify **Replace a process-level token** privilege has been enabled for the server (page 34).

6. Finally, create a folder on the machine where all data files that will be created by the application (page 34).

Installing SQL Server Integration Service

- Install the SQL Server Integration Service on the reports database server machine. To install and configure the SQL Server Integration Service, follow the instructions in the Microsoft SQL Server 2014 documentation. For details, go to http://msdn.microsoft.com and search for SQL Server Integration Service.

Creating Integration Services Catalog

Before you begin, ensure that the SSIS component is installed on the database server machine where the reports database installation is planned.

To create the Integration Services Catalog:

1. From SQL Server Management Studio, log into the reports database server with the domain user that you are going to use to install the application (page 22).

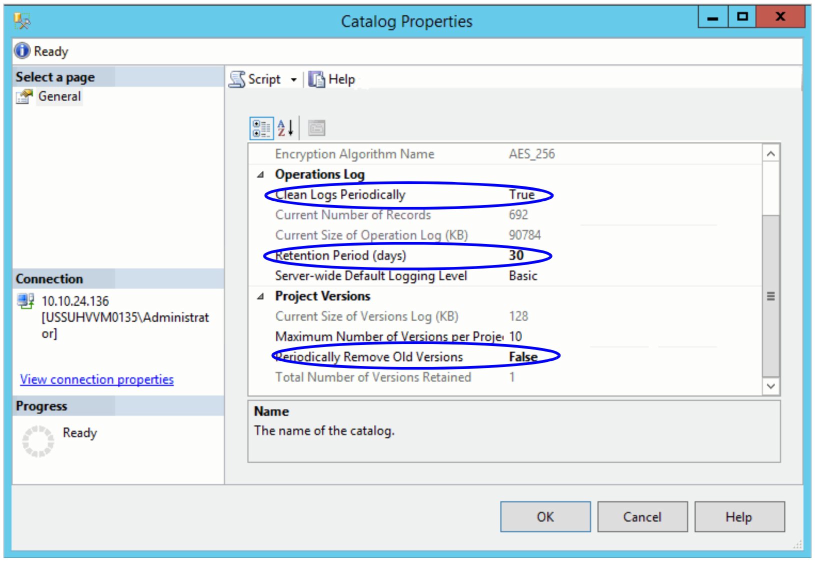
2. Locate the **Integration Services Catalogs** node in the Tree pane and use the context menu to create catalog.

   While creating the catalog, ensure that the **Enable CLR Integration** and **Enable automatic execution of Integration Services stored procedure at SQL Server startup** options are selected.

3. After the catalog is created, you should see it when you expand the SSISDB in the **Integration Services Catalogs** node.

4. Right-click SSISDB and from the context menu, select **Properties**, and configure the following properties:
   - **Clean Logs Periodically:** Set this value to **True**.
   - **Retention Period (days):** Set this value as **30** days.

- **Periodically Remove Old Versions:** Set this value to **False**.



Encryption Algorithm Name	AES_256
Operations Log	
Clean Logs Periodically	True
Current Number of Records	692
Current Size of Operation Log (KB)	90784
Retention Period (days)	**30**
Server-wide Default Logging Level	Basic
Project Versions	
Current Size of Versions Log (KB)	128
Maximum Number of Versions per Proje	10
Periodically Remove Old Versions	**False**
Total Number of Versions Retained	1

Name
The name of the catalog.

Connection
10.10.24.136
[USSUHVVM0135\Administrator]

Configure SSIS properties

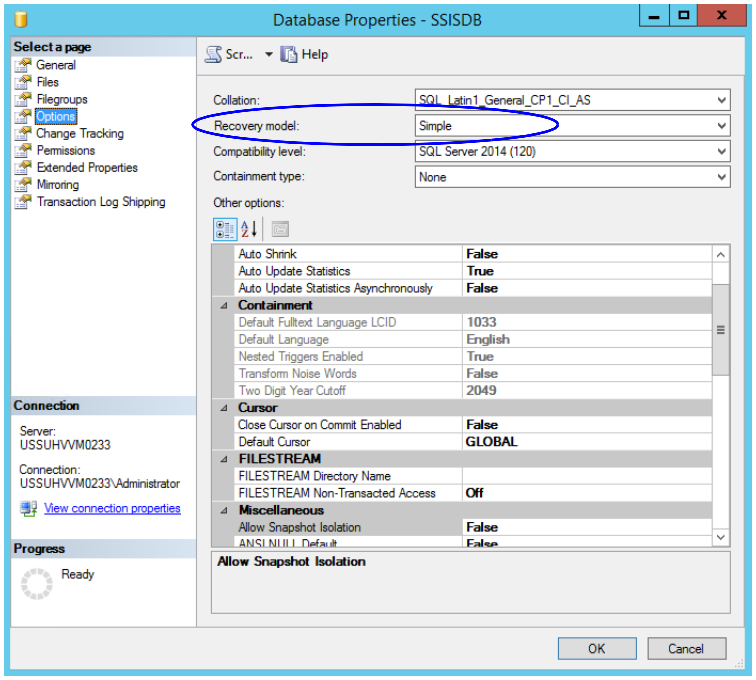
Configuring Recovery Model for SSIS Database

Change the recovery model for the SSIS database to Simple.

To configure the recovery model for SSIS database:

1. From SQL Server Management Studio, log into the reports database server.
2. Browse to **Databases > SSISDB.**
3. Right-click SSISDB and from the context menu, select **Properties**.

4. In the Database Properties window, go to the Options section and change the **Recovery model** to **Simple** and click **OK**.



Server:
USSUHVVM0233

Connection:
USSUHVVM0233\Administrator

View connection properties

Collation: SQL_Latin1_General_CP1_CI_AS

Recovery model: Simple

Compatibility level: SQL Server 2014 (120)

Containment type: None

Other options:

Auto Shrink	False
Auto Update Statistics	True
Auto Update Statistics Asynchronously	False
Containment	
Default Fulltext Language LCID	1033
Default Language	English
Nested Triggers Enabled	True
Transform Noise Words	False
Two Digit Year Cutoff	2049
Cursor	
Close Cursor on Commit Enabled	False
Default Cursor	GLOBAL
FILESTREAM	
FILESTREAM Directory Name	
FILESTREAM Non-Transacted Access	Off
Miscellaneous	
Allow Snapshot Isolation	False
ANSI NULL Default	False

Allow Snapshot Isolation

Set the recovery model for the database

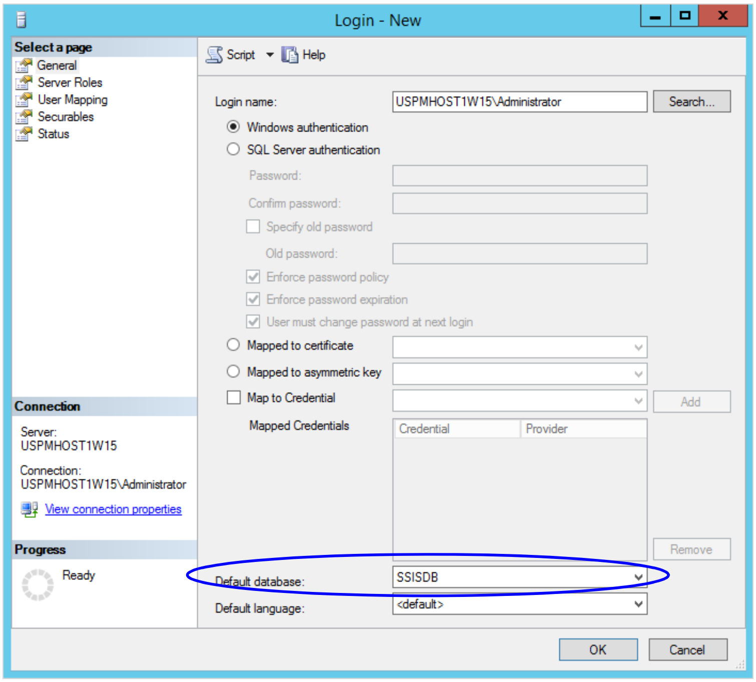
Configuring Permissions for the Domain User

Ensure that the domain user installing the ECE databases has the required permissions.

To configure permissions:

1. From SQL Server Management Studio, log into the reports database server as a database administrator.
2. Browse to **Security > Logins > New login** and do the following:

a. Add the domain login (page 22) and set the default database as `SSISDB`. You need to perform this task if your domain account is not already mapped to the SQL login.



Login name: USPMHOST1W15\Administrator

● Windows authentication

○ SQL Server authentication

Password:

Confirm password:

□ Specify old password

Old password:

☑ Enforce password policy

☑ Enforce password expiration

☑ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential

Mapped Credentials

Default database: SSISDB

Default language: <default>

Connection

Server:
USPMHOST1W15

Connection:
USPMHOST1W15\Administrator

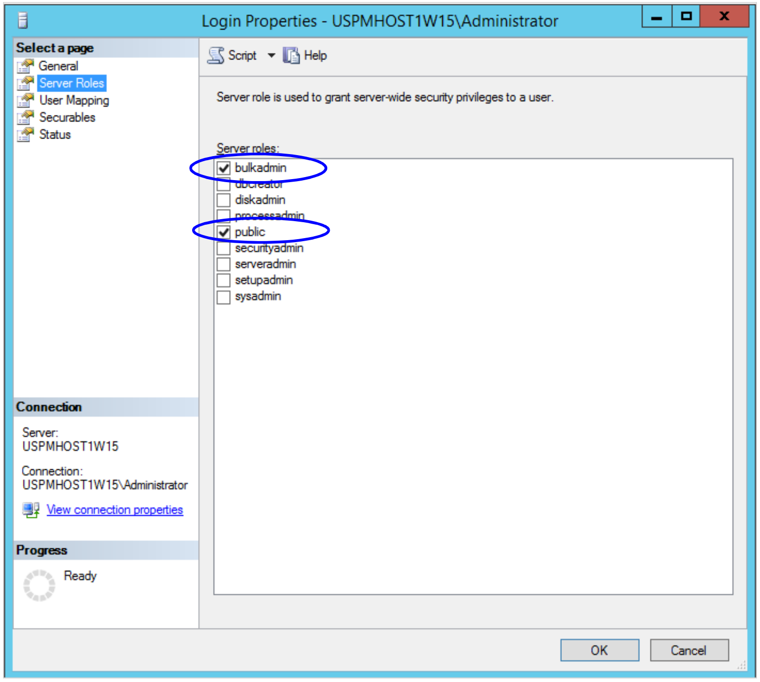
Progress

Ready

Add the new domain user

b. From the Server Roles section, assign the following server roles:

- `public`
- `bulkadmin`



Server role is used to grant server-wide security privileges to a user.

Server roles:

☑ bulkadmin
□ dbcreator
□ diskadmin
□ processadmin
☑ public
□ securityadmin
□ serveradmin
□ setupadmin
□ sysadmin

Connection

Server:
USPMHOST1W15

Connection:
USPMHOST1W15\Administrator

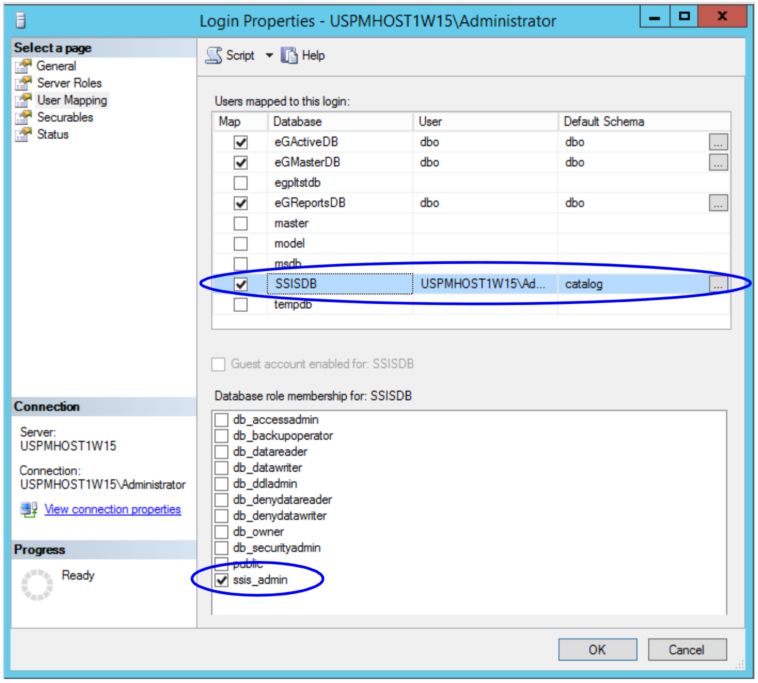
Progress

Ready

Set the server roles

c. In the User Mapping section, do the following:

- Select the **Map** option for **SSISDB** select the default schema as **catalog**.
- In the Database role membership for: SSISDB section assign the **ssis_admin** role.



Server:
USPMHOST1W15

Connection:
USPMHOST1W15\Administrator

Users mapped to this login:

Map	Database	User	Default Schema
☑	eGActiveDB	dbo	dbo
☑	eGMasterDB	dbo	dbo
□	egpltstdb		
☑	eGReportsDB	dbo	dbo
□	master		
□	model		
□	msdb		
☑	SSISDB	USPMHOST1W15\Ad...	catalog
□	tempdb		

□ Guest account enabled for: SSISDB

Database role membership for: SSISDB

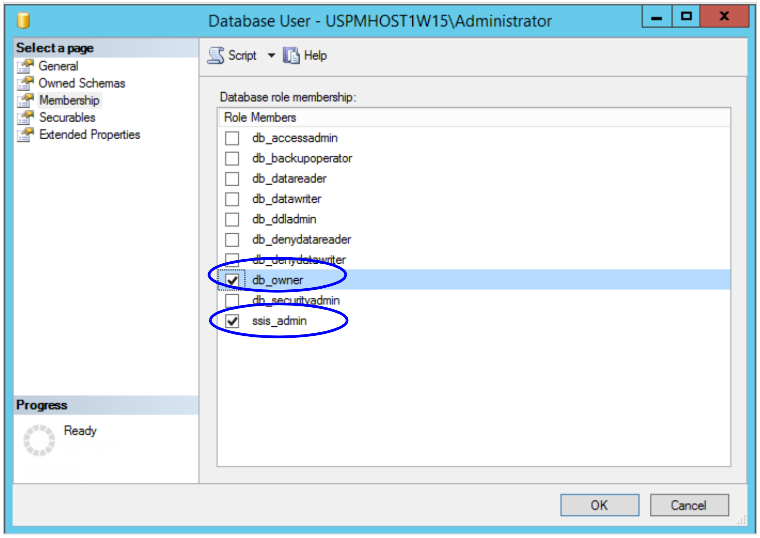
□ db_accessadmin
□ db_backupoperator
□ db_datareader
□ db_datawriter
□ db_ddladmin
□ db_denydatareader
□ db_denydatawriter
□ db_owner
□ db_securityadmin
□ public
☑ ssis_admin

Set user mapping

3. Now, browse to **Databases > SSISDB > Security > Users,** and do the following:

   a. Right-click the domain user and select **Properties**.

   b. In the Database User window, go to the Membership section and select **db_owner** and **ssis_admin**. Click **OK**.



Database role membership:

Role Members

□ db_accessadmin
□ db_backupoperator
□ db_datareader
□ db_datawriter
□ db_ddladmin
□ db_denydatareader
□ db_denydatawriter
☑ db_owner
□ db_securityadmin
☑ ssis_admin

Set membership

Verifying Server Privileges

Ensure 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.
2. Navigate to **Local Computer Policy > Windows Settings > Security Settings > Local Policies > User Right Assignment > Replace a process level token**.
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\MSSQL`*DB_Instance_Name*.
6. To apply your changes, restart the reports database 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 machine, for example, *D:\ssis_data* and ensure that the domain user has **write** and **modify** permissions on this folder.

Running SQL Server Services

Make sure the following SQL services are running. These services should be started using the same domain account that you have created for installing the ECE application. If your MSQL Services are running with a different domain account, then use that account. (page 22).

- **SQL Server Service**
- **SQL Full-text Filter Daemon Launcher Service:** This service is required for text searches.
- **SQL Server Agent Service:** This service is used by the Reports module.
- **SQL Server Integration Service:** This service is used by the Reports module.
- **SQL Server Browser Service:** In configurations where database servers are configured to run on named instances, and no listener port is configured, the SQL Server Browser service needs to be running when you run the installer. This service does not have to be running if the database servers are configured to run on the default instance. It is also not required if the database servers are configured to run on named instances, and specific, static listener ports are configured for the named instances.

To start the services:

1. Go to **Start** > **Programs** > **Administrative Tools** > **Services**.

2. For the SQL Full-text Filter Daemon Launcher, SQL Server Agent, SQL Server, and SQL Server Browser services check if the right domain account is used for starting the services.

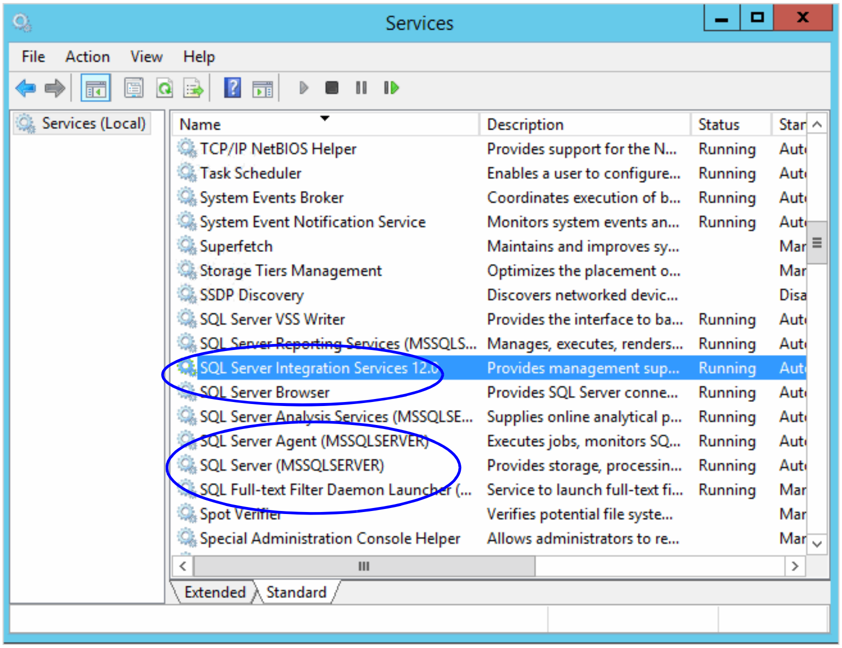
   a. Select a service and right-click to open the menu.

   b. From the menu select **Properties**.

   c. In the Properties window, go to Log On tab and ensure the service is started using the same domain account that you have created for installing the ECE application (page 22).

3. Ensure that the SQL Full-text Filter Daemon Launcher, SQL Server Agent, SQL Server, SQL Server Integration Service, and SQL Server Browser services are running.

4. If they are not running, select the services one by one, and click **Start** to start the service.



Name	Description	Status	Star
TCP/IP NetBIOS Helper	Provides support for the N...	Running	Aut
Task Scheduler	Enables a user to configure...	Running	Aut
System Events Broker	Coordinates execution of b...	Running	Aut
System Event Notification Service	Monitors system events an...	Running	Aut
Superfetch	Maintains and improves sy...		Mar
Storage Tiers Management	Optimizes the placement o...		Mar
SSDP Discovery	Discovers networked devic...		Disa
SQL Server VSS Writer	Provides the interface to ba...	Running	Aut
SQL Server Reporting Services (MSSQLS...	Manages, executes, renders...	Running	Aut
SQL Server Integration Services 12.0	Provides management sup...	Running	Aut
SQL Server Browser	Provides SQL Server conne...	Running	Aut
SQL Server Analysis Services (MSSQLSE...	Supplies online analytical p...	Running	Aut
SQL Server Agent (MSSQLSERVER)	Executes jobs, monitors SQ...	Running	Aut
SQL Server (MSSQLSERVER)	Provides storage, processin...	Running	Aut
SQL Full-text Filter Daemon Launcher (...	Service to launch full-text fi...	Running	Mar
Spot Verifier	Verifies potential file syste...		Mar
Special Administration Console Helper	Allows administrators to re...		Mar

Start the SQL services

Preparing Web Server Machines

Configuring Roles and Features

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

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

- NET Extensibility 4.5
- ASP
- CGI
- ISAPI Extensions

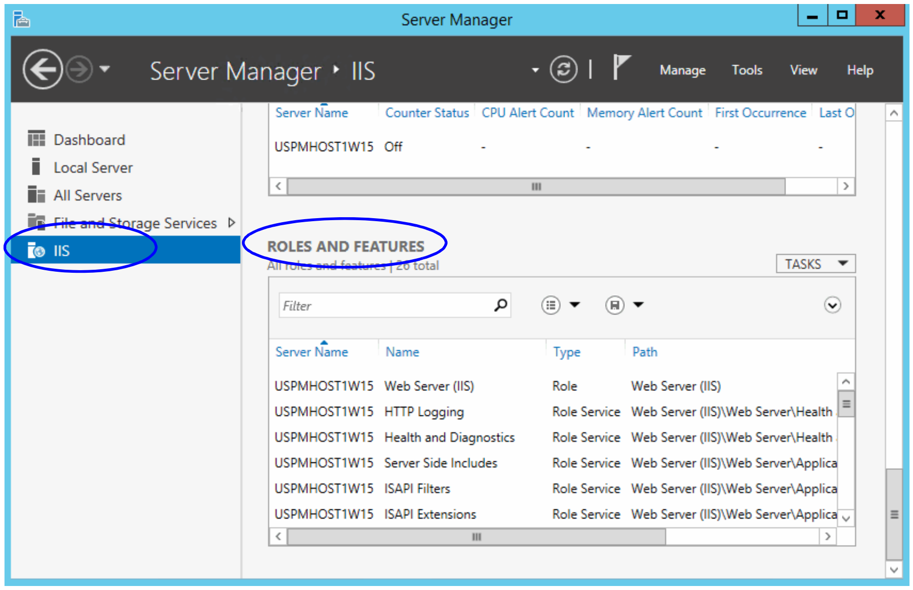
- ISAPI Filters
- Server Side Includes
- Static Content
- Static Content Compression
- Dynamic Content Compression
- Directory Browsing
- Default Document

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

- WebDAV Publishing

To install the roles and features:

1. Go to **Start > Control Panel > Administrative Tools > Server Manager.**
2. In the Server Manager window, Go to IIS section. In the IIS section, locate the Roles and Features section.



Server Name	Counter Status	CPU Alert Count	Memory Alert Count	First Occurrence	Last O
USPMHOST1W15	Off	-	-	-	-

Server Name	Name	Type	Path
USPMHOST1W15	Web Server (IIS)	Role	Web Server (IIS)
USPMHOST1W15	HTTP Logging	Role Service	Web Server (IIS)\Web Server\Health
USPMHOST1W15	Health and Diagnostics	Role Service	Web Server (IIS)\Web Server\Health
USPMHOST1W15	Server Side Includes	Role Service	Web Server (IIS)\Web Server\Applica
USPMHOST1W15	ISAPI Filters	Role Service	Web Server (IIS)\Web Server\Applica
USPMHOST1W15	ISAPI Extensions	Role Service	Web Server (IIS)\Web Server\Applica

Go to Roles and Features section

3. In the Role and Features section, check if the required role services are installed.
4. If any of the roles and features are not installed, from the Tasks menu, click the **Add Roles and Features** button and run through the wizard to install the missing services. In the Server Roles section, expand the **Web Server (IIS)** list, and select the following:
   - In the Common HTTP Features list, select:
     - Default Document
     - Directory Browsing
     - Static Content
   - In the Performance list, select:
     - Static Content Compression

        - Dynamic Content Compression
    - In the Application Development list, select:
        - NET Extensibility 4.5
        - ASP
        - CGI
        - ISAPI Extensions
        - ISAPI Filters
        - Server Side Includes

5. In the Role and Features section, check if the **WebDAV Publishing** feature is installed. If the feature is installed, you need to uninstall it. From the Tasks menu, click the **Remove Roles and Features** button and run through the wizard to uninstall the feature.

Installing IIS Rewrite Module on Web Servers

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

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

Configuring Permissions on IIS Config Folder

- Ensure that the user account you are going to use for installing the application (page 22) has read permissions on the following folder: `%systemroot%\system32\inetsrv\config`

Running the World Wide Web Publishing Service

- On all machines 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.

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

On the Database Servers

Follow the instructions for your virus scanning software to exclude the following folders and file types.

Item	Exclude Subfolders?	Permissions
Windows File Protection	--	Read, Write
All files of type LOG, if any	--	Read, Write
Pagefile.sys	No	Read, Write
Drive:\Path_to_datafile	Yes	Read, Write
Drive:\Path_to_SSIS_datafile	Yes	Read, Write
*.mdf	No	Read, Write
*.ldf	No	Read, Write
*.ndf	No	Read, Write
*.dat	No	Read, Write
*.rll	No	Read, Write

Verifying Unified CCE Configuration

- Verify that Unified CCE and Microsoft Active Directory (AD) have been installed on separate servers. Refer to Unified CCE documentation for more details.

- Verify that the Unified CCE and AD servers are in the same network as the ECE servers and are accessible from the ECE servers.
- Verify that the items to be used in ECE are configured in Unified CCE. These include:
  - Peripherals
  - Application Instance
  - Media Classes
  - Media Routing Domains (MRDs)
  - Network Voice Response Units (Network VRUs)
  - Call Type
  - Media Routing Peripheral Gateways (MR PGs)
  - Script Selector
  - Agent Peripheral Gateway (Agent PG)
  - Network Trunk Groups
  - Network Trunks
  - Application Paths and Path Members
  - Agents
  - Skill Groups
  - ICM Scripts
  - Expanded Call Context (ECC) Variables
  - CTI Gateways (CG)

  For details, see *Enterprise Chat and Email Deployment and Maintenance Guide*.

3

Installation Process

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 18.

Installation Overview

You can do a collocated deployment, where all components, except for the web server, are installed on the same machine and the web server is installed on a separate machine. 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 machine.

When each component is on a different machine, 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 web server components, on the same machine, make sure that you install both application server and web 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 machines where these components need to be installed.

Installing ECE

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

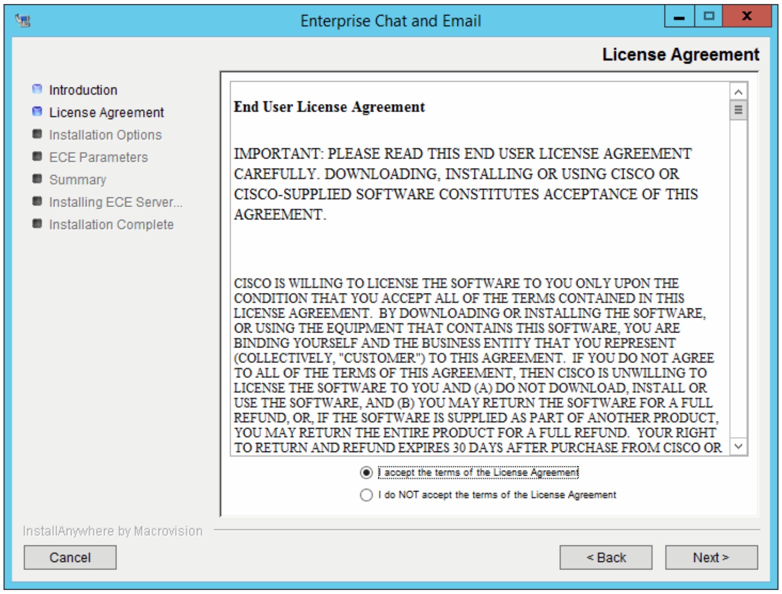
To install ECE:

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**.



End User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND, OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR

● I accept the terms of the License Agreement

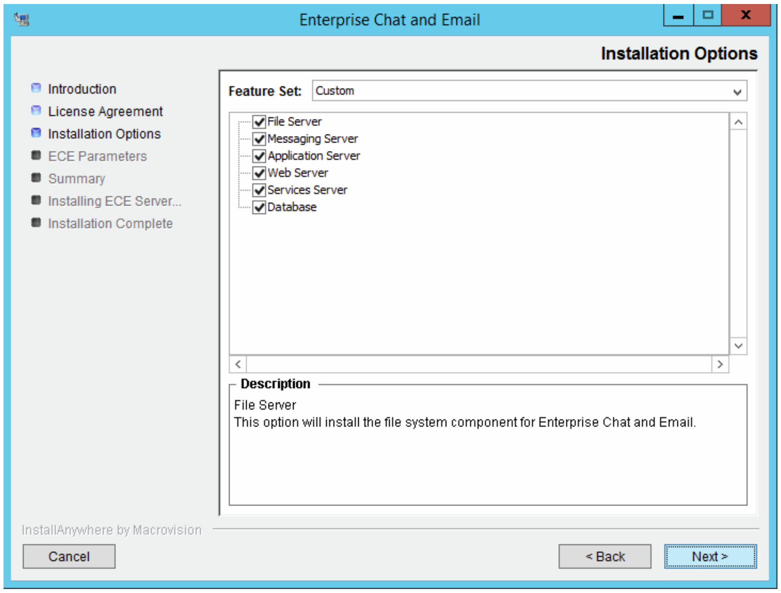
○ I do NOT accept the terms of the License Agreement

Read and accept the terms of the License Agreement

4. In the Installation Options window, select from the following components. Make sure you select all the components you wish to install. For details, see "Installation Overview" on page 41.

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

Click **Next**.



Feature Set: Custom

☑ File Server
☑ Messaging Server
☑ Application Server
☑ Web Server
☑ Services Server
☑ Database

Description

File Server
This option will install the file system component for Enterprise Chat and Email.

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 44
- Database Server Details on page 45
- Web Server Details on page 52
- Messaging Server Details on page 53
- Application Server Details on page 53
- Services Server Details on page 55

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 56).

Installation Details

File Server Details

#	Graphic Installation	Description	Value
Enterprise Chat and Email Home Directory			
1.	File Server Directory/NAS path	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. **Note:** Make sure that the path and folder name do not contain any of the following characters: *?<>|+^'"%`,@	
Domain User Account Parameters			
2.	Domain user name	User name of the domain user account created for use by the application. For more information, refer to "Setting Up User Accounts and Permissions" on page 22.	
3.	Domain user password	Password for the domain user.	

File server details

Database Server Details

#	Graphic Installation	Description	Value
File Sever Parameters			
1.	File Server Name/NAS Path	The fully qualified domain name of the file server. If the file server is installed on a NAS device, provide the path to the shared folder on the NAS device. For example, \\SharedSpace\Cisco. **Note:** Make sure you provide the DNS host name and not the IP address of the server.	
Cisco Application Context Root			
2.	Context Root Name	The name used to identify the document root of the Web Server. The context root of a web application determines which URLs are delegated to the web application. **Note:** Make sure there are no spaces or special characters in the name of the context root.	system
Cisco System Administrator Account			
3.	User name	User name for the system administrator. This is the first user that gets created for accessing the system partition.	sa
4.	Password	Password for the system administrator. **Note:** The password should have at least eight characters and should be a mix of numbers and letters. For example, `password@123`. Do not use the following characters in the password: < (less than), > (greater than), ; (semi colon), : (colon), = (equal to), \ (back slash)	
Cisco Partition Administrator Account and Partition Details			
5.	User name	User name for the partition administrator. This is the first user that gets created for accessing the business partition.	pa
6.	Password	Password for the partition administrator. **Note:** The password should have at least eight characters and should be a mix of numbers and alphabets. For example, `password@123`. Do not use the following characters in the password: < (less than), > (greater than), ; (semi colon), : (colon), = (equal to), \ (back slash)	
7.	Partition name	Name for the business partition. Make sure that the name does not contain any spaces or special characters. Also, the partition name should be different than the context root name.	default
8.	Description of partition	Description for the partition.	
Installation Identifiers			

#	Graphic Installation	Description	Value
9.	Unique name for this installation	Provide a unique name for this installation. For example: PROD, PRD1, TEST, TST2, or DEMO. The length of the name must be between 1 and 4 characters long. The name must not contain any spaces or special characters.	
10.	4-digit identifier for this installation	Provide a 4-digit numerical value, between 2001 and 9998, that will be used internally as system ID.	
Knowledge Base Primary Language			
11.	Knowledge Base Primary Language	The default language for the Knowledge Base.	English (US)
Default Notification Parameters			
12.	Default SMTP server	The SMTP server to be used to send email notifications.	
13.	Notification mail redirection from address	All notification emails are sent from this email address.	
14.	Notification mail redirection to address	All notification emails are sent to this email address.	
SQL Server Database Authentication			
15.	Authentication	Authentication type to be used while connecting to the database. Set the value as **SQL Server Authentication mode** or **Windows Authentication mode.** If you selected Windows Authentication as the only mode of authentication while installing SQL Server, you must set the value as **Windows Authentication mode.**	
Master Database Parameters			
16.	Server name	Name of the local or remote server on which you want to install the master database. **Note:** Make sure you provide the DNS host name and not the IP address.	
17.	Database name	Name of the master database. The installation program creates a database with the name you provide here.	
18.	Server instance name	Name of the MSSQL Server instance to be used while creating the database. Set this value only if you are using a named instance, and not the default instance.	
19.	Database listener port	Port number of the MSSQL Server.	1433
20.	Datafile path	Path to the folder on the database server, where you want to create the data file. For example, `D:\MSSQL\Data`.	
21.	Datafile initial size (MB)	Minimum size of the data file for the database.	100
22.	Datafile maximum size (MB)	Maximum size of the data file for the database.	Unlimited

#	Graphic Installation	Description	Value
23.	Datafile increment size (MB)	Additional file size limit that will be allocated to the database after the initial size is full.	10
24.	Logfile initial size (MB)	Minimum size of the log file.	25
25.	Logfile maximum size (MB)	Maximum size of the log file.	Unlimited
26.	Database administrator user name	User name of the database administrator for MSSQL Server. If you have created a separate user for installing Enterprise Chat and Email databases, provide the name of that user (page 26). **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
27.	Database administrator password	Password of the database administrator. **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
28.	Cisco Database user name	User name required to connect to the master database. The installation program creates the database and its user.	
29.	Cisco Database password	Password for the master database user.	
Active Database Parameters			
30.	Server name	Name of the local or remote server on which you want to install the active database. **Note:** It must be the same server on which the master database is installed.	
31.	Database name	Name of the active database. The installation program creates a database with the name you provide here.	
32.	Server instance name	Name of the MSSQL Server instance to be used while creating the database. This should match the value set for the master database instance name.	
33.	Database listener port	Port number of MSSQL Server. This should match the value set for the master database.	1433
34.	Datafile path	Path to the folder on the database server, where you want to create the data file. For example, `C:\MSSQL\Data`.	
35.	Datafile initial size (MB)	Minimum size of the data file for the database.	2048
36.	Datafile maximum size (MB)	Maximum size of the data file for the database.	Unlimited
37.	Datafile increment size (MB)	Additional file size limit that will be allocated to the database after the initial size is full.	500
38.	Logfile initial size (MB)	Minimum size of the log file.	1024
39.	Logfile maximum size (MB)	Maximum size of the log file.	Unlimited

#	Graphic Installation	Description	Value
40.	Database administrator user name	User name of the database administrator for MSSQL Server. If you have created a separate user for installing Enterprise Chat and Email databases, provide the name of that user (page 26). **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
41.	Database administrator password	Password of the database administrator. **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
42.	Cisco Database user name	User name required to connect to the database. The installation program will create this user. **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
43.	Cisco Database password	Password for the database user. **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
Active Database Filegroup Parameters [Only for Enterprise Edition of MSSQL Server]			
44.	Filegroup Datafile 1 Name	Provide the name of the first file group to be created for the active database.	
45.	Filegroup Datafile 1 Path	Provide the location for the first filegroup. If you created a separate drive for the file groups, then provide the path to that drive (page 25).	
46.	Filegroup Datafile 2 Name	Provide the name of the second file group to be created for the active database.	
47.	Filegroup Datafile 2 Path	Provide the location for the second filegroup. If you created a separate drive for the file groups, then provide the path to that drive (page 25).	
48.	Filegroup Datafile 3 Name	Provide the name of the third file group to be created for the active database.	
49.	Filegroup Datafile 3 Path	Provide the location for the third filegroup. If you created a separate drive for the file groups, then provide the path to that drive (page 25).	
50.	Filegroup Datafile 4 Name	Provide the name of the fourth file group to be created for the active database.	
51.	Filegroup Datafile 4 Path	Provide the location for the fourth filegroup. If you created a separate drive for the file groups, then provide the path to that drive (page 25).	
Reports Database Parameters [Only for Enterprise Edition of MSSQL Server]			
52.	Server name	Name of the local or remote server on which the reports database should be installed. **Note:** Make sure you provide the DNS host name and not the IP address of the server.	

#	Graphic Installation	Description	Value
53.	Database name	Name of the reports database. The installation program creates a database with the name you type here.	
54.	Database server instance	Name of the MSSQL Server instance to be used while creating the database. Set this value only if you are using a named instance, and not the default instance.	
55.	Database listener port	Port number of the MSSQL Server.	1433
56.	Datafile path	Path to the folder on the database server, where you want to create the data file. For example, `D:\MSSQL\Data`.	
57.	Datafile initial size (MB)	Minimum size of the data file for the database.	1024
58.	Datafile maximum size (MB)	Maximum size of the data file for the database.	Unlimited
59.	Datafile increment size (MB)	Additional file size limit that will be allocated to the database after the initial size is full.	500
60.	Logfile initial size (MB)	Minimum size of the log file.	512
61.	Logfile maximum size (MB)	Maximum size of the log file.	Unlimited
62.	Database administrator user name	User name of the database administrator for MSSQL Server. If you have created a separate user for installing Enterprise Chat and Email databases, provide the name of that user (page 26). **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
63.	Database administrator password	Password of the database administrator. **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
64.	Cisco Database user name	User name required to connect to the reports database. The installation program will create this user. **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
65.	Cisco Database password	Password for the database user. **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
Reports Database Filegroup Parameters [Only for Enterprise Edition of MSSQL Server]			
66.	Filegroup Datafile 1 Name	Provide the name of the first file group to be created for the reports database.	
67.	Filegroup Datafile 1 Path	Provide the location for the first filegroup. If you created a separate drive for the file groups, then provide the path to that drive (page 25).	
68.	Filegroup Datafile 2 Name	Provide the name of the second file group to be created for the reports database.	
69.	Filegroup Datafile 2 Path	Provide the location for the second filegroup. If you created a separate drive for the file groups, then provide the path to that drive (page 25).	

#	Graphic Installation	Description	Value
70.	Filegroup Datafile 3 Name	Provide the name of the third file group to be created for the reports database.	
71.	Filegroup Datafile 3 Path	Provide the location for the third filegroup. If you created a separate drive for the file groups, then provide the path to that drive (page 25).	
72.	Filegroup Datafile 4 Name	Provide the name of the fourth file group to be created for the reports database.	
73.	Filegroup Datafile 4 Path	Provide the location for the fourth filegroup. If you created a separate drive for the file groups, then provide the path to that drive (page 25).	
Reports Database SSIS Parameters [Only for Enterprise Edition of MSSQL Server]			
74.	SSIS Datafile Path	Provide the path of the SSIS Directory created on the reports database server (page 34). For example, `D:\ssis_data`	
Archive Database Parameters [Only for Standard Edition of MSSQL Server]			
75.	Server name	Name of the local or remote server on which the archive database should be installed. **Note:** Make sure you provide the DNS host name and not the IP address of the server.	
76.	Database name	Name of the archive database. The installation program creates a database with the name you provide here.	
77.	Database server instance	Name of the MSSQL Server instance to be used while creating the database. Set this value only if you are using a named instance, and not the default instance.	
78.	Database listener port	Port number of the MSSQL Server.	1433
79.	Datafile path	Path to the folder on the database server, where you want to create the data file. For example, `C:\MSSQL\Data`.	
80.	Datafile initial size (MB)	Minimum size of the data file for the database.	512
81.	Datafile maximum size (MB)	Maximum size of the data file for the database.	Unlimited
82.	Datafile increment size (MB)	Additional file size limit that will be allocated to the database after the initial size is full.	10
83.	Logfile initial size (MB)	Minimum size of the log file.	50
84.	Logfile maximum size (MB)	Maximum size of the log file.	Unlimited
85.	Database administrator user name	User name of the database administrator for MSSQL Server. If you have created a separate user for installing Enterprise Chat and Email databases, provide the name of that user (page 26). **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	

#	Graphic Installation	Description	Value
86.	Database administrator password	Password of the database administrator. **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
87.	Cisco Database user name	User name required to connect to the archive 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.	
88.	Cisco Database password	Password for the database user. **Note:** This property needs to be configured only if you are using the SQL Server Authentication mode.	
Domain User Account Parameters			
89.	Domain user name	User name of the domain user account you created for use by the application. For more information, refer to "Setting Up User Accounts and Permissions" on page 22.	
90.	Domain user password	Password for the domain user.	

Database server details

Web Server Details

#	Graphic Installation	Description	Value
Application Server Parameters			
1.	Application server name	Type the name of the application server for which you want to configure the web server. **Note:** Make sure you provide the DNS host name and not the IP address of the server.	
Enterprise Chat and Email Directory			
2.	Enterprise Chat and Email Home Directory	Provide the path of the directory where you would like to install ECE. For example, `C:\Cisco`. **Note:** Make sure that the path and folder name do not contain any of the following characters: *?<>|+^'"%`,@	
IIS Web Site Parameters			
3.	IIS Web Site Name	Name of the IIS Web Site on which the application is to be configured.	Default Web Site
Cisco Application Context Root			
4.	Context Root Name	Provide the same context root name which was provided at the time of installing the Cisco database server (page 45).	
Cisco Partition Name			
5.	Partition Name	Provide the name for the business partition. Make sure you provide the same name which was provided at the time of installing the Cisco database server (page 45).	
Domain User Account Parameters			
6.	Domain user name	User name of the domain user account you created for use by the application. For more information, refer to "Setting Up User Accounts and Permissions" on page 22.	
7.	Domain user password	Password for the domain user.	

Web server details

Messaging Server Details

#	Graphic Installation	Description	Value
File Server Parameters			
1.	File Server name/NAS Path	The fully qualified domain name of the file server. If the file server is installed on a NAS device, provide the path to the shared folder on the NAS device. For example, `\\SharedSpace\Cisco`. **Note:** Make sure you provide the DNS host name and not the IP address of the server.	
Enterprise Chat and Email Home Directory			
2.	Enterprise Chat and Email Home Directory	Provide the path of the directory where you would like to install Enterprise Chat and Email. For example, `C:\Cisco`. The installation program also installs WildFly and JDK at the same location. **Note:** Make sure that the path and folder name do not contain any of the following characters: *?<>|+^'"%`,@	
WildFly Parameters			
3.	WildFly HTTP port	Port number used by WildFly.	9001
4.	WildFly HTTP SSL Port	Secure Sockets Layer port number used by WildFly.	9002
Domain User Account Parameters			
5.	Domain user name	User name of the domain user account you created for use by the application. For more information, refer to "Setting Up User Accounts and Permissions" on page 22.	
6.	Domain user password	Password for the domain user.	

Messaging server details

Application Server Details

#	Graphic Installation	Description	Value
File Server Parameters			
1.	File Server name/ NAS Path	The fully qualified domain name of the file server. If the file server is installed on a NAS device, provide the path to the shared folder on the NAS device. For example, `\\SharedSpace\Cisco` **Note:** Make sure you provide the DNS host name and not the IP address of the server.	

#	Graphic Installation	Description	Value
Enterprise Chat and Email Home Directory			
2.	Enterprise Chat and Email Home Directory	Provide the path of the directory where you would like to install ECE. For example, `C:\Cisco`. The installation program also installs WildFly and JDK at the same location. **Note:** Make sure that the path and folder name do not contain any of the following characters: *?<>|+^'"%`,@	
WildFly Parameters			
3.	WildFly HTTP port	Port number used by JBoss.	9001
4.	WildFly HTTP SSL Port	Secure Sockets Layer port number used by JBoss.	9002
Domain User Account Parameters			
5.	Domain user name	User name of the domain user account you created for use by the application. For more information, refer to "Setting Up User Accounts and Permissions" on page 22.	
6.	Domain user password	Password for the domain user.	

Application server details

Services Server Details

#	Graphic Installation	Description	Value
File Server Parameters			
1.	File Server name/NAS Path	The fully qualified domain name of the file server. If the file server is installed on a NAS device, provide the path to the shared folder on the NAS device. For example, `\\SharedSpace\Cisco` **Note:** Make sure you provide the DNS host name and not the IP address of the server.	
Enterprise Chat and Email Home Directory			
2.	Enterprise Chat and Email Home Directory	Provide the path of the directory where you would like to install ECE. For example, `C:\Cisco`. The installation program also installs JDK at the same location. **Note:** Make sure that the path and folder name do not contain any of the following characters: *?<>|+^'"%`,@	
RMI and RMID Parameters			
3.	RMI registry port	Port number used by the Remote Method Invocation (RMI) registry naming service.	15099
4.	RMI activation port	Port number used by the RMI Daemon Process.	15098
Organization Information			
5.	Name	Provide the name of the organization. Make sure that the name does not contain any special characters.	
6.	Business Unit	Provide the business unit name. Make sure that the value does not contain any special characters.	
7.	Location	Provide the location of your organization. Make sure that the value does not contain any special characters.	
8.	Country	Select the country from the dropdown list.	
Domain User Account Parameters			
9.	Domain user name	User name of the domain user account you created for use by the application. For more information, refer to "Setting Up User Accounts and Permissions" on page 22.	
10.	Domain user password	Password for the domain user.	

Services server details

4

Post-Installation Tasks

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 37). Ensure that the user account that you used for installing the application (page 22) has read permissions on the following folder on the web server: `%systemroot%\system32\inetsrv\config.`

Configuring SSL for Secure Connections

- You must set up Secure Sockets Layer (SSL) for more secure connections between browsers and the servers in your installation. This is a required step. See "SSL Configuration" on page 93 for details.

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 MS SQL Server Enterprise edition. You can do this task any time after installing the ECE application.

To create an encrypted SQL server database:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- Agents always access ECE through Finesse. After installing ECE, configure Finesse to add the ECE gadget. For details about doing this task, see *Enterprise Chat and Email Deployment and Maintenance Guide*.

Configuring Active Directory Federation Services for Single Sign-On

- Single Sign-On with Cisco IDS requires that ECE is connected to Active Directory Federation Services (AD FS). If you are planning to use single sign-on, see "Single Sign-On Configuration" on page 67 for details about configuring AD FS.

Starting ECE

There is no mandatory sequence that should be followed while starting ECE. All the machines 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 22).**

To start ECE:

If you get the following error while starting the Cisco Service, see "Troubleshooting Application Start-Up Issues" on page 60: `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 machines in the configuration are available and connected to the network.

  a. Start Cisco Service on the messaging server by starting the Cisco Windows service from the Windows Services panel.

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

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

Troubleshooting Application Start-Up Issues

Perform these tasks if you get the following error while starting the 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 22) 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 server

To stop ECE:

- In 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 machine, stop the Cisco Service from the Windows Services panel.

  b. On the messaging server machine, stop the Cisco Service from the Windows Services panel.

  c. On the services server machine, stop the Cisco Service from the Windows Services panel.

  d. On the services server machine, open the Windows Task Manager and verify that none of the javaw and java processes (the services) are running.

Signing in to ECE

Signing in to Agent Console

To sign in to the Agent Console:

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

Signing in to All Other Consoles

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

To sign in to the business partition:

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

   Always use the fully qualified domain name of the web server when you type the URL to access ECE.
3. In the Sign In window, type the user name and password you had set up for the partition administrator in the Partition Administrator Login Parameters window during the installation. Click the **Log In** button.

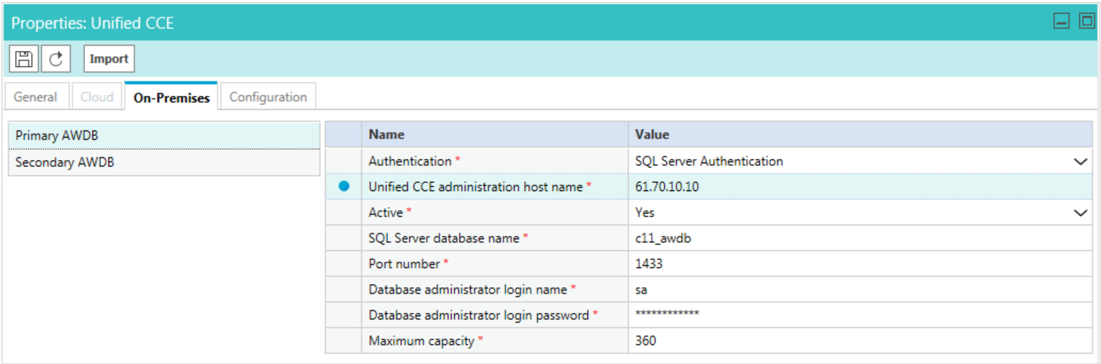
Integrating ECE with Unified CCE

Integration between ECE and Unified CCE is enabled and configured through the Administration Console.

To integrate ECE with Unified CCE:

1. Sign in to the Administration Console as a partition administrator.
2. In the Tree pane, browse to **Administration > Partition:** *Partition Name* **> Integration > Unified CCE > Unified CCE.**
3. Go to the On-Premise tab and provide the following details for the Primary AWDB.

- **Authentication:** Select from **Windows Authentication** or **SQL Authentication.**
- **Unified CCE administration host name:** The server name or IP address of the Unified CCE host.
- **Active:** Set to **Yes**.
- **SQL server database name:** The name of the AWDB database.
- **Port number:** Set the value to match the port configured in Unified CCE. By default the value is set to 1433.
- **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.



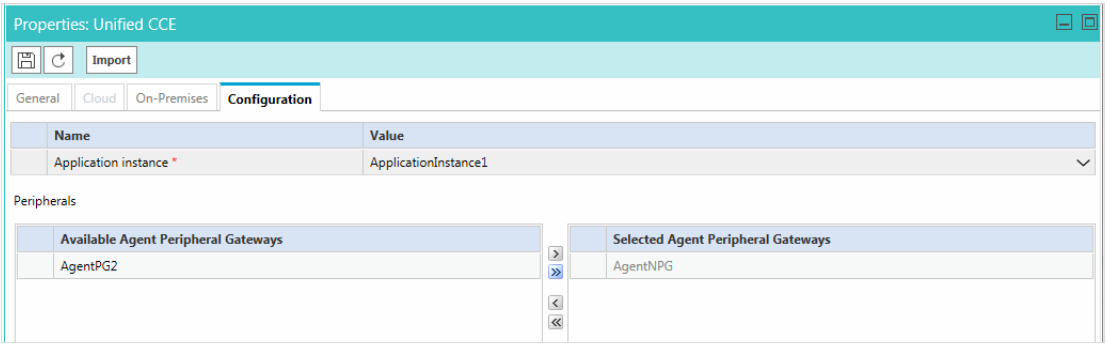
Name	Value
Authentication *	SQL Server Authentication
Unified CCE administration host name *	61.70.10.10
Active *	Yes
SQL Server database name *	c11_awdb
Port number *	1433
Database administrator login name *	sa
Database administrator login password *	************
Maximum capacity *	360

Provide the primary AWDB server details

4. If you have a secondary AWDB and wish to apply it to your integration, click the Secondary AWDB section and provide the necessary details.
5. Click the **Save** button.
6. In the Properties pane, on the Configuration tab, set the following:
    - Select the Application Instance.

- Select any Agent Peripheral Gateways that apply.

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



Name	Value
Application instance *	ApplicationInstance1

Peripherals

Available Agent Peripheral Gateways
AgentPG2

Selected Agent Peripheral Gateways
AgentNPG

Provide configuration details

7. Click the **Save** button. Your system is now connected with Unified CCE. To complete the integration, you must configure your media classes. and import the MRDs users and skill groups from the Unified CCE system. For details about doing this task, see the *Enterprise Chat and Email Administrator's Guide to Administration Console.*

Configuring Important Settings

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

These settings are of two types:

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

Mandatory Settings

At the partition level

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

- Web server URL or Load Balancer URL

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

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

At the department level

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

- From email address for alarm

Optional Settings

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

At the partition level

- Customer departmentalization
- Session time out
- Inactive time out
- Exception email SMTP
- Exception mail redirection to address
- Exception mail redirection from address
- Autopushback time (minutes after logout)
- Chat auto-pushback settings

At the department level

- Business calendar time zone

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

Uninstalling ECE

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

- 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 60.

Stopping IIS

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

Uninstalling ECE

To uninstall in graphical mode:

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

Performing Post Uninstallation tasks

Starting IIS

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

5

Single Sign-On Configuration

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 68).
- **Split AD FS:** In a split AD FS deployment, Resource Federation Server and Account Federation Server are installed on separate machines (page 76).

Configuring Single AD FS Deployment

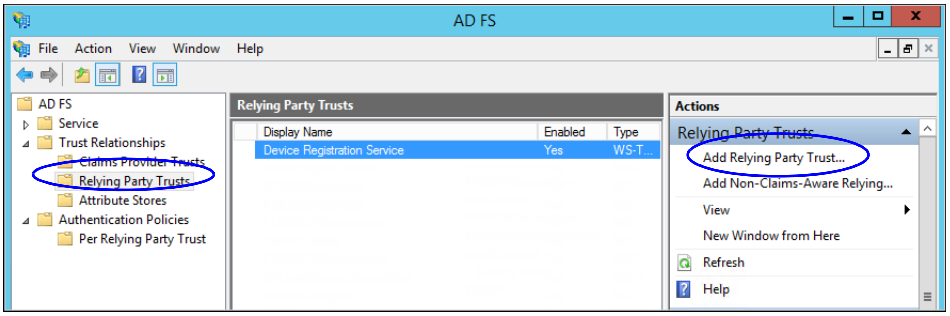
In a single AD FS deployment, Resource Federation Server and Account Federation Server are installed on the same machine.

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...**

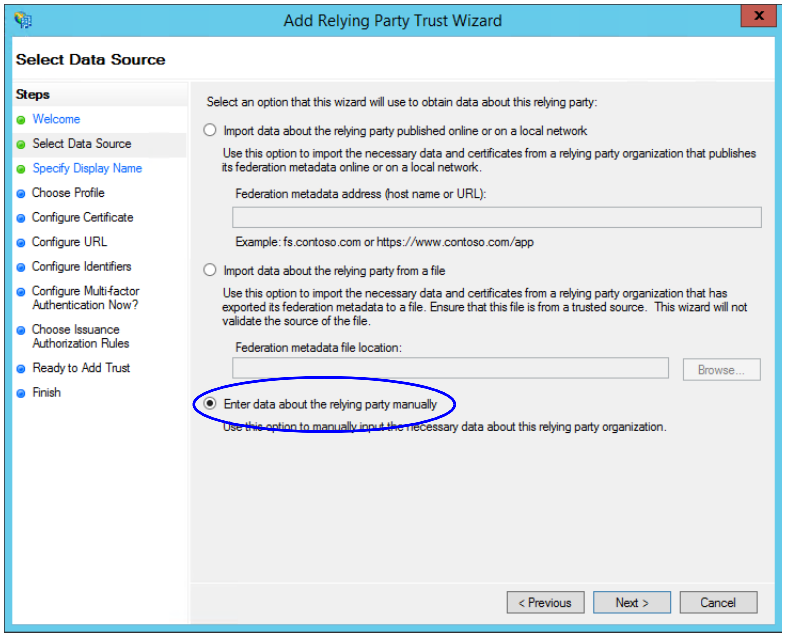


Display Name	Enabled	Type
Device Registration Service	Yes	WS-T...

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 an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

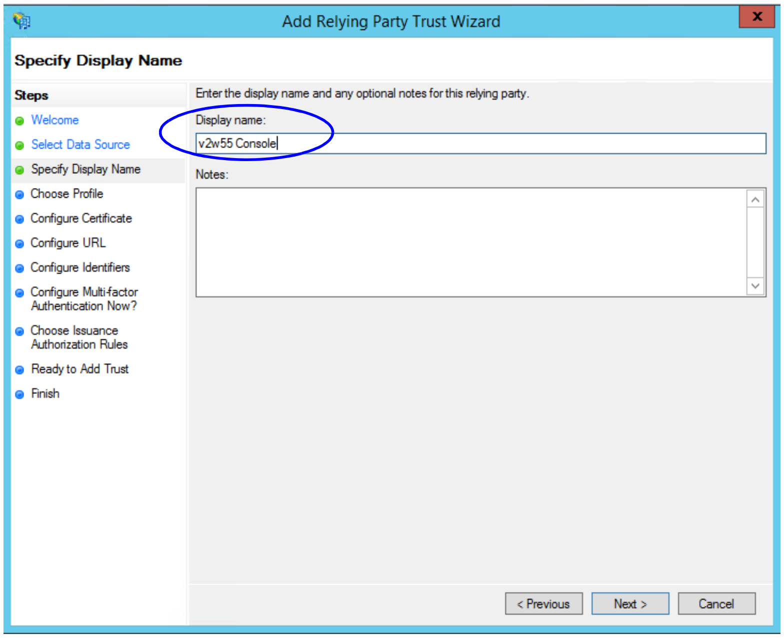
Federation metadata file location:

● Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

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**.



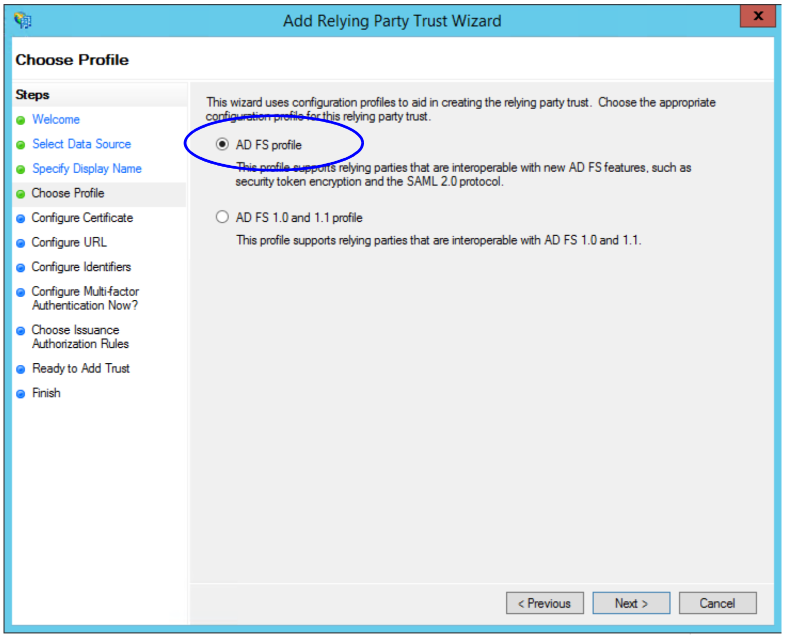
Enter the display name and any optional notes for this relying party.

Display name: v2w55 Console

Notes:

Provide a display name

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



Choose Profile

This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.

● AD FS profile

This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.

○ AD FS 1.0 and 1.1 profile

This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.

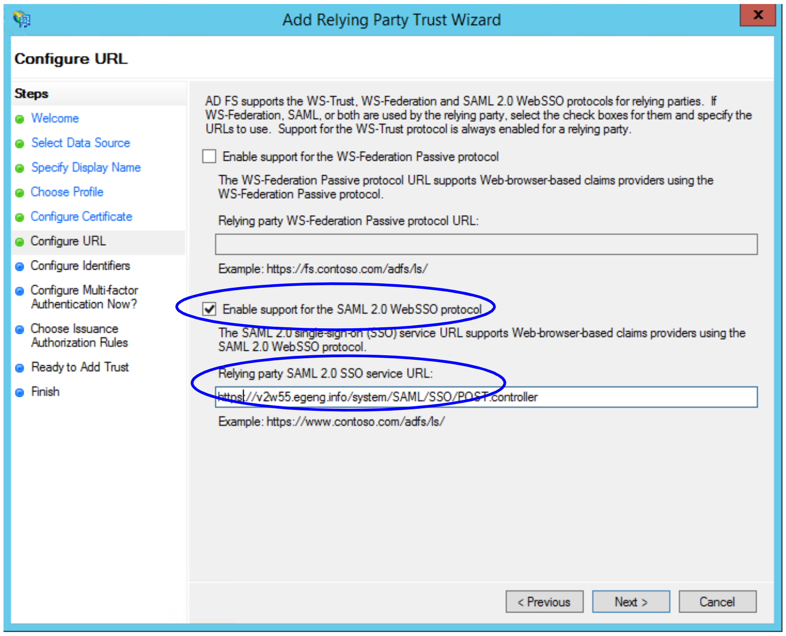
Select AD FS profile

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

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

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

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



Configure URL

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

□ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

☑ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

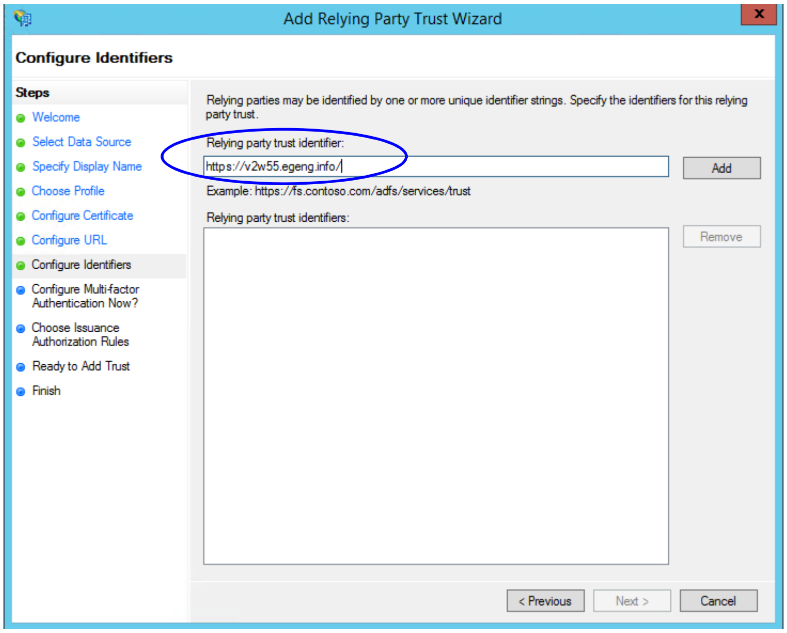
Relying party SAML 2.0 SSO service URL:

https://v2w55.egeng.info/system/SAML/SSO/POST.controller

Example: https://www.contoso.com/adfs/ls/

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.**



Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier: https://v2w55.egeng.info/

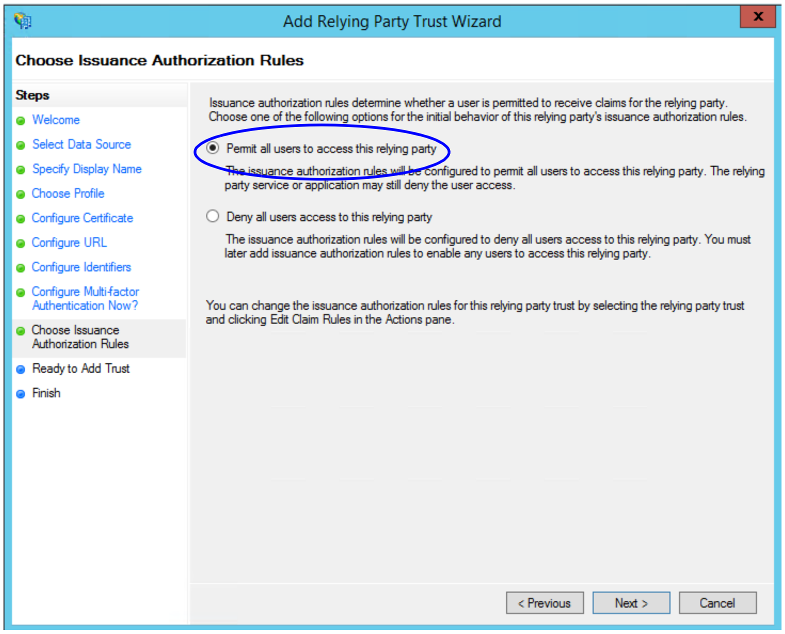
Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

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.



Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

● Permit all users to access this relying party

The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

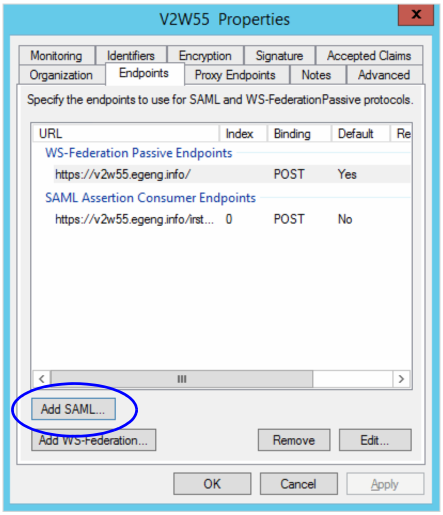
Select the Permit all users to access this relying party option

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.



Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default	Re
WS-Federation Passive Endpoints				
https://v2w55.egeng.info/		POST	Yes	
SAML Assertion Consumer Endpoints				
https://v2w55.egeng.info/irst...	0	POST	No	

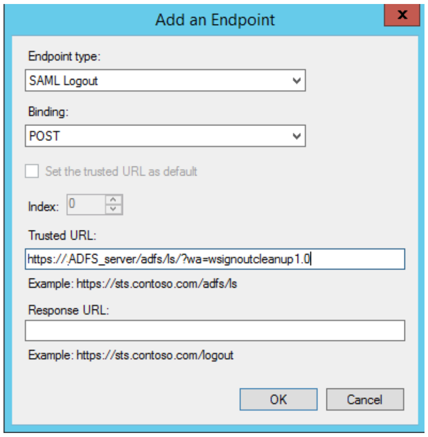
Click Add SAML

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.**



Endpoint type: SAML Logout

Binding: POST

☐ Set the trusted URL as default

Index: 0

Trusted URL: https://ADFS_server/adfs/ls/?wa=wsignoutcleanup1.0

Example: https://sts.contoso.com/adfs/ls

Response URL:

Example: https://sts.contoso.com/logout

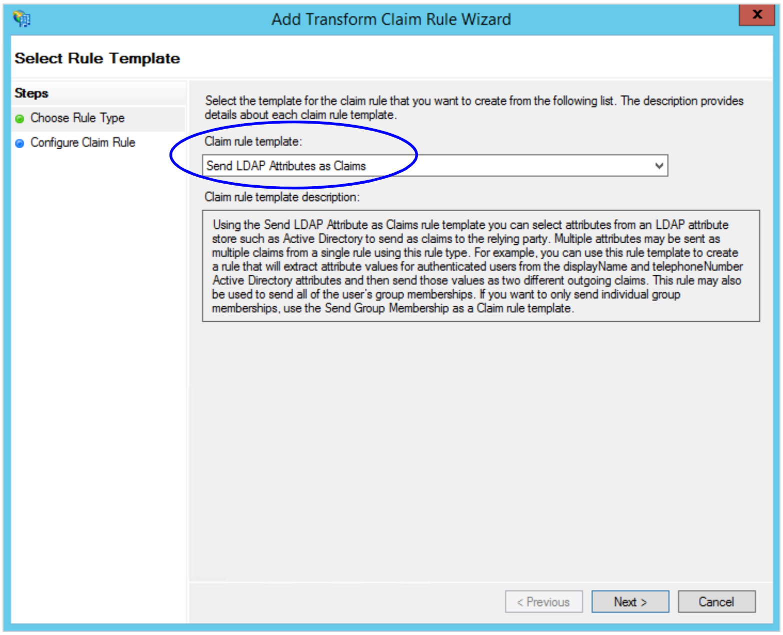
Create an end point

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 template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

Claim rule template description:

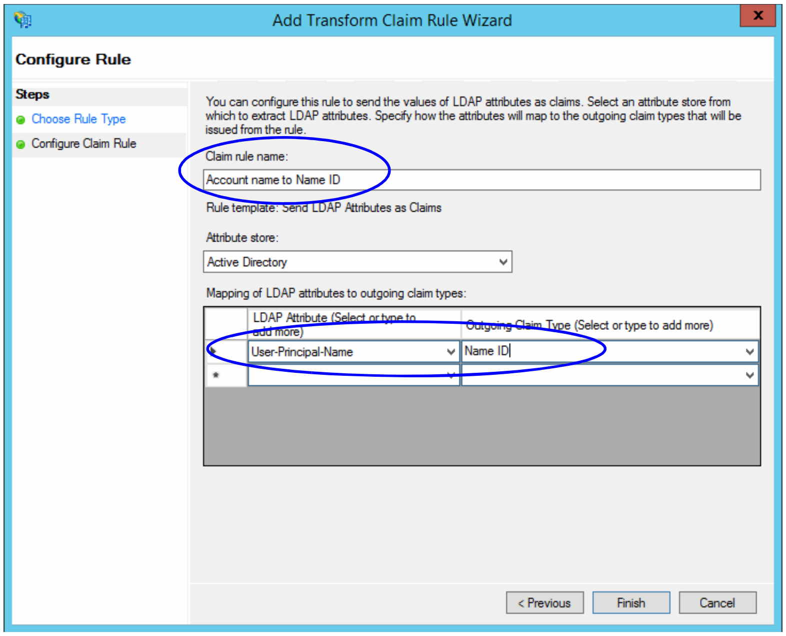
Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

Select the claim rule template

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

      i. Provide the Claim rule name.

      ii. Define mapping of LDAP attribute and the outgoing claim type. Select **Name ID** as the outgoing claim type name. Click **Finish** to go back to the Edit Claim Rules for single AD FS window.



Configure Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: Account name to Name ID

Rule template: Send LDAP Attributes as Claims

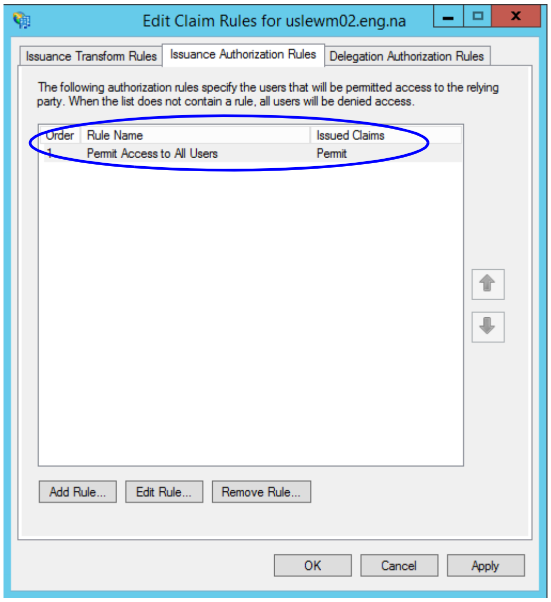
Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
User-Principal-Name	Name ID

Configure the rule

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

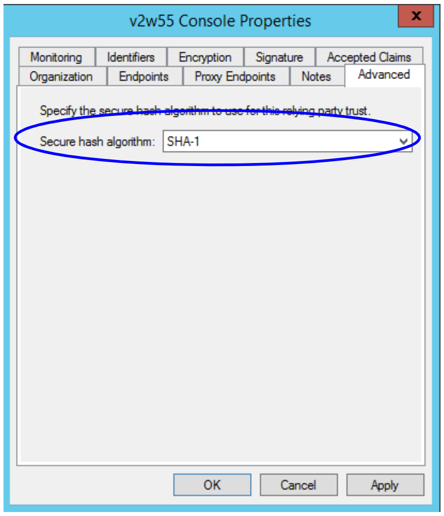

Edit Claim Rules for uslewm02.eng.na
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

The following authorization rules specify the users that will be permitted access to the relying party. When the list does not contain a rule, all users will be denied access.

Order	Rule Name	Issued Claims
1	Permit Access to All Users	Permit

Check the authorization rules

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

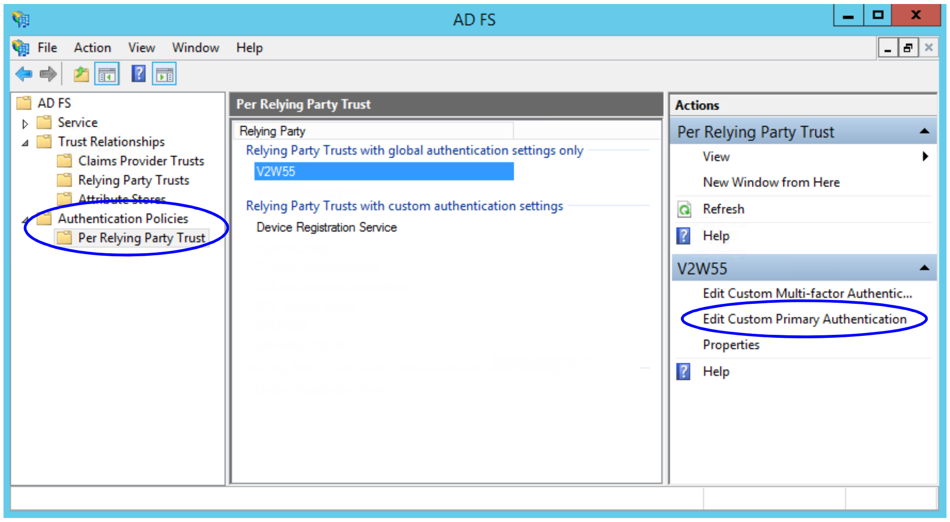


Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-1

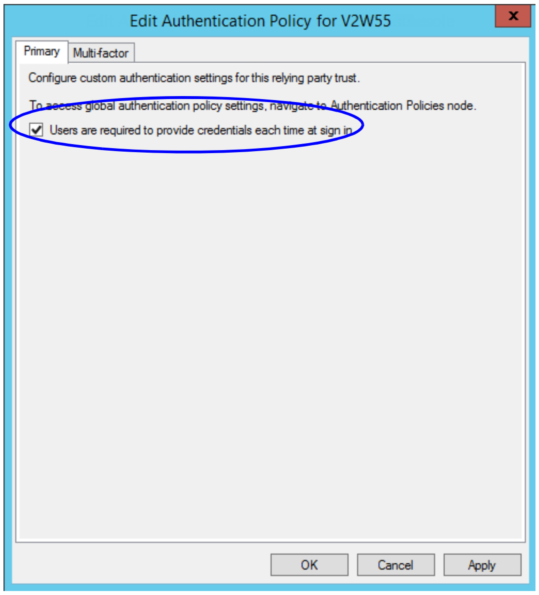
Set the secure hash algorithm

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



Change the authentication policy for ECE

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



Configure custom authentication settings for this relying party trust.

To access global authentication policy settings, navigate to Authentication Policies node.

☑ Users are required to provide credentials each time at sign in

Edit the authentication policy

Configuring Split AD FS Deployment

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

Configuring split AD FS includes:

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

Adding Security Certificates for the AD FS Domains

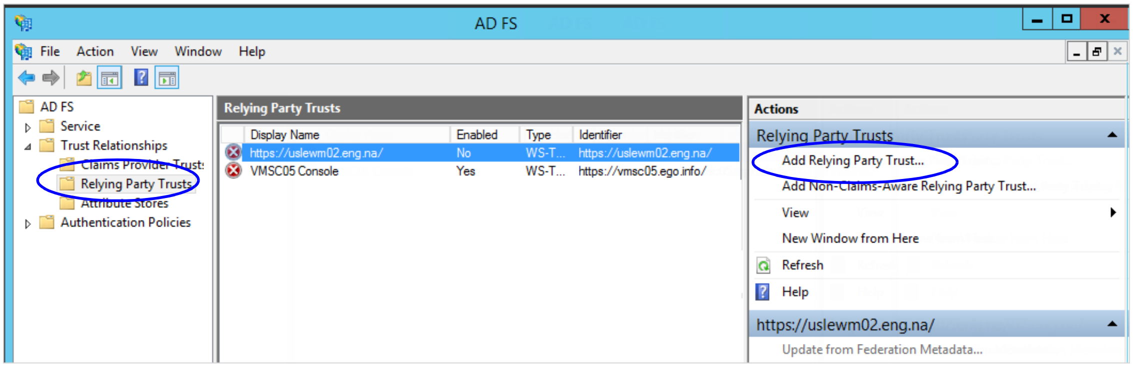
- If Customer AD FS and Shared AD FS are installed in different domain, you need to add certificates of the domains to the **Trusted Root Certification Authorities** store of the servers. On the Customer AD FS server, add the certificate of the Shared AD FS and vice versa. Contact your IT department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

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

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

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

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

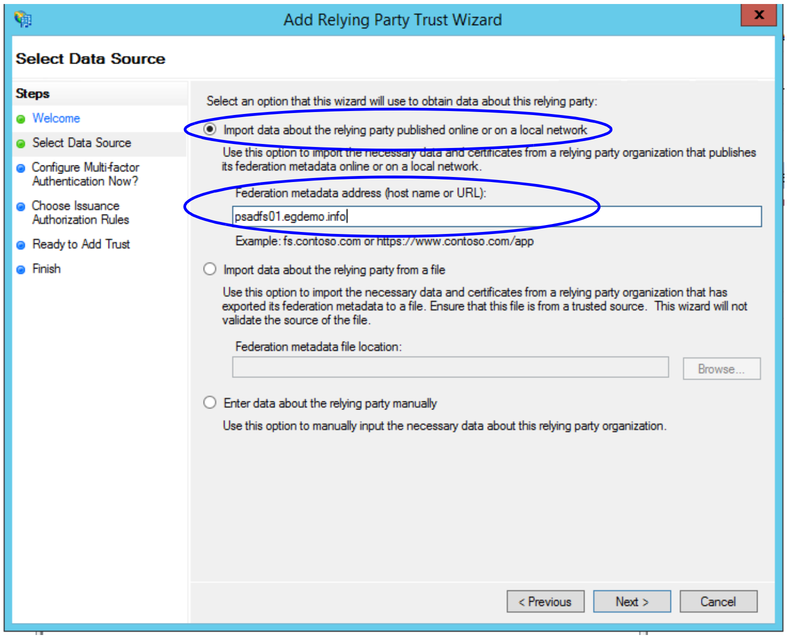


Relying Party Trusts

Display Name	Enabled	Type	Identifier
https://uslewm02.eng.na/	No	WS-T...	https://uslewm02.eng.na/
VMSC05 Console	Yes	WS-T...	https://vmsc05.ego.info/

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**.


Add Relying Party Trust Wizard
Select Data Source
Steps
Welcome
Select Data Source
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
Browse...
< Previous
Next >
Cancel

Select an option that this wizard will use to obtain data about this relying party:

● Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

psadfs01.egdemo.info

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

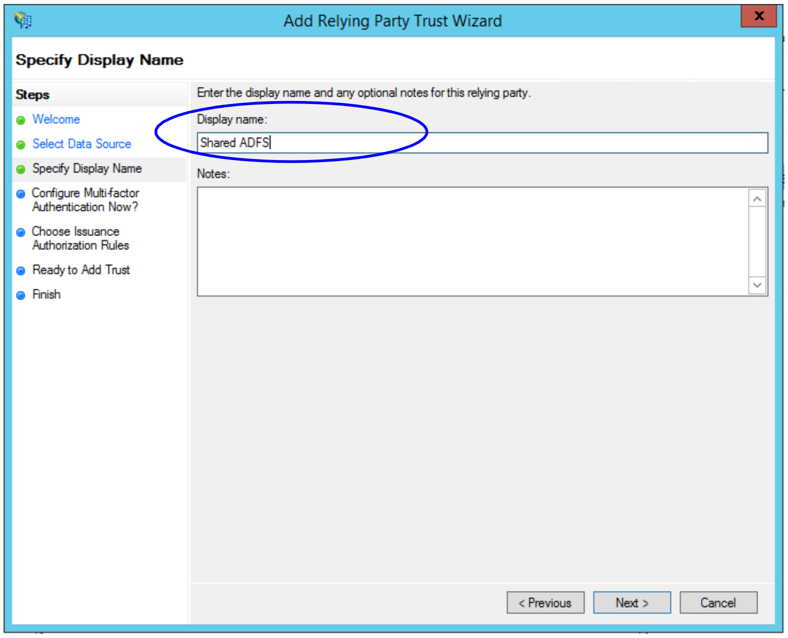
Federation metadata file location:

○ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

Select the data source options

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



Enter the display name and any optional notes for this relying party.

Display name: Shared ADFS

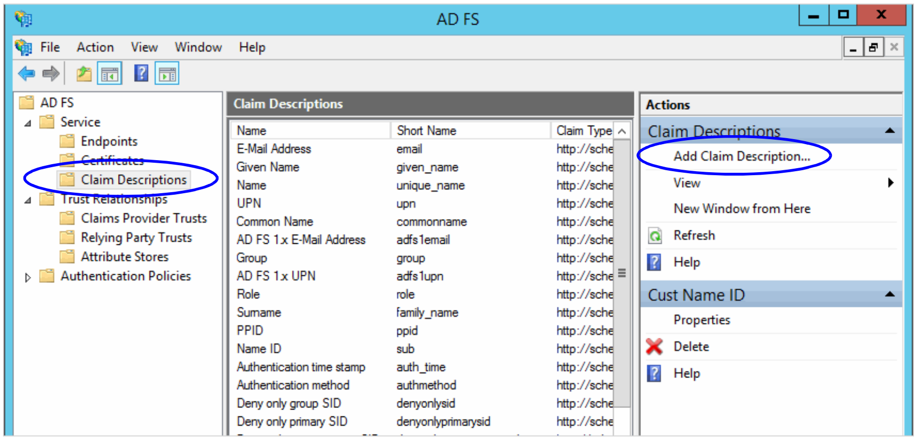
Notes:

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...**



Claim Descriptions

Name	Short Name	Claim Type
E-Mail Address	email	http://sche
Given Name	given_name	http://sche
Name	unique_name	http://sche
UPN	upn	http://sche
Common Name	commonname	http://sche
AD FS 1.x E-Mail Address	adfs1email	http://sche
Group	group	http://sche
AD FS 1.x UPN	adfs1upn	http://sche
Role	role	http://sche
Surname	family_name	http://sche
PPID	ppid	http://sche
Name ID	sub	http://sche
Authentication time stamp	auth_time	http://sche
Authentication method	authmethod	http://sche
Deny only group SID	denyonlysid	http://sche
Deny only primary SID	denyonlyprimarysid	http://sche

Click Add Claim Description

7. In the Add a Claim Description window, provide the following details:

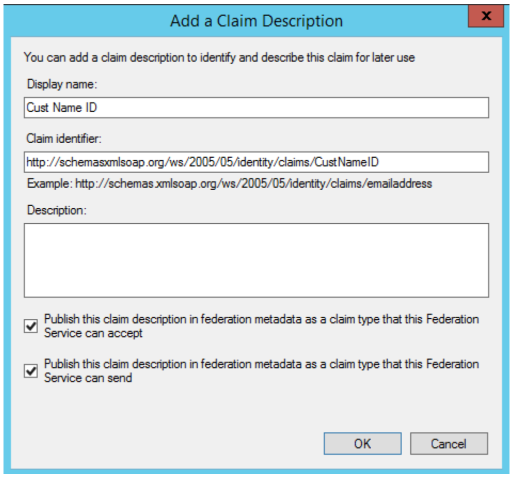
a. Set the **Display name** as **Cust Name ID**.

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.



You can add a claim description to identify and describe this claim for later use

Display name: Cust Name ID

Claim identifier: http://schemasxmlsoap.org/ws/2005/05/identity/claims/CustNameID

Example: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

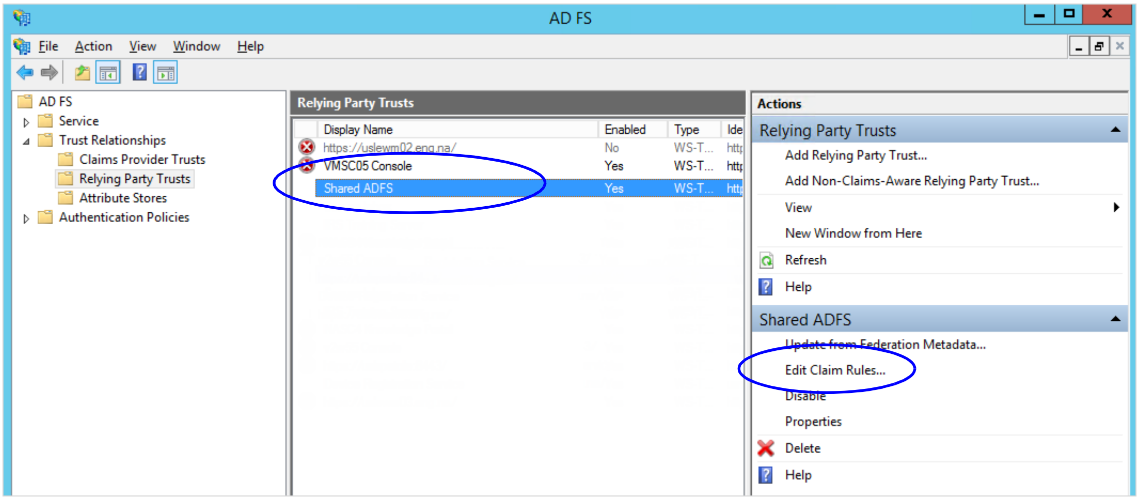
Description:

☑ Publish this claim description in federation metadata as a claim type that this Federation Service can accept

☑ Publish this claim description in federation metadata as a claim type that this Federation Service can send

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.**



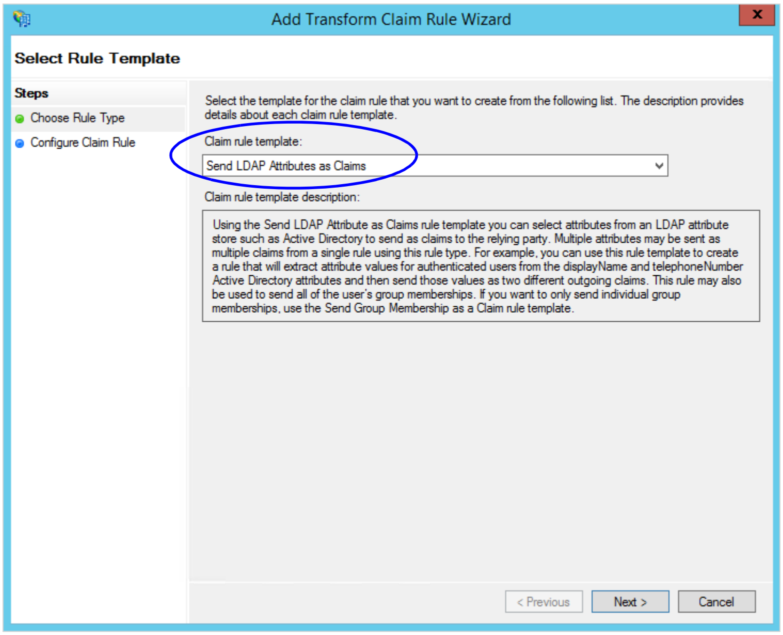
Display Name	Enabled	Type	Ide
https://uslewm02.eng.na/	No	WS-T...	http
VMSC05 Console	Yes	WS-T...	http
Shared ADFS	Yes	WS-T...	http

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**.



Add Transform Claim Rule Wizard

Select Rule Template

Steps
- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

Claim rule template description:

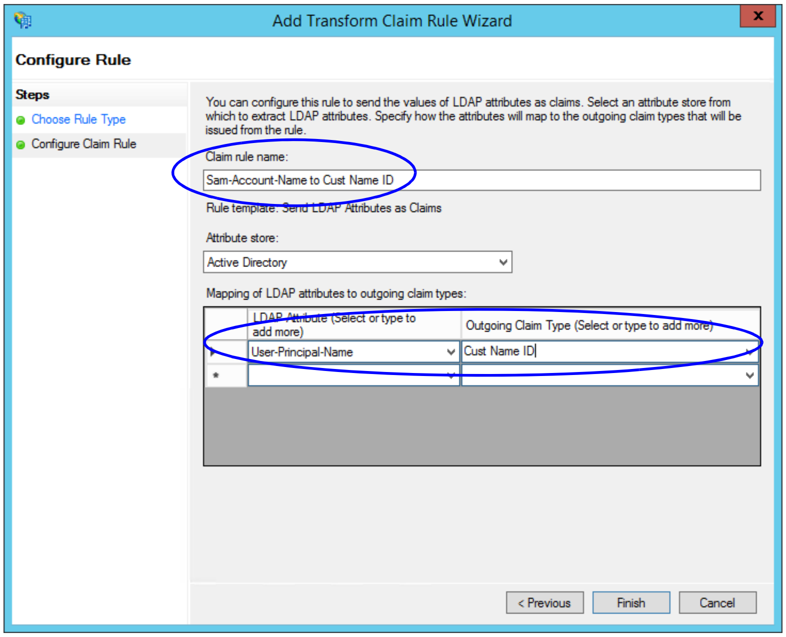
Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

Select the claim rule template

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

i. Provide a claim rule name.

ii. Define mapping of LDAP attribute and the outgoing claim type. The outgoing claim type name must be unique across all the claims defined in all relying party trusts created on this AD FS server. Click **Finish** to go back to the Edit Claim Rules for Shared AD FS window.



Add Transform Claim Rule Wizard

Configure Rule

Steps
- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: Sam-Account-Name to Cust Name ID

Rule template: Send LDAP Attributes as Claims

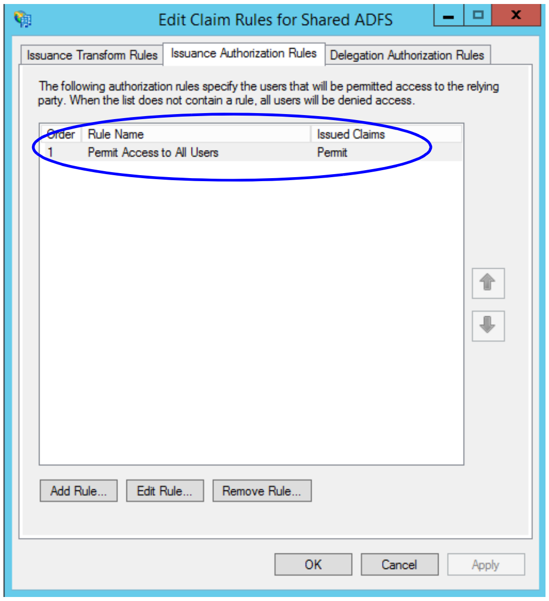
Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▸	User-Principal-Name	Cust Name ID
*		

Configure the claim rule

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


Edit Claim Rules for Shared ADFS
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules

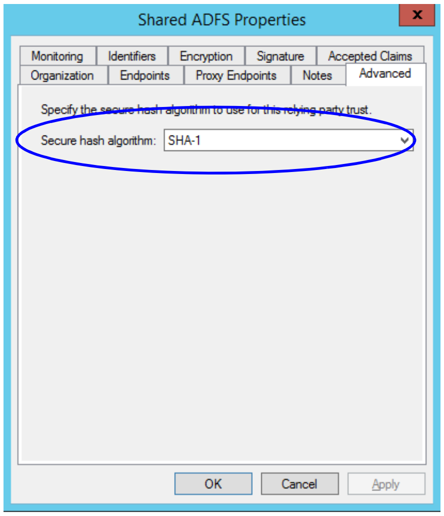
The following authorization rules specify the users that will be permitted access to the relying party. When the list does not contain a rule, all users will be denied access.

Order	Rule Name	Issued Claims
1	Permit Access to All Users	Permit

Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

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.



Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-1

Set the secure hash algorithm

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

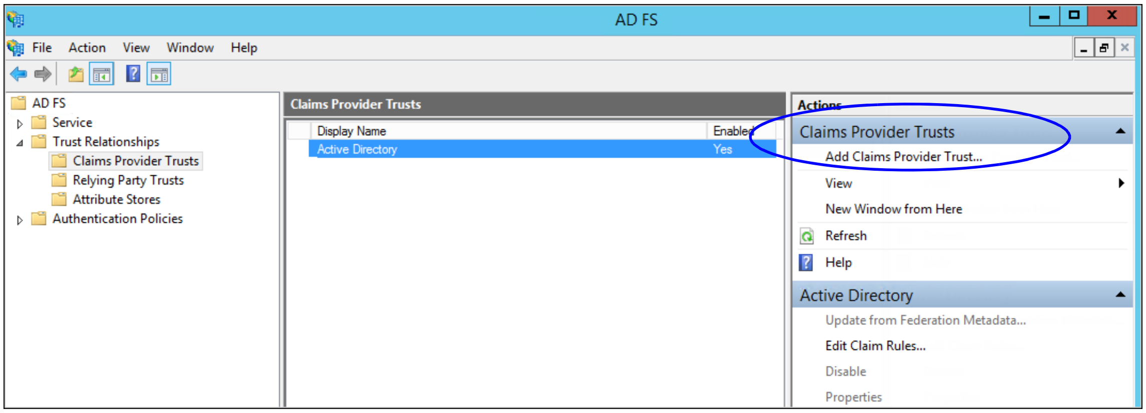
Perform these tasks on the server where shared AD FS is installed.

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

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

2. In the AD FS Management console, navigate to **AD FS > Trust Relationships > Claims Provider Trust**.

3. In the Actions section, go to Claim Provider Trusts, and click **Add Claims Provider Trust...**



Add claims provider trust

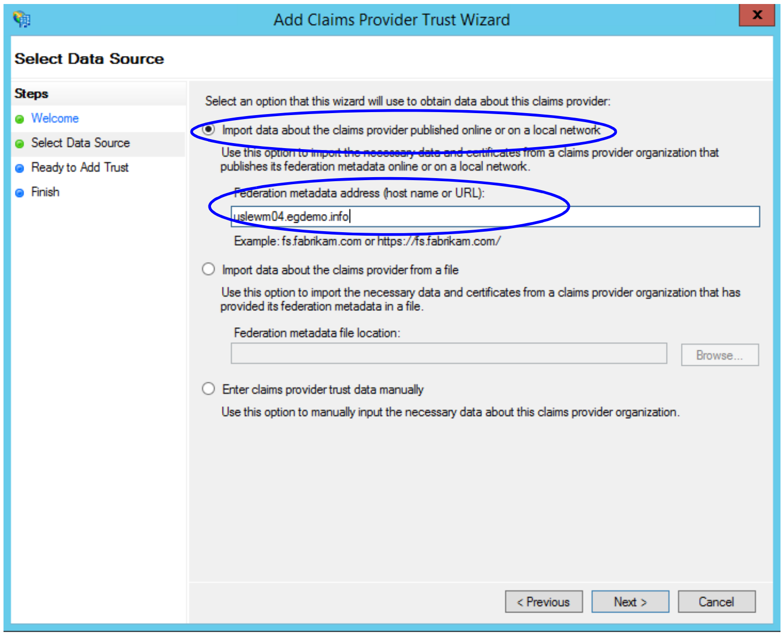
4. In the Add Claims Provider Trust Wizard that appears, do the following:

   a. On the Select Data Source screen, set the following options:

      i. Select the **Import data about the claims provider published on online or on a local network** option.

      ii. In the **Federation metadata address** field, provide the Customer AD FS server name.

      iii. Click **Next**.



Select an option that this wizard will use to obtain data about this claims provider:

● Import data about the claims provider published online or on a local network

Use this option to import the necessary data and certificates from a claims provider organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

uslewm04.egdemo.info

Example: fs.fabrikam.com or https://fs.fabrikam.com/

○ Import data about the claims provider from a file

Use this option to import the necessary data and certificates from a claims provider organization that has provided its federation metadata in a file.

Federation metadata file location:

○ Enter claims provider trust data manually

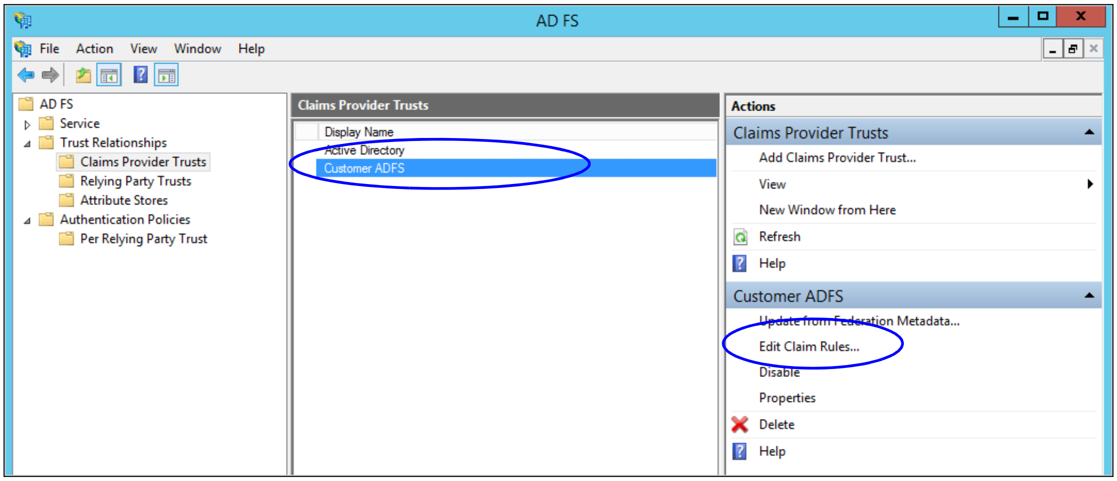
Use this option to manually input the necessary data about this claims provider organization.

Set the data source

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

   c. In the screens that follow, do not alter the default values. Continue to click the **Next** button in the wizard until a trust is created. At the end, an entry is created in the Claim Provider Trusts list.

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

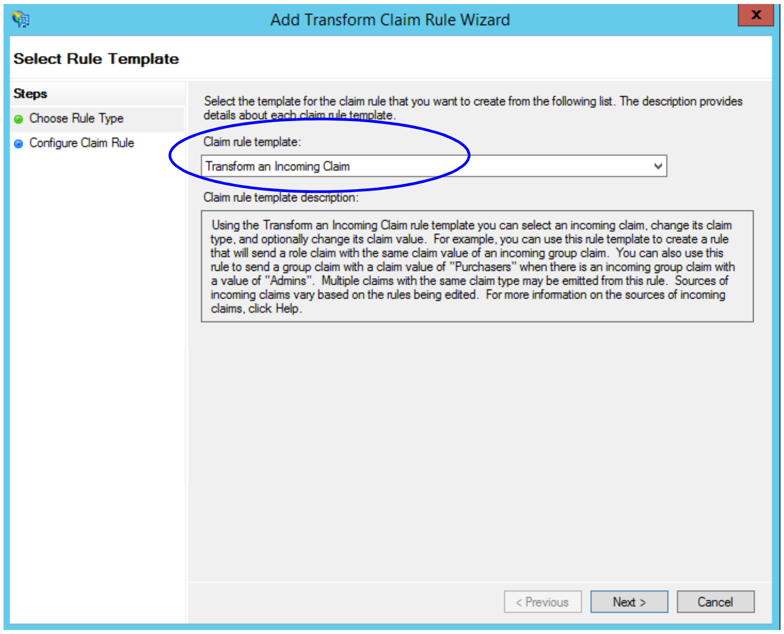


Edit the claim rules

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

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

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



Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Transform an Incoming Claim

Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help.

Choose the claim rule template

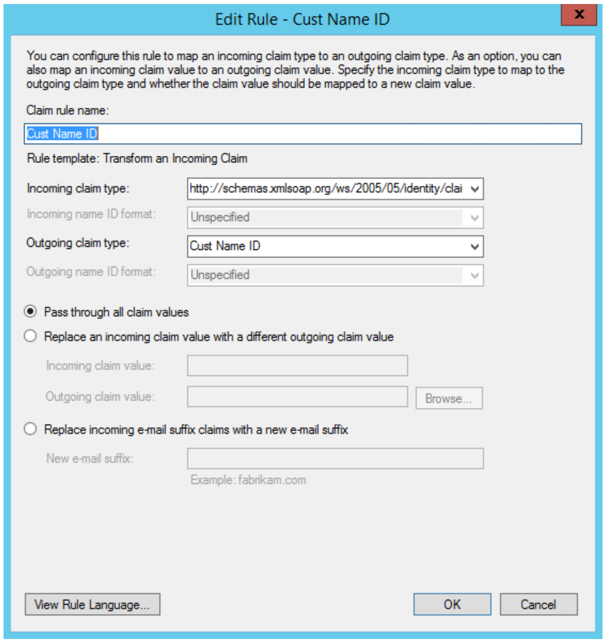
   b. On the Configure Claim Rule screen, set the following:

      i. Provide the claim rule name as **Cust Name ID.**

ii. In the **Incoming claim type** field provide the name as **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/CustNameID**. This is the same value as provided while creating the claim rule description (page 78).

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

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



Edit Rule - Cust Name ID

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name: Cust Name ID

Rule template: Transform an Incoming Claim

Incoming claim type: http://schemas.xmlsoap.org/ws/2005/05/identity/clai

Incoming name ID format: Unspecified

Outgoing claim type: Cust Name ID

Outgoing name ID format: Unspecified

● Pass through all claim values

○ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

○ Replace incoming e-mail suffix claims with a new e-mail suffix

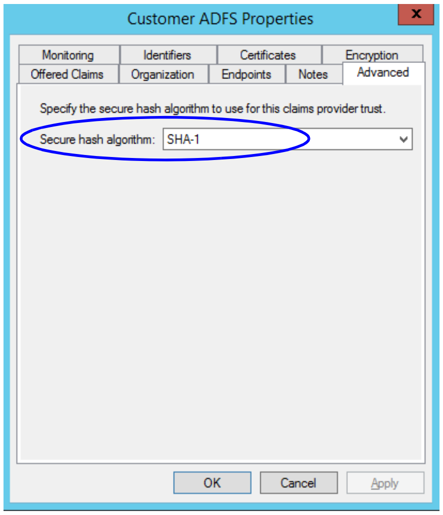
New e-mail suffix:

Example: fabrikam.com

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.



Customer ADFS Properties

Specify the secure hash algorithm to use for this claims provider trust.

Secure hash algorithm: SHA-1

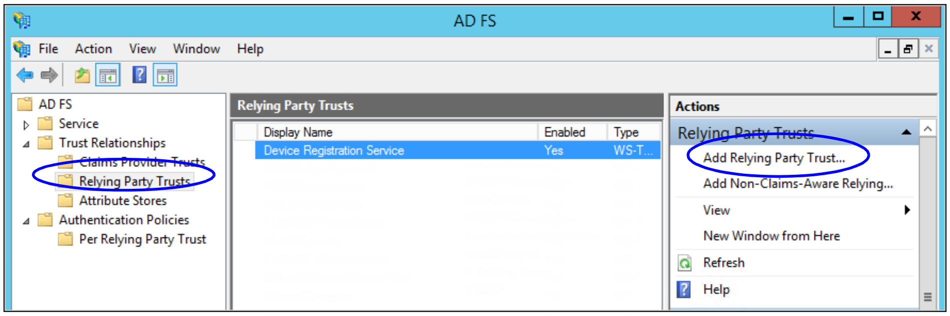
Set the secure hash algorithm

Configuring Relying Party Trust for ECE in Shared AD FS

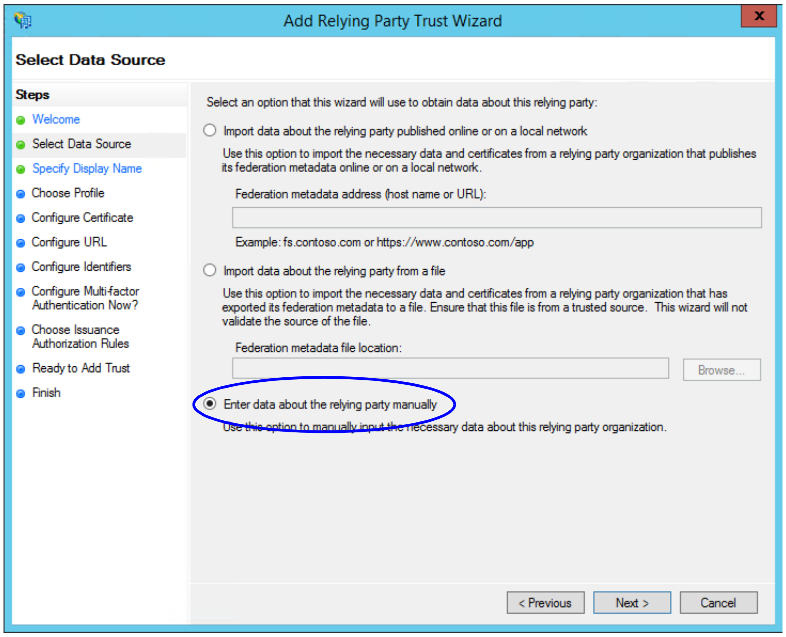
Perform these tasks on the server where shared AD FS is installed.

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 an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

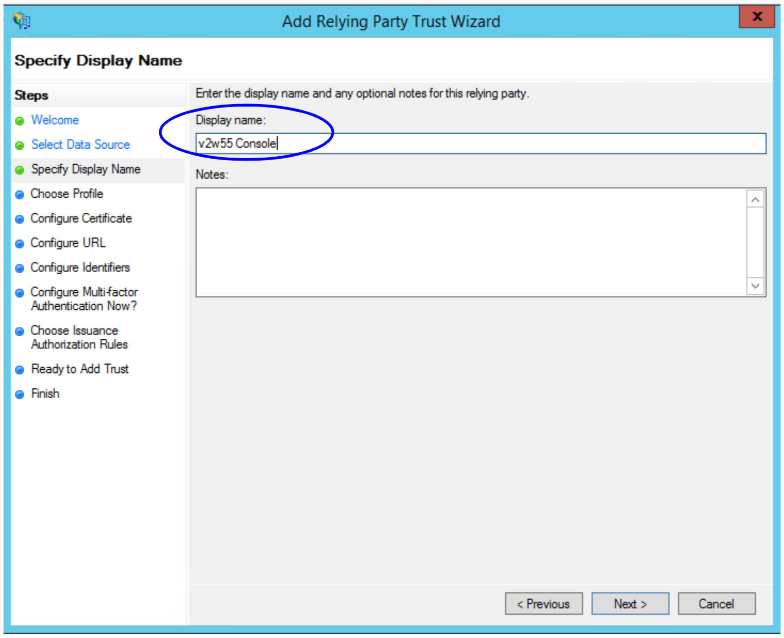
Federation metadata file location:

● Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

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**.



Add Relying Party Trust Wizard

Specify Display Name

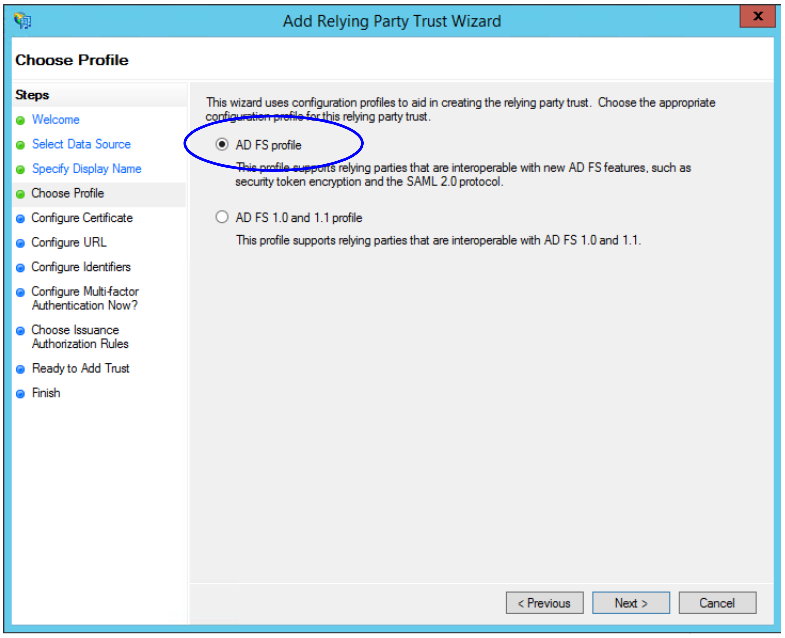
Enter the display name and any optional notes for this relying party.

Display name: v2w55 Console

Notes:

Provide a display name

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



Add Relying Party Trust Wizard

Choose Profile

This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.

● AD FS profile

This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.

○ AD FS 1.0 and 1.1 profile

This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.

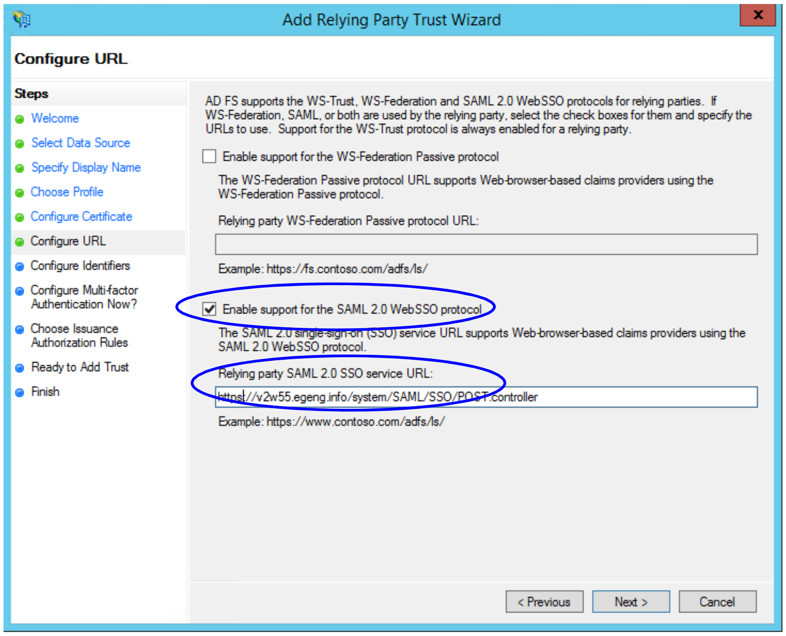
Select AD FS profile

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

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

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

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



AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

□ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

☑ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

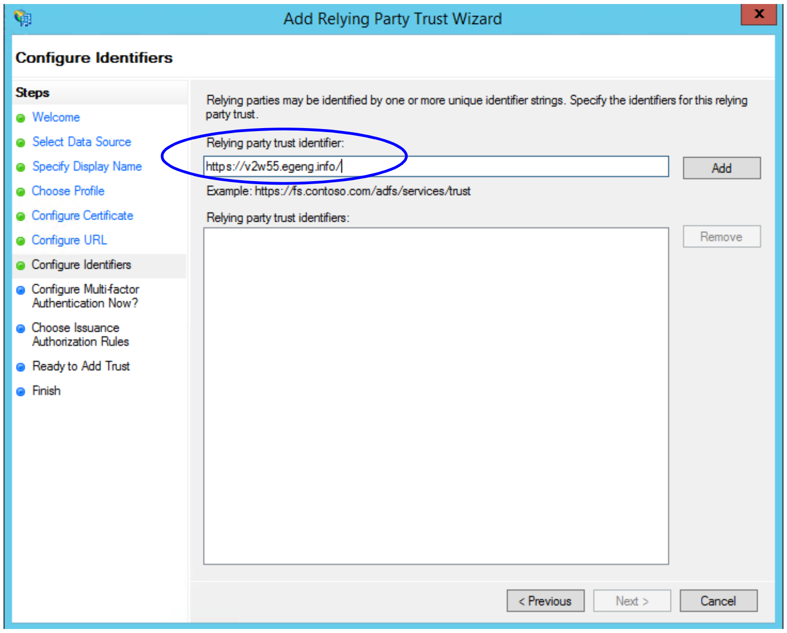
Relying party SAML 2.0 SSO service URL:

https://v2w55.egeng.info/system/SAML/SSO/POST.controller

Example: https://www.contoso.com/adfs/ls/

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.**



Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier:

https://v2w55.egeng.info/

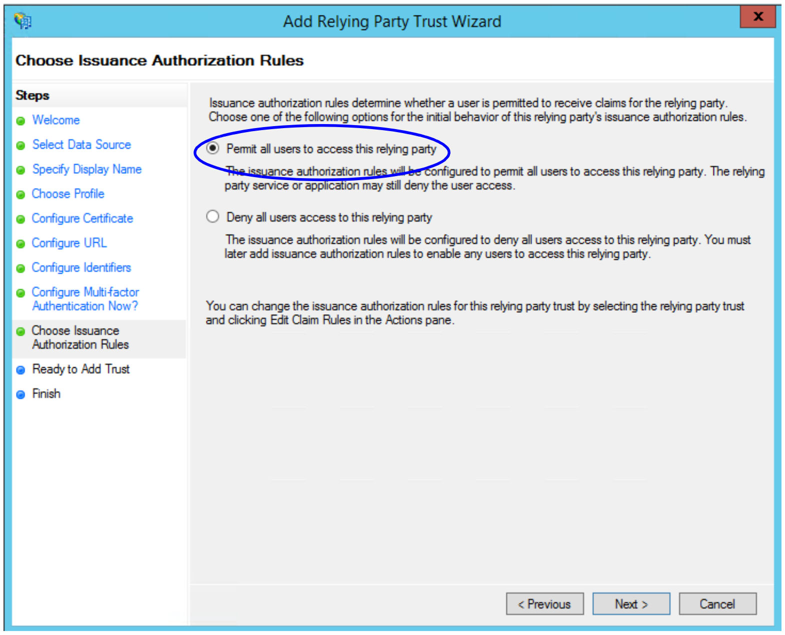
Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

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.



Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

● Permit all users to access this relying party

The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

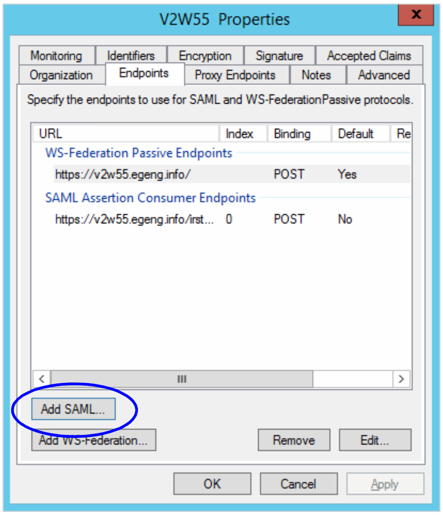
Select the Permit all users to access this relying party option

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.



Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default	Re
WS-Federation Passive Endpoints				
https://v2w55.egeng.info/		POST	Yes	
SAML Assertion Consumer Endpoints				
https://v2w55.egeng.info/irst...	0	POST	No	

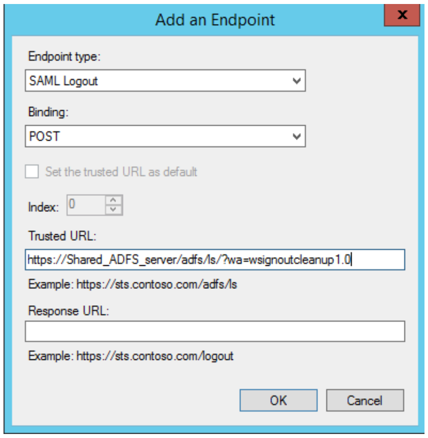
Click Add SAML

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

Endpoint type: SAML Logout

Binding: POST

□ Set the trusted URL as default

Index: 0

Trusted URL: https://Shared_ADFS_server/adfs/ls/?wa=wsignoutcleanup1.0

Example: https://sts.contoso.com/adfs/ls

Response URL:

Example: https://sts.contoso.com/logout

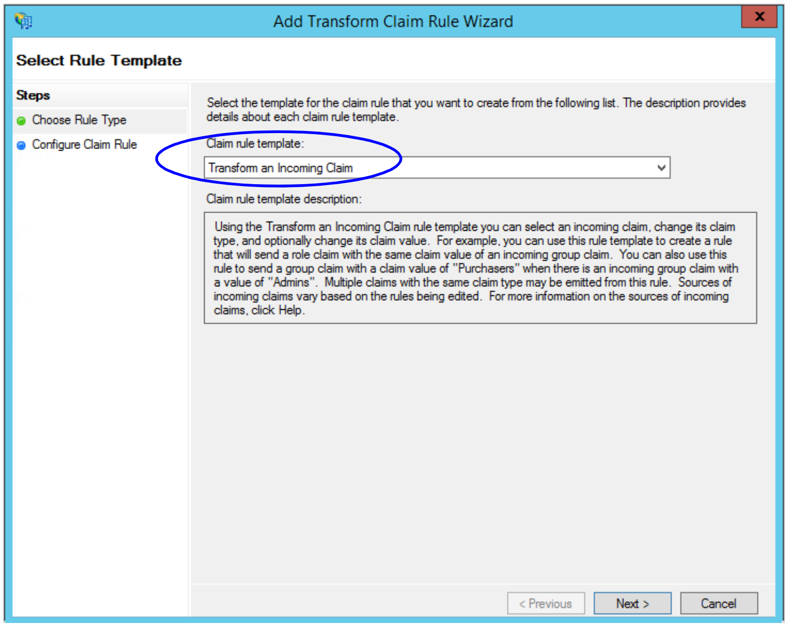
Create an end point

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 Rule Template

Steps
- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Transform an Incoming Claim

Claim rule template description:

Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help.

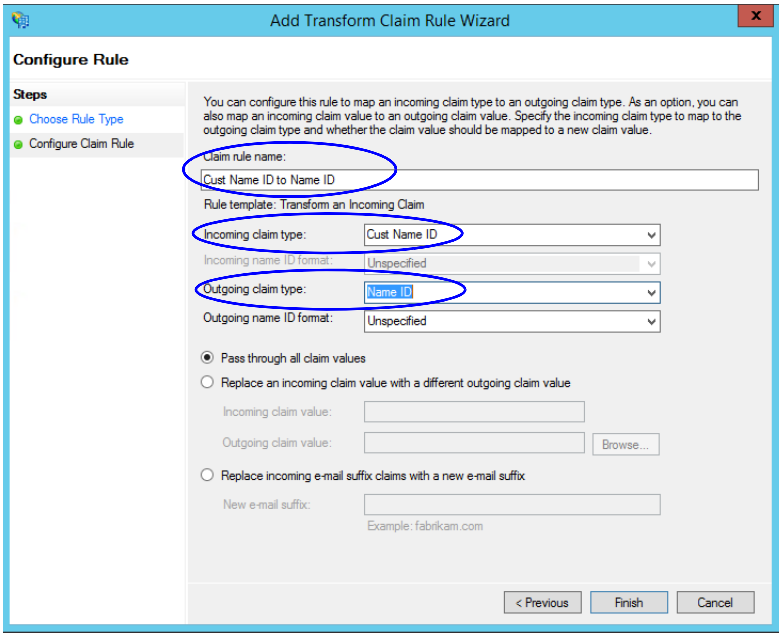
Select the claim rule template

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 80).

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



You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name: Cust Name ID to Name ID

Rule template: Transform an Incoming Claim

Incoming claim type: Cust Name ID

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Unspecified

● Pass through all claim values

○ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

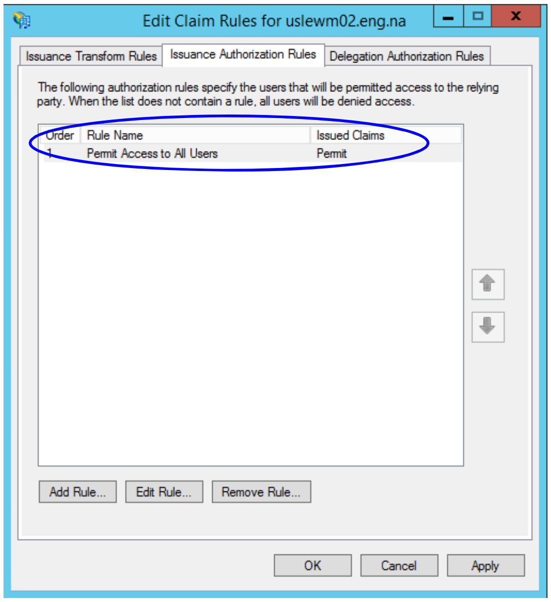
○ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

Configure the rule

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

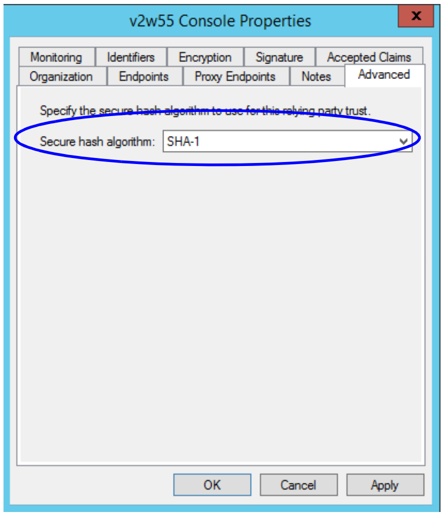

Edit Claim Rules for uslewm02.eng.na
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

The following authorization rules specify the users that will be permitted access to the relying party. When the list does not contain a rule, all users will be denied access.

Order	Rule Name	Issued Claims
1	Permit Access to All Users	Permit

Check the authorization rules

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

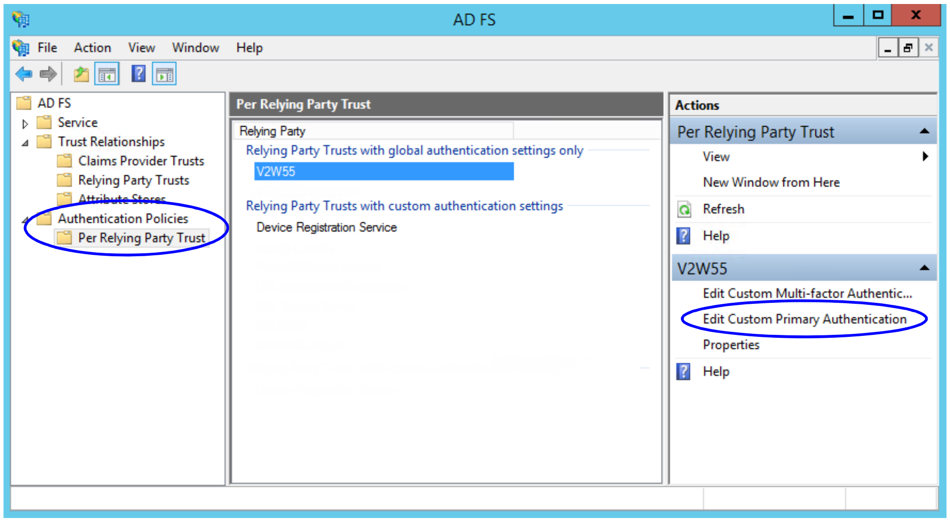


Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-1

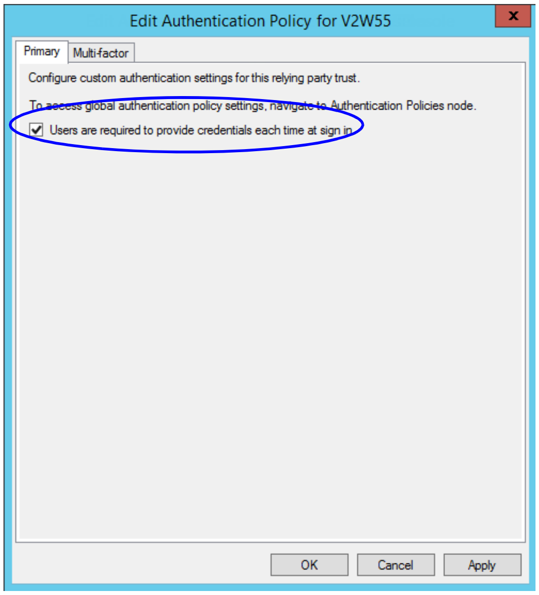
Set the secure hash algorithm

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



Change the authentication policy for ECE

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



Configure custom authentication settings for this relying party trust.

To access global authentication policy settings, navigate to Authentication Policies node.

☑ Users are required to provide credentials each time at sign in

Edit the authentication policy

Configuring Single Sign-On in ECE

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

6 SSL Configuration

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:

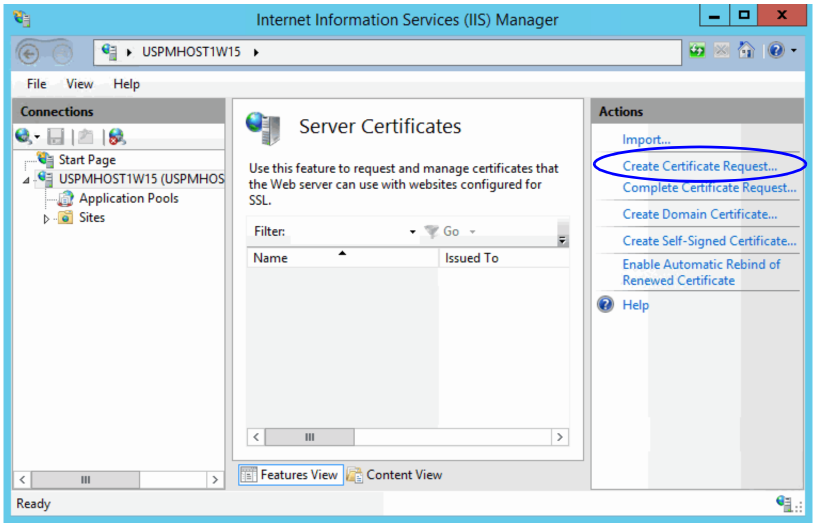
- Generating a Certificate Signing Request
- Submitting the Certificate Request
- Installing the Certificate on the Web Server

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.


Internet Information Services (IIS) Manager
USPMHOST1W15
File
View
Help
Connections
Start Page
USPMHOST1W15 (USPMHOS
Application Pools
Sites
Server Certificates
Filter:
Go
Name
Issued To
Features View
Content View
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Ready

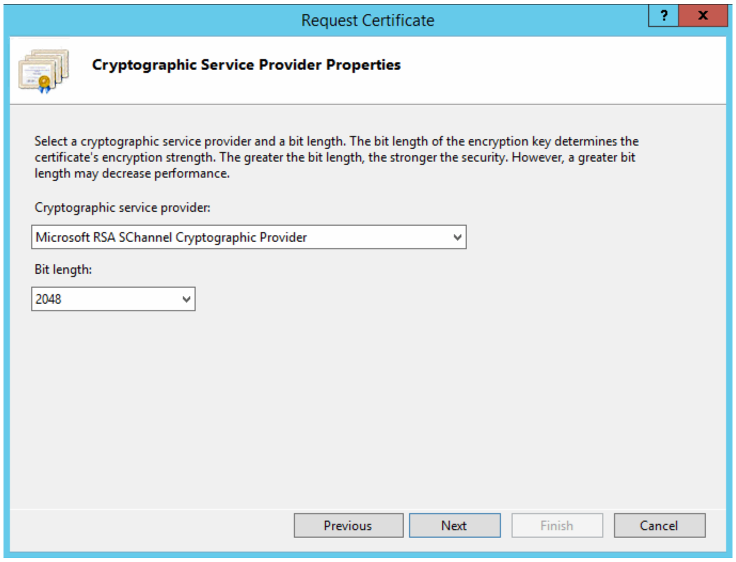
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

*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**.



Request Certificate

Cryptographic Service Provider Properties

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider:

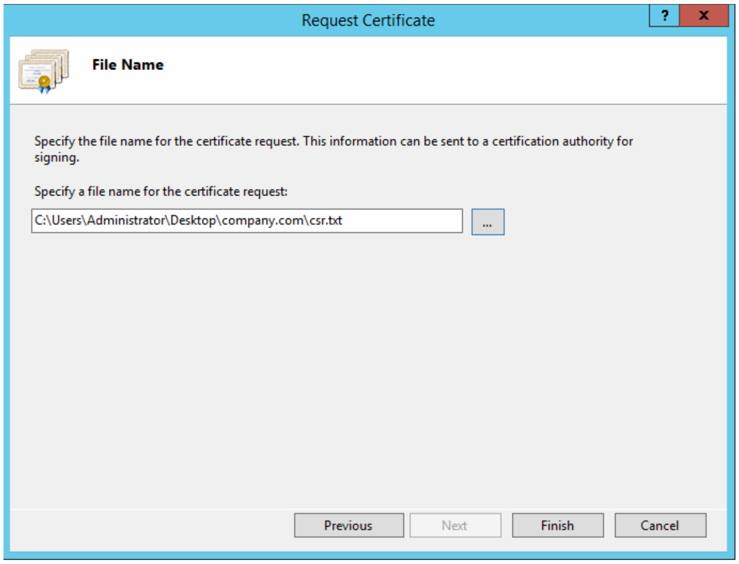
Microsoft RSA SChannel Cryptographic Provider

Bit length:

2048

Select a cryptographic service provider and bit length

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



Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request:

C:\Users\Administrator\Desktop\company.com\csr.txt

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 94).

  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.

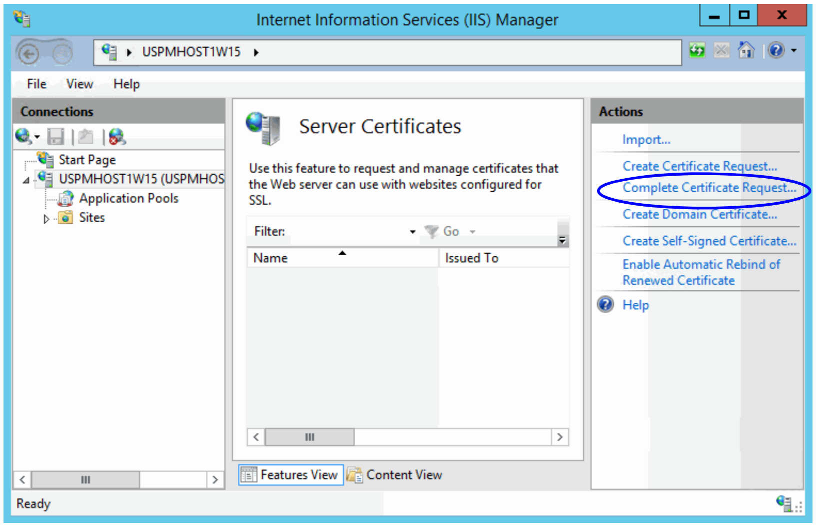
Important: **You need to install the certificate for the website that was specified when the web server component was installed.**

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.

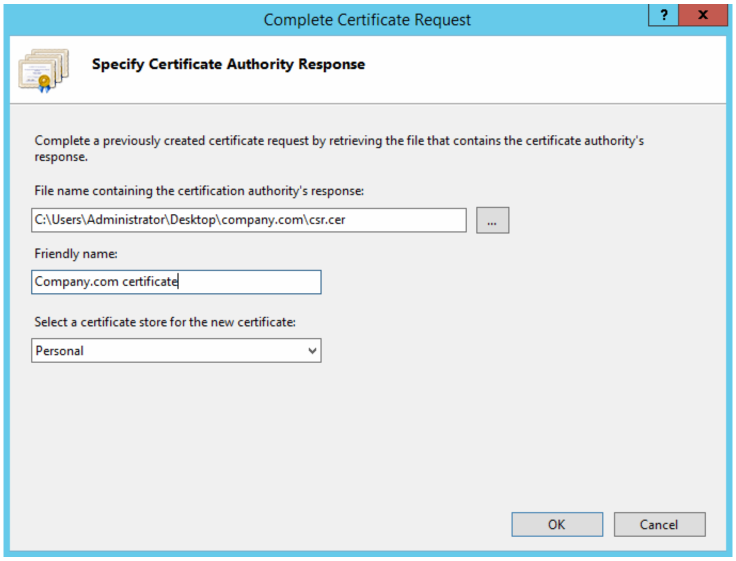


Internet Information Services (IIS) Manager
USPMHOST1W15
File View Help
Connections
Start Page
USPMHOST1W15 (USPMHOS
Application Pools
Sites
Server Certificates
Filter:
Go
Name
Issued To
Features View
Content View
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Ready

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

*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**.



Complete Certificate Request
Specify Certificate Authority Response
...
OK
Cancel

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:
C:\Users\Administrator\Desktop\company.com\csr.cer

Friendly name:
Company.com certificate

Select a certificate store for the new certificate:
Personal

Browse to the server certificate file

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

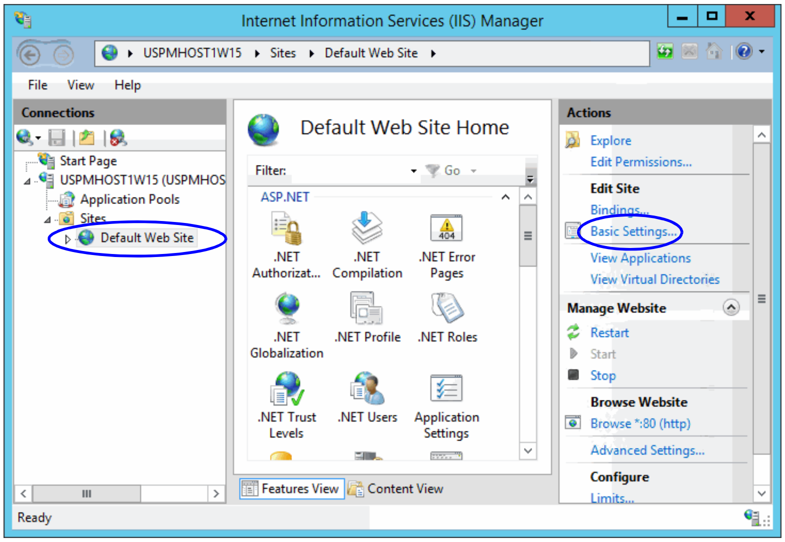
Binding the Certificate to the Application Website

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

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

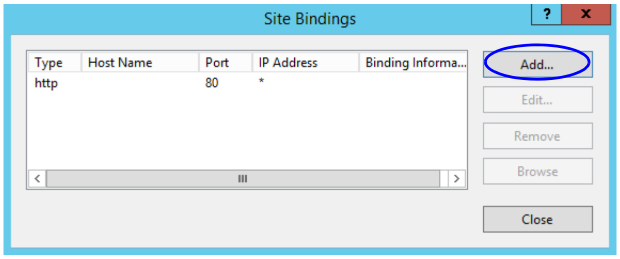
To bind the certificate to the application URL:

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



Select the Web_Site_Name.

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

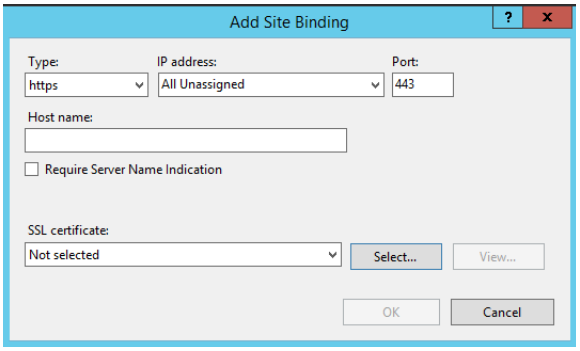


Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	

*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**.



Type: https

IP address: All Unassigned

Port: 443

Host name:

□ Require Server Name Indication

SSL certificate: Not selected

Select SSL certificate

6. The site binding for port 443 is displayed.
7. Restart the IIS Service. Make sure that both websites have started.

   Clients browsing to this virtual directory must now use HTTPS.

Testing SSL Access

To test SSL access to ECE:

1. Open your web browser.
2. Use HTTP in the URL for the application. For example, `http://`*Web_server_FQDN*/ *Partition_name*

   You should see a message asking you to view the page over a secure channel.
3. Now use HTTPS in the URL for the application. For example, `https://`*Web_Server_FQDN*/ *Partition_name.*
4. In the security message that appears, click the **View certificate** button.
5. After verifying the certificate information, click **OK**, then click **Yes** to proceed to the URL.

   The ECE login window appears.

Configuring SSL or TLS for Retriever and Dispatcher Services

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

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

To configure TLS and SSL, you must:

- ❍ Install the certificates on the services servers. (page 100)

a. Modify the alias configuration (page 101)

On the Services Server

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

Installing Certificates

To configure SSL or TLS on the services server:

1. Obtain the certificate for the SSL or TLS enabled mail server on which the email alias is configured. If your POP3, IMAP, SMTP, and ESMTP servers are installed on different machines, obtain the certificates for all the servers.

2. Copy the certificates to a location in *Cisco_Home*.

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

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

4. Execute the following command to install the certificate:

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

   where:

   CERTIFICATE_FILE_PATH is the complete path to the certificate that you copied in Step 2, including the name of the file.

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

   For example the command will look like:

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

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

6. Confirm the action when prompted.

7. To verify that the certificate is installed successfully, run the following command:

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

   where *Alias_Name* is the name you assigned to the certificate in Step 4.

   For example, the command will look like:

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

8. When prompted, provide the keystore password.

   The output will list the installed certificate.

Deleting Certificates

Certificates generally have an expiry date. When your certificate expires, you might need to delete the old certificates and install new ones. The following section describes the steps for deleting the certificates. After deleting the certificates, repeat the steps in "Installing Certificates" on page 100 to install new certificates.

To delete a certificate:

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

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

2. Execute the following command to delete the certificate:

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

   where:

   Alias_Name is the name you assigned to the certificate in Step 4.

   For example the command will look like:

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

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

In the Administration Console

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

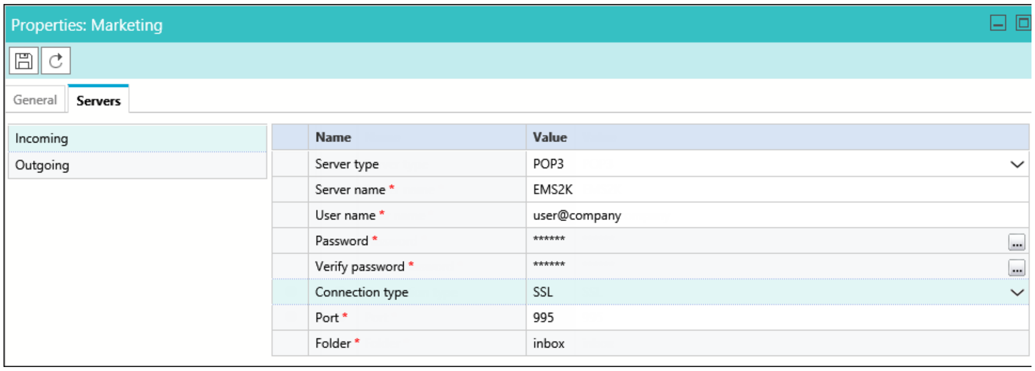
To enable SSL for specific aliases:

1. Log into the application as an administrator who can modify the email alias configuration and go to the Administration Console.

2. In the Tree pane, browse to **Administration** > **Departments** > *Department_Name* > **Email** > **Aliases.**

3. In the List pane, select the appropriate email alias.

4. In the Properties pane, go to the Servers tab and edit the following fields.
   - **Connection type**: Set this to **SSL** or **TLS**.
   - **Port**: Enter the secure port number.



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

Configure the alias properties

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