Cisco Unified Web and E-Mail Interaction Manager Installation Guide

For Unified Contact Center Enterprise

Release 11.0(1)
August 2015

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided "as is" with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice.

In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to http://www.cisco.com/go/trademarks

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, IQ Expertise, the IQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Network Registrar, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Cisco Unified Web and E-Mail Interaction Manager Installation Guide: For Unified Contact Center Enterprise. October 5, 2017

Copyright © 2006–2015, Cisco Systems, Inc. All rights reserved.
# Contents

**Preface** .................................................................................................................................................7

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

**Chapter 1: Planning** ..........................................................................................................................11

- Identifying Components .................................................................................................................. 12
  - File Server ................................................................................................................................... 12
  - Database Server .......................................................................................................................... 12
  - Messaging Server ....................................................................................................................... 13
  - Application Servers ..................................................................................................................... 13
  - Web Servers ............................................................................................................................... 14
  - Services Server ........................................................................................................................... 14
    - Distributed Services Manager (DSM) ..................................................................................... 14
    - RMI Registry and RMID .......................................................................................................... 14
  - Understanding Deployment Models ............................................................................................ 14
    - Single-Server Deployment for Unified EIM ............................................................................ 15
    - Collocated Deployment for Unified WIM .............................................................................. 15
    - Distributed-Server Deployment ............................................................................................. 16
      - Distributed Configuration With Web Server Outside a Firewall .................................. 16
      - Complex Distributed Configuration With Components on Different Machines ........ 16
  - Planning Components for Specific Configurations ........................................................................ 17
    - Planning the Database Server ................................................................................................ 17
      - Installing the Application on a SQL Server 2012 Cluster .............................................. 17
    - Planning Database Server Distribution ............................................................................. 17
    - Choosing Authentication Method for Database Connectivity ...................................... 17
    - Planning Application and Web Servers ............................................................................... 18
    - Planning the Messaging Server ............................................................................................. 18
  - Installing Unified EIM & WIM ..................................................................................................... 18
## Chapter 2: Pre-Installation Tasks

- Disabling Loopback Adapter Configuration ........................................ 20
- Verifying Network Configuration ..................................................... 20
- Configuring Port Number Between Components ............................. 21
- Setting Up User Accounts and Permissions .............................. 23
  - Setting Up Domain Account ....................................................... 24
  - Configuring Permissions on Active Directory Server ............... 24
- Preparing Database Server Machines ............................................. 26
  - Creating SQL User for Installing Unified EIM & WIM Databases .......... 26
  - Verifying Collation Settings ................................................... 26
  - Configuring Database Servers .................................................. 27
  - Configuring Microsoft DTC Settings ......................................... 27
  - Running SQL Server Services .................................................. 29
- Preparing the Messaging Server Machine ...................................... 30
  - Installing JBoss ........................................................................ 30
  - Installing JDK ........................................................................ 32
- Preparing Application Server Machines ......................................... 32
  - Installing JBoss ........................................................................ 32
  - Installing JDK ........................................................................ 32
- Preparing Services Server Machines ............................................ 32
  - Installing JDK ........................................................................ 32
- Preparing Web Server Machines .................................................. 32
  - Configuring Roles and Features ................................................. 32
  - Configuring Permissions on IIS Config Folder ......................... 34
  - Running the World Wide Web Publishing Service ................. 34
- Acquiring Licenses ....................................................................... 34
- Verifying Unified CCE Configuration .......................................... 34

## Chapter 3: Installation Process

- Installation Overview .................................................................. 37
- Installing Unified EIM & WIM ....................................................... 38
- Installation Details .................................................................... 40
  - File Server Details ................................................................. 40
  - Database Server Details ......................................................... 41
Chapter 6: SSL Configuration ................................................................. 73

Installing a Security Certificate ......................................................... 74
  Generating a Certificate Signing Request .................................. 74
  Submitting the Certificate Request .............................................. 76
  Installing the Certificate on the Web Server ................................ 76

Binding the Certificate to the Application Website ............................ 78

Testing SSL Access ............................................................................. 79

Configuring SSL or TLS for Retriever and Dispatcher Services .......... 79
  On the Services Server .................................................................. 80
    Installing Certificates ............................................................... 80
    Deleting Certificates ............................................................... 81
  In the Administration Console ................................................... 81
Preface

- Audience
- Obtaining Documentation and Submitting a Service Request
- Documentation Feedback
- Field Alerts and Field Notices
- Document Conventions
- Other Learning Resources
Welcome to Cisco® Unified EIM & WIM™, multichannel interaction software used by businesses all over the world to build and sustain customer relationships. A unified suite of the industry’s best applications for web and email interaction management, it is the backbone of many innovative contact center and customer service helpdesk organizations.

Cisco Unified EIM & WIM includes a common platform and one or both of the following applications:

- Cisco Unified Web Interaction Manager (Unified WIM)
- Cisco Unified E-Mail Interaction Manager (Unified EIM)

### Audience

*Cisco Unified Web and E-Mail Interaction Manager Installation Guide* is intended for installation engineers, system administrators, database administrators, and others who are responsible for installing and maintaining Unified EIM & WIM 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


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.

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

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.

<table>
<thead>
<tr>
<th>Use</th>
<th>To view</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Help button]</td>
<td>Topics in Cisco Unified Web and E-Mail Interaction Manager Help; the Help button appears in the console toolbar on every screen.</td>
</tr>
<tr>
<td>F1 keypad button</td>
<td>Context-sensitive information about the item selected on the screen.</td>
</tr>
</tbody>
</table>

Online help options
Document Set

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

- All Unified EIM documentation can be found online at http://www.cisco.com/en/US/products/ps7236/tsd_products_support_series_home.html
- All Unified WIM documentation can be found online at http://www.cisco.com/en/US/products/ps7233/tsd_products_support_series_home.html
- In particular, Release Notes for these products can be found at http://www.cisco.com/en/US/products/ps7236/prod_release_notes_list.html
- 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 document set contains the following guides:

- **Hardware and System Software Specification for Cisco Unified Web and E-Mail Interaction Manager**
- **Cisco Unified Web and E-Mail Interaction Manager Installation Guide**
- **Cisco Unified Web and E-Mail Interaction Manager Browser Settings Guide**

**User guides for agents and supervisors**

- **Cisco Unified Web and E-Mail Interaction Manager Agent’s Guide**
- **Cisco Unified Web and E-Mail Interaction Manager Supervisor’s Guide**

**User guides for Knowledge Base managers and authors**

- **Cisco Unified Web and E-Mail Interaction Manager Knowledge Base Author’s Guide**

**User guides for administrators**

- **Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Administration Console**
- **Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Routing and Workflows**
- **Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Chat and Collaboration Resources**
- **Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to Email Resources**
- **Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Data Adapters**
- **Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Offers Console**
- **Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Reports Console**
- **Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to System Console**
- **Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Tools Console**
Planning

- Identifying Components
- Understanding Deployment Models
- Planning Components for Specific Configurations
- Installing Unified EIM & WIM
Unified EIM & WIM can be installed in multiple configurations, ranging from a simple single-server installation, to many flavors of distributed installations. This chapter lists the components that make up a Unified EIM & WIM deployment and available configuration options. It also helps you plan your installation.

**Identifying Components**

All Unified EIM & WIM installations have the following six components:

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

**File Server**

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**

All Unified EIM & WIM 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.

MSSQL Server clustering can be used to achieve failover for the databases.
Messaging Server

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

For example,

- The agent assignment service publishes a message to the application server notifying it that a particular agent who is logged into that server has been assigned a new chat.
- 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.

<table>
<thead>
<tr>
<th>Component</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chat</td>
<td>- The Agent Assignment Service (AAS) notifies the application server when a new chat has been assigned to an agent.</td>
</tr>
<tr>
<td></td>
<td>- The application server notifies all other application servers in the configuration when an agent or a customer sends a chat message, is typing a chat message, or leaves the chat session.</td>
</tr>
<tr>
<td></td>
<td>- The application server notifies the AAS when the chat queue, list of users working on the chat queue, routing method, or chat entry point is modified.</td>
</tr>
<tr>
<td>Knowledge Base</td>
<td>The application server publishes a message to the KB Import Service when an External Attachment is added to a KB article.</td>
</tr>
<tr>
<td>Email Workflow</td>
<td>- The Workflow Assignment Service publishes a message to application servers when a new email is assigned to a user.</td>
</tr>
<tr>
<td></td>
<td>- The application server publishes a message to Workflow Cache Service when any workflow is created or modified from the Administration Console. The Workflow Cache Service publishes a message to the Workflow Service after it rebuilds its cache.</td>
</tr>
<tr>
<td>Email Retriever and Dispatcher</td>
<td>The application server publishes a message to the Retriever and Dispatcher Services when an email alias is created or modified from the Administration Console.</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>- The Scheduler Service publishes a message to the Reports Service when the schedule for a report fires.</td>
</tr>
<tr>
<td></td>
<td>- The application server publishes a message to the Distributed Services Manager (DSM) whenever an agent logs in to or logs out of the application.</td>
</tr>
<tr>
<td></td>
<td>- The application server publishes a message to all other application servers and services when a Custom attribute is created from the Tools Console.</td>
</tr>
<tr>
<td></td>
<td>- The application server publishes a message to other application servers every time an article or topic is added, modified, or removed.</td>
</tr>
</tbody>
</table>

Application Servers

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 Cisco Unified Web and E-Mail Interaction Manager Solutions Reference Network Design Guide.
Web Servers

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 requests for .jsp files 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 Unified EIM & WIM 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

Unified EIM & WIM 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.

Distributed Services Manager (DSM)

The DSM is responsible for starting, stopping, monitoring and managing all the other services running on the services server. The DSM used RMI to communicate with the various services and the application server.

RMI Registry and RMID

All services register themselves with the RMI registry. The RMI registry then stores the location (Server:port) of that service. This enables clients who need to communicate with a service to lookup the information for that service in the RMI registry and initiate a connection.

Understanding Deployment Models

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

- Single-server deployment for Unified EIM: All components are on a single server. This is the simplest type of configuration.
Collocated deployment for Unified WIM: If the installation includes Unified WIM, the collocated deployment option is available, where 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. If the deployment includes only Unified EIM, the web and application servers can be installed on the same machine.

Single-Server Deployment for Unified EIM

All components are installed on a single server.

Collocated Deployment for Unified WIM

If the installation includes Unified WIM, it becomes a collocated deployment, where the web server is installed on a separate machine outside the firewall.
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](diagram)

**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](diagram)
Planning Components for Specific Configurations

Planning the Database Server

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
  - EGML_EMAIL_ATTACHMENT
  - EGML_EMAIL_ATTACHMENT_LINK
  - EGLV_SESSION_CONTENT
  - EGPL_CASEMGMT_ACTIVITY
  - EGPL_EVENT_HISTORY_CASE_MGMT

Installing the Application on a SQL Server 2012 Cluster

Unified EIM & WIM can be installed in a Microsoft SQL Server 2012 clustered environment. To install and configure the SQL Server cluster, follow the instructions in the Microsoft SQL Server 2012 documentation. For details, go to http://msdn.microsoft.com and search for SQL Server clustering.

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 27. You may also need to complete certain tasks described in “Setting Up User Accounts and Permissions” on page 23.

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 23. Also refer to “Configuring Database Servers” on page 27.

Planning Application and Web Servers

- Unified EIM & WIM 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.

  Before installing the application, use the Cisco Unified Web and E-Mail Interaction Manager Solution Reference Network Design Guide to help you determine the best possible configuration for your requirements.

- Unified EIM & WIM 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.

Planning the Messaging Server

- The messaging server can be installed on a separate machine, or on the same machine as one of the application servers in your configuration. 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.

Installing Unified EIM & WIM

- Follow the pre-installation tasks (page 19), installation tasks (page 36), and post-installation tasks (page 63), to install Unified EIM & WIM.

- If you plan to use SSL, follow the instructions in the “SSL Configuration” on page 73.
Pre-Installation Tasks

- Disabling Loopback Adapter Configuration
- Verifying Network Configuration
- Configuring Port Number Between Components
- Setting Up User Accounts and Permissions
- Preparing Database Server Machines
- Preparing the Messaging Server Machine
- Preparing Application Server Machines
- Preparing Services Server Machines
- Preparing Web Server Machines
- Acquiring Licenses
- Verifying Unified CCE Configuration
This chapter describes pre-installation procedures that need to be completed before beginning the installation process. As you need to prepare the installation environment in advance, read this installation guide and the following documents before planning and implementing the installation:

- Cisco Unified Web and E-Mail Interaction Manager Release Notes
- Hardware and System Software Specification for Cisco Unified Web and E-Mail Interaction Manager
- Cisco Unified Web and E-Mail Interaction Manager Solutions Reference Network Design Guide

**Disabling Loopback Adapter Configuration**

Unified EIM & WIM 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 configuration. 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 machines other than the web server, are in the same Active Directory domain. The web server does not need to be installed in the same domain as other Unified EIM & WIM components. It can be located anywhere, for example, in a DMZ. Note that the application cannot be installed in a workgroup.
2. 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 expiry.
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 Number Between Components” on page 21.
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 Number 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 Unified EIM & WIM system architecture. This will help you understand the communication between the different components.
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 *.

<table>
<thead>
<tr>
<th>From Server</th>
<th>To Server</th>
<th>Default Destination Ports and Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workstation (Internet)</td>
<td>Web Server</td>
<td>80 [Protocol: HTTP]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>443 [Protocol: HTTPS]</td>
</tr>
<tr>
<td>Application Server</td>
<td>Services Server</td>
<td>15099 (RMI Registry port) [Protocol: RMI]*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>25000 - 25025 (Cache Manager ports for all services on the Services Server) [Protocol: TCP]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>49152 – 65535 (Dynamic port range used by RMI server objects) [Protocol: TCP]</td>
</tr>
<tr>
<td>Application Server</td>
<td>File Server</td>
<td>139 or 445 [Protocol: NETBIOS - TCP]</td>
</tr>
<tr>
<td>Application Server</td>
<td>Database Server</td>
<td>1433 [Protocol: TCP] *</td>
</tr>
<tr>
<td>Application Server</td>
<td>Messaging Server</td>
<td>4447 [Protocol: Remote], 5445*</td>
</tr>
<tr>
<td>Application Server</td>
<td>Application Server</td>
<td>12345 - 123nn where nn is the number of application servers in the deployment. [Protocol: TCP]</td>
</tr>
<tr>
<td>Application Server</td>
<td>SMTP Server</td>
<td>25 [Protocol: SMTP]</td>
</tr>
<tr>
<td>Application Server</td>
<td>SMTP or ESMTP Server (with SSL enabled)</td>
<td>587 [Protocol: SMTP or ESMTP]</td>
</tr>
<tr>
<td>Application Server</td>
<td>IMAP Server</td>
<td>143 [Protocol: IMAP]</td>
</tr>
<tr>
<td>Application Server</td>
<td>IMAP Server (with SSL enabled)</td>
<td>993 [Protocol: IMAP]</td>
</tr>
<tr>
<td>Web Server</td>
<td>Application Server</td>
<td>15006, 15007, 15008, 15009 [Protocol: TCP] *</td>
</tr>
<tr>
<td>Web Server</td>
<td>File Server</td>
<td>139 or 445 [Protocol: NETBIOS - TCP]</td>
</tr>
<tr>
<td>Web Server</td>
<td>Database Server</td>
<td>1433 [Protocol: TCP] *</td>
</tr>
<tr>
<td>Messaging Server</td>
<td>File Server</td>
<td>139 or 445 [Protocol: NETBIOS - TCP]</td>
</tr>
<tr>
<td>Services Server</td>
<td>File Server</td>
<td>139 or 445 [Protocol: NETBIOS - TCP]</td>
</tr>
<tr>
<td>Services Server</td>
<td>Database Server</td>
<td>1433 [Protocol: TCP] *</td>
</tr>
<tr>
<td>Services Server</td>
<td>Messaging Server</td>
<td>4447* [Protocol: Remote]</td>
</tr>
<tr>
<td>Services Server</td>
<td>Application Server</td>
<td>12345 - 123nn where nn is the number of Application Servers in the deployment [Protocol: TCP]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4447* [Protocol: Remote]</td>
</tr>
<tr>
<td>Services Server</td>
<td>SMTP or ESMTP Server</td>
<td>25 [Protocol: SMTP or ESMTP]</td>
</tr>
<tr>
<td>Services Server</td>
<td>SMTP or ESMTP Server (with SSL enabled)</td>
<td>587 [Protocol: SMTP or ESMTP]</td>
</tr>
</tbody>
</table>
Setting Up User Accounts and Permissions

You will need administrator privileges on the local system to perform the installation and run the Unified EIM & WIM services after installing the application. The type of user account you need for the installation depends on the deployment model and the authentication you pick for the databases - SQL authentication or Windows authentication.

In single-server configurations, a *local* username, with administrator privileges, can be used. In distributed-server configurations, where all databases are on one server and all other Unified EIM & WIM components are on the
same machine, and you are using SQL Authentication for the databases, you can use a local username with administrator privileges. In all other distributed-server configurations, a domain user account is required.

---

**Important:** You must use the same domain account to install the software environment and Unified EIM & WIM. This account is also used to run the Unified EIM & WIM services after installing the application (page 68).

---

**Setting Up Domain Account**

- Request your IT department to create a domain user account for exclusive use by Unified EIM & WIM. The domain user account needs the Log on as a Service and Local Administrator privileges on each of the servers used in the deployment. It does not require the Interactive Logon privilege.

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

---

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

---

**Configuring Permissions on Active Directory Server**

If you are using Windows authentication database connectivity, and 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/PORT accountname
   setspn -A MSSQLSvc/instanceaccountname 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, type:

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

---

Important: You must use the same domain account to install the software environment and Unified EIM & WIM. This account is also used to run the Unified EIM & WIM services after installing the application (page 68).

---

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.
2. Go to **Start > Control Panel > Administrative Tools > Active Directory Users and Computers**.
3. Navigate to the domain user account to be used for installation. 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.
   b. Click the Delegation tab. Ensure that the domain user account is trusted for delegation.
4. In the Active Directory Users and Computers tree, navigate to the database server. Ensure that it is trusted for delegation. Repeat this step for each database server.

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

### Preparing Database Server Machines

#### Creating SQL User for Installing Unified EIM & WIM Databases

Skip this section if you want to use the default sa user to install the Unified EIM & WIM databases.

- Create a user for installing the Unified EIM & WIM databases and make sure the following roles are assigned to the user: dbcreator, securityadmin, sysadmin

#### Verifying Collation Settings

- Collation settings are typically chosen while installing SQL Server 2012. 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 2012, 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.
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 Unified EIM & WIM 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 24. 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. You do not need to perform this task if you are doing a single-server installation.

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 Accounts section, set the value in the Account field to **NT Authority\NetworkService**.
Click OK.

 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 2012.
9. Now, start the two services in the following order:
   a. Distributed Transaction Coordinator
   b. SQL Server (MSSQLSERVER) for Microsoft SQL 2012.
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**.

![Select the Distributed Transaction Coordinator option](image)

**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 Unified EIM and WIM application (page 24).

- **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 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 Unified EIM and WIM application (page 24).

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

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

Start the SQL services

Preparing the Messaging Server Machine

Perform these tasks on the machine where you are going to install the messaging server.

Installing JBoss

Install JBoss on the machine where the messaging server is going to be installed.

To install JBoss:

1. Copy the jboss-as-7.2.0.Final.zip file from the Environment > JBoss folder on the application CD to a temporary location on the hard drive.
2. Use a zip file extraction tool like WinZip to extract the files from the `jboss-as-7.2.0.Final.zip` file to the location where JBoss is to be installed (`JBoss_Home`), for example, `C:\jboss-as-7.2.0.Final`.

   ![Extract JBoss files to JBoss home directory](image1.png)

3. Open the folder to verify that the following folders have been extracted: `appclient`, `bin`, `bundles`, `docs`, `domain`, `modules`, `standalone`, and `welcome-content`. The following files should also be present: `copyright.txt`, `jboss-modules.jar`, `license.txt`, and `readme.txt`.

   ![JBoss home directory](image2.png)

You have now installed JBoss.

4. Take a back-up of the `JBoss_Home\standalone` directory.
5. Once JBoss is installed, the `jboss-as-7.2.0.Final.zip` file can be deleted from the temporary folder.

### Installing JDK

- Install JDK 1.7 Update 2 or higher (64-bit) on the machine where the messaging server component is to be installed. The installation program for JDK 1.7 Update 71 is included in the `Environment\Server Side Java` folder of the installation package.

### Preparing Application Server Machines

Perform these tasks on all the machines where you are going to install the application server.

### Installing JDK

- Install JDK 1.7 Update 2 or higher (64-bit) on all machines where the application server component is to be installed. The installation program for JDK 1.7 Update 71 is included in the `Environment\Server Side Java` folder of the installation package.

### Installing JBoss

- Install JBoss on all the machines where you are going to install the application server. For details, see “Installing JBoss” on page 30.

### Preparing Services Server Machines

### Installing JDK

- Install JDK 1.7 Update 2 or higher (64-bit) on all machines where the services server component is to be installed. The installation program for JDK 1.7 Update 71 is included in the `Environment\Server Side Java` folder of the installation package.

### Preparing Web Server Machines

### Configuring Roles and Features

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

- NET Extensibility 4.5
To install the roles and features:

1. Go to **Start > Control Panel > Administrative Tools > Server Manager**.
2. In the Server Manager window, Go to IIS section. In the IIS section, locate the Roles and Features section.
3. In the Role and Features section, check if the required role services are installed.
4. If any of the roles and features are not installed, from the Tasks menu, click the **Add Roles and Features** button and run through the wizard to install the missing services. In the Server Roles section, select the following:
   - In the Application Development list, select:
     - NET Extensibility 4.5
     - ASP
     - CGI
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.

**Configuring Permissions on IIS Config Folder**

- Ensure that the user account you are going to use for installing the application (page 24) 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.

**Acquiring Licenses**

- Make sure you have the Unified WIM and Unified EIM licenses ready with you before you begin the installation. You will need them to complete the installation process. Contact Cisco Licence Team for the licenses.

**Verifying Unified CCE Configuration**

- Verify that Unified CCE 9.0(4), 10.0, 10.5, or 11.0 and Microsoft Active Directory (AD) 2003 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 Unified WIM and Unified EIM servers and are accessible from the Unified WIM and Unified EIM servers.
- Verify that the items to be used in Unified WIM and Unified EIM 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
- Services
- Skill Groups (IPTA and Non-IPTA)
- ICM Scripts
- Expanded Call Context (ECC) Variables
- CTI Gateways (CG)

For details, see *Cisco Unified Web and E-Mail Interaction Manager Deployment and Maintenance Guide*. 
Installation Process

- Installation Overview
- Installing Unified EIM & WIM
- Installation Details
The installation process consists of two parts:

1. Installing Unified WIM and Unified EIM in your chosen configuration using the Unified EIM & WIM installation program.
2. Integrating Unified WIM and Unified EIM with Unified CCE using the Unified EIM & WIM Wizard for Unified CCE.

This chapter describes the process of installing the product in single-server and distributed-server configurations. After completing the installation process, you can install the integration immediately by starting the Unified EIM & WIM Integration Wizard. The integration can also be installed later by running the Integration Wizard. The process of installing the integration is described in “Unified CCE Integration” on page 52.

Before beginning the installation, ensure that you have complied with all the prerequisites listed in “Pre-Installation Tasks” on page 19.

### Installation Overview

You can do a single-server installation, where all components are installed on the same machine, or you can do a distributed-server installation, where each component is installed on a separate machine.

A true single-server deployment is possible only for Unified EIM installations. If the installation includes Unified WIM, it becomes a collocated deployment, where the web server is installed on a separate machine. The web server may be installed outside the firewall, if required.

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.

While doing a distributed server installation for Unified EIM, if you are installing the 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.

---

**Important:** Make sure you have the licenses ready with you before you begin the installation. You will need them to complete the installation process.
Installing Unified EIM & WIM

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 in graphical mode:

1. Copy the contents of the installation CD to a temporary directory, Temp, on your local machine where you are running the installer.
2. Run setup_wsjb.exe from the Temp\Application directory.
3. When the Introduction window appears, read the installation instructions. Click Next.
4. In the License Agreement window, review the licensing terms and select the I accept the terms of the License Agreement option. Click Next.

![License Agreement](image)

Read and accept the terms of the License Agreement

5. 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 37.

- File Server
- Messaging Server
- Application Server
- Web Server
- Services Server
- Database
Click **Next**.

Based on the components you choose to install, you will see a different set of screens. The installation program for Unified EIM & WIM 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 40
- Database Server Details on page 41
- Web Server Details on page 48
- Messaging Server Details on page 49
- Application Server Details on page 50
- Services Server Details on page 51

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

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

While installing the application on the services server, you get the option to run the Unified EIM & WIM Integration Wizard.

8. After completing the Unified WIM and Unified EIM installation process on the services server, you can either continue to run the Unified EIM & WIM Integration Wizard or you can run it later. Do one of the following:

- Copy the license files provided by Cisco to the following location on the file server:
  
  \(Cisco\_Home\\eService\\config\license\)
  
  Then, click the **Finish** button to launch the Unified EIM & WIM Integration Wizard and follow steps 3 to 22 in “To run the integration wizard:” on page 53.

- Copy the license files and then choose to run the Unified EIM & WIM Integration Wizard later. To run the wizard later, follow the steps in “Integrating Unified EIM & WIM with Unified CCE” on page 53.

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 63).

**Installation Details**

**File Server Details**

<table>
<thead>
<tr>
<th>#</th>
<th>Graphic Installation</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Cisco Unified EIM &amp; WIM Directory</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Location of Unified EIM &amp; WIM Home Directory</td>
<td>Provide the path of the directory where you would like to install Unified EIM &amp; WIM. For example, c:\Cisco, or \SharedSpace\Cisco, if the file server is installed on a NAS device. <strong>Note:</strong> Make sure that the path and folder name do not contain any of the following characters: *&lt;=&gt;</td>
<td>&quot;,;@</td>
</tr>
<tr>
<td></td>
<td><strong>Domain User Account Parameters</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Domain User name</td>
<td>User name of the domain user account created for use by the application. For more information, refer to &quot;Setting Up User Accounts and Permissions&quot; on page 23.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Domain User Password</td>
<td>Password for the domain user.</td>
<td></td>
</tr>
</tbody>
</table>
## Database Server Details

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

### Installation Identifiers
<table>
<thead>
<tr>
<th>#</th>
<th>Graphic Installation</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.</td>
<td>Unique name for this installation</td>
<td>Provide a unique name for this installation. For example: PROD, PRD1, TEST, TST2, or DEMO. The length of the name must be between 1 and 4 characters long. The name must not contain any spaces or special characters.</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>4-digit identifier for this installation</td>
<td>Provide a 4-digit numerical value, between 2001 and 9998, that will be used internally as system ID.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Knowledge Base Primary Language</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td>Knowledge Base Primary Language</td>
<td>The default language for the Knowledge Base.</td>
<td>English (US)</td>
</tr>
<tr>
<td></td>
<td><strong>Default Notification Parameters</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>Default SMTP server</td>
<td>The SMTP server to be used to send email notifications.</td>
<td></td>
</tr>
<tr>
<td>13.</td>
<td>Notification mail redirection from address</td>
<td>All notification emails are sent from this email address.</td>
<td></td>
</tr>
<tr>
<td>14.</td>
<td>Notification mail redirection to address</td>
<td>All notification emails are sent to this email address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SQL Server Database Authentication</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td>Authentication</td>
<td>Authentication type to be used while connecting to the database. Set the value as SQL Server Authentication mode or Windows Authentication mode. If you selected Windows Authentication as the only mode of authentication while installing SQL Server, you must set the value as Windows Authentication mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Master Database Parameters</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16.</td>
<td>Server name</td>
<td>Name of the local or remote server on which you want to install the master database. If you are using MSSQL Server clustering, specify the name of the Virtual MSSQL Cluster Node that integrates the services running on physical nodes in the cluster. <strong>Note:</strong> Make sure you provide the DNS host name and not the IP address.</td>
<td></td>
</tr>
<tr>
<td>17.</td>
<td>Database name</td>
<td>Name of the master database. The installation program creates a database with the name you provide here.</td>
<td></td>
</tr>
<tr>
<td>18.</td>
<td>Server instance name</td>
<td>Name of the MSSQL Server instance to be used while creating the database. Set this value only if you are using a named instance, and not the default instance. If you are using MSSQL Server clustering, provide the name of the Virtual SQL Service Instance.</td>
<td></td>
</tr>
<tr>
<td>19.</td>
<td>Database listener port</td>
<td>Port number of the MSSQL Server.</td>
<td>1433</td>
</tr>
<tr>
<td>#</td>
<td>Graphic Installation</td>
<td>Description</td>
<td>Value</td>
</tr>
<tr>
<td>----</td>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>20</td>
<td>Datafile path</td>
<td>Path to the folder on the database server, where you want to create the data file. For example, D:\MSSQL\Data. If you are using MSSQL Server clustering, provide the path to the drive shared among the clustered nodes.</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Datafile initial size</td>
<td>Minimum size of the data file for the database.</td>
<td>100</td>
</tr>
<tr>
<td>22</td>
<td>Datafile maximum size</td>
<td>Maximum size of the data file for the database.</td>
<td>Unlimited</td>
</tr>
<tr>
<td>23</td>
<td>Datafile increment size</td>
<td>Additional file size limit that will be allocated to the database after the initial size is full.</td>
<td>10</td>
</tr>
<tr>
<td>24</td>
<td>Logfile initial size</td>
<td>Minimum size of the log file.</td>
<td>25</td>
</tr>
<tr>
<td>25</td>
<td>Logfile maximum size</td>
<td>Maximum size of the log file.</td>
<td>Unlimited</td>
</tr>
<tr>
<td>26</td>
<td>Database administrator user name</td>
<td>User name of the database administrator for MSSQL Server. If you have created a separate user for installing Unified EIM &amp; WIM databases, provide the name of that user (page 26). If you are using MSSQL Server clustering, provide the user corresponding to the virtual instance used for this database. <strong>Note:</strong> This property needs to be configured only if you are using the SQL Server Authentication mode.</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Database administrator password</td>
<td>Password of the database administrator. <strong>Note:</strong> This property needs to be configured only if you are using the SQL Server Authentication mode.</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Cisco Database user name</td>
<td>User name required to connect to the master database. The installation program creates the database and its user.</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Cisco Database password</td>
<td>Password for the master database user.</td>
<td></td>
</tr>
</tbody>
</table>

**Active Database Parameters**

<table>
<thead>
<tr>
<th>#</th>
<th>Graphic Installation</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Server name</td>
<td>Name of the local or remote server on which you want to install the active database. <strong>Note:</strong> It must be the same server on which the master database is installed.</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>Database name</td>
<td>Name of the active database. The installation program creates a database with the name you provide here.</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Server instance name</td>
<td>Name of the MSSQL Server instance to be used while creating the database. This should match the value set for the master database instance name.</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>Database listener port</td>
<td>Port number of MSSQL Server. This should match the value set for the master database.</td>
<td>1433</td>
</tr>
<tr>
<td>34</td>
<td>Datafile path</td>
<td>Path to the folder on the database server, where you want to create the data file. For example, C:\MSSQL\Data. If you are using MSSQL Server clustering, provide the path to the drive shared among the clustered nodes.</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>Datafile initial size</td>
<td>Minimum size of the data file for the database.</td>
<td>2048</td>
</tr>
<tr>
<td>#</td>
<td>Graphic Installation</td>
<td>Description</td>
<td>Value</td>
</tr>
<tr>
<td>----</td>
<td>----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>36</td>
<td>Datafile maximum size</td>
<td>Maximum size of the data file for the database.</td>
<td>Unlimited</td>
</tr>
<tr>
<td>37</td>
<td>Datafile increment size</td>
<td>Additional file size limit that will be allocated to the database after the initial size is full.</td>
<td>500</td>
</tr>
<tr>
<td>38</td>
<td>Logfile initial size</td>
<td>Minimum size of the log file.</td>
<td>1024</td>
</tr>
<tr>
<td>39</td>
<td>Logfile maximum size</td>
<td>Maximum size of the log file.</td>
<td>Unlimited</td>
</tr>
<tr>
<td>40</td>
<td>Database administrator username</td>
<td>User name of the database administrator for MSSQL Server. If you have created a separate user for installing Unified EIM &amp; WIM databases, provide the name of that user (page 26). If you are using MSSQL Server clustering, provide the user corresponding to the virtual instance used for this database. Note: This property needs to be configured only if you are using the SQL Server Authentication mode.</td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>Database administrator password</td>
<td>Password of the database administrator. Note: This property needs to be configured only if you are using the SQL Server Authentication mode.</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>Cisco Database user name</td>
<td>User name required to connect to the database. The installation program will create this user.</td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>Cisco Database password</td>
<td>Password for the database user.</td>
<td></td>
</tr>
</tbody>
</table>

**Active Database Filegroup Parameters [Only for Enterprise Edition of MSSQL Server]**

<table>
<thead>
<tr>
<th>#</th>
<th>Graphic Installation</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>44</td>
<td>Filegroup Datafile 1 Name</td>
<td>Provide the name of the first file group to be created for the active database.</td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>Filegroup Datafile 1 Path</td>
<td>Provide the location for the first filegroup.</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>Filegroup Datafile 2 Name</td>
<td>Provide the name of the second file group to be created for the active database.</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>Filegroup Datafile 2 Path</td>
<td>Provide the location for the second filegroup.</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>Filegroup Datafile 3 Name</td>
<td>Provide the name of the third file group to be created for the active database.</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>Filegroup Datafile 3 Path</td>
<td>Provide the location for the third filegroup.</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>Filegroup Datafile 4 Name</td>
<td>Provide the name of the fourth file group to be created for the active database.</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>Filegroup Datafile 4 Path</td>
<td>Provide the location for the fourth filegroup.</td>
<td></td>
</tr>
</tbody>
</table>

**Reports Database Parameters [Only for Enterprise Edition of MSSQL Server]**

<table>
<thead>
<tr>
<th>#</th>
<th>Graphic Installation</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>52</td>
<td>Server name</td>
<td>Name of the local or remote server on which the reports database should be installed. If you are using MSSQL server clustering, specify the name of the virtual MSSQL cluster node that integrates the services running on physical nodes in the cluster. Note: Make sure you provide the DNS host name and not the IP address of the server.</td>
<td></td>
</tr>
<tr>
<td>#</td>
<td><strong>Graphic Installation</strong></td>
<td><strong>Description</strong></td>
<td><strong>Value</strong></td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>53</td>
<td>Database name</td>
<td>Name of the reports database. The installation program creates a database with the name you type here.</td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>Database server instance</td>
<td>Name of the MSSQL Server instance to be used while creating the database. Set this value only if you are using a named instance, and not the default instance. If you are using MSSQL Server clustering, provide the name of the Virtual SQL Service Instance.</td>
<td></td>
</tr>
<tr>
<td>55</td>
<td>Database listener port</td>
<td>Port number of the MSSQL Server.</td>
<td>1433</td>
</tr>
<tr>
<td>56</td>
<td>Datafile path</td>
<td>Path to the folder on the database server, where you want to create the data file. For example, D:\MSSQL\Data. If you are using MSSQL Server clustering, provide the path to the drive shared among the clustered nodes.</td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>Datafile initial size</td>
<td>Minimum size of the data file for the database.</td>
<td>10</td>
</tr>
<tr>
<td>58</td>
<td>Datafile maximum size</td>
<td>Maximum size of the data file for the database.</td>
<td>Unlimited</td>
</tr>
<tr>
<td>59</td>
<td>Datafile increment size</td>
<td>Additional file size limit that will be allocated to the database after the initial size is full.</td>
<td>10</td>
</tr>
<tr>
<td>60</td>
<td>Logfile initial size</td>
<td>Minimum size of the log file.</td>
<td>10</td>
</tr>
<tr>
<td>61</td>
<td>Logfile maximum size</td>
<td>Maximum size of the log file.</td>
<td>Unlimited</td>
</tr>
<tr>
<td>62</td>
<td>Database administrator user name</td>
<td>User name of the database administrator for MSSQL Server. If you have created a separate user for installing Unified EIM &amp; WIM databases, provide the name of that user (page 26). If you are using MSSQL Server clustering, provide the user corresponding to the virtual instance used for this database. <strong>Note:</strong> This property needs to be configured only if you are using the SQL Server Authentication mode.</td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>Database administrator password</td>
<td>Password of the database administrator. <strong>Note:</strong> This property needs to be configured only if you are using the SQL Server Authentication mode.</td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>Cisco Database user name</td>
<td>User name required to connect to the reports database. The installation program will create this user.</td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>Cisco Database password</td>
<td>Password for the database user.</td>
<td></td>
</tr>
</tbody>
</table>

**Reports Database Filegroup Parameters [Only for Enterprise Edition of MSSQL Server]**

<table>
<thead>
<tr>
<th>#</th>
<th><strong>Filegroup Datafile 1 Name</strong></th>
<th>Provide the name of the first file group to be created for the reports database.</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>66</td>
<td>Filegroup Datafile 1 Path</td>
<td>Provide the location for the first filegroup.</td>
<td></td>
</tr>
<tr>
<td>67</td>
<td>Filegroup Datafile 2 Name</td>
<td>Provide the name of the second file group to be created for the reports database.</td>
<td></td>
</tr>
<tr>
<td>68</td>
<td>Filegroup Datafile 2 Path</td>
<td>Provide the location for the second filegroup.</td>
<td></td>
</tr>
<tr>
<td>69</td>
<td>Filegroup Datafile 3 Name</td>
<td>Provide the name of the third file group to be created for the reports database.</td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>Graphic Installation</td>
<td>Description</td>
<td>Value</td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>71</td>
<td>Filegroup Datafile 3 Path</td>
<td>Provide the location for the third filegroup.</td>
<td></td>
</tr>
<tr>
<td>72</td>
<td>Filegroup Datafile 4 Name</td>
<td>Provide the name of the fourth file group to be created for the reports database.</td>
<td></td>
</tr>
<tr>
<td>73</td>
<td>Filegroup Datafile 4 Path</td>
<td>Provide the location for the fourth filegroup.</td>
<td></td>
</tr>
</tbody>
</table>

**Archive Database Parameters [Only for Standard Edition of MSSQL Server]**

<table>
<thead>
<tr>
<th>#</th>
<th>Graphic Installation</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>74</td>
<td>Server name</td>
<td>Name of the local or remote server on which the archive database should be installed. If you are using MSSQL Server clustering, specify the name of the Virtual MSSQL Cluster Node that integrates the services running on physical nodes in the cluster. <strong>Note:</strong> Make sure you provide the DNS host name and not the IP address of the server.</td>
<td></td>
</tr>
<tr>
<td>75</td>
<td>Database name</td>
<td>Name of the archive database. The installation program creates a database with the name you provide here.</td>
<td></td>
</tr>
<tr>
<td>76</td>
<td>Database server instance</td>
<td>Name of the MSSQL Server instance to be used while creating the database. Set this value only if you are using a named instance, and not the default instance. If you are using MSSQL Server clustering, provide the name of the Virtual SQL Service Instance.</td>
<td></td>
</tr>
<tr>
<td>77</td>
<td>Database listener port</td>
<td>Port number of the MSSQL Server.</td>
<td>1433</td>
</tr>
<tr>
<td>78</td>
<td>Datafile path</td>
<td>Path to the folder on the database server, where you want to create the data file. For example, C:\MSSQL\data. If you are using MSSQL Server clustering, provide the path to the drive shared among the clustered nodes.</td>
<td></td>
</tr>
<tr>
<td>79</td>
<td>Datafile initial size</td>
<td>Minimum size of the data file for the database.</td>
<td>512</td>
</tr>
<tr>
<td>80</td>
<td>Datafile maximum size</td>
<td>Maximum size of the data file for the database.</td>
<td>Unlimited</td>
</tr>
<tr>
<td>81</td>
<td>Datafile increment size</td>
<td>Additional file size limit that will be allocated to the database after the initial size is full.</td>
<td>10</td>
</tr>
<tr>
<td>82</td>
<td>Logfile initial size</td>
<td>Minimum size of the log file.</td>
<td>50</td>
</tr>
<tr>
<td>83</td>
<td>Logfile maximum size</td>
<td>Maximum size of the log file.</td>
<td>Unlimited</td>
</tr>
<tr>
<td>84</td>
<td>Database administrator user name</td>
<td>User name of the database administrator for MSSQL Server. If you have created a separate user for installing Unified EIM &amp; WIM databases, provide the name of that user (page 26). If you are using MSSQL Server clustering, provide the user corresponding to the virtual instance used for this database. <strong>Note:</strong> This property needs to be configured only if you are using the SQL Server Authentication mode.</td>
<td></td>
</tr>
<tr>
<td>85</td>
<td>Database administrator password</td>
<td>Password of the database administrator. <strong>Note:</strong> This property needs to be configured only if you are using the SQL Server Authentication mode.</td>
<td></td>
</tr>
<tr>
<td>86</td>
<td>Cisco Database user name</td>
<td>User name required to connect to the archive database. The installation program will create this user.</td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>Graphic Installation</td>
<td>Description</td>
<td>Value</td>
</tr>
<tr>
<td>----</td>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>87</td>
<td>Cisco Database password</td>
<td>Password for the database user.</td>
<td></td>
</tr>
</tbody>
</table>

**Domain User Account Parameters**

<table>
<thead>
<tr>
<th>#</th>
<th>Graphic Installation</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>88</td>
<td>Domain User name</td>
<td>User name of the domain user account you created for use by the application. For more information, refer to “Setting Up User Accounts and Permissions” on page 23.</td>
<td></td>
</tr>
<tr>
<td>89</td>
<td>Domain User Password</td>
<td>Password for the domain user.</td>
<td></td>
</tr>
</tbody>
</table>

*Database server details*
# Web Server Details

<table>
<thead>
<tr>
<th>#</th>
<th>Graphic Installation</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Server Parameters</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Application server name</td>
<td>Type the name of the application server for which you want to configure the web server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Make sure you provide the DNS host name and not the IP address of the server.</td>
<td></td>
</tr>
<tr>
<td><strong>Cisco Unified EIM &amp; WIM Directory</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Location of Cisco home directory</td>
<td>Provide the path of the directory where you would like to install Unified EIM &amp; WIM. For example, c:\Cisco.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Make sure that the path and folder name do not contain any of the following characters: &quot;?&lt;&gt;</td>
<td>+^'&quot;%;@</td>
</tr>
<tr>
<td><strong>IIS Web Site Parameters</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>IIS Web Site Name</td>
<td>Name of the IIS Web Site on which the application is to be configured.</td>
<td>Default Web Site</td>
</tr>
<tr>
<td><strong>Cisco Application Context Root</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Context Root Name</td>
<td>Provide the same context root name which was provided at the time of installing the Cisco database server (page 41).</td>
<td></td>
</tr>
<tr>
<td><strong>Cisco Partition Name</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Partition Name</td>
<td>Provide the name for the business partition. Make sure you provide the same name which was provided at the time of installing the Cisco database server (page 41).</td>
<td></td>
</tr>
<tr>
<td><strong>Domain User Account Parameters</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Domain User name</td>
<td>User name of the domain user account you created for use by the application. For more information, refer to &quot;Setting Up User Accounts and Permissions&quot; on page 23.</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Domain User Password</td>
<td>Password for the domain user.</td>
<td></td>
</tr>
</tbody>
</table>

*Web server details*
# Messaging Server Details

<table>
<thead>
<tr>
<th>#</th>
<th>Graphic Installation</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File Server Parameters</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>File Server name/NAS Path</td>
<td>The fully qualified domain name of the file server. If the file server is installed on a NAS device, provide the path to the shared folder on the NAS device. For example, <code>\SharedSpace\Cisco</code>. <strong>Note:</strong> Make sure you provide the DNS host name and not the IP address of the server.</td>
<td></td>
</tr>
<tr>
<td><strong>Cisco Unified EIM &amp; WIM Directory</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Location of Cisco home directory</td>
<td>Provide the path of the directory where you would like to install Unified EIM &amp; WIM. For example, <code>c:\Cisco</code>. <strong>Note:</strong> Make sure that the path and folder name do not contain any of the following characters: `*&lt;&gt;</td>
<td>^&amp;`</td>
</tr>
<tr>
<td><strong>JDK Home Directory</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Location of JDK home directory</td>
<td>Provide the path to the JDK home directory. For example, <code>C:\Program Files\Java\jdk1.7.0_02</code></td>
<td></td>
</tr>
<tr>
<td><strong>JBoss Parameters</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>JBoss home directory</td>
<td>Complete path to the directory where JBoss is installed. For example, <code>C:\jboss-7.2.0.Final</code></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>JBoss Messaging Port</td>
<td>Messaging port number for JBoss.</td>
<td>5445</td>
</tr>
<tr>
<td>6.</td>
<td>JBoss Remote Port</td>
<td>Remote port number used by JBoss.</td>
<td>4447</td>
</tr>
<tr>
<td>7.</td>
<td>JBoss HTTP port</td>
<td>Port number used by JBoss.</td>
<td>9001</td>
</tr>
<tr>
<td>8.</td>
<td>JBoss HTTP SSL Port</td>
<td>Secure Sockets Layer port number used by JBoss.</td>
<td>9002</td>
</tr>
<tr>
<td><strong>Domain User Account Parameters</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>Domain User name</td>
<td>User name of the domain user account you created for use by the application. For more information, refer to “Setting Up User Accounts and Permissions” on page 23.</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>Domain User Password</td>
<td>Password for the domain user.</td>
<td></td>
</tr>
</tbody>
</table>

*Messaging server details*
## Application Server Details

<table>
<thead>
<tr>
<th>#</th>
<th>Graphic Installation</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File Server Parameters</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>File Server name/ NAS Path</td>
<td>The fully qualified domain name of the file server. If the file server is installed on a NAS device, provide the path to the shared folder on the NAS device. For example, \SharedSpace\Cisco</td>
<td>Note: Make sure you provide the DNS host name and not the IP address of the server.</td>
</tr>
<tr>
<td><strong>Cisco Unified EIM &amp; WIM Directory</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Location of Cisco home directory</td>
<td>Provide the path of the directory where you would like to install Unified EIM &amp; WIM. For example, c:\Cisco.</td>
<td>Note: Make sure that the path and folder name do not contain any of the following characters: `?&lt;&gt;</td>
</tr>
<tr>
<td><strong>JDK Home Directory</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Location of JDK home directory</td>
<td>Provide the path to the JDK home directory. For example, C:\Program Files\Java\jdk1.7.0_02</td>
<td></td>
</tr>
<tr>
<td><strong>JBoss Parameters</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>JBoss home directory</td>
<td>Complete path to the directory where JBoss is installed. For example, C:\jboss-7.2.0.Final</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>JBoss Messaging Port</td>
<td>Messaging port number for JBoss.</td>
<td>5445</td>
</tr>
<tr>
<td>6.</td>
<td>JBoss Remote Port</td>
<td>Remote port number used by JBoss.</td>
<td>4447</td>
</tr>
<tr>
<td>7.</td>
<td>JBoss HTTP port</td>
<td>Port number used by JBoss.</td>
<td>9001</td>
</tr>
<tr>
<td>8.</td>
<td>JBoss HTTP SSL Port</td>
<td>Secure Sockets Layer port number used by JBoss.</td>
<td>9002</td>
</tr>
<tr>
<td><strong>Domain User Account Parameters</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>Domain User name</td>
<td>User name of the domain user account you created for use by the application. For more information, refer to “Setting Up User Accounts and Permissions” on page 23.</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>Domain User Password</td>
<td>Password for the domain user.</td>
<td></td>
</tr>
<tr>
<td><strong>EAR Deployment Parameters</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td>Deploy EAR Automatically</td>
<td>Specify if you want to deploy the EAR automatically when the application is started. You must always select the value as Yes.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Application server details
## Services Server Details

<table>
<thead>
<tr>
<th>#</th>
<th>Graphic Installation</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File Server Parameters</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 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 Unified EIM & WIM Directory**                                                                                                               |                                                                                                                                            |       |
| 2. | Location of Cisco home directory | Provide the path of the directory where you would like to install Unified EIM & WIM. For example, `c:\Cisco`.  
**Note:** Make sure that the path and folder name do not contain any of the following characters: "?<>|+%^",@ |       |
| **JDK Home Directory**                                                                                                                               |                                                                                                                                            |       |
| 3. | Location of JDK home directory | Provide the path of the JDK home directory.  
For example, `C:\Program Files\Java\jdk1.7.0_02` |       |
| **RMI and RMID Parameters**                                                                                                                             |                                                                                                                                            |       |
| 4. | RMI registry port | Port number used by the Remote Method Invocation (RMI) registry naming service. | 15099 |
| 5. | RMI activation port | Port number used by the RMI Daemon Process. | 15098 |
| **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 23. |       |
| 7. | Domain User Password | Password for the domain user. |       |

**Cisco Unified EIM & WIM Integration Wizard**

The wizard can be run as part of the installation, or as a standalone task. For details, see Step 8 on page 39.

*Services server details*
Unified CCE Integration

- Integrating Unified EIM & WIM with Unified CCE
Integrating Unified EIM & WIM with Unified CCE

Unified EIM & WIM is integrated with Unified CCE by running the Unified EIM & WIM Integration Wizard on the services server of Unified EIM & WIM. The wizard imports the media routing domains, agents, and skill groups information from the Unified CCE database to the Unified EIM & WIM database.

Before running the Unified EIM & WIM Integration Wizard, verify that:

- License files provided by Cisco have been copied to the following location:
  \Cisco_Home\eService\config\license.
- Unified CCE has been configured for the integration (for details, see Cisco Unified Web and E-Mail Interaction Manager Deployment and Maintenance Guide).

To run the integration wizard:

1. Browse to \Cisco_Home\eService\bin\IPCC.
2. Locate the uiconfigwizard.bat file. Double-click it to launch the Unified EIM & WIM Integration Wizard.
3. When the first window appears, read the introduction and click Next.
4. In the next window, read the details about the steps and click Next.

![Image of Cisco Unified EIM & WIM Integration Wizard]

**Review the integration procedure**

5. In the next window, type the path or browse to the folder where Unified EIM & WIM is installed. Click Next.

![Image of Specify Cisco Unified EIM & WIM Installation directory]

**Provide the location of the Unified EIM & WIM installation directory**
6. In the next window, select the department for which you want to download MRDs, agents, and skill groups. Click Next.

![Image](image1.png)

*Select the partition and department to integrate*

7. In the next window, provide the following details, and click Next.
   - **Unified CCE Administration Host Name:** Server name or IP address of the Unified CCE Administration Workstation (AW) server.
   - **SQL Server Database Name:** Name of the Unified CCE AW database.
   - **Port Number:** Port number of the Unified CCE AW database server. The default value is 1433.
   - **Database Administrator Login Name:** User name of the database administrator for the Unified CCE AW database server.
   - **Database Administrator Login Password:** Password of the database administrator for the Unified CCE AW database server.

![Image](image2.png)

*Provide Unified CCE primary database details*
8. In the next window, review the database details, and click the **Apply** button.

9. In the next window, to configure a secondary database connection, select **Yes** and provide the following details, and click **Next**. If not, select **No** and click **Next**.
   - **Unified CCE Administration Host Name**: Server name or IP address of the Unified CCE Secondary Administration Workstation (AW) server.
   - **SQL Server Database Name**: Name of the Unified CCE Secondary AW database.
   - **Port Number**: Port number of the Unified CCE Secondary AW database server. The default value is 1433.
   - **Database Administrator Login Name**: User name of the database administrator for the Unified CCE Secondary AW database server.
   - **Database Administrator Login Password**: Password of the database administrator for the Unified CCE Secondary AW database server.
10. In the next window, review the database details, and click the **Apply** button.

![Verify secondary database details](image)

11. In the next window, select the application instance that you have configured in Unified CCE. Click **Next**.

![Select the application instance](image)

12. In the next window, select the Agent PGs that you have configured in Unified CCE for integration. Click **Next**.

![Select Agent PGs](image)
13. In the next window, verify that the correct Agent PGs have been selected. Click **Next**.

![Verify that the correct Agent PGs have been selected](image)

14. In the next window, select the media routing domains (MRDs) that you have configured in Unified CCE for the department selected in **Step 6**. Click **Next**.

![Select MRDs](image)

15. In the next window, verify that the correct MRDs have been selected. Click **Next**.

![Verify that the correct MRDs have been selected](image)
16. In the next window, select the Unified CCE script selector that you have configured in Unified CCE for the integration. Click **Next**.

17. In the next window, verify that the correct script selector has been selected. Click **Next**.

18. In the next window, select the peripherals that you have configured in Unified CCE for the integration. Click **Next**.
19. In the next window, verify that the correct peripherals have been selected. Click Next.

![Summary: Selected Peripherals](Image)

*Verify that the correct peripherals have been selected*

20. In the next window, select agents for the Unified CCE peripherals. Click Next.

![Select Agents for Peripheral](Image)

*Select agents*

21. In the next window, verify that the correct agents have been selected. Click Next.

![Summary: Selected Agents for Peripheral](Image)

*Verify that the correct agents have been selected*
22. In the next window, select the skill groups for the peripherals. Click **Next**.

![Select skill groups from the list](image1)

23. In the next window, verify that the correct skill groups have been selected. Click **Next**.

![Verify that the correct skill groups have been selected](image2)

24. In the next window, click the **Finish** button to save the MRD, agent, and skill-group information in the Unified EIM & WIM database.

![Click the Finish button](image3)
25. In the last window, click the **Close** button to close the wizard.

26. If you ran the integration wizard manually, and not along with the Unified EIM & WIM installation program, then stop and start Unified EIM & WIM. For details, see *Stopping Unified EIM & WIM* and *Starting Unified EIM & WIM*. 
Post-Installation Tasks

- Copying Unified EIM & WIM License Files
- Configuring SSL for Secure Connections
- Creating an Encrypted SQL Server Database
- Applying Updates
- Configuring SMTP Server Relay Address List
- Configuring Virus Scanners
- Starting Unified EIM & WIM
- Stopping Unified EIM & WIM
- Logging in to the Business Partition
- Configuring Important Settings
- Uninstalling Unified EIM & WIM
This chapter guides you through the tasks to be performed after installing the system. It also describes the process of uninstalling Unified WIM and Unified EIM.

Copying Unified EIM & WIM License Files

If you have not done so already, perform this task on the file server. In a distributed-server installation, this could be a separate machine.

**To copy the license file:**

- Copy the license files provided by Cisco to the following location:
  \Cisco_Home\eService\config\license

Configuring SSL for Secure Connections

You can set up Secure Sockets Layer (SSL) for more secure connections between browsers and the servers in your installation. This is an optional step. See “SSL Configuration” on page 73 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 Unified EIM and WIM 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.
   ```sql
   USE master
   GO
   CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'company@123'
   GO
   ```

2. Backup the master key. This creates a certificate in the master database.
   ```sql
   BACKUP MASTER KEY TO FILE = 'C:\temp\masterkey'
   ENCRYPTION BY PASSWORD = 'company@123'
   GO
   ```

3. Now create the server certificate database encryption key ("DEK").
   ```sql
   USE master
   GO
   ```
CREATE CERTIFICATE DEKCert WITH SUBJECT = 'DEK Certificate'  
GO

4. Create a backup of the server certificate database encryption key ("DEK").
BACKUP CERTIFICATE DEKCert TO FILE = 'c:\DEKCert'
WITH PRIVATE KEY ( FILE = 'c:\temp\DEKCertPrivKey' ,
ENCRIPTION 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
ENCRIPTION 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
Applying Updates

For details about performing this task, read the release notes available with the updates.

To apply updates:
1. Stop Unified EIM & WIM (page 69) on all servers in the configuration.
2. Copy the Updates folder from the Application CD to a temporary local folder and apply all the updates.

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 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.
Single-Server Configuration

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Exclude Subfolders?</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows File Protection</td>
<td>--</td>
<td>Read, Write</td>
</tr>
<tr>
<td>All files of type LOG</td>
<td>--</td>
<td>Read, Write</td>
</tr>
<tr>
<td>Pagefile.sys</td>
<td>No</td>
<td>Read, Write</td>
</tr>
<tr>
<td>Drive\Cisco_Home\</td>
<td>Yes [other than Storage]</td>
<td>Read, Write</td>
</tr>
<tr>
<td>*.mdf</td>
<td>No</td>
<td>Read, Write</td>
</tr>
<tr>
<td>*.ldf</td>
<td>No</td>
<td>Read, Write</td>
</tr>
<tr>
<td>*.ndf</td>
<td>No</td>
<td>Read, Write</td>
</tr>
<tr>
<td>*.dat</td>
<td>No</td>
<td>Read, Write</td>
</tr>
<tr>
<td>Drive\jdk\</td>
<td>Yes</td>
<td>Read, Write</td>
</tr>
<tr>
<td>Drive\JBoss\</td>
<td>Yes</td>
<td>Read, Write</td>
</tr>
<tr>
<td>*.rll</td>
<td>No</td>
<td>Read, Write</td>
</tr>
</tbody>
</table>

Distributed-Server Configurations

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.

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

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

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

Important: Run the Unified EIM and WIM application using the same domain account that was used for installing the application (page 23).

Starting Unified EIM & WIM

There is no mandatory sequence that should be followed while starting Unified EIM & WIM. All the machines on which components are installed should be running and available on the network.

When the application starts, it automatically copies the eService.ear file from the Cisco_Home\eService\installation\ear folder on the file server to the JBoss_Home\standalone\deployments folder on each application server in the deployment.

In single-server installations:
- In the Windows Services panel, start the Cisco service to start all Cisco services.

In a distributed-server installation:
- Ensure that all the machines in the configuration are available and connected to the network.
  - Start Cisco Service on the messaging server by starting the Cisco Windows service from the Windows Services panel.
  - On the services server, start the application by starting the Cisco Windows service from the Windows Services panel.
  - On each application server, start the application by starting the Cisco Windows service from the Windows Services panel.
Stopping Unified EIM & WIM

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 Unified EIM & WIM:

- In single-server installations:

- 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.

Logging in to the Business Partition

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 log in to the business partition:

1. Ensure that you have followed the instructions in the Cisco Unified Web and E-Mail Interaction Manager Browser Settings Guide document to configure your browser, and that the desktops meet the requirements outlined in Cisco Unified Web and E-Mail Interaction Manager Solutions Reference Network Design Guide.

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 Unified WIM and Unified EIM.

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

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

These settings are of two types:

1. Mandatory settings: These settings are configured during installation, and must be verified before using the application. Settings related to ESMTP protocol, must be configured manually if you are using ESMTP protocol for email notifications.

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

Mandatory Settings

**At the partition level**

The following setting must be configured if you are using 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

The following settings are required only if you use ESMTP protocol for exception and spam emails and notifications.

- Exception mails SMTP user name
- Exception mails SMTP password
- SPAM mails SMTP user name
- SPAM mails SMTP password
- Notification mails SMTP user name
- Notification mails SMTP password

**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
- Deletion time out
- Exception email SMTP
- Exception mail redirection to address
- Exception mail redirection from address
- Expiry time for auto pushback
- Inactive time out
- SPAM mail SMTP Server
- SPAM mail redirection from address
- SPAM mail redirection to address

At the department level

- Business calendar time zone

For a complete list of all available settings, refer to the Cisco Unified Web and E-Mail Interaction Manager Administration Console User's Guide.

Uninstalling Unified EIM & WIM

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 Unified EIM & WIM. For details, refer to “Stopping Unified EIM & WIM” on page 69.

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

Uninstalling Unified EIM & WIM

**Uninstalling in Graphical Mode**

**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 Unified EIM & WIM and select Uninstall/Change.
5. In the Uninstall Unified EIM & WIM 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 Enterprise Manager 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.
SSL Configuration

- Installing a Security Certificate
- Binding the Certificate to the Application Website
- Testing SSL Access
- Configuring SSL or TLS for Retriever and Dispatcher Services
Secure Sockets Layer (SSL) is widely used to create a secure communication channel between web browsers and servers. Set up SSL for more secure connections to your Unified WIM and Unified EIM installation by following the procedures described in this chapter. If the configuration uses a load balancer, configure SSL on the load balancer.

## Installing a Security Certificate

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

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

### Generating a Certificate Signing Request

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

**To generate a certificate request:**

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

   ![Click the Create Certificate Request link]

Click the Create Certificate Request link
4. In the Distinguished Name Properties window, enter information about the company and the site to be secured:

- **Common Name**: The fully qualified domain name (FQDN) of your server. This must match exactly what users type in the web browser to get to the application. If you are using a load balancer, enter the name of the server on which the load balancer is installed.
- **Organization**: The legal name of your organization. This should not be abbreviated and should include suffixes such as Inc, Corp, or LLC.
- **Organizational Unit**: The division of your organization handling the certificate.
- **City/locality**: The city where your organization is located.
- **State/province**: The complete name of the state or region where your organization is located.
- **Country/region**: The two-letter ISO code for the country where your organization is located.

Click Next.

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

![Select a cryptographic service provider and bit length](image)
6. In the File Name window, click the Assistance ... button and browse to the location where you wish to save the certificate signing request file. Ensure that you enter a file name for the certificate signing request file. Click Finish.

Enter the location and file name

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

Submiting 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 74).

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 your web server.

Important: You need to install the certificate for the website that was specified when the web server component was installed. If you are using load balancer, install it on the load balancer server.

To install the certificate on the web server:

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

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

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

5. Verify that the certificate is added to the list of server certificates. Repeat this process on all web servers.
Binding the Certificate to the Application Website

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

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

To bind the certificate to the application URL:

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

2. In the Connections pane, select the name of the server and browse to **Sites > Web_Site_Name**.

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

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

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

Select the **Web_Site_Name**.

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

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

Testing SSL Access

To test SSL access to Unified WIM and Unified EIM:
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 Unified WIM and Unified EIM login window appears.

Configuring SSL or TLS for Retriever and Dispatcher Services

Important: This section only applies to installations that have upgraded to 11.0(3). Ignore this section if your installation has not been upgraded. For more information, see the Cisco Unified Web and E-Mail Interaction Manager Upgrade Guide for Release 11.0(3) and Cisco Unified Web and E-Mail Interaction Manager ReadMe for Release 11.0(3).
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.

If your installation has an active and a passive services server, perform these tasks on both the servers.

To configure TLS, you must:
- Install the certificates on the services servers. (page 80)

To configure SSL, you must:
- Install the certificates on the services servers. (page 80)
- Modify the alias configuration (page 81)

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:\Program Files\Java\jdk1.7_02\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 \textit{Alias\_Name} is the name you assigned to the certificate in \textbf{Step 4}.

For example, the command will look like:

\texttt{keytool -list -v -keystore ".\lib\security\cacerts" -alias emailcertificate}

8. When prompted, provide the keystore password.

The output will list the installed certificate. Once the SSL certificate is installed, the retriever process must be restarted.

\section*{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 \textit{“Installing Certificates” on page 80} to install new certificates.

\textbf{To delete a certificate:}

1. Open the Command window and navigate to the \texttt{bin} folder in the \texttt{jre} folder in \textit{JDK\_Home}, the installation folder for JDK. For example, the command will look like:

\texttt{cd C:\Program Files\Java\jdk1.7_02\jre\bin}

2. Execute the following command to delete the certificate:

\texttt{keytool -delete -alias \textit{ALIAS\_NAME} -keystore ".\lib\security\cacerts"}

where:

\textit{ALIAS\_NAME} is the name you assigned to the certificate in \textbf{Step 4}.

For example the command will look like:

\texttt{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, \texttt{changeit}.

\section*{In the Administration Console}

You need to perform these tasks only if you are using SSL. Ignore this section if you are using TLS.

\textbf{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 \texttt{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.

\begin{itemize}
  \item \textbf{Use SSL}: Set this to \texttt{Yes}.
  \item \textbf{Port}: Enter the secure port number.
\end{itemize}
Configure the alias properties

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

6. Save the changes.