Cisco Energy Management Installation Guide

Release 5.2
July, 2016

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.
Preface v
Purpose v
Audience v
Organization v
Document Conventions vi
Related Documentation vi

CHAPTER 1
Platform Overview 1-1
Overview 1-1
System Architecture 1-1
Central Server 1-2
Controllers 1-3
Asset Connectors 1-3
Asset Proxies 1-3
Application UI 1-3
API 1-3
BI Database 1-3
NOC 1-4
Deployment Options 1-4
Centralized Controllers 1-4
Distributed Controllers 1-5

CHAPTER 2
System Requirements 2-1
Server Requirements 2-1
Centralized Deployment Option 2-1
Distributed Deployment Option 2-2
Controller Requirements 2-5
Controller Files and Directories 2-6
Supported Browsers 2-7
Windows Services 2-7

CHAPTER 3
Setting up the System 3-1
Installation Checklist 3-1
Installing the Central Server 3-2
Logging in to the Application 3-3
Encrypting Data 3-3
   Using a Public Key 3-3
   Using an Application-Generated Key Pair 3-4
Downloading and Installing the Controller 3-4
   Downloading the Controller 3-4
   Installing the Controller on a Windows System 3-5
   Installing the Controller on a CentOS System 3-6
Configuring the Controller 3-7
Updating the Controller on a CentOS System 3-8
Software Updates 3-8
Controller Ports List 3-9
Running a Controller in the Simulation Mode 3-9
System Security 3-10

CHAPTER 4
Setting up the Remote Controller 4-1
   Extracting the Remote Controller File 4-1
   Generating the RSA Certificate 4-1
   Installing the Remote Controller 4-2
   Configuring the Linux Controller 4-2
   Updating the Linux Controller Settings 4-3

CHAPTER 5
Troubleshooting 5-1
   Server Login Issues 5-1
   Service Component Issues 5-2
   Controller Installation Fails 5-2
   Message Queue Connection Issue 5-2
   Unable to Gain Access to the Application 5-2
   Controller Unreachable 5-3
   Unable to Connect to the Internet via Proxy 5-3
   Windows 2003 Server Shutdown Issue 5-3
   Locked Files 5-3
Preface

This preface describes the purpose, audience, organization, and conventions in this guide, and provides information on the related documents.

- Purpose, page -v
- Audience, page -v
- Organization, page -v
- Document Conventions, page -vi
- Related Documentation, page -vi

Purpose

This guide provides instructions on installing Cisco Energy Management on Windows and Linux computers.

Audience

This guide is intended for the system administrators who install, configure, and maintain Cisco Energy Management and its key components.

Organization

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Overview</td>
<td>Provides an overview of the Cisco Energy Management platform and its deployment options.</td>
</tr>
<tr>
<td>System Requirements</td>
<td>Provides information on the system requirements for deploying the platform.</td>
</tr>
<tr>
<td>Setting up the System</td>
<td>Provides instructions on how to set up the system for use.</td>
</tr>
</tbody>
</table>
Setting up the Remote Controller

Provides information on how to install and set up a remote controller.

Troubleshooting

Provides solutions to common issues.

Server Ports

Provides a list of the ports that are used by the central server.

Settings.json

Provides information on the configuration file that contains the controller settings.

### Document Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong> font</td>
<td>Commands, keywords, and user-entered text appear in the <strong>bold</strong> font.</td>
</tr>
<tr>
<td><em>italic</em> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you assign values are in the <em>italic</em> font.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in the square brackets are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A non-quoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td><strong>courier</strong> font</td>
<td>Terminal sessions and information that the system displays appear in the <strong>courier</strong> font.</td>
</tr>
<tr>
<td><strong>courier bold</strong></td>
<td>Command names and samples appear in the <strong>courier bold</strong> font.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Non-printing characters, such as passwords, are in the angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to the system prompts are in the square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
<tr>
<td>Option &gt; Option</td>
<td>Used to describe a series of menu options.</td>
</tr>
</tbody>
</table>

**Note**

Means *reader takes note*. Notes contain suggestions or references to materials not covered in the manual.

### Related Documentation

*Cisco Energy Management User Guide*
Platform Overview

This chapter describes the architecture of the Cisco Energy Management platform and its deployment options.

- Overview, page 1-1
- System Architecture, page 1-1
- Deployment Options, page 1-4

Overview

The application can be installed on a physical or virtual machine that is running within a network that meets the minimum system requirements. As it provides remote monitoring and control capabilities to the network-connected assets, specific access credentials are required based on the type of assets being managed.

The central server hosts the central database for user management, asset data management, and report generation. It communicates with the controllers in a distributed network and hosts the web server for the application. The controller is a key component of the platform, and is responsible for direct asset communication within the network, asset import, power measurement, and policy control.

Each deployment instance requires a minimum of one controller connected to the central server. Larger deployments typically have multiple controllers deployed across different sites or locations, or even multiple controllers in the same location for large networks.

System Architecture

The core components include the central server and controllers. Each deployment requires a minimum of one controller connected to the central server. Larger deployments have multiple controllers deployed across different sites or locations, or even multiple controllers in the same location for large networks. The platform supports up to 50 concurrently active controllers per central server and a maximum of 25,000 assets per controller.

The other components include the asset connectors, asset proxies, user interface (UI), Application Programming Interfaces (APIs). Additionally, the platform enables integration with the Business Intelligence (BI) tools and Network Operations Center (NOC) systems.

Figure 1-1 illustrates the platform architecture.
Central Server

The Central Server hosts the central database for reporting and managing the user and asset data. It communicates with more than one controller in a distributed network and hosts the web server for the UI.

The following are its key components:

- **Application Server**: Provides the core functionality of the Cisco Energy Management platform and acts as the central component that interfaces with more than one controller in a distributed environment. The application server receives, processes, and stores the asset data and updates from the controllers. Additionally, it triggers alerts and notifications to the external systems, such as the NOC systems.

- **Processor**: Provides the historical and real-time reports and helps in data collection and aggregation.

- **Database**: Stores the asset data, reporting data, and policy and system configurations.

- **Message Queue**: Manages and distributes all of the incoming and outgoing messages between the application server and controllers.

- **Web Server**: Hosts files and resources for the UI and manages the service requests for the Web Service APIs.
Controllers

Controllers are responsible for direct asset communication within the network, asset import, alert management, and policy control. The controllers are available in the customer’s network to enable communication with the assets and asset management systems, which are directories with information about the assets that are in the network.

The primary function of a controller is to gather the sensor data, process it as asset data based on the defined policies and metrics, and forward the asset data to the application server for further processing and storage. Additionally, the controller modifies the asset characteristics and asset condition based on the defined policies, its processing of the sensor data, and the information that the controller receives from the application server.

Asset Connectors

Asset Connectors are a set of software tools that are used to discover and import asset data into the application with the help of the asset management systems. For example, an asset connector can import information that is related to all of the Windows computers from an asset management system, such as the Active Directory.

Asset Proxies

Asset Proxies are communication protocol drivers that enable two-way communication between the assets within a network and the key components of the Cisco Energy Management platform. The controller executes the asset proxies to retrieve data from the assets that were imported through the asset connectors.

Application UI

The UI is available for controller configuration and centralized management. You can gain access to the UI from any browser, but we recommend that you use the latest version of Mozilla Firefox or Google Chrome for the best experience.

Note

The application supports up to 25 concurrently logged-in users.

API

The application offers Web Service-based APIs that are used by the external software tools to communicate and interact with the application.

BI Database

The databases of the external BI tools receive information from the central database, which is part of the Central Server, for business analysis.
The platform can be integrated with the external BI databases, as is indicated in Figure 1-1.

**NOC**

The NOC systems use the alerts from the application server for network monitoring and incident management.

**Deployment Options**

The available deployment options depend on the location of the controllers. That is, you can deploy the platform with a central server and the controllers on the same physical or virtual host or with a central server and distributed controllers.

- **Centralized Controllers:** For up to 25,000 assets, the platform can be deployed at a centralized location where the central server and controllers reside on the same physical or virtual host.

- **Distributed Controllers:** For more than 25,000 assets, the platform can be deployed across multiple hosts with a central server and distributed controllers. Partitioning of the controllers depends on the network segments, geography, or other business requirements.

  With the distributed controllers deployment option, you can host the central server at the corporate headquarters and have the controllers distributed across subsidiaries. In this scenario, the local controllers have low-latency access to the local network to perform asset scanning and measurement, and send consolidated asset data to the central server through the Message Queue.

**Centralized Controllers**

In this deployment option, all components, such as the server, controller, message queue, database, and web server, are installed on a single server, and the installation can scale up to 25,000 assets that are accessible within a single network.

The centralized deployment is the default installation method. Figure 1-2 illustrates the this deployment option, which is recommended for small installations, pilots, and trials to get familiar with the application. You can use the standard installer to install and configure all the components.
For scaling purpose, you can add controllers to this deployment, which are connected to the existing server. You can disable the controller, which was installed for the centralized deployment option and use only the external controllers. Each controller requires access to the central Message Queue server for communication with the server, which can be configured during the installation or after the installation.

**Distributed Controllers**

The application can be deployed across multiple sites for large-scale network to achieve high performance. The platform supports geographically distributed controllers. Figure 1-3 illustrates this deployment option.
We recommend that you deploy the application across multiple servers when you must manage more than 25,000 assets. This deployment requires a central server instance and can have multiple controller instances. Each controller can handle up to 25,000 assets on a selected, high-performance hardware server. A central server can scale up to 500,000 assets on a selected, high-performance hardware server. For large-scale installations, contact Cisco Support.

The distributed controllers deployment option enables implementation of the application in geographically distributed sites or isolated networks. Individual controllers can be deployed across your organization, preferably close to the endpoints in the network, so that network traffic, latency, and scanning times are optimized. Controllers can also be deployed in isolated networks, but these controllers require a single connection with the central server through the Message Queue.

**Distributed Controllers Installation**

**Step 1** Install the central server on a high-performance hardware server. Ensure that you note the port settings for the Message Queue server.

**Step 2** Install the controller on a separate server.

**Step 3** Configure the communication between the controller and server by using the Message Queue settings. Also, ensure that the firewall and network settings are correct.

Recently added controllers automatically appear in the application under **Settings > Controllers**.

**Step 4** Repeat **Step 2** to add more controllers.
Message Queue on a Standalone Server

The integrated Message Queue can also be deployed on a standalone physical or virtual server. For more information, see the “Message Queue” section on page 2-3. The Cisco Energy Management installer does not support this installation out of the box, but the Message Queue can be downloaded directly from the website http://www.rabbitmq.com. After installation, the respective ports on the server and controllers must be changed.
System Requirements

This chapter provides information on the system requirements for deploying the platform components.

- **Server Requirements**, page 2-1
- **Controller Requirements**, page 2-5
- **Supported Browsers**, page 2-7
- **Windows Services**, page 2-7

Server Requirements

To deploy the platform on your network, follow the guidelines outlined in this section. The minimum deployment requirements depend on the number of assets.

Centralized Deployment Option

Table 2-1 lists the minimum requirements for the centralized deployment option.

<table>
<thead>
<tr>
<th></th>
<th>Minimum &lt;500 Assets</th>
<th>Up to 5,000 Assets</th>
<th>Up to 25,000 Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU</strong></td>
<td>Dual Core, 2GHz</td>
<td>Dual Core, 2GHz</td>
<td>2 Quad CPUs</td>
</tr>
<tr>
<td><strong>RAM</strong></td>
<td>4 GB</td>
<td>8 GB</td>
<td>16 GB</td>
</tr>
<tr>
<td><strong>Hard Disk</strong></td>
<td>40 GB</td>
<td>250 GB</td>
<td>500 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2012 R2 (64-bit)</td>
<td>Windows Server 2012 R2 (64-bit)</td>
</tr>
</tbody>
</table>

1Hard disk performance is critical to the deployment. We ship a database to store asset data, power measurement, and other data at a high rate. We recommend a local physical storage or high-performance SAN, especially when you deploy the controllers on virtual machines.
Distributed Deployment Option

For deployments with more than 25,000 assets, we recommend that you use servers with the following minimum requirements. Table 2-2 lists the minimum requirements for the distributed deployment option.

Table 2-2 Minimum requirements for the distributed deployment option

<table>
<thead>
<tr>
<th>Deployment component</th>
<th>up to 100,000 Assets</th>
<th>up to 200,000 Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>2 Quad CPUs</td>
<td>2 Quad CPUs</td>
</tr>
<tr>
<td>RAM</td>
<td>&gt;24 GB</td>
<td>&gt;32 GB</td>
</tr>
<tr>
<td>Hard Disk(^1)</td>
<td>1 TB</td>
<td>2 TB</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows Server 2008 R2 (64-bit)</td>
<td>Windows Server 2008 R2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2 (64-bit)</td>
<td>Windows Server 2012 R2 (64-bit)</td>
</tr>
</tbody>
</table>

\(^1\)Hard disk performance is critical to the deployment. We ship a database to store asset data, power measurement, and other data at a high rate. We recommend a local physical storage or high-performance SAN, especially when you deploy the controllers on virtual machines.

Server Components

The server provides the core functionality of the application and acts as the central component in a distributed deployment with more than one controller.

Typical tasks of the application include:

- Centralized asset and object database
- Centralized policy management
- Role-based access control
- Web Services interface
- Services for application

Application Server

Installation Directory

\%INSTALL\_DIR\%/WebApp

Configuration Files

INSTALL\_DIR%/WebApp/conf/application.conf

INSTALL\_DIR%/WebApp/conf/jemprocessor.conf

Ports (9090)

Opens port 9090 by default, which is used for internal communication from the web server to the application server. To change the application server port number, open the application.conf file in the %INSTALL\_DIR%/WebApp/conf/ path, and edit the following line:
http.port = 9090

These changes must reflect in the web server. That is, you must replace 9090 with the new port number. For more information on the Apache server, see the “Web Server (Apache)” section on page 2-4.

Reporting Data Processor

The Reporting Data Processor is a separate component within the server and provides the following functionality:

- Report data collection and aggregation
- Historical and real-time reports

**Installation Directory**

%INSTALL_DIR%/WebApp

**Configuration Files**

%INSTALL_DIR%/WebApp/conf/jemprocessor.conf

**Ports (9091)**

Opens port 9091 by default, which is used only for internal communication between the application server, report data processor, and system watcher.

Message Queue

The Message Queue is the main communication protocol between the server and controllers. For more information, see www.rabbitmq.com.

**Installation Directory**

%INSTALL_DIR%/RabbitMQ/

**Configuration File**

%INSTALL_DIR%/RabbitMQ/Data/rabbitmq.config

**Message Queue Ports & Protocols (Ports: SSL 5672/AMPQ 5673)**

The default installation configures the Message Queue with the following port settings:

- Port 5672 for SSL
- Port 5673 for AMPQ

To change the ports, edit the Message Queue configuration file. If you change the ports or address of the Message Queue, you must change the port settings in the configuration file of all the controllers. For more information, see the “Configuration File” section on page 2-5.

**Message Queue Administration Console (Port: 55672)**

The Message Queue comes with a separate, preinstalled administration console for administration and debugging purposes. By default, you can gain access to the administration console at the following address:

http://localhost:55672

This assumes that localhost is the server on which the Message Queue is installed. If you changed the port number during installation, use that port number.
Send documentation comments to cem-docfeedback@cisco.com

Web Server (Apache)

The server comes with an integrated Apache web server, which is an industry-grade secure web server. By default, the installation configures ports for HTTP as well as HTTPS for secure login. For more information, see www.apache.org.

Installation Directory

%INSTALL_DIR%/apache/

Configuration File

%INSTALL_DIR%/apache/conf/httpd.conf

Ports (HTTPS/SSL 443, HTTP 8080)

To change the web server port, open the httpd.conf file in the %INSTALL_DIR%/apache/conf/ path and edit the following lines:

```
Listen 8080
Listen 443
```

The first line indicates the port to which the rule should apply. The lines that follow the rule define that the port is an SSL secured one.

```
<VirtualHost *:443>
  ServerName localhost
  DocumentRoot "%INSTALL_DIR%/apache/htdocs"
  SSLEngine On
  SSLCertificateFile conf/cert.pem
  SSLCertificateKeyFile conf/key.pem
  <IfModule !mpm_netware_module>
    <IfModule !mpm_winnt_module>
      User daemon
      Group daemon
    </IfModule>
  </IfModule>
</VirtualHost>
```

The first line indicates the port to which the rule should apply, the lines that follow the rule define that it is a non-secured port.

```
<VirtualHost *:8080>
  ServerName localhost
  DocumentRoot "%INSTALL_DIR%/apache/htdocs"
  <IfModule !mpm_netware_module>
    <IfModule !mpm_winnt_module>
      User daemon
      Group daemon
    </IfModule>
  </IfModule>
</VirtualHost>
```

As IE 8 on Windows XP uses the RC4 cipher, you must edit the httpd.conf file. That is, replace the existing SSLCipherSuite with the following:

```
SSLCipherSuite ECDH+ECDSA+AESGCM ECDH+aRSA+AESGCM ECDH+ECDSA+SHA384
ECDH+ECDSA+SHA256 ECDH+aRSA+SHA256 ECDH+aRSA+SHA384 ECDH+aRSA+SHA256
ECDH+aRSA+RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS
```

Note: Use of RC4 is not recommended because it is a weak cipher and presents security concerns.
Database Server (PostgreSQL)

The server has an integrated database server (PostgreSQL) to store the asset data, policy and system configuration, and reporting data. PostgreSQL is an industry-grade, reliable database server, which is installed automatically along with the server. For more information about PostgreSQL, see www.postgresql.org.

Installation Directory

%INSTALL_DIR%/pgsql/

Configuration File

%INSTALL_DIR%/pgsql/data/pgsql.conf

Ports (5432)

The default port for PostgreSQL server is 5432, which can be changed during installation. To change the port or authentication settings afterwards, edit the PostgreSQL configuration file.

```shell
# CONNECTIONS AND AUTHENTICATION
#---------------------------------------------------------------
port = 5432
```

Configuration File

The server configuration file contains multiple configuration options, for instance, ports, message queue endpoints, and backup options.

File Location

%INSTALL_DIR%/WebApp/conf/jemprocessor.conf

Database Settings

The configuration options for the database need to be changed if changes are made to the database configuration.

```
jdbc.host=localhost
jdbc.port=5432
jdbc.username=postgres
jdbc.password=*****
```

Message Queue Settings

```
queue.hostname = 127.0.0.1
queue.port = 5672
queue.management.port = 55672
```

Controller Requirements

Table 2-3 lists the minimum requirements for the controller.
**Controller Files and Directories**

**Base Directory**

The controller is installed in the Programs directory. You can change the location during the installation process. All of the important files and sub directories are created inside this default directory.

**Important Directories**

All of the important directories and files can be found at: %INSTALL_DIR%/service. Table 2-4 lists these directories.

<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/acfiles</td>
<td>Contains the import files for the CSV asset connector.</td>
</tr>
<tr>
<td>/commands</td>
<td>Location for commands and executable, which are safe to be called from the</td>
</tr>
<tr>
<td></td>
<td>script through runCommand. The administrator must create this directory, as</td>
</tr>
<tr>
<td></td>
<td>it not created by default.</td>
</tr>
<tr>
<td>/edata</td>
<td>TruJoule database signatures.</td>
</tr>
<tr>
<td>/jemupdate</td>
<td>Used by the jemupdate tool for software update, including logs.</td>
</tr>
<tr>
<td>/script</td>
<td>Internal scripts used by a controller to perform remote operations.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Do not modify internal files, as they will be overwritten with a</td>
</tr>
<tr>
<td></td>
<td>software update.</td>
</tr>
<tr>
<td>/PluginProxies</td>
<td>For more information on the asset proxies, see the Cisco Energy Management</td>
</tr>
<tr>
<td></td>
<td><strong>User Guide.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Do not modify internal files, as they will be overwritten with a</td>
</tr>
<tr>
<td></td>
<td>software update.</td>
</tr>
</tbody>
</table>

**Table 2-3 Controller Requirements**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Minimum (up to 25,000 assets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Quad Core, 2GHz</td>
</tr>
<tr>
<td>RAM</td>
<td>4 GB</td>
</tr>
<tr>
<td>Hard Disk</td>
<td>50 GB</td>
</tr>
<tr>
<td>Operating System</td>
<td>Microsoft Windows 7 (32-bit and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows Server 2008 R2 (32-bit and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>Linux CentOS 6.5 and 6.7</td>
</tr>
<tr>
<td>Java SE Runtime</td>
<td>Oracle Java x86 or x64 version 8</td>
</tr>
</tbody>
</table>
Send documentation comments to cem-docfeedback@cisco.com

Table 2-4 List of Important Directories

<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/sshkeys</td>
<td>SSH private keys are used to execute SSH commands on assets.</td>
</tr>
<tr>
<td>/jemscrip t</td>
<td>Contains script files, which can be loaded through the script function, include(). By default, the application comes with predefined scripts in this folder. Also, user-defined and custom scripts can be placed in this folder.</td>
</tr>
</tbody>
</table>

Note: Do not modify internal files, as they will be overwritten with a software update.

Supported Browsers

For better user experience, we recommend that you use the latest versions of browsers, such as Google Chrome, Mozilla Firefox, and Internet Explorer. Older browsers, such as Internet Explorer 8, are not fully supported. Regardless of which browser you use, ensure that you enable JavaScript.

Note: The application does not support browsers on mobile devices, such as tablets and smartphones.

Windows Services

Cisco Energy Management consists of some Windows services, which run in the background and are configured to automatically start when the system is started. You can also stop, restart, or pause these services. However, stopping or pausing any of these services could cause the application to not operate properly.

The controller installs two services: Controller and Controller Watcher. The server installs six services: Database, Message Queue, Processor, Server, System Watcher, and Web Server. These services are listed in Table 2-5.

Table 2-5 Services

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Energy Management Controller</td>
<td>For more information, see the “Controller Requirements” section on page 2-5.</td>
</tr>
<tr>
<td>Cisco Energy Management Controller Watcher</td>
<td>Monitors the controller service.</td>
</tr>
<tr>
<td>Cisco Energy Management Database</td>
<td>Database server (PostgreSQL). For more information, see the “Database Server (PostgreSQL)” section on page 2-5.</td>
</tr>
<tr>
<td>Cisco Energy Management Server</td>
<td>Application server.</td>
</tr>
<tr>
<td>Cisco Energy Management Processor</td>
<td>Reporting Data Processor. For more information, see the “Reporting Data Processor” section on page 2-3.</td>
</tr>
<tr>
<td>Cisco Energy Management Message Queue</td>
<td>Message Queue. For more information, see the “Message Queue” section on page 2-3.</td>
</tr>
</tbody>
</table>
To view the Windows Services:

1. Click the Windows Start button.
2. Enter `services.msc`.
3. Press Enter.

Verify that all of the services have the status as started. You can start, stop, restart, or pause these services only if you have administrative rights.

### Table 2-5: Services

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Energy Management Web Server</td>
<td>Apache web server. For more information, see the “Web Server (Apache)” section on page 2-4.</td>
</tr>
</tbody>
</table>

Setting up the System

This chapter describes the process for setting up Cisco Energy Management.

- Installing the Central Server, page 3-2
- Logging in to the Application, page 3-3
- Encrypting Data, page 3-3
- Downloading and Installing the Controller, page 3-4
- Configuring the Controller, page 3-7
- Updating the Controller on a CentOS System, page 3-8
- Software Updates, page 3-8
- Controller Ports List, page 3-9
- Running a Controller in the Simulation Mode, page 3-9
- System Security, page 3-10

Installation Checklist

Table 3-1 lists the steps that you must perform to set up Cisco Energy Management.

<table>
<thead>
<tr>
<th>Step</th>
<th>Setting up</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install the central server</td>
<td>Installing the Central Server, page 3-2</td>
</tr>
<tr>
<td>2. Log in to the application</td>
<td>Logging in to the Application, page 3-3</td>
</tr>
<tr>
<td>3. Encrypt sensitive data, such as passwords</td>
<td>Encrypting Data, page 3-3</td>
</tr>
<tr>
<td>4. Install the controller</td>
<td>Downloading and Installing the Controller, page 3-4</td>
</tr>
<tr>
<td>5. Configure the controller</td>
<td>Configuring the Controller, page 3-7</td>
</tr>
<tr>
<td>6. Update the controller (Linux only)</td>
<td>Updating the Controller on a CentOS System, page 3-8</td>
</tr>
</tbody>
</table>
Installing the Central Server

To install the central server, perform the following steps:

**Step 1** Download the server installation file from the following software downloads page:

**Step 2** Run the setup file on the system where you want to install the server.

**Step 3** On the welcome page of the installation wizard, click **Next**.

**Step 4** Accept the terms on the License Agreement page, and click **Next**.

**Step 5** On the Create Account page, perform the following steps:

a. Set the login credentials for accessing the application by entering the login user name in the **Username** text box and password in the **Password** and **Re-enter Password** text boxes.

b. In the **Web-Port (SSL)** and **Web-Port** text boxes, enter the port numbers for the HTTPS and HTTP connections respectively, and then click **Next**.

   The default values for these fields are 443 and 8080. If port 443 is unavailable, you can use another port, such as 8443. You can also reconfigure or uninstall the program that is using port 443.

**Step 6** On the Port Configuration page, change the default port numbers, if required, for the following server components, and click **Next**:

- Message Queue Port (SSL): 5672
- Message Queue Management Port: 55672
- Server: 9090
- Database: 5432

If Windows Firewall is turned off or disabled, you must manually open these ports.

**Step 7** On the Installation Options page, enter the credentials for the message queue server, and click **Next**.

**Step 8** On the Select Installation Path page, choose the folder where you want to install Cisco Energy Management, and click **Install**.

**Step 9** Click **Next**, and then click **Finish** to exit the installation wizard.

To verify if the server is installed successfully, check if the following services are running in the Windows Services console:

- Cisco Energy Management Database
- Cisco Energy Management Message Queue
- Cisco Energy Management Processor
- Cisco Energy Management Server
- Cisco Energy Management System Watcher
- Cisco Energy Management Web Server
Logging in to the Application

You can gain access to the application through the standard browsers. For more information, see the “Supported Browsers” section on page 2-7.

To log in to application, perform the following steps:

**Step 1** Enter the following URL:

https://localhost

The application login page appears.

To gain access to the application from a remote location, enter the IP address or hostname of the remote system on which you have installed the server. For example:

https://<server-ip>: port

https://<hostname>: port

**Step 2** On the application login page, enter the login credentials that you created during server installation, and click Login.

When you log in to the application for the first time, you must configure the data encryption settings. Subsequent logins will start the application directly.

Encrypting Data

The application uses public key encryption with PKCS 12 key files to encrypt sensitive data, such as passwords. You can upload the public key of an existing PKCS key pair to the server or use an application-generated key pair. The key pair is a PEM format base64 encoded file. Therefore, to use your key pair for data encryption, ensure that you have the public key of your key pair in the PEM format.

*Note* The application does not store the private key of the key pair.

Using a Public Key

To upload the public key of your key pair, perform the following steps:

**Step 1** Read the instructions on the Configure Data Encryption Settings page, and click Next.

**Step 2** Select the recommended option. That is, select the first radio button, and click Next.

**Step 3** Use one of the following methods to import the public key of your key pair to the server:

- Copy the public key and paste it in the text field.
- Click Browse, and choose the public key file.

**Step 4** Click Import Public Key.
If the server imports the public key, you will see an Import successfully completed message in place of Import Public Key.

**Step 5**  
Click Launch Application.  
The application starts and the setup wizard launches.

---

**Using an Application-Generated Key Pair**

To use an application-generated key pair for data encryption, perform the following steps:

**Step 1**  
Read the instructions on the Configure Data Encryption Settings page, and click Next.

**Step 2**  
Select the second radio button, and click Next.

**Step 3**  
Read the instructions, and click Generate Key Pair.  
The file with the application-generated key pair will be downloaded to your system.

**Step 4**  
Save the file, and select the Yes, I have downloaded the keypair file and stored it in a secure place check box.

⚠️  
**Caution**  
You cannot install the controller without a key pair.

**Step 5**  
Click Launch Application.  
The application starts and the setup wizard launches.

---

**Downloading and Installing the Controller**

After completing the data encryption configuration, install the controller to monitor and manage the assets in your network. Download the controller for Windows or CentOS from the software download page at:


---

**Downloading the Controller**

You can download and install the controller by following the instructions provided in the setup wizard or install the controller later. If you want to install the controller later, click Settings > Controllers on the application user interface, and then click Install New Controller.

To download the controller, perform the following steps:

**Step 1**  
(Optional) On the setup wizard page, type the name of your company in the Your Company field, and click Next.  
You can skip this step and complete it later.

**Step 2**  
On the Controller Detection page, click Install Controller(s).
Chapter 3  Setting up the System

Downloading and Installing the Controller

The Controller Credentials page appears.

Step 3  Copy and save the controller credentials.

Step 4  Select the Yes, I got the credentials check box to confirm that you have saved the credentials, and click Next.

**Caution**

The controller credentials are required to install the controller. If you do not save the credentials, you cannot install the controller.

Step 5  Click Download Controller.

The software download page appears.

Step 6  Click Download, and save the file to your system.

Installing the Controller on a Windows System

For monitoring Windows assets in the application, the controller requires Microsoft .NET 4.0 framework. This framework should be installed on the server prior to the installation. Otherwise, the framework will be automatically downloaded and installed as part of the controller installation.

If the Internet connection on the installation server is slow or unavailable, it is recommended that you manually download and install the Microsoft .NET 4.0 framework before you install the controller installation. You can download and install Microsoft .NET 4.0 framework from the following path:


**Note**

If you have manually defined port 80 as an HTTP port, you cannot activate Internet Information Services (IIS).

To install the controller on a Windows system, perform the following steps:

Step 1  Run the downloaded controller file on the system where you want to install the controller.

The controller installation wizard starts.

Step 2  On the welcome page of the Controller Wizard, click Next.

Step 3  Accept the terms of the license agreement, and click Next.


Step 5  Enter the host and credentials for the Message Queue server, and click Next.

If you change the port number of the Message Queue server, enter that port number in the Port text box.

Step 6  Click the ellipsis icon to select your private key file, and click Next.

The private key file is used to encrypt and decrypt your passwords.

Step 7  Click Browse to select the destination folder where you want to install the controller, and click Install.

Step 8  Click Next after the controller installation is complete.
Installing the Controller on a CentOS System

Prerequisites:

- Ensure that you install the central server. For more information, see the “Installation Checklist” section on page 3-1.
- Ensure that the wget and netcat utility packages are installed on the CentOS system.
- Ensure that you install Oracle Java SE Runtime Environment 8. Download the latest Linux x64 or x86 JRE version 8 .rpm file from http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html
  
  Use the following command to install the package:

  ```bash
  yum install /<path> jre-8u<x>-linux-x<64/86>.rpm
  ```

- Ensure that you have root privileges.
- Ensure that you have the key pair file.

To install the controller on a CentOS system, perform the following steps:

**Step 1**
Log in to the CentOS system.

**Step 2**
Go to the folder that contains the downloaded file. For example, if the controller installation file is in your Downloads folder and your folder structure is /home/admin/Downloads, enter the following command:

```bash
cd /home/admin/Downloads
```

**Step 3**
Enter one of the following commands to install the controller:

```bash
sudo yum install cem-controller-<version>.rpm
```

or

```bash
rpm -ivh cem-controller-<version>.rpm
```

The controller package is extracted and installed in the /var/lib/ewcontroller folder. The folder contains a template, cem-controller.onpremise.init.sample, for reuse.

**Step 4**
Enter the following command to use the template to create a ewcontroller.init file in the /ewcontroller folder.

```bash
sudo cp /var/lib/ewcontroller/ewcontroller.onpremise.init.sample /var/lib/ewcontroller/ewcontroller.init
```

Use a text editor of your choice to edit the ewcontroller.init file, which contains the following details:

- `ctrllogdir="<Local path of the log directory>"`
  
  You can leave this path empty, in which case, the default path applies. The default path is:
  
  `/var/log/ewcontroller`

- `mqip="<IP of the Message Queue>"`
Configure the Controller

After you install the controller, it connects to the server and a New Controller Detected dialog box appears. You can now configure the controller. For example, you can assign folders to the controller.

To assign folders to a controller, go to Settings > Controllers > Edit Settings > Folder Assignment or perform the following steps:

Step 1 On the Controller Detection page, click Start Controller Setup.

The name of the detected controller appears.

Step 2 Click Next to continue.

Step 3 Click Manage Folders to assign a folder to the controller.

Step 4 Click Choose Folder in the Edit Assigned Folders dialog box.

Step 5 Choose the default folder or select an existing folder in the Select Folder dialog box. You can also create a folder.
Setting up folders enable you to manage multiple controllers that are deployed across different sites or locations, or even multiple controllers in the same location for large networks.

**Step 6** Click OK, and then click Next.

**Step 7** Enter a valid license key to activate the application in the Activate Your License dialog box, and click Next.

**Note** You must have an Internet connection so that the server can connect to the license server and register the controller. As the license server listens on port 443, ensure that the port is not blocked by a proxy or firewall. For more information, see Appendix A “Server Ports.”

**Step 8** Choose the access mode from the Windows Access Method drop-down menu in the Controller Options dialog box.

**Step 9** Click Next, and click Finish to complete the controller configuration.

### Updating the Controller on a CentOS System

To update a controller on a CentOS system, download the latest controller rpm package file from the software download page and manually update the controller.

To update the controller, perform the following steps:

**Step 1** Download the latest version of the controller rpm file from the software download page at: https://cem-update.cisco.com/download/index.html

**Step 2** Go to the folder where the rpm file is downloaded, and run the following command to update the controller.

```
yum update EnergyWise-Controller-<version>.rpm
```

### Software Updates

The application supports automatic software updates, which are disabled by default. However, we recommend that you enable this feature to receive the latest updates.

To enable software updates, perform the following steps:

**Step 1** On the application user interface, click **Settings > Controllers**.

The Controller Management page appears.

**Step 2** Click **Edit Settings**.

The Controller Settings page appears with tabs, such as Folder Assignment, Software Updates, License Information, and Controller Health, in the left pane.

**Step 3** On the left-navigation pane, click **Software Updates**.
Step 4  Select the **Enable automatic updates** check box.

Step 5  (Optional) Click **Change** to schedule the update and its frequency.

Step 6  (Optional) Select the **Notify only** check box to receive notifications for the available updates.

Step 7  (Optional) Select the **Hotfixes only** check box to automatically update minor releases and hotfixes.

---

**Controller Ports List**

<table>
<thead>
<tr>
<th>Application</th>
<th>Port</th>
<th>Protocol</th>
<th>Encryption</th>
<th>Usage/Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller</td>
<td>8000/TCP</td>
<td>HTTP</td>
<td>No</td>
<td>Only for internal use.</td>
</tr>
<tr>
<td></td>
<td>localhost</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 3-3  Outbound Connection**

<table>
<thead>
<tr>
<th>Application</th>
<th>Port</th>
<th>Protocol</th>
<th>Encryption</th>
<th>Usage/Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Queue Server</td>
<td>5672</td>
<td>SSL</td>
<td>Yes</td>
<td>Depends on the configuration of the Message Queue endpoint on the server.</td>
</tr>
</tbody>
</table>

---

**Running a Controller in the Simulation Mode**

Instead of measuring and managing real assets, you can run the controller in the simulation mode for testing purpose.

To activate the simulation mode, perform the following steps:

---

**Step 1**  On the application user interface, click **Settings > Controllers**.

The Controller Management page appears. If a controller is available, the controller details appear on the page.

**Step 2**  Click **Edit Settings**.

The Controller Settings page appears with tabs, such as Folder Assignment, Software Updates, License Information, and Controller Health, in the left pane.

**Step 3**  On the left-navigation pane, click **Settings**.

The System page appears with the Add, Show Settings, and Edit tabs.

**Step 4**  Click **Show Settings > Advanced**.

**Step 5**  Click the arrow that is adjacent to the **General** tab to view the available properties.
System Security

Password Strength
We recommend that you harden the system by configuring password strength in the jemprocessor.conf file that is stored in the %INSTALL_DIR%/WebApp/conf directory of the server installation.

To configure password strength, set the cisco.password.policy.enabled property to true. To customize password requirements, add any of the properties that are listed in Table 3-4.

<table>
<thead>
<tr>
<th>Password Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisco.password.policy.minlength</td>
<td>The minimum number of characters that are required. The default is 8 characters.</td>
</tr>
<tr>
<td>cisco.password.policy.maxlength</td>
<td>The maximum number of characters that are allowed. The default is 127 characters.</td>
</tr>
<tr>
<td>cisco.password.policy.cisco</td>
<td>Prevents users from entering cisco or its variants, such as cISco, as the password. The default is true. Set the property to false to disable it.</td>
</tr>
<tr>
<td>cisco.password.policy.username</td>
<td>Prevents users from entering the username or its variants, such as the username in reverse, as the password. The default is true. Set the property to false to disable it.</td>
</tr>
<tr>
<td>cisco.password.policy.repetition</td>
<td>Prevents users from repeating the same character, in sequence, more than twice. The default is true. Set the property to false to disable it.</td>
</tr>
<tr>
<td>cisco.password.policy.fourgroups</td>
<td>Requires users to enter at least one lower case letter, upper case letter, number, and a special character. The default is true. Set the property to false to disable it.</td>
</tr>
</tbody>
</table>

OS Hardening
For hardening guidelines on the operating system that you use, see the following links:

- CentOS 6.x: https://wiki.centos.org/HowTos/OS_Protection#head-b3126b7267f04dc869a18f3547468727e82308d1
System Security

Audit Logging

Activate audit logging to view events related to user login and logout, script execution, change of user roles, permissions, and server start and stop. To activate audit logging, go to the log4j.properties file that is in the %INSTALL_DIR%\WebApps\conf directory of the server installation and add the following:

```
log4j.logger.com.cisco.energywise.management.audit=INFO, AUDIT
log4j.additivity.com.cisco.energywise.management.audit=false
log4j.appender.AUDIT = org.apache.log4j.RollingFileAppender
log4j.appender.AUDIT.File = %INSTALL_DIR%\logs\Audit.log
log4j.appender.AUDIT.MaxFileSize = 50MB
log4j.appender.AUDIT.MaxBackupIndex = 100
log4j.appender.AUDIT.layout = org.apache.log4j.PatternLayout
log4j.appender.AUDIT.layout.ConversionPattern = %m%n
```

Where %INSTALL_DIR% is the installation path. For example, C:\Program Files\Cisco Energy Management. The audit.log file, which the application stores in the logs folder, is in the CSV format. It has two primary entries, Login or Logout Events and Object Updates, with the following subentries:

**Login or Logout Events**

- Timestamp, in UTC
- Tenant ID
- Operation, such as login, logout, or login attempt
- Username
- IP Address
- Description

The following is an example:

```
2016/06/24
12:53:04;bd00d875b5294bd683523f19601f3b42;LOGOUT;tester;unknown;;;"{"reason":"I
DLE_TIMEOUT"}"
```

**Object Updates**

- Timestamp, in UTC
- Tenant ID
- Operation, such as insert, update, or delete
- Username
- IP Address
- Change Object Label
- Change Object ID
- Change Object Type
- Description

The following is an example:

```
2016/06/24
15:08:55;bd00d875b5294bd683523f19601f3b42;INSERT;system;127.0.0.1;jdoe;2f56dc4d16d7
4d7995e7f12854633a1;user;{""auth-tokens"":[""9f06443c46c84...""],""reason""":""API
""}"
```
Send documentation comments to cem-docfeedback@cisco.com
Setting up the Remote Controller

This chapter provides information on how to install and set up a remote controller for Cisco Energy Management. A remote controller is required for integrating Windows Management Instrumentation (WMI) assets in the application with a Linux controller.

The following are the main tasks for completing the remote controller installation and setup:

1. Extracting the Remote Controller File, page 4-1
2. Generating the RSA Certificate, page 4-1
3. Installing the Remote Controller, page 4-2
4. Configuring the Linux Controller, page 4-2
5. Updating the Linux Controller Settings, page 4-3

**Note**
Install a remote controller only after you install the Linux controller and ensure that it is running.

### Extracting the Remote Controller File

To install the remote controller, copy the RemoteController.zip file from the Linux computer where the Linux CentOS controller is installed and extract the zip file in the Windows system where you need to install the remote controller. The RemoteController.zip file contains all the necessary files to install the remote controller.

The RemoteController.zip file is located in the /var/lib/ewcontroller folder of your Linux computer. Copy this file to your local Windows computer where you need to install the remote controller and then extract the zip files.

### Generating the RSA Certificate

Before you install the remote controller, you must generate the RSA certificate, which will secure the connection between the Linux Controller and the remote controller.

To generate the RSA certificate, perform the following steps:

**Step 1**
After extracting the RemoteController.zip file, run the generateCertificate.bat file.
Ingredients in this recipe...
JAVA_PARAMS=-Djavax.net.ssl.trustStore=remoteController.ks
-Djavax.net.ssl.trustStorePassword='<your password>''

Where your password is the password that you entered when you generated the RSA certificate. For example, if you used the default password as secret, add the following line to the java.params file:

JAVA_PARAMS=-Djavax.net.ssl.trustStore=remoteController.ks
-Djavax.net.ssl.trustStorePassword='secret''

**Step 3**  
Save the java.params file.

**Step 4**  
Type the following command in the command prompt to restart the controller:

```
service ewcontroller restart
```

### Updating the Linux Controller Settings

After you configure the Linux controller settings with the remote controller information, update the controller settings of the Linux controller in the application.

To update the controller settings in the application, perform the following steps:

**Step 1**  
On the application user interface, click **Settings > Controllers**.

The Controller Management page appears.

**Step 2**  
For the associated controller, click **Edit Settings**.

**Step 3**  
From the left-navigation page, click **Settings**.

**Step 4**  
In the Settings page of the controller, click **Show Settings > Advanced**.

**Step 5**  
Search for the Remote Controller Settings property, and double-click the property name to edit it.

**Step 6**  
In the Edit JSON dialog box, replace the `host` property with the IP address of the Windows system where you installed the remote controller.

**Step 7**  
Click **OK** to close the dialog box.

The Linux controller is now set up to integrate the WMI assets in the application.
Troubleshooting

This chapter provides solutions to common issues that you might encounter when you use the Cisco Energy Management application.

- Server Login Issues, page 5-1
- Service Component Issues, page 5-2
- Controller Installation Fails, page 5-2
- Message Queue Connection Issue, page 5-2
- Unable to Gain Access to the Application, page 5-2
- Controller Unreachable, page 5-3
- Unable to Connect to the Internet via Proxy, page 5-3
- Windows 2003 Server Shutdown Issue, page 5-3
- Locked Files, page 5-3

Server Login Issues

No login screen / No connection to server
If you do not have an Internet connection, you will see an error message instead of the login page of the application. To troubleshoot the issue, do the following:

- Check the server address and the specified port in the browser URL field.
- Enter the URL, https://localhost, in the address bar to gain access to the application user interface.

Note Use the port number that you entered during the installation.

- From the Windows Start menu, go to Administrative Tools > Services and verify that the web server is running.

Login failed: Service unavailable - Server is probably not running
This happens when you have access to the web server, but the server is not working properly. From the Windows Start menu, go to Administrative Tools > Services to manage the Windows services. Then, locate the Cisco Energy Management services in the list and verify that all services are running.
Service Component Issues

Q. Why does the application report no login screen or no connection to server when logging in to the server?
A. Check if the server is running.

Q. Why does the application report that no reporting data is available when logging into the server?
A. Check if the processor is running.

Q. Why does the application report timeout when starting the services?
A. The application reports timeout when the number of assets connected to the physical machine is approximately 100,000 or more. It also reports timeout due to the performance of the physical machine.

Controller Installation Fails

If you are unable to install the local controller or the controller does not respond and you see an error indicating that the controller cannot be verified, check if the controller is installed on a server that is compatible with the application. For example, the application is incompatible with Windows Vista or MS Windows 2003.

Ensure that you have the following minimum server requirements:
- CPU: Quad Core, 2 GHz
- RAM: 4 GB
- Hard Disk: 50 GB
- Operating System: Windows 7 or Server (64-bit)

Message Queue Connection Issue

If you see the following error message:

Could not connect to Message Queue. Would you like to change your configuration?

Ensure the following:
- No prior versions of the application are installed.
- Port 5672 is available on the network firewall from the controller to the application. The port might be open on the local computer, but it is not open on an upstream firewall.

Unable to Gain Access to the Application

If the browser displays an HTTP error when you try to gain access to the application URL, ensure that port 443 is open from your network to the application. You can also do the following:
- Refresh the browser.
- Ensure that the CapsLock key is off and re-enter your username and password.
Controller Unreachable

If the controller wizard fails to start after you log in to the application, restart the controller as follows:

1. On the local machine, go to Start > Control Panel > Administrative Tools > Services.
2. Stop and restart the following services:
   - Cisco Energy Management Controller Watcher
   - Cisco Energy Management Controller

Unable to Connect to the Internet via Proxy

If the connection times out, check the URL syntax of the proxy server address. It must be: proxy_ip:port.

Windows 2003 Server Shutdown Issue

Q. Why does the application report the `Win32Shutdown failed with 21` error when shutting down the Windows 2003 Server?

A. When shutting down the Windows Server 2003 or Windows XP x64 server, you must login as a user to avoid experiencing difficulties. You also need to install the hotfix that is provided by Microsoft. Only a single version for Windows Server 2003 is available for download at [http://support.microsoft.com/kb/834100](http://support.microsoft.com/kb/834100).

Locked Files

**Indication**

- Controller services do not start and no log entries are made to the controller.log file.
- Windows EventLog contains the following error:

  ```
  Could not load Controller configuration 'C:\%InstallDir%\Service\settings.json' - System.IO.IOException: The process cannot access the file 'C:\%InstallDir%\logs\controller.log' because it is being used by another process.
  ```

Ensure that the controller.log file or any other file that is referred in the error message is not opened by another process. To find out which other process has locked the file, use a tool called Process Explorer by Microsoft.

**Prevention**

Use only the log file viewers and text editors that do not explicitly lock the file. For example, use the following:

- LogMX
- Notepad++
- Lister integrated in TotalCommander
Locked Files

Send documentation comments to cem-docfeedback@cisco.com
Server Ports

The central server installs a number of components and additional services. Many ports can be defined during installation. Table A-1 lists the ports and network addresses opened or used by the central server.

<table>
<thead>
<tr>
<th>Application</th>
<th>Ports</th>
<th>Protocol</th>
<th>Encryption</th>
<th>Usage/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Server</td>
<td>9090 localhost only</td>
<td>HTTP</td>
<td>No</td>
<td>Internal local communication between central management application and web server.</td>
</tr>
<tr>
<td>Reporting Data Processor</td>
<td>9091 localhost only</td>
<td>HTTP</td>
<td>No</td>
<td>Internal local communication.</td>
</tr>
<tr>
<td>Message Queue</td>
<td>5672 (Default)</td>
<td>AMQP</td>
<td>SSL</td>
<td>Message Queue server for communication with controllers.</td>
</tr>
<tr>
<td></td>
<td>5673 (Default)</td>
<td>AMQP</td>
<td>No</td>
<td>Unused by the application. Mandatory for the Message Queue.</td>
</tr>
<tr>
<td></td>
<td>55672 (Default)</td>
<td>HTTP</td>
<td>No</td>
<td>The Message Queue administration console.</td>
</tr>
<tr>
<td>Web Server (Apache)</td>
<td>443 (Default)</td>
<td>HTTPS</td>
<td>SSL</td>
<td>Web server for browser-based user interface, API, and reporting.</td>
</tr>
<tr>
<td></td>
<td>8080</td>
<td>HTTP</td>
<td>No</td>
<td>Not secure. Port forwarding to 443.</td>
</tr>
<tr>
<td>Database Server (PostgreSQL)</td>
<td>5432 (Default) local host only</td>
<td>TCP</td>
<td>No</td>
<td>The application automatically installs a PostgreSQL database server.</td>
</tr>
</tbody>
</table>

The server uses outbound connections for standard functionality. Outbound communication with controllers is done through the Message Queue, and is not listed in Table A-2 as no extra ports will be opened.
### Table A-2: Outbound Connections

<table>
<thead>
<tr>
<th>Destination</th>
<th>Destination Ports</th>
<th>Protocol</th>
<th>Encryption</th>
<th>Usage/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Server</td>
<td>443/TCP</td>
<td>HTTPS</td>
<td>Yes</td>
<td>Depending on the email settings, the application sends emails for notifications and alerts to the mail server provided in the configuration.</td>
</tr>
<tr>
<td>LDAP / Active Directory</td>
<td>1443/TCP</td>
<td>LDAP</td>
<td>Yes</td>
<td>Depending on the user management settings, the application connects to the Active Directory or LDAP servers to read user and user groups.</td>
</tr>
<tr>
<td>Licensing Server</td>
<td>443/TCP</td>
<td>HTTPS</td>
<td>Yes</td>
<td>The License Server holds information about your licensed installation. Its service address is <a href="https://license.joulex.net/LicenseServer/activate">https://license.joulex.net/LicenseServer/activate</a>. Ensure that the port is not blocked by a proxy or firewall.</td>
</tr>
<tr>
<td>Software Update Server</td>
<td>443/TCP</td>
<td>HTTPS</td>
<td>Yes</td>
<td>The application supports automated software updates so that your installation is always the current version. Its service address is <a href="https://update.joulex.net/UpdateServer/checkUpdate">https://update.joulex.net/UpdateServer/checkUpdate</a>. Ensure that the port is not blocked by a proxy or firewall.</td>
</tr>
<tr>
<td>TruJoule Server</td>
<td>443/TCP</td>
<td>HTTPS</td>
<td>Yes</td>
<td>The application TruJoule Server keeps the energy profile database up to date. Its service address is <a href="https://trujoule.joulex.net/TruJoule/upload">https://trujoule.joulex.net/TruJoule/upload</a>. Ensure that the port is not blocked by a proxy or firewall.</td>
</tr>
<tr>
<td>Support Requests</td>
<td>443/TCP</td>
<td>HTTPS</td>
<td>Yes</td>
<td>The service address is <a href="https://update.joulex.net/SupportRequester/check">https://update.joulex.net/SupportRequester/check</a>. Ensure that the port is not blocked by a proxy or firewall.</td>
</tr>
</tbody>
</table>
Settings.json

The settings.json file contains the controller settings that are set when the controller is installed, and these are the startup parameters for the controller that cannot be changed while the controller is running. This file is stored in the `%INSTALL_DIR%\service\` directory of the controller installation.

The server communicates with the controllers through the Message Queue. Therefore, if you change the Message Queue port number, you must update the settings.json file to reflect these changes. Additionally, any configuration changes after the initial setup must reflect in the settings.json file, without which, the controllers will be unable to communicate with the server.

Table B-1 lists the controller settings and their description.

---

**Note**

Changing the default values can cause the application to malfunction.

**Table B-1 Controller Settings and Default Values**

<table>
<thead>
<tr>
<th>Controller Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Internal identifier for a controller instance.</td>
<td>Do not change</td>
</tr>
<tr>
<td>webServiceThreadCount</td>
<td>Defines the number of Web Service threads.</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Do not change</td>
</tr>
</tbody>
</table>

**Database Settings**

<table>
<thead>
<tr>
<th>Database Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>databaseSettings</td>
<td>Database settings to access the PostgreSQL database.</td>
<td>—</td>
</tr>
<tr>
<td>deleteOlderThan</td>
<td>Number of days after which to delete the asset data lock fields.</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Change only if necessary</td>
</tr>
<tr>
<td>maintenanceStartTime</td>
<td>Time at which the daily maintenance schedule takes place.</td>
<td>00:30</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Change only if necessary</td>
</tr>
<tr>
<td>jdbcDriver</td>
<td>Name of the jdbc driver.</td>
<td>org.h2.Driver</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Do not change</td>
</tr>
<tr>
<td>jdbcUrl</td>
<td>Basic settings for jdbc.</td>
<td>Do not change</td>
</tr>
</tbody>
</table>
## Appendix B Settings.json

**lockFile** Path where the database lock file is located. \
\`\`\`db\emdata.lock.db  
Do not change

**databaseDir** Folder of the database installation  
\`\`\`db  
Do not change

**logDir** Specifies the directory where the controller log files are stored.  
%INSTALL_DIR%\logs  
Change only if necessary

**blur** Encryption key for all passwords in database or configuration file. Not to be shared.  
Do not change

**blurOld** Old encryption key used for pre-4.0 passwords.  
Do not change

### Message Queue Settings

<table>
<thead>
<tr>
<th>Controller Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Message Queue host.</td>
<td>Do not change</td>
</tr>
<tr>
<td>port</td>
<td>Message Queue port.</td>
<td>5672</td>
</tr>
<tr>
<td>username</td>
<td>Message Queue username.</td>
<td>Do not change</td>
</tr>
<tr>
<td>password</td>
<td>Message Queue password.</td>
<td>Do not change</td>
</tr>
<tr>
<td>vHost</td>
<td>Tenant name.</td>
<td>Do not change</td>
</tr>
<tr>
<td>exchange</td>
<td>—</td>
<td>Not in use for 5.2</td>
</tr>
</tbody>
</table>

---

**Send documentation comments to cem-docfeedback@cisco.com**

### Table B-1 Controller Settings and Default Values

<table>
<thead>
<tr>
<th>Controller Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
</table>
| lockFile           | Path where the database lock file is located. | \`\`\`db\emdata.lock.db  
Do not change |
| databaseDir        | Folder of the database installation | \`\`\`db  
Do not change |
| logDir             | Specifies the directory where the controller log files are stored. | %INSTALL_DIR%\logs  
Change only if necessary |
| blur               | Encryption key for all passwords in database or configuration file. Not to be shared. | Do not change |
| blurOld            | Old encryption key used for pre-4.0 passwords. | Do not change |
**Table B-1    Controller Settings and Default Values**

<table>
<thead>
<tr>
<th>Controller Setting</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>sslMode</td>
<td>Defines how the controller validates the SSL certificate of the message queue server. This setting can have one of the following values:</td>
<td>STRICT_CHECK_BUT_ACCEPT_FIRST_SEEN</td>
</tr>
</tbody>
</table>
|                           | • STRICT_CHECK_BUT_ACCEPT_FIRST_SEEN  
The controller accepts the first certificate that it receives.                                                                                                                                             |                                                                               |
|                           | • STRICT  
The controller accepts unsigned certificates. However, the controller does not create the trusted file automatically and the user needs to rename the self-signed certificate from untrusted to trusted.                                                                                          |                                                                               |
|                           | • NO_CERTIFICATE_VALIDATION  
The controller does not check the certificate.                                                                                                                                                          |                                                                               |
| syslogHost                | IP address for the system log server.                                                                                                                                                                            | Change only if necessary                                                       |
| updateServerChannel       | Controller channel where controller updates are stored.                                                                                                                                                      | Do not change                                                                  |
| offlineRecoveryDumpInterval | Configuration for starting the controller in the offline mode. That is, without connection to the central server. It defines the interval, in minutes, of the asset data storage to the local hard disk during the offline mode. | 0  
Indicates that the controller is not in the offline mode                        |
Send documentation comments to cem-docfeedback@cisco.com