WebSocket-Based Edge MicroServer and Lua Script Resource Developer's Guide

Version 5.4.9

May 2020

PTC Inc., 121 Seaport Blvd, Boston, MA 02210 USA

Contents

Document Revision History

Revision Date	Version	Description of Change
June 2020	5.4.9	Updated the instructions for creating a self-signed certificate. Refer to Creating a Self-Signed Certificate - for Testing Purposes ONLY on page 41.
April 2020	5.4.8	Based on security fixes in this release, updated related topics: • Data security library: ○ Protecting Data with Encryption on page 50: Formerly entitled "Enabling Encryption", this topic provides details about automatic encryption of WS EMS and LSR configuration files on startup as well as the how to enable encryption. ○ Encrypting Application Keys, Passwords, and Passphrases on page 36 ○ New topic, Certificate Fingerprint Validation on page 45 • Configuring Secure Connections (SSL/TLS) on page 30 • Using a Custom Certificate and Private Key on page 40 • Configuring the HTTP Server Group on page 63
November 2019	5.4.7	Changes related to upgrading to OpenSSL 1.1.1c.
June 2019	5.4.6	Changed version of Open SSL to 1.0.2r. Also removed mention of AxTLSsince it is no longer provided in the distribution bundle.
February 2019	5.4.5	Added chapter on setting up WS EMS to use ThingWorx Asset Advisor for Remote Access, File Transfers, and Software Content Management (SCM). See Using ThingWorx Asset Advisor with WS EMS and LSR

Revision Date	Version	Description of Change
		on page 93. Also added a topic on creating an application key for a WS EMS in ThingWorx Composer. See Create an Application Key for WS EMS on page 24.
December 2018	5.4.5	Updated for removal of the built-in certificate. Instructions for migrating to a custom certificate from the built-in certificate on page 38 are provided for customers who have previously used the built-in ("default") certificate. Added instructions for creating a private key, self-signed certificate, CSR, certificate chain, and Certificate Authority List on page 40. Updated for new configuration option to specify cipher suites on page 37 set for the Edge device to use when communicating with the ThingWorx Platform.
October 2018	5.4.4	Changed the section, Configuring the WebSocket Connection on page 66, to remove the `max_frame_size` property.
September 2018	5.4.3	Changed the section on Duty Cycle Modulation on page 69, based on the software changes for the 5.4.3 release.
July 2018	5.4.2	Added new topic, Running REST API Calls with Postman on WS EMS and LSR on page 134, and updated the HTTP Server configuration topics for the WS EMS and LSR with the new parameters. See Configuring the HTTP Server Group on page 63 and Configuring the HTTP Server for the LSR (SSL/TLS Certificate) on page 140. Added notes about using the colon (`:`) character in a `username` to the topics wherein a username is configured. This includes notes in the topics in Updating, Deleting, and Executing with REST Web Services on page 113.

Revision Date	Version	Description of Change
May 2018	5.4.1	• Added information about support for simplified infotables in the REST Web Service services and a note in the TestPort service on page 132 referring to this information. See the Note in REST Web Services Supported by WS EMS on page 121. • Added information about the requirement for setting the **restart** parameter in the `config.json` file of the WS EMS. See Setting an Option to Use the Restart REST Service on page 60 • The chapter, Getting Started with the Lua Script Resource on page 137, has a new sub-section, called Configuring a Lua Script Resource on page 138, that provides security information for the LSR (HTTP Server on page 140 and Connection to WS EMS on page 139).
January 2018	5.4.0	Restored missing code example for Gateway Mode with Explicitly-Defined Remote Things. on page 90
November 2017	5.4.0	Revisions for change to support for OpenSSL libraries, which are now the default security libraries instead of axTLS. axTLS can still be used, but is no longer the default. Added new appendix with configuration examples for WS EMS and LSR for different levels of security.
June 2017	5.3.4	Revisions for changes to log file, including limitation for size of log files, log message size, and size of chunk to write before flushing to disk. Also the same format for both log messages written to console and to persisted log files. Both are all text. The timestamps now show actual time instead of time that the messages were written to the stream in the logger thread (this affects WS EMS and LSR).
May 2017	5.3.3	Added information for new configuration option, `tick_resolution`.

Revision Date	Version	Description of Change
		: Revised duty cycle description. Removed MODBUS information.
February 2017	5.3.2, build 1693	Fixed config examples.
April 2016	5.3.2	Revised the contents of the distribution bundle to reflect changes. . Added section on using FIPS. Added proxy configuration changes for Tunnel Manager.
January and February 2016	5.3.1	Added the REST Web Services for WS EMS to this document. Reorganized this document. Updates for `config.json.complete`. Added installation script information for WS EMS. Added the versions of libraries required for supported Linux platforms.
October 2015	5.3.0	Initial version of this guide.

About This Guide

TheThingWorx WebSocket-based Edge MicroServer (WS EMS) is used to provide a simple means for remote devices to connect quickly and securely to a ThingWorx Platform.

This document describes how to install, configure and run the WS EMS and the Lua Script Resource (LSR). It also explains how to set up, and use ThingWorx Asset Adviisor with your WS EMS and LSR devices.

Audience

This document is intended for developers with at minimum a basic knowledge of JSON and the Lua scripting language. In addition, you need to be familiar with ThingWorx Platform, its concepts, and ThingWorx Composer.

Note

> This document is accurate at the time of the software release. The content is also available on the PTC ThingWorx Help Centers page of the PTC Support site. From this page, follow the link to the ThingWorx WebSocket-based Edge MicroServer (WS EMS) and Lua Script Resource (LSR)Help Centerr to see the latest documentation (v.5.4.6 and later). This help center is updated if and when additional information becomes available.
>
> To see documentation from v.5.4.5 or earlier, go to the original ThingWorx Edge SDKs and ThingWorx WebSocket-based Edge MicroServer Help Center.

Technical Support

Contact PTC Technical Support via the PTC Web site, phone, fax, or e-mail if you encounter problems using your product or the product documentation.

For complete details, refer to Contacting Technical Support in the *PTC Customer Service Guide*. This guide can be found under the Related Resources section of the PTC Web site at http://www.ptc.com/support/

The PTC Web site also provides a search facility for technical documentation of particular interest. To access this search facility, use the URL above and search the knowledge base.

You must have a Service Contract Number (SCN) before you can receive technical support. If you do not have an SCN, contact PTC Maintenance Department using the instructions found in your *PTC Customer Service Guide* under Contacting Your Maintenance Support Representative.

Documentation for PTC ThingWorx Products

You can access PTC ThingWorx documentation, using the following resources:

- PTC ThingWorx help centers page, which provides links to all ThingWorx help centers.
- ThingWorx Documentation Resources, which provides links to both ThingWorx Help Centers and to ThingWorx PDF documents, including release notes, support matrices, installation and administration, best practices, and developer guides.
- PTC ThingWorx Reference Documentation — The Reference Documents pages provide access to the PDF documents available for all PTC ThingWorx products.

  A Service Contract Number (SCN) is required to access the PTC documentation from the Reference Documents website. If you do not know your SCN, see “Preparing to contact TS” on the Processes tab of the PTC Customer Support Guide for information about how to locate it: http://support.ptc.com/appserver/support/csguide/csguide.jsp. When you enter a keyword in the Search Our Knowledge field on the PTC eSupport portal, your search results include both knowledge base articles and PDF guides.

Comments

PTC welcomes your suggestions and comments on our documentation. To submit your feedback, you can:

- Send an email to documentation@ptc.com. To help us more quickly address your concern, include the name of the PTC product and its release number with your comments. If your comments are about a specific help topic or book, include the title.
- Click the feedback icon in any PTC ThingWorx Help Center toolbar and complete the feedback form. The title of the help topic you were viewing when you clicked the icon is automatically included with your feedback.

1

Introducing the ThingWorx WS EMS

This section provides an overview of the ThingWorx WS EMS, explaining the relationship between theWS EMS and a ThingWorx Platform instance, and summarizes the purpose and key features of the WS EMS.

Features of the ThingWorx WS EMS

This section presents an overview of the capabilities of the ThingWorx WebSocket-based Edge MicroServer (WS EMS). The sections below describe the features that enable your edge devices to communicate with the ThingWorx Platform:

Connecting to ThingWorx

Your Edge devices collect data and respond to commands. How do you get that data to the ThingWorx Platform? It is possible to use REST Web Services over HTTP/HTTPS. However, that option tends to have a high connection overhead. Another alternative is MQTT, which requires a server and additional open ports.

If you need a fast connection that stays on continuously and is always ready to relay your data to the server and execute commands using existing open ports on your firewall, the WS EMS and LSR can provide this connection for your devices. The WS EMS uses the ThingWorx AlwaysOn protocol, which is based on the Open WebSocket Standard RFC6455 (https://tools.ietf.org/html/rfc6455). If you need to create an application for a resource-constrained devices, consider the ThingWorx Edge C SDK. The C SDK also uses the AlwaysOn protocol and enables you to write edge applications with minimal footprints.

AlwaysOn™ Protocol

The ThingWorx AlwaysOn protocol is a binary protocol that uses the WebSocket protocol as its transport. The WS EMS uses the AlwaysOn protocol for communications with WS EMS. This protocol provides a number of benefits:

- The devices that are running a WS EMS initiate all connections, which eliminates the need to open ports for inbound connections if the edge devices are deployed behind a firewall.
- The AlwaysOn protocol uses HTTP and the standard HTTP/HTTPS ports (80 and 443) to initiate and maintain connectivity, which eliminates the need for opening secondary ports for outbound communications.
- The protocol supports the TLS standard for securing the connection to a ThingWorx Platform. Refer to the section below, Security on page 14, for more information.

- Once a connection is established, AlwaysOn binary messages are passed between the Edge device and ThingWorx Platform. AlwaysOn binary messages do not require re-initiating the HTTP connection for each request and therefore do not require the additional overhead of the standard HTTP messages. A ping/pong exchange of messages between a WS EMS and a ThingWorx Platform keep the connection alive during periods when the connection might be closed due to inactivity..
- The connections are persistent, which allows the WS EMS to make outbound requests to an Edge device. ThingWorx Platform can send requests to read or write properties, and to invoke services at the device, all with very low latency.

For devices that need to be offline or that do not need to be constantly connected, the WS EMS also supports duty cycle modulation. This feature allows developers to configure the periods of time that the device running the WS EMS will be online and offline. For more information, refer to Configuring Duty Cycle Modulation on page 69.

Security

The following default settings for the configuration of WS EMS support secure communications:

- Encryption — By default, the WS EMS always attempts to connect to a ThingWorx Platform and communicate with it using TLS. The WS EMS and Lua Script Resource use a data security library that provides automatic encryption of sensitive configuration data, such as application keys and passwords, on startup. For details, refer to Automatic Configuration Encryption on page 52 in the topic, Protecting Data with Encryption on page 50. With this data security library, you no longer need to manually encrypt this sensitive data and copy it into the `config.json` file of your WS EMS or the `config.lua` file of your LSR.
- Certificates — By default, the WS EMS attempts to validate the certificate presented by ThingWorx during TLS negotiation. For details, refer to Setting Up Security for the WS EMS on page 31 and Using a Custom Certificate and Private Key on page 40.
- The following additional security features are supported:
  - TLS Host Name Validation on page 36
  - Configuring the WS EMS to Use a Different Certificate Chain for Edge to Edge Communications (Optional) on page 45
  - Certificate Fingerprint Validation on page 45

Note

Starting with release 5.4.7 of the WS EMS, the distribution bundles for Linux and Windows have version 1.1.1 of OpenSSL binaries for secure connections. This version of OpenSSL implements TLS v.1.3, which you can between the WS EMS and an LSR. Once the ThingWorx Platform is updated to support TLS v.1.3, you will be able to use TLS v.1.3 between the WS EMS and the platform.

Lua Script Resource (LSR)

The optional Lua Script Resource (LSR) is a statically linked application that is used to run Lua scripts and configure Things (devices) for integration with the host system. The LSR supports secure HTTP connections, and as of release 5.4.0, you can customize the certificate or private key that you want to use.

HTTP Interface for REST Web Services

In addition to the AlwaysOn interface, the WS EMS has an HTTP interface that supports REST Web Service calls. This HTTP interface allows other applications to interact with a ThingWorx Platform through the AlwaysOn connection of the WS EMS. Since this other interface is HTTP, a custom application or the Lua Script Resource can be on a machine that is separate from the WS EMS and still communicate with it. The HTTP/REST interface of the WS EMS is a reflection of the REST interface of WS EMS.

Support for ThingWorx SCM Extension in ThingWorx Asset Advisor

The WS EMS and LSR support the use of the file-based package feature of the ThingWorx SCM Extension for the ThingWorx Platform. If you have this extension and ThingWorx Asset Advisor installed (imported) on your ThingWorx Platform, you can use SCM to send software and firmware updates to Edge devices that are running WS EMS or the LSR. To set up SCM for your devices, refer to Using ThingWorx Asset Advisor with WS EMS and LSR on page 93.

WS EMS and ThingWorx Platform

The WS EMS is a stand-alone application that you can install on a remote device. Once configured and running, the WS EMS establishes ™AlwaysOn, bidirectional communications between the device and the ThingWorx Platform. The WS EMS uses a small footprint, and supports a variety of operating systems and architectures. This flexibility allows the WS EMS to work with a large number of devices to provide an easy way to establish communication between an Edge device and a ThingWorx Platform instance. You can use ThingWorx Composer to interact with the Edge devices that are running the WS EMS, and using ThingWorx Mashup Builder, you can build interactive, browser-based mashups for users who monitor the devices..

The Connection Sequence

The process of connecting to a ThingWorx Platform instance consists of three main steps: Connect, Authenticate, and Bind. The WS EMS performs the first two steps. Then, the WS EMS works with the Lua Script Resource or a custom application to perform the third step. Here are the steps in more detail:

1. Connect — The WS EMS opens a physical WebSocket to a ThingWorx Platform instance, using the host and port specified in its configuration file. If configured, SSL/TLS is negotiated at this time.
2. Authenticate — The WS EMS sends an authentication message to the ThingWorx Platform instance. This message must contain an application key that was previously generated by an administrator user.

   Upon successful authentication, the WS EMS can interact with the ThingWorx Platform instance, according to the permissions applied to its application key. For the WS EMS, this implies that any client that makes HTTP calls to its REST interface can access functionality on the ThingWorx Platform instance. For this reason, the WS EMS is set by default to listen for HTTP connections on `localhost` (port 8000). You can change this listening port in the configuration file for the WS EMS.

   At this point, the WS EMS can make requests to the ThingWorx Platform instance and interact with it, much like an HTTP client can interact with the REST interface of the platform instance, but the instance cannot direct requests to the Edge device.
3. Bind — To enable the ThingWorx Platform instance to send requests to the WS EMS, the WS EMS works with the Lua Script Resource (or custom application) to send a BIND message to the ThingWorx Platform instance on behalf of the devices. Note that this step is optional, if you do not want the devices to receive and process requests from the platform instance. It is required if you want to transfer files from the platform instance to your devices or if you want to use tunneling.

   The BIND message can contain one or more names or identifiers for the devices. Note that corresponding *Remote Things* must have been created on the ThingWorx Platform instance to represent your Edge devices. Remote things are things that are created using the **RemoteThing** Thing Template (or one of its derivatives) in ThingWorx platform. When it receives the BIND message, the platform instance associates the matching Remote Things that it has with the WebSocket that received the BIND message. This association allows the instance to use the WebSocket to send requests to the Edge devices, and update the **isConnected** and **lastConnection** time properties for the corresponding Remote Things on the ThingWorx Platform instance.

The WS EMS can send an UNBIND message to the ThingWorx Platform instance that removes the association between the Remote Things on the instance and the WebSocket. The **isConnected** property is then updated to **false**.

Deployment

Once you have properly configured and integrated the WS EMS and Lua Script Resource (or your custom application), you can deploy them in one of the following ways:

- Embedded Deployment — Integrate the WS EMS and Lua Script Resource (or your custom application) directly into the application software stack of the Edge device.
- Tethered Deployment — Deploy the WS EMS to a simple black-box that connects to the diagnostic and sensor ports of an intelligent device. Deploy the Lua Script Resource or your custom application either on the same black-box, or on the intelligent device.
- Networked Gateway Deployment — Deploy the WS EMS on a simple server appliance that exists on the same network as a set of intelligent devices (for example, sensor networks or clusters of network-capable equipment),. Then, deploy the Lua Script Resource or your custom application on other hardware on the same local network.

Configuration Overview

To start connecting your Edge devices to a ThingWorx Platform instance, you need to do the following:

1. Begin the initial configuration of the WS EMS, as described in Configuring the WS EMS on page 26.
2. PTC strongly recommends that you configure and use SSL/TLS certificates for communications between your Edge device that is running the WS EMS and the ThingWorx Platform. If required, you can also use SSL/TLS certificates for communications between your WS EMS and the Edge devices that are running the Lua Script Resource (LSR). If you do not have SSL/TLS

certificates, refer to Using a Custom Certificate and Private Key on page 40 for information on creating a custom certificate and private key and configuring the WS EMS and LSR to use them.

Note

As of v.5.4.5 of the WS EMS, the built-in certificate is no longer provided. You need to migrate to using a custom certificate. Refer to Migrating from the WS EMS/LSR Built-in Certificates on page 38 for more informatinon.

3. Once you have successfully connected to the ThingWorx Platform instance, complete the full configuration of the WS EMS according to your needs. Refer to the section, Viewing All Configuration Options on page 60.
4. To use the Lua Configuration Script to host Remote Things for integration with ThingWorx Platform, begin the initial configuration of the Lua Script Resource, as described in Getting Started with the Lua Script Resource on page 137.

2

Getting Started with the ThingWorx WS EMS

This chapter provides an overview of how to install, initially configure, and run the ThingWorx WS EMS .

Components to Install

To connect to and integrate with a ThingWorx Platform instance, you can install two separate software components remotely on edge devices:

- ThingWorx WebSocket-based Edge MicroServer (WS EMS) — The WS EMS is the communication conduit that provides a secure communication channel to a ThingWorx Platform instance. The WS EMS is a separate process, so it can support communications from one or more devices. In addition, the WS EMS provides a RESTful HTTP interface, allowing other applications to communicate with it. The WS EMS translates the REST Web Services into AlwaysOn protocol messages that it then sends to a ThingWorx Platform instance. For information about the REST interface, refer to REST Web Services and WS EMS on page 113.
- Lua Script Resource — An application for host devices that uses the Lua scripting language to integrate with them. The Lua Script Resource is an optional component. You do not need it to run the WS EMS. As an alternative, you can write your own application that uses HTTP and communicates directly with the WS EMS. For information about the Lua Script Resource, refer to Getting Started with the Lua Script Resource on page 137.

For instructions on downloading and installing the WS EMS, refer to Downloading and Installing the ThingWorx WS EMS and LSR on page 20.

Downloading and Installing the ThingWorx WS EMS and LSR

The ThingWorx WS EMS is available from PTC and is distributed as a `.zip` file.

To install the package, follow these steps:

1. The distribution bundle for WS EMS is available through the PTC Support site, Order or Download Software Updates page, at https://support.ptc.com/appserver/cs/software_update/swupdate.jsp. If you are not already logged in, you are prompted to log in before access to this page is granted.
2. On the Order or Download Software Updates page, click the link appropriate to your situation:
   - Download Software by Sales Order Number — if you are downloading for the first time and have your Sales Order Number (SON).
   - Order or Download Software Updates — if you have a support agreement with PTC that allows software downloads.
3. Either way, on the Customer Search page, enter your Customer Name and Customer Number and click **Next**.
4. If you chose to download by SON, enter your SON in the page that appears, and click **Submit**. Otherwise, continue to the next step.

5. On the PTC Software Download page, select the product family, **THINGWORX EDGE MICROSERVERS**.
6. Click the plus sign to expand the latest major release, which is at the top of the list (for example, **5.4**).
7. Expand **ThingWorx Edge MicroServers**.
8. Expand **Most Recent Datecode**.
9. Choose and download the distribution bundle that is correct for the operating system and platform that you want to use.

   The distribution bundles provide only OpenSSL 1.1.1:

   - `microserver-linux-arm-hwfpu-version.zip`
   - `microserver-linux-arm-version.zip`
   - `microserver-linux-x86_32-version.zip`
   - `microserver-linux-x86_64–version.zip`
   - `microserver-windows-x86_32-version.zip`

   Note

   As of WS EMS v.5.4.6, the distribution bundles no longer provide axTLS libraries. Only the OpenSSL libraries are included in the distribution bundles. Refer to the ThingWorx WebSocket-Based Edge MicroServer Support Matrix for more information.

10. After downloading the distribution bundle, select a location for extracting it.
11. Unzip the distribution archive. You are ready to start configuring the WS EMS on page 26.

ThingWorx WS EMS and LSR Distribution Contents

When unzipped, the WS EMS distribution creates the directory, `<package_name>/microserver` on Linux. On Windows, it creates the directories, `<package_name>\microserver` and `<package_name>\lib`, where the `lib` directory contains DLLs for Windows.

The following table lists the files at the top level of the `microserver` directory, followed by the subdirectories and their contents. Note that the paths use Windows notation.

Item	Description
Files	
`wsems.exe` (Windows) or *`wsems`* (Linux)	The WS EMS executable that is used to run the Edge MicroServer. **Note** Linux users must be granted permissions to the *wsems* file.
Linux - *`libcrypto.so.1.1`* and *`libssl.so.1.1`*	OpenSSL shared libraries for Linux.
Windows - *`libcrypto-1_1.dll`* and *`libssl-1_1.dll`*	OpenSSL Shared Library DLLs (dynamic linked libraries) for Windows.
Windows - *`luaScriptResource.exe`* Linux - *`luaScriptResource`*	The Lua utility that is used to run Lua scripts, configure Remote Things, and integrate with the host system.. **Note** Linux users must be granted permissions to the *`luaScriptResource`* file.
Subdirectories	
`\doc\`	Directory that contains the release notes (PDF) and this document, *ThingWorx WebSocket-based Edge MicroServer (WS EMS) Developer's Guide* for this release (also a PDF). Also contains the files for the luadoc that provides assistance with the Lua Script Resource.
`\doc\lua\`	Subdirectory that contains the luadoc for the Lua Script Resource.
`\etc\`	Directory that contains configuration files and directories for the Lua Script Resource utility.
`\etc\config.json.documented`	A REFERENCE file that contains all of the configuration options available for the WS EMS plue comments to guide you through the options. **Caution** Do not attempt to use `config.json.documented` to run your WS EMS. It is intended as a reference. It is NOT as a valid JSON file that you can use to run WS EMS
`\etc\config.json.complete`	A valid JSON file that contains all the configuration options available for the WS EMS.
`\etc\config.json.minimal`	A reference file that contains the basic settings that are required to establish a connection.
`\etc\config.lua.example`	A reference file that contains a basic configuration for the **luaScriptResource** utility. A *`config.lua`* file is required to run the Lua engine.
`\etc\community\`	Directory from which third-party Lua libraries are deployed. Examples of

Item	Description
Files	
	these libraries include the Lua socket library and the Lua XML parser, .
`\etc\custom\`	Directory that will contain your custom scripts and templates.
`\etc\custom\scripts\`	Directory from which custom integration scripts are deployed. It also contains an example script, called `sample.lua`.
`\etc\custom\templates\`	Directory that contains an example template, called `config.lua.example`, and that is used to deploy custom templates.
`\etc\thingworx\`	Directory that contains WS EMS-specific Lua files that are used by the Lua Script Resource (LSR). Do not modify this directory and its contents because an upgrade will overwrite any changes.
`\install_services\`	Windows subdirectory that contains the following files `install`, `install.bat`, `tw_luaScriptResourced`, and `tw_microServerd`. The install scripts will register the WS EMS anad LSR as services on Windows. For a Linux installation, the following files are in this subdirectory: `ems.service`, `install`, `lua.service`, `tw_luaScriptResourced`, and `tw_microServerd`. The *.service scripts will register the WS EMS and LSR as daemons on Linux. For information on running the scripts, refer to Running WS EMS as a Daemon (Linux) or as a Windows Service on page 54 or Running as a Service on page 149.

Libraries for WS EMS on Linux

The WS EMS uses the following libraries on Linux platforms:

- libpthread
- libstdc++
- libgcc_s
- libc
- libm (math library)

The Lua Script Resource also has libdl (dynamic loader).

Versions of the Libraries for Supported Platforms

The following table shows the supported platforms for the WS EMS and the versions of the libraries that you can use with them:

Platform	libc	libpthread	libstdc++	libgcc	libm	libdl (LSR only)
Linux ARM	2.9 (with gcc version 4.3.3)	2.9	6.0.10	4.3.3	2.9	2.9
	2.8 (with gcc	2.9	6.0.10	4.3.3	2.9	2.8

Platform	libc	libpthread	libstdc++	libgcc	libm	libdl (LSR only)
	version 4.6.0)					
Linux ARM HWFPU	2.8	2.8	6.0.15	4.6.0	2.8	2.8
Linux x86–32	2.8	2.8	6.0.10	4.3.2	2.8	2.8
Linux x86–64	2.8	2.8	6.0.15	4.6.0	2.8	2.8
Linux coldfire	2.11.1	2.11.1	6.0.14	4.5.1	2.11.1	2.11.1
Win32	XP or later	n/a	n/1	n/a	n/a	n/a

Create an Application Key for WS EMS

When connecting to a ThingWorx Platform, the WS EMS needs to present an application key for authentication. This application key needs to be associated with a non-admin user. The sections below explain how to create the non-admin user for a WS EMS and how to configure the application key.

Note

To be able to create a non-admin user or an application key, you must log in as an Administrator of ThingWorx Platform or as a member of a user group that has permissions and visibility to these security entities.

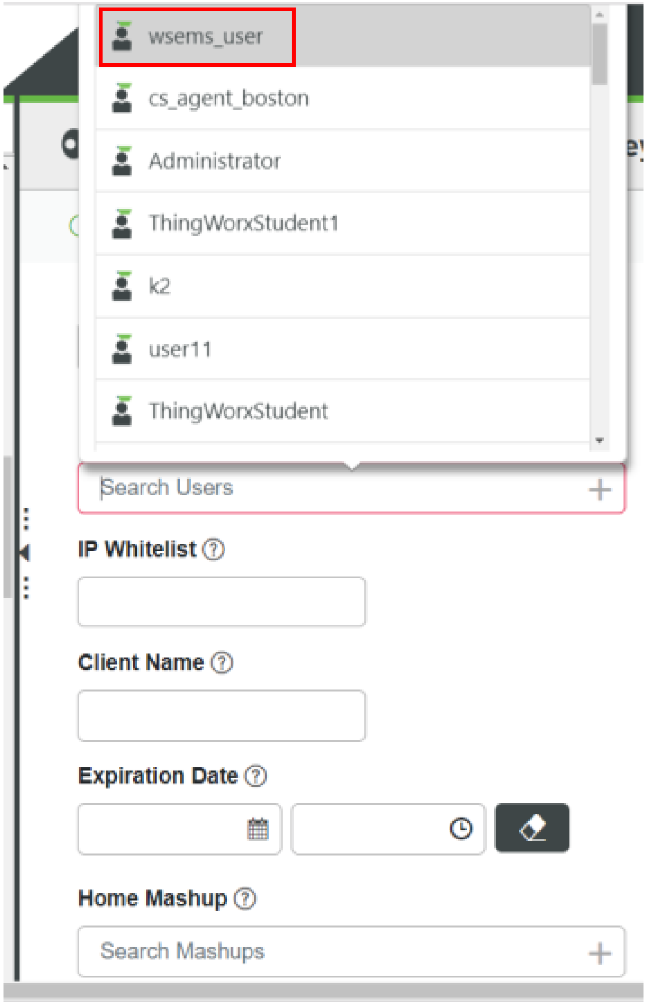
Creating a Non-Admin User in ThingWorx Composer

Follow these steps to create a non-admin user for the WS EMS application key:

1. Log in to ThingWorx Composer.
2. In the left navigation panel, select **Browse** and scroll down to **Security**.
3. Select **Users** to display the list of users currently configured in the platform.
4. In the bar just above the list, click **+New**.
5. In the **General Information** page, type a name for the WS EMS user account. For example, `wsemsUser`. You will associate this user with an application key for the WS EMS, so do not enter a password.
6. If desired, enter a **Description** for this user.
7. Check to make sure that the **Enabled** check box is selected, and click **Save**.

Follow these steps to configure an application key and a Thing for the WS EMS asset in ThingWorx Composer:

1. From **Security** ▸ **Application Keys** ▸ **, click** ▸ **New**.
2. Enter the appropriate values:
   a. **Name** — A name for the application key. For example, `wsemsappkey23`
   b. **User Name Reference** — The name of a user account to associate with the application key. You can select from a list by clicking the plus icon in this field. A list from which you can select a user for the key appears:



wsems_user
cs_agent_boston
Administrator
ThingWorxStudent1
k2
user11
ThingWorxStudent

Search Users +

IP Whitelist ?

Client Name ?

Expiration Date ?

Home Mashup ?

Search Mashups +

   In the example above, the `wsems_user` is selected. The permissions and visibility assigned to this user account affect what the WS EMS can do on the platform. For example, write new values to remote properties.

   c. **Expiration Date** — A date in the future for the application key to expire, based on your company policies. The default value is one day. Use the calendar widget to select a date and the time widget to select a time.
3. Click **Save**.

4. Create a Thing in ThingWorx for the asset that is running the WS EMS. Depending on the features you want to use, choose one of the following Thing Templates or a Thing Template that implements any of the following Thing Templates:
   - **RemoteThingWithTunnelsAndFileTransfer** — Use for assets for which you want file transfers, SCM, and remote access capabilities.
   - **RemoteThingWithFileTransfer** — Use for assets for which you want file transfers (upload and download) and/or SCM capabilities, but not remote access capabilities.
   - **RemoteThingWithTunnels** — Use for assets for which you want to use remote access capabilities but not file transfers or SCM.
5. Once you have an application key, follow the instructions for configuring your WS EMS with an application key in Configuring the WS EMS on page 26.

Configuring the WS EMS

This topic takes you through the basic steps for a simple configuration that establishes a connection to your ThingWorx Platform. First, you need to create the configuration file on page 26 and then you configure the connection on page 28.

Create the WS EMS Configuration File

The configuration file of WS EMS is a text file that uses the JSON format. It is separated into multiple groups. Each group contains sets of name/value pairs (properties) that control different aspects of the configuration. To connect to a ThingWorx Platform instance, only a few properties are required.

Tip

The WS EMS uses the cJSON library for JSON parsing. This library does not parse json with case sensitivity by default. WS EMS v.5.4.8 and later automatically encrypt sensitive data on startup and re-write the configuration file to disk with the newly encrypted secrets. Since cJSON is reposible for that parsing, any keys with uppercase letters are converted to lowercase.

To view an example of a basic configuration file and create your own configuration file:

1. From the WS EMS installation directory, change to the directory, `/etc`. This directory contains the following configuration files for WS EMS:
   - `config.json.complete` — A valid JSON file, with no comments. If you want to use this file, you need to provide information relevant to your environment for such properties as the application key (`appkey`), and the `ws_servers.host` and `ws_servers.port` for the instance of ThingWorx Platform to which the WS EMS will connect.
   - `config.json.documented` — A copy of the `config.json.complete` file with many comments to explain the properties to set. This file is NOT a valid JSON file. Do NOT attempt to run the WS EMS with this configuration file.
   - `config.json.minimal` — A file that provides (in valid JSON) the essential properties that need to be set to communicate with a ThingWorx Platform.

   The fourth configuration file in this directory is a sample configuration file for the Lua Script Resource (`config.lua.example`). Refer to Configuring a Lua Script Resource on page 138 for more information.
2. To run the WS EMS, you need to create a separate configuration file, called `config.json`. To begin with a basic configuration, open `config.json.minimal` in a text editor. This file contains the minimum set of configuration settings required to connect to a ThingWorx Platform.
3. Create a new file in your editor, and save it as `config.json`.
4. Copy the settings from `config.json.minimal` into your `config.json` file.
5. Follow the instructions in the next section to configure the connection between the WS EMS and an instance of ThingWorx Platform.

Configure the Connection to ThingWorx Platform

To connect to a ThingWorx Platform instance, you must configure the `ws_servers` group in the configuration file. This group contains the properties that define the connection between the WS EMS and a ThingWorx platform instance. You need to provide an IP address or host name and port for one instance of ThingWorx platform.

Note

Previous releases of the WS EMS allowed you to configure an array that contained multiple addresses. However, the WS EMS no longer checks for another address if it fails to connect with the first address in the array. If you previously specified multiple addresses, you do NOT have to change your configuration file. The WS EMS will use the first address in the `ws_servers` array and ignore the rest.

As long as you have created your own `config.json` file, follow these steps to set up the connection:

1. Copy the first two lines from the `config.json.minimal` file and paste them in your file:

   ```
   {
     "ws_servers" :  [{
   ```

   You are ready to add the properties that define the connection.

2. Under `"ws_servers"`, add the `"host"` and `"port"` properties. Then, for the `"host"` property, replace `"localhost"` with the URL of your ThingWorx Platform instance. For the `"port"` property, enter the number of the port on the host to use for the connection. If the connection is to be secure, use port 443. For example:

   ```
   {
    "ws_servers": [{
                   "host" : "some_host_url",

                  "port": 443
                  }
    ],

    "resource": "/Thingworx/WS",

    "appkey" : "some_encrypted_application_key",
   ```

   For development purposes, you may want to use a ThingWorx Platform instance that is running on the same computer where you installed your WS EMS. `"localhost"` can be used as the value for `"host"` for these purposes only.

Next set the application key for the WS EMS to use to access the ThingWorx Platform. A platform administrator can generate application keys using ThingWorx Composer. The application key is associated with a user account that determines the privileges that the WS EMS will have when accessing the instance. Best security practices require encrypting the application key and any passwords that you may be using. For example, the password for a certificate or the passphrase for a private key.

Tip

If you are using WS EMS 5.4.8 or later, your version of WS EMS automatically encrypts secret strings such as the application key or a certificate password on the first startup. You can skip to Step 5. For information on the automatic encryption, refer to Automatic Configuration Encryption on page 52.

3. If you are using an earlier version of the WS EMS, you need to manually encrypt the application key and passwords. To do this, open a shell or command prompt, navigate to the WS EMS installation, and enter the following:

   ```
   wsems.exe -encrypt myPasswordString
   ```

   where `myPasswordString` is the application key or a password.
4. Once the encryption generates output, copy the encrypted application key and paste it so that it replaces the current value of the `appkey` property. Using the example configuration properties shown in Step 2, replace `some_encrypted_application_key` with the encrypted key you just generated. Make sure that it is enclosed in the double quotation marks.
5. Save the configuration file.

   If you want to try running the WS EMS to check the connection, refer to Running the ThingWorx WS EMS on page 52 and then Verifying Your Connection on page 57.

Configuring Secure Connections (SSL/ TLS)

About SSL/TLS Certificates

Essentially, SSL/TLS certificates are used for either of two purposes:

- Establishing Trust — Trusted Certificate Authority (CA) certificates verify other certificates. Typically, these files are found on a client that is attempting to establish an SSL/TLS connection with a server. For example, store a valid certificate in the home directory of your WS EMS. The valid certificate must belong to the issuers of the certificates (Certificate Authority or "CA") of the ThingWorx Platform instance ("server") with which the WS EMS communicates. The CA certificates must be stored in the home directory of WS EMS.
- Establishing Identity — Identity certificates with private keys provide a way of communicating the unique identity of an SSL/TLS peer. Identity certificates with private keys are typically used to show the identity of a server to a client. When a server requires client authentication, Identity certificates are also required on the client. In this latter case, the Trusted Certificate Authority certificate would be required on the server (a ThingWorx Platform).

The requirements for products acting as clients, such as WS EMS, or servers, such as a ThingWorx Platform, in SSL/TLS connections follow:

- A server must always have an Identity certificate. Optionally, if the product acting as a server supports and is configured to use client authentication, the server would need a Trusted Certificate Authority certificate.
- A client must always have a Trusted Certificate Authority (CA) certificate. An example of a Trusted CA certificate name is `SSLCACert.pem`. Optionally, if the product acting as a server supports and is configured to use client authentication, the client would also need an Identity certificate. An example of a client-side Identity certificate file name is `SSLCert.pem`, and an example of its private key name is `SSLPrivKey.pem`.

The WS EMS can validate certificates that have been signed using the following algorithms:

- MD5
- SHA-1
- SHA-256 digest

💡 **Tip**

Always configure a secure HTTP server. Otherwise, the WS EMS and LSR log warning messages when SSL, authentication, or certificate validation is disabled or if self-signed certificates are allowed.

As of version 5.4.5 of the WS EMS, FIPS mode is not supported.

As of version 5.4.6 of the WS EMS, the axTLS library is no longer provided in the distribution bundle. Only OpenSSL libraries are provided in the distribution bundle.

As of version 5.4.7 of the WS EMS, the OpenSSL v.1.1.1 libraries are provided in the distribution bundle. Since OpenSSL v.1.1.1 includes TLS v.1.3, communications between the WS EMS and LSR over TLS v.1.3 should work. Once the ThingWorx Platform is updated for TLS v.1.3, communications between the WS EMS and the Platform over TLS 1.3 will work.

💡 **Tip**

The WS EMS provides a property called `http_client_ca_certs` that allows the use of a separate Certificate Authority (CA) certificate file that will only be used for Edge to Edge HTTPS connections. If this option is not used, the default CA certificate list that is used to validate the platform connection will be used. This parameter is in the `certificates` group in the WS EMS configuration file. For more information, refer to Configuring the WS EMS to Use a Different Certificate Chain for Edge to Edge Communications (Optional) on page 45.

Setting Up Security for the WS EMS

If you are installing the WS EMS for the first time with v.5.4.5 or later and have the custom certificates and private keys that you want to use for communications between the WS EMS and the ThingWorx Platform and for communications between the WS EMS and the LSR that is running on the devices behind the WS EMS, this topic is for you. If you are migrating a previous release of the WS EMS and LSR and were using the built-in certificate, refer to Migrating from the WS EMS/LSR Built-in Certificates on page 38. If you do not have custom certificates and private keys, refer to Using a Custom Certificates on page 40 before continuing with the rest of this topic.

This topic provides the following information:

- Setting Up WS EMS to Use Certificates on page 32
    - ○ Properties to Set in config.json for Security on page 33 (table)
- TLS Host Name Validation on page 36
- Validation Criteria on page 35
- Encryption Application Keys, Passwords, and Passphrases on page 36
- Configuring the Cipher Suite Set on page 37
- A Note about Cipher Suites (Java 7) on page 37
- Configuring FIPS Mode on page 37

Setting Up WS EMS to Use Certificates

The properties in the `certificates` group of the configuration file specify whether certificates are validated for the connection between the WS EMS and your ThingWorx Platform instance. This group and its properties are shown here:

```
"certificates": {
  "validate": true,
  "allow_self_signed": false,
  "disable_hostname_validation": false
  "cert_chain": " /path/to/ca/cert/file",
  "client_cert": "/path/to/client/cert/file",
  "key_file": "/path/to/key/file",
  "key_passphrase": "some_encrypted_passphrase",
  "cipher_suite":
"ALL:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ADH:!I
DEA:!3DES:!SRP",
  "http_client_ca_certs": "/path/to/ca/cert/file",
  "validation_criteria": {
    "Cert_Common_Name": "common name",
    "Cert_Organization": "organization name",
    "Cert_Organizational_Name": "organizational name",
    "CA_Cert_Common_Name": "cert common name",
    "CA_Cert_Organization": "cert organization",
    "CA_Cert_Organizational_Name": "cert organizational name"
    }
  "http_client_ca_certs_: "/path/to/ca_cert/file"
  "fingerprint_whitelist" : [
    ""E6:EF:5D:37:22:FC:EF:EA:4B:22:92:45:BD:49:D2:29:3D:84:19:BC:
C3:45:23:A1:22:A4:01:20:9D:03:E6:47",
    "D1:BA:B0:17:66:6D:7F:42:7B:91:1E:22:7E:3A:27:D2:EF:5D:37:22:FC:E
F:EA:4B:22:92:45:BD:01:7E:92:52"
  ]
},
```

Tip

If you are using v.5.4.8 or later of the WS EMS and LSR, secrets such as passphrase, password, and application keys are automatically encrypted. For details, refer to Automatic Configuration Encryption on page 52. If you are using an older version of the WS EMS and LSR, refer to Encrypting Application Keys, Passwords, and Passphrases on page 36.

For examples of secure configurations for communications between the WS EMS and the LSR, refer to Examples of Configuring Secure Communications between the WS EMS and an LSR on page 159. These examples are presented in order of least secure (testing purposes ONLY) to most secure (strongly recommended for production environments).

The following table describes the properties configuring SSL/TLS certificates. Refer to the section below for definitions of the validation criteria.

Note

When specifying the paths to any certificate, use forward slashes (/) for a Linux platform and either backslashes with escapes ("d:\\path\\to\\ca\\cert\\file") or forward slashes ("d:/path/to/ca/cert/file") for Windows platforms.

Properties to Set in config.json for Security

Property	ThingWorx Base Type	Description
validate	BOOLEAN	Whether or not to perform validation on certificates presented by a ThingWorx Platform instance. The default value of this property is true. For production, enabling validation is strongly recommended. If you set this property to true, you **must** create and configure a Certificate Authority (CA) list and specify the path to the file as the value of the cert_chain property. Refer to Creating a Custom CA Certificate List on page 44 for details on creating a Certificate Authority list file.
allow_self_signed	BOOLEAN	Whether or not to permit self-signed certificates to be used. The default value of this property is false. For production, allowing self-signed certificates is strongly discouraged. If you need to create a self-signed certificate for testing purposes, refer to Creating a Self-Signed Certificate on page 41.
disable_hostname_validation	BOOLEAN	Whether or not to use TLS host name validation. The default value of this property is false, meaning that

Properties to Set in config.json for Security (continued)

Property	ThingWorx Base Type	Description
		this validation is enabled. If you want to disable it (not recommended), set this property to `true`. For more information, refer to TLS Host Name Validation on page 36.
`cert_chain`	`STRING`	Certificate Authority list to be used to validate the ThingWorx Platform ("server") certificate. Used if `allow_self_signed` is `false` and `validate` is `true`. You **must** specify the CA list here if you set `validate` to `true`. Here is an example for a WS EMS running on Linux: `"cert_chain": "/path/to/ca/cert/file",` To learn how to create a Certificate Authority list, refer to Creating a Custom CA Certificate List on page 44. **Note** The `cert_chain` property expects a string that specifies a single Certificate Authority list file. If you want to load multiple certificates, add them to the Certificate Authority file and specify the path to that file, as shown above. The WS EMS will load multiple certificates from that CA list file.
`cipher_suite`	`STRING`	The cipher suites for the Edge device to use when communicating with the ThingWorx Platform. The default setting is `ALL`. This option supports the OpenSSL cipher list format, which you can find at https://www.openssl.org/docs/man1.0.2/apps/ciphers.html. Refer to Configuring the Cipher Suite Set on page 37 below.
`client_cert (optional)`	`STRING`	The path to the X.509 certificate file for the client. If you are using an X.509 certificate file, you need to set the `validation_criteria` property. Refer to Validation Criteria on page 35 below.
`http_client_ca_certs`	`STRING`	A list of Certificate Authority certificates to use when validating TLS connections at the Edge. If left unset, the CA certificates specified for the property, `cert_chain` will be used. The CA Certificates are used if `allow_self_signed` is set to `false` and `validate` is set to `true`.
`validation_criteria`	`STRING`	Refer to the section below for details about this property.
`fingerprint_whitelist`	N/A	Certificate fingerprint validation is a security feature that allows a user to restrict HTTPS communication to a known set of trusted server endpoints in addition to TLS certificate validation. This feature is not enabled by default.

Properties to Set in config.json for Security (continued)

Property	ThingWorx Base Type	Description
		To enable this feature, you must add the `fingerprint_whitelist` property with an array of strings to the `config.json` file of each edge microserver with which you want to communicate. If you do not include this configuration option in the `config.json` file, it is not enabled. Refer to Certificate Fingerprint Validation for WS EMS and LSR on page 45 for more details. **Note** Do not add an empty `fingerprint_whitelist` property to the config.json file. This renders the configuration file invalid. When the WS EMS starts, it attempts to read the configuration file. If the configuration file is invalid, the WS EMS stops. For information on the startup process, refer to How the Startup Process Works on page 52.
The following properties are all passed to the underlying C SDK and are not used by the WS EMS. They are associated with the WebSocket connection		
`key_file (optional)`	`STRING`	The path to the key file to load for client certificates (supports .pem, .p8, and .p12 files). If you need to create a private key file, refer to Creating a Private Key on page 40.
`key_passphrase (optional)`	`STRING`	A string password for opening the key file. It is strongly recommended that the passphrase be encrypted. To encrypt this passphrase, refer to Encrypting Application Keys, Passwords, and Passphrases on page 36.

Validation Criteria

To validate a certificate, you can configure the fields of the certificate that should be validated:

- Subject common name
- Subject organization name
- Subject organizational unit
- Issuer common name
- Issuer organization name
- Issuer organizational unit

When creating a Certificate Signing Request (CSR), you are prompted for the fields that need to be validated. The following definitions may help you determine the values for these fields:

- Common Name — Typically, a combination of the host and domain names, the value of these fields looks like “www.your_site.com” or “your_site.com”. Certificates are specific to the Common Name that they have been issued to at the Host level. This Common Name must be the same as the web address that the WS EMS accesses when connecting to a ThingWorx Platform using SSL/TLS. If the platform and the WS EMS are located on an intranet, the Common Name can be just the name of the host machine of the platform.
- Organization Name — Typically, the name of the company.
- Organizational Unit — Typically, a department or other such unit within a company. For example, IT.

TLS Host Name Validation

The WS EMS supports TLS host name validation. This security feature compares the requested host name with subject identifiers in the server certificate, such as the subject common name (CN) and subject alternative names. TLS host-name validation occurs during the TLS Handshake. If the host name on the server certificate does not exactly match the host provided in the WS EMS configuration, the TLS handshake fails with the error, `TW_SOCKET_INIT_ERROR`, and the connection to the ThingWorx Platform fails.

This feature is enabled by default. To disable it, add the `disable_hostname_validation` property in the `certificates` group in the `config.json` file for your WS EMS and set it to `true`, as shown here:

```
"certificates" : {
  . . .
  "disable_hostname_validation" = true
  . . .
```

Encrypting Application Keys, Passwords, and Passphrases

The WS EMS and LSR, v.5.4.8 and later, use a different data security library for encrypting data at rest than previous releases. The data security library uses the XChaCha20-Poly1305 Cipher for encryption of data at rest. This library automatically encrypts configuration files on the first startup of the WS EMS or LSR. For details, refer to Protecting Data with Encryption on page 50. With this library you can, but no longer need to, run the `wsems.exe -encrypt` command to encrypt an application key, certificate password, or keystore passphrase.

For versions prior to v.5.4.8, the legacy data at rest encryption, AES, is supported. In addition, you can improve security for an application by encrypting the application key, certificate password, and keystore passphrase before adding them to the configuration file for WS EMS. Follow these steps:

1. Open a shell or command prompt, navigate to the WS EMS installation, and enter the following:
   ```
   wsems.exe -encrypt String_to_Encrypt
   ```
   where `String_to_Encrypt` is the application key, password, or passphrase to encrypt.
2. Once the output is generated, copy the encrypted string and paste it so that it replaces the current value of the related property in the configuration file. Make sure that the encrypted string is enclosed in double quotation marks.

For examples of medium and high security configurations for the WS EMS and LSR, refer to Medium Security on page 160 and High Security on page 163.

Configuring the Cipher Suite Set

Starting with v.5.4.5 of the WS EMS, you can specify what cipher suites are used by the Edge device when communicating with the ThingWorx Platform. This configuration option supports the OpenSSL Cipher List form, as described at https://www.openssl.org/docs/man1.1.0/apps/ciphers.html.

This configuration option should be placed in the `certificates` group in the `config.json` file for your WS EMS:

```
"certificates": {
    ...
  "cipher_suite":
"ALL:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ADH:!I
DEA:!3DES:!SRP",
    ...
},
```

A Note about Cipher Suites with ThingWorx Platform (Java 7)

If your application communicates with an instance of the ThingWorx Platform that uses Java 7, the cipher suite list should include !kEDH (as shown below) to disable ephemeral Diffie-Hellman ciphers .Otherwise, ephemeral Diffie-Hellman (EDH) key exchange fails, and your WS EMS cannot connect to the platform.

```
<CipherSuites>DEFAULT:!kEDH</CipherSuites>
```

Configure FIPS Mode

Version 1.1.1 of OpenSSL is provided in the distribution bundle of the WS EMS starting with version 5.4.7 of the WS EMS. This version of OpenSSL does not support FIPS mode. If you require FIPS mode, make sure that you have downloaded version 5.4.0 or *earlier* of the WS EMS that supports FIPS mode.

Refer to the ThingWorx WebSocket-Based Edge MicroServer Support Matrix for a table of versions of WS EMS and the versions of OpenSSL they support. The rest of this section is for users of v.5.4.0 or earlier of the WS EMS.

By default FIPS mode is disabled. To enable FIPS mode, you need to set the FIPS option in your `config.json` file. The WS EMS checks if FIPS mode is enabled on startup.

In release 5.4.0, a "switch" was added in the form of a group and property to enable or disable FIPS mode. If you created the `config.json` file for your WS EMS using `config.json.minimal` as the starting point, you need to add the group to your configuration file and change the value of the `enabled` property to `true`, as follows:

```
"fips" " {
          "enabled" : true
},
```

If you used `config.json.complete` as your `config.json` file, the group and property are already present in the file. Set the value of the `enabled` property to `true` to enable FIPS mode, as shown above.

Should you need to disable or enable FIPS mode at any time, open the `config.json` file for your WS EMS, and locate the `fips` group. To disable FIPS mode, set the `enabled` property to `false`, as shown here:

```
"fips" : {
          "enabled" : false
},
```

Migrating from the WS EMS/LSR Built-in Certificates

The 5.4.5 release of the WS EMS and Lua Script Resource (LSR) removes the built-in key and certificate that has existed in previous releases. This change means that you will no longer be able to use the `use_default_certificate` option in the WS EMS, or the `script_resource_use_default_certificate` option in the LSR.

Both the WS EMS and LSR have built-in web servers that support communicating over TLS. You are now required to provide your own certificate and private key file when the WS EMS and Lua ScriptResource are configured to communicate over TLS. This next two sections summarize the configuration changes for the WS EMS and the LSR. For detailed information on creating a private key or a certificate, using a certificate chain between the WS EMS and the LSR, or using a Certificate Authority List for validation, refer to Using a Custom Certificate and Private Key on page 40.

Configuration Changes for WS EMS (config.json)

The `use_default_certificate` option has been removed from the `http_server` group in `config.json`. You will now need to add three configuration options when running with SSL

- `certificate` — Path to a PEM encoded certificate file. This can be a self-signed certificate or a certificate chain, meaning it contains the end entity (that is, the server) certificate, followed by *n* number of Intermediate Certificate Authority certificates.
- `private_key` — Path to a PEM encoded, encrypted private key file.
- `passphrase` — The passphrase to decrypt the private key. This field should be encrypted. To learn how, refer to Encrypting Application Keys, Passwords, and Passphrases on page 36)

Below is an example configuration

Example

Changes to config.json

```
"http_server": {
    "host": "localhost",
    "port": 8443,
    "ssl": true,
    "certificate": "/path/to/certificate/file",
    "private_key": "/path/to/private/key",
    "passphrase": "some_encrypted_passphrase"
},
```

Configuration Changes to Lua ScriptResource (config.lua)

The changes for `config.lua` are:

- `script_resource_certificate_chain`—Path to a PEM encoded certificate file. This can be a self-signed certificate or a certificate chain, meaning it contains the end entity (that is, the server) certificate, followed by *n* number of Intermediate Certificate Authority certificates.
- `script_resource_private_key`—Path to a PEM encoded, encrypted private key file.
- `script_resource_passphrase`—The passphrase to decrypt the private key. This field should be encrypted. For details on how to encrypt the passphrase, refer to Encrypting Application Keys, Passwords, and Passphrases on page 36.

Below is an example configuration

Example

Changes to config.lua

```
scripts.script_resource_host = "127.0.0.1"
scripts.script_resource_port = 8443
scripts.script_resource_ssl = true
scripts.script_resource_certificate_chain = "/path/to/certificate/
file"
scripts.script_resource_private_key = "/path/to/private/key/file"
scripts.script_resource_passphrase = "some_encrypted_passphrase"
```

Using a Custom Certificate and Private Key

All commands contained in this section use OpenSSL. OpenSSL is typically shipped with Linux systems, but can be downloaded if it is not installed on your system from https://www.openssl.org/. This topic is written to work with Linux, but should work with Windows as well. PTC recommends using Linux to create the certificate and key because it is easier to obtain OpenSSL binaries and configuration files required. On Windows you need either to build OpenSSL from source, or to use a third-party installer (an informal list can be found here: https://wiki.openssl.org/index.php/Binaries).

To use custom certificates, private keys, certificate chains, and Certificate Authority list, refer to the following sections:

1. Creating a Private Key on page 40
2. Creating a Self-Signed Certificate — for Testing Purposes ONLY on page 41
3. Creating a Certificate Signing Request (CSR) on page 43
4. Creating a Certificate Authority (CA) on page 43
5. Creating a Custom Certificate Chain on page 44
6. Configuring the WS EMS and LSR to Use the Certificate Chain on page 44
7. Configuring the WS EMS to Use a Different Certificate Chain for Edge to Edge Communications (Optional) on page 45

Creating a Private Key

A private key is used to identify the WS EMS when it communicates with the LSR or other edge device. To create a private key, use the following command: `openssl genrsa -aes256 -out private_key.pem 2048`

When prompted, as shown below, enter a passphrase to be used to decrypt the private key:

```
openssl genrsa -aes256 -out private_key.pem 2048
Generating RSA private key, 2048 bit long modulus
.................................................................................-
.......................................................++
..................................................++
e is 65537 (0x10001)
Enter passphrase for private_key.pem:

Verifying - Enter passphrase for private_key.pem:
```

At this point you have a private key that can be used with the WS EMS or LSR. You now have a couple of options for creating or acquiring a certificate

Creating a Self-Signed Certificate - for Testing Purposes ONLY

⚠ Caution

For testing purposes ONLY, you can create a self-signed certificate to use with the WS EMS and Lua Script Resource (LSR). For security best practices, never use a self-signed certificates in production because they cannot be validated.

Run the following command to create a new self-signed certificate using the private key created in the preceding step:

```
openssl req -key private_key.pem -new -x509 -days 365 -out self_signed_
certificate.crt
```

Output similar to the following should be displayed when you run the command. When prompted, fill in the passphrase for the private key and then the X509 identity information:

```
openssl req -key private_key.pem -new -x509 -days 365 -out self_signed_
certificate.crt
Enter pass phrase for key.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:MA
Locality Name (eg, city) []:Boston
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PTC
Organizational Unit Name (eg, section) []:Thingworx
Common Name (e.g. server FQDN or YOUR name) []:Example Certificate
Email Address []:example@ptc.com
```

Note that the `-days 365` argument is used, which means this certificate is valid for one year. Consult the OpenSSL user's guide for more details on how to customize the length of time your certificate is valid.

You now have a self-signed certificate that you can use with the WS EMS and LSR. To inspect the contents of the certificate, use the following command:

```
openssl x509 -in self_signed_certificate.crt -text -noout
```

This command products output similar to the following, which shows the X509 identity information entered earlier in the `Issuer` and `Subject` fields:

```
openssl x509 -in self_signed_certificate.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 10278892931034865755 (0x8ea5f6a92e9b605b)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=MA, L=Boston, O=PTC, OU=Thingworx, CN=Example
Certificate/emailAddress=example@ptc.com
        Validity
            Not Before: Apr 20 20:46:33 2020 GMT
            Not After : Apr 20 20:46:33 2021 GMT
        Subject: C=US, ST=MA, L=Boston, O=PTC, OU=Thingworx, CN=Example
Certificate/emailAddress=example@ptc.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a4:ed:ba:e0:f7:97:21:ce:b3:97:0f:68:49:1f:
                    d7:fa:de:48:d8:98:37:38:a4:ef:72:5d:c0:1c:e8:
                    23:77:dc:b6:bc:8a:3d:b0:b0:5a:45:77:f7:d4:1e:
                    78:c9:f3:e0:4e:ce:4d:1d:47:6c:09:a2:18:b8:32:
                    df:16:ff:24:34:b6:84:3f:3e:eb:65:f7:96:77:a4:
                    ad:eb:e2:38:f6:3b:24:63:64:45:bb:37:1f:71:81:
                    59:9d:81:bb:d2:9e:f6:03:cc:d3:05:30:95:4d:94:
                    96:ba:35:df:c3:7b:25:12:5a:bd:a0:b6:51:47:a8:
                    54:5d:2f:18:e2:3e:e8:39:1c:a6:3c:cc:2c:b2:7f:
                    25:4a:12:8c:27:d5:73:c2:95:71:e6:ec:9a:9a:01:
                    70:c2:09:6f:15:f7:e4:ad:c2:dc:d1:9b:55:5f:b6:
                    d4:a8:ca:e3:a8:45:9a:f9:84:c7:dd:17:c7:a3:bb:
                    19:e3:ef:75:53:2c:24:01:5c:31:c6:ad:1a:bd:e3:
                    76:e5:57:6e:4d:4e:c6:8f:a9:52:cb:52:01:5d:c2:
                    3d:b4:3b:62:8f:dd:20:2f:e9:b3:2e:32:cb:f6:c0:
                    c0:38:e1:9b:16:4a:6d:45:45:24:c7:b4:a9:12:75:
                    9f:7c:df:a8:20:96:31:22:42:53:ae:8e:5b:0d:86:
                    a7:2b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                60:24:2D:3F:C3:62:74:63:21:9E:71:06:4C:C3:8F:
D8:86:19:80:03
            X509v3 Authority Key Identifier:
                keyid:60:24:2D:3F:C3:62:74:63:21:9E:71:06:4C:C3:8F:
D8:86:19:80:03

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         6b:95:88:b4:6f:13:d6:2f:56:29:cb:1c:fb:3f:95:c0:a2:71:
         32:96:1c:87:dd:47:7a:c8:71:26:c4:b6:cf:f6:2a:ac:ce:07:
         03:51:b5:d4:b5:22:91:d4:4a:8c:12:7b:8e:1e:4c:4b:10:51:
         da:d4:9e:c0:43:0d:bf:dd:08:60:b8:d0:35:10:d7:1a:7a:72:
```

```
        e2:29:c3:9a:4c:89:20:53:f3:5e:5c:e8:87:d0:1c:bb:8f:67:
        ab:d6:b2:ce:29:64:dc:27:bd:5d:a5:71:e4:6c:c2:f5:5e:0a:
        9c:fd:c3:7a:f3:74:6c:ba:ae:bb:7b:86:95:e0:00:0d:e9:e2:
        7a:18:3b:a5:39:c8:77:15:23:39:8e:1b:40:c1:2f:5c:fc:dc:
        24:6a:e8:7b:f9:14:93:7d:1a:4b:f0:f5:54:34:a1:23:16:44:
        f8:43:99:ba:52:cf:5c:67:70:94:e0:7d:2d:5f:d5:a3:95:ac:
        b5:ad:2c:07:6e:05:c3:a7:37:8d:f4:7f:00:81:48:08:81:13:
        45:ec:23:8c:0d:79:ce:da:68:c8:91:01:66:e4:53:7b:8f:f7:
        0e:55:4e:08:91:77:d2:79:7b:df:05:40:f3:a6:9d:de:98:28:
        3d:00:fa:c9:de:c5:f1:1e:d6:ef:43:05:a5:0b:f3:b5:cc:b2:
        e2:ff:cc:65
```

Note

If you must use a self signed certificate for testing purposes, you must enable self-signed certificate support in the `config.json` file for the WS EMS:

```
"certificates": {
  . . .
  "allow_self_signed": true
  . . .
}
```

and in the `config.lua` file for the LuaScriptResource (LSR):

```
scripts.rap_deny_selfsigned = false
```

Do not use this configuration in production!

Creating a Certificate Signing Request (CSR)

If you are purchasing your certificate from a commercial organization or your company runs its own certificate authority, you most likely have to create a Certificate Signing Request (CSR) to acquire a certificate. This process should be detailed by whoever manages the signing request.

Creating a Certificate Authority (CA)

Creating a Certificate Authority (CA) can be the most flexible, but also the most complicated option, the details of which are outside the scope of this guide. Creating your own CA allows you to control the entire chain of trust. A detailed guide to accomplish this can be found here.

Creating a Custom CA Certificate List

To validate that the ThingWorx Platform (server) with which it is communicating is trusted, an Edge device (client) must have a list of trusted certificate authorities that are expected from the ThingWorx Platform (server). This list is referred to as a Certificate Authority list and as a certificate chain. The rest of this section uses certificate chain.

To create a certificate chain, create a file that contains all the Certificate Authority (CA) certificates that you want your agent to trust. This file will typically contain the root and intermediate CA certificates that are used on the ThingWorx Platform (server) with which the WS EMS (client) communicates, as well as the root and intermediate CA certificates that were used to create the certificates used by the WS EMS and the LSR. Here is an example of a Certificate Authority List:

```
-----BEGIN CERTIFICATE-----
(Root CA Certificate)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Intermediate CA Certificate)
-----END CERTIFICATE-----
```

Store the chain in a PEM-encoded certificate file. This file allows the client to validate each node in the certificate chain presented by the server during the TLS handshake. If you have certificate validation enabled, you must create and configure a certificate chain. If you are using a self-signed certificate, you do not need to configure a chain.

Certificate validation requires that root keys be distributed independently, so the self-signed certificate that specifies the root certificate authority may optionally be omitted from the chain. In this case, it is assumed that the remote device must already possess the root certificate authority in order to validate it.

Example

Certificate Chain Example

```
-----BEGIN CERTIFICATE-----
(Your EMS Server Certificate)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(The Intermediate CA Certificate of the issuer of the EMS Server
Certificate)
-----END CERTIFICATE-----
```

Configuring the WS EMS and LSR to Use the Certificate Chain

To use the certificate chain, you can enable it in the same way you would configure a certificate, using the following options in `config.json` for the WS EMS and in `config.lua` for the Lua Script Resource. The following examples show what to add in both of these configuration files:

Example

config.json

```
"certificates": {
  . . .
  "cert_chain": "/path/to/certificate_chain/file"
  . . .
}
```

Example

config.lua

```
scripts.script_resource_certificate_chain = "/path/to/certificate_chain/
file"
```

Configuring the WS EMS to Use a Different Certificate Chain for Edge to Edge Communications (Optional)

The WS EMS provides a parameter called `http_client_ca_certs` that allows the use of a separate Certificate Authority (CA) certificate file that will only be used for Edge-to-Edge HTTPS connections. If this option is not used, the default CA certificate list set in the `cert_chain` property that is used to validate the platform connection will be used. This parameter is in the `certificates` group in the WS EMS configuration file.

Like the `cert_chain` property, the `http_client_ca_certs` is set in the `certificates` group of the WS EMS configuration file.

```
"certificates": {
    "cert_chain": "/path/to/ca_cert/file"
    . . .
    "http_client_ca_certs_: "/path/to/ca_cert/file"
}
```

Certificate Fingerprint Validation for WS EMS and LSR

The WS EMS/LSR support a security feature called "certificate fingerprint validation" that allows you to restrict HTTPS communication to a known set of trusted HTTPS server endpoints at the Edge While TLS certificate validation ensures that your Edge device is talking to a server endpoint that uses a certificate issued by a trusted Certificate Authority (CA), certificate fingerprint validation ensures that your Edge device is talking only to a subset of explicitly trusted server endpoints.

The trusted HTTPS server endpoints can be REST endpoints that are configured with `auto_bind` to access a ThingWorx Platform through the WS EMS. They cannot be a ThingWorx Platform. The `auto_bind` feature provides a way of letting the WS EMS talk to HTTPS servers at the Edge that you want to represent as Things in ThingWorx. When you configure `auto_bind`, you must supply a REST endpoint for the WS EMS to communicate with. If the ThingWorx Platform makes a request down to that device, the WS EMS makes an HTTPS connection to the HTTPS server defined in the `auto_bind` configuration.

Note

Use of certificate fingerprint validation requires that SSL/TLS is enabled and configured for the WS EMS and LSR.

How Does Certificate Fingerprint Validation Work?

When an Edge device communicates with a server using HTTPS, it first validates that the server's certificate is issued by a Certificate Authority that is trusted. Next, it takes the SHA256 hash of the server's certificate, referred to as the certificate fingerprint, and compares it against an internal list of trusted fingerprints. If the fingerprint is found in the list, the connection is allowed to proceed. If it is not found, the connection is terminated.

Note

This feature is disabled by default. To enable it, you must generate certificate fingerprints and then add the `fingerprint_whitelist` property and the fingerprints to the configuration file. If you do not want to use it, do not add the property to the configuration file, not even as a placeholder for future use. Adding the property without adding fingerprint strings renders the configuration file invalid. The WS EMS does not start as a result.

Is Certificate Fingerprint Validation Used for Secure WebSocket Connections?

No, Certificate fingerprint validation is not supported on Secure WebSocket Connections to the ThingWorx Platform. TLS certificate and host name validation are used to confirm that the platform server endpoint is trusted.

Generating Certificate Fingerprints

The instructions for generating certificate fingerprints in this section apply to both WS EMS and LSR.

You can use OpenSSL used to generate certificate fingerprint values for a given certificate using the following command:

```
openssl x509 -noout -fingerprint -sha256 -inform pem -in
[certificate-file.crt]
```

Where `[certificate-file.crt]` is the path to your certificate. This command produces strings similar to the output below.

```
C:\OpenSSL-Win32\bin>openssl x509 -noout -fingerprint -sha256
-inform pem -in c:\test\cert.cer
SHA256 Fingerprint=E6:EF:5D:37:22:FC:EF:EA:4B:22:92:45:BD:49:
D2:29:3D:84:19:BC:C3:45:23:A1:22:A4:01:20:9D:03:E6:47
```

Copy the fingerprint value that is printed to the console and place it into the WS EMS or LSR configuration file. Fingerprints can contain the characters 0-9, A-F, and `:`. The `:` character is optional and ignored when the value is read.

Using the example above, the fingerprint of the certificate to copy and place in your configuration file would be

```
E6:EF:5D:37:22:FC:EF:EA:4B:22:92:45:BD:49:D2:29:3D:84:19:BC:
C3:45:23:A1:22:A4:01:20:9D:03:E6:47
```

Adding Certificate Fingerprints to the WS EMS Configuration File

To enable fingerprint validation, you must add the `fingerprint_whitelist` property to the `certificates` group in the `config.json` configuration file of the WS EMS. The `fingerprint_whitelist` must consist of an array of strings in which each string contains a certificate fingerprint. For example:

```
{
  "certificates": {
      . . .
      "fingerprint_whitelist" : [
         "E6:EF:5D:37:22:FC:EF:EA:4B:22:92:45:BD:49:D2:29:3D:84:19:
BC:C3:45:23:A1:22:A4:01:20:9D:03:E6:47",
         "D1:BA:B0:17:66:6D:7F:42:7B:91:1E:22:7E:3A:27:D2:
EF:5D:37:22:FC:EF:EA:4B:22:92:45:BD:01:7E:92:52"
      ]
      . . .
  }
}
```

⚠ Caution

If you leave this property in the configuration file without any fingerprint strings, the `config.json` file is invalid, causing the WS EMS to stop when it attempts to read this configuration file.

Adding Certificate Fingerprints to the LSR Configuration File

To enable fingerprint validation for the LSR, you must add the `fingerprint_whitelist` property to the `certificates` group in the `config.lua` configuration file of the LSR. The `fingerprint_whitelist` must consist of one or more strings, each string containing a certificate fingerprint. If multiple strings are used, separate them using a comma, as shown here:

```
-- Single fingerprint
scripts.fingerprint_whitelist = "E6:EF:5D:37:22:FC:EF:
EA:4B:22:92:45:BD:49:D2:29:3D:84:19:BC:C3:45:23:A1:22:
A4:01:20:9D:03:E6:47"
-- Multiple Fingerprints
scripts.fingerprint_whitelist = "E6:EF:5D:37:22:FC:EF:
EA:4B:22:92:45:BD:49:D2:29:3D:84:19:BC:C3:45:23:A1:22:
A4:01:20:9D:03:E6:47,
D1:BA:B0:17:66:6D:7F:42:7B:91:1E:22:7E:3A:27:D2:EF:5D:37:22:FC:EF:
EA:4B:22:92:45:BD:01:7E:92:52"
```

⚠ Caution

If you leave this property in the configuration file without any fingerprint strings, the `config.lua` file is invalid, causing the LSR to stop when it attempts to read this configuration file.

Enabling Certificate Fingerprint Validation on Communications Between WS EMS and LSR

To enable certificate fingerprint validation on communication between the WS EMS and LSR, you must follow these steps:

1. Add the fingerprint of the certificate used by the HTTP server of the WS EMS to the `scripts.fingerprint_whitelist` of the LSR. Recall that the WS EMS HTTP server certificate is configured using `http_server.certificate`.
2. Add the fingerprint of the certificate used by the HTTP server of the LSR to the`fingerprint_whitelist` of the WS EMS. Recall that the LSR HTTP server certificate is configured using `scripts.script_resource_certificate_chain`.

Tip

If the LSR or WS EMS inter-operates with any other devices on the local area network using HTTPS, such as a device defined by an `auto_bind` configuration, the fingerprint of the certificate used by that device must be added to the fingerprint whitelist of the WS EMS and/or LSR

Authenticating and Binding

The `appkey` group of the configuration file is used for authentication. The WS EMS must be authenticated to connect to a ThingWorx platform instance.

An application key is an authentication token that is generated by the ThingWorx platform instance and that represents a specific user. The application key is sent along with the connection request to authenticate the WS EMS with the ThingWorx Platform instance, and apply the correct permissions that are associated with the application key's user account.

Tip

To encrypt your application key before copying it to the `config.json` file for your WS EMS, refer to Encrypting Application Keys, Passwords, and Passphrases on page 36.

The application key is set by a simple top-level key in the JSON structure.

```
"appkey": "some_encrypted_application_key",
```

Note

The code sample above is provided for example purposes only. Copy and paste the application key that you generated and encrypted into the value side of `"appkey":"some_encrypted_application_key"`.

💡 **Tip**

Enabling authentication is an important component of a secure configuration. For examples of secure configurations for communications between the WS EMS and the LSR, refer to Examples of Configuring Secure Communications between the WS EMS and an LSR on page 159 . These examples are presented in order of least secure (testing purposes ONLY) to most secure (strongly recommended for production environments).

Binding

Once another device registers with the WS EMS (by sending an auto bind message), the WS EMS sends a BIND message to the ThingWorx Platform instance on behalf of that device. The ThingWorx Platform instance then associates the WebSocket on which WS EMS is communicating with a Remote Thing on the platform instance whose name or identifier matches the name or identifier sent by the WS EMS (the Remote Thing must have been created on the platform instance, using the **RemoteThing** Thing Template or one of its derivative templates). This association is the binding that must exist so that the platform instance can send requests to the device that is communicating through the WS EMS. For information about automatic binding and the WS EMS, refer to the section, Configuring Automatic Binding for WS EMS on page 73. For information about configuring the gateway option for automatic binding, refer to Auto-bound Gateways on page 75.

Protecting Data with Encryption

The WS EMS and LSR use a data protection library that provides automated encryption of application keys, passwords, and other sensitive information in configuration files. Data is protected by a unique data protection key, `dp.dat`, that is automatically created by the WS EMS or LSR the first time it runs. Any existing encrypted data in configuration files is automatically converted to use the updated encryption method.

This topic first explains how to enable and disable encryption for the WS EMS. It then provides information about using the new data protection library for automatic encryption with both the WS EMS and LSR, in the following sections:

- Automatic Configuration Encryption on page 52
- Modifying Encrypted Parameters on page 52
- Data Security Key on page 52

How to Enable and Disable Encryption

You enable or disable encryption in the `ws_connection` group of the configuration file. By default, the WS EMS always attempts to connect to a ThingWorx Platform instance, using SSL/TLS (that is, encryption is enabled).

Note

The code samples below are provided for example purposes only.

To enable encryption, specify the properties as shown below:

```
"ws_connection": {
  "encryption" : "ssl"
}
```

To disable encryption (NOT recommended), specify the properties as shown below:

```
"ws_connection": {
  "encryption" : "none"
}
```

Tip

Always enable encryption. Otherwise, the WS EMS and LSR will log warning message (console).

The `ws_connection` group contains the following property:

Property	Description
`encryption`	Whether or not encryption is enabled for communications with the ThingWorx Platform instance, and the type of encryption used. Valid values are: • `none` • `ssl` **Note** The previously available `fips` value has been replaced with a group (`fips`) and a property (`enabled`. Refer to Configure FIPS Mode on page 37for information about configuring FIPS mode.

Automatic Configuration Encryption

The WS EMS provides an automatic encryption feature that automatically encrypts sensitive data in configuration files on start-up. This feature is designed to make it easy to update existing configuration files that use either the legacy encryption format, or no encryption at all. This feature is always enabled and cannot be disabled. The data security library uses the XChaCha20-Poly1305 Cipher for encryption of data at rest.

When the WS EMS or LSR is started, all data previously encrypted with the legacy encryption format (AES) is automatically updated to use the latest format. Additionally, any plaintext values considered to be sensitive, such as application keys, passwords, or passphrases for private keys are also automatically encrypted.

Modifying Encrypted Configuration Properties

You can replace a parameter that has been encrypted in a configuration file with a new plaintext value, and it will be automatically encrypted when the WS EMS or LSR starts.

Data Security Key

The WS EMS automatically appends a property, called "Data Security Key Hash", to the configuration files for the WS EMS and LSR The WS EMS and LSR check the value of this property to detect any potential modification to the data security key between start ups. If this value is determined to be different than the value expected, a warning message is written to the log. In addition, decryption may fail if the key has changed.

This field should not be modified by users and can be ignored. The value appears at the end or your configuration file

- `data_security.key_hash` in WS EMS `config.json`
- `scripts.data_security_key_hash` in LSR `config.lua`

Running the ThingWorx WS EMS

The ThingWorx WS EMS can be run either from a command line or as a Linux daemon or Windows service on page 54 to establish a to ThingWorx Platform.

Running WS EMS from a Command Line

The WS EMS can be run from a command line as follows:

1. Open a command window or terminal session on the system or device that is hosting the WS EMS.
2. Change to the directory, `\microserver\etc`.

3. For a basic configuration, copy the file, `config.json.minimal`, and rename it to `config.json`. Even for a complex configuration, start with your basic `config.json` file to ensure first that you can run the WS EMS.

⚠ Caution

Do not attempt to use `config.json.documented` as is to run your WS EMS. It is intended as a reference, not as a valid JSON file that you can use to run WS EMS. Instead, use `config.json.complete` to run WS EMS using all available properties. Make sure that you save `config.json.complete` as `config.json` , and set all of the minimally required properties (refer to the next step).

4. Set the configuration properties:
   - For a simple configuration that establishes a connection to ThingWorx Platform, refer to the section, Creating a Configuration File on page 26.
   - For a more complex configuration, start with the section, Creating a Configuration File on page 26, and then continue to the section, Viewing All Configuration Options on page 60.
5. Save the configuration file as `config.json`.

Note

The configuration file must be named `config.json` and reside in the `\microserver\etc` directory.

6. Change directories back to the top-level directory, `\microserver`.

You are ready to run the WS EMS, as follows:

1. To run the WS EMS, enter the command, `wsems`.

   As part of initialization, the WS EMS checks the configuration file settings. Once initialized, the WS EMS prints its version number to the console and log file, attempts to connect to ThingWorx Platform, and returns a message that the connection was successful to the console. You can tell that WS EMS is running and connected to ThingWorx platform by looking at the console prompt — two plus signs (++) indicate that it is running and connected.
2. Should you need to shut down the WS EMS, press ENTER to display the console prompt and type `q`.

Note

The Windows-based operating systems have a tick resolution (15ms) that is higher than the tick resolutions requested by the C SDK (5ms). For information about achieving the best performance in a Windows-based operating system, refer to Running on a Windows-based Operating System on page 169.

Running WS EMS as a Daemon (Linux) or as a Windows Service

To run WS EMS and the LSR as daemons or services, you first need to "install" them and then you can start them as you would any other daemon or service. Follow these steps:

1. Open a command window or terminal session on the system or device that is hosting the WS EMS.
2. Change to the `\microserver\etc` directory.
3. For a basic configuration, copy the file, `config.json.minimal`, and rename it to `config.json`. Even for a complex configuration, start with your basic `config.json` file to ensure that you can run WS EMS.

   Caution

   Do not attempt to use `config.json.documented` as is to run your WS EMS. It is intended as a reference, not as a valid JSON file that you can use to run WS EMS. Instead, use `config.json.complete` to run WS EMS using all available properties. Make sure that you save `config.json.complete` as `config.json` , and set at least all of the minimally required properties (refer to the next step).

4. Set the configuration properties:
   - For a simple configuration that establishes a connection to ThingWorx Platform, refer to Create the WS EMS Configuration File on page 26 and Configure the Connection to ThingWorx Platform on page 28.
   - For a more complex configuration, start with the section, Create the WS EMS Configuration File on page 26, and then continue to the section, Additional Configuration Options on page 58.

5. Save the configuration file as `config.json`.

Note

The configuration file must be named `config.json` and reside in the `\microserver\etc` directory.

6. Follow the steps for your operating system:

- For Windows:

  a. Change into the `\microserver\install_services\` directory.

  b. Run the following command to install WS EMS and LSR as Windows services, with or without the options to create custom names:

  ```
  install.bat [-wsems your_name_for_wsems_service_here]
  [-lsr your_name_for_lsr_service_here]
  ```

  Use only one hyphen (-) for the options. There is a space between the option and the argument, but for Windows, you must use the full option name.

- For Linux:

  a. Change to the `\microserver\install_services\` directory.

  b. To make the install script executable, use the following command:

  ```
  sudo chmod +x microserver/install_services/install
  ```

  c. Run one of the following commands to install the WS EMS and LSR as daemons:

  ○ Linux, using short names for the options

  ```
  sudo ./microserver/install_services/install \
       [-w your_name_for_ws_ems_service_here] \
       [-l your_name_for_lsr_service_here]
  ```

  Use only one hyphen (-) for the options. There is a space between the option and the argument.

  ○ Linux, using long names for the options:

  ```
  sudo ./microserver/install_services/install \
       [--wsems=your_name_for_ws_ems_service_here] \
       [--lsr=your_name_for_lsr_service_here]
  ```

  Note that the long options require two hyphens (--) before the option name, an equal sign following the name, and no space between the equal sign and the argument (your name for the service).

Note

To uninstall the service, remove the service from `/etc/init.d/<Service Name>`.

As part of initialization, the WS EMS checks the configuration file settings. Once initialized, the WS EMS prints its version number to the console and log file, attempts to connect to WS EMS, and returns a message that the connection was successful to the console. You can tell that WS EMS is running and connected to ThingWorx Platform by looking at the console prompt — two plus signs (++) indicate that it is running and connected.

How the Startup Process Works and What May Happen

When the WS EMS starts, it attempts to read the `config.json` configuration file. If the configuration file is invalid, the WS EMS stops. The configuration file may be invalid because, for example, the `fingerprint_whitelist` property was added without any content. When the WS EMS fails to start, it writes a warning message to the log. By checking the log of the WS EMS, you can determine that this empty property group was the cause of the problem

Note

The validation process is not necessarily done on every single configuration value in the file. Only certain explicit values are checked.

If the WS EMS can read the configuration file, it starts to process it. If it encounters a logical error, the WS EMS writes an error to the log and exits. For example, you enabled SSL on your HTTP server but did not provide a path to a certificates file.

If a connection to a server is rejected, you can determine the cause of the failure by looking in the WS EMS log. If a connection is rejected because of a mismatch in TLS host names or certificate fingerprint validation, a warning message is written to the log. For fingerprint validation, no message is written to the log if it succeeds.

Tip

The data security library provided with v.5.4.8 and later of the WS EMS and LSR uses the XChaCha20-Poly1305 Cipher for encryption of data at rest. For more information about automatic encryption, refer to Automatic Configuration Encryption on page 52. The legacy encryption method for WS EMS and LSR v.5.4.7 and earlier is AES encryption for data at rest.

Verifying Your Connection

Following the initial message that indicates a successful connection to the ThingWorx Platform instance, you can verify your connection as follows:

1. Open a web browser on the system or device that is hosting the WS EMS, and enter the following URL in the address bar:

   ```
   http://localhost:8000/Thingworx/Things/LocalEms/Properties/isConnected
   ```

   This request returns an `InfoTable` that contains a single row that indicates whether the WS EMS is online or offline.
2. If the result of this request is true, the WS EMS is online. To test that you can access data on the ThingWorx Platform instance, enter the following URL in the address bar:

   ```
   http://localhost:8000/Thingworx/Things/SystemRepository/Properties/
   name
   ```

   This request returns an `InfoTable` that is serialized to JSON, where the `row` of the `InfoTable` contains the name of the requested Thing, “SystemRepository”.
3. If both of these tests succeed, the WS EMS is successfully connected to the ThingWorx platform instance.

3

Additional Configuration of WS EMS

This section describes how to configure additional options of the WS EMS.

The `config.json.complete` and the `config.json.documented` files provided in the WS EMS installation contains all possible configuration properties. To allow you to run WS EMS using `config.json.complete`, all of the comments have been removed from the file. Instead, `config.json.documented` is provided as the reference file for configuration information for all of the possible configuration properties for WS EMS.

⚠ Caution

Do not attempt to use `config.json.documented` as is to run your WS EMS. It is intended as a reference, NOT as a valid JSON file that you can use to run WS EMS. Instead, use `config.json.complete` to run WS EMS, using all of the possible configuration properties.

Some properties in the *`config.json.complete`* file have default values that you may not need to change. The rest of this section describes the properties that are used most often.

Note

If you are using the Lua Script Resource (`luaScriptResource.exe`) to communicate with one or more local devices, you also need a `config.lua` in the `/etc` directory. This file tells the Lua process how to initialize and communicate with ThingWorx Platform through the WS EMS. For more information, refer to Configuring a Lua Script Resource on page 138.

Viewing All Configuration Options

The file, config.json.documented, is provided in the WS EMS distribution. It contains all the possible options that you can configure for your WS EMS plus a few comments to help you understand each group and property. To view these options, follow these steps:

1. From the WS EMS installation directory, change to the directory, /etc.
2. Open the file, config.json.documented in a text editor.
3. Refer to this file while you read about the groups of the configuration file.

The comments in this file provide brief descriptions of the properties. The rest of this section walks you through the properties that are used most often.

⚠ Caution

Do not attempt to use config.json.documented as is to run your WS EMS. It is intended as a reference, not as a valid JSON file that you can use to run WS EMS. Instead, if you want to copy all properties, open config.json.complete in a text editor and save it as config.json. Make sure that you preserve the original configuration files.

Setting an Option to Use the Restart REST Service

The **Restart** REST service on page 130 requires on a configuration option to be added to the *config.json* file of the WS EMS so that any edge-side restart requests work correctly. Otherwise, only requests from the ThingWorx platform can restart the WS EMS. The **restart** configuration option is a top-level option in *config.json* and should be set to one of the three values, as shown here:

```
"restart" : "any"     // Allow anyone to restart the WS EMS (Local or
Server)
"restart" : "local"   // Only allow local Edge devices to restart the WS
EMS
"restart" : "server"  // Only allow the ThingWorx Platform to restart the
WS EMS
```

Configuring the Logger Group

Use the logger settings to configure a WS EMS to collect logging information. Here is an example of this group:

```
 "logger":{
    "level": "WARN",
    "audit_target": "file:// or http://",
    "publish_directory":"/_tw_logs/",
    "publish_level":"WARN",
    "max_file_storage":2000000,
    "auto_flush":true,
    "flush_chunk_size":16384,
    "buffer_size":4096
},
```

The following table lists and describes the properties of the `logger` element :

Use	To Specify
`level`	The level of information that you want to include in the audit log file. The default level is `WARN`. Valid values include: • `AUDIT` • `ERROR` • `WARN` • `INFO` • `DEBUG` • `TRACE` **Tip** When troubleshooting a problem, set the `level` to `TRACE` so that you can monitor all the activity. For production, set the `level` to `ERROR` if you want to view error messages.
`audit_target`	The path to the audit log file where audit events will be written Alternatively, specify an HTTP address for the audit log file, where these events will be sent using a POST command. Audit events are also written to the normal log destination. If no target is specified, no additional auditing takes place. Valid values include: • `file://`*`path_to_file`* • `http://`*`hosted_location`*
`publish_directory`	A location for writing to log files those log events that meet or exceed the `publish_level`. If you do not specify a location for this property, this logging information is not written to log files. The default value is `"publish_directory":"/_tw_logs/",` **Caution** The LSR and WS EMS use the same naming scheme for log files. Specify a directory that is different from the one specified in the `publish_directory` property in the `config.json` file of the WS EMS.
`publish_level`	The level of information that you want to include in the alternate log

Use	To Specify
	files. The default value is `logger:level`, which tells WS EMS to use the same level as set in the `level`property. Valid values are the same as for the `logger.level` property: • AUDIT • ERROR • WARN • INFO • DEBUG • TRACE
`max_file_storage`	The maximum amount of space that log files can take up. Keep in mind that there are two concurrent log files. The maximum size of each individual log file is `max_file_storage` divided by 2. The default value is `2000000` bytes.
`auto_flush`	Whether WS EMS should flush every `N` bytes to the `publish_directory`. The `N` value is defined by `flush_chunk_size`. WS EMS also flushes the buffer if a message has not been written to the log in the last second. A setting of `true` for `auto_flush` forces WS EMS to flush every `16384` bytes by default.
`flush_chunk_size`	The number of bytes to write before flushing to disk. The default setting is 16KB.. **Tip** It is strongly recommended that you keep the default setting . You cannot effectively go lower than the value of your setting for the `buffer_size` property. Although no limits are enforced, it strongly recommended that you NOT use a value that is higher than the default value.
`buffer_size`	The maximum number of bytes that can be printed in a single logging message. The default setting is 4096 bytes. **Tip** It is strongly recommended that you keep the default setting. Modify this value only if you have issues with logging speed or other performance issues, or if you are getting truncated messages in the log. If you expect to have very long messages that you want logged, increase this value.

As of version 5.4.0, the actual time is no longer used in the logs for the WS EMS and the Lua Script Resource (LSR). Instead, the logs use UTC timestamps.

As of version 5.3.4 of WS EMS, logging behavior changed, as follows:

- The same format is used in log messages written to the console (text) as in log messages written to the persisted log files (formerly JSON). The log messages are no longer wrapped in a JSON object. The persisted log files are just text files. Their content will match what is printed out on the console.
- You can specify certain limitations for logging. The property, `buffer_size`, allows you to specify the maximum number of bytes that can be printed in a single log message. In addition, the property, `flush_chunk_size`, allows you to specify a maximum of bytes to write before flushing to disk. If a message has not been written to the log in the last second, the buffer is flushed. These properties and their default values are shown in the `config.json.documented` configuration file in the WS EMS installation.

⚠ Caution

Do not attempt to use `config.json.documented` to run your WS EMS. This file is intended as a reference. Instead, if you want to use all possible properties, use `config.json.complete`. Be sure to save the file as `config.json` before running WS EMS.

Configuring the HTTP Server Group

The `http_server` group is used to allow a WS EMS to accept local calls from the machine or device code that may be running in a different process, such as the Lua Script Resource.

Note

If you are connecting from the Lua Script Resource and have changed the `host` and `port` properties for the WS EMS, you must update the `config.lua` file (in the `/microserver/etc` directory) and modify the properties, `scripts.rap_host` and `scripts.rap.port`.

Here is an example of the `http_server` group. Change the values of the properties to fit your environment; do not use this example as is.

```
 "http_server":  {
     "host" : "localhost",
     "port": 8000,
     "ssl": true,
     "certificate" : "/path/to/certificate/file",
     "private_key" : "/path/to/private/key",
     "passphrase" : "password"
     "authenticate" : true,
     "user" : "johnsmith",
     "password" : "some_encrypted_user_password",
     "content_read_timeout": 20000
     "ports_to_try" : 10
     "max_clients" : 15
     "enable_csrf_tokens" : true
     "csrf_token_rotation_period" : 10
},
```

⚠ Caution

Always configure a secure HTTP server. Otherwise, the WS EMS and LSR will log warning messages when SSL, authentication, or certificate validation is disabled or when self-signed certificates are allowed. Starting with v.5.4.8 of the WS EMS and LSR, application keys and passwords are automatically encrypted on the first startup of the WS EMS or LSR. For information about automatic encryption, refer to Automatic Configuration Encryption on page 52. For earlier versions, you can learn how to encrypt these secrets in Encrypting Application Keys, Passwords, and Passphrases on page 36.

For examples of secure configurations for communications between the WS EMS and the LSR, refer to Setting Up Secure Communications for the WS EMS and LSR on page 159. These examples are presented in order of least secure (testing purposes ONLY) to most secure (strongly recommended for production environments).

Tip

The WS EMS provides a parameter called `http_client_ca_certs` that allows the use of a separate Certificate Authority (CA) certificate file that will only be used for Edge to Edge HTTPS connections. If this option is not used, the default CA certificate list that is used to validate the platform connection will be used. This parameter is in the `certificates` group in the WS EMS configuration file. For more information, refer to Using a Custom Certificate and Private Key on page 45.

The following table lists and describes the properties in the `http_server` group
:

Property	ThingWorx Base Type	Description
`host`	STRING	The name of the host that the WS EMS listens to. The default value is `localhost`, but this value means IPV6 `localhost` and not `127.0.0.1`. Change this value to `127.0.0.1` to use IPV4 instead. To configure an IP address other than `localhost` or `127.0.0.1` for REST Web Service calls, refer to Configuring WS EMS to Listen on IP Other Than localhost on page 88
`port`	NUMBER	The port number on which the WS EMS listens for messages from clients running the LSR. Typically, incoming messages on this port are from an LSR instance/application, but it is possible for any other application to send messages to the WS EMS HTTP Server.. The default port is `8000`.
`ssl`	BOOLEAN	Whether or not to use SSL/TLS for communications between clients running the LSR and WS EMS. The default value is `true`.
`certficate`	STRING	When `ssl` is `true`, specifies the complete path to the certificate file that WS EMS will use when connecting to LSR clients. The default value is an empty STRING. **Note** The file does not need to be located in the installation directory for the WS EMS. However, you must specify the full path to the certificate file, no matter where you store the file.
`private_key`	STRING	When `ssl` is `true`, specifies the complete path to the private key that WS EMS will use when connecting to LSR clients. **Note** The file does not need to be located in the installation directory for the WS EMS. However, you must specify the full path to the private key file, no matter where you store the file.
`passphrase`	STRING	When `ssl` is `true` and a `private_key` is used for connections with LSR clients, specifies the password defined for the private key. This value should be encrypted for security. For information about encrypting a passphrase, refer to Encrypting Application Keys, Passwords, and Passphrases on page 36.
`authenticate`	BOOLEAN	Whether or not to enable authentication between the

Property	ThingWorx Base Type	Description
		LSR clients and the WS EMS. The default value is `true`.
`user`	STRING	The user name to pass to the HTTP server. The example above shows a name as all lowercase and all one word. However, there are no restrictions on the user name other than it must be a valid STRING.
`password`	STRING	The encrypted password for the user named in the `user` property. For information about encrypting passwords, refer to Encrypting Application Keys,, Passwords, and Passphrases on page 36.
`content_read_timeout`	NUMBER	The maximum amount of time (in milliseconds) that the WS EMS will wait before timing out when it tries to read a PUT or POST. The default value is `20000` milliseconds (20 seconds).
`ports_to_try`	NUMBER	The number of additional ports to try. If it cannot bind on the configured port, WS EMS increments the port number by 1. The default value is `10`. For example, if the configured port is 8000, the next port to try would be 8001. If it could not bind to that port, the next port to try would be 8002, and so on. Port retries continue until the WS EMS binds to a port or until 10 ports plus the configured port have been tried. In this example, a total of 11 ports might be tried.
`max_clients`	NUMBER	The maximum number of clients that can be connected to the WS EMS at the same time. In this context, "clients" are devices that are running the LSR, connected to the WS EMS, and communicating with a ThingWorx Platform through the WS EMS. The default value is `15` clients.
`enable_csrf_tokens`	BOOLEAN	A flag to enable (`true`)or disable (`false`) the use of CSRF tokens with the REST services. By default the use of CSRF tokens is enabled. For more information, refer to Running REST API Calls with Postman on WS EMS and LSR on page 134.
`csrf_token_rotation_period`	NUMBER	The number of minutes between rotations of the CSRF token for a given session. The default value is 10 minutes.

Configuring the WebSocket Connection

The `ws_connection` group is used to configure the WebSocket connection between the WS EMS and the ThingWorx Platform. If the default settings meet your needs, there is no need to include this group in the configuration file.

The code sample below is provided for example purposes only. It shows the group as it appears in the `config.json.complete` file.

Caution

Do not attempt to use `config.json.documented` as is to run your WS EMS. It is intended as a reference, not as a valid JSON file that you can use to run WS EMS. Instead, use `config.json.complete`. All of the comments have been removed from this file to enable you to run WS EMS using it.

```
"ws_connection": {
     "encryption" : "ssl ",
     "verbose" : false,
     "msg_timeout" : 10000,
     "ping_rate" : 55000,
     "pingpong_timeout" : 10000,
     "message_idle_time" : 50000,
     "max_msg_size" : 1048576,
     "message_chunk_size" : 8192,
     "max_messages" : 500,
     "connect_timeout" : 10000,
     "connect_retry_interval" : 10000,
     "max_threads" : 4,
     "max_connect_delay" : 10000,
     "socket_read_timeout" : 0,
     "frame_read_timeout" : 10000,
     "ssl_read_timeout" : 500,
     "connect_retries" : -1,
     "compression" : true
  },
```

Note

As of v.5.4.3 of the WS EMS, duty-cycle modulation behavior and configuration have changed. The configuration of duty cycle has its own group in the `config.json` file. The two properties, `connect_period` and `duty_cycle`, have been moved from the `ws_connection` group to the `duty_cycle` group. A third property, `delay_duty_cycle` has been added. For details, refer to Configuring Duty Cycle Modulation on page 69.

The following table lists and describes properties available to configure the WebSocket connection, in alphabetical order:

Use	To Specify
encryption	Whether SSL/TLS is used for the WebSocket connection. The default value is ssl. To disable SSL/TLS (NOT recommended), set this property to none.
verbose	Whether or not the WS EMS is in extremely verbose logging mode. The default value is false.
msg_timeout	The time in milliseconds to wait for a response to return from the ThingWorx platform. The default value is 10000 milliseconds (10 seconds).
ping_rate	The rate in milliseconds to send pings to the ThingWorx Platform. The default value is 55000 milliseconds.
pingpong_timeout	The amount of time in milliseconds to wait for a pong response after sending a ping. A timeout initiates a reconnect. The default value is 10000 milliseconds.
message_idle_time	The time in milliseconds to wait to refer to if messages are being sent before disconnecting for the off time of the duty cycle. The default value is 50000 milliseconds.
max_msg_size	The maximum size, in bytes, of a complete message, even if broken into frames. The default value is 1048576 bytes (1 MB).
message_chunk_size	The maximum size of a chunk — a piece of a large message that has been broken up into chunks. The default value is 8192 bytes.
max_messages	The maximum number of requests that can be waiting for a response at any one time. The default value is 500 requests.
connect_timeout	The maximum number of milliseconds, to wait for a connection to a ThingWorx platform instance to be established. The default value is 10000 milliseconds (10 seconds).
connect_retry_ interval	The number of milliseconds, to wait between attempts to connect to a ThingWorx platform instance. The default value is 10000 milliseconds (10 seconds).
max_threads	The maximum number of incoming message handler threads to use. The default value is 4.
max_connect_delay	The maximum amount of random delay time, in milliseconds, to wait before connecting. The default value is 10000 milliseconds (10 second delay before connecting).
socket_read_timeout	The maximum amount of time, in milliseconds, to wait for data before timing out. To match the best practices recommendation for transferring large files, the default value is 0 milliseconds. If your WS EMS does not transfer large files, consider setting this property to 100 ms. When set to a non-zero value, this property defines how long a process is allowed to wait for data before it must try again. Another process would be allowed to read from the socket between tries. A timeout does not trigger an error. Refer to the Note above for frame_read_timeout.
frame_read_timeout	The maximum amount of time, in milliseconds, to wait for a full SSL/TLS

Use	To Specify
	frame during a socket read operation. The default value is `10000` milliseconds. A timeout occurs if the WS EMS requests something from the ThingWorx platform and receives no data at all The timeout triggers an error and causes a disconnect. **Note** The difference between `socket_read_timeout` (described below) and `frame_read timeout` lies in the scope and context in which these timeouts are used. The `socket_read_timeout` is used everywhere — in tunnels, e.g. — and anywhere there is a raw socket read. The `frame_read timeout` is used in one place only — `twWs_Receive()` and then only after a WebSocket header has been received. After that, there is an expectation that the remainder of the frame described in the header will arrive in a timely manner. This specialized amount of time is the `frame_read_timeout`.
`ssl_read_timeout`	The maximum amount of time, in milliseconds, to wait for a full SSL/TLS record during a socket read operation. The default value is `500` milliseconds. A timeout does not trigger an error. This property effectively allows a read to continue after the `socket_read_timeout` is reached IF a partial amount of the SSL/TLS record is received on the socket before the `socket_read_timeout` expires.
`connect_retries`	The number of times to retry the connection when it fails, as an INTEGER. The default value, `-1`, causes the WS EMS to retry forever.
`compression`	As of v.5.4.5, you can specify whether compression is enabled or disabled for websocket connections. By default this property is set to `true`, meaning that compression is enabled. Set this property to `false` to disable compression.

Configuring Duty Cycle Modulation

Duty cycle modulation enables developers to control the time that a WS EMS is connected to the ThingWorx Platform. It defines the frequency and duration of the connection between a WS EMS and a ThingWorx Platform. If you need to conserve power or bandwidth at the expense of availability/responsiveness, you can use duty cycle modulation. This feature may be useful if you have critical processes during which you want to disable communications for a device. By configuring duty cycle modulation in the `duty_cycle` group in the `config.json` file of your WS EMS, you can put the WS EMS into an offline mode.

As of v.5.4.3, duty cycle modulation keeps the WebSocket connection alive as long as there is activity within a configurable amount of time on the WS EMS (`delay_duty_cycle` property). The WebSocket connection enters a duty cycle **OFF** state only if there have not been any messages from the ThingWorx platform in the configured number of seconds. For example, if a file transfer is in progress, you may need to keep the connection open for an additional two minutes. The duty cycle has a separate configuration group in `config.json`, as follows:

```
"duty_cycle" : {
       "connect_period" " 60000,
       "duty_cycle" " 100,
       "delay_duty_cycle" : 60000
}
```

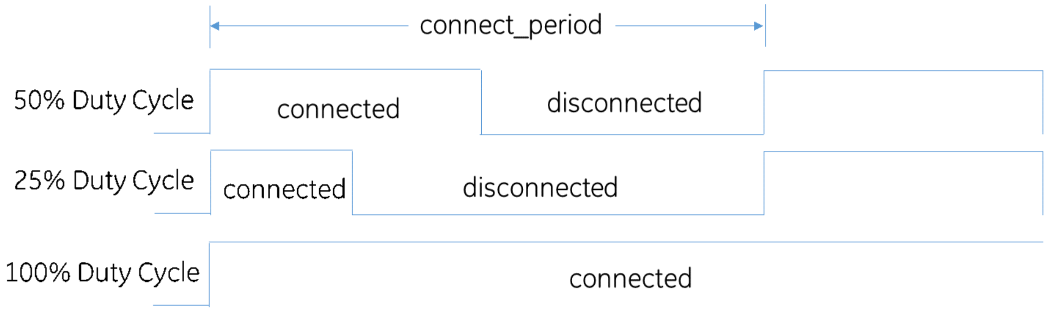
where

- `connect_period` — Defines the period of time set for duty cycle intervals. A value of 0 means that the WS EMS is always connected. The default rate is 60000 (one minute).
- `duty_cycle` — Determines what percentage of time during the connection period that the WS EMS is connected to the ThingWorx Platform. The default value is 100 percent, which means that the WS EMS is always connected. This value is also the maximum value for this property. A value of 0 also means that the WS EMS is always connected during the connection period.
- `delay_duty_cycle` — Defines the time interval (in milliseconds) for which the duty cycle should not be entered after receiving a message from the platform. The default value is 60000 milliseconds (one minute).

Note

If the `config.json` file does not have the `"duty_cycle"` group, the WS EMS assumes that its connection is always on (that is, `duty_cycle` is set to 0 or 100 percent).

The following diagram illustrates the effects of the duty cycle parameters on the connection between a WS EMS and a ThingWorx Platform:



In addition to the configuration file changes for duty cycle in v.5.4.3, the WS EMS has changed to enable it to track file transfers and tunnels, as well as property and service requests from the ThingWorx Platform. Duty cycle will not disconnect the WS EMS from the platform if any of the following conditions are true:

- A message has been received from the platform during the last `delay_duty_cycle` time interval.
- A message has been sent to the platform but no response has been received yet.
- A file transfer is pending or in progress.
- A remote session (tunnel) is in progress (open).

Finally the WS EMS will not be disconnected from the ThingWorx platform immediately after starting up. Instead, the WS EMS will disconnect at the next Duty Cycle event after startup. The next Duty Cycle event is the next time when the WS EMS should connect to or disconnect from the platform.

If the WS EMS is connected to the ThingWorx Platform, the next Duty Cycle event is calculated as follows:

```
nextDutyCycleEvent = Current time + ((connect_period * duty_
cycle)/100)
```

For example, if the `connect_period` is one minute (60,000 ms) and the `duty_cycle` is 30 percent, the WS EMS will disconnect after 18,000 milliseconds. That is, the WS EMS will remain connected for 30 percent of the `connect_period`:

```
(30/100) * 60000 = 18000
```

If the WS EMS is disconnected from the platform, the next Duty Cycle event is calculated as follows:

```
nextDutyCycleEvent = Current time + ((connect_period * (100  duty_
cycle))/100)
```

For example, if the `connect_period` is one minute (60,000 ms) and the `duty_cycle` is 30 percent, the WS EMS will connect after 42,000 milliseconds. That is, the WS EMS will remain disconnected for 70 percent of the `connect_period`:

```
((100 = 30)/100) * 60000 = 42000
```

Duty cycle is considered to be enabled if the following conditions are true:

- The `connect_period` is greater than zero. That is, the total number of milliseconds that the WebSocket will stay connected is greater than zero. The value of 0 indicates “AlwaysOn”.
- The `duty_cycle` is less than 100 and greater than 0. That is the percentage of the `connect_period` that the WS EMS remains connected to a ThingWorx platform is less than 100 and greater than 0. A value of 100 or 0 indicates “AlwaysOn”.

If an LSR pushes data (e.g., property value changes) to a WS EMS while the WS EMS is in the **OFF** state of a duty cycle, the data is stored in the offline message store and sent to the ThingWorx Platform once the WS EMS is connected again (duty cycle ON state).

Configuring a Proxy Server

The `proxy` group is used to configure the WS EMS to use a proxy server to connect to a ThingWorx Platform. For authentication with a proxy server, the WS EMS supports the following options:

- No authentication
- Basic authentication
- Digest authentication
- NTLM

Note

The code sample below is provided for example purposes only.

```
"proxy" : {
    "host" : "localhost",
    "port" : 3128,
    "user" " "username",
    "password" : "some_encrypted_password"
},
```

The following table lists and describes the properties for setting up a proxy server:

Use	To Specify
`host`	The host name of the proxy server used to connect to the ThingWorx Platform. The value of the host property can be an IP address, or a host name.
`port`	The port number used to communicate with the proxy server. The default value is 3128.
`user`	The name of the user account that is used to connect with the proxy server. In general, do NOT use the colon (`:`) character in user names.
`password`	The password of the user account that is used to connect with the proxy server. If you select to provide the user name and password for authentication with the proxy server, it is recommended that you encrypt the password as shown in the example above. To encrypt a password, refer to Encrypting Application Keys, Passwords, and Passphrases on page 36.

Storing Messages Received While WS EMS Is Offline

The `offline_msg_store` group is used to configure how the WS EMS handles and stores messages that are received while it is offline.

The following example shows the default configuration. If you do not want to use it, you do not have to change the configuration. When this feature is disabled, the other settings are ignored. However, if you do want to use this store, make sure you set the `enabled` property to `true` and add the appropriate directory for storing messages. Depending on the space available on your system, you may also want to change the `max_size` property.

```
"offline_msg_store": {
     "enabled": true,
     "directory" : "/path/to/offline/message/store/directory",
     "max_size": 65535
    },
```

The following table lists and describes the properties for storing messages that are received while the WS EMS is offline; it also provides the default values:

Property	Description
`enabled`	Whether or not the store is enabled. The default setting of `true` enables offline message store. Set this property to `false` to disable it.
`directory`	The path to the directory of the store where messages are stored. The default value is `"/path/to/offline/message/store/directory"`. Here is an example: `directory: "/opt/thingworx"` where `"/opt/thingworx"` is the directory where the WS EMS executable is installed (Linux).
`max_size`	The maximum size (in bytes) of the directory where messages are stored. The default value is `65535` bytes.

Configuring Automatic Binding for WS EMS

The automatic binding feature provides a way of letting the WS EMS talk to HTTP servers at the Edge that you want to represent as Things in ThingWorx. When you configure `auto_bind` you must supply a REST endpoint for the WS EMS to communicate with. If the ThingWorx Platform makes a request down to that device, the WS EMS makes an HTTPS connection to the server defined in the `auto_bind` configuration group.

The `auto_bind` group is used to define specific local things that are always expected to be bound through this WS EMS, or to define a WS EMS as a gateway. For more information about configuring WS EMS as a gateway, refer to Auto-bound Gateways on page 75.

⚠ **Caution**

When configuring the WS EMS for automatic binding, you can define only one gateway.

The `auto_bind` property is an array, allowing you to statically define more than one device or machine Thing.

Note

The code sample below is provided for example purposes only.

```
"auto_bind": [{
  "name" : "EdgeThing001",
  "host" : "localhost",
  "port" : 8001,
  "path" : "/",
  "timeout" : 30000,
  "protocol" : "http",
  "user" : "username",
  "password" : "some_encrypted_password",
  "gateway" : false
 }],
```

Best Practices

When configuring a host and a port for automatic binding, always use the same host and port as for the `http_server` configuration. This best practice prevents failure of a file transfer between the ThingWorx Platform, and a WS EMS. This includes transfers of file-based SCM packages. Refer to Troubleshooting File Transfers When Using Automatic Binding on page 167.

When using SSL/TLS between this device and the WS EMS, ensure optimal security by adding certificate fingerprint validation to the WS EMS configuration file. For details, refer to Certificate Fingerprint Validation for WS EMS and LSR on page 45.

The following table lists and describes the properties for automatic binding:

Property	Description
`name`	REQUIRED. This property specifies the Thing Name of the entity as it exists on the configured ThingWorx Platform instance. If an identifier is configured for the Thing on the platform instance, you must specify that identifier here. For more information, refer to the section, “Identifiers”, below.
`host`	This property specifies the name of the host machine for the Thing. The default

Property	Description
	value is `localhost`, but this likely means IPV6, and not 127.0.0.1.
`port`	This property specifies the port number used by the Thing/device for communications. The default value is `8001`.
`path`	This property specifies the path to prepend to the path received in the request from the ThingWorx Platform instance.
`timeout`	This property specifies the maximum amount of time to wait for a response from the target, in milliseconds. The default value is `30000` milliseconds (30 seconds).
`protocol`	This property specifies whether the protocol to use for communications is HTTP or HTTPS. The default value is `http`.
`user`	This property specifies the name of the user account to use for authentication when connecting. In general, do not use the colon (`:`) character in user names.
`password`	This property specifies the password for the user account specified for the `user` property. If you specify a user name and password, it is recommended that you encrypt the password. For details, refer to Encrypting Application Keys, Passwords, and Passphrases on page 36.
`gateway`	This property specifies whether this automatically bound Thing is a gateway or non-gateway Thing. By default, this property is set to `false`. To understand the differences between these two settings, refer to Auto-bound Gateways on page 75.

Identifiers

Identifiers provide a way to specify an alternate name for a given Thing. An identifier can be set for a Thing on the **General Information** tab of the Thing in ThingWorx Composer. If a Thing has an identifier set, the ThingWorx Platform must bind the Thing using the identifier. A typical use case for an identifier is the serial number for a device, as opposed to an intuitive name.

You can use an identifier when dynamically registering a Thing or when configuring the `auto_bind` group. To use an identifier, prepend an asterisk (*) to the identifier and specify it as the value for the `"name"` property, as follows:

```
{
   "name" : "*SN0012",
   "host" : "localhost",
   "port" : 9000,
   "path" : "/"
 }
```

Auto-bound Gateways

When you configure the `auto_bind` group of a WS EMS, it is very important to note the difference between the settings, `"gateway":true` and `"gateway":false`. When used with a valid `"name"` property, either value results in the WS EMS attempting to bind the Thing with the ThingWorx

Platform. In addition, either value allows the WS EMS to respond to file transfer and tunnel services that are related to the automatically bound things. However, the similarities end here.

Gateway

An auto-bound gateway can be bound to a ThingWorx Platform instance ephemerally if there is no Thing to bind with on the instance. Ephemeral binding is a temporary association between a platform instance and the WS EMS that lasts only until the WS EMS unbinds the gateway. In general, ephemeral things are created on a ThingWorx Platform when no Remote Things with a matching Thing Name exist on it.

When the WS EMS is attempting to bind a gateway, a Thing is automatically created on the ThingWorx Platform, using the **EMSGateway** Thing Template. The ThingWorx platform binds the auto-bound gateway with this ephemeral Thing. This Thing is accessible only through the WS EMS REST Web Service. Once the WS EMS unbinds the gateway, the ephemeral Thing is deleted

If you do not want the automatically bound gateway to be ephemeral, you can create a Thing for it and choose the **EMSGateway** Thing Template in ThingWorx Composer. If you do not choose this template for the Thing, the platform does not bind the gateway with your Thing.

When used both normally and ephemerally, the **EMSGateway** template provides some services that are specific to gateways. These services are not accessible to things that are created with the **RemoteThing** (and derivatives) Thing templates.

Note

The devices for which a WS EMS acts as a gateway can be set up to identify themselves to the WS EMS when they initialize and connect to it. Alternatively, when these devices are well known, you may want to define them explicitly in the WS EMS configuration. For examples of these two types of gateway configurations for a WS EMS, refer to the section, Example Configurations on page 89.

Non-Gateway

A Thing that is automatically bound but is not a gateway has the following requirements:

- For the WS EMS to respond to messages that are related to properties, services, or events for a non-gateway, automatically bound Thing, a LuaScriptResource must exist. Custom Lua scripts must exist within the LSR to provide the capabilities to handle services, properties, and events.

- For the non-gateway Thing to bind successfully, you must first create a corresponding Thing on ThingWorx Platform, using the **RemoteThing** Thing Template (or any template derived from **RemoteThing**, such as **RemoteThingWithFileTransfer**).

The most common use of this type of automatically bound Thing is to bind a simple Thing that can handle file transfer and tunnel services but does not need any custom services, properties, or events.

Note

For an example of a non-gateway configuration for WS EMS, refer to the section, Example Configurations on page 89.

Configuring File Transfers

To execute a file transfer, you need to configure options for both your client application and your ThingWorx instance. Transfers can be executed in either direction: from the edge application to your ThingWorx Platform or from the platform to the edge application.

Note

Keep in mind that the account associated with the application key must have the correct Read/Write permissions to the target and destination directories for a file transfer.

To transfer a file, the WS EMS must be configured with a set of virtual directories. The paths that you specify for the virtual directories must be absolute; the paths for the files must be relative to the virtual directories. For the WS EMS, these properties might look like this:

```
"file": {
  "virtual_dirs":[
   { "In" : "c:\\microserver_5.4.6-win32\\microserver\\in" },
   { "Out" : "c:\\microserver_5.4.6-win32\\microserver\\out" },
   { "staging" : "c:\\microserver_5.4.6-win32\\microserver\\staging" }
  ],
  "staging_dir" : "staging"
}
```

Note that when specifying the virtual directory paths for a Windows system, the backwards slash needs to be doubled (`c:\\microserver_5.4.6-win32\\microserver\\in`

If you use the additional parameters available for the `file` group, it might look like this:

```
"file": {
  "buffer_size": 1024000,
  "max_file_size": 8000000000,
  "virtual_dirs":[
      { "In" : "c:\\microserver_5.4.6-win32\\microserver\\in" },
      { "Out" : "c:\\microserver_5.4.6-win32\\microserver\\out" }
  ],
  "idle_timeout": 12000,
  "staging_dir" : "c:\\microserver_5.4.6-win32\\microserver\\staging"
 }
}
```

In this example, note in particular the value of the `buffer_size` property. This value affects performance of file transfers. The default value of 1024000 is recommended as a best practice to achieve optimal performance when transferring large files.

The `file` group configuration is important because you must pass the names of virtual directories in the parameters to the ThingWorx **Copy** service. As shown in the example above, you must use absolute paths.

The following table lists and describes the properties for file transfers:

Property	Description
`buffer_size`	The size of the buffer used for the file transfer, in bytes. The default value is `1024000` bytes (1MB), which is recommended as a best practice to achieve optimal performance when transferring large files. **Note** Setting the `socket_read_timeout` in the `ws_connection` group to 0 ms is also a best practice when transferring large files. Refer to the topic for the the `ws_connection` group on page 66
`max_file_size`	The maximum size of a file that can be transferred, in bytes. The default value is `8000000000` bytes (8GB).
`virtual_dirs`	An array of virtual directories that are used when browsing and sending files to the configured ThingWorx Platform. The directories are defined using absolute paths, as shown in the example above.

Property	Description
`idle_timeout`	The amount of time, in milliseconds, that the WS EMS waits before timing out a file transfer when the transfer is idle. Note that this value must be larger than the value of the `frame_read_timeout` property (in the `ws_connection` group on page 66). If this property is not set, the actual default value is 1.2 times the value of the `frame_read_timeout`. For example, if the `frame_read_timeout` is set to its default value of 10000 milliseconds, the default value of this property is 1.2 times 10000, or 120000 milliseconds (2 minutes).
`staging_dir`	A directory to use as a staging directory for files that will be transferred to the Edge device. As shown in the example above, this path must be an absolute path.

Tip

You do not have to have LSR running to perform a file transfer using WS EMS. However, you do need a bound Thing. In versions 8.3.5 and 8.4.x of the ThingWorx Platform, a service call was introduced, called **GetSupportedChecksums**. This service breaks previously working WS EMS configurations that use `auto_bind` for identity but do not specify a host and port. The workaround for this change is to make sure that your `auto_bind` configuration specifies the host and port used by the `http_server` configuration. Refer to Troubleshooting File Transfers When Using Automatic Binding on page 167.

Example

This example uses the **Copy** service of the **FileTransferSubsystem** entity for a file transfer. It makes the following assumptions:

- A **RemoteThingWithFileTransfer** named RT1 exists on the ThingWorx instance.
- The files are being transferred to/from the **SystemRepository** Thing.
- The WS EMS is installed in the directory, `C:\microserver` and that `C:\microserver\in`, `C:\microserver\out`, and `C:\microserver\staging` exist.
- The source file is located in the `files` directory of the **SystemRepository** Thing.
- The source and destination directories MUST exist AND be accessible to the WS EMS (Read/Write permissions).

In this example, the **Copy** service parameters to specify for a transfer from the ThingWorx Platform to the Edge device would be:

- **sourceRepo**: `SystemRepository // Name of the Thing to transfer from`
- **targetRepo**: `RT1 // Name of the Thing to transfer to`
- **sourcePath**: `/files // Directory in the SystemRepository` (absolute path)
- **targetPath**: `/in // The name of a virtual dir`

  In this case, it is pointing to `C:\microserver\in`. You can also specify subdirectories.
- **sourceFile**: `abc.json`
- **targetFile**: `abc.json // Optional`
- The default name for the **targetFile** is the name of the **sourceFile**. You can rename files during the transfer.

The paths on the WS EMS must be relative to a virtual directory that is registered to the remote Thing (that is, they must start with the `"/<virtual_dir>"`). In the case of a file repository on the ThingWorx Platform, the paths need to be relative to the root directory of the file repository (must start with `"/"`).

Note that the things must be instances of one of the following templates:

- **FileRepository**
- **RemoteThingWithFileTransfer**
- **RemoteThingWithFileTransferAndTunneling**

Also, as of versions 5.0 and later of the WS EMS, you do not need the Lua Script Resource to do file transfers. You can add the `auto_bind` group to your configuration file to specify the name of a Thing that will participate in file transfers:

```
"auto_bind":[
    {"name": "RT1" }
]
```

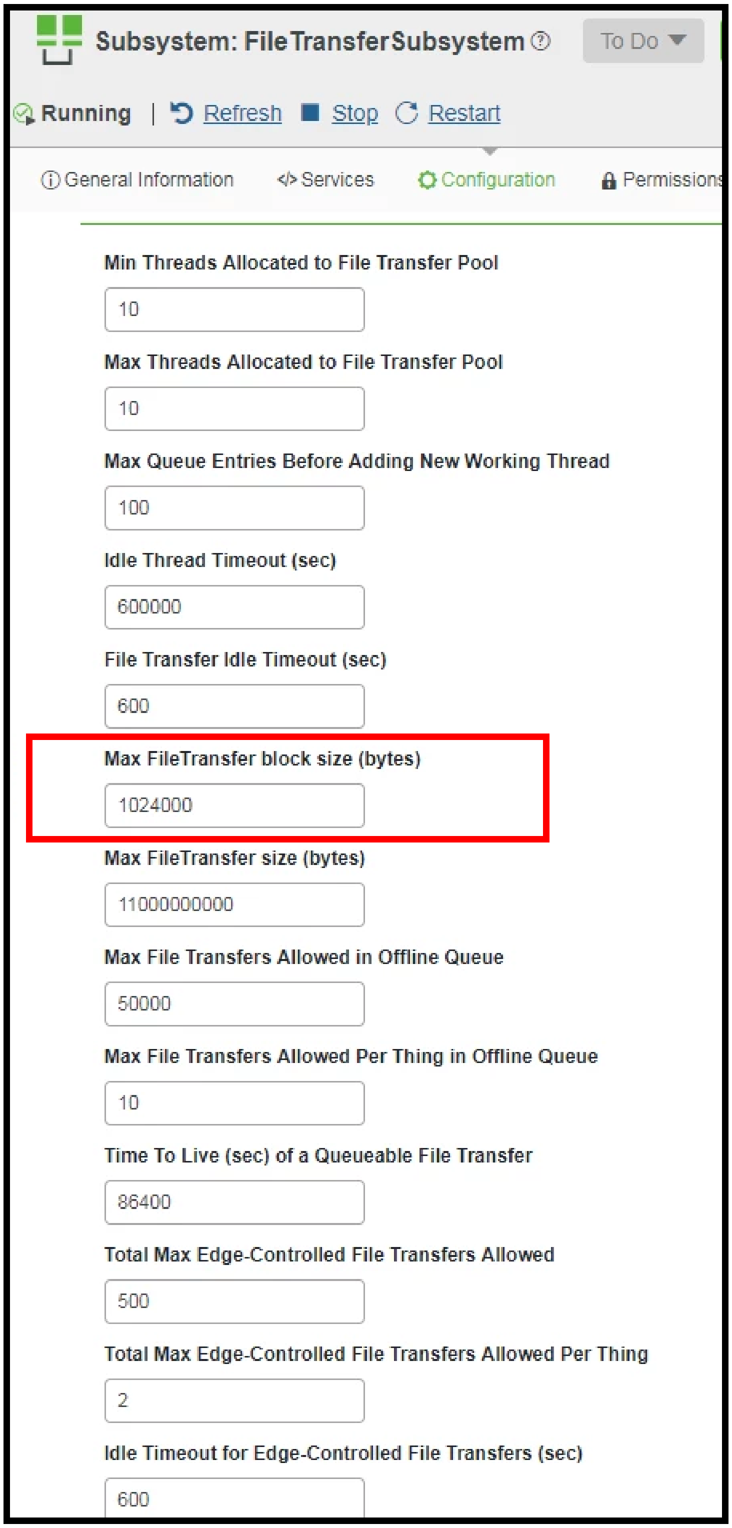
Best Practices for Transferring Large Files

When transferring large files, following these best practices is critical to ensuring optimal performance:

1. Set the `block_size` parameter to 1MB (1,024,000 bytes) for maximum bit rate on average. The proper setting of this parameter is essential to improving file transfer performance.

2. File transfer times depend on Internet bandwidth, which varies and increases in load at certain times of the day. Choose a time of day when network traffic is low to transfer large files from Edge devices to a ThingWorx platform. When possible, improve the quality of your network. Testing has shown that results vary by both time of day and the network being used. When network performance degrades, the performance of large file transfers can be negatively affected very quickly.
3. Removing any socket read timeouts also increases performance. Make sure to set the `socket_read_timeout` to zero (0).
4. Make sure that `log_level` is not set to `TRACE`. A level of `ERROR` is recommended.

5. Set up the File Transfer Subsystem (FTSS) on your ThingWorx Platform as shown in the following screen shot. These settings have been tested and shown to be optimal when transferring large files:



Min Threads Allocated to File Transfer Pool: 10

Max Threads Allocated to File Transfer Pool: 10

Max Queue Entries Before Adding New Working Thread: 100

Idle Thread Timeout (sec): 600000

File Transfer Idle Timeout (sec): 600

Max FileTransfer block size (bytes): 1024000

Max FileTransfer size (bytes): 11000000000

Max File Transfers Allowed in Offline Queue: 50000

Max File Transfers Allowed Per Thing in Offline Queue: 10

Time To Live (sec) of a Queueable File Transfer: 86400

Total Max Edge-Controlled File Transfers Allowed: 500

Total Max Edge-Controlled File Transfers Allowed Per Thing: 2

Idle Timeout for Edge-Controlled File Transfers (sec): 600

Tip

The lower of the two block size values, namely for the WS EMS and the FTSS of the ThingWorx Platform, is used at runtime. The platform is hard-coded with a maximum block size of 1MB. To be safe, set both the FTSS and WS EMS block sizes to 1MB. The platform FTSS configuration table currently defaults to 128,000.

Configuring Edge Settings for Tunneling

Application tunnels allow for secure, firewall-transparent tunneling of TCP client/server applications, such as VNC and SSH. As long as the WebSocket connection between the edge device and a ThingWorx Platform is secure (for example, uses an SSL/TLS certificate), the client/server applications can run securely. How is this possible? The application opens a second WebSocket to the same host and port that is used for other communications between the Edge device and the platform. You do not need to open other ports in the firewall to run these applications. However, it is important to note that it connects to a different URL that is specifically for the tunnel.

Note

Only TCP client/instance applications are supported at this time. UDP is not supported.

Configure tunneling for your WS EMS when you want to be able to access remotely the Edge device that is running WS EMS. You can remotely access such a device through a remote desktop session (for example, UltraVNC) or remote terminal session (for example, SSH). By default, tunneling is enabled for the WS EMS. For the most part, if you are using UltraVNC or SSH, the Platform sets the values for timeouts when it sends a service call to the WS EMS. The only default tunnel setting that you will find in `config.json.complete` follows:

```
// Default tunnel setting for tick_resolution
{
    "tick_resolution": 5
}
```

You can modify the default tunnel setting by adding the property to the `config.json` configuration file for your WS EMS. A service call from the ThingWorx Platform may override it..

The following table lists and briefly describes the tunneling configuration property:

Property	Description
`tick_resolution`	Tunnel performance can be greatly affected by tick resolution. The tick resolution determines how fast a tunnel manager checks the status of its managed tunnels. The smaller this value, the faster the tunnel responds. Tick resolution is especially important when running multiple tunnels concurrently, but be aware that a smaller tick resolution consumes more CPU resources. The default value is 5 ms. Refer to Running on a Windows-based Operating System on page 169.

Configuring Tunneling on the ThingWorx Platform Side

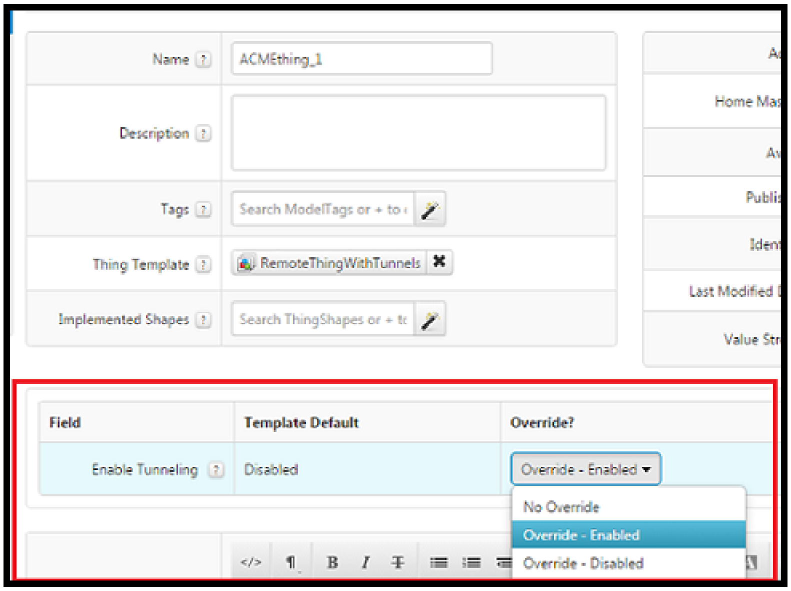
The rest of the tunneling configuration takes place in the server side of the client/server application (UltraVNC Server, for example) and on the ThingWorx Platform through ThingWorx Composer.

The main steps for the built-in client/server application for the ThingWorx Platform (UltraVNC) follow:

1. If you have not already, install UltraVNC Server on the edge device where the WS EMS is running.
2. Access the **Admin Properties** configuration screen for UltraVNC Server and make sure that the following configuration parameters are set:
   - **Allow loopback connections** — Make sure that this check box is selected if you want to test the connection on the Edge device itself (the VNC Viewer is installed on the same machine as the VNC Server).
   - **VNC password** — Type the password that VNC Viewer users must type to access this Edge device remotely.
   - **Multi viewer connection** — Select the option, **Keep existing connections**, so that a new session with this Edge device does not disconnect any existing VNC Viewer sessions.

The main steps in ThingWorx Composer follow:

1. In the **Configuration** page for the Tunneling Subsystem, check the field, **Public host name used for tunnel**. If the IP address is a local network address, the tunnel will not work. Set this field to the external host/IP address that tunnels should use for connections. For more detail, refer to Required Setting for the Tunneling Subsystem on page 87.
2. If you have not already, use the **RemoteThingWithTunnels** or the **RemoteThingWithFileTransferAndTunnels** template to create a Remote Thing to represent the edge device that is running WS EMS.
3. After creating the Thing, from the **General Information** page for the new Thing, enable the template **Override?** setting for **Enable Tunneling**, as shown below. By default, this setting is disabled.



Name: ACMEthing_1

Description:

Tags: Search ModelTags or + to

Thing Template: RemoteThingWithTunnels

Implemented Shapes: Search ThingShapes or + tc

Field	Template Default	Override?
Enable Tunneling	Disabled	Override - Enabled

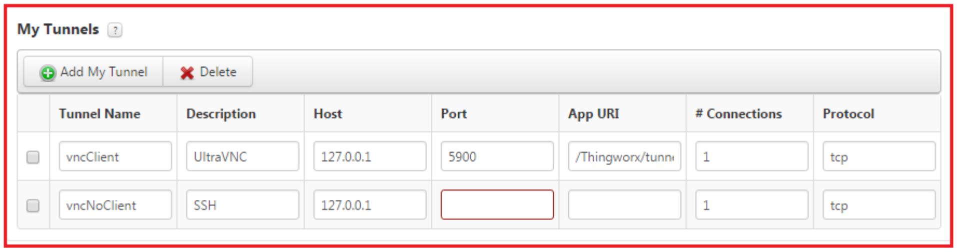
4. Determine which remote applications will be used to access the Edge device and whether you want to use the VNC client that is built into the ThingWorx Platform. These applications may be any of the following types:

   - Desktop remote sessions — VNC Server on the Edge devices and the corresponding Viewer client on the user machines that will access the device. The VNC Viewer is the built-in application available through the ThingWorx instance. You might create a tunnel, using the name `vncClient`.
   - SSH — An SSH client/server application, such as PuTTY. For information on OpenSSH, refer to http://www.openssh.com/ or http://support.suso.com/supki/SSH_Tutorial_for_Linux. For information on PuTTY, visit http://www.putty.org/.
   - Microsoft RDP — Refer to the Microsoft web site, more specifically, http://windows.microsoft.com/en-us/windows/connect-using-remote-desktop-connection#connect-using-remote-desktop-connection=windows-7.
   - Custom client application that you have built

5. As long as you have enabled the template **Override?** setting for **Enable Tunneling** in the **General** tab for the Remote Thing, configure the tunnels for the Thing that you created:

   a. Under **ENTITY INFORMATION**, select **Configuration**. If you are not in Edit mode for the Thing, click **Edit**.

   b. Under **Configuration for RemoteThingWithTunnels**, click **Add My Tunnel** and in the displayed fields, enter the information for the client/server application. Here are examples for VNC and SSH:



	Tunnel Name	Description	Host	Port	App URI	# Connections	Protocol
□	vncClient	UltraVNC	127.0.0.1	5900	/Thingworx/tunn	1	tcp
□	vncNoClient	SSH	127.0.0.1			1	tcp

Tip

When configuring a mashup for the Edge device, you will need to provide the names that you assign to the tunnels. To access the list of tunnel names available on a Thing, use the **GetTunnelNames** service.

Configure the **Host** and **Port** fields from the point of view of the *Edge device* where the server component of the client/server application is running. For example, when a user wants to access the Edge device from VNC Viewer, the user would type the IP address of the device and then the port number 5900. For SSH, you might enter 22 in the field.

By default, the URL is the location of the VNC client application on the ThingWorx Platform. If you are using SSH, make sure that supply the port number and then make this field empty.

The values that are displayed for the **# Connections** and **Protocol** fields are the default values and are the only values that are currently supported.

6. Save the configuration of your new Thing.
7. When creating your mashup, add a **Web Socket Tunnel** widget if you are using the built-in VNC viewer (client) that is provided with ThingWorx Mashup Builder. At minimum, you need to set the following parameters for the **Web Socket Tunnel** widget:

   - **RemoteThingName** — You must supply the name of your Thing (**RemoteThingWithTunnels**) that will use this tunnel (for example, the one that was created in Step 2 or earlier).
   - **TunnelName** — Enter the name that you assigned to the tunnel for the built-in VNC Viewer in the configuration of the Thing.
   - **VNCPassword** — Type the password that the VNC Server that is running on the Edge device will expect from VNC Viewer.

Note

If this widget is not displayed, you need to download and import the `WebSocketTunnel_ExtensionPackage.zip` package into the ThingWorx platform. Refer to the ThingWorx Help Center for your release of the ThingWorx Platform, and search for the widget by name.

If you are NOT using the built-in VNC Viewer, add a **RemoteAccess** widget. For example, you might use another type of TCP client/server application. For the **RemoteAccess** widget, set the following parameters:

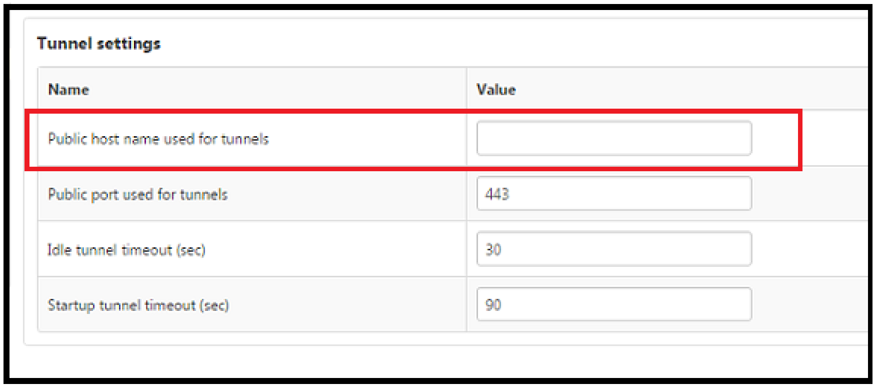
- **RemoteThingName** — You must supply the name of your Thing (**RemoteThingWithTunnels**) that will use this tunnel (for example, the one that was created in Step 2 or earlier).
- **TunnelName** — Enter the name that you assigned to the tunnel for the other type of application in the configuration of the Thing (for example, PuTTY or another SSH client/server application).
- **ListenPort** — Enter the number of the port that the Java Web Start application will listen on when it starts up. For example, if you want to run an SSH session and the listen port is 9005, you would connect your SSH client to `localhost:9005`.
- **AcceptSelfSignedCerts** — If SSL/TLS is used for this connection and you are testing with a self-signed certificate, select the check box.

For complete information about configuring the **RemoteAccess** widget, refer to the ThingWorx Help Center for your release of the ThingWorx Platform and search for “RemoteAccess widget”.

8. Save your mashup.
9. For the WS EMS, tunneling is enabled by default. As long as your WS EMS is running and connected to a ThingWorx Platform, you can test your mashup.

Required Setting for the Tunneling Subsystem

When attempting to configure tunneling, you must check the configuration for the Tunneling Subsystem of the ThingWorx instance. There is a field where you can specify the host/IP of the end point for the tunnel, called **Public host name used for tunnel**. The following figure shows the configuration parameters for the Tunneling Subsystem, with this field highlighted:



Tunnel settings

Name	Value
Public host name used for tunnels	
Public port used for tunnels	443
Idle tunnel timeout (sec)	30
Startup tunnel timeout (sec)	90

Why do you need to configure this address? Suppose that you start up your ThingWorx platform in Amazon EC2. The default IP address for the Tunneling Subsystem when the ThingWorx instance is running in EC2 might be 10.128.0.x. Unless you change that address, the Tunneling Subsystem will tell the clients to attempt to connect to that address for the tunnel websocket. Since that IP address is a local network address, the tunnel will not work. Therefore, you must populate that configuration field with the external host/IP address that tunnels will use for connections.

Configuring the WS EMS to Listen on IP Other Than localhost

You can configure a WS EMS to listen on a specific IP address or on all IP addresses available on the device, using the `http_server` group of the configuration file. If a device has one network card and it is configured with an IP address of 11.11.11.1, the device effectively has two IP addresses, 11.11.11.1 and 127.0.0.1 (localhost). To configure the specific IP address, set the `host` property, as follows:

```
"http_server" : {
  "host" : "11.11.11.1",
  "port": 9010
}
```

In this configuration, any application must use the specific IP address to access the device. “localhost” does not work.

If a device has two or more network cards with corresponding IP addresses and you want users to access the device using any of the IP addresses available, use `0.0.0.0` for the host IP address, as follows:

```
"http_server" : {
  "host": “0.0.0.0”,
  "port": 9010
}
```

⚠ **Caution**

When making a connection to a device, do NOT use the 0.0.0.0 address. Instead, you MUST use one of the actual IP addresses to connect. This configuration setting just makes it possible to connect on any of the possible IP addresses.

In either configuration, you can leave the port number as is or change it.

It is important to keep in mind that these configurations expose the REST interface to any client on the network that wants to access the WS EMS. To provide secure access, configure a user name and password for the HTTP server as well as SSL, as shown here:

```
"http_server" : {
  "user": "acmeAdmin”,
  "password": "some_encrypted_password",
  "ssl": true
}
```

To encrypt the user password, refer to Encrypting Application Keys, Passwords, and Passphrases on page 36.

Example Configurations

This section provides examples of how the WS EMS can be configured for several typical use cases:

- Gateway Mode with Self-Identifying Remote Things Example on page 89
- Gateway Mode with Explicitly-Defined Remote Things Example on page 90
- Non-Gateway Mode with Self-Identifying Remote Things Example on page 91

Gateway Mode with Self-Identifying Remote Things Example

The WS EMS can be configured to run as a gateway, acting as the communication conduit and providing message relaying services for one or more Remote Things.

The WS EMS keeps a registry of the Remote Things it acts as a gateway for. You can set up the Remote Things to “self-identify” with the WS EMS. That is, when the Remote Things initialize and connect to the WS EMS, they send the information that uniquely identifies them to the WS EMS. This information is stored in the registry of the WS EMS.

For more information on configuring the `auto_bind` group of the configuration file, refer to the section, Configuring Automatic Binding for WS EMS on page 73 and to the section, AutoBound Gateways on page 75.

The example below illustrates how to configure the WS EMS for this scenario:

```
{
"ws_servers": [{
                 "host" : "acmeServer.mycompany.com",
                 "port": 443
               },
               {
                 "host" : "fallback_server.somewhere.com",
                 "port": 443
               }]
"appkey" : "some_encrypted_application_key",
"ws_connection": {
                  "encryption" : "ssl"
                 },
"auto-bind": [{
               "name" : "EdgeGateway001",
               "gateway": true
              },
              {
               "name" : "EdgeThing001",
               "host" : "some_ip_address",
               "port": 8443
             }]
}
```

To encrypt an application key, refer to Encrypting Application Keys, Passwords, and Passphrases on page 36.

Gateway Mode with Explicitly-Defined Remote Things Example

Although Remote Things can be set to identify themselves to the WS EMS, in many cases the remote things that connect to the WS EMS are well-known. In this case, you can explicitly define them within the configuration of the WS EMS.

For more information on configuring the `auto_bind` group of the configuration file, refer to the section, Configuring Automatic Binding for WS EMS on page 73 and to the section, AutoBound Gateways on page 75.

The example below illustrates how to configure the WS EMS for this scenario:

Note

In the example below, `EdgeThing001` is an explicitly defined Remote Thing that runs at a specified IP Address and listens on port `8001`.

```
{
"ws_servers":[{
               "host":"",
               "port":443
             }]
"appkey":"some_encrypted_application_key",
"ws_connection":{
                 "encryption::"ssl"
                },
"auto_bind"[{
             "name":"EdgeGateway001",
             "gateway":true
            }
            {
             "name":"EdgeThing001",
             "host":some_ip_address>",
             "port":8001
            }
           ]
}
```

To encrypt an application key, refer to Encrypting Application Keys, Passwords, and Passphrases on page 36.

Non-Gateway Mode with Self-Identifying Remote Things Example

The WS EMS can be configured to run in non-gateway mode, so things that attach to the WS EMS will pro-actively identify themselves with its process.

The example below illustrates how the WS EMS can be configured for this scenario:

```
{
 "ws_servers":[{
                "host" : "localhost",
                "port" : 443
              }
],
"appkey" : "some_encrypted_application_key",

"ws_connection":{
                  "encryption": "ssl"
                 },
"auto_bind": [{
               "name" : "EdgeThing001",
               "host" : "127.0.0.1”,
               "port": 8001
             }]
}
```

To learn how to encrypt the application key, refer to Encrypting Application Keys, Passwords, and Passphrases on page 36.

4

Using ThingWorx Asset Advisor with WS EMS and LSR

This section provides the setup required for WS EMS and LSR Things in ThingWorx to enable end users to access the devices remotely, download packages to devices, and perform file transfers using ThingWorx Asset Advisor. The emphasis here is on what you need to do using ThingWorx Composer.

Features of ThingWorx Asset Advisor to Use with WS EMS and LSR

The ThingWorx Asset Advisor application provides file transfer and remote access capabilities through its Asset Remoting Extension. Referred to as Remote Access and Control, this application adds a set of optional features into ThingWorx Composer. These features enable you to upload and download files to a remote asset, and access the asset remotely to interact directly with its software system from Asset Advisor.

In addition, Asset Advisor provides access to the ThingWorx Software Content Management (SCM) Extension that enables you to create file-based packages that can be downloaded to edge devices. Using the SCM and Remote Access and Control features from Asset Advisor with your WS EMS and LSR devices, you can upload and download files or access an asset remotely to interact directly with its software.

Remote Access and Control Extension

The Remote Access and Control Extension includes the following optional Asset Advisor features, which display on the detail page for an asset in Asset Advisor:

- **Remote Access** — Displays for WS EMS Things whose base Thing Templates extend from the `RemoteThingWithTunnelsAndFileTransfer` Thing Template, or that implement the `RemoteAccessible` Thing Shape. If you have imported the ThingWorx Remote Access Extension AND the Remote Access and Control Extension for Asset Advisor into your ThingWorx Platform and your WS EMS Things are based on the `RemoteThingWithTunnelsAndFileTransfer` Thing Template, your WS EMS Things should be ready to use Remote Access and Control.
- **File Transfer** — Displays for WS EMS Things whose base Thing templates extend from the `RemoteThingWithTunnelingAndFileTransfer` Thing Template.
- **File Transfer History** — Displays for WS EMS Things whose base Thing templates extend from the `RemoteThingWithTunnelingAndFileTransfer` Thing Template.

ThingWorx Software Content Management (SCM) Extension

The ThingWorx Software Content Management (SCM) Extension allows for the creation of software content and distribution of that software content to a set of target assets in a controlled manner. SCM automates the manually-intensive and error prone process of distributing and installing new software to your assets.

SCM is comprised of the following high-level pieces:

- Package — The software content to be delivered.

- Deployment — A request to the ThingWorx Platform to deliver and (optionally) execute the software content described in a Package to a set of target Assets
- Assets — The Edge devices receiving the software content defined in the Package and requested by a Deployment.

The ThingWorx SCM Extension supports the creation of file-based packages for Edge devices running the WS EMS. These devices should be able to use non-administrator application keys and still use SCM, as long as permissions are set up correctly.

What's Next

First, read through the prerequisites on page 95 and make sure that your environment and configuration files for WS EMS and LSR meet the requirements.

Next, a ThingWorx administrator should set the parameters for the subsystems as explained in Administrator Tasks for Using Remote Access, File Transfers, and SCM in Asset Advisor on page 97.

Depending on which features of Asset Advisor you want to use refer to one of the following sections:

- Remote Access and Control — Setting Up a WS EMS or LSR Thing for the Remote Access and Control Application on page 102
- SCM — Setting Up to Use ThingWorx Software Content Management (SCM) with WS EMS Devices on page 105

For information on using these features in Asset Advisor, refer to the section, Asset Advisor in the ThingWorx Apps Help Center.

Prerequisites to Setting Up a WS EMS Thing for Asset Advisor

It is important to remember that WS EMS performs all transactions with the ThingWorx Platform and passes any requests for an LSR device on to that device.

You need to configure your WS EMS and LSR, as follows:

- Using ThingWorx Composer, create a non-administrator user and an application key for the WS EMS to use when connecting to a ThingWorx Platform. When creating the application key, associate that non-administrator user with the application key. For assistance, refer to application keys in the ThingWorx Platform Help Center.
- Configure the WS EMS for file transfers. For assistance, refer to Configuring File Transfers on page 77.

- Configure the WS EMS for tunneling. For assistance, refer to Configuring Edge Settings for Tunneling on page 83.
- Configure the parameters for the Lua Script Resource (LSR):
  - Connection to the WS EMS over HTTP or HTTPS Server (with an SSL/TLS certificate) — Refer to Configuring the HTTP Server for the LSR (SSL/TLS Certificate) on page 140
  - Edge Thing (asset) to which you want to bind the properties — Refer to Configuring Edge Things on page 145. Make sure that you use the name of the Thing here, not an Identifier.

Complete the following tasks using ThingWorx Composer, IN THE FOLLOWING ORDER:

1. Make sure that ThingWorx Composer v.8.2.0 or higher is installed on your ThingWorx platform.

Caution

If you are using ThingWorx v.8.4.0 or later, you MUST configure the platform to allow the import of extensions and then restart the platform. For details, refer to Importing Extensions, "Enabling Extension Import", and platform-settings.json Configuration Details in the ThingWorx 8 Help Center for complete details.

2. Import the ThingWorx Remote Access Extension into your ThingWorx Platform. For more information about the import procedure, refer to Importing Extensions in the ThingWorx Platform Help Center.

Note

This extension adds a new widget to Mashup Builder for remote sessions, the RAClientLinker widget. If you want to use the new Remote Access functionality and you have previously used the Remote Access Widget in a mashup and want to continue using your mashup, you need to change the widget in your mashup and configure it.

3. Import the ThingWorx Software Content Management (SCM) Extension into your ThingWorx platform. For more information, refer to Importing Extensions in the ThingWorx Platform Help Center.
4. Import the ThingWorx Apps Extension and the ThingWorx Asset Remoting Extension into your ThingWorx Platform. For more information, refer to Importing Extensions in the ThingWorx Platform Help Center.

5. If you have not already done so, create a non-admin user and an application key for the WS EMS to present for authentication with the ThingWorx Platform. For details, refer to Create an Application Key for WS EMS on page 24.
6. Make sure that an Administrator has configured the settings for the subsystems, as explained in Administrator Tasks for Using Remote Access, File Transfers, and SCM in Asset Advisor on page 97.

For details about ThingWorx Apps, refer to the ThingWorx Apps 8.5 Help Center.

Administrator Tasks for Using Remote Access, File Transfers, and SCM in Asset Advisor

The following sections provide recommended configuration settings for the **TunnelSubsystem**, **WSCommunicationsSubsystem**, and **FileTransferSubsystem** can improve performance when performing remote sessions and file transfers for EMS assets.

Note

The SCM application uses the File Transfer Subsystem, so the administrator tasks for file transfers are required for using SCM in Asset Advisor.

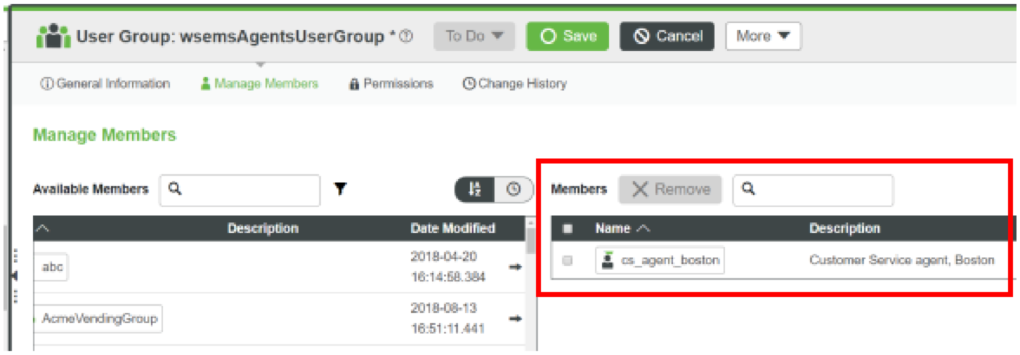
Creating Users, User Groups, and Organizations

Depending on which application end users need to access and on which devices they need to access, a ThingWorx administrator needs to create non-admin users, user groups, and at least one organization. When you create a user group, you add individual users to the group and then grant visibility and permissions to that user group. If you have multiple user groups that require the same visibility and permissions, consider creating an organization and adding user groups to it. You would then grant the visibility and permissions at the organization level to all users in the user groups within the organization.

To create these entities, follow these steps:

1. Log in to ThingWorx Composer, and use the navigation panel on the left to expand **Security** and then select **Users**.
2. In the **Users** page, select **+New**, and enter the following information for the user:
   - `Name` — For example, `cs_agent_boston` for a customer service agent..

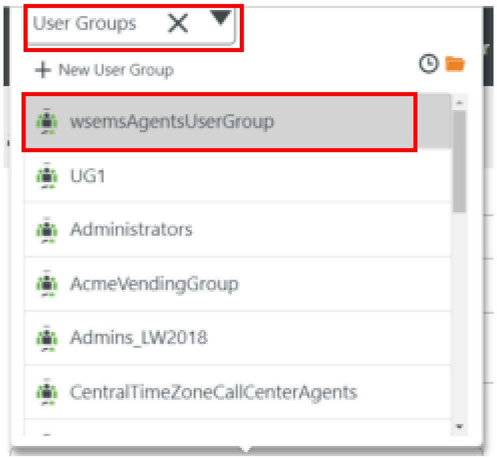
   - `Description` — For example, `user account for customer service agents in Boston`.
   - Make sure the check box next to `Enabled` is checked.
3. Click **Save**.
4. To create additional users, click 📁 and repeat steps 1 through 3.
5. When ready to create a user group, click 📁 to return to the **Browse** list, and under **Security**, select **User Groups**.
6. In the User Groups page, click **+New**.
7. In the General Information page, type a Name for the group. For example, `wsemsAgentsUserGroup`, and click **Save**.
8. Click **Manage Members**, and under Available Members on the Manage Members page, select the check box next to the name of the user(s) you just created. Using the example, you would select the `cs_agent_boston`. Then, click the right-facing arrow to add this user to the new User Group. The end result should look similar to the following screen:



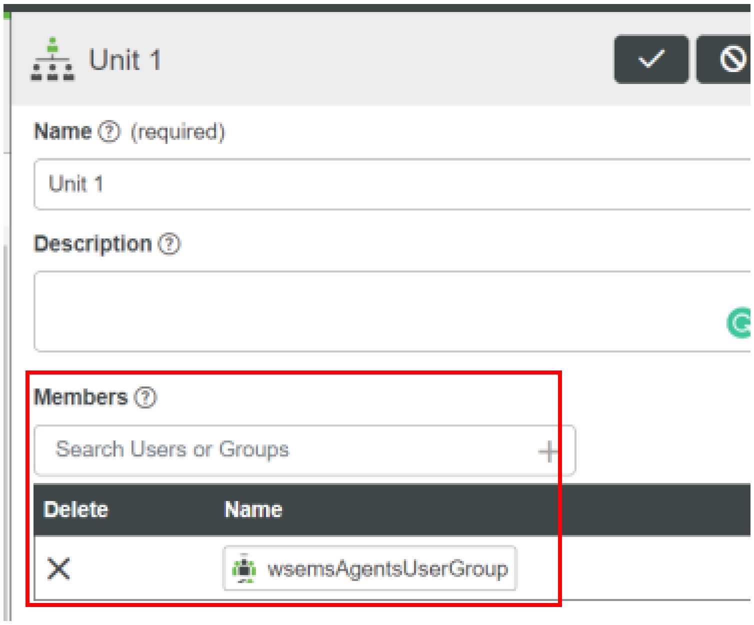
	Description	Date Modified	
abc		2018-04-20 16:14:58.384	→
AcmeVendingGroup		2018-08-13 16:51:11.441	→

■	Name	Description
□	cs_agent_boston	Customer Service agent, Boston

9. Click **Save**.
10. To create another user group, repeat Steps 5 through 8 for that user group and assign the users who should be able to perform remote sessions to that group. For example, you may want to create a user group for remote access (`raUserGroup`) or for SCM (`scmUserGroup`).
11. From the navigation panel, click 📁 to return to the **Browse** list, and under **Security**, select **Organizations**.
12. In the Organizations page, click **+New**.
13. In the General Information page, type a Name for the organization. For example, `wsemsOrg`, `raOrg`, or `scmOrg` and click **Save**.
14. Click **Organization** and in the Organization page, click Unit1.
15. In the Unit 1 page, go to the Members field and click the plus icon to display a list of user groups and users that you can add to the organization. From the **Search entity types** drop-down list, select `User Groups`



16. As indicated in the figure above, select a user group. In the example above, it is the `wsemsAgentsUserGroup`. The list of Members displays your addition:



Unit 1

Name (required)

Unit 1

Description

Members

Search Users or Groups

Delete	Name
✕	wsemsAgentsUserGroup

17. To save, click the checkmark icon in the upper right corner of the Unit 1 page. The page closes and returns you to the Organization page.
18. To create another organization, repeat Steps 11 through 16 now.
19. Depending on how you want to set permissions, you can do so at the Organization level, the User Group level, and the User level. To use the Remote Access and Control application, users need visibility and permissions to the Things that they either want to access through a remote session or to and from which they want to transfer files. They also need permissions to run (Service Execute permission) to the ThingWorx **Copy** service for file transfers.

For information on visibility and permissions for SCM, refer to Setting Up to Use ThingWorx Software Content Management (SCM) with WS EMS Devices on page 105.

For more information on visibility and permissions in ThingWorx, refer to the following topics in the ThingWorx Help Center:

- Visibility in Organizations — Visibility in Organizations
- Entity Permissions — Entity Permissions
- Inheriting Permissions from a Thing Template
- Collection Permissions — Collection Permissions

Recommended Settings for the Tunnel Subsystem

To set up the ThingWorx Platform for tunneling with WS EMS assets through Asset Advisor, follow these steps:

1. In ThingWorx Composer, under **System**, click **Subsystems**.
2. In the list of subsystems, click **TunnelSubsystem**.
3. Under **Configuration**, set the following values:

   -
     - **Public host name used for tunnels** — The URL for the host computer of the ThingWorx Platform with which the device is communicating. Do not use an IP address for the Tunnel Subsystem configuration.
     - **Public port used for tunnels** — The number of the port on the public host to use for tunnels. By default, this port number is a secure port, 8443. Although NOT recommended, if you need to use an insecure port for testing, make sure that you change this port number before attempting to connect through the Remote Access Client. Otherwise, the platform will reject the request for a tunnel. The error message in the Remote Access Client does not explain that reason for rejecting the request.

Caution

To ensure that tunnels will work, you must set up a secure port if that is what the WS EMS will use when communicating with the ThingWorx platform.

- ○ **Idle timeout (sec)** —The number of seconds to allow the tunnel to start. Both the WS EMS and Remote Access Client connect into the tunnel endpoint. The default value is 90 seconds.
- ○ **Tunnel startup timeout (sec)** — The number of seconds to wait for additional data to be transferred before shutting down the tunnel. By default, if no data is transferred for 30 seconds, the platform shuts the tunnel down.

4. Click **Save**.

Recommended Settings for the WSCommunications Subsystem

If file transfers are expected to involve large files (greater than 20mb in size), increase the timeout value for request response messages to 180 seconds by completing the following steps:

1. In ThingWorx Composer, under **System**, click **Subsystems**.
2. In the list of subsystems, click **WSCommunicationsSubsystem**.
3. Under **Configuration**, enter 100 in the **Amount of time a request will wait for the response message before timing out (secs)** field.
4. Click **Save**.

Recommended Settings for the File Transfer Subsystem

To set up the File Transfer Subsystem for use by WS EMS devices, follow these steps:

1. In ThingWorx Composer, under **System**, click **Subsystems**.
2. In the list of subsystems, click **FileTransferSubsystem**.
3. Under **Configuration**, enter the following recommended values for each file transfer setting.

Field	Value
Min Threads Allocated to File Transfer Pool	100
Max Threads Allocated to File Transfer Pool	100
Max Queue Entries Before Adding New Working Thread	10000
Idle Thread Timeout (sec)	60
File Transfer Idle Timeout (sec)	300
Max FileTransfer size (bytes)	1000000000

4. Click **Save**.

Setting Up a WS EMS or LSR Thing for the Remote Access and Control Application

For devices running the WS EMS or LSR to be available in ThingWorx Asset Advisor, you need to set up Thing Templates for the types of devices. These Thing Templates must implement the following Thing Shapes:

- **PTC.Factory.PhysicalAssetThingShape**
- **PTC.SCA.SCO.AssetIdentifierThingShape**
- **PTC.SCA.SCO.StatusThingShape**
- **PTC.ISA95.IdentifierThingShape**
- **PTC.SCA.SCO.MonitoredPropertiesThingShape**

For complete details, refer to the topic, Creating Custom Thing Templates for Equipment Types in the ThingWorx Apps Help Center.

The Remote Access and Control application in Asset Advisor enables users to create remote sessions with devices at remote sites and also to transfer files to and from those remote devices. The next two sections explain the setup for a Thing in ThingWorx Composer required to take advantage of these features.

Remote Access

The procedure below is focused on getting you started with a single WS EMS or LSR Thing. For a large number of devices of the same models, create Thing Templates for your models and apply the appropriate Thing Shapes and other settings for to the Thing Templates. For details, refer to the topic, Creating Custom Thing Templates for Equipment Types in the ThingWorx Apps Help Center.

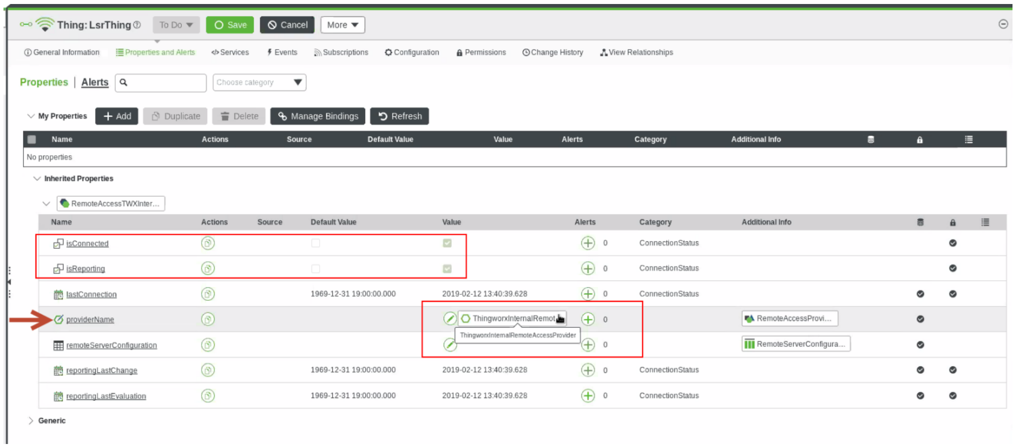
1. In ThingWorx Composer, navigate to the Thing and on the **General Information** page, add the following Thing Shapes for Remote Access:

   - **PTC.SCA.SCO.FIleTransferHistoryHandlerThingShape**
   - **RemoteAccessible**
   - **PTC.SCA.SCO.RemoteTunnelingThingShape**

   For details, refer to Creating Custom Thing Templates for Equipment Types in the ThingWorx Apps Help Center.

2. Click **Save** and select **Properties | Alerts**

3. On the Properties page, verify that `isConnected` or `isReporting` property shows a value of a check mark (dimmed), as shown below:



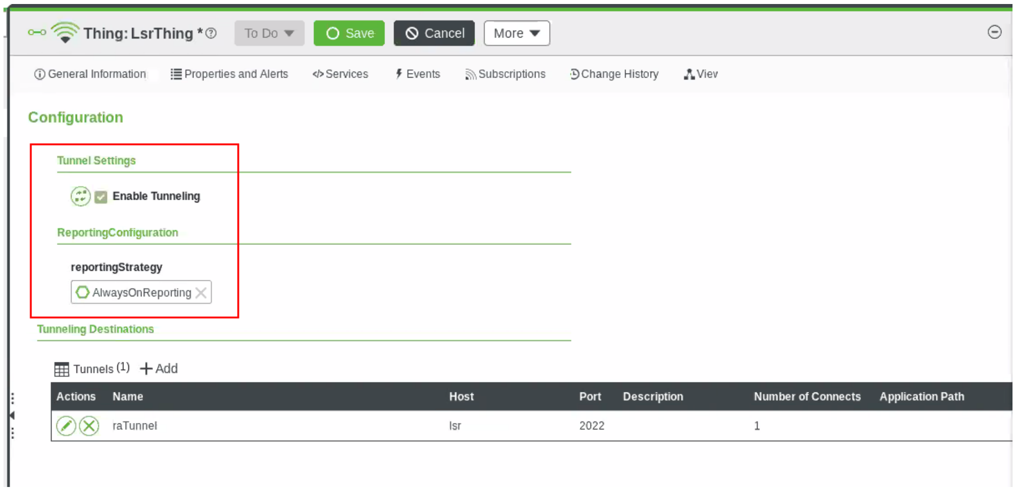
Name	Actions	Source	Default Value	Value	Alerts	Category	Additional Info
No properties							

Name	Actions	Source	Default Value	Value	Alerts	Category	Additional Info			
isConnected			☐	☑	0	ConnectionStatus			✓	
isReporting			☐	☑	0	ConnectionStatus			✓	
lastConnection			1969-12-31 19:00:00.000	2019-02-12 13:40:39.628	0	ConnectionStatus		✓	✓	
providerName				ThingworxInternalRemot ThingworxInternalRemoteAccessProvider	0		RemoteAccessProvi...	✓		
remoteServerConfiguration					0		RemoteServerConfigura...	✓		
reportingLastChange			1969-12-31 19:00:00.000	2019-02-12 13:40:39.628	0	ConnectionStatus		✓	✓	
reportingLastEvaluation			1969-12-31 19:00:00.000	2019-02-12 13:40:39.628	0	ConnectionStatus		✓	✓	

Note

The `isReporting` property was added for ThingWorx v.8.4.0, the Thing Presence feature. Checking `isConnected` suffices for earlier versions of the platform.

4. As indicated in the screen shot above, set the value of the `providerName` property to `ThingworxInternalRemoteAccessProvider`.
5. Click **Save** and select **Configuration**.
6. On the Configuration page, select the `Enable Tunneling` check box and make sure that the `reportingStratey` is `AlwaysOnReporting`.

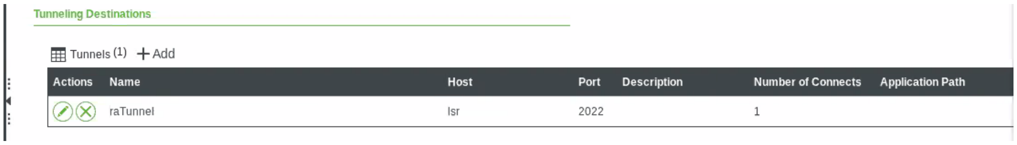


☑ Enable Tunneling

reportingStrategy: AlwaysOnReporting

Actions	Name	Host	Port	Description	Number of Connects	Application Path
	raTunnel	lsr	2022		1	

7. Under **Tunneling Destinations**, click **+ Add**. The Tunnels window appears. Here is an example of a configured Tunnel:



Tunneling Destinations

Tunnels (1) + Add

Actions	Name	Host	Port	Description	Number of Connects	Application Path
✎ ⊗	raTunnel	lsr	2022		1	

a. Enter the **Name** that will be used to identify what tunnel to use.Choose a name that indicates the type of remote interface. For example, `vnc` or `ssh`.

b. Configure the **Host** and **Port** from the point of view of the Edge device where the server component of the client/server application is running, not the ThingWorx Platform. For example, when you want to access the Edge device from an SSH client you would type the host name of the device, and then the number of the port on which the WS EMS is listening. Typically, this port is 22. If you have secure communications set up between the WS EMS and the platform, the port might be 8443. The port for a VNC tunnel is typically 5900.

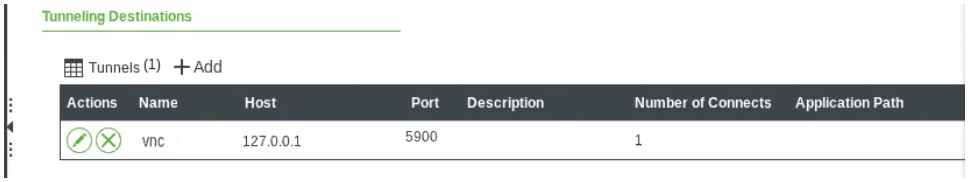
c.

Note

The port should be any public port not already in use.

d. The **Number of Connects** and **Protocol** should retain their default values, unless you have a reason to change them.

e. Click **Save**. The tunnel and the settings appear in the table of Tunneling Destinations on the Configuration page:



Tunneling Destinations

Tunnels (1) + Add

Actions	Name	Host	Port	Description	Number of Connects	Application Path
✎ ⊗	vnc	127.0.0.1	5900		1	

8. Click **Save**.

To test the Remote Access functionality, download the ThingWorx Remote Access Client (RAC) from the ThingWorx Remote Access Client Downloads page. This tool works in conjunction with the RAClientLinker widget and the Remote Access and Control application in Asset Advisor to establish a connection (tunnel) to use for a remote session.

Note

For any end user to connect to a remote device, the user needs to have a tunnel created between the local machine and the remote device. The Remote Access Client creates that tunnel.

Configuring a WS EMS Thing for File Transfer and File Transfer History in Asset Advisor

The Remote Access and Control application of Asset Advisor provides file transfer and file transfer history functionality. Assuming that you have configured the WS EMS for file transfers, follow these steps to configure a WS EMS Thing for file transfers and file transfer history in Asset Advisor:

1. Connect the Edge device to ThingWorx Platform.
2. Log in to ThingWorx Composer, navigate to the WS EMS Thing
3. Under **General Information**, set the `Identifier`.
4. Click **Save**.

Note

The **File Transfer** action in the Asset Advisor UI enables you to copy files from the local system repository (**TW>RSM.Thing.FileRepository**) to a remote location (a device), and from the remote location to the local system repository. For information about setting up a custom file repository, refer to "Configuring a Custom File Repository Location in the ThingWorx Help Center.

Setting Up to Use ThingWorx Software Content Management (SCM) with WS EMS Devices

For devices running the WS EMS or LSR to be available in the Asset Advisor, you need to set up Thing Templates for the types of devices. These Thing Templates must implement the following Thing Shapes:

- **PTC.Factory.PhysicalAssetThingShape**
- **PTC.SCA.SCO.AssetIdentifierThingShape**
- **PTC.SCA.SCO.StatusThingShape**

- **PTC.ISA95.IdentifierThingShape**
- **PTC.SCA.SCO.MonitoredPropertiesThingShape**

For complete details, refer to Creating Custom Thing Templates for Equipment Types in the ThingWorx Apps Help Center.

Creating Security Entities and Granting Visibility and Permissions for SCM

The procedure below explains how to set up the required security entities and then assign the required visibility and permissions for using SCM with WS EMS and LSR.

As long as the ThingWorx Software Content Management (SCM) Extension has been imported into your ThingWorx Platform, follow these steps to set up the required permissions for using SCM with WS EMS devices:

1. Create a new Organization. For example, `SCMEdgeDevicesOrg`.
2. Create a new User Group. For example, `SCMEdgeDevicesGroup`.
3. Add the `SCMEdgeDevicesGroup` to the `SCMEdgeDevicesOrg`.
4. Add the `SCMEdgeDevicesGroup` as a member of the **TW.RSM.RemoteAssets User Group**.
5. Add the **SCMEdgeDevicesOrg** to the Visibility permissions of the following things:
   a. **TW.RSM.SFW.SoftwareManager** Thing
   b. **TW.RSM.SFW.SoftwareManager.DeliveryTarget** Thing
   c. **TW.RSM.SFW.SoftwareManager.Campaign** Thing
   d. **TW.RSM.SFW.SoftwareManager.Definition** Thing
6. Add an override, giving the Service Invoke permission to **SCMEdgeDevicesGroup** on the **GetDataTableEntryByKey** service of the **TW.RSM.SFW.SoftwareManager.DeliveryTarget** Thing.
7. Add an override, giving the Service Invoke permission to **SCMEdgeDevicesGroup** on the following services of **TW.RSM.SFW.SoftwareManager** Thing:
   a. **UpdateState**
   b. **CompleteDeliveryTarget**
   c. **StartDownload**
8. Assuming that you created a non-admin user for the WS EMS application key, add that non-admin user to the **TW.RSM.EdgeDevices** user group. Using the example in Create an Application Key for WS EMS on page 24, add the `wsemsUser` to the **TW.RSM.EdgeDevices** user group.

Configuring WS EMS/LSR Things for Use in Software Content Management (SCM)

For WS EMS/LSR Things to be available in the SCM module of Asset Advisor, follow these steps;

1. In ThingWorx Composer, navigate to the Thing.
2. On the **General Information** page, add thee following **Implemented Shapes**:
   - **PTC.Asset.ManagedAsset**
   - **TW.RSM.SFW.ThingShape.Updateable**
   - **PTC.Resource.Asset.SCMResourceThingShape**
3. Add **PTC:AssetType** to **Tags**.
4. Click **Save**.

For details on creating and deploying packages using the UI of the ThingWorx SCM Extension, refer to the ThingWorx Utilities Help Center. For information on using SCM via the ThingWorx Apps, refer to the Software Content Management topic in the ThingWorx Apps 8.5 Help Center.

Lua Scripts and Software Content Management (SCM)

SCM services on the Lua Script Resource (LSR) are provided by a pair of Lua scripts

- `softwareupdate.lua` — A script that exposes services that can be used to download and install a software package
- `swupdate.lua` — A Thing Shape that wraps calls to `softwareupdate.lua`. Needs to be extended from in a Thing Template for a lua Thing to support SCM services..

REST API

This section lists and briefly definies the REST APIs that you can use for SCM with the LSR.

Trigger Update Action — Start

Description	Starts a Software Update
URI	`scripts/Thingworx/[ThingName]/Services/TriggerUpdateAction`
Type	`POST`
Headers	`Content-Type: application/json`

Trigger Update Action — Start (continued)

Body	{
	    "action" : "start",
	    "params" : {
	        "id" : 1234,
	        "name" : "Name",
	        "thing" : "Thing",
	        "repository" : "Repository",
	        "path" : "Path",
	        "script" : "Script",
	        "updateManager" : "updateManager"
	    },
	}

Side Effects	Sets internal state to `notified`, which will quickly transition to `waitingForDownload` in the state machine. Triggers a call to the **UpdateState** service on the **updateManager** Thing to set the `State` property to 'notified'.

Trigger Update Action — Abort

Description	Aborts a software update.
URI	`scripts/Thingworx/[ThingName]/Services/TriggerUpdateAction`
Type	`POST`
Headers	`Content-Type: application/json`

Body	{
	"action" : "abort"
	"params" : {
	"id" : 1234
	}
	}

Side Effects	Sets internal state to `aborted`. Job metadata will be reset to nil. Triggers a call to the **CompleteDeliveryTarget** service on the **updateManager** with failure metadata.

Trigger Update Action — Download

Description	Notifies the LSR that a file is b eing downloaded.
URI	`scripts/Thingworx/[ThingName]/Services/TriggerUpdateAction`
Type	`POST`
Headers	`Content-Type: application/json`

Trigger Update Action — Download (continued)

Body	`{`
	`"action" : "download"`
	`"params" : {`
	`"id" : 1234`
	`}`
	`}`

Side Effects	Sets internal state to `downloading`. Triggers a call to the **UpdateState** service on the **updateManager** Thing to set the `State` property to `downloading`.

Triggger Update Action — Downloaded

Description	Notifies the LSR that a file has been downloaded
URI	`scripts/Thingworx/[ThingName]/Services/TriggerUpdateAction`
Type	`POST`
Headers	`Content-Type: application/json`

Body	`{`
	`"action" : "downloaded"`
	`"params" : {`
	`"id" : 1234`
	`}`
	`}`

Side Effects	Sets internal state to `downloaded`, which will quickly transition to `waitForInstall` in the state machine. Triggers a call to the **UpdateState** service on the **updateManager** Thing to set the `State` property to `downloaded`.

Schedule Download

Description	Schedules a software package ffor download.
URI	`scripts/Thingworx/[ThingName]/Services/ScheduleDownload`
Type	`POST`
Headers	`Content-Type: application/json`

Schedule Download (continued)

Body	`{`
	`"time" : "123456789"}`
	`}`

Side Effects	Sets the `job.downloadTime` property to `time`. While in the `waitForDownload` state, the state machine will check each tick to see if `job.downloadTime` has been reached. If it has, it will call the **StartDownload** service on the **updateManager** Thing.

Schedule Install

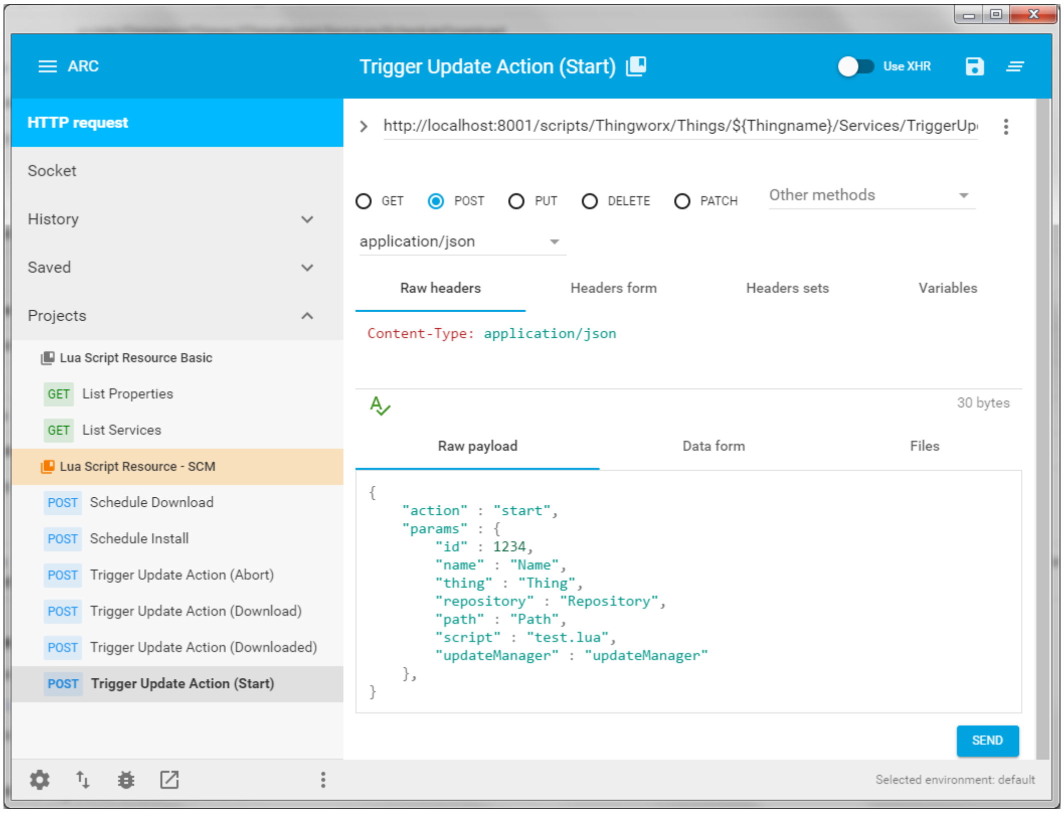
Description	Schedules the installation of a package.
URI	`scripts/Thingworx/[ThingName]/Services/ScheduleInstall`
Type	`POST`
Headers	`Content-Type: application/json`

Body	`{`
	`"time" : "123456789"}`
	`}`

Side Effects	Sets the `job.installTime` property to `time`. While in the `waitForInstall` state, the state machine will check each tick to see if `job.installTime` has been reached. If it has, it will call the **UpdateState** service on the **updateManager** Thing to set the `State` property to `installing`.

Advanced REST Client Project

You can use Advanced Rest Client (ARC) for Chrome to send pre-configured REST calls to the LSR by importing the Lua Script Resource Project. For example:


ARC
Trigger Update Action (Start)
Use XHR
HTTP request
Socket
History
Saved
Projects
Lua Script Resource Basic
GET List Properties
GET List Services
Lua Script Resource - SCM
POST Schedule Download
POST Schedule Install
POST Trigger Update Action (Abort)
POST Trigger Update Action (Download)
POST Trigger Update Action (Downloaded)
POST Trigger Update Action (Start)
○ GET ● POST ○ PUT ○ DELETE ○ PATCH
Other methods
Raw headers
Headers form
Headers sets
Variables
30 bytes
Raw payload
Data form
Files
SEND
Selected environment: default

http://localhost:8001/scripts/Thingworx/Things/${Thingname}/Services/TriggerUp

application/json

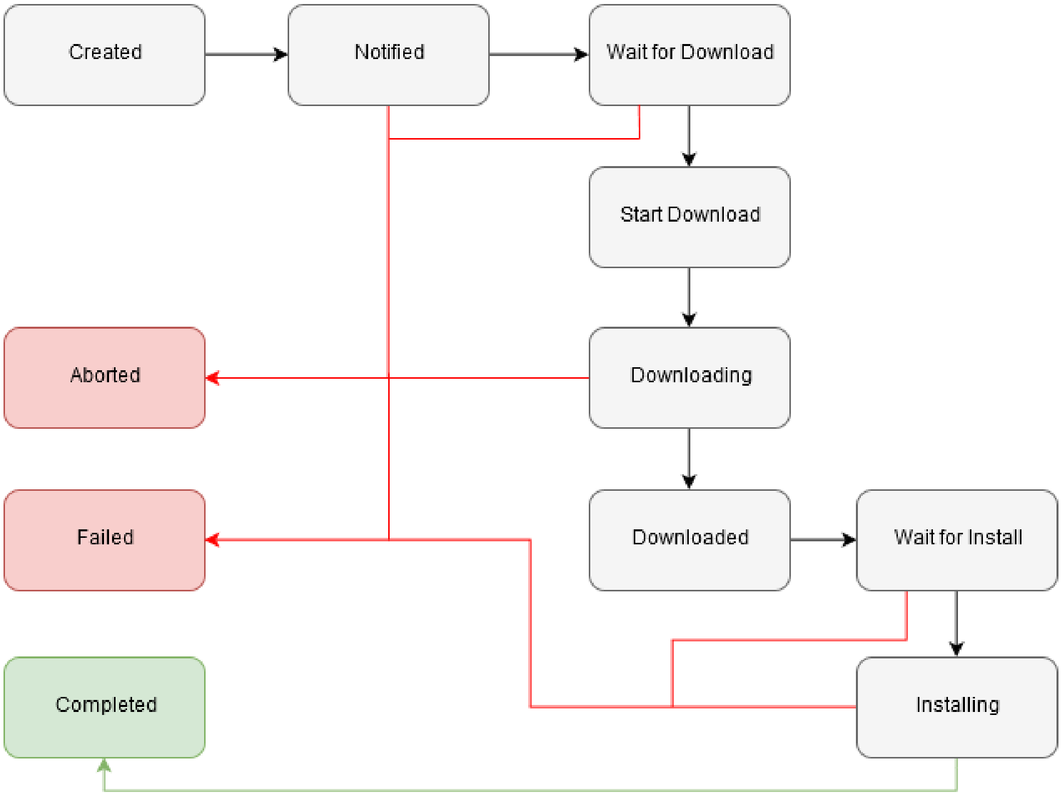
```
Content-Type: application/json
```

```
{
    "action" : "start",
    "params" : {
        "id" : 1234,
        "name" : "Name",
        "thing" : "Thing",
        "repository" : "Repository",
        "path" : "Path",
        "script" : "test.lua",
        "updateManager" : "updateManager"
    },
}
```

You must set the `Thingname` environment variable to the name of your lua Thing.

SCM State Machine

The following diagram shows the states of a Software Update Package and how the package may flow through them The red lines show the flow when an error occurs or the Abort action is called. The black lines show the flow for a package as each stage is successful, and finally the green line indicates that the package was successfully downloaded and installed.


Created
Notified
Wait for Download
Start Download
Aborted
Downloading
Failed
Downloaded
Wait for Install
Completed
Installing

5

REST Web Services and WS EMS

REST (Representational State Transfer) is an important communication tool that provides much of the communication functionality that Web Services are used for, but without many of the complexities. As a result, REST is much easier to work with and can be used by any client that is capable of making an HTTP request.

Note

The examples in this topic assume that you are familiar with executing HTTP **POST** methods in your web development environment or application.

URL Pattern

The following URL pattern is used when communicating with a ThingWorx platform:

```
<http|https>://<host>:<port>/Thingworx/<entity collection>/
<entity>/<characteristic collection>/<characteristic>?<query parameters>
```

You can use this URL pattern when you want to access information that is stored on a ThingWorx Platform for a remote device or machine that is running a WS MES. The pattern to use when you want to access the WS EMS that is running on a remote device or machine is similar:

```
<http|https>://<host>:<port>/Thingworx/<entity collection>/
```

```
<entity>/<characteristic collection>/<characteristic>?<query parameters>
```

Note

Anything enclosed in angle brackets (< >) is information that you may need to provide. Some user-supplied information in the URLs above is required, while some is optional. The information that is required depends on the type of request that is being made.

Example

The following REST Web Service call executes the service **GetLogData** that is associated with the Thing called `ACMElocking_valve`.

```
http://localhost/Thingworx/Things/ACMElocking_valve/Services/GetLogData
  {
    "startDate": 1572566400,
    "endDate": 1572652800,
    "maxItems: 50
  }
```

The REST method is GET for this example. To view the returned data in JSON format, select the value `application-json` for the Accept Header in the REST client.

Built-in Collection Values

The ThingWorx Platform has a finite list of entity collections. Each entity collection contains entities (for example, `Things`) of the respective type (for example, `/Things` contains all things). The WS EMS supports the `Things` entity collection and the `Properties` and `ThingName` characteristic collections. It also supports the File Transfer Subsystem and Services that are associated with Things. For more information, refer to the section. REST Web Services Supported by WS EMS on page 121.

Updating, Deleting, and Executing with REST Web Services

The following rules help to understand what is needed based on the type of request being made.

Requested Action	Notes	Sample URL	HTTP Action	Content Type
UPDATE	Updates require specifying the entity part (“`thing_name`” in the sample)	`http://host/Thingworx/Things/thing_name/`	`PUT`	application/json or text/xml
DELETE	Deletes require specifying the entity part as well	`http://host/Thingworx/Things/thing_name`	`DELETE`	n/a
INVOKING SERVICES	Calling a service requires specifying the complete URL, including the specific characteristic	`http://host/Thingworx/Things/MyThing/Services/myService` If your service requires them, these inputs should be passed in the form fields of your `POST`.	`POST`	application/json

Executing HTTP Requests

When executing HTTP requests, use UTF-8 encoding, and specify the optional port value if required.

Tip

Use HTTPS in production or any time network integrity is in question.

Handling HTTP Response Codes

In most cases, you should expect to get back either content or the status code of 200, which indicates that the operation was successful. In the case of an error, you receive an error message.

Working with HTTP Content

If you are sending or receiving any HTTP content (JSON, XML, HTML [for responses only]), set the request content-type header to the appropriate value based on the HTTP content you are sending. The following table lists and briefly describes the HTTP methods that are supported:

Supported HTTP Methods

Use	To
GET	Retrieve a value.
PUT	Write a value or create new things or properties.
POST	Execute a service.
DELETE	Delete a Thing or property.

For Content Type	In Accept Header, Use
JSON	`application/json`
XML	`text/xml`
HTML	`text/html` (or omit Accept header)

Metadata

You can display the metadata of any specific Thing, Thing Template, or Data Shape you build by going to the following URL in a web browser: `*NameoftheThing*/Metadata`

Note

To view it, this information must be in JSON format.

Passing in Authentication with your REST Web Service Call

To authenticate with the ThingWorx Platform for a REST Web Service call, use an application key that is associated with a user account that has the privileges to perform the actions that you intend to invoke, using the REST Web Services. If the HTTP Server configuration for your WS EMS has authentication enabled, you need to include your credentials in basic authentication form.

Tip

Although you can pass in a username and password combination with your REST call, the recommended best practice is to use an application key. Generate the key in ThingWorx Composer and then pass it with your REST call. The user account associated with the application key should have privileges to read/write properties and run services on the related devices/machines in the ThingWorx Platform.

If you pass in a user name and password, note that username and password are Base64 encoded in the Authorization Header. As the delimiter symbol is a ":" (colon) between username and password (e.g. "ptc:ptc") the username must not contain a ":" (colon) character. Otherwise, the requests will fail with an error message, HTTP 401 Status - Authentication Required.

CSRF Tokens and REST Web Service Calls

When CSRF tokens are enabled, you need to add certain header values to your requests. Upon the first successful authenticated request from the client to the WS EMS/LSR, the WS EMS/LSR returns a response that includes a random CSRF token in the x-csrf-token header The client *must* include this token in any subsequent **PUT**, **POST**, or **DELETE** requests, or those requests are rejected as not authenticated. This token value may be changed, or ‘rotated’, at a defined interval.

For more information about using the REST services in Postman and the CSRF token support provided in the REST API for WS EMS and LSR as of v.5.4.2, refer to Running REST API Calls with Postman on WS EMS and LSR on page 134.

Reading and Writing Properties Using the REST Web Services

This topic explains how to read a property value and how to write a property value on page 118.

Reading a Property Value

To read a property from the local WS EMS, you can use a **GET** from the REST client and the following URL:

```
http://localhost:8000/Thingworx/Things/thing_name/Properties/prop_name
```

Notice that you are pointing at the local WS EMS, on port 8000, to retrieve a description. By default, the WS EMS listens on port 8000. Also by default, the WS EMS accepts requests only from an application that is running on the same machine as it is (i.e., localhost). You can configure a WS EMS to accept requests from other IP addresses.

When you execute this request, the WS EMS pushes it to the ThingWorx Platform. Keep in mind that the WS EMS has no state. It does not even know that the property exists. It just takes the request URL, breaks it up and repackages it, translates it into the AlwaysOn protocol, and forwards it to the ThingWorx Platform. The platform responds with its current value for that property. The result type is always of base type INFOTABLE, with the property name and current value.

Tip

To debug a problem with a property not updating or a service not executing, set the `level` and `publish_level`properties (in the `logger` group of the `config.json` file) to `TRACE` and in the `ws_connection` group, set the `verbose` property to `true`. That way, you can monitor all the activity passing between the WS EMS and the ThingWorx Platform.

For example, if the response appears to be returned slowly, by logging at the `TRACE` level and setting `verbose` to true, you can check the timestamps for the request and response to calculate the actual time. To match a request with a response, locate the `Request ID` of the outgoing message and the `Request ID` included in the incoming response message.

Writing a Property Value

To write a property value to the ThingWorx Platform through a WS EMS for an Edge device managed by a Lua Script Resource, select the **PUT** method in the REST client and use the same URL as a read (**GET**) for the property. For example:

```
http://localhost:8000/Thingworx/things/thing_name/Properties/<prop_name>
```

Then, in the area provided in the client, enter the property name and value, using JSON format:

```
{
  "<prop_name>": "Hello World from Thingworx"
}
```

It is important to remember that the ThingWorx Platform recognizes the **PUT** as coming from the Edge device and updates the value for the device and does not attempt to write it to the device.

If you shut down the Lua Script Resource and execute the same **PUT**, the value is written to the ThingWorx Platform for the device that is running WS EMS rather than the LSR device. The distinction is between writing the value directly to the platform, as opposed to writing the value through the WS EMS. In both instances the value is accessibl through ThingWorx Composer and available to any subscription or custom Javascript code you write to access the value.

You also need to set the `Content-type` for a write to the format you are using. In this case, it is `application/json`. If the device for the property is a Remote Thing, the property is also remote. If that device is not bound, you cannot write the value to the property. If the device is connected through a WS EMS and

Lua Script Resource and the WS EMS is running, you can start up the Lua Script Resource that is configured for the Remote Thing. Once the Remote Thing is bound, the ThingWorx Platform can send the write request to the WS EMS.

Note that the ThingWorx Platform instance does not change the property value until the request has made the full round trip:

1. A request is sent from a REST client to the specified ThingWorx Platform.
2. The ThingWorx Platform recognizes it as a remote property and forwards to the remote Thing.
3. If the Remote Thing is running a WS EMS, the WS EMS sends it to LSR, which writes it internally.

   At this point, the in-memory value on the ThingWorx Platform is still the old value. The LSR should be set up to send the value back up to the platform.
4. Only after the LSR sends the new value back to the ThingWorx Platform does the value change there.

Transferring Files through the REST Web Services

To prepare for file transfers, set up the WS EMS with virtual directories to send and receive files. If it is not already running, start the LSR for the device so that the virtual Thing at the edge is up and running and the ThingWorx Platform knows it is connected.

To invoke a file transfer from the platform, use the HTTP POST method and the following URL:

```
http://<server_name>:<port>/Thingworx/Subsystems/FileTransferSubsystem/Services/
Copy
```

In the area provided in the REST client, enter the parameters for the `Copy` service (in a JSON object), as indicated here:

```
{
  "sourceRepo": "<Enter a Valid Repository"
  "sourcePath": "<Enter a Valid Path>"
  "sourceFile": "<Enter a Valid File>"
  "targetRepo": "<Enter a Valid Thing>"
  "targetPath": "<Enter a Valid Path>"
  "targetFile": "<Enter a New Name for the file (optional>"
}
```

The parameters are broken down by target and source (you can view the parameters by looking at the definition for the Copy service in ThingWorx Composer).

Note

Refer to the ThingWorxHelp Center for more information about the Copy services, specifically the details concerning what is a valid file repository (that is, which templates support file transfer).

When you run the request, you can view the results (in JSON) format in the REST client. Scroll down until you locate the rows of the `infotable`. The value of the `state` parameter is `"validated"` if the file was transferred successfully.

You can also execute a file transfer through the WS EMS, using the same parameters and same POST, with the URL pointed at the local WS EMS:

```
http://localhost:8000/Thingworx/Subsystems/FileTransferSubsystem/Services/Copy
```

The headers for the WS EMS differ in that you have only the `content-type` header for the WS EMS. The results are the same (except that the WS EMS puts the rows at the top and the Data Shape at the bottom).

Why use the WS EMS or an SDK with the REST Web Service instead of just calling the ThingWorx platform REST Web Services from an application? There are some benefits to using the WS EMS or an SDK just to interact with the ThingWorx Platform, using the REST Web Services:

- You can have a secure connection when you use a WS EMS or an SDK to interact with a ThingWorx platform.
- The AlwaysOn protocol persists the connection between an application and a configured ThingWorx platform.
- When a WS EMS or an SDK makes the REST calls instead of your application, you save a lot in terms of resource usage on the ThingWorx Platform. The platform could potentially have to handle hundreds of HTTP requests coming from an application that is running on hundreds of devices, all sending multiple requests. Typically, the most expensive part of HTTP request is opening the socket — all the headers that are sent across the wire and so forth. When you use a WS EMS or SDK, you eliminate the burden on the ThingWorx Platform. The WebSocket connection is already set up (and persisted), and the multiple requests for an application are sent over the single WebSocket. In addition, the WS EMS and the SDKs send the requests using binary data, which results in more efficient use of bandwidth (in terms of the number of bytes that go across the wire).

- With the WS EMS or an SDK, the step to set up the socket is eliminated. Requests and responses can be exchanged more quickly. Especially if you have multiple applications that are making multiple requests behind a WS EMS, performance improvements are significant when you use the WS EMS to pass REST requests instead of passing them directly to your ThingWorx Platform.

REST Web Services Supported by WS EMS

The WS EMS is built to reflect the ThingWorx REST Web Service, but it is not a complete reflection. Rather, it is reflection of those Web Services that are most useful at the Edge. For example, if you try to look at Resources, nothing is returned. If you try to look at properties for a Thing that either is running the WS EMS or that is registered with it (WS EMS is running as a gateway), you can view all the properties. By default, the WS EMS returns data in JSON format.

For example, these Web Services do work with a WS EMS:

- **/Thingworx/Things/thing_name/Properties**
- **/Thingworx/Things/thing_name/Properties/prop_name**

where **thing_name** represents the name of any device that is connected to the local WS EMS where you are using a REST Web Service, and **prop_name** represents the name of any property for the specified device.

Note

As of v.5.4.2, support for CSRF tokens has been added to the REST API for WS EMS and LSR. It is enabled by default. Before using the REST API, be sure to read CSRF Token Support on page 135.

Browser-based Use of REST Web Services

The REST Web Services of the ThingWorx Platform can be used in a browser or an application that supports the HTTP commands. However, the behavior of the REST Web Services on a WS EMS is slightly different.

You cannot use a **PUT** through a query parameter of the REST Web Service in a browser, as on a ThingWorx Platform. For example, the following use of **PUT** works on a platform, but not on a WS EMS:

```
https://<server_ip/Thingworx/Things/<thing_name>/Properties/<property_name>/
        method=put&<prop_name>=<value>
```

You actually must do an HTTP **PUT** to the WS EMS, using a REST client that can do an HTTP **PUT**.

Another difference with the ThingWorx REST Web Services lies in how a WS EMS returns the information for a specific property. Both ThingWorx and a WS EMS use an infotable to return the information. However, a WS EMS returns the rows first and the Data Shape second. This order is the opposite from the order in which the ThingWorx REST Web Services return the information.

Similarly, for services, the following use of a service such as **GetDescription** works on a ThingWorx Platform, but not on a WS EMS:

```
https://<server_ip>/Thingworx/Things/thing_name/Services/GetDescription
```

For WS EMS, you must request to run services by using a **POST** through a client that can do an HTTP **POST**.

Note

You cannot send **POST** commands using a web browser if CSRF tokens are enabled (enabled by default and strongly recommended to keep enabled). You *must* use POSTMAN or another REST client.

As long as you do not have any input parameters for the service and if CSRF tokens are not enabled (strongly discouraged), you could do it this way from a browser:

```
https://localhost:8000/Thingworx/Things/thing_name/Services/GetDescription/method=
POST
```

However, if you have parameters and leave CSRF tokens enabled, use a client that can do an HTTP **POST**.

Here are a few of the REST Web Services of the ThingWorx that do not work with WS EMS:

- **/Thingworx/Things**
- **/Thingworx/Things/thing_name**
- **/Thingworx/Resources**

By default, a WS EMS uses `application/json` for the `Accept` header.

Note

As of v.5.4.2, support for CSRF tokens has been added to the REST API for WS EMS and LSR. It is enabled by default. Before using the REST API, be sure to read CSRF Token Support in REST API for WS EMS and LSR on page 135.

Using a REST Client with a WS EMS

You can use a REST client such as Postman to run REST Web Services against a WS EMS. You can save them and even set up collections of them. In addition, you can export a collection and import them into a Javascript engine such as Node.js.

Note

Before using Postman, be sure to read Running REST API Calls with Postman on WS EMS and LSR on page 134 and in particular, the section, CSRF Token Support in REST API for WS EMS and LSR on page 135.

When you are using REST Web Services, it is important to set your headers correctly:

- `Accept` — Specifies the format in which the data should be returned — JSON for WS EMS. For ThingWorx Platform, you can also choose XML or text.
- Application key (`appkey`) — Provides the authentication you need with the platform. You do not need it when running a REST Web Service against a local WS EMS.

  Although the application key is strongly recommended when running a REST Web Service against a remote WS EMS, you can use basic authentication. In Postman, you can select **Basic Authorization** and specify a user name and password to access the ThingWorx Platform.
- `x-thingworx-session` — Determines if your request will set up an HTTP session with the ThingWorx instance. Having a session makes it possible to send multiple requests from a browser to ThingWorx Composer without having to authenticate with each request. When you set up a session, the browser and Composer authenticate each request in the background.

  However, in an application, you do not want a session because sessions take up memory. For an application, set this header to `false` so that the ThingWorx platform does not create a session every time that the application sends a request. Sending the `appkey` with each request does not impact memory.

Note

If you use Basic authentication, you always get a session with the ThingWorx Platform. With an application, use an `appkey` for authentication and set the `x-thingworx-session` header to `false`.

- `x-csrf-token` — A random string used for Cross-Site Request Forgery (CSRF) protection in the WS EMS. When authentication and CSRF tokens are enabled on the WS EMS, the WS EMS will return a random CSRF token with each response that must be used in the next client request. If this token is not included or is incorrect, the request will fail with a `401 Unauthorized` error.

Using Services with a WS EMS

The following services work as REST Web Services with both a ThingWorx Platform and a WS EMS:

- AddEdgeThing on page 125
- GetConfiguration on page 125
- GetEdgeThings on page 126
- GetLogData on page 127
- GetMicroserverVersion on page 127
- HasEdgeThing on page 128
- RemoveEdgeThing on page 128
- ReplaceConfiguration on page 129
- Restart on page 130
- StartFileLogging on page 131
- StopFileLogging on page 132
- TestPort on page 132
- UpdateConfiguration on page 133

The WS EMS also supports using the `isConnected` property with a REST Web Service.

Note

As of v.5.4.2, support for CSRF tokens has been added to the REST API for WS EMS and LSR. It is enabled by default. Before using the REST API, be sure to read CSRF Token Support in REST API for WS EMS and LSR on page 135.

AddEdgeThing

The **AddEdgeThing** service adds an Edge device to the devices that are currently connected to the WS EMS.

Inputs

Pass in `TW_INFOTABLE` that has one row and two columns. The row object must contain the following parameters:

- The `name` of the device (Thing) that you want to add. Keep in mind that the device must exist on the ThingWorx Platform as a Thing that was created with the **RemoteThing** Thing Template. For example: `"name":"NameOfThing",`
- `persist`, which specifies whether the device should be added to the list of devices that are automatically bound to the corresponding Thing on the ThingWorx Platform. The format for this parameter is `"persist": true | false`.

Outputs

This service returns an HTTP response only. If the operation was successful, it returns HTTP 200. Otherwise, it returns an HTTP error.

Example

Here is an example of a REST call that adds an Edge Thing:

```
http://localhost:8000/Thingworx/Things/LocalEms/Services/AddEdgeThing
  {
    "name" : "acmeEdgeThing1",
    "persist": true
  }
```

GetConfiguration

The **GetConfiguration** service retrieves the configuration that the WS EMS is currently using

Note

This service does not return the current `config.json` file. Rather it returns the configuration that is currently loaded into the WS EMS. For example, if you call **UpdateConfiguration** but do not restart the WS EMS, the **GetConfiguration** service returns the configuration parameters and their values that the WS EMS is currently using, not the `config.json` file. The changes that were passed in with **UpdateConfiguration** are not available until you restart the WS EMS.

Inputs

This service does not take any input parameters.

Outputs

This service returns a `TW_INFOTABLE` that contains a json object. The object contains the configuration parameter/value pairs that are currently loaded in the WS EMS.

Example

Here is an example of a REST call that retrieves the configuration of a WS EMS:

```
http://localhost:8000/Thingworx/Things/LocalEms/Services/GetConfiguration
```

GetEdgeThings

The **GetEdgeThings** service returns a list of edge things that are registered with the WS EMS gateway.

Inputs

The name of the WS EMS gateway.

Outputs

This service returns a `TW_INFOTABLE` that contains the names of the Edge things that are registered with the WS EMS gateway.

Example

Here is an example of the REST call that retrieves the names of the Edge things that are registered with the WS EMS gateway:

```
http://localhost:8000/Thingworx/Things/LocalEms/Services/GetEdgeThings
```

GetLogData

The **GetLogData** service retrieves the log entries from the WS EMS.

Inputs

Pass in a `TW_INFOTABLE` that contains one row and three columns. The row object must contain the following parameters;

- `startDate` — The oldest log entry to retrieve, as a `DATETIME`.
- `endDate` — The newest log entry to retrieve, as a `DATETIME`.
- `maxItems` — The maximum number of entries to retrieve, as an `INTEGER`.

Outputs

This service returns a `TW_INFOTABLE` that contains the log entries. (The related Data Shape is `logEntry`.)

Example

Here is an example of a REST call that retrieves log entries for a WS EMS:

```
http://localhost:8000/Thingworx/Things/LocalEms/Services/GetLogData
  {
    "startDate": 1572566400,
    "endDate":1572652800,
    "maxItems":50
  }
```

GetMicroserverVersion

The **GetMicroserverVersion** service returns the version of the WS EMS.

Inputs

None

Outputs

This service returns a string that contains the version of the WS EMS. For example, `5.4.0`

Example

Here is an example of a REST call that retrieves the version of a WS EMS:

```
http://localhost:8000/Thingworx/Things/LocalEms/Services/GetMicroserverVersion
```

HasEdgeThing

The **HasEdgeThing** service checks whether a certain Thing is connected to the WS EMS.

Inputs

You can pass in raw JSON or an infotable that contains the name of the Thing whose connection you want to check:

- `TW_INFOTABLE`, that contains the name of the Thing to check. The infotable can be passed in as raw json. For example, `{"name":"ThingName"}`

Outputs

- `TW_INFOTABLE`, which contains the result, as `TW_BOOLEAN`. Returns `true` if the specified Thing is connected, `false` otherwise.

Example

Here is an example of a REST call that determines if a specified edge Thing is connected to a WS EMS:

```
http://localhost:8000/Thingworx/Things/LocalEms/Services/HasEdgeThing
  {
    "name": "acmeEdgeThing1"
  }
```

RemoveEdgeThing

The **RemoveEdgeThing** service removes the specified device from the set of devices that are connected to the WS EMS. In addition, it removes the device from the list of devices that should bind automatically when the WS EMS contacts the ThingWorx platform.

Inputs

You pass in an infotable that contains the name of the Thing that you want to remove from the WS EMS:

- `TW_INFOTABLE`, that contains the name of the Thing to remove. The infotable can be passed in as raw json. For example, `{"name" : "ThingName"}`

Note

If the removal is permanent, make sure that you also delete the Thing on the ThingWorx Platform side.

Outputs

This service returns an HTTP response only. If the operation was successful, it returns HTTP 200. Otherwise, it returns an HTTP error.

Example

Here is an example of a REST call that deletes an Edge Thing from the list of devices that should bind automatically when the WS EMS contacts the ThingWorx platform:

```
http://localhost:8000/Thingworx/Things/LocalEms/Services/RemoveEdgeThing
  {
    "name" : "acmeEdgeThing1"
  }
```

ReplaceConfiguration

The **ReplaceConfiguration** service allows you to replace the configuration file for the WS EMS (`config.json`).

Tip

The new configuration file does not take effect until you restart the WS EMS. Use the Restart on page 130 service to force the changes to take effect.

Inputs

Pass in a `TW_INFOTABLE` that contains a JSON object. This object must contain

- `"config"` — A JSON string that is used to replace the current configuration file.

Outputs

This service returns an HTTP response only. If the operation was successful, it returns HTTP 200. Otherwise, it returns an HTTP error.

Example

Here is an example of a REST call that replaces the configuration of a WS EMS that is running on your computer, using this service:

```
http://localhost:8000/Thingworx/Things/LocalEms/Services/ReplaceConfiguration
  {
    "ws_servers" {
                  "host":newServer.acme.com",
                  "port":80,
                  appkey="some_application_key"
    }
    "certificates" {
                    "disableCertValidation":true
    }
  }
```

Restart

The **Restart** service restarts the WS EMS.

Inputs

Pass in the following parameter:

- The *name* of the device (Thing) that you want to restart. For example:

```
{
  "name": "NameOfThing"
}
```

Note

The **Restart** service requires that you set the **restart** property in the `config.json` file of your WS EMS for any edge-side restart requests to work correctly. Otherwise, only requests from the ThingWorx Platform can restart the WS EMS. For more information, refer to Viewing All Configuration Options on page 60.

Outputs

This service returns an HTTP response only. If the operation was successful, it returns HTTP 200. Otherwise, it returns an HTTP error.

Example

Here is an example of a REST call that restarts the WS EMS:

```
http://localhost:8000/Thingworx/Things/LocalEms/Services/Restart
  {
    "name": "NameOfThing"
  }
```

StartFileLogging

The **StartFileLogging** service tells the WS EMS to begin writing log messages to a file. The WS EMS generates log messages at the level defined by a call to this service.

Inputs

You pass in `TW_INFOTABLE` that has one row and two columns. The row object must contain the following parameters:

- The `level` of the log messages to write to a file. Choose among the following levels: `TRACE`, `DEBUG`, `WARN`, `INFO`, or `AUDIT`, where `TRACE` provides the most information.
- `directory`, which specifies the path to the file on the computer where the WS EMS is running. Use the following format: `/twx/wsems/logfiles/directory`.

Note

The `TRACE` level is useful when testing and troubleshooting. It provides both the operational and functional log messages for a WS EMS.

Outputs

This service returns an HTTP response only. If the operation was successful, it returns HTTP 200. Otherwise, it returns an HTTP error.

Example

Here is an example of a REST call that tells a WS EMS to start logging messages that it generates to a file, with the log level set to TRACE:

```
http://localhost:8000/Thingworx/Things/LocalEms/Services/StartFileLogging
  {
    "level": "TRACE",
    "directory": "./ws_ems/logfiles"
  }
```

StopFileLogging

The **StopFileLogging** service tells the WS EMS to stop writing log messages to a file.

Inputs

You pass in the following parameter:

- `"delete" : true | false`. Set to `true` to stop the logging to a file, or `false` to continue logging to a file.

Outputs

This service returns an HTTP response only. If the operation was successful, it returns HTTP 200. Otherwise, it returns an HTTP error.

Example

StopFileLogging

Here is an example of a REST call that tells a WS EMS to stop logging messages that it generates to a file and to delete the existing log file:

```
http://localhost:8000/Thingworx/Things/LocalEms/Services/StopFileLogging
  {
    "delete": true
  }
```

TestPort

The **TestPort** service tests the connection to a specified ThingWorx instance and port.

Inputs

Pass in the following, required parameters:

- `host` - The URL of the WS EMS instance to connect to (as a `STRING`)
- `port` - The number of the port to connect to (as an `INTEGER`)

As of v.5.4.1, the **TestPort** service supports simplified infotables. With that release, support for additional, optional parameters was expanded. As a result, you can pass in optional parameters as well as the required parameters. For example:

```
{
  "host": "127.0.0.1",   // Required
  "port": "80",          // Required
  "useSSL": false,       // Optional
  "useProxy": false      // Optional
}
```

Outputs

This service returns a `true` if the connection is successful, or `false` if it cannot connect.

UpdateConfiguration

The **UpdateConfiguration** service of the WS EMS allows you to change or replace its configuration file (`config.json`).

Tip

The changes or new configuration file that you pass in do not take effect until you restart the WS EMS. Use the Restart on page 130 service to force the changes to take effect.

Inputs

Pass in a `TW_INFOTABLE` that contains a JSON object. This object must contain

- `"config"` — A JSON string that is used to update or replace the current configuration file.
- `"replace"` — A Boolean that determines whether to update the current `config.json` file or to delete it entirely and replace it with the JSON string specified with the `"config"` parameter.

Outputs

This service returns an HTTP response only. If the operation was successful, it returns HTTP 200. Otherwise, it returns an HTTP error.

Example

Here is an example of a REST call that updates the configuration of a WS EMS running on your computer, using this service:

```
http://localhost:8000/Thingworx/Things/LocalEms/Services/UpdateConfiguration
  {
    "config": "config.json",
    "replace": true
}
```

Running REST API Calls with Postman on WS EMS and LSR

- Calling REST API calls directly on the ThingWorx Platform requires authentication set, using the `userid` / `password` or `appkey` header.

> **Note**
>
> `username` and `password` are Base64 encoded in the Authorization Header. As the delimiter symbol is a ":" (colon) between `username` and `password` (e.g. `"ptc:ptc"` in the example above) the `username` must not contain a ":" (colon) character. Otherwise, the requests will fail with an error message, `HTTP 401 Status - Authentication Required.`

- The EMS / LSR REST API calls need to be called with the following configuration:
  - Instead of supplying credentials in the **Headers** section in Postman, you can use the **Authorization** tab.
  - The **Type** must be set to `Basic Auth` and a valid **username.password** combination must be provided.
  - In the **Headers**, **Content-Type** and **Accept** must be present. Postman will automatically add an **Authorization** key, based on the values provided in the **Authorization** tab.
  - In the **Headers**, you must also include the `x-csrf-token` header. The token is a random string used for Cross-Site Request Forgery (CSRF) protction in the WS EMS. When authentication and CSRF tokens are enabled on the WS EMS, the WS EMS will return a random CSRF token with each response. That token must be used in the next client request. If this token is not included or is incorrect, the request will fail with a `401 Unauthorized` error.

  As of v.5.4.2, CSRF token support is provided in the REST API for the WS EMS and LSR. This support is enabled by default. For more information, refer to the section below, CSRF Token Support in REST API for WS EMS and LSR on page 135.
- Use the following URLs to test the authentication mechanism:
  - *WS EMS* — Verify the System Repository name property.

    - `https://<ems_host>:8000/Thingworx/Things/SystemRepository/Properties/name`.
    - Should return `"name": "SystemRepository"`.
  - *WS EMS* — Verify the *isConnected* property of the **LocalEMS**.
    - `https://<ems_host>:8000/Thingworx/Things/LocalEms/Properties/isConnected`.
    - Should return `"isConnected": true`.
  - *LSR* — Verify that you get a `200 OK` response when connecting to the LSR.
    - https://<lsr_host>:8000/
    - Should return `200 OK` HTTP response with no content in the body.

Note

It is highly recommended that you use a secure password with more than three letters, as used in above example. For more information, refer to Password policy.

To learn what REST services are available for the LSR, refer to the `/help` on the LSR in a web browser.

CSRF Token Support in REST API for WS EMS and LSR

As of v.5.4.2, CSRF token support is provided in the REST API for the WS EMS and LSR. The support for CSRF tokens requires any requests from a client that can change state (such as POST, PUT or DELETE) include a CSRF token in the headers of their request. This token will be provided by the server and put into the response header with the key `x-csrf-token`. The client must include this same header and token value with any request that can change state.

The token will change periodically based on the `http_server_csrf_token_rotation_period` (WS EMS) and `scripts.script_resource_csrf_token_rotation_period` (LSR) values set in `config.json` and `config.lua`, respectively. The default period is every 10 minutes.

Neither the WS EMS nor the LSR require changes or configuration updates to support CSRF tokens. The tokens are enabled by default. Applications that use the REST interface of the WS EMS or LSR will need to be updated to include the CSRF token, or CSRF protection must be disabled (not recommended). You can disable CSRF protection by adding the line `enable_csrf_tokens = false` in the `http_server` `struct` of `config.json` (WS EMS) or `scripts.script_resource_enable_csrf_tokens` = `false`` in `config.lua` (LSR).

CSRF protection is enabled *only* when authentication is enabled as well. If authentication is disabled, no token values will be used. PTC recommends always using TLS, enabling authentication, and encrypting sensitive credentials in configuration files.

In addition to the CSRF token support, changes have been made in v.5.4.2 to how the Lua Script Resource's `/script` and `/scriptcontrol` REST endpoints work out-of-the-box. By default, you will not be able to use these endpoints to dynamically create, update, delete, or restart scripts using the REST API. Any requests to these services will result in a `405` – `Method Not Allowed` error. This feature can be enabled by adding the line `scripts.script_resource_enable_rest_services` = `true` to your `config.lua`

6

Getting Started with the Lua Script Resource

The following sections explain how to get started working with the Lua Script Resource (LSR). It is assumed that you installed the LSR with your WS EMS.

- Create a Lua Script Resource configuration file to set logging preferences, define Edge things that will run in the Lua Script Resource environment, define any extensions, etc. For details, refer to Configuring a Lua Script Resource on page 138.
- Create a Lua Script Resource Template File to define properties, services, and tasks for Edge things. For more information, refer to Configuring a Template for the Lua Script Resource on page 150.
- Run the LSR. For more information, refer to Running the Lua Script Resource on page 148.

7

Configuring a Lua Script Resource

When creating a Lua Script Resource (LSR), you create a configuration file, using the name, `config.lua`. This configuration file should be modeled after the example, `config.lua.example`. Your configuration file should be a text file that is separated into groups, with a group that sets logging levels, another one that configures edge things to run in the scripting environment, and a final one that defines any Lua Script extensions that are to be used by the Lua Script Resource.

To view this example of an LSR configuration file:

1. Open a command window or terminal session on the system or device that is hosting the Lua Script Resource.
2. Change into the `\microserver\etc` directory.
3. Open `config.lua.example`. Use this example as a reference while reading about the various groups of the configuration file.

The example file shows the main sections for configuring a Lua Script Resource. Follow the links below to read more about the properties of the configuration file:

- Logging on page 143
- HTTP Server Configuration on page 140 (SSL/TLS certificates)
- Configuring the Connection to the WS EMS on page 139
- Edge Thing on page 145

Configuring the Connnection from the LSR to the WS EMS

The sample configuration file, `config.lua.example`, for the Lua Script Resource (LSR) shows the properties to set for the connection between the LSR and the WS EMS. You should add these properties to your `config.lua` file:

```
scripts.rap_host = "<IP_address_for_WS_EMS>"
scripts.rap_port = "port_number_for_WS_EMS"
scripts.rap_ssl = true
scripts.rap_userid - "user_ID_for_WS_EMS_HTTP_Server"
scripts.rap_password = "some_encrypted_password"
scripts.rap_server_authenticate = true
scripts.fips_enabled = false
scripts.rap_cert_file = "path_to_CA_certificate_file"
scripts.rap_validate = true
scripts.rap_deny_selfsigned = true
```

Tip

For examples of secure configurations for communications between the WS EMS and the LSR, refer to Setting Up Secure Communications for WS EMS and LSR on page 159. These examples are presented in order of least secure (testing purposes ONLY) to most secure (strongly recommended for production environments).

As of v.5.4.8, encryption of application keys, passwords, and passphrases is automatic on startup of the LSR. For details, refer to Automatic Configuration Encryption on page 52. For previous versions of the LSR, you can manually encrypt these configuration settings. Refer toEncrypting Application Keys, Passwords, and Passphrases on page 36 to learn how.

Wherever `rap` appears in the `config.lua` file, the property is referring to the WS EMS.

The following table briefly describes the properties:

Property	Description
`scripts.rap_host`	The host name or IP address of the machine that is running the WS EMS.
`scripts.rap_port`	The port on which the WS EMS listens for connections from LSR clients.
`scripts.rap_ssl`	Whether to enable the use of SSL/TLS for the connection to the WS EMS. By default the value of this property is `true`.
`scripts.rap_userid`	The user id to present to the HTTP Server of the WS EMS for authentication.

Property	Description
scripts.rap_password	The password for that user, AES encrypted. For information about encrypting passwords, refer to Encrypting Application Keys, Passwords, and Passphrases on page 36.
scripts.rap_server_authenticate	Whether to require authentication
scripts.fips_enabled	If ssl is true, whether FIPS is also used for the connection. The default value is false. Note that if you want to use FIPS, make sure that you download the WS EMS distribution package that has fips in its name.
scripts.rap_cert_file	The path to the CA certificate on the machine that is running the LSR.
scripts.rap_validate	Whether to enable certificate validation when the LSR communicates with the WS EMS. The default value is true.
scripts.rap_deny_selfsigned	When certificate validation is enabled and the LSR initiates communication to the WS EMS, this property is checked. If the value of this property is trueand the WS EMS is using a self-signed certificate (such as the default one shipped with the WS EMS), the LSR will refuse to connect and log an error. The default value of this property is true.

Tip

In v.5.4.8 of the WS EMS and LSR, all sensitive data such as passwords is encrypted on startupand a data security key property is appended to the end of the configuration file. For details, refer to Automatic Configuration Encryption on page 52.

Configuring the HTTP Server for the LSR (SSL/TLS Certificate)

Suppose you want to set up a Lua Script Resource on a device that is external to the WS EMS. To prevent external sources from sniffing packets on your network, it is strongly recommended that you enable SSL/TLS on the HTTP servers on both the WS EMS and the Lua Script Resource. You can also require a user name and password for both HTTP server to ensure that only authenticated applications can access the LSR model and WS EMS communication channels.

Tip

Always configure a secure HTTP server. Otherwise, the WS EMS and LSR will log warning messages when any one or more of the following conditions is true:

- SSL is disabled. That is, the `ssl` property is set to `false`
- Authentication is disabled.
- Certificate validation is disabled.
- Self-signed certificates are allowed.

For examples of secure configurations for communications between the WS EMS and the LSR, refer to Setting Up Secure Communications for WS EMS and LSR on page 159. These examples are presented in order of least secure (testing purposes ONLY) to most secure (strongly recommended for production environments).

As of release 5.4.0 of the WS EMS, the Lua Script Resource (LSR) is configured to secure HTTP connections by default.

To load a PEM-encoded certificate for use by the LSR's HTTP server when TLS is enabled, you need to configure the following properties in your `config.lua` file:

```
-- HTTP Server Configuration
--
scripts.script_resource_host = "localhost"
scripts.script_resource_port = "8001"
scripts.script_resource_ssl = "true"
scripts.script_resource_certificate_chain = "/path/to/lsr_http_server_certificate_
chain/file"

scripts.script_resource_private_key = "/path/to/private/key"
scripts.script_resource_passphrase = "some_encrypted_passphrase"
scripts.script_resource_authenticate = "true"
scripts.script_resource_userid = "johnsmith"
scripts.script_resource_password = "some_encrypted_password"

scripts.script_resource_enable_csrf_tokens = true
scripts.script_resource_csrf_token_rotation_period = 10
scripts.script_resource_enable_rest_services = false
```

Note

The use of double quotation marks in `config.lua` is required only for Strings. For numbers and Boolean values, you do not need to use them. The LSR will work if you do use them for Booleans or numbers.

The port number is 8001 by default. You can choose whatever port is available for the HTTP server of the LSR.

To encrypt the passphrase and password, refer to Encrypting Application Keys, Passwords, and Passphrases on page 36.

The following table lists and briefly describes the properties for the HTTP Server of the LSR:

Property	Description
`scripts.script_resource_host`	The host name or IP address of the machine where the LSR is running. The default value is `"localhost"`
`scripts.script_resource_port`	The number of the port used on the host for communicating with the WS EMS. The default value is `"8001"`. Choose whichever port is available on the device for the HTTP Server of the LSR.
`scripts.script_resource_ssl`	Whether to use SSL/TLS for communication (Boolean). The default value is `"true"`
`scripts.script_resource_certificate_chain`	The path to the PEM-encoded certificate file. Use forward slashes when specifying the path, regardless of the operating system of the device.
`scripts.script_resource_private_key`	The path to the private key for the certificate. Use forward slashes when specifying the path, regardless of the operating system of the device..
`scripts.script_resource_passphrase`	The passphrase for the private key and certificate. Enclose the string in double quotation marks. For best security,this property value should be encrypted. If you are running v.5.4.8 or later, the encryption is automatically done on startup. For earlier bersions, you can manually encrypt the passphrase, as explained in Encrypting Application Keys, Passwords, and Passphrases on page 36.
`scripts.script_resource_authenticate`	Whether to authenticate the sender of an incoming request (Boolean). The default value is `"true"`.
`scripts.script_resource_userid`	The user name that will be presented for authentication when attempting to access the LSR..
`scripts.script_resource_password`	The encrypted password that should be presented when attempting to access the LSR. For information about encryption, refer to Encrypting Application Keys, Passwords, and Passphrases on page 36.
`scripts.script_resource_enable_csrf_tokens = true`	Flag that enables (`true`) or disables (`false`) the use of CSRF tokens for REST APIs with the LSR. By default, use of CSRF tokens is enabled. Refer to CSRF Token Support on page 135.

Property	Description
scripts.script_resource_csrf_token_rotation_period = 10	The number of minutes between changes to the CSRF token for a given session. The default value is 10 minutes.
scripts.script_resource_enable_rest_services = false	Flag that enables (true) or disables (false) the use of REST services with the LSR. By default, use of REST services is disabled. **Note** Changes were made for WS EMS/LSR v.5.4.2 to how the Lua Script Resource's /script and /scriptcontrol REST endpoints work out-of-the-box. By default, you will not be able to use these endpoints to dynamically create, update, delete, or restart scripts using the REST API. Any requests to these services will result in a 405 – Method Not Allowed error. This feature can be enabled by adding the line scripts.script_resource_enable_rest_services = true to your config.lua, as shown here.

Configuring the Logger for the LSR

As of version 5.4.0, the Lua Script Resource provides the same logging configuration properties as the WS EMS.

The scripts.log_level group (refer to the config.lua example configuration file) is used to configure the Lua Script Resource to collect logging information.

```
scripts.log_level = "INFO"
scripts.log_audit_target = "file:// or http:// "
scripts.log_publish_directory = "/_tw_logs/"
scripts.log_publish_level = "WARN"
scripts.log_max_file_storage = "2000000"
scripts.log_auto_flush = "true"
scripts.log_flush_chunk_size = "16384"
scripts.log_buffer_size = "4096"
```

Logging Properties

The following table lists and describes the properties of the `logger` element:

Property	Description
`scripts.log_level`	The level of information that you want to include in the audit log file. Valid values include: • `FORCE` • `ERROR` • `WARN` • `INFO` (the default value) • `DEBUG` • `TRACE` **Tip** When troubleshooting a problem, set the `level` to `TRACE` so that you can monitor all the activity. For production, set the `level` to `ERROR` if you want to view error messages.
`scripts.log_audit_target`	The path to the audit log file where audit events will be written. Alternatively, specify an HTTP address for the audit log file, where these events will be sent using a POST command. Audit events are also written to the normal log destination . If no target is specified, no additional auditing takes place. Valid values include: • `file://`*`path_to_file`* • `http://`*`hosted_location`*
`scripts.log_publish_directory`	A location for writing to log files those log events that meet or exceed the `publish_level.`. **Caution** sThe LSR and WS EMS use the same naming scheme for log files. Specify a directory that is different from the one specified in the `publish_directory` property in the `config.json` file of the WS EMS.
`scripts.log_publish_level`	The level of information that you want to include in the alternate log files. Valid values include: • `AUDIT` • `ERROR` • `WARN` • `INFO` • `DEBUG` • `TRACE`
`scripts.log_max_file_`	The maximum amount of space that log files can take up, in bytes. Keep

Property	Description
storage	in mind that there are two concurrent log files. The maximum size of each individual log file is max_file_storage divided by 2. The default value is 2000000 bytes (2MB).
scripts.log_auto_flush	Whether the LSR should flush every N bytes to the publish_directory. The N is defined by flush_chunk_size. The LSR also flushes the buffer if a message has not been written to the log in the last second. A setting of true forces the LSR to flush every N bytes.
scripts.log_flush_chunk_size	The number of bytes to write before flushing to disk. The default setting is 16384 bytes.
scripts.log_buffer_size	The maximum number of bytes that can be printed in a single logging message. The default setting is 4096 bytes.

Configuring Edge Things

The **EdgeThing** group is used to configure an Edge Thing to run in the Lua Script Resource environment. Of all the parameters that can be included in the **EdgeThing** group of the configuration file, only the *file* and *template* parameters are required. All other parameters are optional and can be included anywhere between the curly braces {}.

Note

The entry that defines the *Thing.lua* Edge Thing must exist in the configuration file. You can define additional Edge things with their own **EdgeThing** statements.

```
scripts.EdgeThing = {
    file = "Thing.lua",
    template = "example",
}
```

Parameters

The **EdgeThing** group contains the following parameters:

Parameter	Description
file	Define an Edge Thing. This parameter is required.
template	Specify the script identifying the information that you want to send from the device to your Edge Thing. The template file defines the behavior of the Edge Thing. This parameter is required. The template file must be placed in the \microserver\etc\custom\templates directory.
scanrate	Specify how frequently to evaluate the properties and possibly push them

Parameter	Description
	to the ThingWorx platform, in milliseconds. The default value is 60000 milliseconds.
taskrate	Specify how frequently to execute the tasks that are defined in the template of the edge Thing, in milliseconds. The default value is 15000 milliseconds.
scanRateResolution	Specify how long the main execution thread for this edge Thing pauses between iterations, in milliseconds. Each iteration checks the scan rate and task rate to determine if any properties are to be evaluated, or any tasks are to be executed. The value must be less than the scan rate or task rate. The default is 500 milliseconds. Refer to Configuring the scanRateResolution on page 146.
register	Specify whether or not the Edge Thing registers with the WS EMS. The default value is true (recommended).
keepAliveRate	Specify how frequently this edge Thing should renew its registration with the WS EMS, in milliseconds. If the WS EMS is restarted, this parameter controls the maximum amount of time before this edge Thing is re-registered. This value also controls how frequently the WS EMS performs a keep-alive check on the Lua Script Resource. If the Lua Script Resource is unavailable, the registered Thing is unbound from the ThingWorx Platform and appears to be offline. The default value is 60000 milliseconds.
requestTimeout	Specify the amount of time to wait for a response to an HTTP request to the WS EMS before timing out.
maxConcurrentPropertyUpdates	Specify the maximum number of properties that can be included in a single property update call to the ThingWorx Platform. This value can be decreased if the overall size of the batch property pushes is larger than what is supported by the WS EMS. The default value is 100 properties.
getpropertiesubscriptionsOnReconnect	Specify whether or not the edge Thing re-requests its property subscriptions when it reconnects to the WS EMS. This value is useful if the Lua Script Resource is running on a different Edge device from the WS EMS. The default value is true.
identifier	Specify the identifier used to register the edge Thing with the WS EMS and the ThingWorx platform.
useShapes	Specify whether or not to use Data Shapes for property definitions. The default value is true.

Configuring the scanRateResolution

The `scanRateResolution` setting controls the frequency at which the main loop of a script for a Thing executes in the LSR. Once it is started, a script enters into a loop that executes until the script resource is shut down. Each iteration of this main loop takes a number of actions, potentially increasing CPU usage.

At a high level, a script takes the following actions:

1. Goes through all your configured properties. If the `scanRate` amount of time for each property has expired, the property is evaluated to check whether it should be pushed. To evaluate the property, the LSR calls the read method of the property handler for each property. The new value is compared to the old (if necessary). If it needs to be pushed to the ThingWorx instance, the property and its value are added to a temporary list of properties to be pushed.
2. The temporary list of properties is pushed to the ThingWorx instance. If no properties have been evaluated, or no properties need to be pushed, this list is empty and nothing is pushed.
3. The registration of the Thing with the WS EMS is checked, using a call to the WS EMS.
4. If the `taskRate` time has expired, configured tasks are executed.
5. GC (garbage collection) is run if five seconds or more have elapsed.
6. The thread then sleeps for the number of milliseconds specified in the `scanRateResolution` parameter.

If you do not need the main loop to drive calls to the handlers that read your properties, you could set your `scanRateResolution` fairly high. A high setting would cause the main loop to sleep longer between iterations, which could have a few side effects:

1. The registration check will happen at the `scanRateResolution`, unless you adjust the `keepAliveRate` to be greater than the `scanRateResolution`.
2. You will need to set your `taskRate` and `scanRate` parameters to be greater than the `scanRateResolution`, or the script resource will complain during startup. Since it controls the pause of the main loop, the `scanRateResolution` is the main limiting factor in how often the main loop actions occur.
3. Shutting down the script resource can be delayed by up to the number of milliseconds specified for the `scanRateResolution` parameter, since the main loop must exit for the script to shut down.

The default value for the `scanRateResolution` is 500 milliseconds. If however, you do not require the loop to execute that often, consider setting this value much higher, even 10,000 milliseconds or more, to slow the execution of the loop and save CPU load.

8

Running the Lua Script Resource

The Lua Script Resource (LSR) can be run either from a command line or as a service to host things on the remote device.

Running from a Command Line

To run the Lua Script Resource from a command line, follow these steps:

1. Open a command window or terminal session on the system or device that is hosting the Lua Script Resource.
2. Change to the `\microServer\etc\` directory.
3. Copy and rename the `config.lua.example` file to `config.lua`.
4. Configure the file as necessary. Refer to Configuring a Lua Script Resource on page 138.
5. Change directories back to the to the top level `\microserver` directory.
6. Enter the `luaScriptResource` command to run the Lua Script Resource executable. To include a specific configuration file, use a command similar to the following:

   ```
   luaScriptResource -cfg .\etc\config.lua
   ```

   Note

   If no configuration file is specified, the default file, `etc\config.lua`, is used.

   This command causes the Lua Script Resource to start listening on port 8001, if the default values are used.

7. To access the interface of the extension, open a browser and enter the following address to view a list of executing scripts:

```
http://localhost:8001/scripts
```

8. Should you need to shut down the Lua Script Resource, press ENTER to display the console prompt and type `q`.

Running as a Service

To run the Lua Script Resource as a Windows service, follow these steps:

1. Open a command window or terminal session on the system or device that is hosting the Lua Script Resource.
2. Change to the `\microServer\etc` directory.
3. Copy and rename the `config.lua.example` file to `config.lua`.
4. Configure the file as necessary. Refer to Configuring a Lua Script Resource on page 138.
5. Run the following command:

```
C:\microserver\luaScriptResource.exe -cfg "C:\microserver\etc\config.lua"
                                     -i "ThingWorx Script Resource"
```

Where:

`cfg`	Specifies the full path to the location of the configuration file.
`i`	Specifies the name to be used for the installed service.

Note

Run the `luaScriptResource` executable and the reference to the configuration file using the full path (even if it is running from the directory where the `luaScriptResource.exe` file is located).

Due to space constraints, the command shown above has the second argument/value pair on a second line. Do NOT just copy and paste this command without removing the extra line break and spaces.

6. Should you need to uninstall the service, run the following command:

```
C:\microserver\luaScriptResource -u "ThingWorx Script Resource"
```

Where:

`u`	Specifies the name of the service to be un-installed. This name must exactly match the name that you assigned to the Lua Script Resource service.

9

Configuring a Template for the Lua Script Resource

The template file is a text file that is separated into groups. Each group is used to define the overall behavior, properties, services, and tasks for edge things that reference the template file. Template files must be placed in the `\microserver\etc\custom\templates` directory.

To view an example of a template file:

1. Open a command window or terminal session on the system or device that is hosting the Lua Script Resource.
2. Change into the directory, `\microserver\etc\custom\templates`.
3. Open the file, `config.lua.example`. Use this example as a reference while reading about the various groups of the template file.

Including a Data Shape

The `require` statement pulls the functionality of a Data Shape into the template. A Data Shape can define properties, services, and tasks. If a template defines a property, service, or task that has the same name as one defined in the shape file, the definition in the shape file is ignored. Be careful that you do not have duplicate names for these characteristics.

```
require "yourshape"
```

The following table describes the `require` parameter:

Use	To
`require`	Specify the name of the shape file that contains the properties, services, and task definitions that are to be added to the template file configuration. The shape file must be located in the directory, `\microserver\etc\custom\shapes`. **Note** If you intend to use file transfer with this Edge device, you must include the following statement: `require "thingworx.shapes.filetransfer"`

Configuring the Module Statement

The `module` statement is required. This statement tells the software component of the Edge device to operate according to the configuration instructions contained in the template file that you specify.

```
module ("templates.example", thingworx.template.extend)
```

The following table describes the two parts of the `module` statement:

Part	Description
Name of template file	The first part of the `module` statement must contain the name of the template file that contains the configuration for the software component of the Edge device. For example, `template.acmedevice`.
Extension of the ThingWorx template	The second part of the module statement, `thingworx.template.extend`, identifies the file as a template file to the system and extends the base ThingWorx template implementation. Do not modify this part of the statement.

Configuring Data Shapes

The `dataShapes` group is used to define Data Shapes that describe the structure of an infotable.

Data shapes that are declared can be used as input or output for services. In addition, you can use Data Shapes to generate strongly typed data structures.

Each Data Shape is defined using a series of tables, with each table representing a field within the Data Shape. These fields must have a name and base type, but may also include other parameters. For example:

```
dataShapes.MeterReading(
  { name = "Temp", baseType = "INTEGER" },
  { name = "Amps", baseType = "NUMBER" },
  { name = "Status", baseType = "STRING", aspects = {defaultValue="Unknown"} },
  { name = "Readout", baseType = "TEXT" },
  { name = "Location", baseType = "LOCATION" }
```

The following table lists and describes these parameters:

Parameter	Description
`dataShape.nameOfDataShape`	Declares a Data Shape.
`name`	Required. Specify the name of a field in the Data Shape.
`baseType`	Required. Specify the WS EMS base type of the field in the Data Shape. For a list of base types, refer to ThingWorx Base Types on page 172.
`description`	Provides a description of the Data Shape.
`ordinal`	Specify the order.
`aspects`	Specify a table that can provide additional information, such as a default value, or a Data Shape if the base type of the field is `INFOTABLE`.

Defining Properties

The `properties` group is used to define the properties associated with an Edge Thing. While remote data properties can be read on demand, you can also define data push rules so that the data does not have to be polled by the ThingWorx Platform from the Edge device.

A property is defined by specifying a name, `baseType`, `pushType`, the threshold for determining a data change push to the ThingWorx Platform, and any other necessary parameters.

Note

When these properties are bound at the ThingWorx Platform, it respects the template settings. However, if changes to the push and cache settings are made at the platform, those settings override the local template settings.

```
properties.IParametersnMemory_Imagelink =    { baseType="IMAGELINK", pushType=
"NEVER",
                                       value="http://www.thingworx.com" }
```

```
properties.InMemory_InfoTable =    { baseType="INFOTABLE", pushType="NEVER",
                                      dataShape="AllPropertyBaseTypes" }
properties.InMemory_Integer =      { baseType="INTEGER", pushType="NEVER", value=1
}
properties.InMemory_Json =         { baseType="JSON", pushType="NEVER", value="{}"
}
properties.InMemory_Large_String = { baseType="STRING", pushType="NEVER",
                      value=string.rep("Lorem ipsum dolorsi ", 15000) .. "the end"
}
properties.InMemory_Location =     { baseType="LOCATION", pushType="NEVER",
       value = { latitude=40.03, longitude=-75.62, elevation=103 }, pushType=
"NEVER" }
```

The following table lists and describes the parameters for defining properties:

Use	To
`properties.nameOfProperty`	Declare a property.
`baseType`	Required. Specify the base type of the property.
`dataChangeType`	Provide a default value for the Data Change Type field of the property definition on the ThingWorx Platform, if the property is initially created using the Manage Bindings feature of ThingWorx Composer. Valid values include: • `ALWAYS` • `VALUE` • `ON` • `OFF` • `NEVER`
`dataChangeThreshold`	Provide a default value for the Data Change Threshold field of the property definition on the ThingWorx Platform, if the property is initially created using the Manage Bindings feature of ThingWorx Composer.
`pushType`	Specify whether the property should push new values upon change to the ThingWorx Platform. Valid values include: • `ALWAYS` • `VALUE` • `NEVER` The default is `NEVER`. A `pushType` of `NEVER` does not push data to the platform, so when a property with `pushType=NEVER` is queried on the ThingWorx Platform, the platform queries the software of the Edge device for the data value. A `pushType` of `ALWAYS` pushes the data every time the property is read at the Edge device, which is determined by the `scanRate` parameter. If the `scanRate` is not set on the property, the `scanRate` from the Lua Script Resource configuration file is used. If not defined in either location, a default of 60000 milliseconds (1 minute) is used. The Edge

Use	To
	device pushes all properties that have a `pushType` of `ALWAYS` and the same scan rate in one call, rather than make individual calls per property. For `NUMBER` or `INTEGER` property types, a `pushType` of `VALUE` pushes data to the ThingWorx Platform only when the data value change exceeds the `DataChangeThreshold` setting.
`pushThreshold`	For properties with a `baseType` of `NUMBER`, and a `pushType` of `VALUE`. specify how much a property value must change before the new value is pushed to the ThingWorx Platform.
`handler`	Specify the name of the handler to use for property reads/writes. Valid values include: • `script` • `inmemory` • `http` • `https` • `generator` The default handler is `inmemory`. The `script`, `http`, and `https` handlers use the key field to determine the endpoint where their read/writes are to be executed. **Note** Custom handlers can specify other property attributes. When a handler is used to read or write a property, the entire property table is passed to the handler.
`key`	Define a key that the handler can use to look up or set the value of the property. In the case of a `script` handler, this key is a URL path. For `http` or `https` handlers, this key should be a URL and not the protocol. This parameter is not required for `inmemory` or nil handlers.
`value`	Specify the default value of the property. The value is updated as the value changes on the Edge device. The default value is 0.
`time`	Specify the last time the value of the property was updated, in milliseconds since the beginning of the epoch. When things are created from this template, the current time is set automatically, unless a default value is provided in the definition of the property.
`quality`	Specify the quality of the value of the property. A default value should be provided for the quality. Otherwise, the value defaults to `GOOD` for properties without a handler, and `UNKNOWN` for properties with a handler.

Use	To
scanRate	Specify the frequency of checking the property for a change event, in milliseconds. The default value is 5000 milliseconds (every 5 seconds). If you do not define a scanRate, the scanRate in the Lua Script Resource configuration file is used. Defining the scanRate within the property overrides the scanRate setting in the configuration file. Refer to Configuring the scanRateResolution on page 146.
cacheTime	Initialize the cache time of the value for the property at the ThingWorx Platform. The default value is –1 if the dataChangeType is NEVER, and is 0 when dataChangeType is ALWAYS or VALUE. If a value that is greater than 0 is specified, it is used by the ThingWorx Platform as the initial value for the cache time, and is applied only when using the browse functionality of ThingWorx Composer to bind the property.

Defining Services

The serviceDefinition group is used to provide metadata for a service that is used when browsing services from the ThingWorx Platform.

A service definition is a separate entry in the template file from the actual implementation of the service. The name of the service definition must match the name of the service it is defining in order for the service to work as expected.

```
serviceDefinitions.Add(
  input { name="p1", baseType="NUMBER", description="The first addend of the
operation" },
  input { name="p2", baseType="NUMBER", description="The second addend of the
operation" },
  output { baseType="NUMBER", description="The sum of the two parameters" },
  description { "Add two numbers" }
)

serviceDefinitions.Subtract(
  input { name="p1", baseType="NUMBER", description="The number to subtract from"
},
  input { name="p2", baseType="NUMBER", description="The number to subtract from
p1" },
  output { baseType="NUMBER", description="The difference of the two parameters"
},
description { "Subtract one number from another" }
```

Parameters

The following table lists and describes the parameters that you can use to define services:

Use	To
`serviceDefinition.nameOfService`	Declare a Service Definition.
`input`	Describe an input parameter to the service that is referenced within the data table that is passed to the service at runtime. Valid values include: • `name` — The name of the input parameter. • `baseType` — The type of input parameter used by the service. • `description` — A description of the input parameter.
`output`	Describes the output produced by the service. Valid values include: • `baseType` — The type of output that the service produces. • `description` — A description of the output that the service produces.
`description`	Provide information about the purpose and operation of the service.

Implementing Services Using the Lua Script Engine

Use the `services` group to implement the services that you declared when defining services.

Once a service has been defined, you can implement custom logic for the service, using the Lua Script engine. To speed implementation, you can use the add-ons of the Lua community and ThingWorx-specific Web Services. The Web Services are included in the WS EMS distribution to facilitate the development of custom scripts.

Services are defined as Lua functions that can be executed remotely from the ThingWorx Platform, and must provide a valid response in their return statement. For example:

```
services.Add = function(me, headers, query, data)
  if not data.p1 or not data.p2 then
    return 400, "You must provide the parameters p1 and p2"
  end
  return 200, data.p1 + data.p2
end

services.Subtract = function(me, headers, query, data)
  if not data.p1 or not data.p2 then
    return 400, "You must provide the parameters p1 and p2"
  end
  return 200, data.p1 - data.p2
end
```

Parameters

The following table lists and describes the parameters that you can use to define a service:

Parameter	Description
`services.nameOfService`	Implement a service. The name must match the name that is specified for the service in the service definition.
`me`	Create a table that refers to the Thing.
`headers`	Create a table of HTTP headers.
`query`	Specify the query parameters from the HTTP request.
`data`	Create a Lua table that contains the parameters of the service call.

A service function must return the following values, in the following order:

1. An HTTP return code (200 for success).
2. A table of HTTP response headers that should contain a valid Content-Type header, typically with a value of application/json.
3. (Optional) A default table can easily be generated by calling **tw_utils.RESP_HEADERS()**.
4. The response data, in the form of a JSON string. This data can be generated from a Lua table using `json.encode`, or **tw_utils.encodeData()**.

Configuring Tasks

Use the `task` group to define Lua functions that are executed periodically by the Lua Script Resource (LSR), such as background tasks, resource monitoring, event firing, and so on. These tasks allow you to introduce any customized functionality that you may need. You should follow the general pattern shown in the sample below:

```
tasks.Compare = function(me)
  -- Do task
end
```

The following table lists and describes the parameters that you can use to configure tasks:

Parameter	Description
`task.nameOfTask`	Implement a task that is scheduled in the Lua Script Resource to run periodically.
`me`	Create a table that refers to the Thing.
`end`	Define the end of the Lua function that defines the task.

10

Examples of Configuring Secure Communications between the WS EMS and an LSR

This section provides example security configurations for the connection between the WS EMS and an LSR, from least secure (for testing purposes ONLY) to most secure (strongly recommended for production environments). Remember that only the most secure configuration is recommended for anything other than a testing environment.

Included are examples of the following:

- No security — for testing purposes ONLY
- Configuring a custom certificate/private key for the WS EMS/LSR HTTP server
- Configuring a certificate chain when using a certificate issued by a Certificate Authority (CA)
- Configuring authorization for communication between the WS EMS and LSR

No Security — for Testing ONLY

This configuration disables all secure communication and authorization settings. All communication will be transmitted in clear text, and the WS EMS and LSR can be accessed by anyone. This configuration should be used for testing purposes ONLY.

Insecure Configuration

WS EMS — `config.json`

```
"http_server": {
  "host": "localhost",
  "port": 8000,
  "ssl": false,
  "authenticate": false
},
"certificates": {
  "validate": false,
  "allow_self_signed": true,
  "disable_hostname_validation"
: true
}
```

LSR — `config.lua`

```
-- EMS Connection Configuration
scripts.rap_host = "localhost"
scripts.rap_port = 8000

-- EMS Connection TLS Configuration
scripts.rap_ssl = false

-- EMS Connection Authentication
-- Configuration
scripts.rap_server_authenticate = false

-- HTTP Server Configuration
scripts.script_resource_host =
localhost"
scripts.script_resource_port = 8001

-- HTTP Server TLS Configuration
scripts.script_resource_ssl = false

-- HTTP Server Authentication
-- Configuration
scripts.script_resource_authenticate =
false
```

Medium Security

The following examples provide a medium level of security. All communication between the WS EMS and LSR are encrypted and require basic authentication to be accessed. The examples use a self-signed certificate and private key.

Note

This configuration allows self-signed certificates, which is strongly discouraged for a production environment.

To fit the lines of configuration on the page, the lines have been broken up. If you copy/paste the lines, make sure that you adjust the line breaks accordingly. For example, the line containing the `cert_chain` property in the `config.json` example has been broken with a CR and extra spaces. You need to remove that line break and extra spaces after pasting it in your configuration file.

To learn about encrypting the passwords and passphrases, refer to Protecting Data with Encryption on page 50.

Security Configuration with Authentication, Validation, and Custom Self-Signed Certificate / Key

WS EMS — `config.json`

```
"http_server": {
  "host": "localhost",
  "port": 8000,
  "ssl": true,
  "certificate": "/ path/to/
    certificate/file.pem",
  "private_key": "/path/to/
    private/key.pem",
  "passphrase": "some_encrypted_
passphrase",
  "authenticate": true,
  "user": "emsuser",
  "password": "some_encrypted_
password""
},
"certificates": {
  "validate": true,
  "allow_self_signed": true,
  "disable_hostname_validation":
true,
  "cert_chain" : "/path/to/
    ca/cert/list.pem"
}
```

LSR — `config.lua`

```
-- EMS Connection Configuration
scripts.rap_host = "localhost"
scripts.rap_port = 8000

-- EMS Connection TLS Configuration
scripts.rap_ssl = true
scripts.rap_deny_selfsigned = false
scripts.rap_validate = true
scripts.rap_cert_file =
  "/path/to/ca/cert/list.pem"

-- EMS Connection Authentication
--  Configuration
scripts.rap_server_authenticate =
true
scripts.rap_userid = "emsuser"
scripts.rap_password = "some_
encrypted_password"

-- HTTP Server Configuration
scripts.script_resource_host =
"localhost"
scripts.script_resource_port = 8001

-- HTTP Server TLS Configuration
scripts.script_resource_ssl = true
scripts.script_resource_
certificate_chain =
  "/path/to/web/server/
certificate.pem"
scripts.script_resource_private_key
=
  "/path/to/web/server/private/
key.pem"
scripts.script_resource_passphrase
= "some_encrypted_passphrase"

-- HTTP Server Authentication
--  Configuration
scripts.script_resource_
authenticate = true
```

Security Configuration with Authentication, Validation, and Custom Self-Signed Certificate / Key (continued)

WS EMS — `config.json`	LSR — `config.lua`

	`scripts.script_resource_userid =`
	`"luauser"`
	`scripts.script_resource_password =`
	`"some_encrypted_password"`

High Security

The following examples provide a high level of security. All communication between the WS EMS and LSR are encrypted and require basic authentication to be accessed. The examples use a custom certificate and private key. The certificate is validated against a custom CA list. This configuration disallows self-signed certificates. This configuration is the recommended configuration for all production systems.

To learn about encrypting passwords and passphrases, refer to Protecting Data with Encryption on page 50.

Highly Secure Configuration: Authentication, Validation, and Custom Certificate / Key

WS EMS — `config.json`

```
"http_server": {
  "host": "localhost",
  "port": 8000,
  "ssl": true,
  "certificate":
   "/pathto/cert/file.pem",
  "private_key":
    "/pathto/private/key.pem",
  "passphrase": "some_encrypted_
passphrase",
  "authenticate": true,
  "user": "emsuser",
  "password": "some_encrypted_
password"
},
"certificates": {
 "validate": true,
 "allow_self_signed": false,
 "disable_hostname_validation":
false,
 "cert_chain" :
   "/path/to/ca/cert/list.pem",
 "http_client_ca_certs"" : "/path/
to/ca/cert/client_list.pem"
}
```

LSR — `config.lua`

```
-- EMS Connection Configuration
scripts.rap_host = "localhost"
scripts.rap_port = 8000

-- EMS Connection TLS Configuration
scripts.rap_ssl = true
scripts.rap_deny_selfsigned = true
scripts.rap_validate = true
scripts.rap_cert_file =
  "/path/to/ca/cert/list.pem"

-- EMS Connection Authentication
-- Configuration
scripts.rap_server_authenticate =
true
scripts.rap_userid = "emsuser"
scripts.rap_password = "some_
encrypted_password"

-- HTTP Server Configuration
scripts.script_resource_host =
"localhost"
scripts.script_resource_port = 8001

-- HTTP Server TLS Configuration
scripts.script_resource_ssl = true
scripts.script_resource_
certificate_chain =
  "/path/to/web/server/
certificate.pem"
scripts.script_resource_private_key
=
  "/path/to/web/server/private/
key.pem"
scripts.script_resource_passphrase
= "some_encrypted_passphrase"

-- HTTP Server Authentication
-- Configuration
scripts.script_resource_
authenticate = true
```

Highly Secure Configuration: Authentication, Validation, and Custom Certificate / Key (continued)

WS EMS — `config.json`	LSR — `config.lua`

	`scripts.script_resource_userid = "luauser"`
	`scripts.script_resource_password = "`*`some_encrypted_password`*`"`

11

Troubleshooting the WS EMS and the LSR

Troubleshooting the WS EMS

This section discusses issues that can arise when using the WS EMS, along with recommended solutions.

Problem	Possible Solution
The WS EMS connects, but reports a time-out error when trying to authenticate.	Verify that you are running the required version of Tomcat. Refer to the ThingWorx WebSocket-Based Edge MicroServer Support Matrix in the help center.
The WS EMS is failing to connect to my local server.	If your server is not configured to use HTTPS, set the `encryption` option of the WS EMS to `none`. Before deployment, set the option back to `ssl`.
I've started the WS EMS, made changes to `config.json`, but these changes are not reflected when I restart the WS EMS.	There is likely a syntax error (such as an extra comma, or similar) in your `config.json`. If the WS EMS is unable to start with the current `config.json`, it will use the last known good configuration file (`config.json_booted`). To verify that the problem is in `config.json`, delete the `config.json_booted` file and restart the WS EMS. If it fails to start, check the `config.json` for errors.

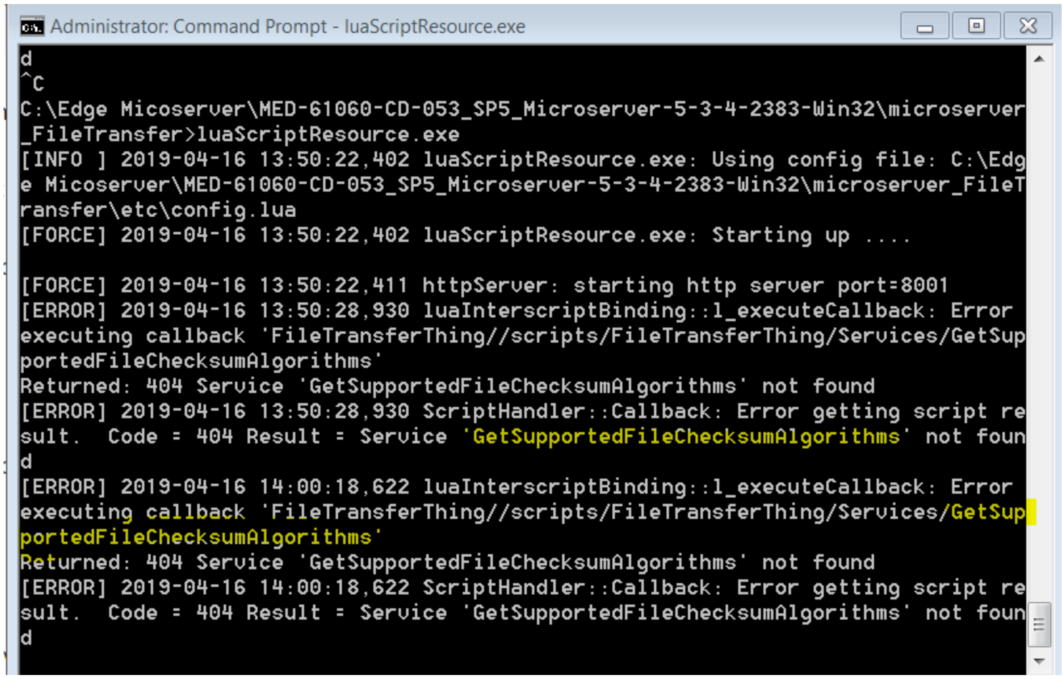
The WS EMS connects to a ThingWorx Platform, authenticates successfully, but the Thing I specified in the "auto_bind" group of my configuration file is not being created on the THingWorx platform.	The "auto_bind" group is an array of objects. Verify that you've enclosed the JSON object that represents your Thing in square brackets as follows:
	`"auto_bind": [{`
	`"name": "RemoteThing001",`
	`"gateway": true`
	`}]`
	Instead of this, which would lead to this Thing not being created on ThingWorx Platform:
	`"auto_bind": {`
	`"name" : "RemoteThing001",`
	`"gateway": true`
	`}`

Troubleshooting File Transfers When Using Automatic Binding

Problem

A download of a file to a WS EMS that is configured to use automatic binding fails, with the following error messages:

WS EMS Error Message During File Transfer



```
d
^C
C:\Edge Micoserver\MED-61060-CD-053_SP5_Microserver-5-3-4-2383-Win32\microserver
_FileTransfer>luaScriptResource.exe
[INFO ] 2019-04-16 13:50:22,402 luaScriptResource.exe: Using config file: C:\Edg
e Micoserver\MED-61060-CD-053_SP5_Microserver-5-3-4-2383-Win32\microserver_FileT
ransfer\etc\config.lua
[FORCE] 2019-04-16 13:50:22,402 luaScriptResource.exe: Starting up ....

[FORCE] 2019-04-16 13:50:22,411 httpServer: starting http server port:8001
[ERROR] 2019-04-16 13:50:28,930 luaInterscriptBinding::l_executeCallback: Error
executing callback 'FileTransferThing//scripts/FileTransferThing/Services/GetSup
portedFileChecksumAlgorithms'
Returned: 404 Service 'GetSupportedFileChecksumAlgorithms' not found
[ERROR] 2019-04-16 13:50:28,930 ScriptHandler::Callback: Error getting script re
sult.  Code = 404 Result = Service 'GetSupportedFileChecksumAlgorithms' not foun
d
[ERROR] 2019-04-16 14:00:18,622 luaInterscriptBinding::l_executeCallback: Error
executing callback 'FileTransferThing//scripts/FileTransferThing/Services/GetSup
portedFileChecksumAlgorithms'
Returned: 404 Service 'GetSupportedFileChecksumAlgorithms' not found
[ERROR] 2019-04-16 14:00:18,622 ScriptHandler::Callback: Error getting script re
sult.  Code = 404 Result = Service 'GetSupportedFileChecksumAlgorithms' not foun
d
```

This failure can also occur if you download an SCM package from the ThingWorx Platform to the WS EMS.

In addition, the ThingWorx Platform logs show a Gateway Timeout error

```
2019-04-16 14:04:08.235-0400 [L: ERROR] [O: E.c.t.s.s.f.e.FileCopyTask]
[I: ]
 [U: Administrator] [S: ] [T: FileTransfer-3]
 [context: Error occurred during transfer.: service execution failure
 resultCode=STATUS_GATEWAY_TIMEOUT:
 job=TransferJob [tid: 205bbb83-63c9-4e5f-8f4f-05f654cdc360, sourceRepo:
FileTransferThing,
 sourcePath: \In\Welcab6.jpg, targetRepo: Repo2, targetPath: \new
\Welcab6.jpg,
 partPath: \new\Welcab6.jpg.Repo2.part, sourceChecksum: , targetChecksum:
,
 state: ACTIVE, code: 202,
 message: Transfer request accepted, isAsync: false, isRestartEnabled:
true,
 isComplete: false, bytesTransferred: 0, blockcount: 0, blocksize: 8192,
size: 1089448,
 maxsize: 100000000, transferTime: 0, transferControl: platform,
reservationId: ,
 isQueueable: false, enqueueTime: 0, enqueueCount: 0, metadata: null,
 Job [id: 205bbb83-63c9-4e5f-8f4f-05f654cdc360, lastTouch: 1555437847173,
timeout: 30000,
 TimedLock [createTime: 1555437847148, signalTime: 0, duration: 0,
signaled: false]]]]
2019-04-16 14:04:08.241-0400 [L: ERROR] [O: E.c.t.s.s.f.e.FileCopyTask]
[I: ] [U: ]
```

```
[S: ] [T: FileTransfer-3] [context: Error occurred during transfer.]
```

Recommended Workaround

To perform a file transfer using WS EMS, you can but do not need to have an LSR running. However, you do need a bound Thing. In versions 8.3.5 and 8.4.x of the ThingWorx Platform, a service was introduced, called **GetSupportedChecksumAlgorithms**. This service breaks previously working WS EMS configurations that use `auto_bind` for identity but do not specify a host and port. The workaround for this change is to make sure that your `auto_bind` configuration specifies the host and port used by the `http_server` configuration. This workaround resolves both file transfer and tunneling errors that occur when `auto_bind` does not specify a host and port.

Caution

It is not recommended to use an `auto_bind` configuration without specifying a host and port. The `auto_bind` configuration should be u sed to bind an existing HTTP server on your LAN as a Remote Thing. Using `auto_bind` just to define a Thing and have it show up in ThingWorx Composer without running an LSR can cause problems when the platform sends requests to the Edge Thing and there is nothing to which the WS EMS can route the request.

Running on a Windows-based Operating System

When running the WS EMS on Windows-based operating systems, it is possible for the Windows OS to have a tick resolution that is higher that the tick resolution requested by WS EMS. For example, the default Windows tick resolution is 15ms and the default tick resolution for WS EMS is 5ms. In this scenario WS EMS executes only at the limit interval of 15ms instead of the requested 5ms interval. To achieve the best performance, it is recommended that the Windows tick resolution be changed, using the Windows API functions, to one half of the maximum sampling rate (Nyquist Sampling). Note that some systems will experience high CPU load due to the increased tick timer.

Troubleshooting the Lua Script Resource

The following table discusses issues that can arise when using the Lua Script Resource, along with recommended solutions.

Problem	Possible Solution
I have a tunnel configured on my Thing (created using the **RemoteThing** Thing Template) on the ThingWorx Platform, but it is not working.	Verify that the Public Host and Public Port settings of the Tunnel Subsystem's Configuration are set to the externally available host name/IP and port.
The Thing that I have configured in `config.lua` cannot communicate with my Thing on the ThingWorx Platform.	Verify that the name of the Thing in your `config.lua` matches the name of the Thing on the ThingWorx Platform. You can also specify an identifier, if using matching names is a problem. Refer to Configuring File Transfers on page 77.

The WS EMS connects to the ThingWorx Platform, authenticates successfully, but the Thing that I specified in the `auto_bind` group of my `config.lua` file is not being created on the platform.	The `auto_bind` group is an array of objects. Verify that you enclosed the JSON object that represents your Thing in square brackets as follows:
	`“auto_bind”: [{`
	`  “name”: “RemoteThing001”,`
	`  “gateway:” true`
	`}]`
	vs. the following, which leads to this scenario:
	`"auto_bind": {`
	`  "name": "RemoteThing001",`
	`  "gateway": true`
	`}`
	For more information about the auto_bind group and setting the gateway parameter, refer to Configuring Automatic Binding for WS EMS on page 73 and to Auto-bound Gateways on page 75

A

ThingWorx Base Types

This appendix provides a table of the ThingWorx Base Types.

ThingWorx Base Types

The following table lists and briefly describes the ThingWorx Base Types:

ThingWorx Base Types

Type Name	Description
`BASETYPENAME`	A valid name of a Base Type.
`BOOLEAN`	True or false values only
`BLOB`	A Binary Large Object.
`DASHBOARDNAME`	The name of a dashboard.
`DATASHAPENAME`	A reference to a Data Shape in a model, and therefore has special handling.
`DATETIME`	Date and time value
`GROUPNAME`	ThingWorx Group Name
`GUID`	Globally Unique IDentifier. **Note** If using GUID as the Base Type, it is recommended to set the GUID value. Do not leave blank (default).
`HTML`	HTML value
`HYPERLINK`	Hyperlink value
`IMAGE`	Image Value
`IMAGELINK`	Image link value
`INFOTABLE`	ThingWorx data structure used to define the results of a service or a set of properties for a Thing
`INTEGER`	32–bit integer value
`JSON`	JSON structure
`LOCATION`	ThingWorx Location structure
`MASHUPNAME`	ThingWorx Mashup name
`MENUNAME`	ThingWorx Menu name
`NOTHING`	No type (used for services to define void result)
`NUMBER`	Double-precision value
`PASSWORD`	A masked password value.
`QUERY`	ThingWorx Query structure
`SCHEDULE`	A CRON-based schedule (in ThingWorx Composer, can b e configured using the Schedule Editor).
`STRING`	Any amount of alphanumeric characters.
`TAGs`	ThingWorx tag valaues.
`TEXT`	Any amount of alphanumeric characters. The difference with strings is that `TEXT` is indexed.
`THINGCODE`	A numerical representation of a Thing containing a DomainID and InstanceID. For example: 2:1.
`THINGNAME`	A reference to a Thing and therefore has special handling.
`THINGSHAPENAME`	A reference to a Thing Shape in the model, and therefore has special handling.
`THINGTEMPLATENAME`	The name of a Thing Template.
`USERNAME`	A reference to a ThingWorx user defined in the system. In general to avoid

ThingWorx Base Types (continued)

Type Name	Description
	issues with REST APIs, do not use the colon (`:`) character in user names.
`VEC2`	A collection of two numbers. For example, 2D coordinates, x and y.
`VEC3`	A collection of three numbers. For example, 3D coordinates, x, y, and z.
`VEC4`	A collection of four numbers. For example, 4D coordinates, x, y, z, and w.
`XML`	An XML snippet or document.

B

Remote Things

This section explains what Remote Things are, briefly describes some of the templates available in ThingWorx Composer for Remote Things, and provides information about configuring them and their properties and services.

- About Remote Things on page 175
- Remote Thing Configuration at the Device on page 175

About Remote Things

A Remote Thing is an Edge device or data source whose location is at a distance from the location of the ThingWorx Platform. A Remote Thing accesses the platform, and can itself be accessed, over the network (Intranet/Internet/WAN/LAN). The device is represented on the platform by a Thing that is created using the **RemoteThing** template, or one of the derivatives of that template (for example, **RemoteThingWithFileTransfer**).

The default Thing templates that you can use to create things for remote devices follow:

- **RemoteThing** — A basic Thing that provides the ability to interact with a remote device.
- **RemoteThingWithFileTransfer** — A remote Thing that can also transfer files.
- **RemoteThingWithTunnels** — A Remote Thing that supports tunneling.
- **RemoteThingWithTunnelsAndFileTransfer** — A Remote Thing that supports both file transfers and tunneling.
- **RemoteDatabase** — A remote OLE-DB data source
- **EMSGateway** — Addresses the WS EMS as a standalone Thing. This template may be useful in situations where the WS EMS is running on a gateway computer and is handling communication for one or more Remote Things, which may reside on different IP addresses within a local area network
- **SDKGateway** — Similar to the **EMSGateway** template, but used when you are using an SDK implementation as a gateway.

Use the **RemoteThing**, **RemoteThingWithFileTransfer**, **RemoteThingWithTunnels**, and **RemoteThingWithTunnelsAndFileTransfer** templates for vendor-specific devices. The recommended approach is to use one of these templates to create a Thing for your vendor-specific device, and when you have added the properties, services, and events for the Thing, save it as your own template. That way, you can add more of the same devices quickly and easily by using your template as the base.

Remote Thing Configuration at the Device

The Remote Thing at the device level is implemented using the Lua Script Resource (luaScriptResource.exe). This component shares the configuration file with the WSEMS (config.lua, or per your configuration). Make a copy of the file and place it in the etc directory. The example configuration file is self-documented.

```
scripts.MyEdgeThing = {
file = "Thing.lua",
template = "example",
```

This section defines a Thing, and references a Template = example. In this case, that refers to a file named config.lua.example in the `microserver\etc\custom\templates` directory. This file is installed with the WS EMS to be used for reference. The template file is for defining properties, services, and tasks at the edge software.

Any of the Remote Thing configuration parameters can be inserted between the brackets { } defined by scripts.MyEdgeThing=.

The template setting is critical. The template file is the definition of the behavior for this edge Thing. Each edge Thing utilizing the Lua script engine requires a template file reference. The template file should be placed in the `\microserver\etc\custom\templates` directory. An example file is available after install.

Basic Configuration

The `config.lua`.example file has a section for module configuration.

The **require** statements pull a specified shape's functionality into the template. A shape can define properties, services, and tasks, just like a template. If the template defines a property, service, or task with the same name as one defined in a shape, then the definition in the shape will be ignored. Therefore, you must take care not to define characteristics with duplicate names. require "thingworx.shapes. myshape”

The following line is required in all user-defined templates: 'template.example' should be replaced with the name of template, for example: 'template.mydevice'. module ("templates.example", thingworx.template.extend)

Shapes

A shape file is the same in structure as a template file. The idea is to create building block files of properties, services, and tasks, and identify them as shapes, which is consistent with the server model terminology. The expected location for these shape files is the `\microserver\etc\custom\shapes` directory. Using the **require** statement essentially adds the shape file configuration to the configuration in the template

Configure Properties for Remote Things

It is possible to browse the configuration of a Remote Thing and "mass" bind its remote properties. The ability to bind the properties of a remote device all at once allows you to fully configure the Remote Thing on the ThingWorx Platform, alleviating much of the manual configuration.

1. In ThingWorx Composer, on the **Properties** tab of the Remote Thing, click **Manage Bindings.**
2. In the **Manage Property Bindings** dialog box, click the **Remote** tab.

3. YA list of the properties of the remote device appears on the left. You can drag them individually to the **Drag HERE to create new properties area**) or click **Add All.**
4. You can then individually edit the property details to suit your needs. You can also bind the remote properties to properties that you have already defined on the ThingWorx Platform. To bind remote properties to existing properties on the platform, drag a remote property onto an existing platform property. When you bind properties from the edge, the cache and push settings from the edge are set based on the configuration settings of the Edge device. You can choose to override them by changing the settings at the platform (using ThingWorx Composer, for example).

   You can also manually create the properties by using the standard property configuration dialog box.

Configure Services for Remote Things

There are two types of services for Remote Things, as follows:

- **Local (JavaScript)** - JavaScript business logic executing on the server.
- **Remote** - a direct call to a remote service on a Remote Thing (such as a custom-defined Lua script).

Remote Services and Binding

When you define a remote service, you are defining the metadata for the service so that it can be properly consumed from the server. The definition includes the service name at the server, the description, remote service name, and the inputs and outputs of the service. This will bind the service to the remote service, and the remote service is executed when the service runs. From a Mashup or REST Web Service perspective, it will appear the same as a local service.

When the WSEMS opens a connection to a ThingWorx Platform, it goes through a three step process:

1. Initiation: This establishes the physical WebSocket connection and prepares it to handle inbound and outbound messages.
2. Authentication: The WS EMS can authenticate using an application key. All communication that is passed over the connection from the WS EMS to the ThingWorx Platform will run under the security context of this application key. After authentication is complete applications can use the REST interface of WS EMS to interact with the ThingWorx Platform.
3. Binding: After authentication, Remote Things on the ThingWorx Platform can bind to the connection of the WS EMS. Binding is the process that notifies the platform that a particular Remote Thing is associated with an established connection. After a Thing is bound to a connection, the platform will indicate

a change in the value of its **isConnected** property to `true` and update its **lastConnection** property. The platform can then send outbound requests to Thing.

You can also directly browse and bind to remote services if the Remote Thing is running and is connected. Click **Browse Remote Services** to view the services that are currently defined for the Remote Thing. You can then add them to the local service definitions through the drag and drop interface (similar to how you bind remote data properties).

The process of registering a Thing with the WS EMS also causes the Thing to bind. The de-registering of a Thing causes it to unbind.