

METDaemon Application Server SSL Installation Guide

Copyright © 2024 On Time Support

This manual, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. The content of this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by On Time Support Inc®.

Although every precaution has been taken in the preparation of this manual, the publisher and author assume no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of such information contained herein. On Time Support Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in this book.

Except as permitted by such license, no part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of On Time Support Inc.

All terms mentioned in this manual that are known to be trademarks or service marks have been appropriately denoted. Use of a term in this manual should not be regarded as affecting the validity of any trademark or service mark.

Table of Contents

Introduction.....4

Getting Started.....5

Introduction

METDaemon(TM) is an Application Server provided by On Time Support that serves as the foundation for a variety of products offered by OTS. This application server is a software package that is designed to host web-based applications and provide built-in services for interacting with a number of database packages.

This document describes creating an SSL keystore, Certificate Signing Request(CSR), and installing the certificate chains that allow METDaemon to use SSL(<https://>).

Getting Started

In Windows Explorer, navigate to the "METDaemon\etc\" installation directory. Verify that a file named "keystore" does not exist.

If it **does** exist, stop the METDaemon service, then rename this file to "keystore.bak".

Open a Windows CMD window and navigate to the METDaemon installation directory.

ex. cd "[c:\program files\on time support\metdaemon\](#)"

The following command will generate a key pair and a new keystore:

jre\bin\keytool.exe -genkey -keysize 2048 -keyalg RSA -alias metdaemon -keystore etc\keystore

The keystore file name must be "keystore" for METDaemon to find it. This file must be in the "METDaemon\etc\" directory.

This command will prompt for information about the certificate and for passwords to protect both the keystore and the keys within it (You can use the same password for both).

The only mandatory response is to provide the fully qualified host name of the server at the "first and last name" prompt.

Important: "First and Last name" must be the fully qualified domain name(FQDN).

At the password prompt, enter any password you want.

Note: password **cannot** contain an asterisk(*).

```
Enter keystore password: 123456
What is your first and last name?
[Unknown]: metdaemon.yourcompany.org
What is the name of your organizational unit?
[Unknown]: Company Org. Unit
What is the name of your organization?
[Unknown]: Company Name
What is the name of your City or Locality?
[Unknown]:
What is the name of your State or Province?
[Unknown]:
What is the two-letter country code for this unit?
[Unknown]:
Is CN=metdaemon.yourcompany.org, OU=Company Org. Unit, O=Company Name, L=Unknown
, ST=Unknown, C=Unknown correct?
[no]: y
```

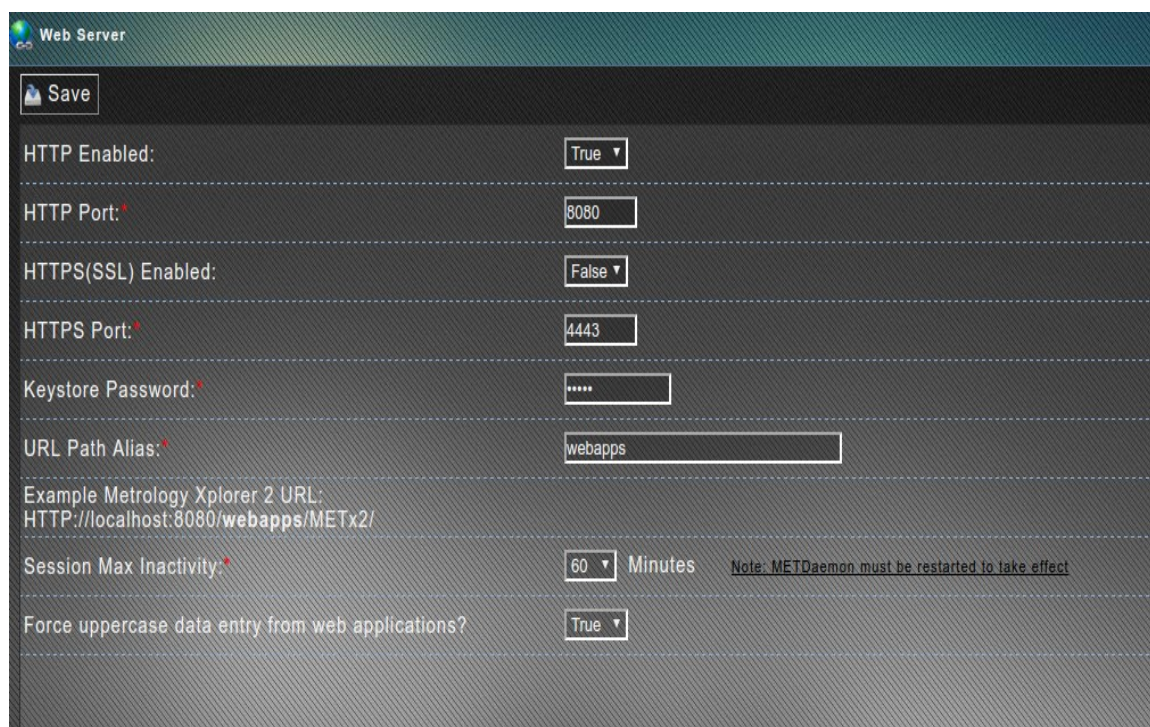
METDaemon - SSL Installation Guide

Build 1.5+

ON TIME SUPPORT, INC.

You now have the minimal requirements to run an SSL connection. However, the certificate you have generated will not be trusted by the browser and the user will be prompted to this effect.

Log in to METDaemon Admin, then go to "Network\Web Server Settings".



Web Server

Save

HTTP Enabled: True ▾

HTTP Port: 8080

HTTPS(SSL) Enabled: False ▾

HTTPS Port: 4443

Keystore Password: *****

URL Path Alias: webapps

Example Metrology Xplorer 2 URL:
HTTP://localhost:8080/webapps/METx2/

Session Max Inactivity: 60 ▾ Minutes Note: METDaemon must be restarted to take effect

Force uppercase data entry from web applications? True ▾

Set "**HTTPS(SSL) Enabled:**" to TRUE.

Set "**Keystore Password:**" to the same password used when creating the keystore.

Click the "Save" button.

Restart the METDaemon service.

You should now be able to access METDaemon Admin, or METx2, as follows:

<https://localhost/webapps/admin/>

or

<https://localhost/webapps/METx2/>

Modify this URL to reflect your system.

The keys and certificates generated in step 1 are sufficient to run an SSL connector. However, the certificate you have generated will not be trusted by the browser and the user will be prompted to this effect.

Once the self signed certificate is operating properly, you will want to generate a certificate signing request(CSR) that will be sent to a certificate authority.

Each CA will have their own instructions which should be followed (look for JSSE, Jetty, or Tomcat sections), but all will involve a step to generate a certificate signing request (CSR).

The following command generates the "metdaemon.csr" file and places it in METDaemon\etc\:

```
jre\bin\keytool.exe -certreq -alias metdaemon -keystore etc\keystore -file etc\metdaemon.csr
```

After sending the CSR to the certificate authority of your choice, they will send back, or make available for download, a zip file containing a certificate chain(several certificates).

These certificates will need to be loaded into the keystore that was originally created using the following command(or a variation thereof).

Each certificate authority may have their own instructions for importing certificates into the keystore(look for JSSE, Jetty, or Tomcat instructions), and usually include more than one certificate that needs to be imported (root certificate, intermediate certificate, site certificate, etc.)

Certificates need to be loaded in a specific order:

Root Cert → Intermediate Cert → Site Cert.

Root Cert:

```
jre\bin\keytool.exe -keystore etc\keystore -import -alias root -file root_cert.crt -trustcacerts
```

Intermediate Cert:

```
jre\bin\keytool.exe -keystore etc\keystore -import -alias intermediate -file intermediate_cert.crt -trustcacerts
```

Site Cert:

```
jre\bin\keytool.exe -keystore etc\keystore -import -alias metdaemon -file site_cert.crt -trustcacerts
```

At this point, all certificates should be installed. Restart the METDaemon service, then try connecting using "https://".

Note: The certificate will only be valid for the Fully Qualified Domain Name used when creating the store.

<https://localhost/webapps/admin>, etc., will not be valid and will result in SSL errors.