

# Mobile Enterprise Gateway (MEG) 2.92 FIPS Setup Guide

## How to enable

Before making changes, stop Cloud Extender (CE) and Mobile Enterprise Gateway (MEG) by running the `stopMobileGateway.bat` located under the default CE install location at `C:\Program Files (x86)\MaaS360\Cloud Extender\`.

To enable FIPS mode for CE and MEG, the following registry key must be set to 3. You can manually set this through Windows regedit or by saving the following code block as a .reg file and executing it on the CE/MEG machine.

### ENABLE\_FIPS\_CE\_AND\_MODULES.reg

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fiberlink\V360]  
"FIPSComplianceMode"=dword:00000003
```

Once FIPS mode is enabled for MEG, the `java.security` file located under the default install directory at `C:\Program Files (x86)\MaaS360\Cloud Extender\Java\jre\lib\security` requires an additional provider and removing another.

The required provider is `com.ibm.crypto.fips.provider.IBMJCEFIPS` which must be added at the top of the list before the `com.ibm.jsse2.IBMJSSEProvider2` provide. Ensure that the provider numbers are updated correctly in order starting at 1.

An example of a correct FIPS compliant `java.security` provider list is as follows:

### java.security - FIPS compliant

```
security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS  
security.provider.2=com.ibm.jsse2.IBMJSSEProvider2  
security.provider.3=com.ibm.crypto.provider.IBMJCE  
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider  
security.provider.5=com.ibm.security.cert.IBMCertPath  
security.provider.6=com.ibm.security.sasl.IBMSASL  
security.provider.7=com.ibm.xml.crypto.IBMXMLCryptoProvider  
security.provider.8=com.ibm.xml.enc.IBMXMLEncProvider  
security.provider.9=com.ibm.security.jgss.mech.spnego.IBMSPNEGO  
security.provider.10=sun.security.provider.Sun
```

Now that the registry and `java.security` have been updated, run the `startMobileGateway.bat` located under the default CE install location at `C:\Program Files (x86)\MaaS360\Cloud Extender\`.

CE and MEG should now be running in FIPS mode. Check the Verification section for verifying FIPS mode was enabled correctly.

## **FIPS Enabled Verification**

### **CE Verification**

To verify that CE is running with FIPS enabled, the following log snippet can be seen in the EMSAgent.log under the default directory located at C:\ProgramData\MaaS360\Cloud Extender\logs.

#### **EMSAgent.log - CE FIPS mode enabled log**

```
[2017-08-29 01:16:34] INFO ThreadID:11240 [SecurityAgentModule::Run] FIPS
140-2 Compliance Mode enabled [Visibility.CSecurityAgentModule:372]
```

If MEG is also FIPS enabled, you will see these logs lines in the EMSAgent.log.

#### **EMSAgent.log - MEG FIPS mode enabled logs**

```
[2017-08-28 23:57:16] DEBUG ThreadID:4604 MEGFipsMode,1
[Visibility.CModuleMgr:3616]
[2017-08-28 23:57:46] INFO ThreadID:4604 [ST0] MEG-SETUP-MONITOR Entering
SetMegFipsModeConfigValue() [Visibility.CCoreAPI:109]
[2017-08-28 23:57:46] INFO ThreadID:4604 [ST0] MEG-SETUP-MONITOR Entering
CEFipsModeIsOn() [Visibility.CCoreAPI:109]
[2017-08-28 23:57:46] INFO ThreadID:4604 [ST0] MEG-SETUP-MONITOR Leaving
CEFipsModeIsOn() with value true [Visibility.CCoreAPI:109]
[2017-08-28 23:57:46] INFO ThreadID:4604 [ST0] MEG-SETUP-MONITOR Leaving
SetMegFipsModeConfigValue with value 1 [Visibility.CCoreAPI:109]
```

### **MEG Verification**

To verify that MEG is running with FIPS enabled, the following log snippets can be seen in the MobileGateway.log under the default directory located at C:\ProgramData\MaaS360\Cloud Extender\logs.

## MEG FIPS mode disabled

```
08-Aug-2017 16:33:56.968 INFO [main] | c.f.m.g.Launcher.main.481 | Running
MaaS360 Enterprise Gateway with args: [-data_dir,
C:\ProgramData\MaaS360\Cloud Extender]
08-Aug-2017 16:33:56.970 INFO [main] | c.f.m.g.Launcher.main.483 | OS FIPS
mode enabled: false
08-Aug-2017 16:33:56.970 INFO [main] | c.f.m.g.Launcher.main.493 | MEG FIPS
mode enabled: false
08-Aug-2017 16:33:56.972 DEBUG [main] | c.f.m.g.PropertiesBase.getProps.122 |
Reading properties file C:\ProgramData\MaaS360\Cloud
Extender/logs/MobileGateway.properties
08-Aug-2017 16:33:56.976 INFO [main] | c.f.m.g.p.GatewayPolicy.<init>.34 |
Creating the GatewayPolicy instance with data dir as:
C:\ProgramData\MaaS360\Cloud Extender
08-Aug-2017 16:33:56.976 DEBUG [main] | c.f.m.g.PropertiesBase.getProps.122 |
Reading properties file C:\ProgramData\MaaS360\Cloud
Extender/logs/MobileGatewayPolicy.properties
08-Aug-2017 16:33:56.978 INFO [main] |
c.f.m.g.u.PACFileUtils.loadJSEngine.82 | Proxy.pac file not in use
08-Aug-2017 16:33:56.978 DEBUG [main] | c.f.m.g.Launcher.initializeSNI.138 |
meg.enable_sni_extension is not defined in the MEGproperties file
08-Aug-2017 16:33:56.978 INFO [main] |
c.f.m.g.u.CertificateHelper.initialize.101 | Loading Gateway certificate from
path: C:/ProgramData/MaaS360/Cloud Extender/Logs/mobilegateway.p12, and Root
certificate from path: C:/ProgramData/MaaS360/Cloud
Extender/Logs/mobilegatewayroot.crt
08-Aug-2017 16:33:56.980 DEBUG [main] |
c.f.m.g.u.CertificateHelper.initialize.111 | Reading from p12 file as FIPS
mode was detected as disabled
08-Aug-2017 16:33:57.580 INFO [main] |
c.f.m.g.u.CertificateHelper.initialize.127 | Successfully loaded Gateway's
certificate and private key
08-Aug-2017 16:33:57.581 INFO [main] |
c.f.m.g.u.CertificateHelper.initialize.140 | Successfully loaded Root
certificate
```

## MEG FIPS mode enabled - First time running with FIPS enabled

```
08-Aug-2017 16:39:47.567 INFO [main] | c.f.m.g.Launcher.main.481 | Running
MaaS360 Enterprise Gateway with args: [-data_dir,
C:\ProgramData\MaaS360\Cloud Extender]
08-Aug-2017 16:39:47.572 INFO [main] | c.f.m.g.Launcher.main.483 | OS FIPS
mode enabled: false
08-Aug-2017 16:39:47.572 INFO [main] | c.f.m.g.Launcher.main.493 | MEG FIPS
mode enabled: true
08-Aug-2017 16:39:47.574 DEBUG [main] | c.f.m.g.PropertiesBase.getProps.122 |
Reading properties file C:\ProgramData\MaaS360\Cloud
Extender/logs/MobileGateway.properties
08-Aug-2017 16:39:47.577 INFO [main] | c.f.m.g.p.GatewayPolicy.<init>.34 |
Creating the GatewayPolicy instance with data dir as:
C:\ProgramData\MaaS360\Cloud Extender
08-Aug-2017 16:39:47.578 DEBUG [main] | c.f.m.g.PropertiesBase.getProps.122 |
Reading properties file C:\ProgramData\MaaS360\Cloud
Extender/logs/MobileGatewayPolicy.properties
08-Aug-2017 16:39:47.579 INFO [main] |
c.f.m.g.u.PACFileUtils.loadJSEngine.82 | Proxy.pac file not in use
08-Aug-2017 16:39:47.580 DEBUG [main] | c.f.m.g.Launcher.initializeSNI.138 |
meg.enable_sni_extension is not defined in the MEGproperties file
08-Aug-2017 16:39:47.580 INFO [main] |
c.f.m.g.u.CertificateHelper.initialize.101 | Loading Gateway certificate from
path: C:/ProgramData/MaaS360/Cloud Extender/Logs/mobilegateway.jks, and Root
certificate from path: C:/ProgramData/MaaS360/Cloud
Extender/Logs/mobilegatewayroot.crt
08-Aug-2017 16:39:47.581 WARN [main] |
c.f.m.g.u.CertificateHelper.initialize.144 | Could not find the mobilegateway
keystore file. If running in FIPS mode for the first time then please wait
while a new keystore is created and MEG is restarted.
08-Aug-2017 16:39:47.581 WARN [main] | WinNTEventsLogger.initialize.146 |
Could not find the mobilegateway keystore file. If running in FIPS mode for
the first time then please wait while a new keystore is created and MEG is
restarted.
08-Aug-2017 16:39:47.583 DEBUG [main] |
c.f.m.g.u.CertificateHelper.initialize.148 |
java.io.FileNotFoundException: C:\ProgramData\MaaS360\Cloud
Extender\Logs\mobilegateway.jks (The system cannot find the file specified.)
    at java.io.FileInputStream.open(FileInputStream.java:212) ~[na:1.8.0-
internal]
    at java.io.FileInputStream.<init>(FileInputStream.java:152) ~[na:1.8.0-
internal]
    at java.io.FileInputStream.<init>(FileInputStream.java:104) ~[na:1.8.0-
internal]
    at
com.fiberlink.meg.gateway.utils.CertificateHelper.initialize(CertificateHelve
r.java:105) ~[MobileGateway.jar:na]
    at com.fiberlink.meg.gateway.Launcher.<init>(Launcher.java:102)
[MobileGateway.jar:na]
    at com.fiberlink.meg.gateway.Launcher.main(Launcher.java:496)
[MobileGateway.jar:na]
```

## MEG FIPS mode enabled - When running for subsequent runs

```
08-Aug-2017 16:37:49.395 INFO [main] | c.f.m.g.Launcher.main.481 | Running
MaaS360 Enterprise Gateway with args: [-data_dir,
C:\ProgramData\MaaS360\Cloud Extender]
08-Aug-2017 16:37:49.398 INFO [main] | c.f.m.g.Launcher.main.483 | OS FIPS
mode enabled: false
08-Aug-2017 16:37:49.398 INFO [main] | c.f.m.g.Launcher.main.493 | MEG FIPS
mode enabled: true
08-Aug-2017 16:37:49.399 DEBUG [main] | c.f.m.g.PropertiesBase.getProps.122 |
Reading properties file C:\ProgramData\MaaS360\Cloud
Extender/logs/MobileGateway.properties
08-Aug-2017 16:37:49.403 INFO [main] | c.f.m.g.p.GatewayPolicy.<init>.34 |
Creating the GatewayPolicy instance with data dir as:
C:\ProgramData\MaaS360\Cloud Extender
08-Aug-2017 16:37:49.403 DEBUG [main] | c.f.m.g.PropertiesBase.getProps.122 |
Reading properties file C:\ProgramData\MaaS360\Cloud
Extender/logs/MobileGatewayPolicy.properties
08-Aug-2017 16:37:49.405 INFO [main] |
c.f.m.g.u.PACFileUtils.loadJSEngine.82 | Proxy.pac file not in use
08-Aug-2017 16:37:49.405 DEBUG [main] | c.f.m.g.Launcher.initializeSNI.138 |
meg.enable_sni_extension is not defined in the MEG properties file
08-Aug-2017 16:37:49.406 INFO [main] |
c.f.m.g.u.CertificateHelper.initialize.101 | Loading Gateway certificate from
path: C:/ProgramData/MaaS360/Cloud Extender/Logs/mobilegateway.jks, and Root
certificate from path: C:/ProgramData/MaaS360/Cloud
Extender/Logs/mobilegatewayroot.crt
08-Aug-2017 16:37:49.411 DEBUG [main] |
c.f.m.g.u.CertificateHelper.initialize.115 | Reading from jks file as FIPS
mode was detected as enabled
08-Aug-2017 16:37:49.481 INFO [main] |
c.f.m.g.u.CertificateHelper.initialize.127 | Successfully loaded Gateway's
certificate and private key
08-Aug-2017 16:37:49.482 INFO [main] |
c.f.m.g.u.CertificateHelper.initialize.140 | Successfully loaded Root
certificate
```

## Additional Verification

When adding a second cluster to MEG in HA mode, there are 2 web services that are affected by FIPS mode, `addCEToCluster` and `getConfiguredGatewayDetails`.

Ensure that in the logs, the `gatewayCertSHA256` parameter is used when in FIPS mode instead of the `gatewayCertMD5` parameter (request URL varies depending on environment that is M1, IQ1).

The following log snippets can be seen in the `EMSAgent.log` under the default directory located at `C:\ProgramData\MaaS360\Cloud Extender\logs` when adding another cluster in FIPS mode.

## `addCEToCluster` - FIPS compliant

```
[2017-08-25 10:46:07] INFO ThreadID:2676 [ST0] AddCEToCluster postData: gatewayCertSHA256=fipscompliantdata [Visibility.CCoreAPI:110]
```

### **getConfiguredGatewaydetails - FIPS compliant**

```
[2017-08-24 00:38:53] INFO ThreadID:9532 [ST0] GetConfiguredGatewayDetails url to get configured gateway details : https://iqlservices.fiberlink.com/device-apis/cloudExtender/1.0/getConfiguredGatewayDetails/123456?gatewayCertSHA256=fipscompliantdata [Visibility.CCoreAPI:109]
```

## **How to disable**

Stop CE and MEG by running the `stopMobileGateway.bat` located under the default CE install location at `C:\Program Files (x86)\MaaS360\Cloud Extender\`.

To disable FIPS mode for CE and MEG, the following registry key must be set to 0. You can manually set this through Windows regedit or by saving the following code block as a .reg file and executing it on the CE/MEG machine.

### **ENABLE\_FIPS\_CE\_AND\_MODULES.reg**

```
Windows Registry Editor Version 5.00
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fiberlink\V360] "FIPSComplianceMode"=dword:00000003
```

Once FIPS mode is disabled for MEG, the `java.security` file located under the default install directory at `C:\Program Files (x86)\MaaS360\Cloud Extender\Java\jre\lib\security` must revert the changes made prior to FIPS mode as a backup. Here is an example of a correct non FIPS compliant `java.security` provider list:

### **java.security - Non FIPS compliant**

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.security.jgss.IBMJGSSProvider
security.provider.4=com.ibm.security.cert.IBMCertPath
security.provider.5=com.ibm.security.sasl.IBMSASL
security.provider.6=com.ibm.xml.crypto.IBMXMLCryptoProvider
security.provider.7=com.ibm.xml.enc.IBMXMLEncProvider
security.provider.8=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
security.provider.9=sun.security.provider.Sun
security.provider.10=org.bouncycastle.jce.provider.BouncyCastleProvider
```

Now that the registry and `java.security` have been updated, run the `startMobileGateway.bat` located under the default CE install location at `C:\Program Files (x86)\MaaS360\Cloud Extender\`.

CE and MEG should now be running in non FIPS mode. Check the Verification section for verifying FIPS mode was disabled correctly.

## **FIPS Disabled Verification**

### **CE Verification**

To verify that CE is running in non FIPS mode, you should see the following log snippet in the EMSAgent.log under the default directory located at C:\ProgramData\MaaS360\Cloud Extender\logs.

#### **EMSAgent.log - CE FIPS mode enabled log**

```
[2017-08-29 01:16:34] INFO ThreadID:11240 [SecurityAgentModule::Run] FIPS
140-2 Compliance Mode disabled [Visibility.CSecurityAgentModule:372]
```

If MEG is also FIPS disabled, you will see these logs lines in the EMSAgent.log.

#### **EMSAgent.log - MEG FIPS mode disabled logs**

```
[2017-09-19 10:17:59] DEBUG ThreadID:16256 MEGFipsMode,0
[Visibility.CModuleMgr:3616]
[2017-09-19 10:18:29] INFO ThreadID:16256 [ST0] MEG-SETUP-MONITOR Entering
SetMegFipsModeConfigValue() [Visibility.CCoreAPI:109]
[2017-09-19 10:18:29] INFO ThreadID:16256 [ST0] MEG-SETUP-MONITOR Entering
CEFipsModeIsOn() [Visibility.CCoreAPI:109]
[2017-09-19 10:18:29] INFO ThreadID:16256 [ST0] MEG-SETUP-MONITOR Leaving
CEFipsModeIsOn() with value false [Visibility.CCoreAPI:109]
[2017-09-19 10:18:29] INFO ThreadID:16256 [ST0] MEG-SETUP-MONITOR Leaving
SetMegFipsModeConfigValue with value 0 [Visibility.CCoreAPI:109]
```

### **MEG Verification**

To verify that MEG is not running in FIPS mode, the following log snippets can be seen in the MobileGateway.log under the default directory located at C:\ProgramData\MaaS360\Cloud Extender\logs.

#### **MEG FIPS mode disabled**

```
08-Aug-2017 16:33:56.968 INFO [main] | c.f.m.g.Launcher.main.481 | Running
MaaS360 Enterprise Gateway with args: [-data_dir,
C:\ProgramData\MaaS360\Cloud Extender]
08-Aug-2017 16:33:56.970 INFO [main] | c.f.m.g.Launcher.main.483 | OS FIPS
mode enabled: false
```

```
08-Aug-2017 16:33:56.970 INFO [main] | c.f.m.g.Launcher.main.493 | MEG FIPS
mode enabled: false
08-Aug-2017 16:33:56.972 DEBUG [main] | c.f.m.g.PropertiesBase.getProps.122 |
Reading properties file C:\ProgramData\MaaS360\Cloud
Extender/logs/MobileGateway.properties
08-Aug-2017 16:33:56.976 INFO [main] | c.f.m.g.p.GatewayPolicy.<init>.34 |
Creating the GatewayPolicy instance with data dir as:
C:\ProgramData\MaaS360\Cloud Extender
08-Aug-2017 16:33:56.976 DEBUG [main] | c.f.m.g.PropertiesBase.getProps.122 |
Reading properties file C:\ProgramData\MaaS360\Cloud
Extender/logs/MobileGatewayPolicy.properties
08-Aug-2017 16:33:56.978 INFO [main] |
c.f.m.g.u.PACFileUtils.loadJSEngine.82 | Proxy.pac file not in use
08-Aug-2017 16:33:56.978 DEBUG [main] | c.f.m.g.Launcher.initializeSNI.138 |
meg.enable_sni_extension is not defined in the MEG properties file
08-Aug-2017 16:33:56.978 INFO [main] |
c.f.m.g.u.CertificateHelper.initialize.101 | Loading Gateway certificate from
path: C:/ProgramData/MaaS360/Cloud Extender/Logs/mobilegateway.p12, and Root
certificate from path: C:/ProgramData/MaaS360/Cloud
Extender/Logs/mobilegatewayroot.crt
08-Aug-2017 16:33:56.980 DEBUG [main] |
c.f.m.g.u.CertificateHelper.initialize.111 | Reading from p12 file as FIPS
mode was detected as disabled
08-Aug-2017 16:33:57.580 INFO [main] |
c.f.m.g.u.CertificateHelper.initialize.127 | Successfully loaded Gateway's
certificate and private key
08-Aug-2017 16:33:57.581 INFO [main] |
c.f.m.g.u.CertificateHelper.initialize.140 | Successfully loaded Root
certificate
```

## **Known Issues / Limitations**

### **Adding another cluster after upgrading from non-FIPS to FIPS**

When MEG is first configured, the MobileGateway certificate is generated and stored at the default location `C:/ProgramData/MaaS360/Cloud Extender/Logs/mobilegateway.p12`. This certificate is generated differently depending on whether or not MEG was set to FIPS mode at the time of generation.

If CE/MEG was not FIPS compliant at the time of generation, then the `mobilegateway.p12` is not FIPS compliant. This behavior is acceptable for Standalone and existing HA clusters. However, adding a second cluster in FIPS mode has issues.

Since the `mobilegateway.p12` was not FIPS compliant at the time of generation, when attempting to join a cluster using the non FIPS compliant `mobilegateway.p12` there will be an error indicating that the join failed.

This is because CE is in FIPS mode and cannot parse the non-FIPS compliant `mobilegateway.p12` certificate. The `ASConfig.log` will show the following error message:



**ASConfig.log - When attempting to join a new cluster when CE is in FIPS mode with a non-FIPS compliant mobilegateway.p12**

```
[2017-08-20 23:03:31] ERROR ThreadID:00004864 [ParseCertificate] Error parsing PKCS#12 file. [.\CertHelper.cpp:736]
```

To work around this issue, the CE/MEG must not be in FIPS mode while joining another cluster. Once joined, FIPS mode can then be enabled on the new cluster.