



Knowledge Base Article ETM57716

Configuring the Enhanced Java Security Policy in ETM[®] System v9.0.3

Synopsis

A means to restrict Java processing to only the processing required by the ETM[®] System has been implemented in ETM System v9.0.3, using special configuration. Use the instructions below to configure this capability.

Configuration Instructions

To configure enhanced Java security, you must modify or replace the Java Security Policy file. Then, in order to use the enhanced security policy file, you must make the changes for the system you are using. Follow the procedures below.

Make sure to save your changes when editing the policy file.

In order for the changes to take effect, the Management Server and Report Server services will need to be restarted.

Replace the Default Policy File with the Enhanced Policy File

In the ETM System installation directory, there is a default Java Security “policy” file that begins with the following line:

```
grant {  
  // Allow everything for now  
  permission java.security.AllPermission;  
};
```

This line must be commented out, and then the network details for your deployment must be specified, replacing the placeholder values.

To use Java’s enhanced security policy, replace (or modify) the default policy file with the enhanced policy file. This file is located at the following path:

Windows systems:

<INSTALL_DIR>\apps\SecureLogix\ETM\scripts\java.security\policy

Linux systems:

/opt/SecureLogix/scripts/java.security/policy

Original policy file:

```
permission java.net.SocketPermission "127.0.0.1:", "accept,connect,resolve";  
permission java.net.SocketPermission "localhost:6990-6993",  
  "listen,accept,connect,resolve";  
permission java.net.SocketPermission "<windows computer name>.<windows
```



```
domain>.local:", "listen,accept,connect,resolve";  
permission java.net.SocketPermission "<LAN IP>:6990-6993",  
"listen,accept,connect,resolve";
```

Policy file with changes:

```
permission java.net.SocketPermission "127.0.0.1:*", "accept,connect,resolve";  
permission java.net.SocketPermission "localhost:6990-6993",  
"listen,accept,connect,resolve"; permission java.net.SocketPermission "My-  
Computer.MyDomain.local:", "listen,accept,connect,resolve"; permission  
java.net.SocketPermission "10.1.2.202:6990-6993",  
"listen,accept,connect,resolve";
```

Modify System Settings

Database Configuration

You must add the following line for the ETM Database if the Database is not on the same system as the Management Server and Report Server, or the services will not start:

```
permission java.net.SocketPermission "<DATABASE IP ADDRESS>:1521",  
"listen,accept,connect,resolve";
```

Example:

```
permission java.net.SocketPermission "10.1.52.99:1521",  
"listen,accept,connect,resolve";
```

ESC Configuration

For every system using the ESC to connect to the Management Server system where the enhanced policy is used, you will need a line like this in the policy file:

```
permission java.net.SocketPermission "<HOST IP>:6990-6993",  
"listen,accept,connect,resolve";
```

Example:

```
permission java.net.SocketPermission "10.1.52.101:6990-6993",  
"listen,accept,connect,resolve";
```

So, the new enhanced policy file will look like this:

```
grant codeBase "file:/C:/apps/SecureLogix/ETM/*" {  
  
permission java.net.SocketPermission "127.0.0.1:*", "accept,connect,resolve";  
  
permission java.net.SocketPermission "localhost:6990-6993",  
"listen,accept,connect,resolve";  
  
permission java.net.SocketPermission "MyComputer.MyDomain.local:",  
"listen,accept,connect,resolve";
```



```
permission java.net.SocketPermission "10.1.2.202:6990-6993",
"listen,accept,connect,resolve";

permission java.net.SocketPermission "10.1.52.99:1521",
"listen,accept,connect,resolve";

permission java.net.SocketPermission "10.1.52.101:6990-6993",
"listen,accept,connect,resolve";
```

Multi-Instance

When using the multi-instance configuration for the Management Server, you will need to add the RMID port which will be used by the sub instance.

For example, here we are using the RMID port of 7990 and will need to add the range to the policy file for **localhost**:

```
permission java.net.SocketPermission "localhost:6990-7993",
"listen,accept,connect,resolve";
```

Make sure to save your changes when editing the policy file.

In order for the changes to take effect, the Management Server and Report Server services will need to be restarted.

LINUX Systems

The following changes must be made to the default policy file for Linux systems.

1. Change this:

```
grant codeBase "file:/opt/SecureLogix/ETM/*" {

permission java.net.SocketPermission "127.0.0.1:*", "accept,connect,resolve";

permission java.net.SocketPermission "localhost:6990-6993",
"listen,accept,connect,resolve";

permission java.net.SocketPermission "5298etm:*",
"listen,accept,connect,resolve";

permission java.net.SocketPermission "10.1.52.98:6990-6993",
"listen,accept,connect,resolve";

permission java.net.SocketPermission "10.1.52.92:1521",
"listen,accept,connect,resolve"; I changed the line 34 in policy from this:

permission java.io.FilePermission "C:/apps/SecureLogix/ETM/-",
"read,write,delete";
```



To this:

```
permission java.io.FilePermission "/opt/SecureLogix/ETM/-",  
"read,write,delete";
```

2. Change lines 61-62 in policy from this:

```
grant codeBase  
"file:/C:/apps/SecureLogix/ETM/JRE/jre8/lib/ext/sunjce_provider.jar" {  
permission java.io.FilePermission  
"C:/apps/SecureLogix/ETM/JRE/jre8/lib/ext/sunjce_provider.jar", "read";
```

To this:

```
grant codeBase  
"file:/opt/SecureLogix/ETM/JRE/jre/lib/ext/sunjce_provider.jar" {  
permission java.io.FilePermission  
"/opt/SecureLogix/ETM/JRE/jre/lib/ext/sunjce_provider.jar", "read";
```

3. Ensure that the **ETMReportserver.cfg** file has the following:

```
-C-Dorg.owasp.esapi.resources=/opt/SecureLogix/ETM
```

Updated Windows Java Security Policy File

```
// https://bugs.java.com/bugdatabase/view_bug.do?bug_id=JDK-8229532  
//  
https://stackoverflow.com/questions/57433655/classnotfoundexception-  
issued-by-urlclassloader-when-the-security-manager-is-ena  
  
// https://community.oracle.com/tech/developers/discussion/91474/jce-  
javacryptographicextension-javavm  
  
//grant {  
    // Allow everything for now  
    //permission java.security.AllPermission;  
//};  
  
grant codeBase "file:/C:/apps/SecureLogix/ETM/*" {  
  
    permission java.net.SocketPermission "127.0.0.1:*",  
"accept,connect,resolve";  
    permission java.net.SocketPermission "localhost:6990-6993",  
"listen,accept,connect,resolve";  
    permission java.net.SocketPermission "<windows computer  
name>.<windows domain>.local:*", "listen,accept,connect,resolve";  
    permission java.net.SocketPermission "<LAN IP>:6990-6993",  
"listen,accept,connect,resolve";
```



```
permission java.util.PropertyPermission "user.dir", "read";
permission java.util.PropertyPermission "user.home", "read";
permission java.util.PropertyPermission "LicenseFilename",
"read";
    permission java.util.PropertyPermission "HostId", "read";
    permission java.util.PropertyPermission "InstanceID", "read";
    permission java.util.PropertyPermission "slc.ps_loc", "write";
    permission java.util.PropertyPermission
"org.owasp.esapi.SecurityConfiguration", "read";
    permission java.util.PropertyPermission
"org.owasp.esapi.logSpecial.discard", "read";
    permission java.util.PropertyPermission
"org.owasp.esapi.resources", "read";
    permission java.util.PropertyPermission "*", "read,write";
    permission java.util.PropertyPermission
"org.owasp.esapi.opsteam", "read";

    permission java.util.logging.LoggingPermission "control";

    permission java.io.FilePermission ".", "read";
    permission java.io.FilePermission "C:/apps/SecureLogix/ETM/-",
"read,write,delete";

    permission java.lang.management.ManagementPermission "monitor";

    permission java.lang.reflect.ReflectPermission
"suppressAccessChecks";

    permission java.lang.RuntimePermission "setFactory";
    permission java.lang.RuntimePermission "getClassLoader";
    permission java.lang.RuntimePermission "setContextClassLoader";
    permission java.lang.RuntimePermission "getenv.*";
    permission java.lang.RuntimePermission "getProtectionDomain";
    permission java.lang.RuntimePermission "accessDeclaredMembers";
    permission java.lang.RuntimePermission
"accessClassInPackage.sun.reflect";
    permission java.lang.RuntimePermission "loadLibrary.sunec";
    permission java.lang.RuntimePermission "loadLibrary.sunmscapi";
    permission java.lang.RuntimePermission "loadLibrary.twms";
    permission java.lang.RuntimePermission
"accessClassInPackage.sun.util.calendar";

    permission java.lang.management.ManagementPermission "control";

    permission javax.management.MBeanTrustPermission "register";
    permission javax.management.MBeanServerPermission
"createMBeanServer";
    permission javax.management.MBeanPermission "*", "queryNames";
    permission javax.management.MBeanPermission "*",
"registerMBean,unregisterMBean";
```



```
        permission java.security.SecurityPermission
"putProviderProperty.SunJCE";
};

grant codeBase
"file:/C:/apps/SecureLogix/ETM/JRE/jre8/lib/ext/sunjce_provider.jar" {
    permission java.io.FilePermission
"C:/apps/SecureLogix/ETM/JRE/jre8/lib/ext/sunjce_provider.jar",
"read";
    permission java.lang.RuntimePermission "getProtectionDomain";
    permission java.security.SecurityPermission
"putProviderProperty.SunJCE";
};
```

Updated Linux Java Security Policy File

```
// https://bugs.java.com/bugdatabase/view_bug.do?bug_id=JDK-8229532
//
https://stackoverflow.com/questions/57433655/classnotfoundexception-
issued-by-urlclassloader-when-the-security-manager-is-ena

// https://community.oracle.com/tech/developers/discussion/91474/jce-
javacryptographicextension-javavm

//grant {
//    // Allow everything for now
//    //permission java.security.AllPermission;
//};

grant codeBase "file:/opt/SecureLogix/ETM/*" {

    permission java.net.SocketPermission "127.0.0.1:*",
"accept,connect,resolve";
    permission java.net.SocketPermission "localhost:6990-6993",
"listen,accept,connect,resolve";
    permission java.net.SocketPermission "<Linux hostname>:*",
"listen,accept,connect,resolve";
    permission java.net.SocketPermission "<MS IPADDR>:*",
"listen,accept,connect,resolve";
    permission java.net.SocketPermission "<Database IPADDR>:*",
"listen,accept,connect,resolve";

    permission java.util.PropertyPermission "user.dir", "read";
    permission java.util.PropertyPermission "user.home", "read";
```



```
    permission java.util.PropertyPermission "LicenseFilename",
"read";
    permission java.util.PropertyPermission "HostId", "read";
    permission java.util.PropertyPermission "InstanceID", "read";
    permission java.util.PropertyPermission "slc.ps_loc", "write";
    permission java.util.PropertyPermission
"org.owasp.esapi.SecurityConfiguration", "read";
    permission java.util.PropertyPermission
"org.owasp.esapi.logSpecial.discard", "read";
    permission java.util.PropertyPermission
"org.owasp.esapi.resources", "read";
    permission java.util.PropertyPermission "*", "read,write";
    permission java.util.PropertyPermission
"org.owasp.esapi.opsteam", "read";

    permission java.util.logging.LoggingPermission "control";

    permission java.io.FilePermission ".", "read";
    permission java.io.FilePermission "/opt/SecureLogix/ETM/-",
"read,write,delete";

    permission java.lang.management.ManagementPermission "monitor";

    permission java.lang.reflect.ReflectPermission
"suppressAccessChecks";

    permission java.lang.RuntimePermission "setFactory";
    permission java.lang.RuntimePermission "getClassLoader";
    permission java.lang.RuntimePermission "setContextClassLoader";
    permission java.lang.RuntimePermission "getenv.*";
    permission java.lang.RuntimePermission "getProtectionDomain";
    permission java.lang.RuntimePermission "accessDeclaredMembers";
    permission java.lang.RuntimePermission
"accessClassInPackage.sun.reflect";
    permission java.lang.RuntimePermission "loadLibrary.sunec";
    permission java.lang.RuntimePermission "loadLibrary.sunmescapi";
    permission java.lang.RuntimePermission "loadLibrary.twms";

    permission java.lang.management.ManagementPermission "control";

    permission javax.management.MBeanTrustPermission "register";
    permission javax.management.MBeanServerPermission
"createMBeanServer";
    permission javax.management.MBeanPermission "*", "queryNames";
    permission javax.management.MBeanPermission "*",
"registerMBean,unregisterMBean";

    permission java.security.SecurityPermission
"putProviderProperty.SunJCE";
```



```
        permission java.lang.RuntimePermission
"accessClassInPackage.sun.util.calendar";
};

grant codeBase
"file:/opt/SecureLogix/ETM/JRE/jre/lib/ext/sunjce_provider.jar" {
    permission java.io.FilePermission
"/opt/SecureLogix/ETM/JRE/jre/lib/ext/sunjce_provider.jar", "read";
    permission java.lang.RuntimePermission "getProtectionDomain";
    permission java.security.SecurityPermission
"putProviderProperty.SunJCE";
};
```

Last Update: 4/5/2023



SecureLogix Corporation

13750 San Pedro, Suite 820 • San Antonio, Texas 78232
(210) 402-9669 • www.securelogix.com

Support (877) SLC-4HELP • EMAIL support@securelogix.com • support.securelogix.com

ETM, We See Your Voice, SecureLogix, SecureLogix Corporation, and the SecureLogix Emblem are registered trademarks and registered service marks of SecureLogix Corporation in the U.S.A. and other countries. PolicyGuru is a registered trademark of SecureLogix Corporation in the U.S.A. Orchestra One, Call Secure, Call Defense, Contact, Reputation Defense, TrueCall, and VOX are trademarks or trademarks and service marks of SecureLogix Corporation in the U.S.A. All other trademarks mentioned herein are believed to be trademarks of their respective owners.

© Copyright 2023 SecureLogix Corporation. All Rights Reserved. SecureLogix technologies are protected by one or more of the following patents: US 11,349,987 B2 and US 11,356,551 B2. U.S. Patent Pending.