Application Note:
Accessing web devices running Unsigned or Self-signed Java applets (from Java 7 update 51)

Starting with Java 7 Update 51, Oracle has enhanced their Java security model to make user systems less vulnerable to external exploits.

The new version of Java does not allow users to run applications that are not signed, Self signed (not signed by trusted authority) or applications that are missing permission attributes.

It is likely that older Java applets are not compliant with the security guide-lines implemented in Java 7 Update 51

This guide explains about the issue, and possible work-arounds.

Version: 1.0, January 2014

secomea

Table of Contents

1. General Consequence to the to the Secomea solution

The Secomea solution is NOT based on Java.

The GateManager Portal, SiteManager, LinkManager or LinkManager Mobile will not be affected by this security update from Oracle.

2. LOCAL access to Java enabled Web devices

The security add-on will affect 3.part products like a PLC with a build in WEB server that is using a Java applet that is not signed or self signed – this will usually result in this error:
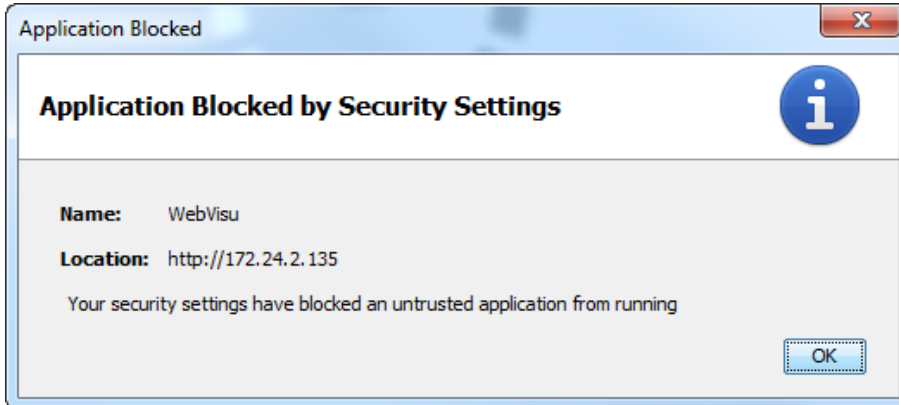
The following options exist for resolving this issue:

1) Signing the Java applet.

2) Set Java Security Level to Medium (Temporary solution!)

3) Add the device IP to the Exception list

4) Downgrade Java to Update 45 (Not recommended!)

2.1. OPTION 1, Signing the Java applet

You will need to contact the vendor of the device for a software update containing the Java applet in a signed version.

If that does not exist, it is in yours and the vendors to let them know about the application being blocked. Refer to this link:
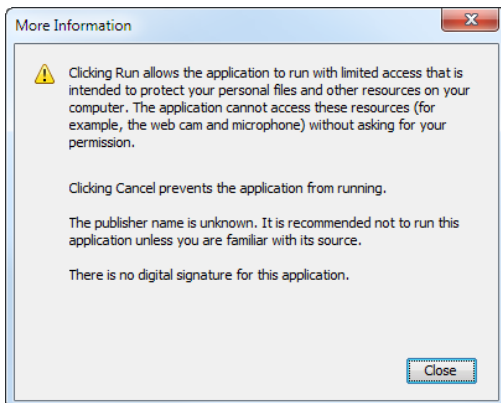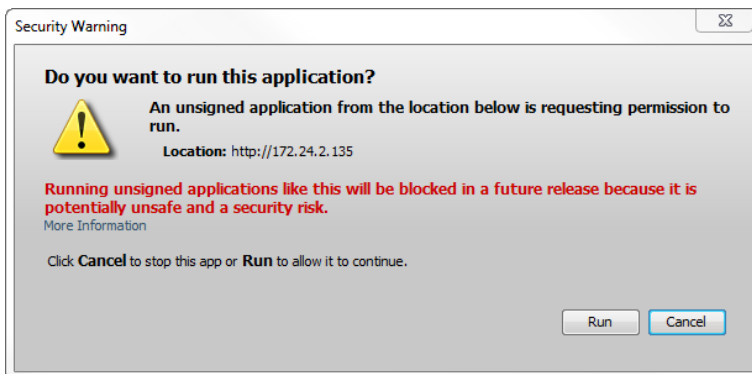
http://www.java.com/en/download/help/java_blocked.xml

2.2. OPTION 2, Adjusting the Java Security Level to Medium
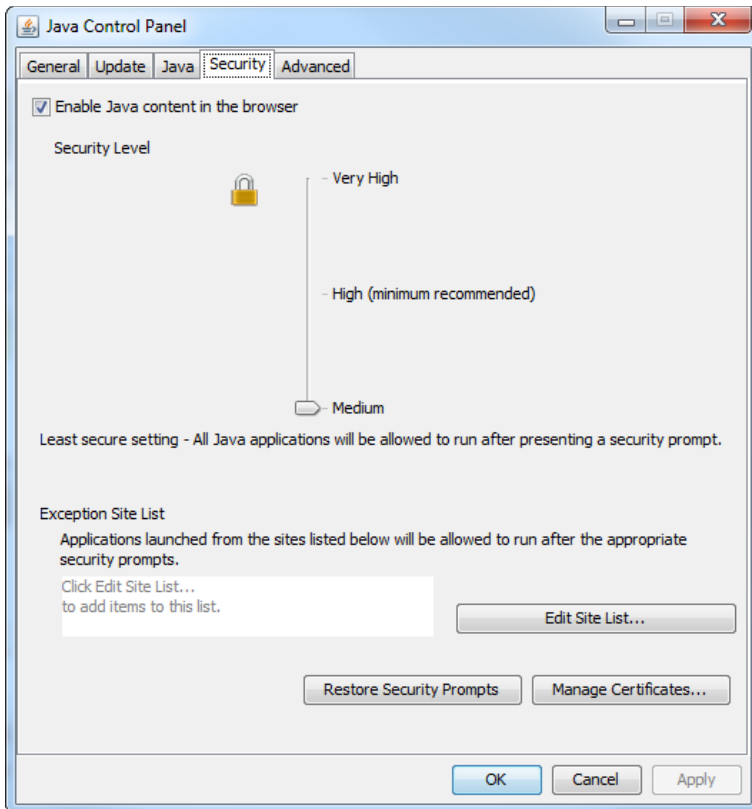
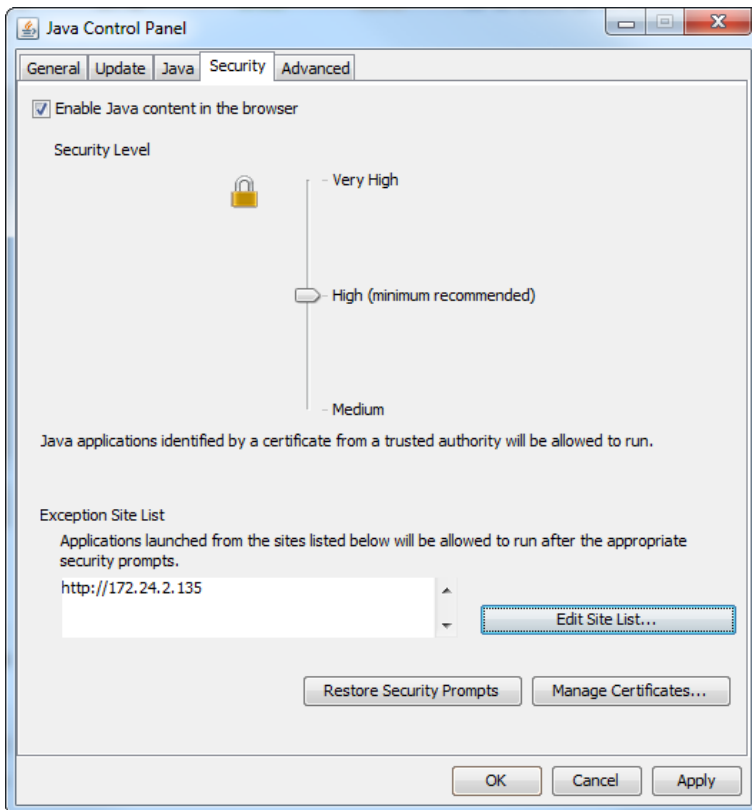If Security is set to Medium, you will get a warning, but can **Run** the application.

As the warning indicates, this may not be recommended as a permanent solution. Oracle warns that this may be blocked in a future Java update.
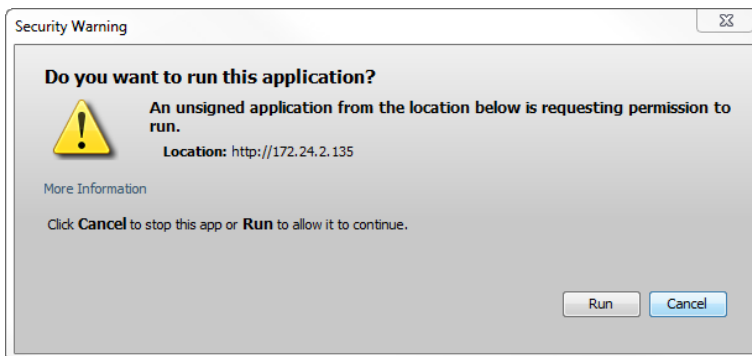
secomea

2.3. OPTION 3, Adding the device IP to the Exception list

For details refer to:

http://docs.oracle.com/javase/7/docs/technotes/guides/jweb/exception_site_list.html

If Security is High and the IP address (172.24.2.135) is added to the Exception Site List, you will still get a warning prompt and can press Run.

secomea

3. REMOTE access to Java enabled Web devices

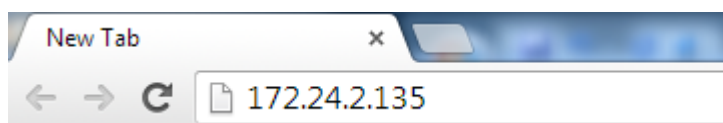## 3.1. Access from LinkManager after device Connect

Prerequisite: *The device IP must be accessible as if you Windows PC was Locally connected to it, ref. one of the three OPTIONS described above.*

Connecting to a device using LinkManager and subsequent using the Globe icon in the Connected window, will launch the Java applet the exact same way as if your PC was locally attached to the network of the device.

When connected either click the Globe icon

Or type the IP address of the device in your web browser address bar:

3.2. Access from LinkManager before device Connect

Prerequisite: *The Java applet must be signed ref. OPTION 1, or Security level must be decreased ref. OPTION 2.*

The LinkManager allow for connecting to web enabled devices without making a full connection to the device. This method uses a dynamic port number that cannot be added to the Java exception list.

secomea
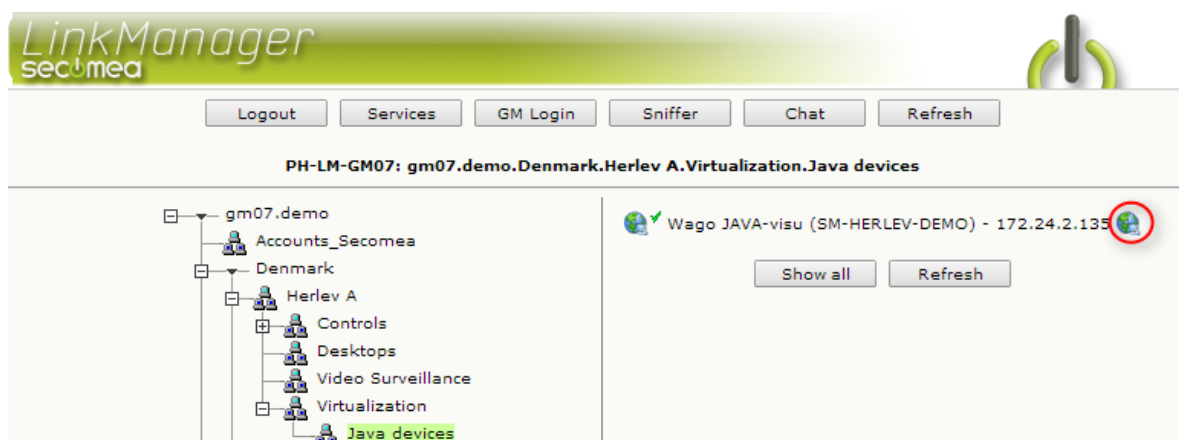
3.3. Access from LinkManager Mobile

Prerequisite: *The Java applet must be signed ref. OPTION 1, or Security level must be decreased ref. OPTION 2.*

The LinkManager Mobile uses a dynamic port number that cannot be added to the Java exception list.
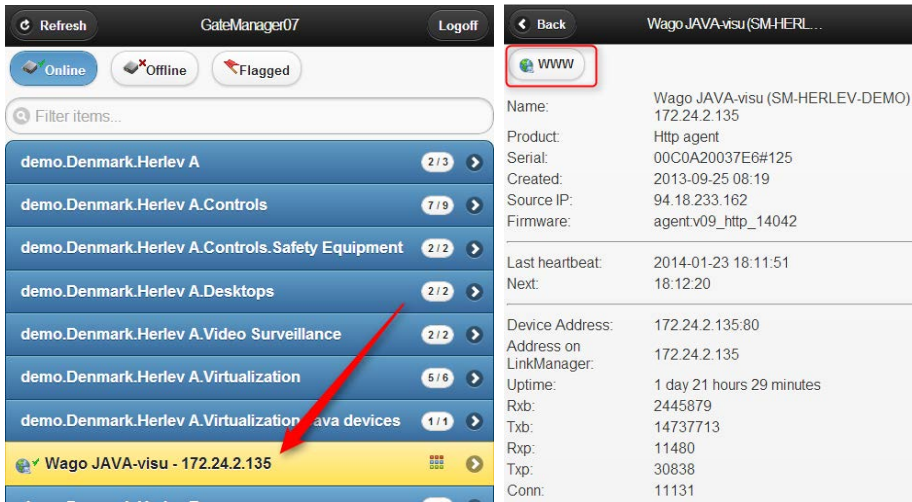
secomea

Notices

Publication and copyright

Trademarks

SiteManager™, LinkManager™ and GateManager™ are trademarks of Secomea A/S. Other trademarks are the property of their respective owners.

Disclaimer

secomea