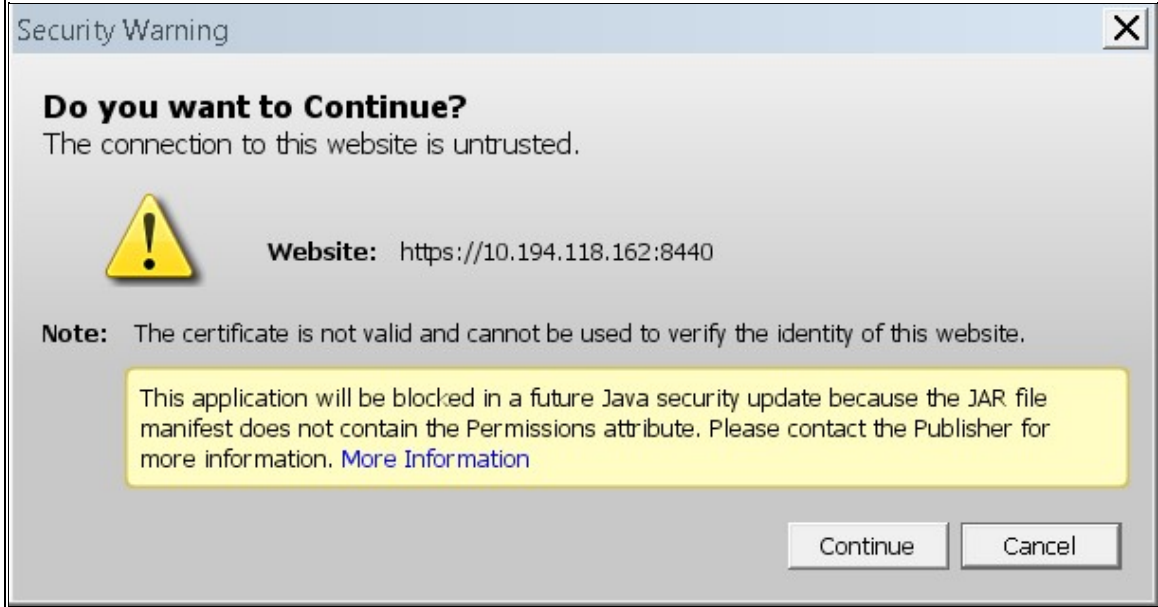
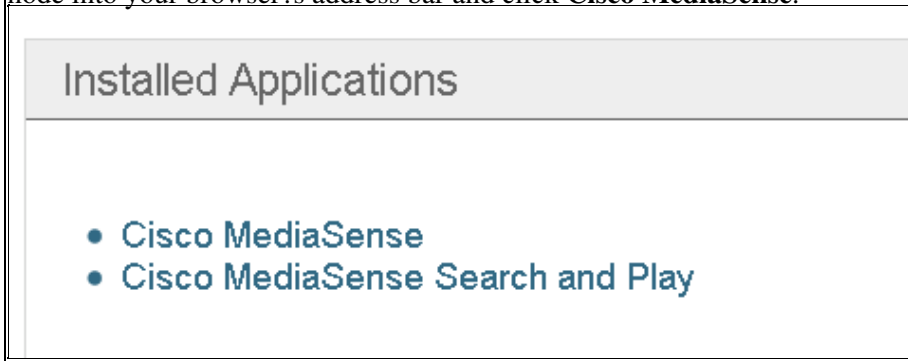


Search and Play application users encounter security warning before each playback

<p>Problem Summary</p>	<p>Users are presented with a pop-up warning every time the Search and Play Java application is executed (whenever they attempt to play a recording).</p>
<p>Error Message</p>	<p>Users see a pop-up similar to this one</p> 
<p>Possible Cause</p>	<p>The MediaSense media player is a downloadable Java application. Since it does not actually run as part of browser executable, it is subject to the security requirements of the Java Virtual Machine (JVM) installed on the user's computer (rather than those of the browser). Any security warnings that the browser user has acknowledged and accepted need to be acknowledged and accepted again with respect to the JVM.</p> <p>Due to recent security enhancements in Java, users must accept a pop-up warning every time the Java application is executed.</p>
<p>Recommended Action</p>	<p>Follow this procedure on each client desktop where the Search and Play application is executed.</p> <p>1. Download the MediaSense Site Certificate. Enter the hostname or IP address of your MediaSense primary node into your browser's address bar and click Cisco MediaSense.</p>  <p>You may be asked to accept a security warning.</p> <p>2. Go to the upper right corner of the screen and select Cisco Unified OS Administration and click Go.</p>

Navigation

3. On the OS Administration page, select **Security -> Certificate Management**.

4. Click **Find**.

Certificate Name	Certificate Type	.PEM File	.DER File	Description
tomcat	certs	tomcat.pem	tomcat.der	Self-signed certificate generated by system
ipsec	certs	ipsec.pem	ipsec.der	Self-signed certificate generated by system
tomcat-trust	trust-certs	VeriSign Class 3 Secure Server CA -	VeriSign Class 3 Secure Server CA -	Call Home Server

5. Click on the tomcat.pem link.

The screenshot displays the Cisco Unified Operating System Administration web interface. The top navigation bar includes the Cisco logo, the title "Cisco Unified Operating System Administration", and the subtitle "For Cisco Unified Communications Solutions". The user is logged in as "admin". The main menu shows "Show", "Settings", "Security", "Software Upgrades", "Services", and "Help". The current page is "Certificate Configuration", with a "Related Links" section containing "Back To Find/List".

Under "Certificate Configuration", there are three buttons: "Regenerate", "Download", and "Generate CSR". Below this is a "Status" section showing "Status: Ready". The "Certificate Settings" section lists the following details:

- File Name: tomcat.pem
- Certificate Name: tomcat
- Certificate Type: certs
- Certificate Group: product-cpi
- Description: Self-signed certificate generated by system

The "Certificate File Data" section shows the following information:

```

[
Version: V3
Serial Number: 166556129613405032830167051369559802784
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: L=seattle, ST=wa, CN=uc-tm-lab2.disco.com, OU=cabbau, O=bu, C=US
Validity From: Sun Dec 08 11:18:26 PST 2013
To: Fri Dec 07 11:18:25 PST 2018
]

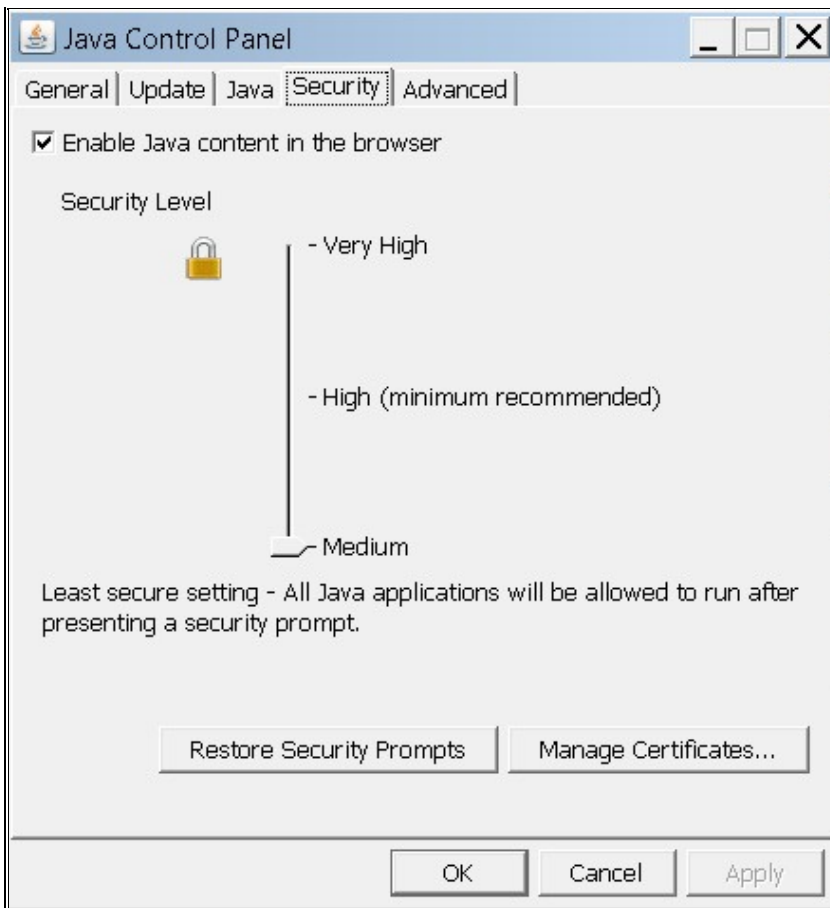
```

6. Click the **Download** button and save the file to a location on your disk. (You can also copy this tomcat.pem file to a USB key or a network share and use it when you complete the remainder of this procedure for each desktop client.)

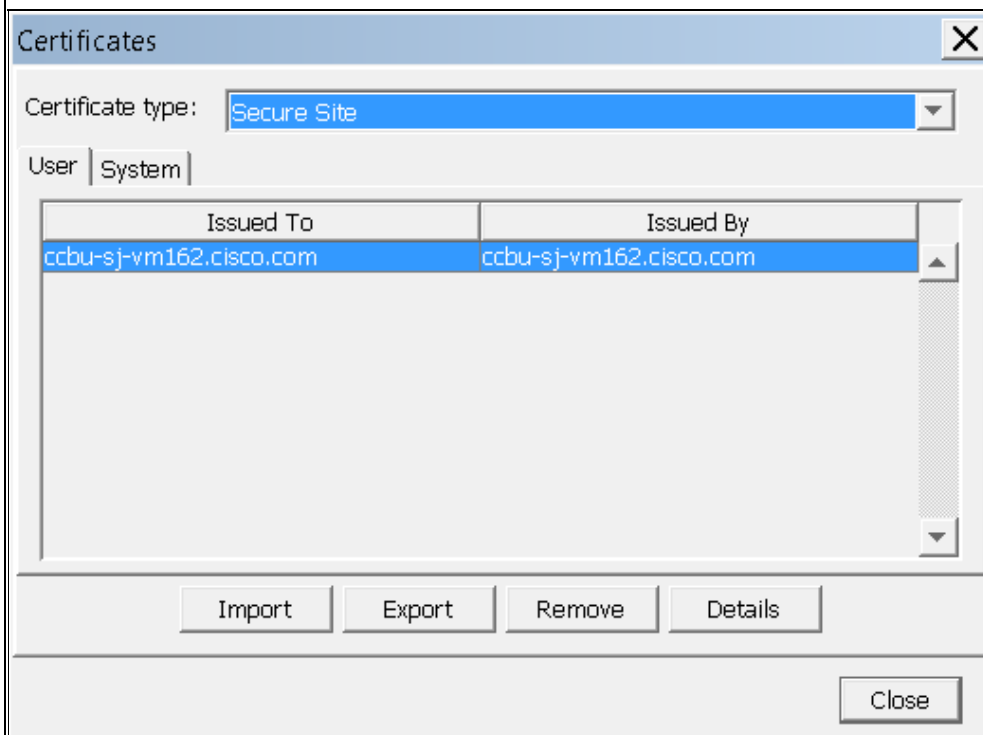
7. Import the site certificate into Java by finding and opening the Java control panel on your client system.

The screenshot shows the Windows Control Panel window titled "java - Control Panel". The address bar indicates the location is "Control Panel" and the search term is "java". The main content area displays the "Java (32-bit)" control panel icon, which includes a Java logo and the text "Java (32-bit)". Below the icon is a search prompt: "Search Windows Help and Support for 'java'".

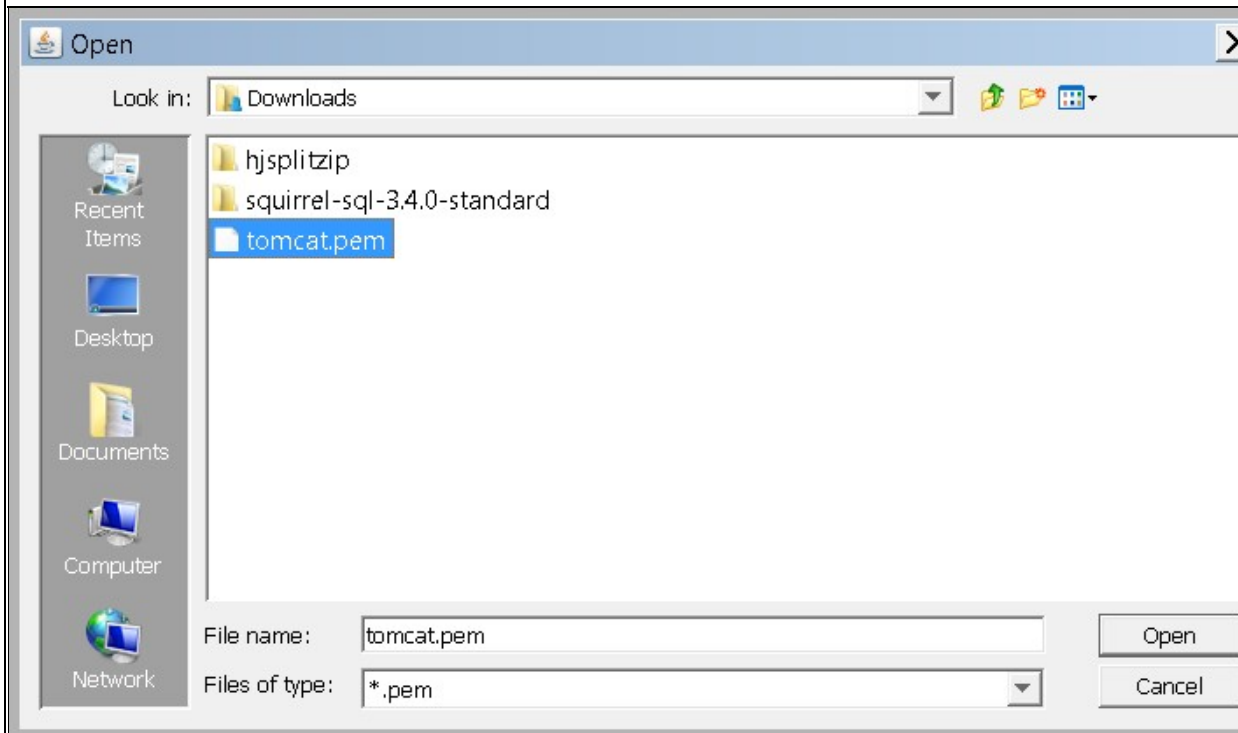
8. On the Security tab, click **Manage Certificates**.



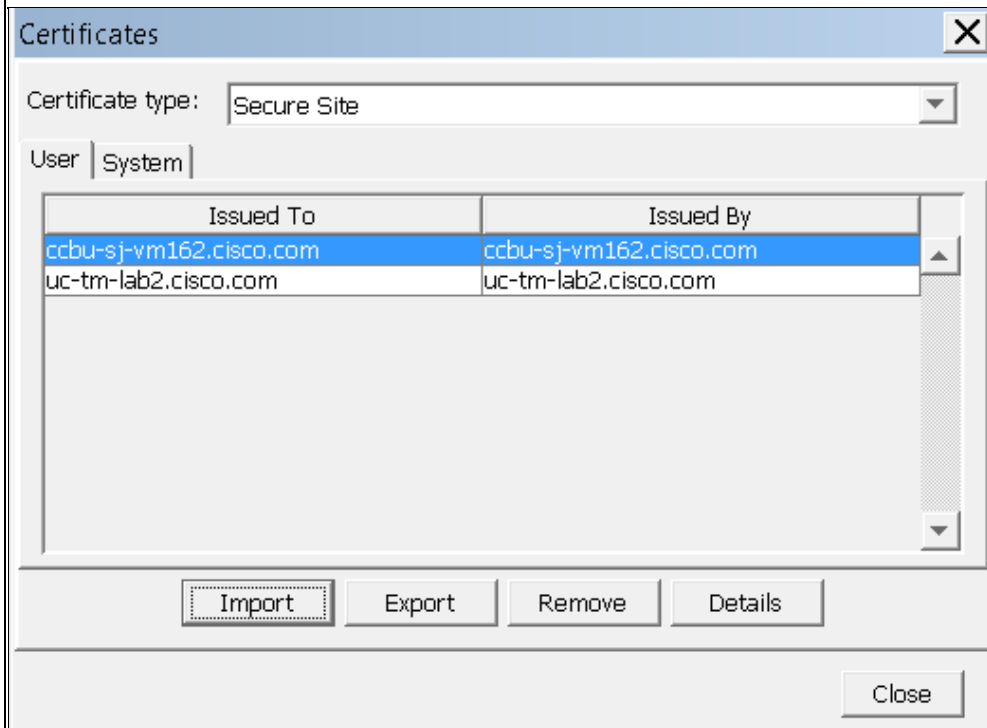
9. For Certificate Type, select **Secure Site**.



10. Click **Import** and find the tomcat .pem file that you downloaded previously. Select it and click **Open**



You see your MediaSense node hostname in the list.

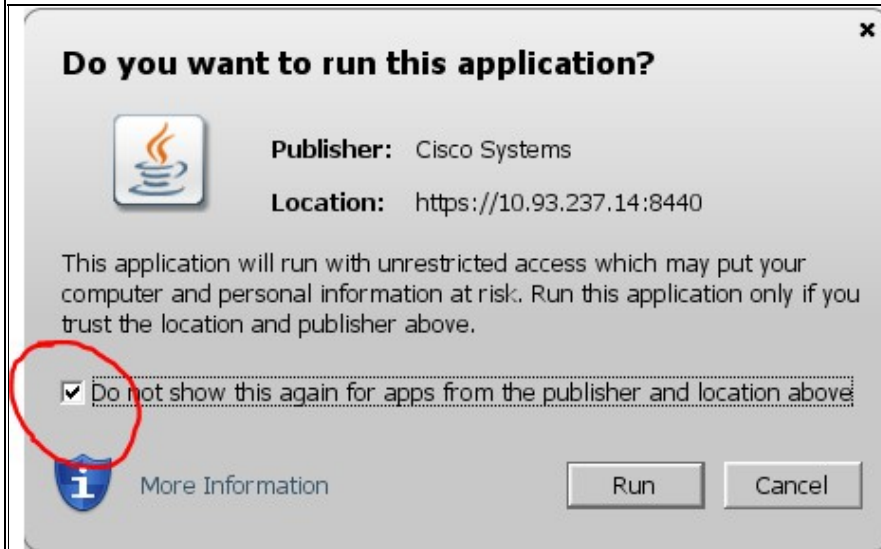


Click **Close**.

11. Return to the MediaSense landing page and select **Cisco MediaSense Search and Play**. Sign in using your API user credentials.

12. Find a recording and click the Play button.

13. If you see this pop-up



Check the box indicated and click **Run**.

If you see this pop-up



Click **Run with the latest version**.

14. Close and re-open the media player, and then play the video again with no security warnings.

Release	All releases.
Associated CDETS #	None