

Dear mSuite customer;

**Warning: CommonTime Evaluation Certificate (2007) - imminent expiry**

If you are still using the CommonTime Evaluation Certificate (2007), you need to take prompt action to avoid loss of service.

The CommonTime Personal and Root certificates are due to expire soon - on the following dates:

Personal Certificate (CommonTimeEval2007.pfx) - Expiry date: January 8<sup>th</sup>, 2008

Root Certificate (CommonTimeCA.cer) - Expiry date: January 30<sup>th</sup>, 2008

CommonTime supplies these certificates to enable you to evaluate mSuite without needing to create your own certificate. They are not recommended for a production environment because everyone has the same certificate and this leaves you vulnerable to 'man in the middle' attacks.

This would be a good opportunity to transition to your own certificate. There are KnowledgeBase articles on the CommonTime website (web.commontime.com) outlining the type of certificate you require and how to create one.

If this is not possible or you are still evaluating, you will need to install and apply a new CommonTime Evaluation certificate both on the server and on the mobile devices. Please follow the steps listed below:

## STEP 1.

Please download the following two files to your mSuite server and place them in your mSuite program folder (by default, this is C:\Program Files\CommonTime\mSuite).

Root Certificate for device:

<http://hosting.commontime.com/downloads/certificate/CommontimeCA.cer>

Personal Certificate for server:

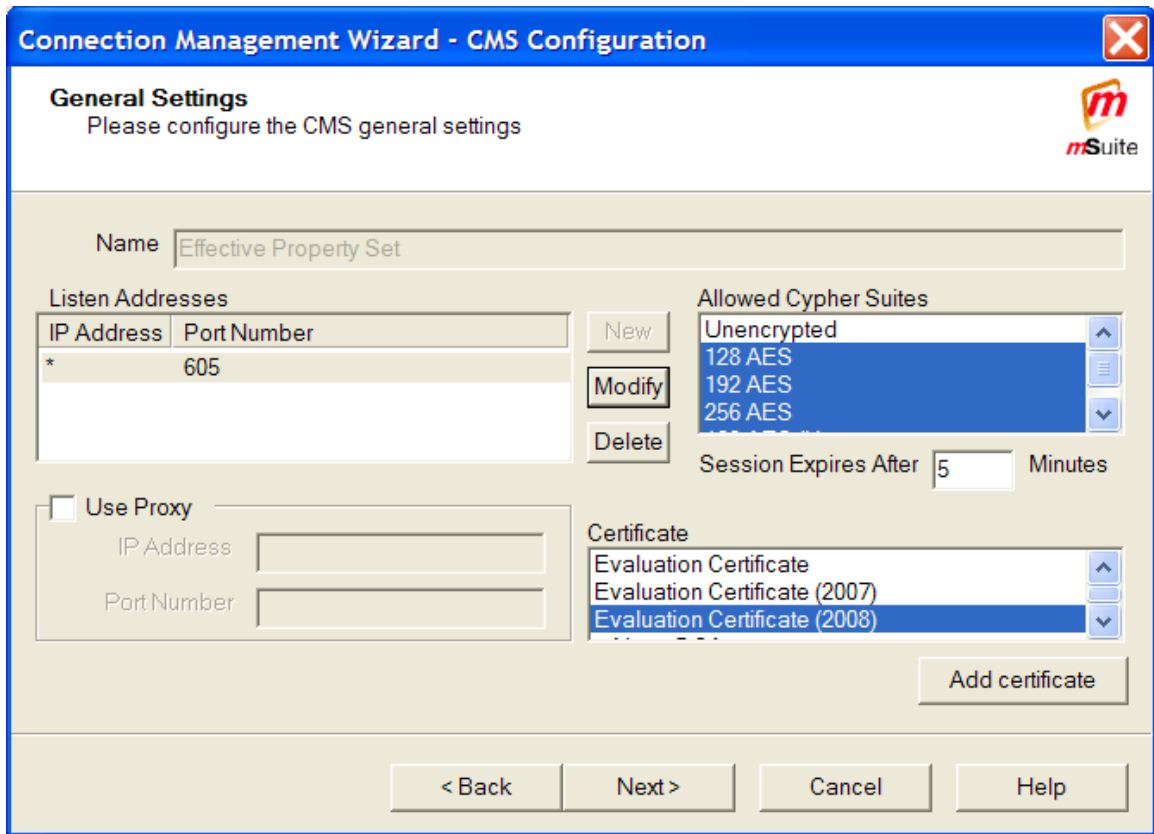
<http://hosting.commontime.com/downloads/certificate/CommontimeEval2008.pfx>

## STEP 2.

You will need to install and activate the new server certificate before it expires on **January 8<sup>th</sup>, 2008**.

- a) Go to the **All Servers** view
- b) Double click on the server that runs the Connection Management Service (CMS)
- c) Go to the **Connection Management** tab and run the first of the two wizards on that page (the one to the right of **Default CMS Template**)
- d) On the **General Settings** page, click the **Add certificate** button (below the Certificates panel).
- e) Browse to the **CommonTimeEval2008.pfx** certificate, select it and click **Open**.
- f) Enter the password which is **Commontime** (it is case sensitive!) and click **OK**.
- g) In the **Certificate** panel, select **Evaluation Certificate (2008)**.

If Evaluation Certificate (2008) does not appear in the Certificate panel or, when you select it, you see the warning message **\*\* The Selected certificate does not exist in server... \*\***, repeat steps d), e) and f) above.



- h) Click **Next** to the end of the wizard and then click **Finish**. Finally, go to **Monitoring > Status > [servername]** and right click on **Connection Manager Server** and click **Restart**.

The new server certificate is now active and you can verify this by checking the configuration information printed at startup in the CMS log. To do this, go the CdzConnMgr subfolder of the mSuite program folder and open the log file for today. You should see log lines similar to these:

```

2007-12-03 18:36:57 info app : mCenter database is v2.8
2007-12-03 18:36:57 trace app : connection manager configuration:
2007-12-03 18:36:57 trace app : ip address = *
2007-12-03 18:36:57 trace app : port = 605
2007-12-03 18:36:57 trace app : session-expiry = 5
2007-12-03 18:36:57 trace app : certificate = Evaluation Certificate (2008)
2007-12-03 18:36:57 trace app : suites = aes-128, aes-192, aes-256, aes-128 (k)
2007-12-03 18:36:57 trace app : mnotes-servers = MYSERVER
2007-12-03 18:36:57 trace app : cap-servers = MYSERVER
2007-12-03 18:36:57 trace app : auth-servers = MYSERVER
2007-12-03 18:36:57 trace app : chat-servers = MYSERVER

```

In particular, the 'certificate' should now show as **"Evaluation Certificate (2008)"**.

## STEP 3.

For the mobile devices, you need to take the following actions before **January 30<sup>th</sup>, 2008**.

### **Palm OS (Garnet) devices.**

No action required. Once the new server certificate has been activated, the first time a client needs to (re)authenticate, the user will be asked to accept a new certificate (from the server).

### **All other device types (includes all Windows Mobile plus Symbian S80 & S60-3 devices)**

You will need to install the new client root certificate (CommonTimeCA.cer) on the device. There are several ways of doing this:

1. **(Windows Mobile only)** If you have mControl licenses and have already upgraded your mSuite server to version 4.3.13, you should now have the 4.3.13 client packages in your mSuite database. If so, you can deploy the 4.3.13 version of the client software to the device using mControl. Version 4.3.13 of the Framework client software includes the new root certificate for Windows Mobile devices. (Version 4.3.13 of mSuite is expected to be available towards the end of December 2007.)

2. **(Windows Mobile only)** If you are not in a position to install/deploy mSuite 4.3.13, you can add the new root certificate (.cer file) into your existing Framework package and deploy it:

a) via **mControl**: over the air or via the cradle – wait for the next device management session to occur (default, once a day) or, force it to occur on the Next Connection using by right clicking the user or group and using **All Tasks > Deployment > Schedule Deployment**

b) via a **Device Package**: use **All Tasks > Deployment > Generate Device Package** to build a new device package, then copy the two package files (.bin and .exe) to same location on the mobile device and execute the .exe.

For detailed information about how to add the new root certificate (.cer file) into your existing Framework package, please read the CommonTime KnowledgeBase article at:

[http://web.commontime.com/Support/KnowledgeBase/tabid/136/606\\_catID/1/606\\_artID/7/Default.aspx](http://web.commontime.com/Support/KnowledgeBase/tabid/136/606_catID/1/606_artID/7/Default.aspx)

**IMPORTANT:** Please note that, before you add the new root certificate (.cer file) to the Framework package, you will need to delete the existing root certificate from the package. This will not affect the root certificates on the mobile device.

3. **(Windows Mobile & Symbian)** Send the root certificate (on its own) to the user as an email attachment which the user can download to the device and execute on the device.

4. **(Windows Mobile & Symbian)** Instruct the user to run the internet browser on their mobile device and go to:

- for Symbian devices: <http://symbiancert.commontime.com>

- for Windows Mobile devices: <http://wmcert.commontime.com>

then follow the on-screen prompts.