Harmonia Install Guide (using the installer)

Pre-Install System Requirements

* 1. Hardware Requirements
     1. Hardware Requirements for the Harmonia Server
        + At least 1 GHz Pentium CPU (at least 2GHz recommended).
        + Minimum 256 MB of RAM (512 MB recommended).
        + A hard disk partition with enough space to accommodate the Harmonia Server code - approx. 150 KB.
        + Adequate space in the Active Directory for Harmonia data.
        + VGA or higher-resolution monitor.
        + Keyboard.
        + Mouse.
        + Network adapter.
     2. Hardware Requirements for the Target Systems
        + At least 400 MHz CPU.
        + Minimum 128 MB of RAM.
        + A hard disk partition with enough space to accommodate the User Environment Simulator code – approx. 100KB.
        + VGA or higher-resolution monitor.
        + Keyboard.
        + Mouse.
        + Network adapter.
  2. Software Requirements
     1. Software Requirements for the Harmonia Server
        + Windows XP or higher.
        + MySQL Server 5.7 version should be installed before starting installation of Harmonia. Installation process will assume MySQL installed on the same machine and will prompt user for MySQL password.
     2. Software Requirements for the Target Systems
        + Windows XP or higher.

1. Installation Process - Download Harmonia Installer from Github (HarmoniaInstaller.zip). Unpack at your convenient location and double click on the setup (shortcut) from the unpacked directory. The installation wizard will guide the user through two perquisite software installation (Java 1.6 32 bits and Open Office). It then continues to the main Harmonia installation. While installing the schema for MySQL, it will prompt user for the password for root user. This will be the last step in the installation process.
2. Before Running the Harmonia Application after the install.
   1. Certificate Generation
      1. Harmonia Server Certificate

Clients like PM Administrative Tool communicate with the PM Engine (server) using SSL, hence the need for the server (and the client) to identify itself to the other party through public key certificates. This section explains how to obtain a server certificate from a MS Stand-alone Certification Authority (CA).

Step 1. Log as Administrator on the computer that will host the PM engine (server). Make sure that a stand-alone certification authority is installed, and that it automatically issues the requested certificates (in order to simplify the procedure). Install the CA root certificate in the Trusted Root Certification Authorities.

Step 2. Create a folder named Keystores. This folder will contain the PM server key store and trust store. The key store is a repository for the PM server’s private key and certificate. The trust store is a repository for public key certificates that the PM server trusts. For simplicity, we assume that the same CA is used to issue all certificates. Then the trust store needs only contain the CA’s root certificate.

Step 3. Open a MS-DOS command window, cd to the Keystores folder, and run the following commands:

>keytool -genkey -keyalg RSA -alias pmserver -keystore serverKeystore

Enter keystore password: aaaaaa

What is your first and last name?

[Unknown]: pmserver

What is the name of your organizational unit?

[Unknown]: CSD

What is the name of your organization?

[Unknown]: NIST

What is the name of your City or Locality?

[Unknown]: Gaithersburg

What is the name of your State or Province?

[Unknown]: Maryland

What is the two-letter country code for this unit?

[Unknown]: US

Is CN=pmserver, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US correct?

[no]: yes

Enter key password for <pmserver>

(RETURN if same as keystore password):

>keytool -certreq -alias pmserver -file pmserver.csr -keystore serverKeystore

Enter keystore password: aaaaaa

The file pmserver.csr contains a standard certificate request.

Step 4. Use the MS Internet Explorer to submit the certificate request to the CA installed on the MS Windows Server 2000 or 2003. Namely, open the URL

<http://mymachine/certsrv>

where “mymachine” must be replaced by the server’s host name. From the web page displayed, select the radio button “Request a certificate” and click the “Next” button. From the next page, select the radio button “Advanced request” and click the “Next” button. From the next page, select the radio button “Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file” and click the “Next” button. Copy the contents of the pmserver.csr file and paste it in the text area titled “Saved Request”. Click the “Submit” button.

In the next page, select the radio button “Base 64 encoded” and select the link “Download CA certificate”. When asked, save the downloaded certificate under the name “pmserver.cer” to the Keystores folder.

Step 5. In the Windows Explorer window, double-click on the certificate pmserver.cer. In the certificate manager, select the tab “Details” and click the “Copy to File…” button. This launches the Certificate Export Wizard. Click the “Next” button, select the radio button “Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)”, check the checkbox “Include all certificates in the certification path if possible”, and click the “Next” button. Export the certificates under the name pmserver.p7b to folder Keystores. Click “Next”, then “Finish”.

Step 6. In the MS-DOS command window, run the following command:

>keytool -import -alias pmserver -file pmserver.p7b -keystore serverKeystore

Enter keystore password: aaaaaa

Top-level certificate in reply:

Owner: CN=PMCA, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US, EMAILADDRESS=

serban.gavrila@nist.gov

Issuer: CN=PMCA, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US, EMAILADDRESS

=serban.gavrila@nist.gov

Serial number: 186ae6f14015eb86435db3746312cab9

Valid from: Fri Aug 26 12:26:08 EDT 2005 until: Mon Aug 25 12:34:37 EDT 2008

Certificate fingerprints:

MD5: 68:F5:23:C4:7F:11:AF:D5:B1:1D:EB:0A:7B:22:6E:96

SHA1: D6:E0:29:DF:3E:D4:A7:44:F2:86:3E:F9:09:1C:E4:E6:11:93:CE:59

... is not trusted. Install reply anyway? [no]: yes

Certificate reply was installed in keystore

Step 7. Using the same certificate manager, save the CA root certificate base 64-encoded as root.cer, then run the command:

>keytool -import -alias root -file root.cer -keystore serverTruststore

Enter keystore password: aaaaaa

Owner: CN=PMCA, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US, EMAILADDRESS=

serban.gavrila@nist.gov

Issuer: CN=PMCA, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US, EMAILADDRESS

=serban.gavrila@nist.gov

Serial number: 186ae6f14015eb86435db3746312cab9

Valid from: Fri Aug 26 12:26:08 EDT 2005 until: Mon Aug 25 12:34:37 EDT 2008

Certificate fingerprints:

MD5: 68:F5:23:C4:7F:11:AF:D5:B1:1D:EB:0A:7B:22:6E:96

SHA1: D6:E0:29:DF:3E:D4:A7:44:F2:86:3E:F9:09:1C:E4:E6:11:93:CE:59

Trust this certificate? [no]: yes

Certificate was added to keystore

* + 1. Harmonia User Certificate

Obtaining a user’s certificate is very similar to obtaining the server’s certificate. Here we detail the procedure for the user “super”. For other users, simply replace “super” with the user’s name everywhere.

Step 1. Log as Administrator on the computer whose CA was used to issue the PM server’s certificate.

Step 2. Create a folder named Keystores. This folder will contain the PM user key store and trust store. The key store is a repository for the user’s private key and certificate. The trust store is a repository for public key certificates that the user trusts. For simplicity, we assume that the same CA issues all certificates. Hence, the trust store needs only contain the CA’s root certificate.

Step 3. Open a MS-DOS command window, cd to the Keystores folder, and run the following commands:

>keytool -genkey -keyalg RSA -alias super -keystore superKeystore

Enter keystore password: aaaaaa

What is your first and last name?

[Unknown]: super

What is the name of your organizational unit?

[Unknown]: CSD

What is the name of your organization?

[Unknown]: NIST

What is the name of your City or Locality?

[Unknown]: Gaithersburg

What is the name of your State or Province?

[Unknown]: Maryland

What is the two-letter country code for this unit?

[Unknown]: US

Is CN=super, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US correct?

[no]: yes

Enter key password for <super>

(RETURN if same as keystore password):

>keytool -certreq -alias super -file super.csr -keystore superKeystore

Enter keystore password: aaaaaa

The file super.csr contains a standard certificate request.

Step 4. Use the MS Internet Explorer to submit the certificate request to the CA installed on the MS Windows Server 2000 or 2003. Namely, open the URL

<http://mymachine/certsrv>

where “mymachine” must be replaced by the server’s host name. From the web page displayed, select the radio button “Request a certificate” and click the “Next” button. From the next page, select the radio button “Advanced request” and click the “Next” button. From the next page, select the radio button “Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file” and click the “Next” button. Copy the contents of the super.csr file and paste it in the text area titled “Saved Request”. Click the “Submit” button.

In the next page, select the radio button “Base 64 encoded” and select the link “Download CA certificate”. When asked, save the downloaded certificate under the name “super.cer” to the Keystores folder.

Step 5. In the Windows Explorer window, double-click on the certificate super.cer. In the certificate manager, select the tab “Details” and click the “Copy to File…” button. This launches the Certificate Export Wizard. Click the “Next” button, select the radio button “Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)”, check the checkbox “Include all certificates in the certification path if possible”, and click the “Next” button. Export the certificates under the name super.p7b to folder Keystores. Click “Next”, then “Finish”.

Step 6. In the MS-DOS command window, run the following command:

>keytool -import -alias super -file super.p7b -keystore superKeystore

Enter keystore password: aaaaaa

Top-level certificate in reply:

Owner: CN=PMCA, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US, EMAILADDRESS=serban.gavrila@nist.gov

Issuer: CN=PMCA, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US, EMAILADDRESS

=serban.gavrila@nist.gov

Serial number: ...

... is not trusted. Install reply anyway? [no]: yes

Certificate reply was installed in keystore

Step 7. Using the same certificate manager, save the CA root certificate base 64-encoded as root.cer, then run the command:

>keytool -import -alias root -file root.cer -keystore superTruststore

Enter keystore password: aaaaaa

Owner: CN=PMCA, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US, EMAILADDRESS=

serban.gavrila@nist.gov

Issuer: CN=PMCA, OU=CSD, O=NIST, L=Gaithersburg, ST=Maryland, C=US, EMAILADDRESS

=serban.gavrila@nist.gov

Serial number: 186ae6f14015eb86435db3746312cab9

Valid from: Fri Aug 26 12:26:08 EDT 2005 until: Mon Aug 25 12:34:37 EDT 2008

Certificate fingerprints:

MD5: 68:F5:23:C4:7F:11:AF:D5:B1:1D:EB:0A:7B:22:6E:96

SHA1: D6:E0:29:DF:3E:D4:A7:44:F2:86:3E:F9:09:1C:E4:E6:11:93:CE:59

Trust this certificate? [no]: yes

Certificate was added to keystore

* + 1. Where the certificate and keystore needs to be located

The user’s certificate and keystore needs to be put in the keystores folder. The proper naming format for the keystore is: *computername***Keystore.**

1. Running Harmonia
   1. Server

To run the server, double click on the server.bat file this should have been added on the Desktop after installing Harmonia. If you are running Harmonia for the first time, it will prompt user for the MySQL root password. The user will then be prompted to enter your password as well as the keystore password. **Note:** The default keystore password is: aaaaaa.

* 1. Administrator Tool

To run the administrator tool, first start the server and then double click on the super.bat file found on the Desktop. The user will be prompted to enter the keystore password. Finally the user will need to input super’s password which is: super. Please note that in order to see sample data provided with the package, please import PMConfiguration.pm file (under C:\PM\conf directory) by using File🡪Import menu.

* 1. Client Tool

To run the client tool, first start the simulator by double clicking the simulator.bat file found on the Desktop. After that is running double click on the sesmgr.bat file found on the Desktop, a prompt will pop up that instructs the user to input the username and the user’s password. By default we have 5 users: Dave, Bob, Katie, Alice and Charlie. Their passwords are their names, everything is in lowercase when putting it in the prompt.