Document Title: **ISEEU Global: Courier Scripting Project**

Document Version: **Version 2**
Publish Date: **10th June 2012**
Document Author: **Tony Donoghue**

MAGIKOS IT LIMITED
Registered in England Number 07995124
Registered Office: 77 South Meadow, Crowthorne, Berkshire, RG45 7HP
Tel: 0843 289 2272
www.magikos.co.uk

Content:

Section 1 – Pre-Requisite Considerations

The bullet list below represents the high level pre-requisites that you will need to hand before completing an ISEEU Global Courier build:

- Physical or Virtual server which meets the minimum specification.
- Red Hat Enterprise Linux V6.2 media in ether physical format or in ISO format.
- Copy of the 'current' directory for the correct version of ISEEU Global Courier in physical format, ISO format or a ZIP format to enable sending via pre-built ISEEU Global Courier service. This contains all source code, courier software and configuration files required to undertake the build.
- Documentation to assist with the process or site specific pre-requisites which are documented below.
- Network configuration and Firewall configuration for any site specific installation.

The following list represents the pre-requisite notes and site considerations that should be documented before undertaking the installation of ISEEU Global Courier. Some of the information required may not be known at the time the server is configured, but in order to have an operational server to test at the end of the process valid information will need to be entered at various points during the installation. These can be changed after the installation to customer specific settings as required. Please find below a table containing the pre-requisite information that has been completed to match the example installation notes found below:

Pre-Requisite Description	Example Value
Host Name - crr-<id number>.iseeuglobal.com	crr-75012.iseeuglobal.com
Linux root password - <placename><person name>123	crowthornetony123
LUKS Passprase - <element><instrument><random 2 digits>	golddrum77
Boot loader password - <same as for root>	crowthornetony123
Password for iseeuglobal account - <same as root>	crowthornetony123
DNS / Fully Qualified Domain Name	tonys-courier.iseeuglobal.com
MySQL Password - <As root with upper-case leading letters and no numbers>	CrowthorneTony
<ALL OTHER SETTINGS DERIVED FROM THESE ABOVE>	

Section 2 – Courier V4 – Operating System Installation

The following section is a formatted and coloured version of the RAW notes found in the supporting documentation which shows how to install the Red Hat Enterprise Linux V6.2 software and which settings to choose to enable it to have the ISEEU Global Courier V4.2 software installed.

- Ensure you have a physical system or virtual system that meets the minimum ISEEU Global Courier specification and either put the Red Hat Enterprise Linux V6.2 DVD into the drive or mount using a virtual DVD drive and an ISO file. Once configuration completed start your system.
- The initial splash screen will appear and the default setting Install or upgrade an existing system will be selected. Press **return** to continue.
- The system starts and probes the hardware then displays that the media has been found and asks if you want to test the media before you continue. It is only necessary to test the software if it has never been used before. Use the tab key to select skip and press **return** to continue.
- The Anaconda Linux installer starts and displays its initial splash screen where now the mouse should be operational and you can click **next** to continue.
- On the language screen choose English (English) and then click **next** to continue.
- On the keyboard screen choose United Kingdom and click **next** to continue.
- On the devices screen leave the default setting of Basic Storage Devices selected and click **next** to continue.
- If a warning appears regarding storage, this is normal and you should click **Yes, discard any data** to continue.
- You are then prompted for a host name for the system which should take the format crr-<id number>.iseeuglobal.com (e.g. crr-75012.iseeuglobal.com). Once a host name has been entered click **next** to continue.
- On the time zone screen click on the map so that **Europe/London** is selected before clicking **next** to continue.
- You are then prompted for a root password. This will be used in several formats throughout the application and should be sufficient in length to withstand attack. It should be in the format <place name followed by person name>123 (e.g. crowthornetony123). Once a root password has been entered click **next** to continue.
- On the type of installation screen you should select **Use All Space** at the top and also tick both the selection boxes labelled **Encrypt system** and **Review and modify partitioning layout** before clicking **next** to continue.
- When then default layout for the system is displayed this will need to be modified by selecting the **volume group** towards the top which has been labelled with the host name (e.g. vg_crr75012) and clicking **edit** to make changes.
- The Edit VLM Volume Group box is displayed. Choose the **root partition** from the list and click **delete**, clicking **delete** again on the confirm delete pop up. Then choose the **home partition** and click **delete**, again clicking **delete** on the confirm delete popup. This should then leave just the swap partition left.
- Now the correct partitions are created by clicking **add**, choosing **/** from the Mount Point

dropdown, setting **10240** in the Size (MB) and leaving the other settings as default. Note: Do not set encryption again here as its done for the entire disk not at the partition level.

- Repeat the previous step again for **/var** and **/tmp** using the same settings.
- Then add a further partition for **/home** but instead assign the remaining disk space (Max) to this partition still with all other settings as default.
- Once all partitions are added click on **OK** to continue.
- Review the changes you have made to ensure that you have 10240 size partitions for / and /tmp and /var and the remaining disk for /home. Once happy the partitions are setup correctly click **next** to continue.
- If a warning appears regarding Format Warnings, click **format** to continue.
- You are prompted for a passphrase for the encrypted disks. As this password must go to the customer it must be different to the root password. These passwords are in the following format <element followed by instrument followed by 2 digit random number> (e.g. golddrum77). Once entered click **OK** to continue.
- Again if a warning appears regarding writing storage information to disk, click **Write changes to disk** to continue.
- The partitions are then created and formatted and this can take some time larger disks.
- On the Boot Loader screen, select **Use a boot loader password** and when the popup appears enter the same password as used for the root password earlier before clicking **OK** to continue.
- Once the boot loader password box has disappeared click on **next** to continue.
- On the software selection screen ensure the default of **Basic Server** is selected and select the **Customize now** radio button before clicking **next** to continue.
- On the software customisation screen ensure the following packages a chosen as detailed below:
    - Base System - Base - Add logwatch - Remove abrt-addon-ccpp, abrt-addon-kerneloops, abrt-addon-python, abrt-cli, sysstat (66 of 113)
    - Servers - None Selected
    - Web Services - None Selected
    - Databases - MySQL Database server (0 of 2)
    - System Management - None Selected
    - Virtualisation - None Selected
    - Desktops - Desktop (15 of 18)
    - Desktops - Desktop Debugging and Performance Tools - Remove abrt-desktop (0 of 6)
    - Desktops - Desktop Platform (0 of 6)
    - Desktops - General Purpose Desktop (37 of 49)
    - Desktops - Graphical Admin Tools (8 of 15)
    - Desktops - X Window System (11 of 12)
    - Applications - Internet Browser (3 of 3)
    - Development - Additional Development - Remove libcgroup-devel (37 of 102)
    - Delevlopment - Development tools (16 of 44)
    - Development - Server Platform Development (no optional packages listed)

    - Languages - English (UK) Support (no optional packages listed)
    - Once all options have been correctly chosen or removed, click on **next** to continue. The system then checks for dependencies before installing the operating system files onto the hard disk. This can take some time depending on the specification of the server.
- When this has finished the splash screen tells you that it has completed and click **reboot** to finish the installation.

Section 3 – Courier V4 – First Time Boot Configuration

- When the system is either rebooted or powered on you are prompted for a password by the system. Enter the **disk encryption password** (sometimes referred to as the LUKS password). Once entered press **return** to continue which starts the system boot process.
- You are presented with the Welcome splash screen with the various steps listed down the left hand side. To continue click **Forward** at the bottom right.
- On the Licence Information screen, read then licence agreement and if you agree, click **Forward** to continue.
- Although you are prompted on the Set Up Software Updates screen to configure your system for updates, the network interface will not always be available which can sometimes cause some issues. It's better to leave this and do it later during the 'Configuring the Server' step as the process is then always the same. Click **Forward** to continue.
- On the Create User account screen you are required to set up an account for everyday use. The standard credentials added here should be as follows:
    - Username - iseeuglobal
    - Full Nmame - ISEEU Global Standard User Account
    - Password - <same as root password defined previously>
    - Confirm Passowrd - <as above>

- Once you have entered the details click **Forward** to continue.
- On the Date and Time screen you should always check to see if the date and time are correct and adjust if required. However depending on the network configuration and firewall rules set by the customer or location the server is being installed, it's preferable to have the system use network time protocol (NTP) to automatically keep the server in sync. Either check the option for synchronize date and time over the network or ensure manual date and time correct before clicking **Forward** to continue.
- On the Kdump screen a warning popup may be displayed explaining there is Insufficient memory to configure Kdump (if under 4Gb normally), to move on click **OK**. When the full Kdump screen is displayed, click **Finish** to complete the first time boot wizard (optionally disable Kdump if the server has enough memory to support Kdump before clicking **finish**).
- The server will complete its reboot after you follow the various prompts (will depend on memory and server specification) and present the login screen where you can login as ISEEU Global to continue to install Courier.

Section 4 – Courier V4 – Server Configuration

- Login to the server by clicking on the ISEEU Global Standard User Account user and entering the correct password when prompted. The system is then logged in and creates the familiar desktop ready for configuration.
- The next step is to configure the network adaptor. Select from the top menu, **System, Preferences** and click **Network Connections.**
- On the Network Connections dialog box **click the entry under name** and then click **Edit**.
- On the Editing System Eth0 screen tick the option for **Connect automatically** and then choose the **IPv4 Settings tab** by clicking on it.
- If the system is being set-up in the lab, then DHCP will be fine. However before shipping to the customer, remember to set the IP address as required. When complete, click **Apply**.
- You will be prompted for the root password to make this change. Enter the password and click **Authenticate** to continue.
- This returns you to the Network Configuration dialog box. Click **Close** to complete the network configuration.
- The next step is to remove some software that Red Hat installs by default irrespective of the settings we choose during set-up. To remove these software packages open a terminal from the top menu by selecting **Applications, System Tools** and clicking **Terminal** from the menu.
- To remove software packages you will need to be root, so on the command line type **su -** and when prompted, **type the root password** followed by **return**.
- Then type **yum erase httpd** followed by **return**. This displays that 2 packages will be erased which if correct continue by entering **y** followed by **return**.
- Then type **yum erase kexec-tools** followed by **return**. This displays that 2 packages will be erased which if correct continue by entering **y** followed by **return**.
- Then type **yum erase libvirt-client** followed by **return**. This displays that 4 packages will be erased which if correct continue by entering **y** followed by **return**.
- Then close the terminal window by typing **exit** followed by **return** and again type **exit** followed by **return**.
- The next step is to configure the built-in Firewall. To open the dialog box choose from the menu **System, Administration** and clicking on **Firewall** from the menu.
- A dialog is displayed explaining that basic firewall config is carried out using the dialog and advanced config is carried out by hand. Click **Close** to continue however before it can be closed, behind is an Authentication dialog which needs the **root password entered** and the **Authenticate** button clicked before it will respond.
- On the main Firewall dialog, scroll down the right hand bar to locate the existing SSH selected service and **de-select it** (may need to be left if remote administration is set-up depending on the site configuration but will need to be configured to use key authentication and not password first)
- Above the SSH service just de-selected is listed **Secure WWW (HTTPS)** which needs to be selected. Once this is complete click **Apply** on the top menu and on the popup dialog box click **Yes** to apply the settings. The dialog can then be closed by selecting **File** and clicking **quit** on the menu.

- The last step is to configure updates and patch the system. Open the Red Hat configuration dialog by navigating to **System, Administration** and clicking on **RHN Registration**.
- When the authentication popup appears, type in the **root password** and click on **OK** to continue.
- A splash screen is displayed for Registration, click **forward** to continue.
- When choosing an update location, leave the default top setting selected and click **forward** to continue.
- You are now prompted to type your Red Hat Network account details to authenticate. Type the **username** and **password** into the system and click **forward** to continue.
- Once the system has been able to communicate with Red Hat Network service you are prompted to set a System Name and supply profile information for the system. **Type a suitable name** and leave both the profile tick boxes selected, after which click **forward** to continue.
- Once the system has sent all the information, which can take a few minutes, you are prompted by a Review screen where you can click **forward** to continue.
- This completes the system registration and when prompted you can click **finish** to complete this task.
    - (optional testing: check repositories are able to be listed using yum and repolist and also check system appears on Red Hat Network system lists before proceeding with system patching)
- The last step which could be left to run overnight is to patch the system (can be skipped for test and demo systems if required or timescales permit). This is completed by opening a terminal window from the **Applications, System Tools** and by clicking on **Terminal** from the menu.
- To perform patches you need to be root, so type **su - on** the terminal prompt and click **return** to continue. When prompted type the **root password** followed by **return**.
- Next on the command line type **yum updates** followed by **return** to initialise the process. Depending on the patches available the system can prompt you to **accept keys**, **accept the wrapped up packages** and finally accept (all by typing **y** on the prompt followed by **return**) to allow the system to continue.
- Once complete reboot the system with the **reboot** command typed on the command line followed by **return**.

Section 5 – Courier V4 – Courier Code Installation

- Boot up the system and login with the standard ISEEU Global user account using the same Password as the root account.
- Copy the content of the 'current' directory to the desktop by a suitable method - this may be via an internal fileshare, from CD/DVD, by mounting the local ISO directory or from a secure file transfer using ISEEU Global Courier.
- Next open a terminal window by navigating to **Applications, System Tools** and then clicking **Terminal** from the menu.
- Ensure you are root by typing **su -** on the command line and **entering the root password** followed by **return**.
- On the command line change directory to the 'current' directory by typing **cd /home/iseeuglobal/Desktop** followed by **return**.
- Now set the permissions so the scripts can run without errors by typing **chmod 777 -R current** followed by **return** and then also type **chown root:root -R current** followed by **return**.
- Now change directory to where you can run the script by typing **cd /home/iseeuglobal/Desktop/current** followed by **return**.
- Start the script with the following command **./courier4_2_install_script** followed by **return**.

The script begins and prompts the user for actions or details. The next part of these instructions detail what the user needs to enter and the choices that they make. The script can only be run once. Ensure you have sufficient time and understanding of the system because if the script fails or with wrong details are entered the user will need to be able to manually fix the system by hand or begin again.

- First the user is prompted for the existing LUKS password to allow them to enter an additional passphrase for the disk encryption. When prompted **enter the passphrase** used during the operating system installation (e.g. golddrum77) followed by **return**.
- The system then prompts for the new passphrase (ISEEU Global have always used labolgueesi123 in the past for this key). Enter a **new passphrase key** followed by **return**. The system then writes the key passphrase to the system and confirms this by displaying the current key status where slot 1 should not be filled along with the original key, set when installing the operating system, in slot 0.
- The script then prompts you to enter the systems DNS host name. This is the name that the system will be accessed from when typing or clicking a link in the end users browser (e.g. tonys-courier.iseeuglobal.com). This name is also used to bind certificates to the server. **Enter the fully qualified domain name** (FQDN) followed by **return**.
- Once this has completed the script starts and initialises MySQL and prompts you to enter a root MySQL password. As no password has yet been set for the root In MySQL press **return** to continue.
- The script then asks if you would like to set a root password which you type an **uppercase Y** followed by **return**.
- The format for this password has always been based on the root password but with no

numerical characters and changing each word to use upper case leading characters (e.g. CrowthorneTony). **Enter a root MySQL password** followed by **return, re-entering it again** when prompted.

- To better protect the system we secure the service next by removing unwanted test entries. For each of the following 4 questions answer with an **uppercase Y** followed by **return**.
- Next the script moves and unpacks the source files to a temp location. To continue press **return** which you will see the script open and unpack the files.
- Once complete the script uses a configuration file to layout and compile the Apache web server. Press **return** to continue. This can take some time depending on the specification of the server. When complete scroll up the screen where the bottom line should start with 'make[1]' to show it finished correctly.
- Next the script will prompt before it compiles PHP and configures it for use with Courier. Press **enter** to continue. This can also take some time (longer than Apache to compile). Again when complete look above to notice any errors and the last line should begin 'Installing PDO headers...'.
- Next the script will unpack the Courier code into the correct location. Press **enter** to continue which finished almost instantly.
- Next the script will create the initial default database for Courier. Press **return** to continue when you are prompted for the root MySQL password you set earlier. After **entering the password** follow this by hitting **return**.
- Next the script creates the necessary directories. Press **return** to continue..
- Then the script configures the systems with default settings. Press **return** to continue.
- Next the script creates a secure server key to enable certificates tone created for this server. Press **return** to continue.
- Next the server the creates a certificate request file which you can later apply for a live certificate from a Certificate Authority. Press **return** to continue and enter the following details when prompted:
- Country Code : **GB**
- State or Province Name: **North Somerset**
- Locatity Name: **Bristol**
- Organisation Name : **ISEEU Global Limited**
- Organisation Unit Name: **Information Technology**
- Common Name: **tonys-courier.iseeuglobal.com**
- Email Address: **technical@iseeuglobal.com**
- A Challenge Password: **<just press enter>**
- An Optional Company Name: **<just press enter>**
- The self signed certificate is then created and the output sent to the screen to enable you to check if correct.
- Next the script creates a self signed certificate from the certificate request file until a real certificate can be installed. Press **return** to continue.
- Next the scrip installs the IonCube software used for code obfuscation and licensing. Press **return** to continue.
- Next the script installs the GPG keys used for encrypting the grid card information to ensure

they stay secure in transit. Press **return** to continue. You should notice that the success of this process is provided by screen output which enables you to see that 1 key was sucessfully imported to the system.

- Next the script will stop in-necessary running processes and clean up from itself. This output does not look clean and several services look like they fail but when the server reboots this is completed and cleaned up. Press **return** to continue.
- The installation is largely completed now but some final customisation can be made to the configuration files. For each of the files the following edits should be made/considered by typing **y** and pressing **return**.
-
- You are now informed that you are going to edit the Courier Configuration File. By pressing **enter** you go into editing mode where you can make the following edits using the **standard Vi commands** remembering to save your edits when complete with vi command :wq :
- change all parts of the script where **<SITE SPECIFIC> is found - 7 places**
    - $user – root
    - $password - <MySQL password from earlier>
    - _SYSNAME_ - <host name of system e.g. crr-1234:>
    - _BASEURL_ - <full URL of site e.g. https://tonys-courier.iseeuglobal.com>
    - _ADMAIL_ - email address for the system e.g. tonys-courier-service.iseeuglobal.com
    - _SMSURL_ - either remove the site specific notice or add new username for SMS messages
    - _SMSUNAME_ - as above remove the site specific notice or add new password for SMS messages

- The script then prompts you to edit the SSL config file which is started as above by pressing **return**. Again using the standard Vi editing commands change the following 3 settings:
    - ServerName – tonys-courier.iseeuglobal.com:443
    - SSLCertificateFile - add the name of the certificate from earlier in the process <tonys-courier.iseeuglobal.com.crt>
    - SSLCertificateKeyFile - add the name of the servers key file here from earlier <tonys-courier.iseeuglobal.com.key>

- The last part of the configuration files is to edit the log watch file if the server is going to be managed correctly. Again press **enter** to continue and edit the following 3 settings:
    - MailTo - technical@iseeuglobal.com (remember to remove root from the settings if you don't want to fill the disks)
    - MailFrom – crr-75012-logwatch
    - Detail - Med

- This concludes the installation and configuration and the script prompts you to restart the server if you would like now. Its recommended to reboot at this stage so to complete the process type y and press enter to restart the server.

Section 6 – Courier V5 – Operating System Installation

The following section is a formatted and coloured version of the RAW notes found in the supporting documentation which shows how to install the Red Hat Enterprise Linux V6.2 software and which settings to choose to enable it to have the ISEEU Global Courier V4.2 software installed.

- Ensure you have a physical system or virtual system that meets the minimum ISEEU Global Courier specification and either put the Red Hat Enterprise Linux V6.2 DVD into the drive or mount using a virtual DVD drive and an ISO file. Once configuration completed start your system.
- The initial splash screen will appear and the default setting Install or upgrade an existing system will be selected. Press **return** to continue.
- The system starts and probes the hardware then displays that the media has been found and asks if you want to test the media before you continue. It is only necessary to test the software if it has never been used before. Use the tab key to select skip and press **return** to continue.
- The Anaconda Linux installer starts and displays its initial splash screen where now the mouse should be operational and you can click **next** to continue.
- On the language screen choose English (English) and then click **next** to continue.
- On the keyboard screen choose United Kingdom and click **next** to continue.
- On the devices screen leave the default setting of Basic Storage Devices selected and click **next** to continue.
- If a warning appears regarding storage, this is normal and you should click **Yes, discard any data** to continue.
- You are then prompted for a host name for the system which should take the format crr-<id number>.iseeuglobal.com (e.g. crr-75012.iseeuglobal.com). Once a host name has been entered click **next** to continue.
- On the time zone screen click on the map so that **Europe/London** is selected before clicking **next** to continue.
- You are then prompted for a root password. This will be used in several formats throughout the application and should be sufficient in length to withstand attack. It should be in the format <place name followed by person name>123 (e.g. crowthornetony123). Once a root password has been entered click **next** to continue.
- On the type of installation screen you should select **Use All Space** at the top and also tick both the selection boxes labelled **Encrypt system** and **Review and modify partitioning layout** before clicking **next** to continue.
- When then default layout for the system is displayed this will need to be modified by selecting the **volume group** towards the top which has been labelled with the host name (e.g. vg_crr75012) and clicking **edit** to make changes.
- The Edit VLM Volume Group box is displayed. Choose the **root partition** from the list and click **delete**, clicking **delete** again on the confirm delete pop up. Then choose the **home partition** and click **delete**, again clicking **delete** on the confirm delete popup. This should then leave just the swap partition left.
- Now the correct partitions are created by clicking **add**, choosing **/** from the Mount Point

dropdown, setting **10240** in the Size (MB) and leaving the other settings as default. Note: Do not set encryption again here as its done for the entire disk not at the partition level.

- Repeat the previous step again for **/var** and **/tmp** using the same settings.
- Then add a further partition for **/home** but instead assign the remaining disk space (Max) to this partition still with all other settings as default.
- Once all partitions are added click on **OK** to continue.
- Review the changes you have made to ensure that you have 10240 size partitions for / and /tmp and /var and the remaining disk for /home. Once happy the partitions are setup correctly click **next** to continue.
- If a warning appears regarding Format Warnings, click **format** to continue.
- You are prompted for a passphrase for the encrypted disks. As this password must go to the customer it must be different to the root password. These passwords are in the following format <element followed by instrument followed by 2 digit random number> (e.g. golddrum77). Once entered click **OK** to continue.
- Again if a warning appears regarding writing storage information to disk, click **Write changes to disk** to continue.
- The partitions are then created and formatted and this can take some time larger disks.
- On the Boot Loader screen, select **Use a boot loader password** and when the popup appears enter the same password as used for the root password earlier before clicking **OK** to continue.
- Once the boot loader password box has disappeared click on **next** to continue.
- On the software selection screen ensure the default of **Basic Server** is selected and select the **Customize now** radio button before clicking **next** to continue.
- On the software customisation screen ensure the following packages a chosen as detailed below:
    - Base System - Base - Add logwatch - Remove abrt-addon-ccpp, abrt-addon-kerneloops, abrt-addon-python, abrt-cli, sysstat (66 of 113)
    - Servers - None Selected
    - Web Services - None Selected
    - Databases - MySQL Database server (0 of 2)
    - System Management - None Selected
    - Virtualisation - None Selected
    - Desktops - Desktop (15 of 18)
    - Desktops - Desktop Debugging and Performance Tools - Remove abrt-desktop (0 of 6)
    - Desktops - Desktop Platform (0 of 6)
    - Desktops - General Purpose Desktop (37 of 49)
    - Desktops - Graphical Admin Tools (8 of 15)
    - Desktops - X Window System (11 of 12)
    - Applications - Internet Browser (3 of 3)
    - Development - Additional Development - Remove libcgroup-devel (37 of 102)
    - Delevlopment - Development tools (16 of 44)
    - Development - Server Platform Development (no optional packages listed)

    - Languages - English (UK) Support (no optional packages listed)
    - Once all options have been correctly chosen or removed, click on **next** to continue. The system then checks for dependencies before installing the operating system files onto the hard disk. This can take some time depending on the specification of the server.
- When this has finished the splash screen tells you that it has completed and click **reboot** to finish the installation.

Section 7 – Courier V5 – First Time Boot Configuration

- When the system is either rebooted or powered on you are prompted for a password by the system. Enter the **disk encryption password** (sometimes referred to as the LUKS password). Once entered press **return** to continue which starts the system boot process.
- You are presented with the Welcome splash screen with the various steps listed down the left hand side. To continue click **Forward** at the bottom right.
- On the Licence Information screen, read then licence agreement and if you agree, click **Forward** to continue.
- Although you are prompted on the Set Up Software Updates screen to configure your system for updates, the network interface will not always be available which can sometimes cause some issues. It's better to leave this and do it later during the 'Configuring the Server' step as the process is then always the same. Click **Forward** to continue.
- On the Create User account screen you are required to set up an account for everyday use. The standard credentials added here should be as follows:
    - Username - iseeuglobal
    - Full Nmame - ISEEU Global Standard User Account
    - Password - <same as root password defined previously>
    - Confirm Passowrd - <as above>

- Once you have entered the details click **Forward** to continue.
- On the Date and Time screen you should always check to see if the date and time are correct and adjust if required. However depending on the network configuration and firewall rules set by the customer or location the server is being installed, it's preferable to have the system use network time protocol (NTP) to automatically keep the server in sync. Either check the option for synchronize date and time over the network or ensure manual date and time correct before clicking **Forward** to continue.
- On the Kdump screen a warning popup may be displayed explaining there is Insufficient memory to configure Kdump (if under 4Gb normally), to move on click **OK**. When the full Kdump screen is displayed, click **Finish** to complete the first time boot wizard (optionally disable Kdump if the server has enough memory to support Kdump before clicking **finish**).
- The server will complete its reboot after you follow the various prompts (will depend on memory and server specification) and present the login screen where you can login as ISEEU Global to continue to install Courier.

Section 8 – Courier V5 – Server Configuration

- Login to the server by clicking on the ISEEU Global Standard User Account user and entering the correct password when prompted. The system is then logged in and creates the familiar desktop ready for configuration.
- The next step is to configure the network adaptor. Select from the top menu, **System, Preferences** and click **Network Connections.**
- On the Network Connections dialog box **click the entry under name** and then click **Edit**.
- On the Editing System Eth0 screen tick the option for **Connect automatically** and then choose the **IPv4 Settings tab** by clicking on it.
- If the system is being set-up in the lab, then DHCP will be fine. However before shipping to the customer, remember to set the IP address as required. When complete, click **Apply**.
- You will be prompted for the root password to make this change. Enter the password and click **Authenticate** to continue.
- This returns you to the Network Configuration dialog box. Click **Close** to complete the network configuration.
- The next step is to remove some software that Red Hat installs by default irrespective of the settings we choose during set-up. To remove these software packages open a terminal from the top menu by selecting **Applications, System Tools** and clicking **Terminal** from the menu.
- To remove software packages you will need to be root, so on the command line type **su -** and when prompted, **type the root password** followed by **return**.
- Then type **yum erase httpd** followed by **return**. This displays that 2 packages will be erased which if correct continue by entering **y** followed by **return**.
- Then type **yum erase kexec-tools** followed by **return**. This displays that 2 packages will be erased which if correct continue by entering **y** followed by **return**.
- Then type **yum erase libvirt-client** followed by **return**. This displays that 4 packages will be erased which if correct continue by entering **y** followed by **return**.
- Then close the terminal window by typing **exit** followed by **return** and again type **exit** followed by **return**.
- The next step is to configure the built-in Firewall. To open the dialog box choose from the menu **System, Administration** and clicking on **Firewall** from the menu.
- A dialog is displayed explaining that basic firewall config is carried out using the dialog and advanced config is carried out by hand. Click **Close** to continue however before it can be closed, behind is an Authentication dialog which needs the **root password entered** and the **Authenticate** button clicked before it will respond.
- On the main Firewall dialog, scroll down the right hand bar to locate the existing SSH selected service and **de-select it** (may need to be left if remote administration is set-up depending on the site configuration but will need to be configured to use key authentication and not password first)
- Above the SSH service just de-selected is listed **Secure WWW (HTTPS)** which needs to be selected. Once this is complete click **Apply** on the top menu and on the popup dialog box click **Yes** to apply the settings. The dialog can then be closed by selecting **File** and clicking **quit** on the menu.

- The last step is to configure updates and patch the system. Open the Red Hat configuration dialog by navigating to **System, Administration** and clicking on **RHN Registration**.
- When the authentication popup appears, type in the **root password** and click on **OK** to continue.
- A splash screen is displayed for Registration, click **forward** to continue.
- When choosing an update location, leave the default top setting selected and click **forward** to continue.
- You are now prompted to type your Red Hat Network account details to authenticate. Type the **username** and **password** into the system and click **forward** to continue.
- Once the system has been able to communicate with Red Hat Network service you are prompted to set a System Name and supply profile information for the system. **Type a suitable name** and leave both the profile tick boxes selected, after which click **forward** to continue.
- Once the system has sent all the information, which can take a few minutes, you are prompted by a Review screen where you can click **forward** to continue.
- This completes the system registration and when prompted you can click **finish** to complete this task.
    - (optional testing: check repositories are able to be listed using yum and repolist and also check system appears on Red Hat Network system lists before proceeding with system patching)
- The last step which could be left to run overnight is to patch the system (can be skipped for test and demo systems if required or timescales permit). This is completed by opening a terminal window from the **Applications, System Tools** and by clicking on **Terminal** from the menu.
- To perform patches you need to be root, so type **su - on** the terminal prompt and click **return** to continue. When prompted type the **root password** followed by **return**.
- Next on the command line type **yum updates** followed by **return** to initialise the process. Depending on the patches available the system can prompt you to **accept keys**, **accept the wrapped up packages** and finally accept (all by typing **y** on the prompt followed by **return**) to allow the system to continue.
- Once complete reboot the system with the **reboot** command typed on the command line followed by **return**.

Section 9 – Courier V5 – Courier Code Installation

- Boot up the system and login with the standard ISEEU Global user account using the same password as the root account.
- Copy the content of the 'current' directory to the iseeuglobal desktop by a suitable method - this may be via an internal fileshare, from CD/DVD, by mounting the local ISO directory or from a secure file transfer using a previous working copy of ISEEU Global Courier.
- Next open a terminal window by navigating to **Applications, System Tools** and then clicking **Terminal** from the menu.
- Ensure you are root by typing **su -** on the command line and entering the **root password** followed by **return**.
- On the command line change directory to view the 'current' directory by typing **cd /home/iseeuglobal/Desktop** followed by **return**.
- Now set the permissions so the scripts can run without errors by typing **chmod 777 -R current** followed by **return** and then also type **chown root:root -R current** followed by **return**.
- Now change directory to where you can run the script by typing **cd /home/iseeuglobal/Desktop/current** followed by **return**.
- Start the script with the following command **./courier_v5_install_script** followed by **return**.

The script begins and when running prompts the user for actions or details required for the installation. The next part of these instructions detail what the user must enter and the choices that they need to make. **The script can only be run once**. Ensure you have sufficient time and understanding of the system because if the script fails or if the wrong details are entered, the operator will need to be able to manually fix the system by hand or begin again.

- First the user is prompted for the existing LUKS password to allow them to enter an additional passphrase for the disk encryption. When prompted **enter the passphrase** used during the operating system installation (e.g. golddrum77) followed by **return**.
- The system then prompts for the new passphrase (ISEEU Global have always used labolgueesi123 in the past for this key). **Enter a new passphrase** followed by **return**. The system then writes the key passphrase to the system and confirms this by displaying the current key status where slot 1 should now be filled along with the original key, set when installing the operating system, in slot 0.
- Next the software will prompt you to install an additional software package that is required for Courier V5. To start the installation follow on-screen prompts for accepting Red Hat keys (sometimes two keys) if required and by typing **y** followed by **return** to install the software.
- The script then prompts you to enter the systems DNS host name. This is the name that the system will be accessed from when typing or clicking a link in the end users browser (e.g. tonys-courier.iseeuglobal.com). This name is also used to bind certificates to the server. Enter the **fully qualified domain name** (FQDN) followed by **return**.
- Once this has completed the script starts and initialises MySQL and prompts you to enter a root MySQL password. As no password has yet been set for the root in MySQL press **return** to continue.

- The script then asks if you would like to set a root password which you type an **upper-case Y** followed by return.
- The format for this password has always been based on the root password but with no numerical characters and changing each word to use upper-case leading characters (e.g. CrowthorneTony). Enter a **root MySQL password** followed by **return re-entering it again** when prompted.
- To better protect the system we secure the service next by removing unwanted test entries. For each of the prompted **4 questions** answer with an **upper-case Y** followed by **return**.
- Next the script moves and unpacks the source files to a temp location. To continue press **return** which you will see the script open and unpack the files.
- Once the unpack is complete the script uses a configuration file to layout and compile the Apache web server and automatically goes on to compile PHP. When ready to complete this task, press **return**. NOTE: This can take some time depending on the specification of the server. When its complete look above in the scroll-back to observe any errors. The last line should begin 'Installing PDO headers...'.
- Next the script will unpack the Courier code into the correct location. Press **enter** to continue which finishes almost instantly.
- Next the script will create the initial default database for Courier. Press **return** to continue.
- When you are prompted for the root **MySQL password** you set earlier, type the password and follow this by hitting **return**.
- Next the script creates the necessary directories. Press **return** to continue..
- Then the script configures the systems with default settings. Press **return** to continue.
- Next the script creates a secure server key to enable certificates to be created for this server. Press **return** to continue.
- Next the server the created a certificate request file which you can later apply for a live certificate from a Certificate Authority from within the application. Press **return** to continue and enter the following details when prompted:
    - Country Code : **GB**
    - State or Province Name: **North Somerset**
    - Locatity Name: **Bristol**
    - Organisation Name : **ISEEU Global Limited**
    - Organisation Unit Name: **Information Technology**
    - Common Name: **tonys-courier.iseeuglobal.com**
    - Email Address: **technical@iseeuglobal.com**
    - A Challenge Password: **<just press enter>**
    - An Optional Company Name: **<just press enter>**
- The self signed certificate is then created and the output sent to the screen to enable you to check if correct.
- Next the script creates a self signed certificate from the certificate request file until a real certificate can be requested from a Certificate Authority and installed, which is not completed within the application. Press **return** to continue.
- Next the scrip installs the IonCube software used for code obfuscation and licensing. Press **Return** to continue.
- Next the script installs the GPG keys used for encrypting the grid card information to ensure

they stay secure in transit. Press **return** to continue. You should notice that the success of this process is provided by screen output which enables you to see that 1 key was successfully imported to the system.

- Next the script will stop in-necessary running processes and clean up from itself. This output does not look clean on-screen and several services look like they fail but when the server reboots this is finalised and cleaned-up. Press **return** to continue.

The installation is largely complete now but some final site specific customisation can be made to the configuration files in order to test the system and/or configure for a specific customer.

You are now informed that you are going to edit the Courier Configuration File. By pressing **enter** you enter editing mode where you can make the following edits **using the standard Vi** commands; remembering to save your edits when complete with vi command :wq
Change all parts of the script where **<EDIT HERE> is found - 13 places**

- $user – root
- $password - <MySQL password from earlier>
- _DOMAIN_ - enter the FQDN used earlier.
- _SYSNAME_ - <host name of system e.g. crr-1234:>
- _ADMAIL_ - email address for the system e.g. tonys-courier-service.iseeuglobal.com
- _SYSMAIL_ - email address for system messages – should be real.
- _PROVINCE_ - normally North Somerset unless not in iseeuglobal.com domain.
- _LOCALITY_ - normally Bristol unless not in iseeuglobal.com domain.
- _ORGNAME_ - normally ISEEU Global unless unless not in iseeuglobal.com domain.
- _ORGUNIT_ - normally Information Technology unless not in iseeuglobal.com domain.
- _SITEMAIL_ - normally technical@iseeuglobal.com unless not in iseeuglobal.com domain.
- _SMSURL_ - either remove the site specific notice or add new username for SMS messages
- _SMSUNAME_ - as above remove the site specific notice or add new password for SMS messages

The script then prompts you to edit the SSL config file which is opened in the same way by pressing **return**. Again using the **standard Vi editing commands** change the following 3 settings:

- ServerName - tonys-courier.iseeuglobal.com:443
- SSLCertificateFile - add the name of the certificate from earlier in the process <tonys-courier.iseeuglobal.com.crt>
- SSLCertificateKeyFile - add the name of the servers key file here from earlier <tonys-courier.iseeuglobal.com.key>

The last part of the configuration files is to edit the log watch file if the server is going to be

managed correctly. Again press enter to continue and edit the following 3 settings:

- MailTo - technical@iseeuglobal.com (remember to remove root from the settings if you don't want to fill the disks)
- MailFrom - crr-75012-logwatch
- Detail - Med

This concludes the installation and configuration of Courier V5 and the script prompts you to reboot the server if the operator chooses. Its recommended to reboot at this stage, so to complete the process type **y** and press **enter** to restart the server.

When you log in for the first time after the Courier V5 installation you should now clean-up by deleting the 'current' directory from the desktop and emptying the trash so no build scripts are located on the server. The system should then be tested using a standard process which is documented before configuring the application for the specific customer.

ONCE CUSTOMER SPECIFIC EDITING IS COMPLETE – REMEMBER TO OBFUSCATE AND SAVE THE LOCALCFG.INC FILE LOCATED IN /usr/local/include/iseeu USING THE LICENCE SERVER BEFORE SHIPPING THE SERVER TO SITE OR HANDING OVER TO A CUSTOMER.

Section 10 – Outstanding Tasks and/or Issues to Address

The following points were noted during the process of scripting the new Courier V5 installation, software and services. These points are necessary to enable the code to be as clean as possible and ready for deployment to live customers and sites. The scripting project was scoped to include getting the system operational but not intended to test the application for faults or bugs but some were found just in the process of writing the script. The points below are observations made during the scripting:

- A bug seemed to be introduced after an update was applied late (over the weekend) which seemed to break the publishing process. Further investigation is required – unable to check bug tracking or change controls to verify testing sign-off or indeed what the new files fixed in terms of functionality.
- Script tested with Red Hat Enterprise Linux 6.2 for both V4 and V5 of Courier. The script should be tested on CentOS Linux as well as this provides the same platform without the ongoing costs which would be useful for hosted Instances.
- There appears to be no checksum found in the transaction logs when first checked. This needs to be checked against the specs when we designed Version 5.
- Log output now includes more detail than Version 4 and the print output and standard output need to be improved.
- The help text built within the application still only contains development wording and has not had anything added in terms of real help for the users. Once added this could be included in standard builds.
- Most of the templates for Emails, SMS messages and notifications include development text and need to be addressed before system goes live. Again this can be included in standard build files so no re-keying of information is required.
- For systems that are to be hosted in multi-homed environments there is no facility to toggle or disable the system wide controls for Email, Certificates and log file review. This would potentially be a security risk to the people using the system.
- When a transaction has been created, the information view needs its look and feel adjusted as the 256bit key and other fields are too short and the text overlaps the size of the field.
- No checksums are performed against the secure messages function. Without this the messages can not be sure, if they came under scrutiny, to be accurate or proven to be a true reflection of what was sent.
- All files that make up the Version 5 code, need to be documented in terms of each ones job, function and dependencies.
- Can't find any evidence of change controls for the finish of version 5 and the sign-off for the code. Although this is now not my concern, it will make ISEEU Global's like more difficult when undertaking a company sale, valuation or for the yearly R&D return.
- Project notes, change controls and sign-off not documented which includes the wish-list and potential functions list for any future revisions.
- The code has now been obfuscated and therefore a full system wide test needs to be performed and any issues with the application need to be addressed in this finished format.
- The system, once signed-off by ISEEU Global, will need to be security checked before any

live customers are given access to the platform as this is likely to impact the service and the expectations have been set at sale time that the systems are security tested and functional. ISEEU Global Courier V5 represents a very different architecture and significant increases in functionality so issues are bound to be found which again will need to be addressed and this phase of the roll-out planned.

- Although for this script the supporting software (Apache, MySQL, Linux and PHP were updated to the latest secure versions that are available. Brand new architecture versions are available for Apache and PHP are now available and design considerations need to be understood, tested and a platform migration planned if the security of the service is to be maintained.
- By default no publishers address books have been defined within the application and therefore users will be unable to send any files before this step is undertaken. If a standard one is desired then this could be made as part of the standard build reducing the number of re-keying information tasks after the system has been built.
- It appears that the CESG are developing a new set of standards and assessments that products, staff and companies may need to comply. This should be investigated and the impact of the changes be assessed so that any changes can be added to the Courier project for review or modifications.
- Although as part of the scripting the certificate signing request files (CSR) have been reviewed for functions related to the script the process of testing the applications functions for applying certificates from a certificate authority is out of scope as this does not impact on the script in any way. However some system level functions could not be tested by AWT on their development platform because of the shared nature of the platform. Therefore all system wide functions (e.g. mail queue management, system logs, certificates, etc) should be tested on private test systems before Courier is signed-off.
- Is the default skin, finished? As I can't find any change controls and review status, I can't see if the default skin settings that the application currently has is complete.