A to Z Mobility Suite

April 19

2016

A walk-through with common troubleshooting steps; outlining the deployment of a production on premise Symantec Mobility Suite solution. This is meant to be used supplementary to the published Mobility Suite Administration and On-premise Installation guides. If there are any recommendations made in this walkthrough which contradict the above mentioned guides, use the recommendations in the guides.

Contents

Mobility Suite A to Z

Important: Read the following two knowledge base (KB) articles to gain an overview understanding of what is ahead in the installation of the Mobility Suite:

An introduction: HOWTO94487
Gathering the required information: HOWTO94492

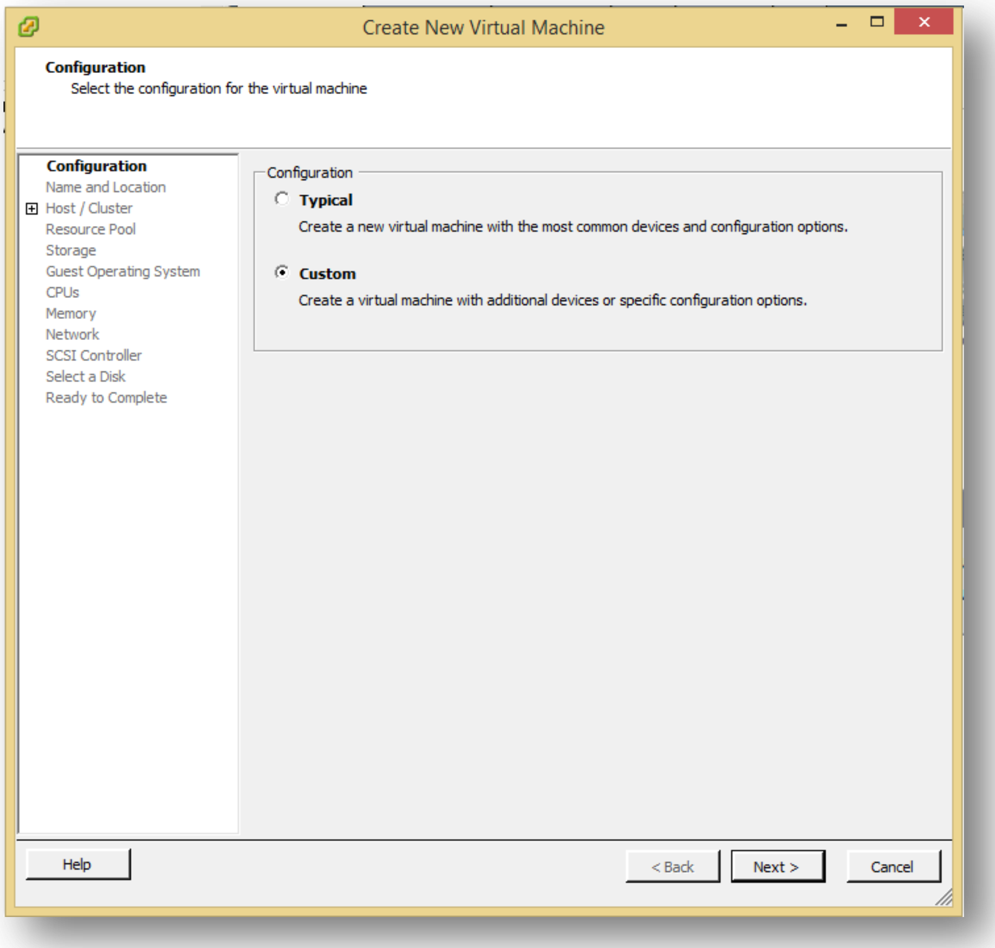
By using this guide you are agreeing to the legal terms, as stated in:

http://www.symantec.com/about/profile/policies/legal.jsp

Deploy a Virtual Machine for Symantec Mobility Suite (HOWTO110252)

1. Create a new virtual machine (VM) on the virtual host. In this example, VMware will be shown. **File** > **New** > **Virtual Machine**, select **Custom** and click **Next**:

Note: The fundamental steps to deploy a VM are essentially the same among virtual server providers.



Create New Virtual Machine

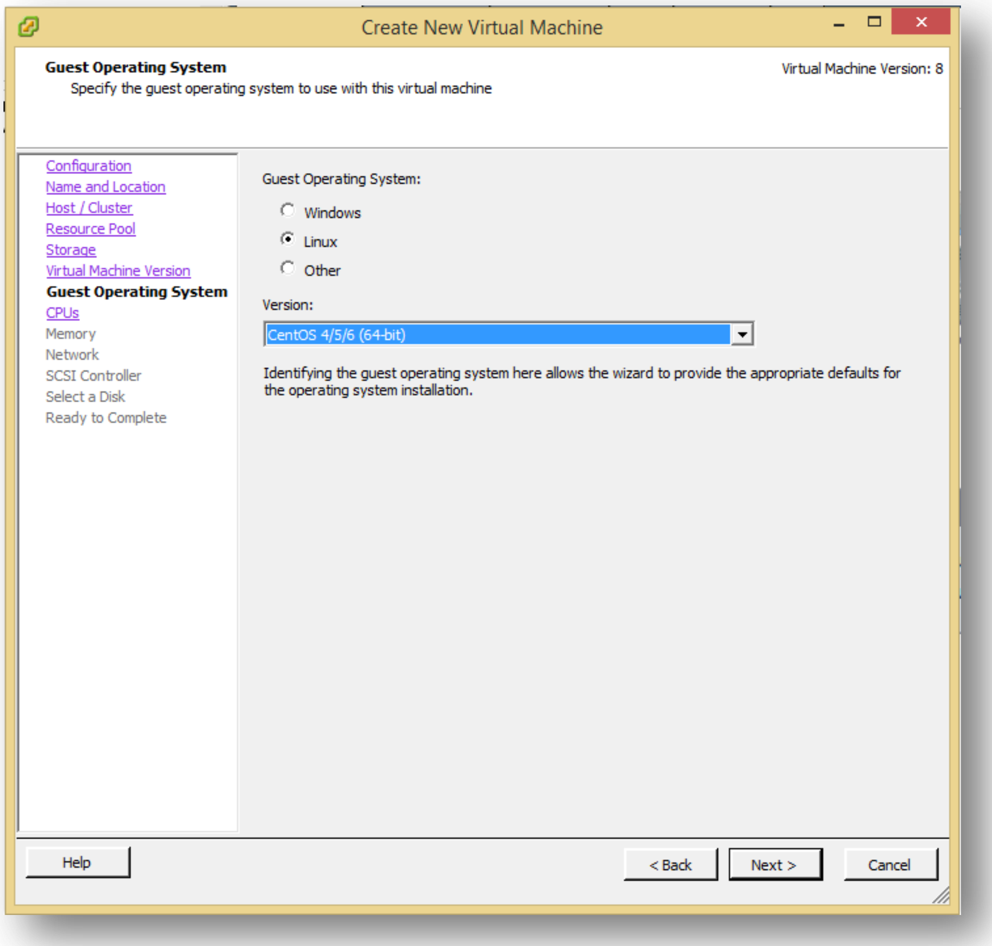
Configuration
Select the configuration for the virtual machine

Configuration

○ **Typical**
Create a new virtual machine with the most common devices and configuration options.

● **Custom**
Create a virtual machine with additional devices or specific configuration options.

2. Name the virtual machine and **Next**.
3. Select Host /Cluster (If applicable) and **Next**.
4. Chose a resource pool (if applicable) and **Next**.
5. Select destination storage for the virtual machine files and **Next** to continue.
6. Set the Virtual Machine Version (if applicable) and click **Next**.
7. Select **Linux** as the Guest Operating System (OS) and set Version to **CentOS 4/5/6 (64-bit)**.



Guest Operating System

Specify the guest operating system to use with this virtual machine

Virtual Machine Version: 8

Guest Operating System:

○ Windows

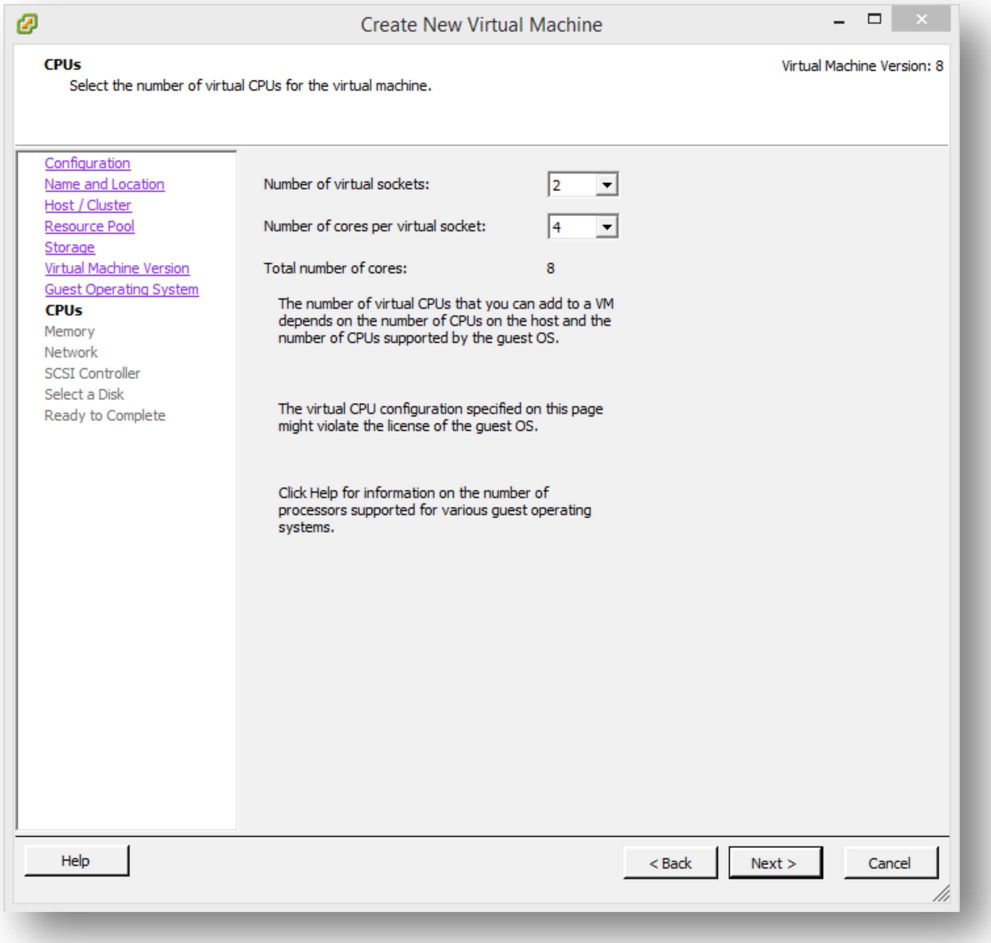
● Linux

○ Other

Version: CentOS 4/5/6 (64-bit)

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

8. Set the number of virtual sockets to **2** and the number of cores per virtual socket to **4**:



CPUs

Select the number of virtual CPUs for the virtual machine.

Virtual Machine Version: 8

Number of virtual sockets: 2

Number of cores per virtual socket: 4

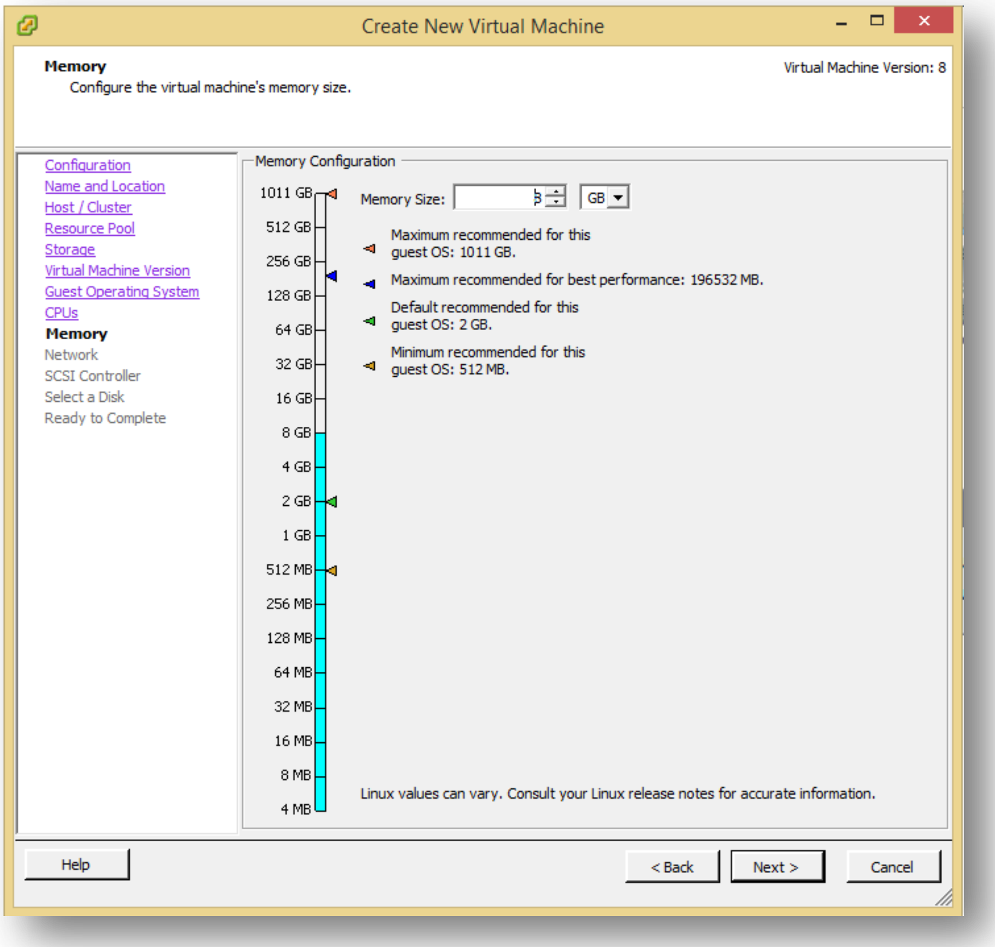
Total number of cores: 8

The number of virtual CPUs that you can add to a VM depends on the number of CPUs on the host and the number of CPUs supported by the guest OS.

The virtual CPU configuration specified on this page might violate the license of the guest OS.

Click Help for information on the number of processors supported for various guest operating systems.

9. Set the memory to **8GB**:



Create New Virtual Machine

Memory

Configure the virtual machine's memory size.

Virtual Machine Version: 8

Memory Configuration

Memory Size: 3 GB

Maximum recommended for this guest OS: 1011 GB.

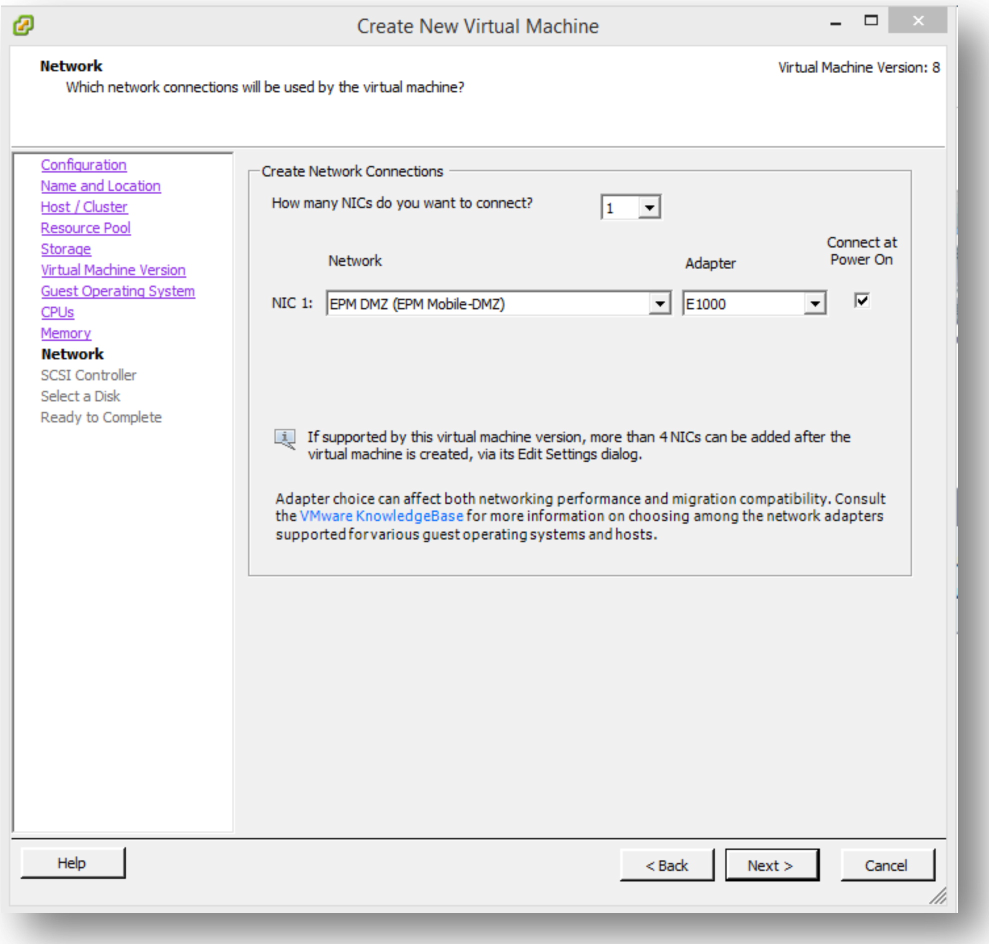
Maximum recommended for best performance: 196532 MB.

Default recommended for this guest OS: 2 GB.

Minimum recommended for this guest OS: 512 MB.

Linux values can vary. Consult your Linux release notes for accurate information.

10. For NIC 1 select the network and adapter type and ensure that it is set to **connect at power on**:
    Note: A single network interface card (NIC) is required for the Mobility Suite server.



Create New Virtual Machine

Network

Which network connections will be used by the virtual machine?

Virtual Machine Version: 8

Create Network Connections

How many NICs do you want to connect? 1

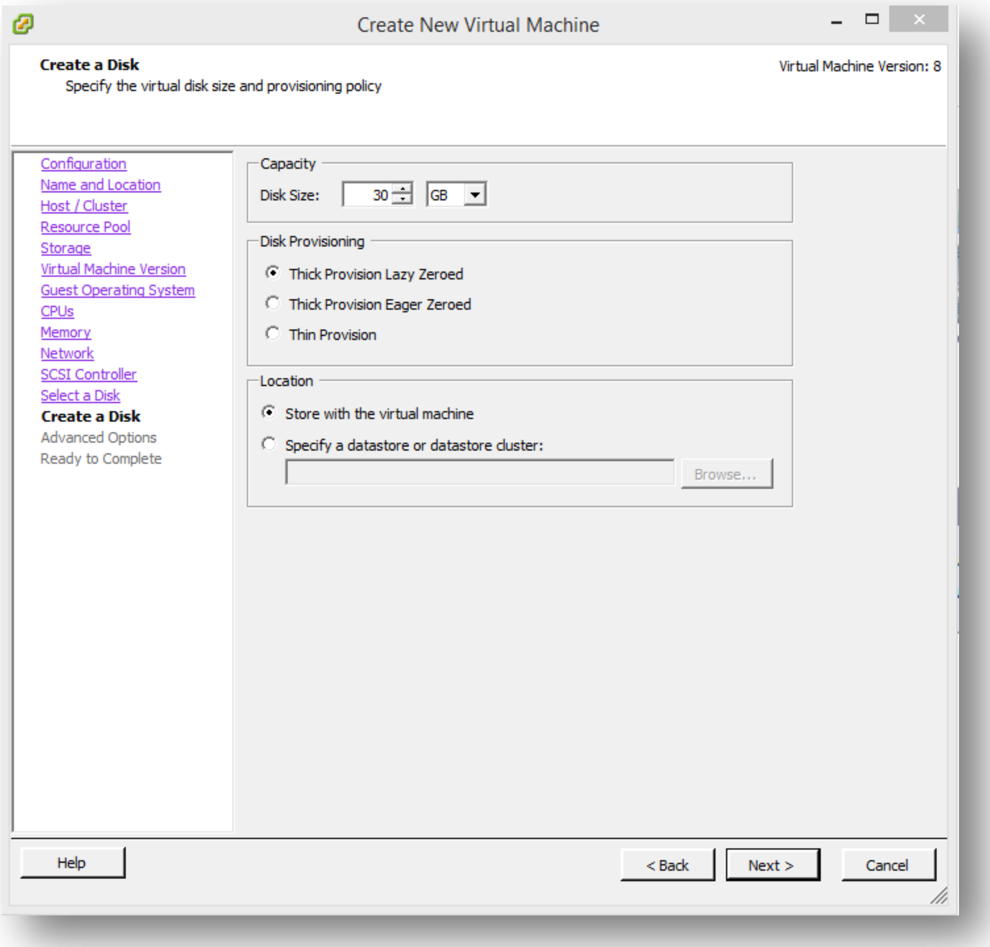
	Network	Adapter	Connect at Power On
NIC 1:	EPM DMZ (EPM Mobile-DMZ)	E1000	☑

If supported by this virtual machine version, more than 4 NICs can be added after the virtual machine is created, via its Edit Settings dialog.

Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supported for various guest operating systems and hosts.

11. Choose a SCSI Controller, taking into account any future fall-over requirements. **Next** to continue.
12. Select **Create a new virtual disk** and **Next.**

13. Set **Disk Size** to 30G; **Disk Provisioning** to **Thick Provisioning**:



Create a Disk
Specify the virtual disk size and provisioning policy

Virtual Machine Version: 8

Capacity
Disk Size: 30 GB

Disk Provisioning
● Thick Provision Lazy Zeroed
○ Thick Provision Eager Zeroed
○ Thin Provision

Location
● Store with the virtual machine
○ Specify a datastore or datastore cluster:

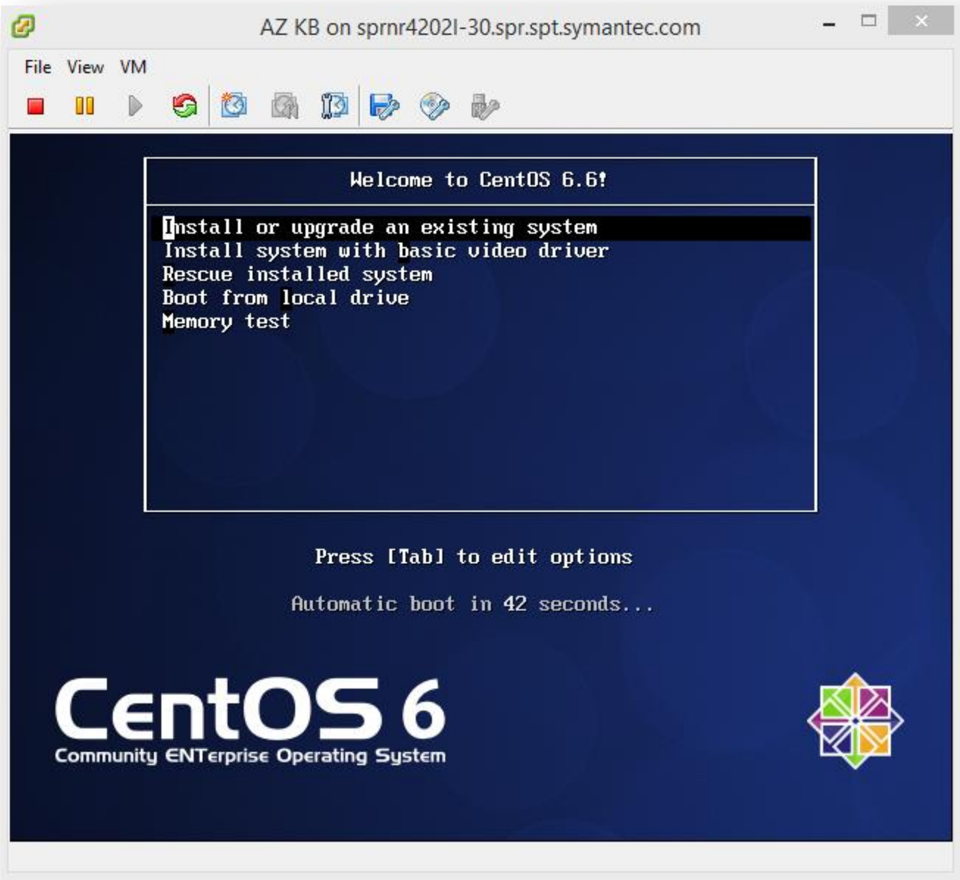
14. Set Virtual Device Node to **SCSI** and **Next**.
15. Review the settings for the new virtual machine and select **Finish** to build the VM. Build usually takes less than a minute to complete.
16. Power on the newly created virtual machine.

Install CentOS/RHEL 6.5 (HOWTO110253)

Important: For this guide, the minimal CentOS/RHEL 6.5 is shown; the minimal CentOS/RHEL 6.6 ISO also is compatible. It is highly recommended to use the minimal ISO rather than selecting **minimal** when installing a full ISO.

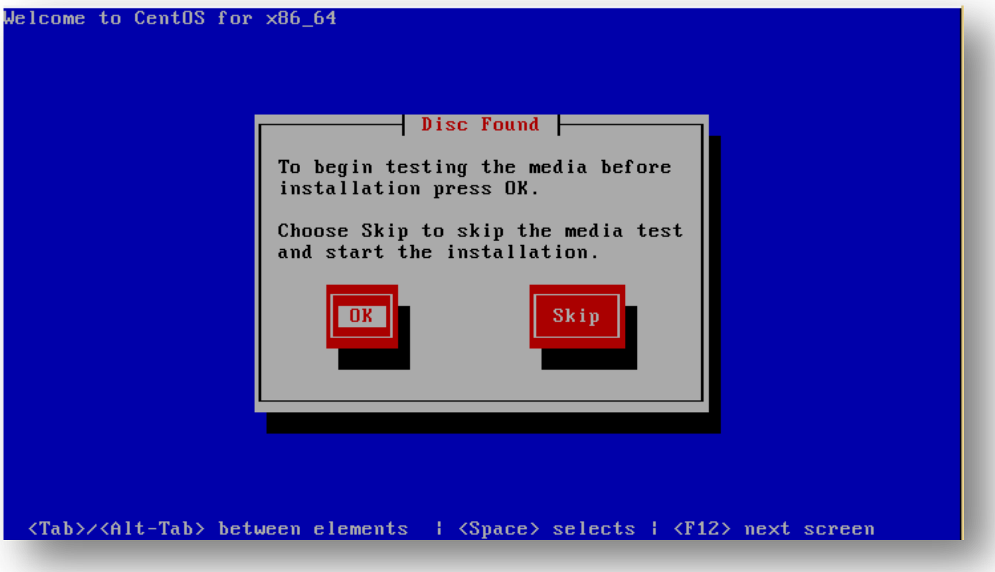
Download CentOS 6.5 (HOWTO110236)

17. Download the CentOS 6.5 minimal operating system to a workstation by clicking here and navigating to the **USA HTTP Link > 6.5 > isos > x86_64 > CentOS-6.5-x86_64-minimal.iso**
18. After the download completes, open a console to the VM and select the (disk) icon and select **Connect to ISO on Local Disk**.
19. Browse to the CentOS 6.5 ISO and click **open**.
20. Click anywhere in the console and hit **enter**. (This forces the VM to look for a new boot source).
21. Ensure that **Install or upgrade an existing system** is selected:


AZ KB on sprnr4202l-30.spr.spt.symantec.com
File
View
VM
CentOS 6
Community ENTerprise Operating System

```
Welcome to CentOS 6.6!

Install or upgrade an existing system
Install system with basic video driver
Rescue installed system
Boot from local drive
Memory test

Press [Tab] to edit options

Automatic boot in 42 seconds...
```

22. Allow about 10 minutes (if workstation ISO is used) to load. Hit **tab** to select **Skip** and **Enter** to continue:

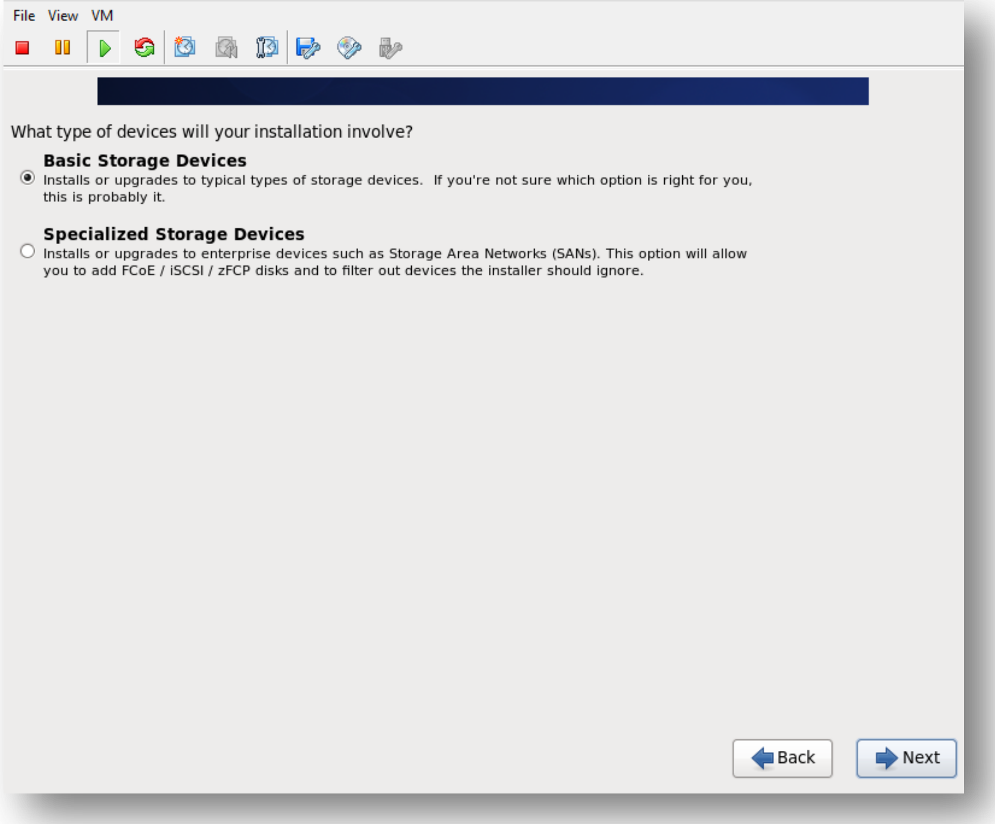


```
Welcome to CentOS for x86_64

                    Disc Found
  To begin testing the media before
  installation press OK.

  Choose Skip to skip the media test
  and start the installation.

        OK                 Skip

<Tab>/<Alt-Tab> between elements  | <Space> selects | <F12> next screen
```

23. **Next** to continue.
24. Select **English (English)** for the install language and **Next.**
25. If using a non-QWERTY keyboard, select the language used on the workstation and click **Next** to continue.

Note: When typing passwords into a remove VM the keyboard selection can cause an incorrect password to be created. Be sure that the keyboard selection is the preferred before continuing.

26. Select **Basic Storage Devices** and **Next:**

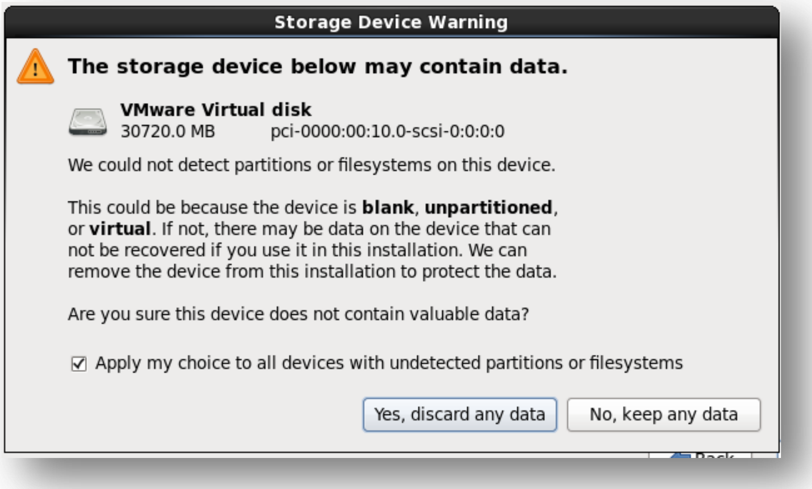


What type of devices will your installation involve?

● **Basic Storage Devices**
Installs or upgrades to typical types of storage devices. If you're not sure which option is right for you, this is probably it.

○ **Specialized Storage Devices**
Installs or upgrades to enterprise devices such as Storage Area Networks (SANs). This option will allow you to add FCoE / iSCSI / zFCP disks and to filter out devices the installer should ignore.

27. When prompted click **Yes, discard any data:**


Storage Device Warning

The storage device below may contain data.

VMware Virtual disk
30720.0 MB pci-0000:00:10.0-scsi-0:0:0:0

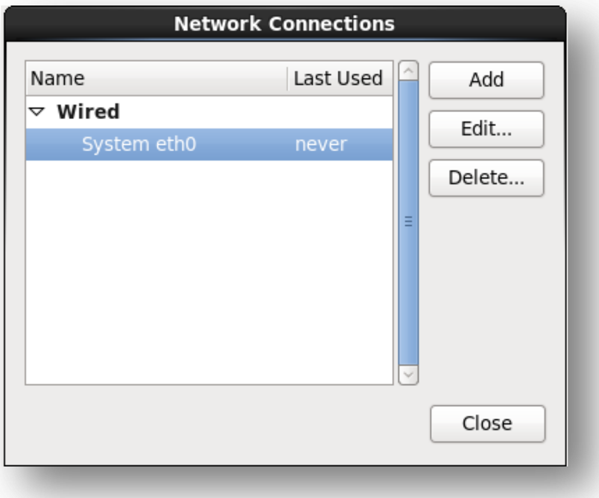
We could not detect partitions or filesystems on this device.

This could be because the device is **blank**, **unpartitioned**, or **virtual**. If not, there may be data on the device that can not be recovered if you use it in this installation. We can remove the device from this installation to protect the data.

Are you sure this device does not contain valuable data?

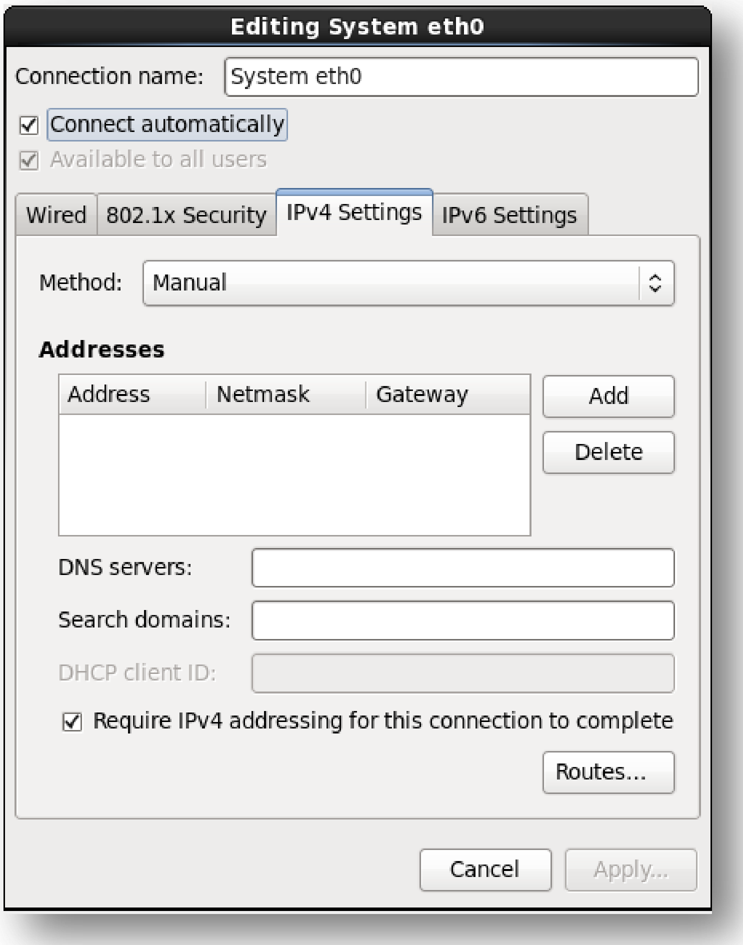
☑ Apply my choice to all devices with undetected partitions or filesystems

28. If the tenant's hostname were **mobile.**mydomain.com, enter **mobile** for the hostname. Enter the server's hostname replacing **localhost.localdomain** and click **Configure Network**.
29. Select **System eth0** (or the available NIC) and click **Edit…**:


Network Connections

Name	Last Used
Wired	
System eth0	never

30. Within the **Editing System eth0** window, check the box next to **Connect automatically** and click on the **IPv4 Settings** tab:



Connection name: System eth0

☑ Connect automatically

☑ Available to all users

Method: Manual

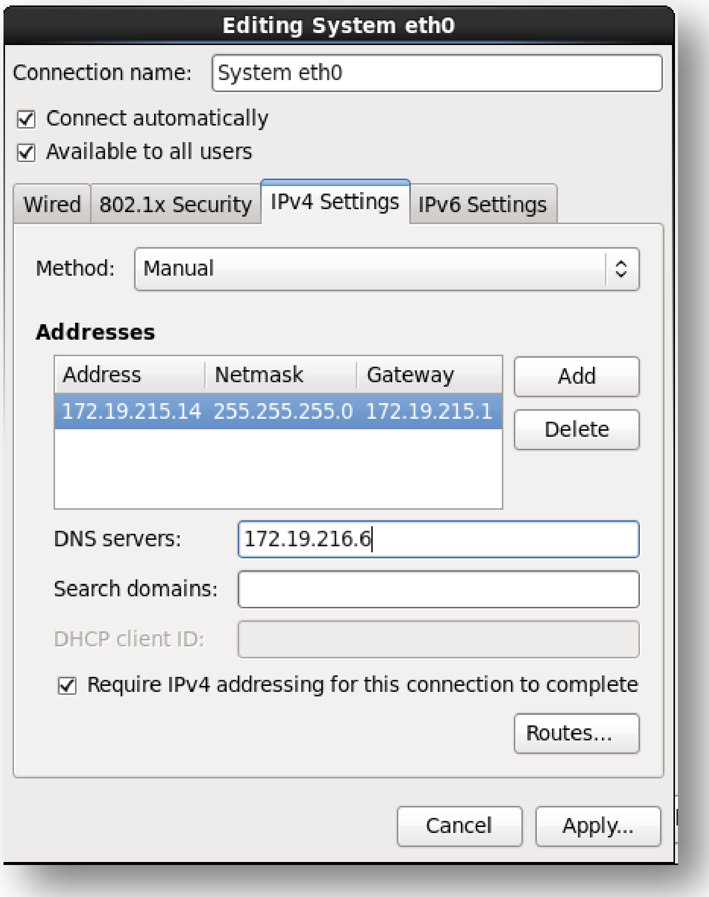
☑ Require IPv4 addressing for this connection to complete

31. For **Method** select **Manual** and in the **Addresses** area click **Add** and enter the internet protocol (IP) information for this server.

Important: It is necessary for the Mobility Suite Front End (FE) to be able to fully communicate, without outbound proxy. See HOWTO94496 for a complete list of required ports.

32. Confirm the IP information and **Apply:**

Note: The IP information for this server will vary from the example shown below. Obtain a valid static IP address for the organization’s systems administrator.



Connection name: System eth0

☑ Connect automatically

☑ Available to all users

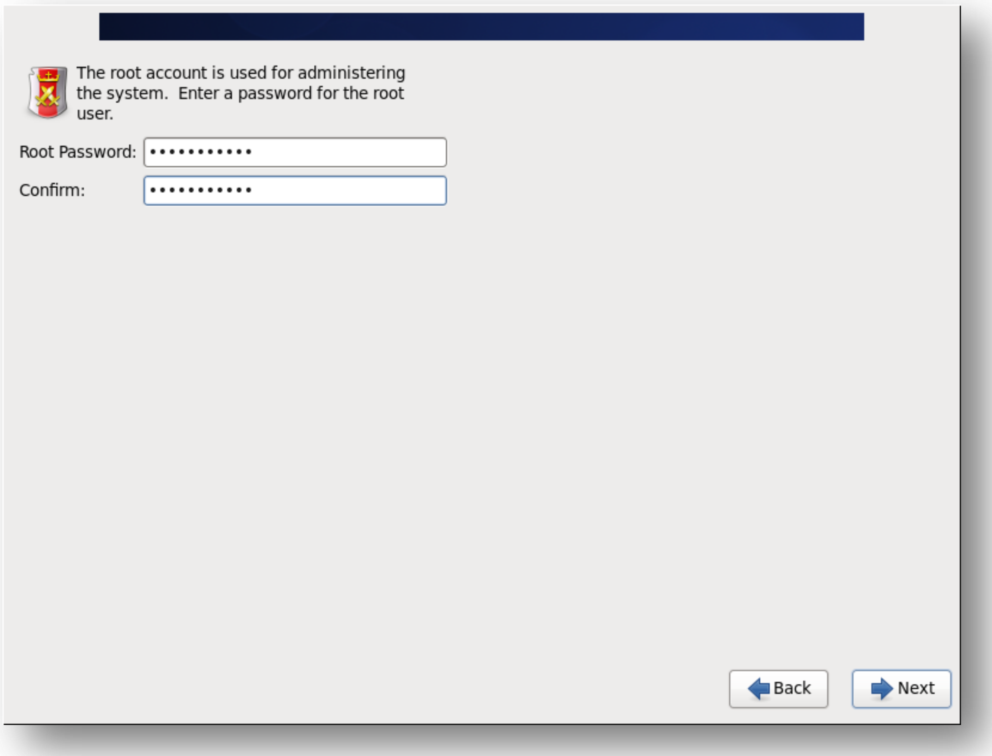
Method: Manual

Address	Netmask	Gateway
172.19.215.14	255.255.255.0	172.19.215.1

DNS servers: 172.19.216.6

☑ Require IPv4 addressing for this connection to complete

33. Click **Close** on the Network Connections sub-window and **Next** on the parent window.
34. Ensure that the **System clock uses UTC** is checked and the **America/Los Angeles** time zone is selected and **Next**.
35. Enter and confirm a complex root password and **Next:**

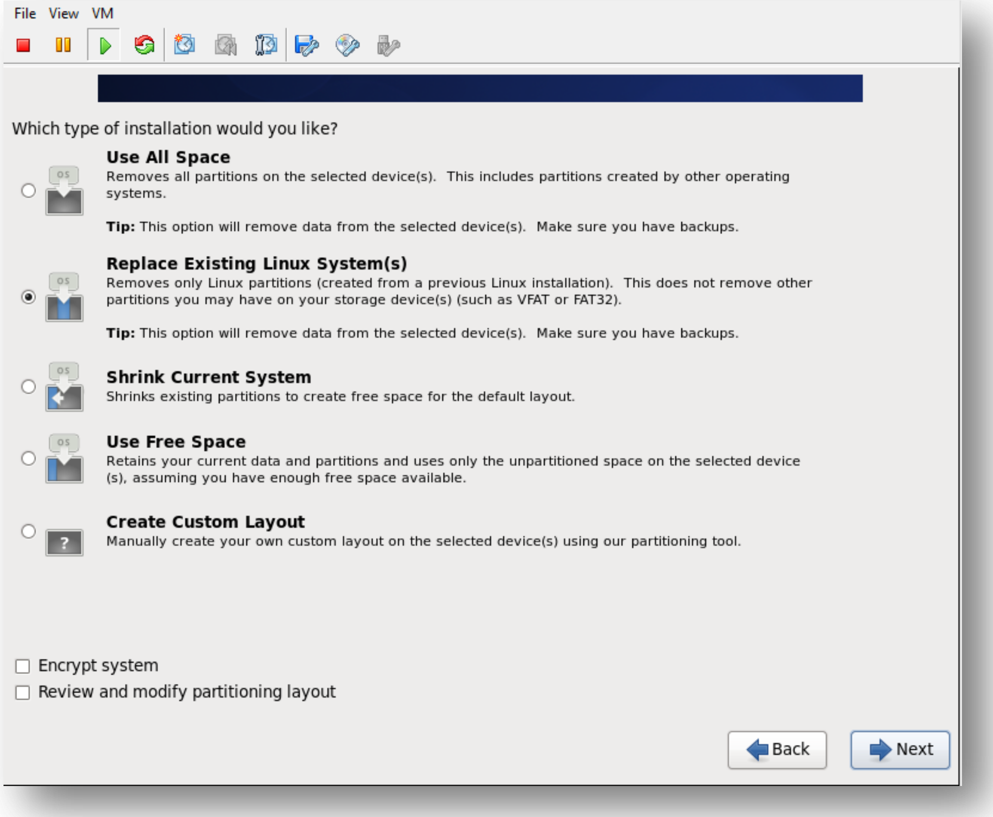


The root account is used for administering the system. Enter a password for the root user.

Root Password: •••••••••••

Confirm: •••••••••••

36. Use the default installation type: **Replace Existing Linux System(s)** and leave the encryption and partition layout options unchecked:



Which type of installation would you like?

○ **Use All Space**
Removes all partitions on the selected device(s). This includes partitions created by other operating systems.

Tip: This option will remove data from the selected device(s). Make sure you have backups.

● **Replace Existing Linux System(s)**
Removes only Linux partitions (created from a previous Linux installation). This does not remove other partitions you may have on your storage device(s) (such as VFAT or FAT32).

Tip: This option will remove data from the selected device(s). Make sure you have backups.

○ **Shrink Current System**
Shrinks existing partitions to create free space for the default layout.

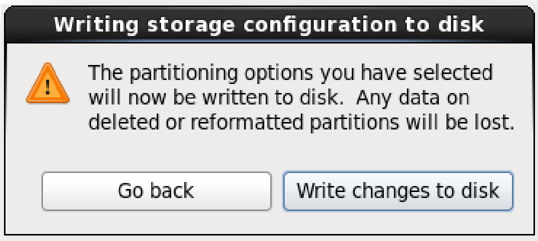
○ **Use Free Space**
Retains your current data and partitions and uses only the unpartitioned space on the selected device (s), assuming you have enough free space available.

○ **Create Custom Layout**
Manually create your own custom layout on the selected device(s) using our partitioning tool.

□ Encrypt system

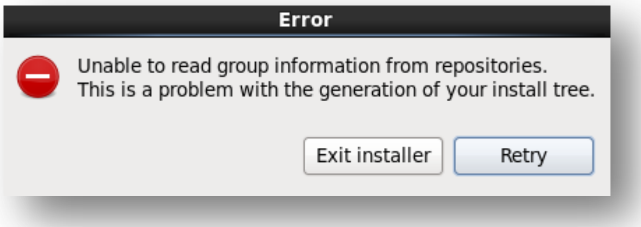
□ Review and modify partitioning layout

37. When prompted select **Write changes to disk:**


Writing storage configuration to disk

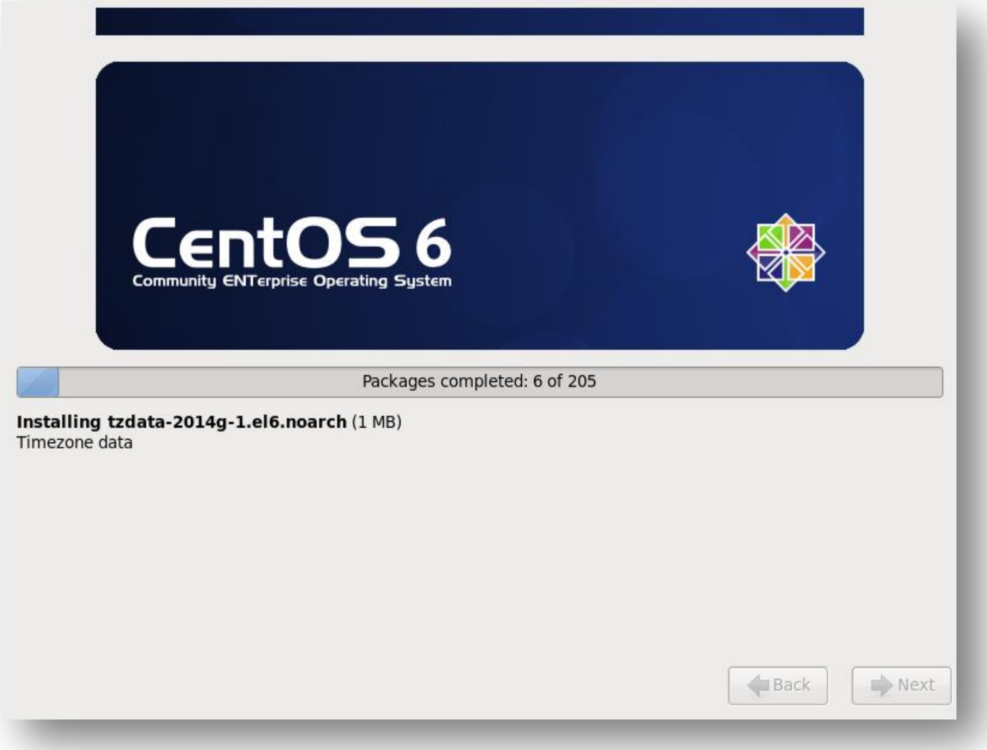
The partitioning options you have selected will now be written to disk. Any data on deleted or reformatted partitions will be lost.

Note: If the following error occurs reconnect the CentOS ISO to the VM console (steps 18-19) and select **Retry** Allow about 10 minutes for the disk to reconnect. If that fails, select **Exit installer**, power off and delete the VM. Repeat steps 1-35 and ensure that there is a solid connection between the workstation and VMware host:


Error

Unable to read group information from repositories. This is a problem with the generation of your install tree.

38. If prompted for installation type, select **Minimal**.
39. The OS installation should now proceed. This can take up to 1 hour depending on host performance/utilization factors :



Packages completed: 6 of 205

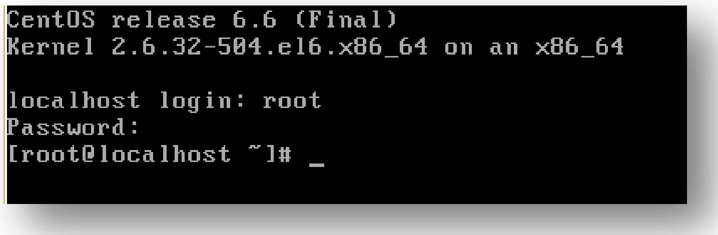
Installing tzdata-2014g-1.el6.noarch (1 MB)
Timezone data

40. Once the CentOS installation is complete, select **Reboot.**

Tip: To view a detailed (retro) startup menu press the **F2** key.

Note: If the boot priority is set to boot from optical drive, the CentOS ISO needs to be un-mounted from the system.

41. Log into the system as **root** using the complex password created during the OS installation. Continue to Root Shell Access:


```
CentOS release 6.6 (Final)
Kernel 2.6.32-504.el6.x86_64 on an x86_64

localhost login: root
Password:
[root@localhost ~]# _
```

Configure Networking and Firewall (HOWTO110254)

Root Shell Access

1. The **#** symbol at the beginning of the command line signifies that this session has root privileges.

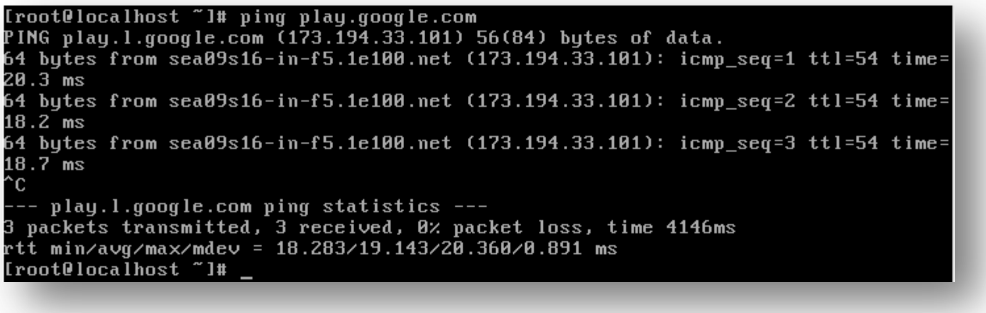
Note: If the server was deployed using a template and a user account is needed to access the console. Log into the console with the provided user credentials. Type **su** and hit **Enter** to elevate the session to root privileges. If the sudoer's methodology is being used type **sudo su** to elevate the account. Prefixing any command with **sudo** will elevate that command with root privileges. Mobility Suite requires full root shell access to complete its installation.

2. Continue to Confirm Network Connectivity.

Tip: Press the **Tab** key after typing a few characters of the filename listed in a command, it should finish the remainder of it. This should make typing commands quicker. Pressing **Tab** twice will display all the available options beginning with that word, file or directory.

Confirm Network Connectivity

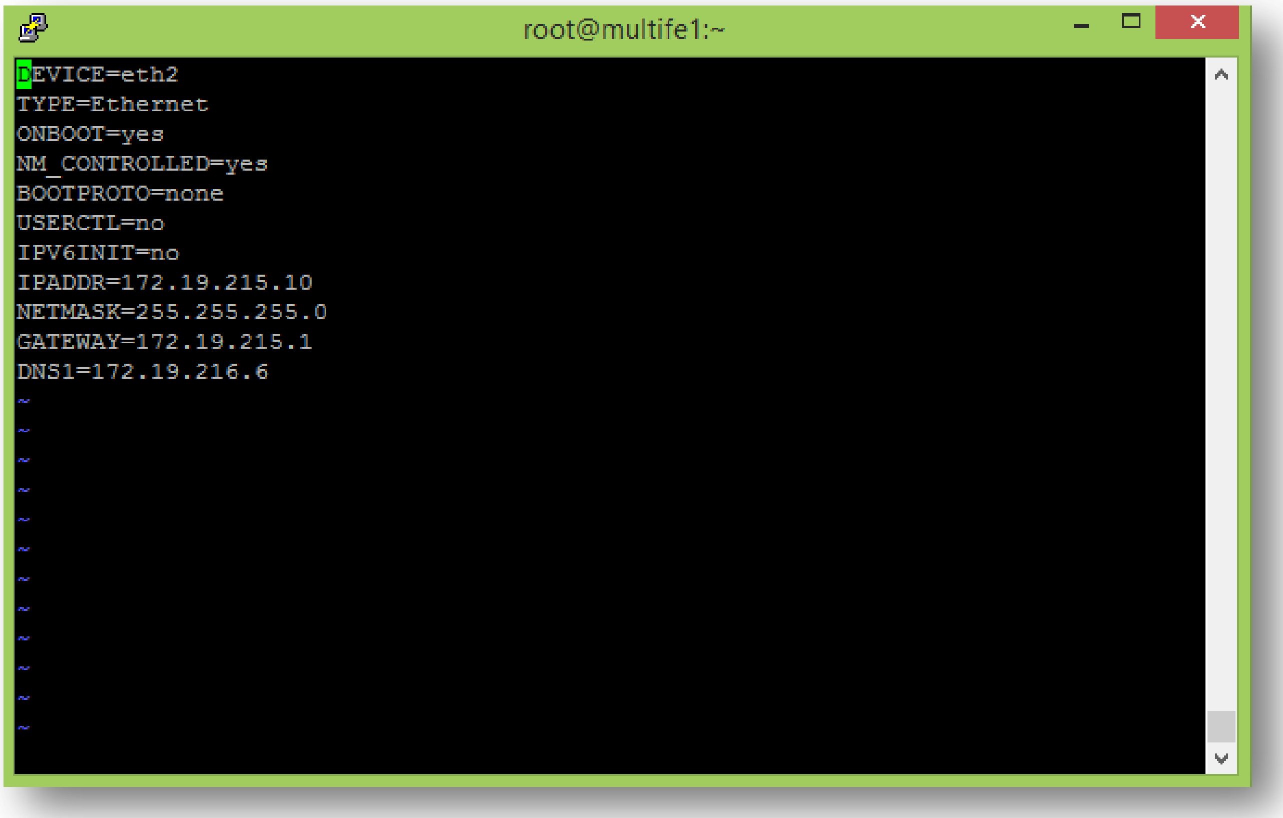
1. Verify Internet communication by typing, as root: **ping play.google.com**, to cancel the echo: while holding down the **Ctrl** key press **c** this will return the console back to the **root** shell:



```
[root@localhost ~]# ping play.google.com
PING play.l.google.com (173.194.33.101) 56(84) bytes of data.
64 bytes from sea09s16-in-f5.1e100.net (173.194.33.101): icmp_seq=1 ttl=54 time=
20.3 ms
64 bytes from sea09s16-in-f5.1e100.net (173.194.33.101): icmp_seq=2 ttl=54 time=
18.2 ms
64 bytes from sea09s16-in-f5.1e100.net (173.194.33.101): icmp_seq=3 ttl=54 time=
18.7 ms
^C
--- play.l.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 4146ms
rtt min/avg/max/mdev = 18.283/19.143/20.360/0.891 ms
[root@localhost ~]# _
```

Tip: If no ICMP response is received, verify whether ICMP is blocked or type **/sbin/ifconfig** to verify the network settings. To edit the network configuration type **vi /etc/sysconfig/network-scripts/ifcfg-eth0** and **Enter.** A vi edit view will appear. Type **i** to begin editing. The up, down, left & right arrows must be used to navigate through this configuration file. Make the appropriate changes to the network settings. Hit the **Esc** key once and while holding **Shift** press the **:** (colon) key once and release. Now type **wq** and hit **Enter**; this will write the changes to the file. To exit without making any changes, instead of **wq** type **q!** and hit **Enter.** Now restart the network services to reapply this configuration script by typing, as root: **service network restart** and **Enter**. Repeat these steps until the correct network configuration is obtained.

For example:

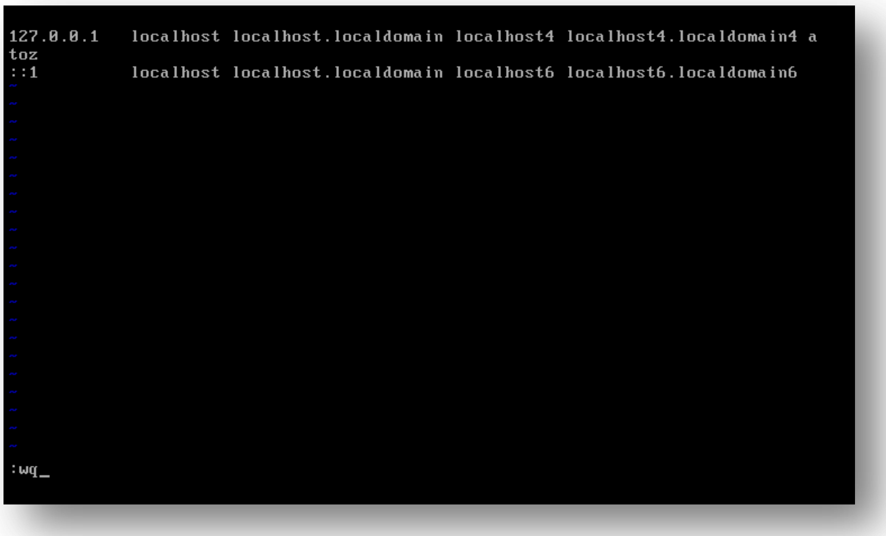


```
DEVICE=eth2
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=none
USERCTL=no
IPV6INIT=no
IPADDR=172.19.215.10
NETMASK=255.255.255.0
GATEWAY=172.19.215.1
DNS1=172.19.216.6
~
~
~
~
~
~
~
~
~
~
~
~
```

Important: A working network configuration is required before proceeding further. It is highly recommended to set the **ONBOOT=** to **yes** as shown above. The hardware and ID of the NIC may be shown but they are optional. Remember that after any changes are made it will be necessary to restart the network services.

Tip: Quick guide to **vi**:
i → Insert
Esc key → End insert mode and returns to command mode which allows the below two commands:
:q! → Colon followed by **q!** quits without making any changes.
:wq → Colon followed by **wq** writes and quits, saving changes.

2. Ping the server's hostname, which was set in step 28 of Install CentOS 6.5 (HOWTO110253). The return should be on the IPV4 loopback address: **127.0.0.1**. If it is not then **vi** into **/etc/hosts** and append the server's hostname to the end of the line containing **127.0.0.1**:



```
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4 a
toz
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:wq_
```

3. Follow the **Tip: Quick guide to vi**; writing and saving the changes to the file.
4. Restart network services by entering the following into the console:
   sudo service network restart
5. Ping the server's hostname a second time to ensure that it resolves to 127.0.0.1.

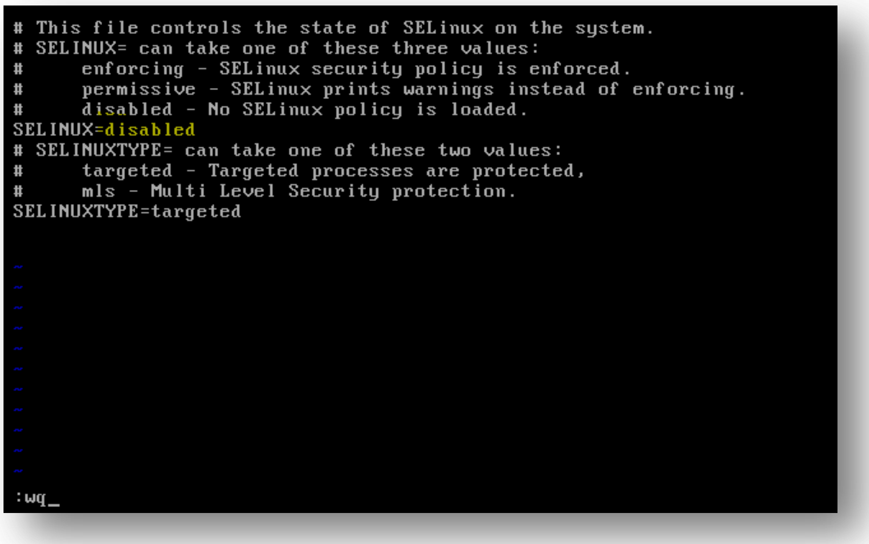
Tip: On-box RabbitMQ (installed as part of Mobility) will bind to 127.0.0.1 using the server's hostname.

6. Once network communication is confirmed continue to Disable SELinux.

Disable SELinux (HOWTO110257)

Note: Disabling SELinux is not required for mobility suite as the Bootstrapping step will automatically add the required exceptions to SELinux. For more information on hardening Linux for Mobility see HOWTO110230.

1. To disable selinux edit its configuration file by typing, as root:
   vi /etc/selinux/config and **Enter.** A vi edit view will appear.
2. Type **i** to begin editing. The up, down, left & right arrows must be used to navigate through this configuration.
3. Change the line: SELINUX=enforcing to **SELINUX=disabled**. Hit the **Esc** key once, while holding **Shift** press the **:** (colon) key once and release.
4. Now type **wq** and hit **Enter**; this will write the changes to the file. To exit without making any changes, instead of **wq** type **q!** and hit **Enter.**



```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted


~
~
~
~
~
~
~
~
~
~
~
:wq_
```

5. Coninute to Configure IPTables.

Configure IPTables (HOWTO110255)

For more information on hardening Linux for Mobility see HOWTO98546.

Using IPTables (HOWTO110235):

Add 80 and 443 to the IPTables chain by entering the following lines, as root:

```
/sbin/iptables --insert INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
/sbin/iptables --insert INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
/etc/init.d/iptables save
```

No IPTables (HOWTO110255):

If the Mobility Suite FE (server) is deployed behind a firewall and IPTABLES is not needed, run the following two commands, as root:

```
/etc/init.d/iptables stop
chkconfig iptables off
```

For more information on ports used by Symantec Mobility Suite see HOWTO94496. More information on IPTables may be found at http://wiki.centos.org/HowTos/Network/IPTables.

Once IPTables is configured, as needed, continue to SSH.

SSH (HOWTO110256)

1. To install SSH, as root enter:
   ```
   sudo yum –y install openssh-server openssh-clients
   ```
2. Set the service to start with the machine:
   ```
   chkconfig sshd on
   ```
3. Start the service:
   ```
   service sshd start
   ```
4. Make sure port 22 is opened:
   ```
   netstat –tulpn | grep :22
   ```

   Look for a link showing TCP 22 as open.

Tip: The **| (pipe)** symbol in the above command can is **shift** (key) **+** \

5. If port 22 is not open, enter the following two lines into terminal:
   ```
   /sbin/iptables --insert INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
   /etc/init.d/iptables save
   ```
6. Reboot the system by typing:
   ```
   sudo reboot
   ```

Tip: Now is a good time to take a snapshot of the current hard drive state.

7. Once SSH is fully configured continue to Obtain the Symantec Mobility ISO.

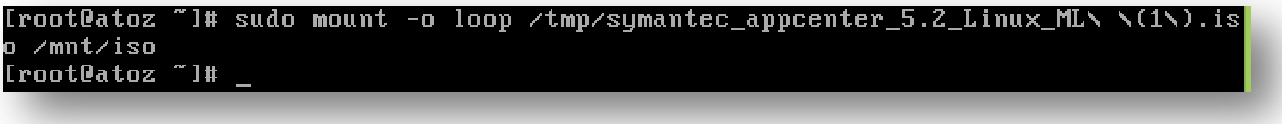
Obtain the Symantec Mobility Suite ISO

1. Once the system restarts, log back into the console, as root.
2. Install **wget** by entering the following:
   ```
   sudo yum –y install wget
   ```
3. The Symantec Mobility ISO may be either uploaded to the FE see How to transfer files to a Linux machine or downloaded using **wget…**
4. Download the Symantec Mobility Suite ISO by typing the following, as root:
   sudo wget <Direct link to the Symantec Mobility 5.2 or later ISO> **/tmp/symantec.iso**

Note: To obtain a valid copy of Mobility Suite or the direct download-link, contact a Symantec Sales Engineer or Partner.

Important: The Symantec Mobility ISO must be downloaded onto the Linux machine and not mounted through VMWare interface.

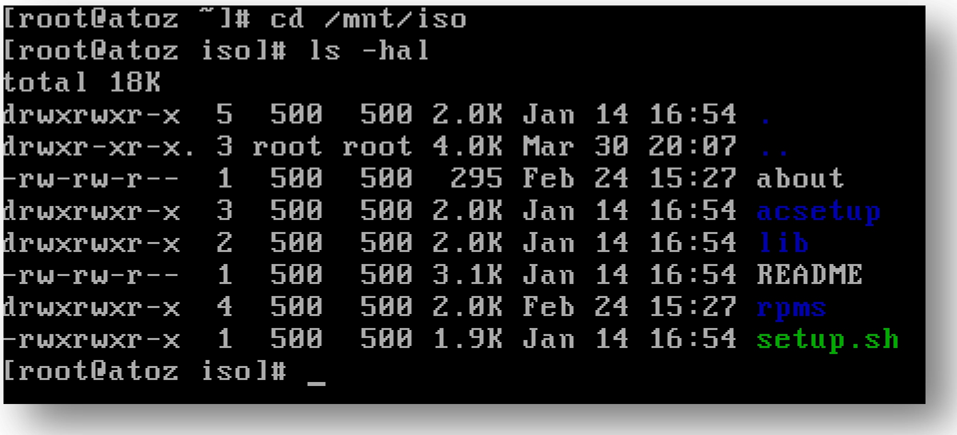
5. Mount the **symantec.iso** by entering the following two lines:
   ```
   mkdir /mnt/iso
   sudo mount –o loop /tmp/symantec.iso /mnt/iso
   ```



```
[root@atoz ~]# sudo mount -o loop /tmp/symantec_appcenter_5.2_Linux_ML\ \(1\).is
o /mnt/iso
[root@atoz ~]# _
```

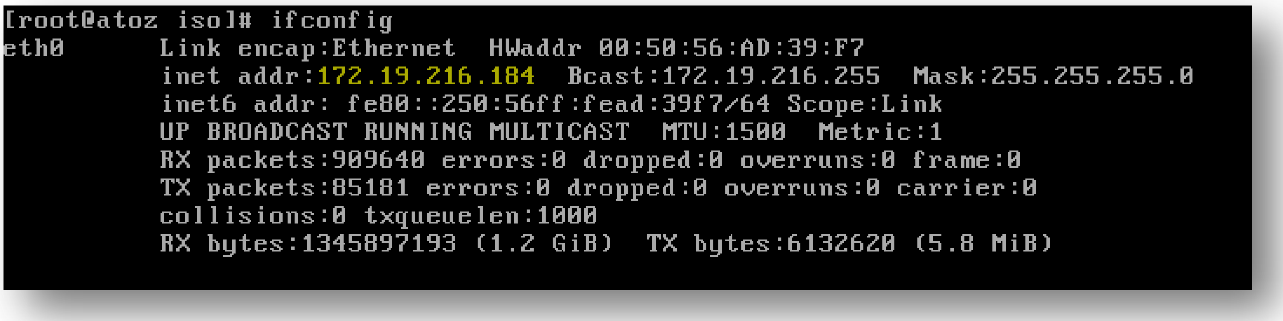
Note: In this step, the ISO name is **symantec.iso**, substitute the actual name and/or path to the ISO.

6. Change the working directory to the mounted location:
   cd /mnt/iso
7. Verify the contents of the ISO were properly loaded by entering:
   ls –hal



```
[root@atoz ~]# cd /mnt/iso
[root@atoz iso]# ls -hal
total 18K
drwxrwxr-x  5  500  500 2.0K Jan 14 16:54 .
drwxr-xr-x. 3 root root 4.0K Mar 30 20:07 ..
-rw-rw-r--  1  500  500  295 Feb 24 15:27 about
drwxrwxr-x  3  500  500 2.0K Jan 14 16:54 acsetup
drwxrwxr-x  2  500  500 2.0K Jan 14 16:54 lib
-rw-rw-r--  1  500  500 3.1K Jan 14 16:54 README
drwxrwxr-x  4  500  500 2.0K Feb 24 15:27 rpms
-rwxrwxr-x  1  500  500 1.9K Jan 14 16:54 setup.sh
[root@atoz iso]# _
```

8. Write down the server’s IP address (if issued via DHCP) that is displayed after entering the following command:
   /sbin/ifconfig



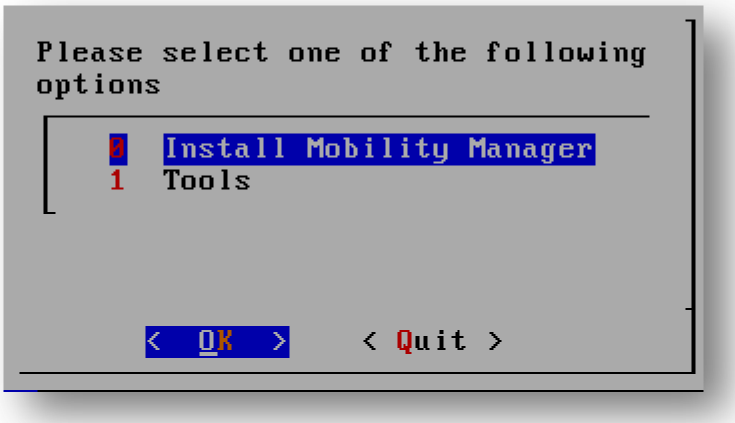
```
[root@atoz iso]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:AD:39:F7
          inet addr:172.19.216.184  Bcast:172.19.216.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fead:39f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:909640 errors:0 dropped:0 overruns:0 frame:0
          TX packets:85181 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1345897193 (1.2 GiB)  TX bytes:6132620 (5.8 MiB)
```

9. After the ISO is successfully mounted, as shown above, continue to Installation Part I.

Installation Part I (HOWTO110258)

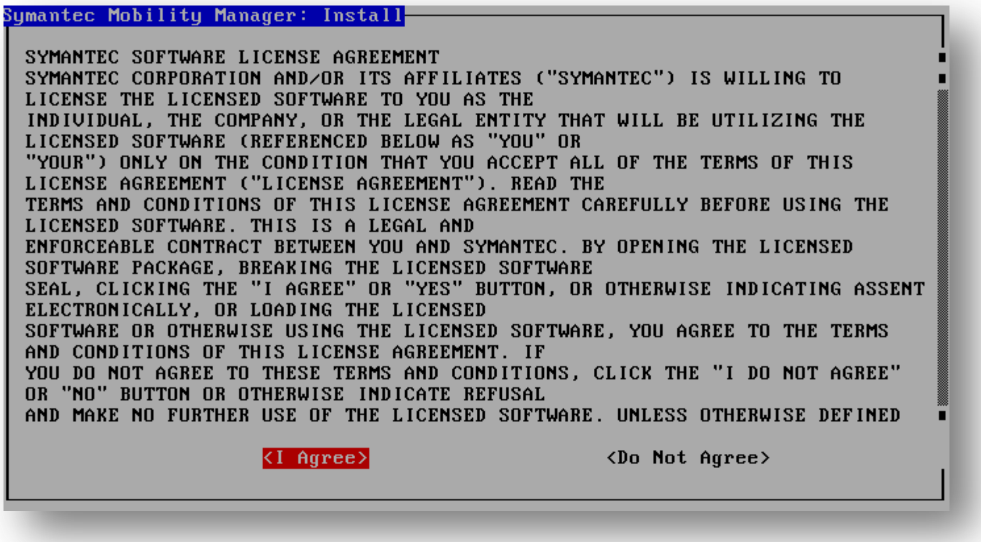
1. First install three required packages by entering the following, as root:
   sudo yum -y install unzip libtool-ltdl mysql
2. Begin the Mobility Suite installation by entering the following, as root:
   sudo ./setup.sh
3. Ensure that **Install Mobility Manager** is selected and **OK** to continue.

Tip: Use the **Tab** and **arrow** keys to toggle the selection.



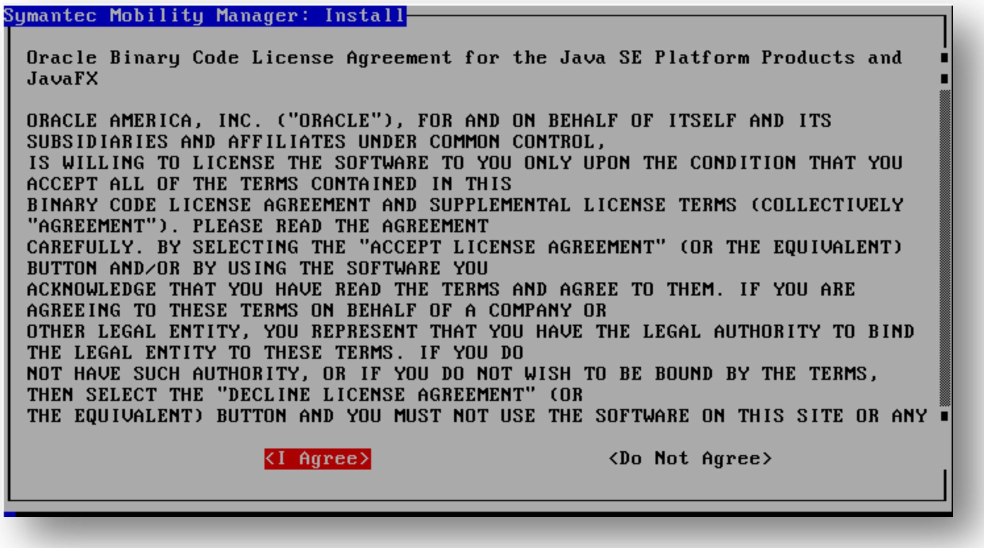
```
Please select one of the following
options

    0   Install Mobility Manager
    1   Tools

      <  OK  >        < Quit >
```

4. Agreeing to the Symantec Corporation terms will allow the installation to proceed:



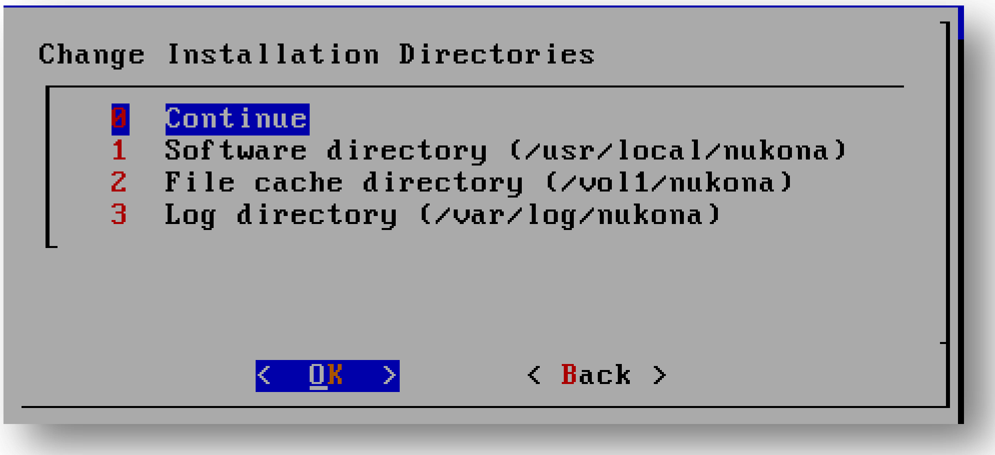
```
SYMANTEC SOFTWARE LICENSE AGREEMENT
SYMANTEC CORPORATION AND/OR ITS AFFILIATES ("SYMANTEC") IS WILLING TO
LICENSE THE LICENSED SOFTWARE TO YOU AS THE
INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE
LICENSED SOFTWARE (REFERENCED BELOW AS "YOU" OR
"YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS
LICENSE AGREEMENT ("LICENSE AGREEMENT"). READ THE
TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE
LICENSED SOFTWARE. THIS IS A LEGAL AND
ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THE LICENSED
SOFTWARE PACKAGE, BREAKING THE LICENSED SOFTWARE
SEAL, CLICKING THE "I AGREE" OR "YES" BUTTON, OR OTHERWISE INDICATING ASSENT
ELECTRONICALLY, OR LOADING THE LICENSED
SOFTWARE OR OTHERWISE USING THE LICENSED SOFTWARE, YOU AGREE TO THE TERMS
AND CONDITIONS OF THIS LICENSE AGREEMENT. IF
YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE"
OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL
AND MAKE NO FURTHER USE OF THE LICENSED SOFTWARE. UNLESS OTHERWISE DEFINED
```

5. Same for Java, as above:



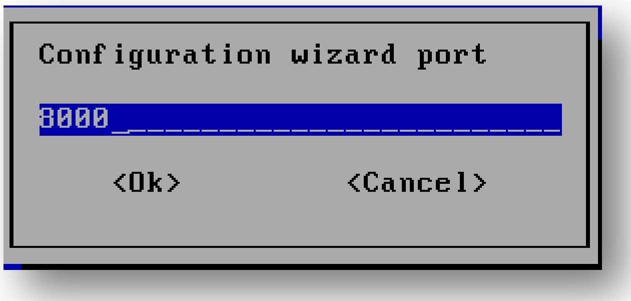
```
Oracle Binary Code License Agreement for the Java SE Platform Products and
JavaFX

ORACLE AMERICA, INC. ("ORACLE"), FOR AND ON BEHALF OF ITSELF AND ITS
SUBSIDIARIES AND AFFILIATES UNDER COMMON CONTROL,
IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU
ACCEPT ALL OF THE TERMS CONTAINED IN THIS
BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY
"AGREEMENT"). PLEASE READ THE AGREEMENT
CAREFULLY. BY SELECTING THE "ACCEPT LICENSE AGREEMENT" (OR THE EQUIVALENT)
BUTTON AND/OR BY USING THE SOFTWARE YOU
ACKNOWLEDGE THAT YOU HAVE READ THE TERMS AND AGREE TO THEM. IF YOU ARE
AGREEING TO THESE TERMS ON BEHALF OF A COMPANY OR
OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE LEGAL AUTHORITY TO BIND
THE LEGAL ENTITY TO THESE TERMS. IF YOU DO
NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO BE BOUND BY THE TERMS,
THEN SELECT THE "DECLINE LICENSE AGREEMENT" (OR
THE EQUIVALENT) BUTTON AND YOU MUST NOT USE THE SOFTWARE ON THIS SITE OR ANY
```

6. Take note of the default directories and **OK** to continue:



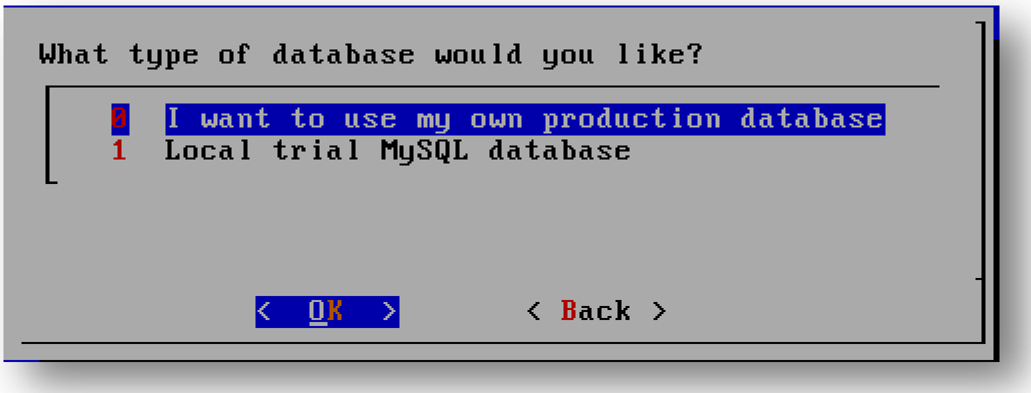
```
Change Installation Directories

    0  Continue
    1  Software directory (/usr/local/nukona)
    2  File cache directory (/vol1/nukona)
    3  Log directory (/var/log/nukona)
```

7. Set the HTTP **Configuration wizard port** as 8000 (default) and **Tab** to **OK** to continue:



```
Configuration wizard port

8000
```

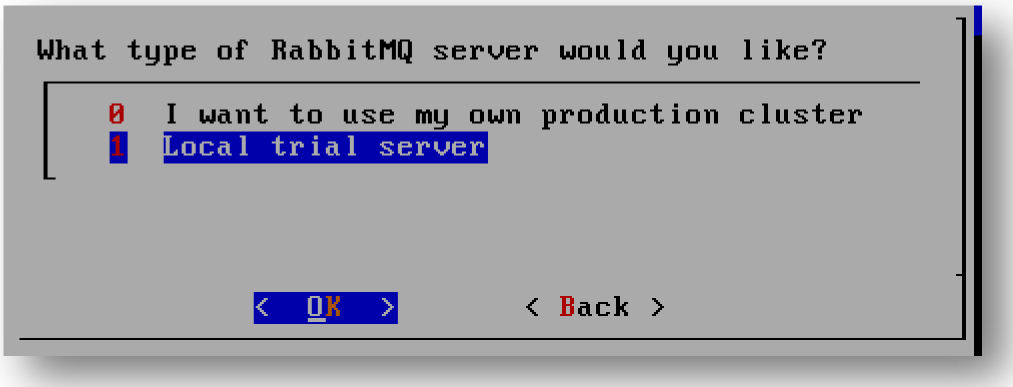
8. Select: **I want to use my own production database** option and **OK**:



```
What type of database would you like?

    0  I want to use my own production database
    1  Local trial MySQL database
```

Note: The local-trial-database is not recommended for a production environment. For a Proof of Concept (POC) managing less than 250 devices, the trial database will be sufficient.

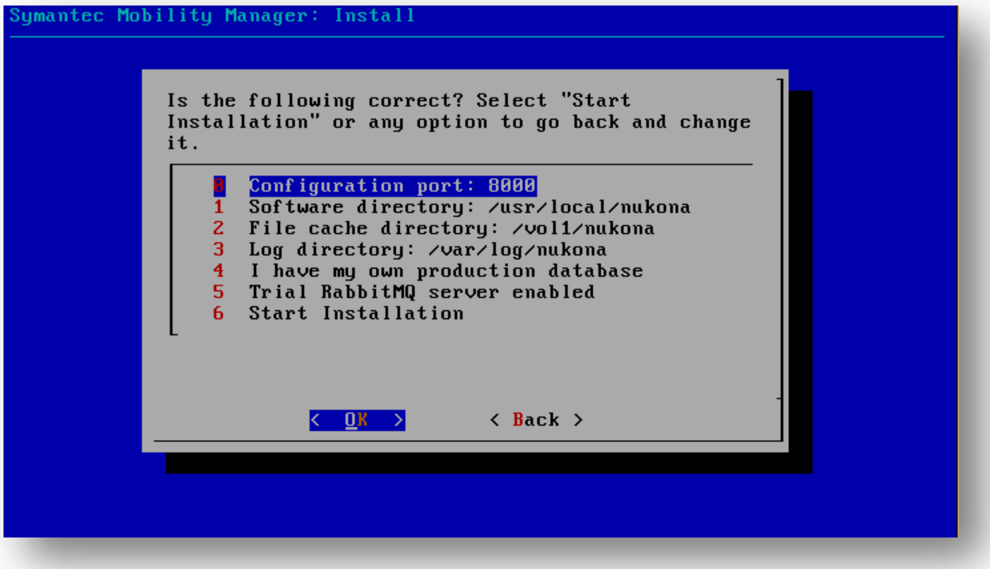
9. For deployments managing less than 15,000 devices select **Local trial server**, otherwise an off-box RabbitMQ server and fall-over server must be created see HOWTO107258



```
What type of RabbitMQ server would you like?

    0  I want to use my own production cluster
    1  Local trial server
```

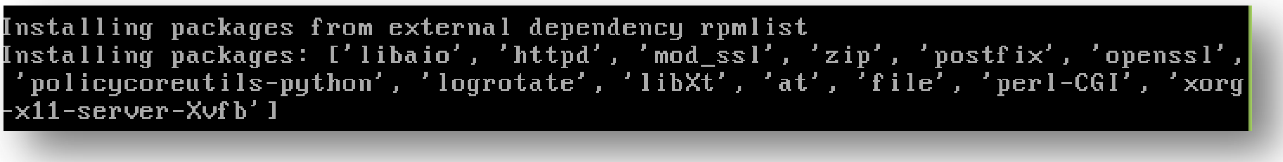
Note: The local trial RabbitMQ instance may only be accessed from the local host, a future off-box RabbitMQ server may be added at a later time.

10. After reviewing the configuration, **arrow-down** to select **Start Installation** and **OK** to continue.



```
Symantec Mobility Manager: Install

    Is the following correct? Select "Start
    Installation" or any option to go back and change
    it.

        0   Configuration port: 8000
        1   Software directory: /usr/local/nukona
        2   File cache directory: /vol1/nukona
        3   Log directory: /var/log/nukona
        4   I have my own production database
        5   Trial RabbitMQ server enabled
        6   Start Installation

              <  OK  >          < Back >
```

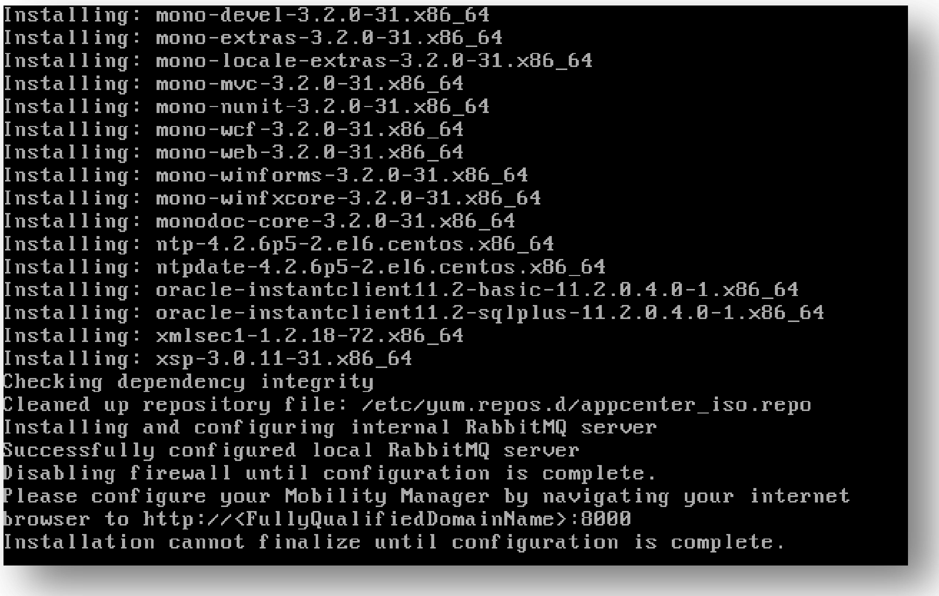
11. The primary installation will take about 10-30 minutes to complete:



```
Installing packages from external dependency rpmlist
Installing packages: ['libaio', 'httpd', 'mod_ssl', 'zip', 'postfix', 'openssl',
 'policycoreutils-python', 'logrotate', 'libXt', 'at', 'file', 'perl-CGI', 'xorg
-x11-server-Xvfb']
```

Tip: If there is any problem accessing the yum repositories verify that there is outbound communication and see TECH228347.

Important: Do **not** cancel this process. When the script completes the following line will appear:
Please configure your Mobility Manager by navigating your internet browser to http://<FullyQualifiedDomainName>:8000 Installation cannot finalize until configuration is complete:



```
Installing: mono-devel-3.2.0-31.x86_64
Installing: mono-extras-3.2.0-31.x86_64
Installing: mono-locale-extras-3.2.0-31.x86_64
Installing: mono-mvc-3.2.0-31.x86_64
Installing: mono-nunit-3.2.0-31.x86_64
Installing: mono-wcf-3.2.0-31.x86_64
Installing: mono-web-3.2.0-31.x86_64
Installing: mono-winforms-3.2.0-31.x86_64
Installing: mono-winfxcore-3.2.0-31.x86_64
Installing: monodoc-core-3.2.0-31.x86_64
Installing: ntp-4.2.6p5-2.el6.centos.x86_64
Installing: ntpdate-4.2.6p5-2.el6.centos.x86_64
Installing: oracle-instantclient11.2-basic-11.2.0.4.0-1.x86_64
Installing: oracle-instantclient11.2-sqlplus-11.2.0.4.0-1.x86_64
Installing: xmlsec1-1.2.18-72.x86_64
Installing: xsp-3.0.11-31.x86_64
Checking dependency integrity
Cleaned up repository file: /etc/yum.repos.d/appcenter_iso.repo
Installing and configuring internal RabbitMQ server
Successfully configured local RabbitMQ server
Disabling firewall until configuration is complete.
Please configure your Mobility Manager by navigating your internet
browser to http://<FullyQualifiedDomainName>:8000
Installation cannot finalize until configuration is complete.
```

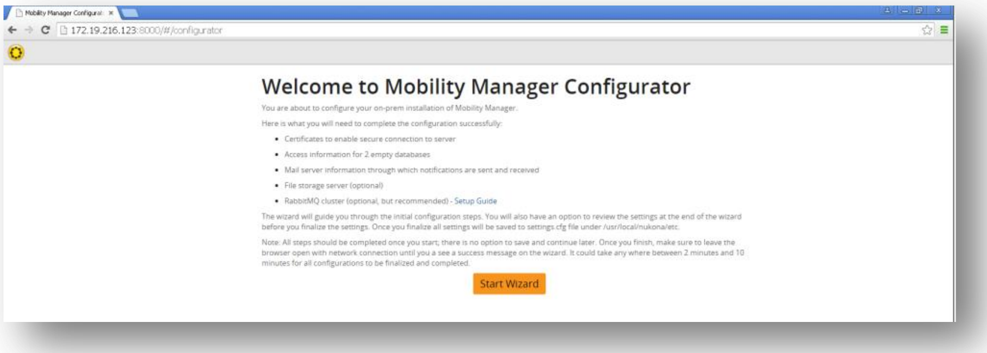
Note: If any errors in this process will be logged to **/var/log/nukona/appcenter-install.log**. If the above is not shown, reboot the server and repeat part I. To troubleshoot the Installation Part II section, refer to Troubleshooting the pre configurator Symantec Mobility Suite installation.

12. Only after the terminal shows message from the previous step, continue to Installation Part II: Bootstrapping.

Installation Part II: Bootstrapping (HOWTO110260)

Note: Do not cancel the setup.sh script; if it is terminated early before the setup is completed, repeat Installation Part I.

1. Go to a workstation running Internet Explorer (IE) 11, Chrome or Firefox; with network communication to the FE over TCP port 8000. As stated in the last two lines from the installation script above navigate to http://<FullyQualifiedDomainName>:8000 For example: http://172.19.216.123:8000 :



Mobility Manager Configurat
172.19.216.123:8000/#/configurator

Welcome to Mobility Manager Configurator

You are about to configure your on-prem installation of Mobility Manager.

Here is what you will need to complete the configuration successfully:

- Certificates to enable secure connection to server
- Access information for 2 empty databases
- Mail server information through which notifications are sent and received
- File storage server (optional)
- RabbitMQ cluster (optional, but recommended) - Setup Guide

The wizard will guide you through the initial configuration steps. You will also have an option to review the settings at the end of the wizard before you finalize the settings. Once you finalize all settings will be saved to settings.cfg file under /usr/local/nukona/etc.

Note: All steps should be completed once you start; there is no option to save and continue later. Once you finish, make sure to leave the browser open with network connection until you a see a success message on the wizard. It could take any where between 2 minutes and 10 minutes for all configurations to be finalized and completed.

2. Click **Start Wizard** to begin.

Public SSL Certificate

Note: If you already have a .pfx/.p12 file use the following article to extract the three required certificates used with Mobility: http://www.symantec.com/docs/HOWTO106999

3. Mobility Suite requires a valid Public SSL Certificate which is, most importantly, valid from the managed mobile devices. Click here to purchase an SSL certificate from VeriSign. To request a certificate from VeriSign or any other certificate authority (CA) a certificate signing request (CSR) is required. See how to create a CSR to generate the request. If a valid SSL certificate has already been issued, continue to Upload SSL Certificates to Configurator.

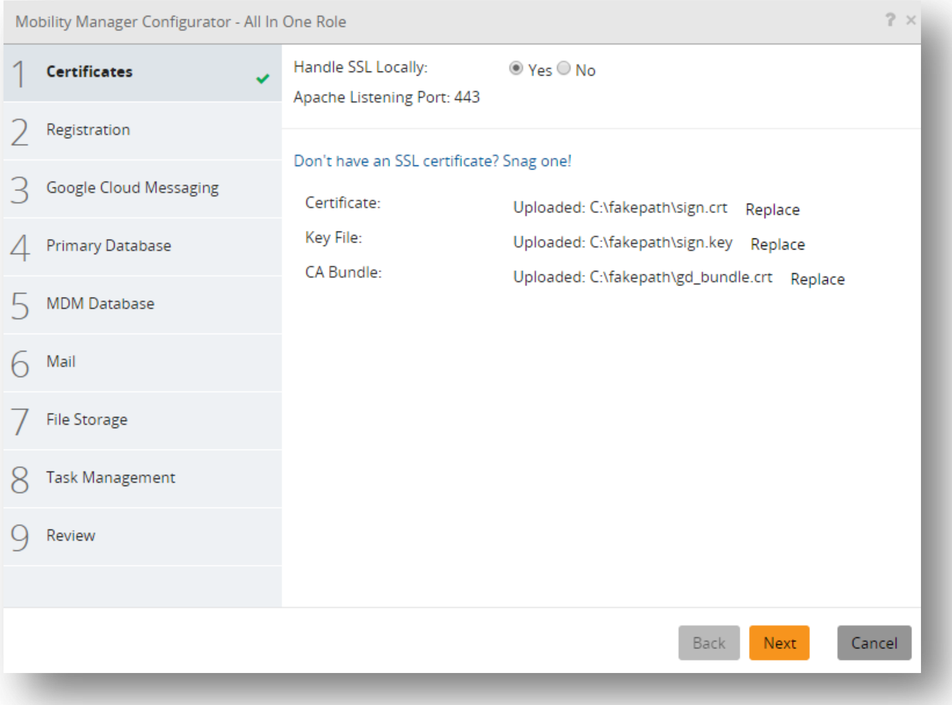
Note: Other valid public Certificate Authorities (CAs) may be used. The certificate's common name (CN) must match the published FQDN of the Mobility Server. For example, if the server's FQDN was **mobile.mydomain.com**, when making a certificate signing request (CSR) the administrator would us this FQDN for the CN in the CSR.

Upload SSL Certificates to Configurator

4. From the Internet browser select **Yes** to handle SSL locally and click **Choose File** for each of the following, browsing to the provided (or created) certificate files:
   Certificate → sign.crt
   Key File → sign.key
   CA Bundle → cacert.pem

Tip: The CA Bundle is the certificate issuer's certificate. If an intermediate certificate is required, copy and paste its certificate into this file. It is also recommended to remove all extra properties from the **sign.crt** file see: How to remove extended properties from a PEM SSL certificate (HOWTO110259) .

5. **Next** to continue:



Handle SSL Locally: ● Yes ○ No

Apache Listening Port: 443

Don't have an SSL certificate? Snag one!

Certificate: Uploaded: C:\fakepath\sign.crt Replace

Key File: Uploaded: C:\fakepath\sign.key Replace

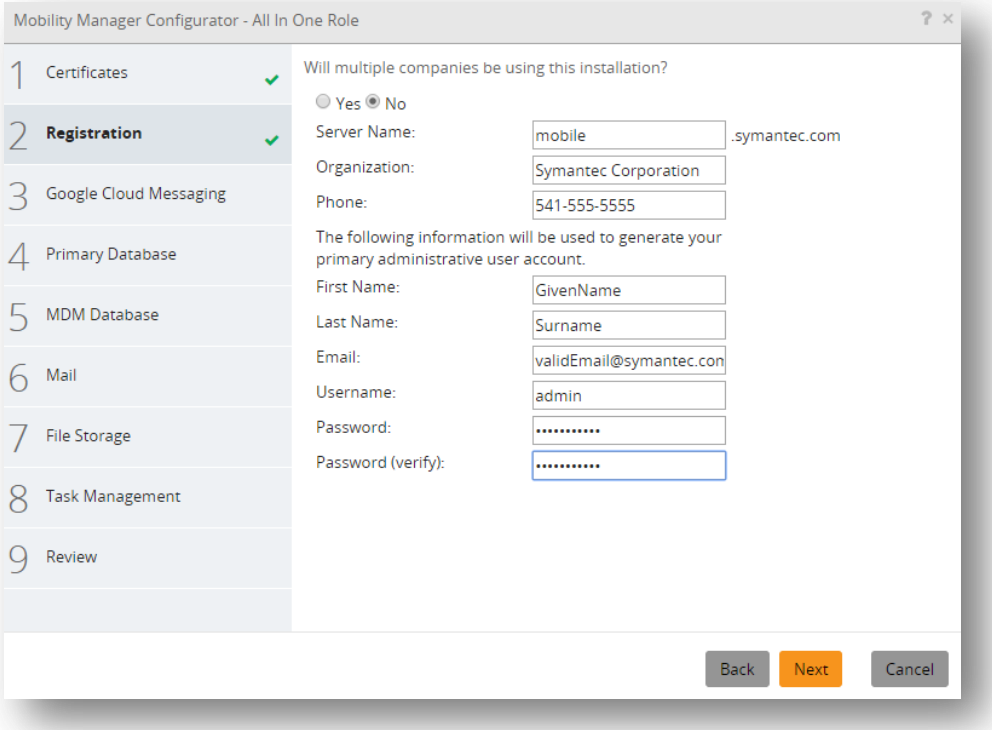
CA Bundle: Uploaded: C:\fakepath\gd_bundle.crt Replace

6. Will multiple companies be using this installation? Select **No.**
7. Enter the Server name found in the FQDN and CN of the CSR, fill in the rest of the form information as requested.

Tip: A valid dedicated email account should be used for the primary administrator. This may be changed later but having a valid email account is vital to be able to reset the accounts password.

Note: Wildcard certificates may be used.

8. Click **Next** to continue:



Mobility Manager Configurator - All In One Role

Will multiple companies be using this installation?

○ Yes ● No

Server Name: mobile .symantec.com

Organization: Symantec Corporation

Phone: 541-555-5555

The following information will be used to generate your primary administrative user account.

First Name: GivenName

Last Name: Surname

Email: validEmail@symantec.con

Username: admin

Password: ••••••••••

Password (verify): ••••••••••

Note: The domain name is parsed from the uploaded SSL certificate. If the domain name is an internal domain and not published with a registrar, meaning it cannot be accessed from the Internet. Recreate and re-upload the SSL certificate(s) for the published domain name. This information is written into the database (DB) and written into the Mobile agents for device to FE communication. If the FQDN is not yet known, the domain name of the server may be changed at a later time by following HOWTO80680. This will also require that the SSL certificates be updated. However the **server-name cannot be changed** post installation, again, the residing domain can be changed but the **Server name** cannot.

9. Paste the information from following Google Cloud Messaging into the Mobility Manager Configuration Wizard and **Next** to continue.

Tip: These fields may be left blank and entered after the installation is complete.

10. Select **MySql** as the database engine.

Create a MySQL database host (HOWTO107280)

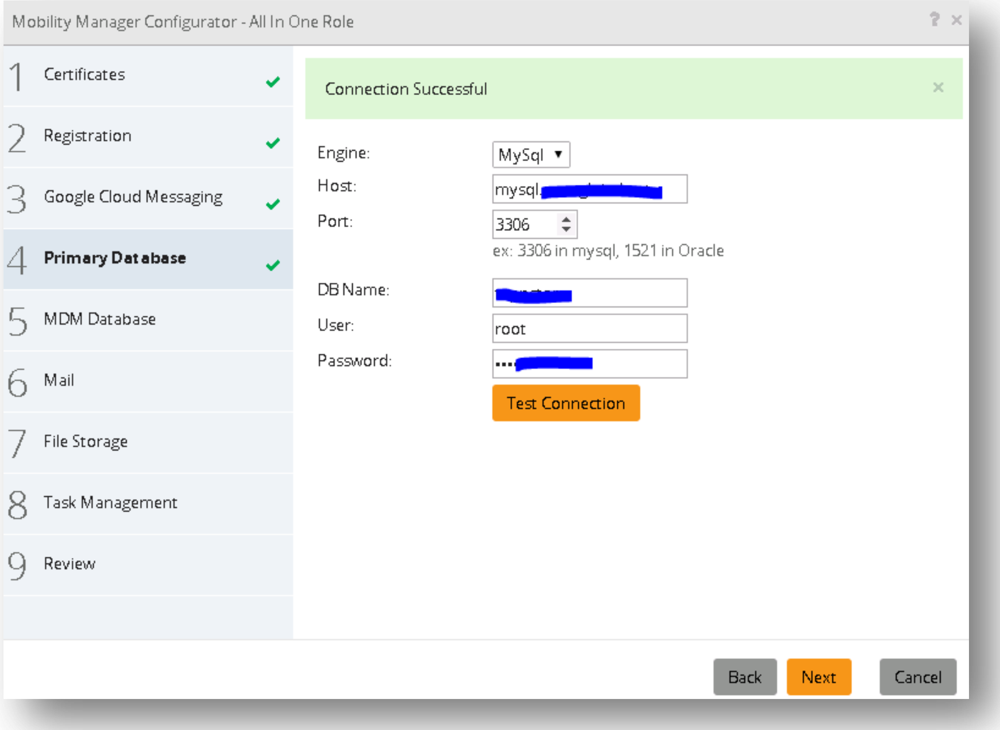
11. Repeat Part I: The Virtual Machine; entering the required information for the MySQL server rather than the Mobility Suite FE. (HOWTO110252)

Note: A production MySQL 5.6 database (For Mobility Suite) requires at least 30GB storage, 4GB Memory and a dual core processor. (Roughly half of the hardware requirements for the Mobility FE)

12. Once root shell access is obtained to the new server, open a new tab and follow: HOWTO107280 to download and configure the MySQL host and the two required databases.
13. Once the DB host and two databases are created continue to Enter MySQL Connection Information.

Enter MySQL Connection Information

14. Enter the required connection info for the **Primary Database** into the Wizard and **Test Connection**. Once a successful connection is established click **Next** to continue:



Connection Successful

Engine: MySql

Host: mysql[redacted]

Port: 3306

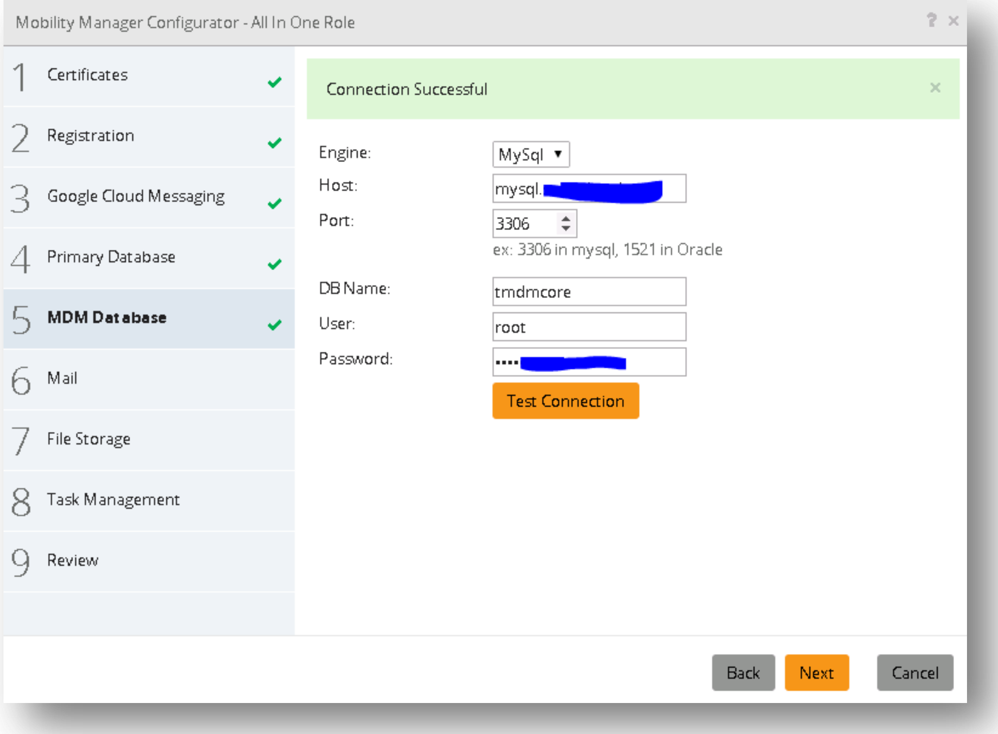
ex: 3306 in mysql, 1521 in Oracle

DB Name: [redacted]

User: root

Password: •••[redacted]

15. Enter the required connection info for the **MDM Database** into the Wizard and **Test Connection**. Once a successful connection is established click **Next** to continue:



Connection Successful

Engine: MySql

Host: mysql.[redacted]

Port: 3306

ex: 3306 in mysql, 1521 in Oracle

DB Name: tmdmcore

User: root

Password: ••••[redacted]

Tip: For troubleshooting MySQL connectivity see Troubleshooting MySQL Connectivity.

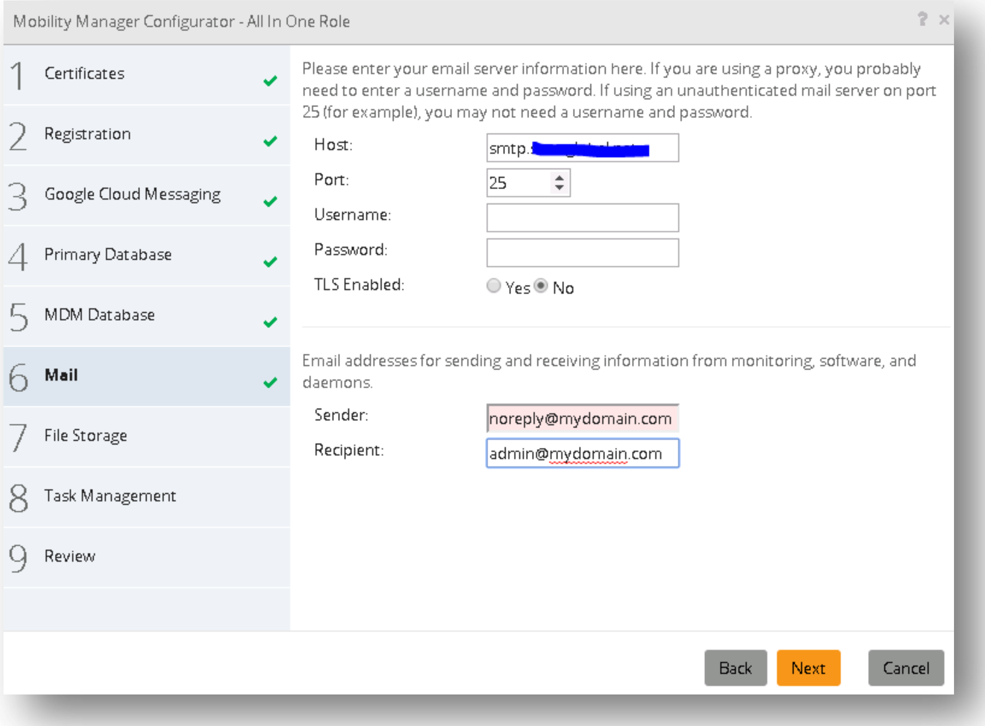
16. Continue to Mail Relay Configuration

Mail Relay Configuration (HOWTO110249)

17. Enter the email server information. If a proxy is being used, most likely, a username and password is required. If using an unauthenticated mail server on port 25 (for example), a username and password may not be needed. If no mail relay server is available follow the Temporary Email Option External: (HOWTO110251).

Tip: To change the mail relay after the installation completes see Changing the Mail-relay Post Configurator. External: (HOWTO110249)

18. Once valid mail relay information is entered click **Next** and continue to Caching



Please enter your email server information here. If you are using a proxy, you probably need to enter a username and password. If using an unauthenticated mail server on port 25 (for example), you may not need a username and password.

Host: smtp.[redacted]

Port: 25

Username:

Password:

TLS Enabled: ○ Yes ● No

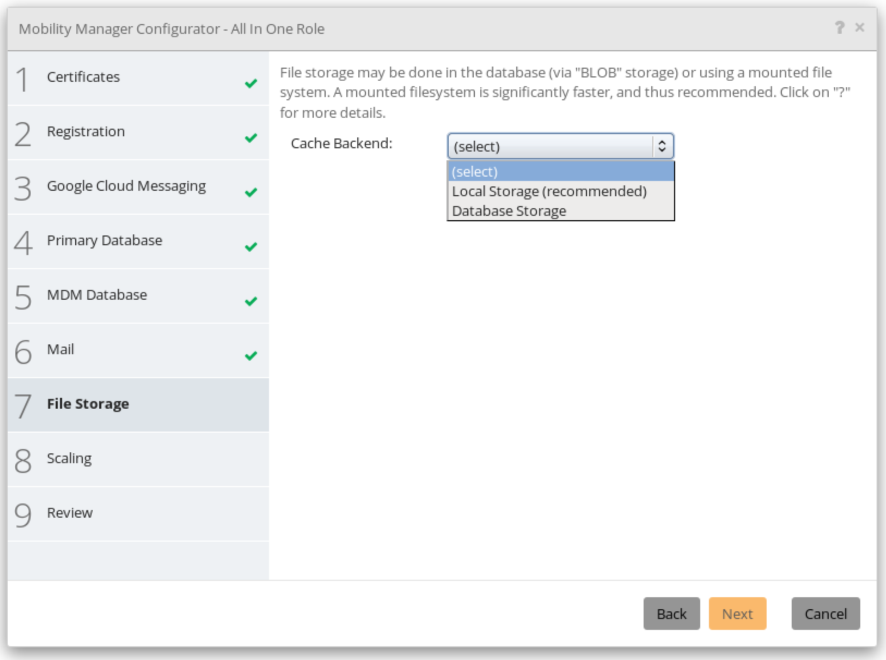
Email addresses for sending and receiving information from monitoring, software, and daemons.

Sender: noreply@mydomain.com

Recipient: admin@mydomain.com

Caching (TECH228357)

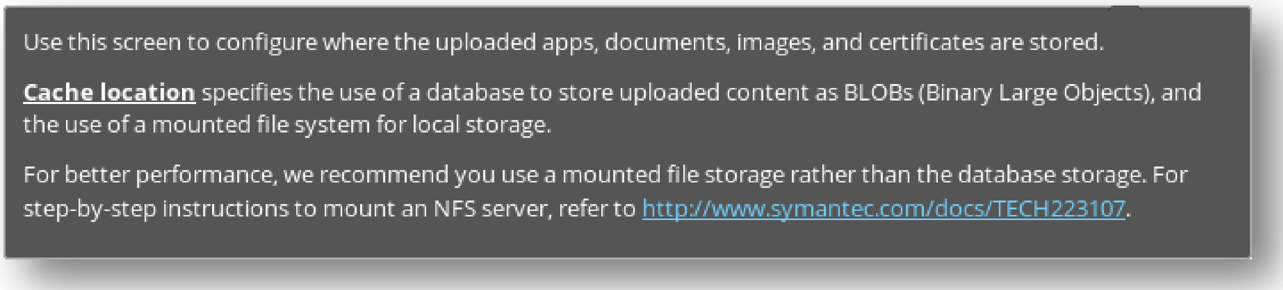
19. For the cache backend, select **Database Storage** and **Next** to continue:



File storage may be done in the database (via "BLOB" storage) or using a mounted file system. A mounted filesystem is significantly faster, and thus recommended. Click on "?" for more details.

Cache Backend: (select)

Note: For more details on **Cache Backend** options see TECH228357



Use this screen to configure where the uploaded apps, documents, images, and certificates are stored.

Cache location specifies the use of a database to store uploaded content as BLOBs (Binary Large Objects), and the use of a mounted file system for local storage.

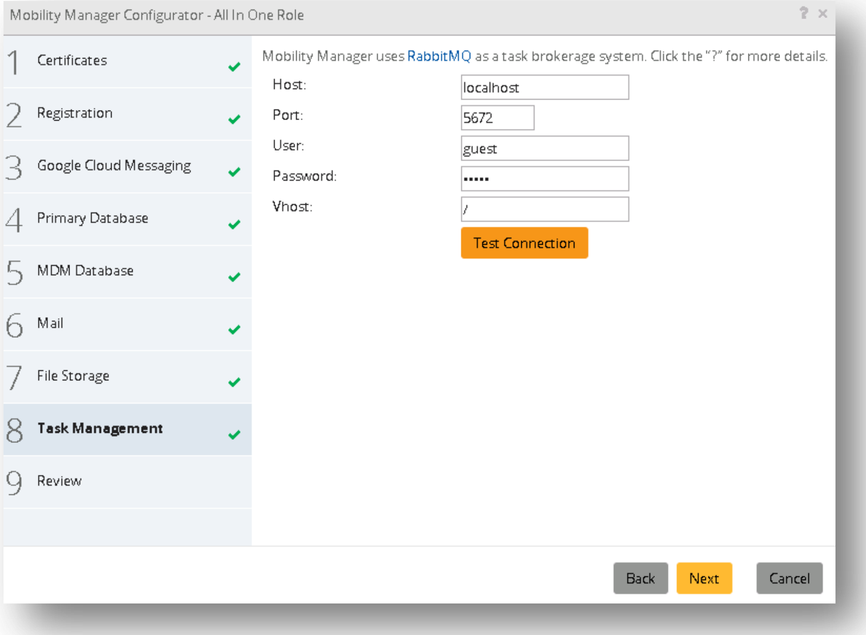
For better performance, we recommend you use a mounted file storage rather than the database storage. For step-by-step instructions to mount an NFS server, refer to http://www.symantec.com/docs/TECH223107.

20. Once the cache backend is completed continue to RabbitMQ.

RabbitMQ (HOWTO107254)

21. Accept the default settings for the RabbitMQ role. Click **Test Connection**; once a successful connection is established **Next** to continue.

Note: The hashed password for the default local instance is: **guest**



Mobility Manager uses RabbitMQ as a task brokerage system. Click the "?" for more details.

Host: localhost

Port: 5672

User: guest

Password: •••••

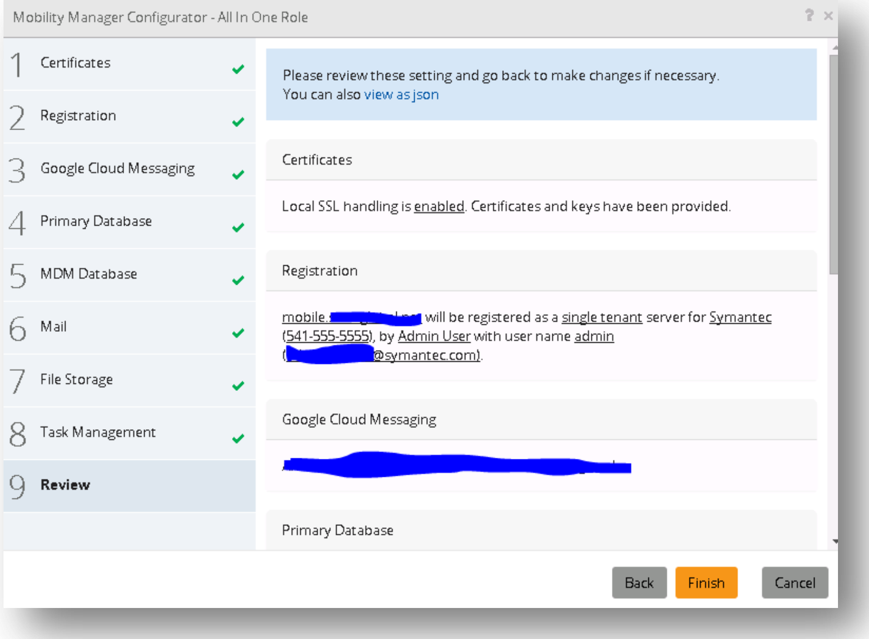
Vhost: /

Tip: If the connection times out, verify that localhost resolves to 127.0.0.1 and not an IPV6 address. IPTables may also block 5672. Keep in mind that terminating the script will bring the process back to the Installation Part II: Bootstrapping step; use Putty to SSH into the FE to further troubleshoot. For troubleshooting RabbitMQ refer to TECH215945. If an off-box RabbitMQ is needed refer to HOWTO110356 .

22. Continue to the Verify Configurator Settings step below.

Verify and Commit Settings

23. Verify that the settings entered are correct and click **Finish** to complete and finalize the installation:



Please review these setting and go back to make changes if necessary.
You can also view as json

Certificates

Local SSL handling is enabled. Certificates and keys have been provided.

Registration

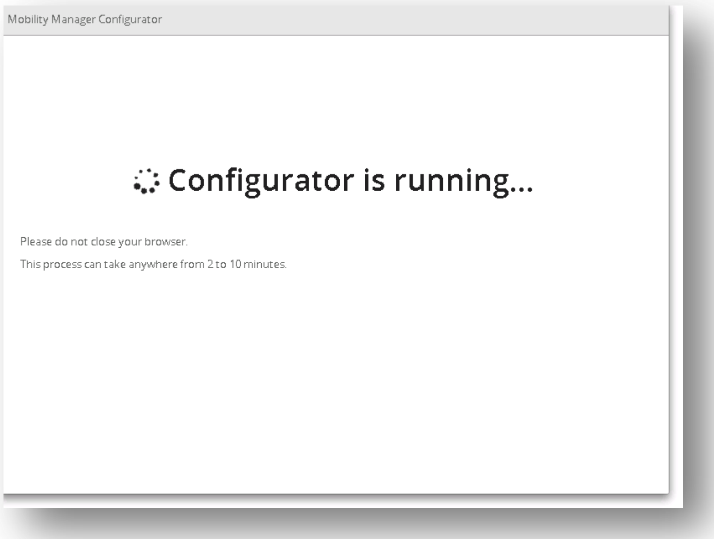
mobile.[redacted] will be registered as a single tenant server for Symantec (541-555-5555), by Admin User with user name admin ([redacted]@symantec.com).

Google Cloud Messaging

[redacted]

Primary Database

Note: This process can take up to 15 minutes to complete. To view live progress use Putty to open an SSH shell to the FE and type: **tail –f /var/log/nukona/load_settings.log**

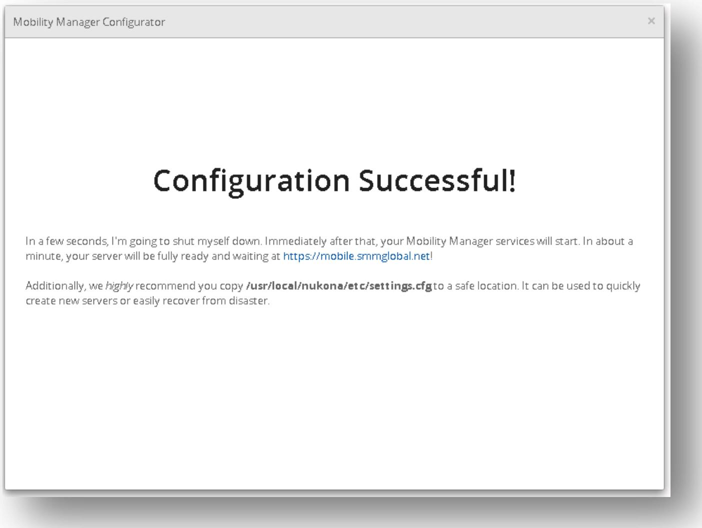


Configurator is running...

Please do not close your browser.

This process can take anywhere from 2 to 10 minutes.

24. After the configurator completes, allow another 5 minutes for the setup.sh script to finalize.



Configuration Successful!

In a few seconds, I'm going to shut myself down. Immediately after that, your Mobility Manager services will start. In about a minute, your server will be fully ready and waiting at https://mobile.smmglobal.net!

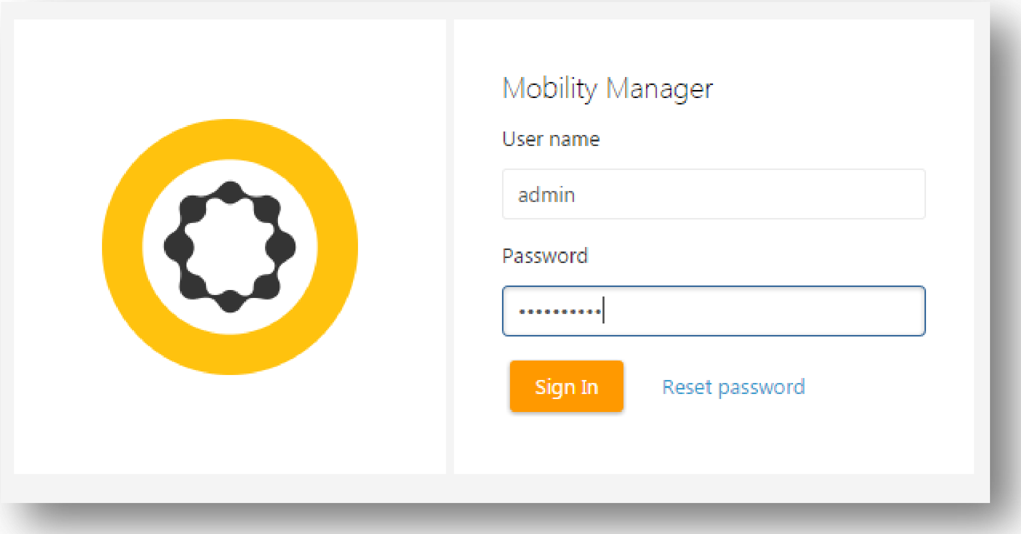
Additionally, we *highly* recommend you copy **/usr/local/nukona/etc/settings.cfg** to a safe location. It can be used to quickly create new servers or easily recover from disaster.

Tip: For troubleshooting the Bootstrapping process see the Troubleshooting the Bootstrap / Configurator Process section of this document.

Configure an External Identity Provider (IDP) (HOWTO110276)

Note: An

1. To log into the console, for the first time, go to the tenant admin URL. For example: https://mobile.mydomain.com/admin/login

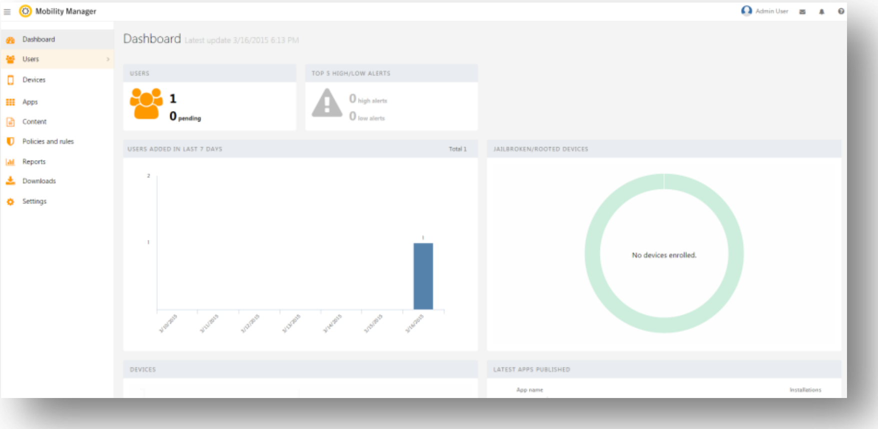


User name: admin

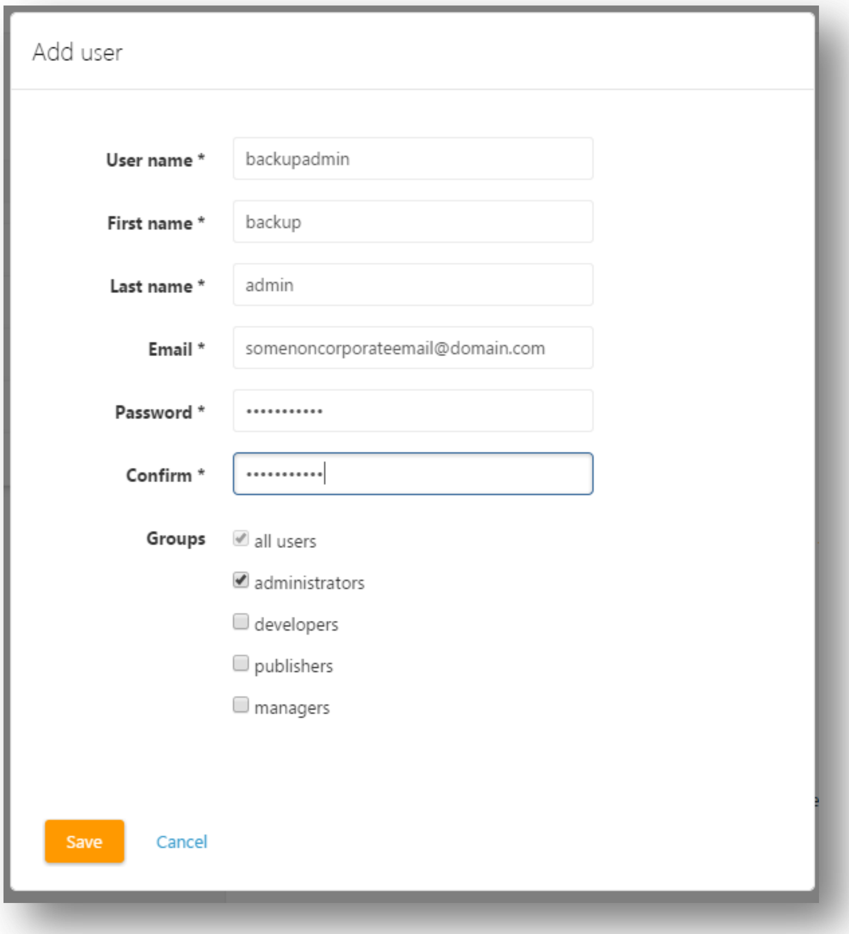
Password: ••••••••••

Note: If a temporary internal or self-sign certificate was used, there may be an SSL error when accessing the console.

2. The first page is the administrative dashboard. This contains a heads-up view of the tenant's health and usage.



3. Before setting up and external IDP, first create a backup local administrative account which does not share a corporate email address. To do this go to **Users > Add New User** enter the new administrative account's vital information, check **Administrators** for groups and click **Save**:



Add user

User name * backupadmin

First name * backup

Last name * admin

Email * somenoncorporateemail@domain.com

Password * •••••••••••

Confirm * •••••••••••

Groups

☑ all users

☑ administrators

☐ developers

☐ publishers

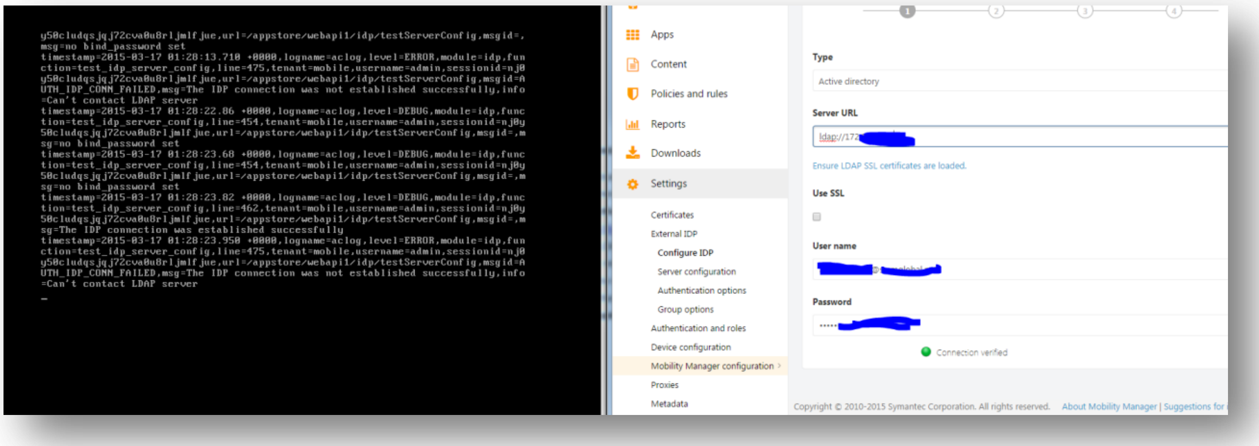
☐ managers

4. Now that a backup administrative account has been created go to **Settings > External IDP > Configure IDP**, review the message and click **Start** to begin.

Note: In this example an **Active Directory (AD)** will be used. For SAML via ADFS see HOWTO84940.

5. To use Active Directory or LDAP, there must be communication between the Mobility FE and the LDAP/AD server. Enter the required server information, once a successful connection is made click **Save** to continue.

Tip: The connection will auto-test with any form changes. To see the exact reason for the connection failure, review the **/var/log/nukona/appstore.log** entries. Use a command like:
tail –f /var/log/nukona/appstore.log to view a live feed of this log while testing the connection:



```
y50cludqsjqj72cva0u8rljmlfjue,url=/appstore/webapi1/idp/testServerConfig,msgid=,
msg=no bind_password set
timestamp=2015-03-17 01:28:13.710 +0000,logname=aclog,level=ERROR,module=idp,fun
ction=test_idp_server_config,line=475,tenant=mobile,username=admin,sessionid=nj0
y50cludqsjqj72cva0u8rljmlfjue,url=/appstore/webapi1/idp/testServerConfig,msgid=A
UTH_IDP_CONN_FAILED,msg=The IDP connection was not established successfully,info
=Can't contact LDAP server
timestamp=2015-03-17 01:28:22.86 +0000,logname=aclog,level=DEBUG,module=idp,func
tion=test_idp_server_config,line=454,tenant=mobile,username=admin,sessionid=nj0y
50cludqsjqj72cva0u8rljmlfjue,url=/appstore/webapi1/idp/testServerConfig,msgid=,m
sg=no bind_password set
timestamp=2015-03-17 01:28:23.68 +0000,logname=aclog,level=DEBUG,module=idp,func
tion=test_idp_server_config,line=454,tenant=mobile,username=admin,sessionid=nj0y
50cludqsjqj72cva0u8rljmlfjue,url=/appstore/webapi1/idp/testServerConfig,msgid=,m
sg=no bind_password set
timestamp=2015-03-17 01:28:23.82 +0000,logname=aclog,level=DEBUG,module=idp,func
tion=test_idp_server_config,line=462,tenant=mobile,username=admin,sessionid=nj0y
50cludqsjqj72cva0u8rljmlfjue,url=/appstore/webapi1/idp/testServerConfig,msgid=,m
sg=The IDP connection was established successfully
timestamp=2015-03-17 01:28:23.950 +0000,logname=aclog,level=ERROR,module=idp,fun
ction=test_idp_server_config,line=475,tenant=mobile,username=admin,sessionid=nj0
y50cludqsjqj72cva0u8rljmlfjue,url=/appstore/webapi1/idp/testServerConfig,msgid=A
UTH_IDP_CONN_FAILED,msg=The IDP connection was not established successfully,info
=Can't contact LDAP server
_
```

Type: Active directory

Server URL: ldap://172[redacted]

Ensure LDAP SSL certificates are loaded.

Use SSL: □

User name: [redacted]

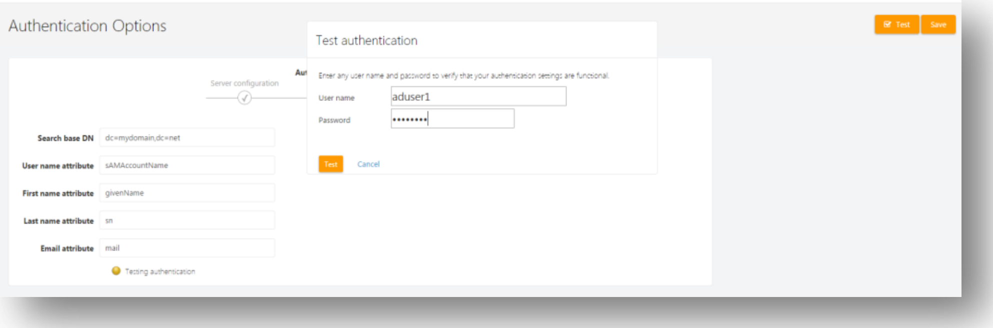
Password: •••••[redacted]

● Connection verified

Copyright © 2010-2015 Symantec Corporation. All rights reserved. About Mobility Manager | Suggestions for

Note: A user with sufficient credentials to query the AD/LDAP schema must be used. The Distinguished Name (DN) of the user may be required. In the above example the sAMAccountName@<domain> is shown. If the LDAP server requires SSL, try using a combination of ldaps://<serverURL> or ldap://<serverURL> and checking and unchecking the use SSL box. Also for LDAPS, the issuing CA LDAP certificate must be uploaded to **Settings > Certificates > LDAP Certificates**. See How to determine which certificate is used by my AD/LDAP.

6. Enter the **Search Base Domain Name (DN)** leaving the rest of the AD attributes as they are. Click **Test** to confirm that Mobility is able to query the DN.
   IMPORTANT: Test a non-administrative account as this can overwrite the tenant-administrator's privileges.



Search base DN: dc=mydomain,dc=net

User name attribute: sAMAccountName

First name attribute: givenName

Last name attribute: sn

Email attribute: mail

● Testing authentication

Test authentication

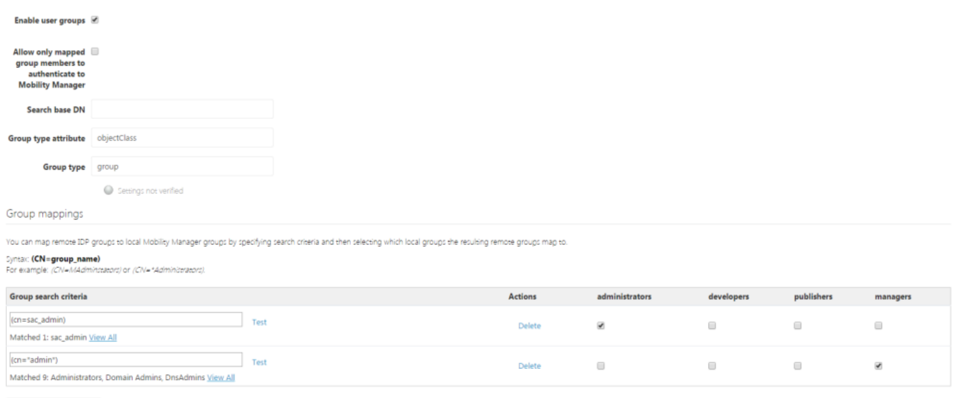
Enter any user name and password to verify that your authentication settings are functional.

User name: aduser1

Password: ••••••••

Tip: If the organization's domain name is: mydomain.com then the base DN would be **dc=mydomain,dc=com**. The purpose of the base DN is to limit queries to a domain or an organizational unit (OU). When testing the connection only use the defined **User name attribute**. For AD it would be the user's **sAMAccountName**.

7. IDP setup cannot proceed until a successful AD/LDAP bind is completed. Once a successful authentication occurs click **Save** to continue.
8. Group mapping allows Mobility Suite to map AD groups to locally created groups. The search base DN may be left blank. The wildcard attribute ***** (asterisk) may be used:



Enable user groups ☑

Allow only mapped group members to authenticate to Mobility Manager □

Search base DN:

Group type attribute: objectClass

Group type: group

○ Settings not verified

Group mappings

You can map remote IDP groups to local Mobility Manager groups by specifying search criteria and then selecting which local groups the resulting remote groups map to.

Syntax: **(CN=group_name)**
For example: *(CN=MAdministrators)* or *(CN=*Administrators)*.

Group search criteria		Actions	administrators	developers	publishers	managers
(cn=sac_admin) Matched 1: sac_admin View All	Test	Delete	☑	□	□	□
(cn=*admin*) Matched 9: Administrators, Domain Admins, DnsAdmins View All	Test	Delete	□	□	□	☑

Tip: Click **Test** next to each **Group search criteria**, this will query the AD/LDAP for the specific group.

9. In the above screen capture, the AD administrator has already created a group designated for Mobility Suite administrators. Custom groups and roles may be created at a later time. See the Mobility Suite Administration Guide for more details. It is highly recommended not to enable IDP until an administrative group is successfully mapped. Once this is completed, click **Save** and on the next page, **Enable IDP.**

Tip: Re-visit this page to toggle the IDP settings on/off.

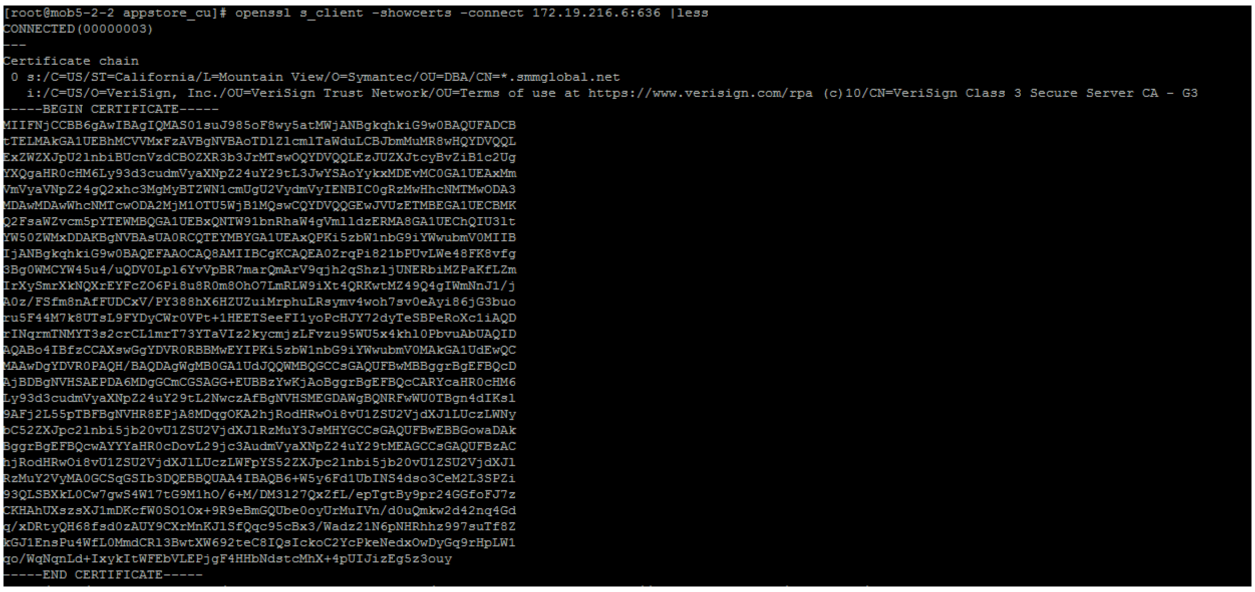
How to determine the certificate issuer for AD-SSL/LDAPS

1. Using a linux/unix machine use the following openssl syntax to determine the certificate that is being used by the LDAP/AD provider:

openssl s_client -showcerts -connect <FQDN_of_LDAP>:<PORT> | less

For example:

openssl s_client -showcerts -connect 172.19.216.6:636 |less



```
[root@mob5-2-2 appstore_cu]# openssl s_client -showcerts -connect 172.19.216.6:636 |less
CONNECTED(00000003)
---
Certificate chain
 0 s:/C=US/ST=California/L=Mountain View/O=Symantec/OU=DBA/CN=*.smmglobal.net
   i:/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=Terms of use at https://www.verisign.com/rpa (c)10/CN=VeriSign Class 3 Secure Server CA - G3
-----BEGIN CERTIFICATE-----
MIIFNjCCBB6gAwIBAgIQMAS01suJ985oF8wy5atMWjANBgkqhkiG9w0BAQUFADCB
tTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoYykxMDEvMC0GA1UEAxMm
VmVyaVNpZ24gQ2xhc3MgMyBTZWN1cmUgU2VydmVyIENBIC0gRzMwHhcNMTMwODA3
MDAwMDAwWhcNMTcwODA2MjM1OTU5WjB1MQswCQYDVQQGEwJVUzETMBEGA1UECBMK
Q2FsaWZvcm5pYTEWMBQGA1UEBxQNTW91bnRhaW4gVmlldzERMA8GA1UEChQIU3lt
YW50ZWMxDDAKBgNVBAsUA0RCQTEYMBYGA1UEAxQPKi5zbW1nbG9iYWwubmV0MIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0ZrqPi821bPUvLWe48FK8vfg
3Bg0WMCYW45u4/uQDV0Lpl6YvVpBR7marQmArV9qjh2qShzljUNERbiMZPaKfLZm
IrXySmrXkNQXrEYFcZO6Pi8u8R0m8OhO7LmRLW9iXt4QRKwtMZ49Q4gIWmNnJ1/j
A0z/FSfm8nAfFUDCxV/PY388hX6HZUZuiMrphuLRsymv4woh7sv0eAyi86jG3buo
ru5F44M7k8UTsL9FYDyCWr0VPt+1HEETSeeFI1yoPcHJY72dyTeSBPeRoXc1iAQD
rINqrmTNMYT3s2crCL1mrT73YTaVIz2kycmjzLFvzu95WU5x4khl0PbvuAbUAQID
AQABo4IBfzCCAXswGgYDVR0RBBMwEYIPKi5zbW1nbG9iYWwubmV0MAkGA1UdEwQC
MAAwDgYDVR0PAQH/BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcD
AjBDBgNVHSAEPDA6MDgGCmCGSAGG+EUBBzYwKjAoBggrBgEFBQcCARYcaHR0cHM6
Ly93d3cudmVyaXNpZ24uY29tL2NwczAfBgNVHSMEGDAWgBQNRFwWU0TBgn4dIKsl
9AFj2L55pTBFBgNVHR8EPjA8MDqgOKA2hjRodHRwOi8vU1ZSU2VjdXJlLUczLWNy
bC52ZXJpc2lnbi5jb20vU1ZSU2VjdXJlRzMuY3JsMHYGCCsGAQUFBwEBBGowaDAk
BggrBgEFBQcwAYYYaHR0cDovL29jc3AudmVyaXNpZ24uY29tMEAGCCsGAQUFBzAC
hjRodHRwOi8vU1ZSU2VjdXJlLUczLWFpYS52ZXJpc2lnbi5jb20vU1ZSU2VjdXJl
RzMuY2VyMA0GCSqGSIb3DQEBBQUAA4IBAQB6+W5y6Fd1UbINS4dso3CeM2L3SPZi
93QLSBXkL0Cw7gwS4W17tG9M1hO/6+M/DM3l27QxZfL/epTgtBy9pr24GGfoFJ7z
CKHAhUXszsXJ1mDKcfW0SO1Ox+9R9eBmGQUbe0oyUrMuIVn/d0uQmkw2d42nq4Gd
q/xDRtyQH68fsd0zAUY9CXrMnKJlSfQqc95cBx3/Wadz21N6pNHRhhz997suTf8Z
kGJ1EnsPu4WfL0MmdCRl3BwtXW692teC8IQsIckoC2YcPkeNedxOwDyGq9rHpLW1
qo/WqNqnLd+IxykItWFEbVLEPjgF4HHbNdstcMhX+4pUIJizEg5z3ouy
-----END CERTIFICATE-----
```

In the above example, a public SSL certificate issued by Verisign is shown. If an in-house certificate is used, take note of the "i:…" section and continue below to export that issuer certificate. Otherwise, simply copy and paste the first certificate into a txt file (if it is shown) and upload it to the Mobility Admin console > Settings > Certificates > LDAP Certificates section.

Exporting the certificate from AD

2. Access the Active Directory server and open the MMC console.
3. Click File > Add/Remove snap-in…
4. Select Certificates and click **Add.**
5. Select **Computer Account** and **Next**.
6. Accept the default option and **Next** again.
7. Search through the Trusted Root Certification Authorities for the issuer matching the CN from step.
8. Once the CA is found right-click the certificate and select All Tasks > Exports…
9. On the Welcome screen click **Next**.
10. Ensure that Base-64 is selected and **Next**.
11. Browse to a name and save the file.

Note: Ensure that the Save as Type is **Base64 Encoded X.509(*.cer)**.

Upload LDAP certificate to Mobility

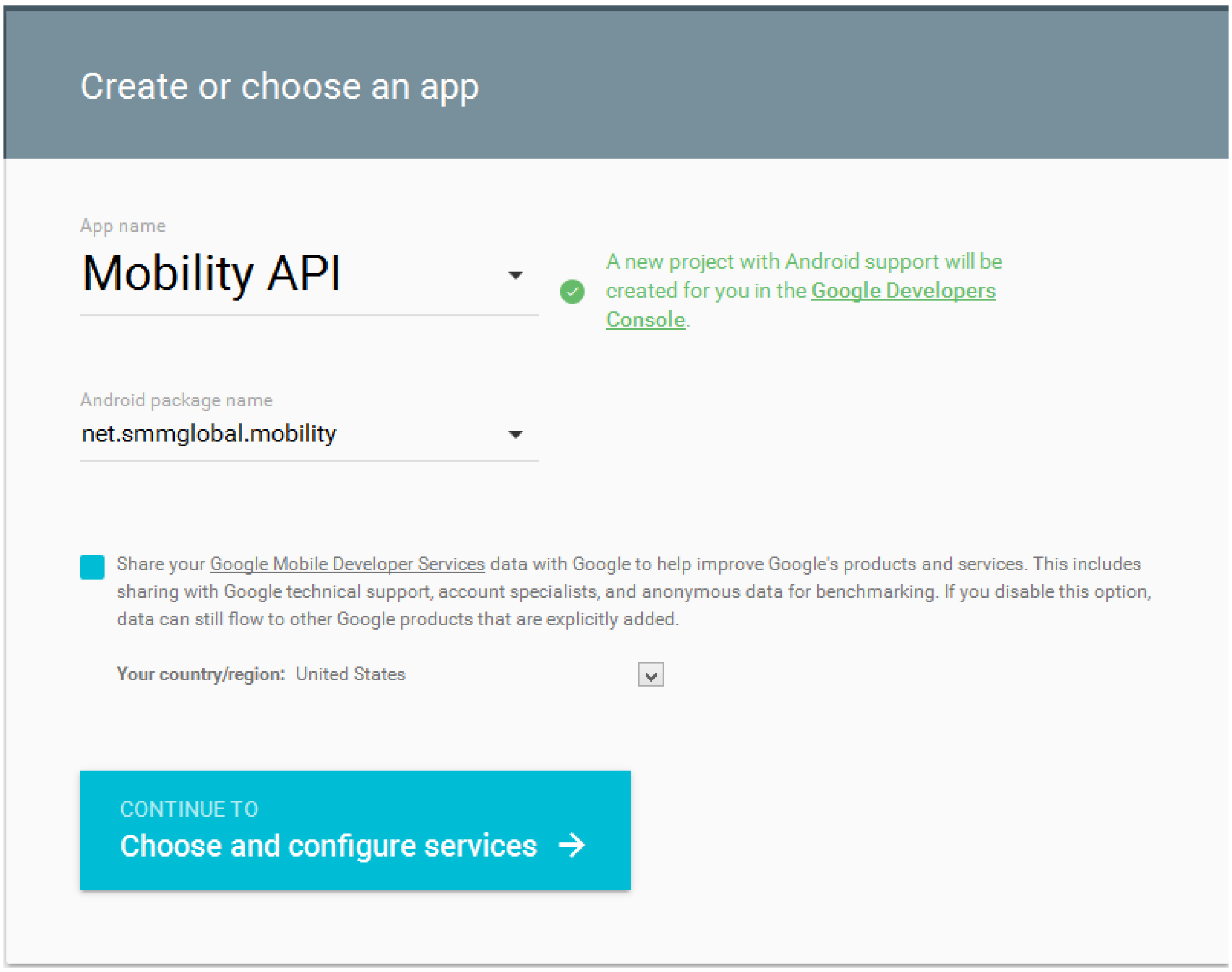
12. Finally upload the certificate to Mobility Admin console > Settings > Certificates > LDAP Certificates.

Google Cloud Messaging (HOWTO110277)

1. In a new tab, with a valid Google Account log into the Google API Console by opening the following link in a new tab: https://developers.google.com/mobile/add
2. Sign into the console with a Google credential.

Note: It may be necessary to update this information for the tenant in the future. Ensure that this account may be accessed by other members of the organization.

3. Click **Pick a platform** and select **Android App**.
4. For the App-name enter **Mobility API**.
5. For the **Android package name** enter reverse FQDN of tenant. For example if the tenant name is, mobility.smmglobal.net the Android package name would be net.smmglobal.mobility.
6. Click **Chose and configure services**:



Create or choose an app

App name

Mobility API

A new project with Android support will be created for you in the Google Developers Console.

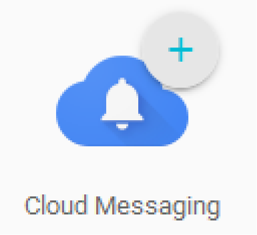
Android package name

net.smmglobal.mobility

☑ Share your Google Mobile Developer Services data with Google to help improve Google's products and services. This includes sharing with Google technical support, account specialists, and anonymous data for benchmarking. If you disable this option, data can still flow to other Google products that are explicitly added.

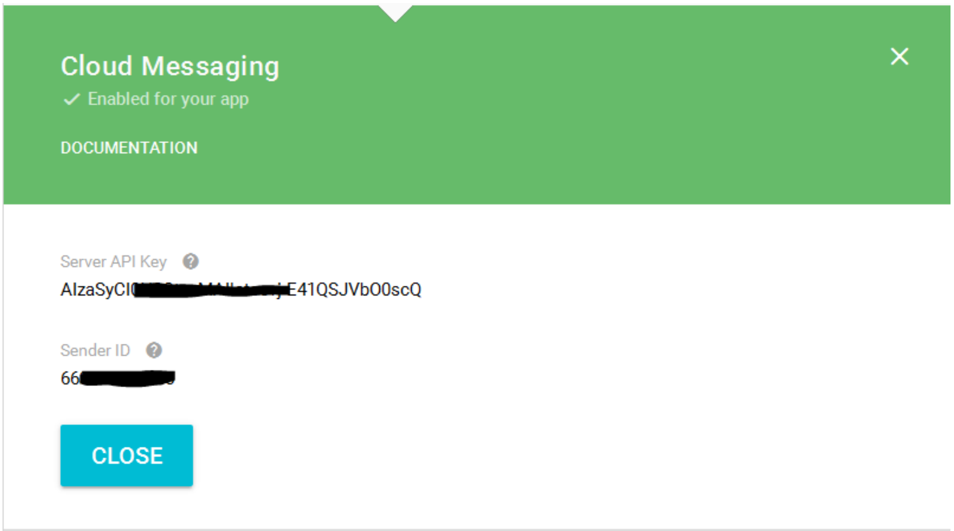
Your country/region: United States

7. Add **Cloud Messaging**:



8. Now click **ENABLE GOOGLE CLOUD MESSAGING**

9. Take note of the Server **API Key** and the **SenderID:**



Cloud Messaging

✓ Enabled for your app

Server API Key

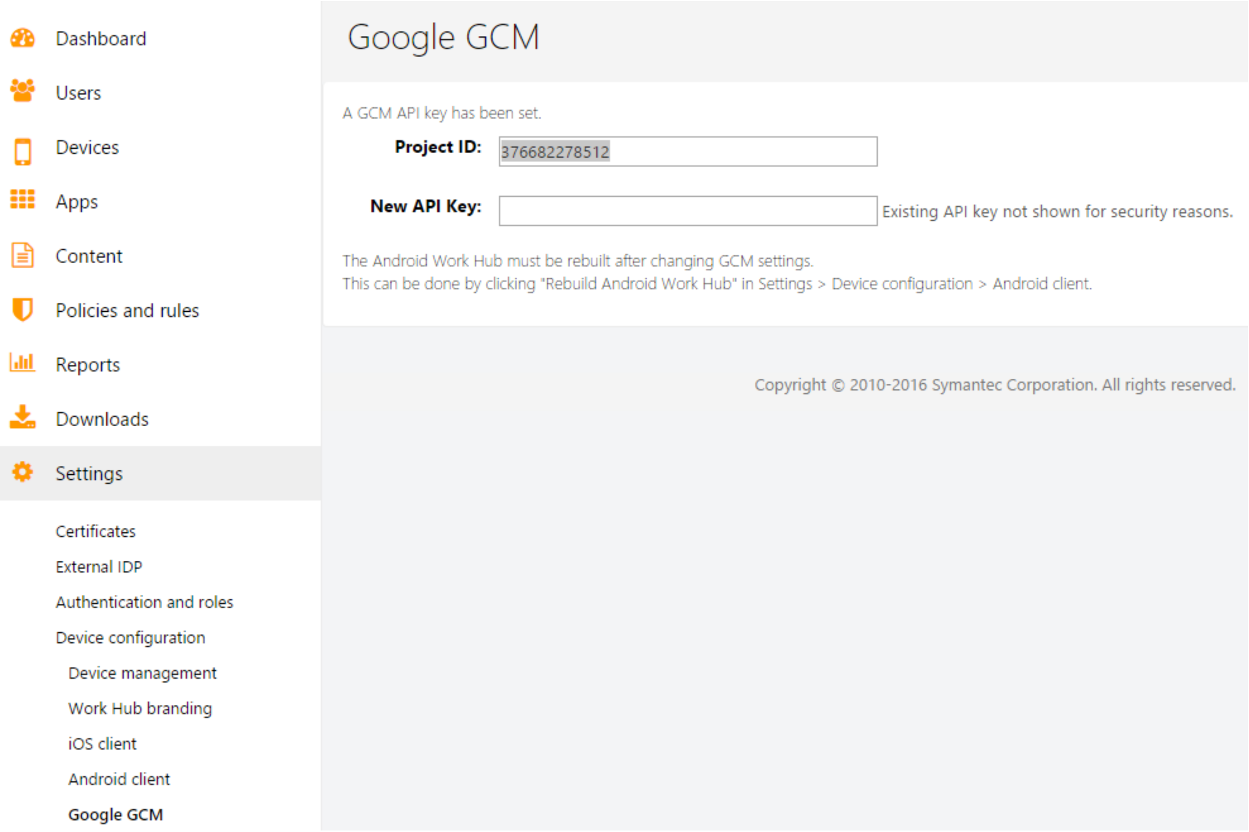
AlzaSyCl[redacted]E41QSJVb00scQ

Sender ID

66[redacted]

10. Copy the **API KEY** value to a notepad on the workstation. Here is an example API Key: **AlzaSyatnIND7uhqORFyaV-qcCyM3vuwm1mqiro**
11. Click **Overview** under the Project Name. Copy the **Project Number** to the same notepad. Example Project number: **76274530254**
12. Finally paste the project number and API key into the Mobility Admin console > Settings > Device configuration Google GCM and click **Save**:

Note: After the Work Hub agent completes its rebuild, it is required for all Android devices to download and install the updated Agent for GCM commands to complete.



Google GCM

A GCM API key has been set.

Project ID: 376682278512

New API Key: Existing API key not shown for security reasons.

The Android Work Hub must be rebuilt after changing GCM settings.
This can be done by clicking "Rebuild Android Work Hub" in Settings > Device configuration > Android client.

Copyright © 2010-2016 Symantec Corporation. All rights reserved.

13. Build the Android Work Hub agent

If following Installation Part 2: Continue return to Create a MySQL database host

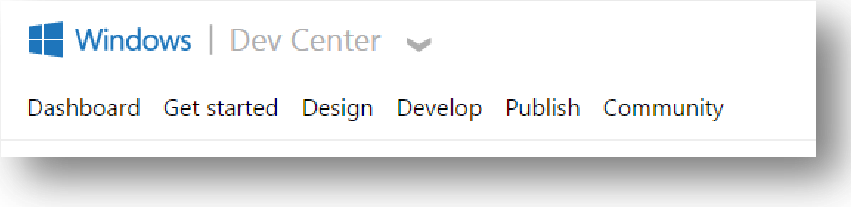
Windows Push Service (WNS) (HOWTO110271)

Items needed to complete this process:

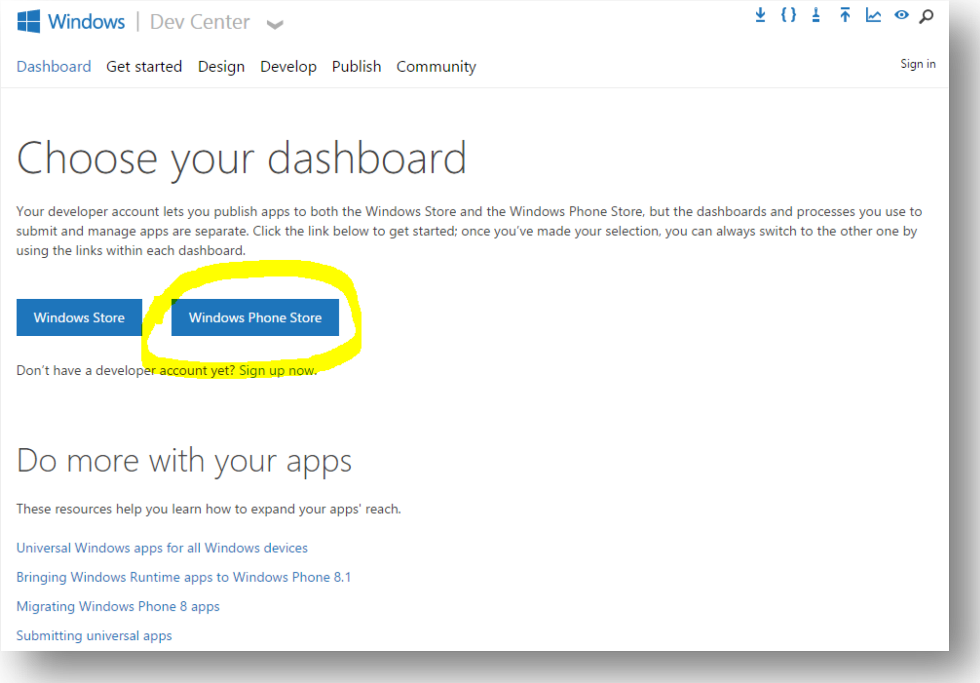
- Windows Developer account. There are two types of developer accounts, small business and enterprise. The small business account should suffice.
- The latest version of Visual Studio.
- Windows 8.1 < workstation.

Tip: A Windows Developer account token may be created for free using an MSDN account. Go to https://msdn.microsoft.com > **My Account** and **Windows and Windows Phone developer accounts**.

1. Go to https://dev.windows.com and sign-in:



2. Click **Dashboard** and under Choose your dashboard click **Windows Phone Store**:



Choose your dashboard

Your developer account lets you publish apps to both the Windows Store and the Windows Phone Store, but the dashboards and processes you use to submit and manage apps are separate. Click the link below to get started; once you've made your selection, you can always switch to the other one by using the links within each dashboard.

Don't have a developer account yet? Sign up now.

Do more with your apps

These resources help you learn how to expand your apps' reach.

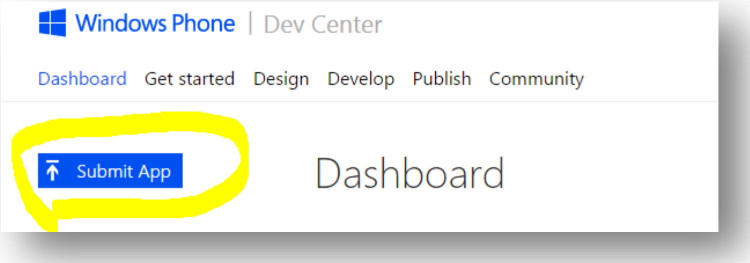
Universal Windows apps for all Windows devices

Bringing Windows Runtime apps to Windows Phone 8.1

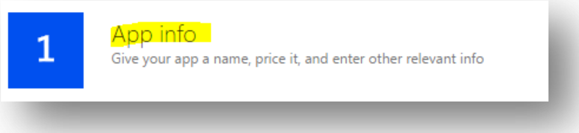
Migrating Windows Phone 8 apps

Submitting universal apps

3. Click **Submit App:**

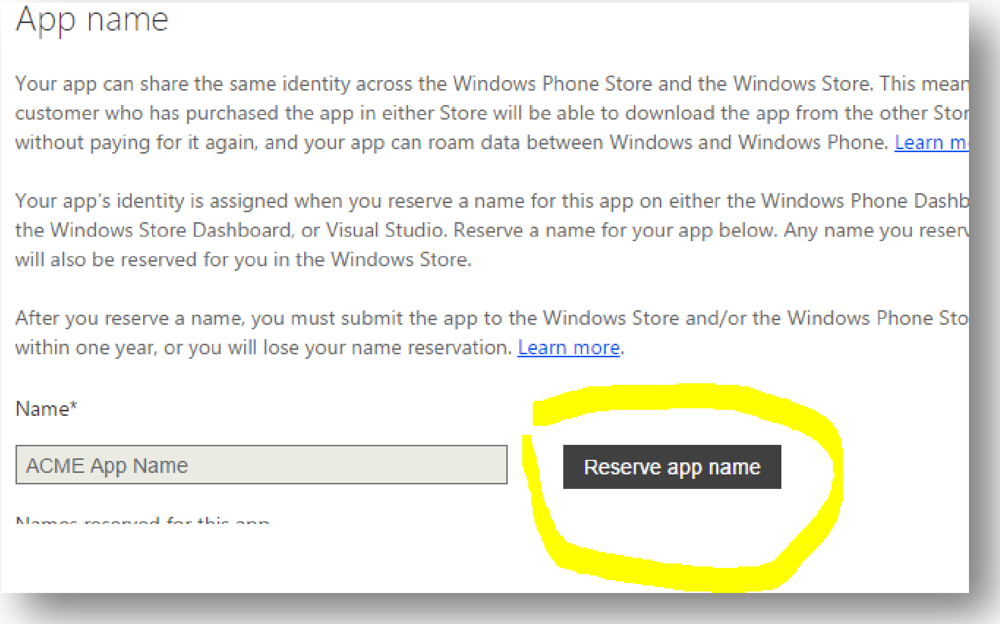

Windows Phone | Dev Center
Dashboard Get started Design Develop Publish Community
Submit App
Dashboard

4. Click **App info:**



Give your app a name, price it, and enter other relevant info

5. Create an app **name** and click **Reserve app name**:



App name

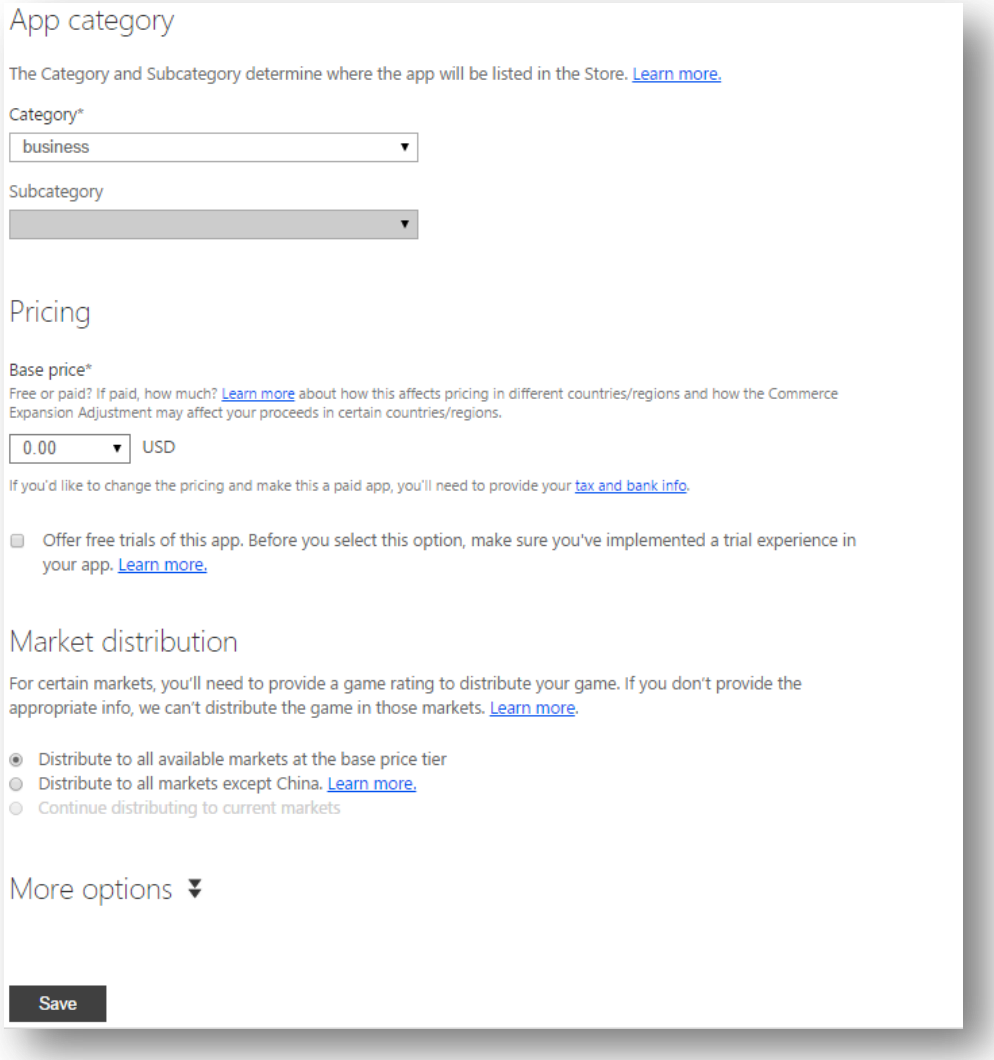
Your app can share the same identity across the Windows Phone Store and the Windows Store. This mean customer who has purchased the app in either Store will be able to download the app from the other Stor without paying for it again, and your app can roam data between Windows and Windows Phone. Learn m

Your app's identity is assigned when you reserve a name for this app on either the Windows Phone Dashb the Windows Store Dashboard, or Visual Studio. Reserve a name for your app below. Any name you reserv will also be reserved for you in the Windows Store.

After you reserve a name, you must submit the app to the Windows Store and/or the Windows Phone Sto within one year, or you will lose your name reservation. Learn more.

Name*: ACME App Name

6. Select any **App Category** and **Save**:



App category

The Category and Subcategory determine where the app will be listed in the Store. Learn more.

Category*

business ▾

Subcategory

▾

Pricing

Base price*

Free or paid? If paid, how much? Learn more about how this affects pricing in different countries/regions and how the Commerce Expansion Adjustment may affect your proceeds in certain countries/regions.

0.00 ▾ USD

If you'd like to change the pricing and make this a paid app, you'll need to provide your tax and bank info.

□ Offer free trials of this app. Before you select this option, make sure you've implemented a trial experience in your app. Learn more.

Market distribution

For certain markets, you'll need to provide a game rating to distribute your game. If you don't provide the appropriate info, we can't distribute the game in those markets. Learn more.

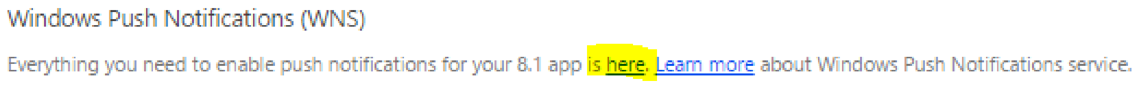
● Distribute to all available markets at the base price tier

○ Distribute to all markets except China. Learn more.

○ Continue distributing to current markets

More options

7. After the app is saved get back into **App info** and click **More options.**
8. Under Windows Push Notifications (WNS) click **Everything you need to enable push notifications for your 8.1 app is here**:

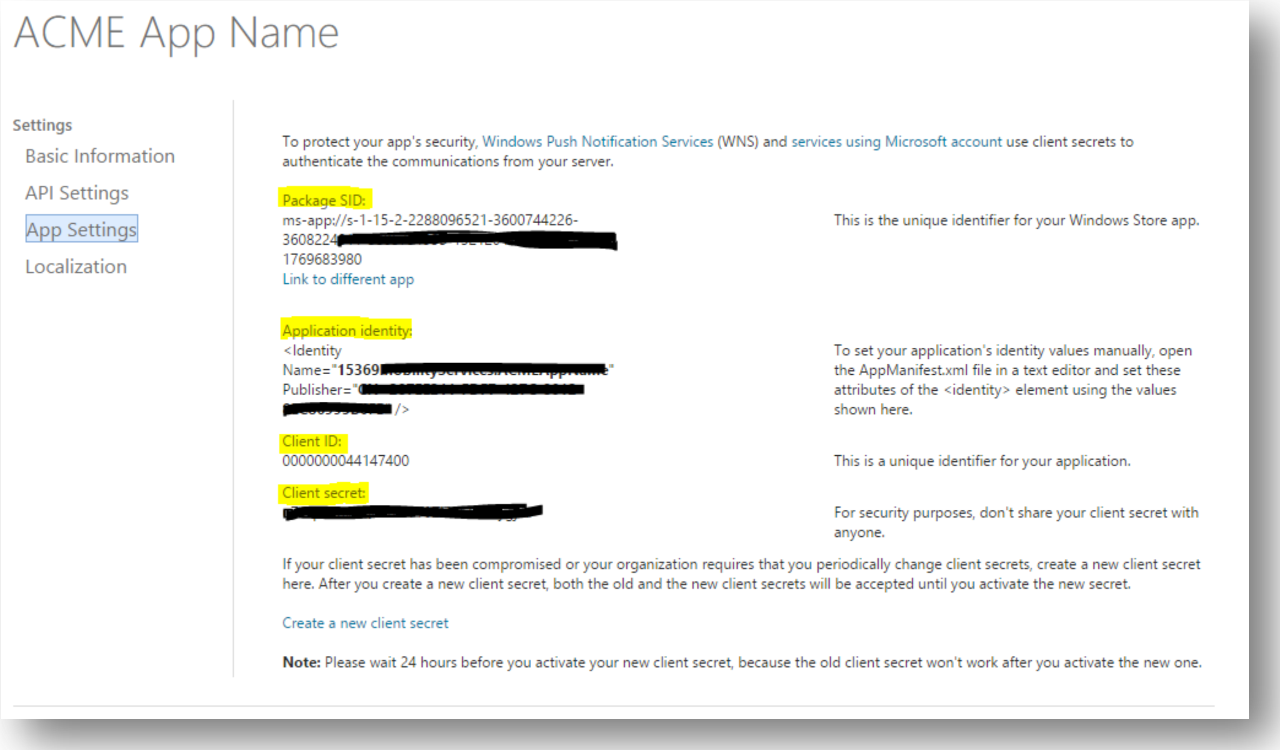


Windows Push Notifications (WNS)

Everything you need to enable push notifications for your 8.1 app is here. Learn more about Windows Push Notifications service.

Tip: The WNS page can take up to 1 minute to load.

9. Now **copy and paste** the following items to a notepad, for later use:
   Package SID
   Application identity
   Client ID
   Client secret



ACME App Name

Settings

Basic Information

API Settings

App Settings

Localization

To protect your app's security, Windows Push Notification Services (WNS) and services using Microsoft account use client secrets to authenticate the communications from your server.

Package SID:
ms-app://s-1-15-2-2288096521-3600744226-
3608224[redacted]
1769683980
Link to different app

This is the unique identifier for your Windows Store app.

Application identity:
<Identity
Name="15369[redacted]"
Publisher="[redacted]
[redacted] />

To set your application's identity values manually, open the AppManifest.xml file in a text editor and set these attributes of the <identity> element using the values shown here.

Client ID:
0000000044147400

This is a unique identifier for your application.

Client secret:
[redacted]

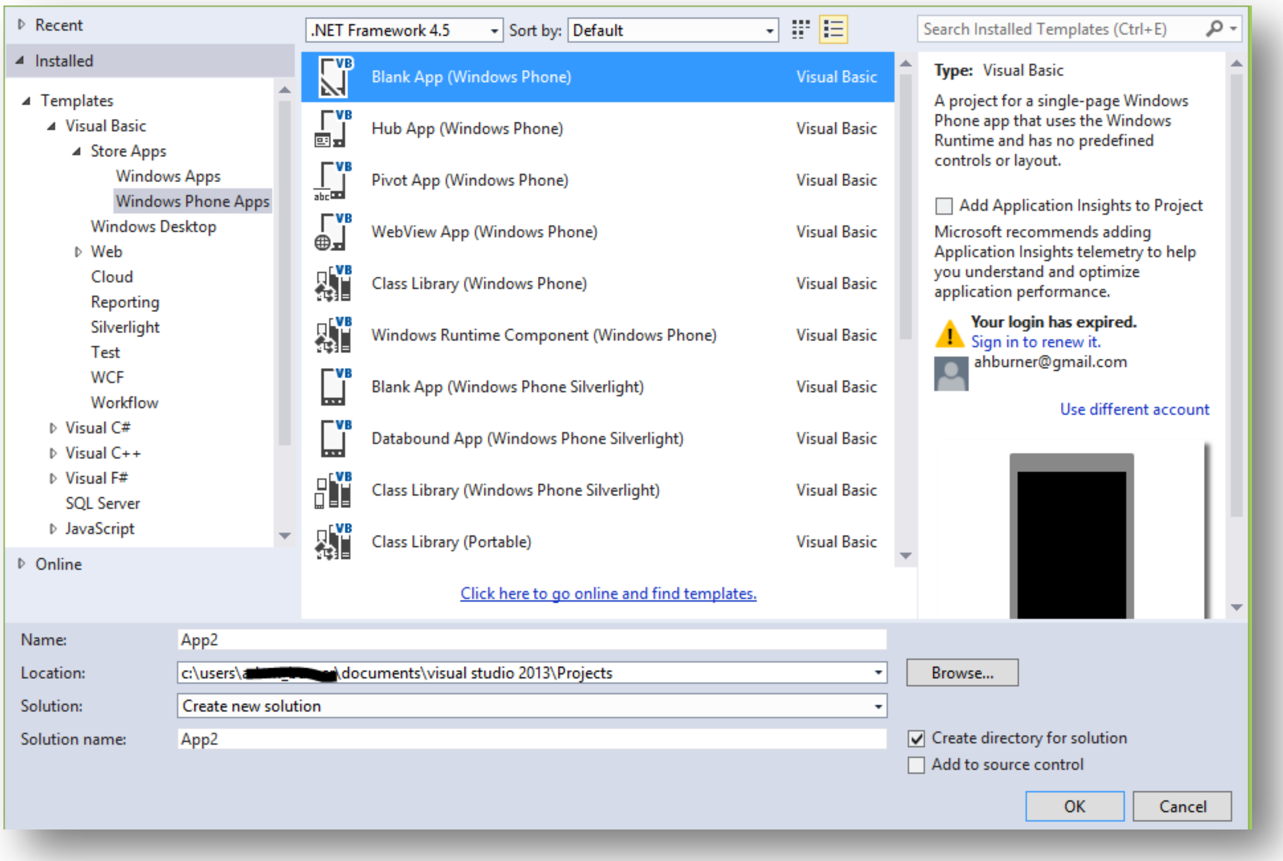
For security purposes, don't share your client secret with anyone.

If your client secret has been compromised or your organization requires that you periodically change client secrets, create a new client secret here. After you create a new client secret, both the old and the new client secrets will be accepted until you activate the new secret.

Create a new client secret

Note: Please wait 24 hours before you activate your new client secret, because the old client secret won't work after you activate the new one.

10. Launch Visual Studio on an 8.1 system. Click **File** > **New** > **Project**. Within the menu listing, on the right, select **Templates** > **Visual Basic** > **Store Apps** > **Windows Phone Apps**. Select the **'Blank App (Windows Phone)** within the template listing. Click **OK**:


Recent
Installed
Templates
Visual Basic
Store Apps
Windows Apps
Windows Phone Apps
Windows Desktop
Web
Cloud
Reporting
Silverlight
Test
WCF
Workflow
Visual C#
Visual C++
Visual F#
SQL Server
JavaScript
Online
.NET Framework 4.5
Sort by: Default
Search Installed Templates (Ctrl+E)
Blank App (Windows Phone) Visual Basic
Hub App (Windows Phone) Visual Basic
Pivot App (Windows Phone) Visual Basic
WebView App (Windows Phone) Visual Basic
Class Library (Windows Phone) Visual Basic
Windows Runtime Component (Windows Phone) Visual Basic
Blank App (Windows Phone Silverlight) Visual Basic
Databound App (Windows Phone Silverlight) Visual Basic
Class Library (Windows Phone Silverlight) Visual Basic
Class Library (Portable) Visual Basic
Click here to go online and find templates.
Browse...
OK
Cancel

Type: Visual Basic

A project for a single-page Windows Phone app that uses the Windows Runtime and has no predefined controls or layout.

□ Add Application Insights to Project

Microsoft recommends adding Application Insights telemetry to help you understand and optimize application performance.

Your login has expired. Sign in to renew it.

ahburner@gmail.com

Use different account

Name: App2

Location: c:\users\[redacted]\documents\visual studio 2013\Projects

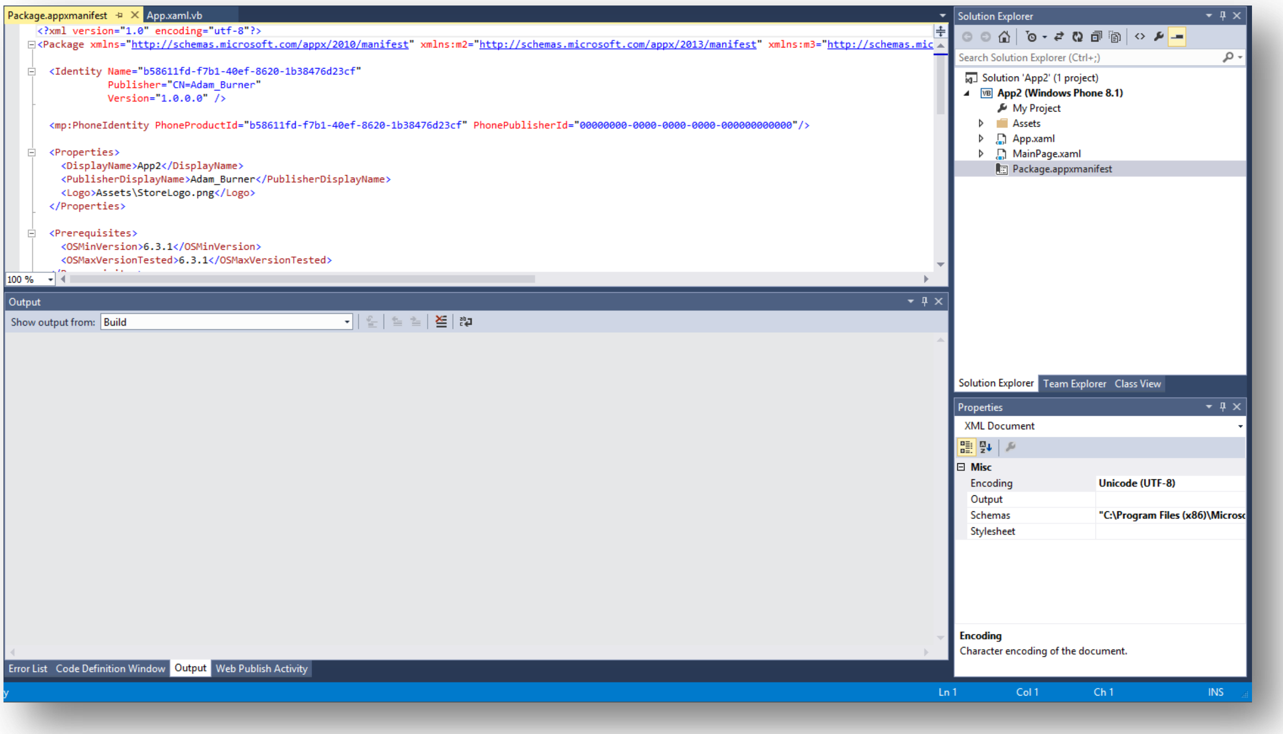
Solution: Create new solution

Solution name: App2

☑ Create directory for solution

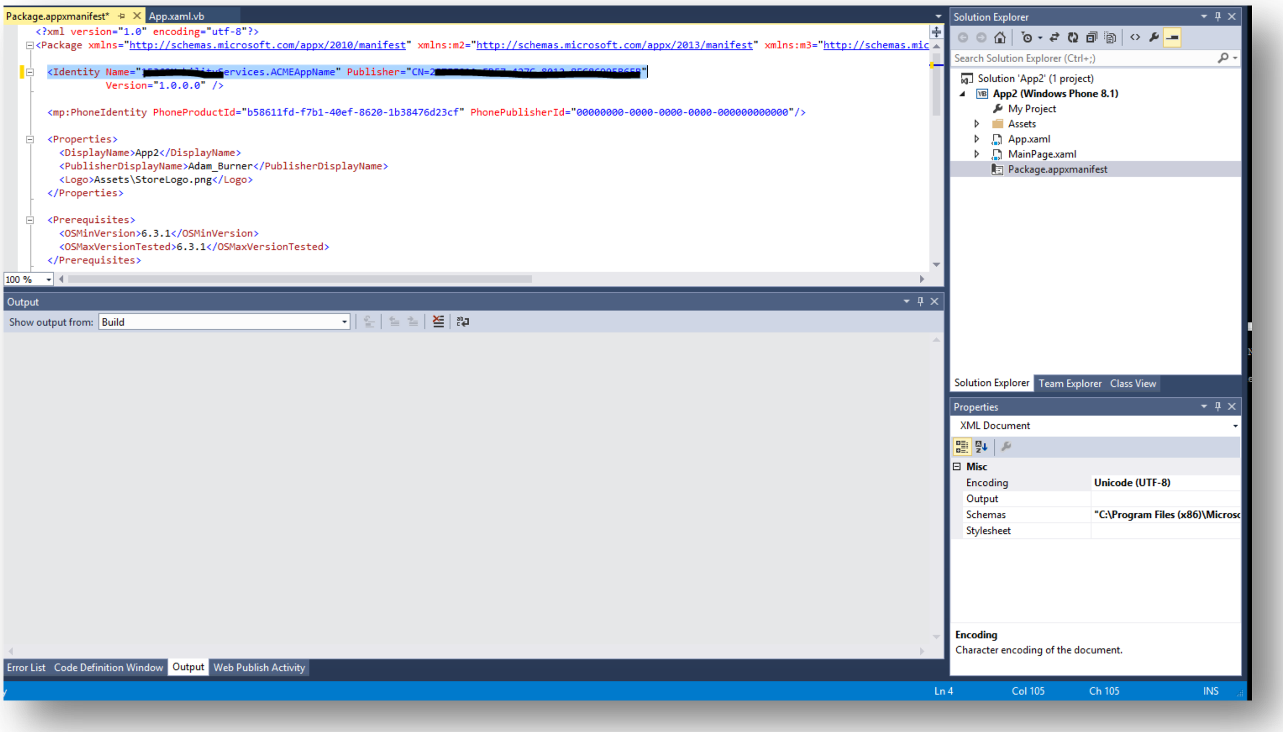
□ Add to source control

11. From the right pane, right-click **Package-appxmanifest** and click **View code**:



```
<?xml version="1.0" encoding="utf-8"?>
<Package xmlns="http://schemas.microsoft.com/appx/2010/manifest" xmlns:m2="http://schemas.microsoft.com/appx/2013/manifest" xmlns:m3="http://schemas.mic

  <Identity Name="b58611fd-f7b1-40ef-8620-1b38476d23cf"
            Publisher="CN=Adam_Burner"
            Version="1.0.0.0" />

  <mp:PhoneIdentity PhoneProductId="b58611fd-f7b1-40ef-8620-1b38476d23cf" PhonePublisherId="00000000-0000-0000-0000-000000000000"/>

  <Properties>
    <DisplayName>App2</DisplayName>
    <PublisherDisplayName>Adam_Burner</PublisherDisplayName>
    <Logo>Assets\StoreLogo.png</Logo>
  </Properties>

  <Prerequisites>
    <OSMinVersion>6.3.1</OSMinVersion>
    <OSMaxVersionTested>6.3.1</OSMaxVersionTested>
```

12. Within the Package.appxmanifest xml, (shown in the middle pane) replace the **Identity Name** and **Publisher** values with the corresponding **Identity Name** and **Publisher** values you retrieved from the **Services** item noted in **step 9**.



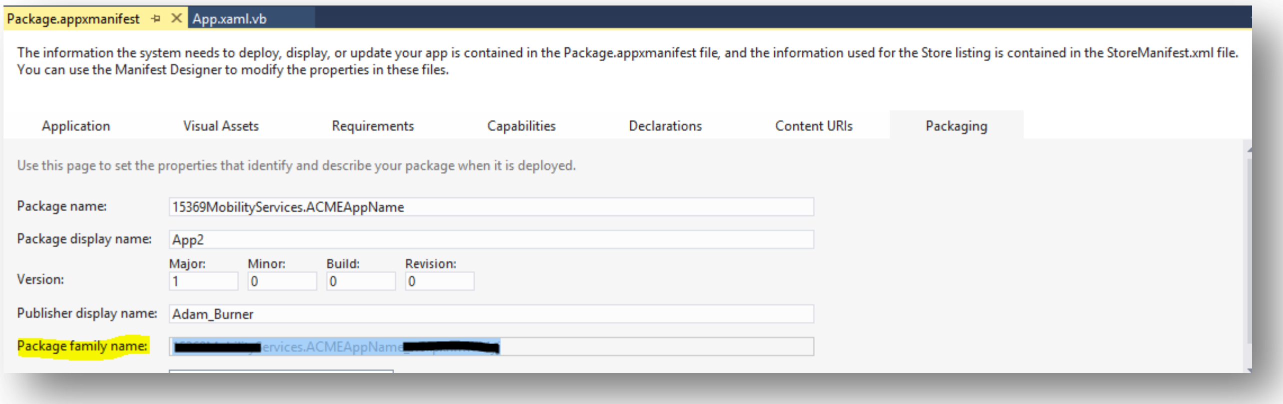
```
<?xml version="1.0" encoding="utf-8"?>
<Package xmlns="http://schemas.microsoft.com/appx/2010/manifest" xmlns:m2="http://schemas.microsoft.com/appx/2013/manifest" xmlns:m3="http://schemas.mic

  <Identity Name="[redacted]ervices.ACMEAppName" Publisher="CN=2[redacted]"
            Version="1.0.0.0" />

  <mp:PhoneIdentity PhoneProductId="b58611fd-f7b1-40ef-8620-1b38476d23cf" PhonePublisherId="00000000-0000-0000-0000-000000000000"/>

  <Properties>
    <DisplayName>App2</DisplayName>
    <PublisherDisplayName>Adam_Burner</PublisherDisplayName>
    <Logo>Assets\StoreLogo.png</Logo>
  </Properties>

  <Prerequisites>
    <OSMinVersion>6.3.1</OSMinVersion>
    <OSMaxVersionTested>6.3.1</OSMaxVersionTested>
  </Prerequisites>
```

Tip: A version string is required, as shown above.

13. Within the right pane, (where you right-clicked Package.appxmanifest) right click the **App name** reference at the top level (i.e, App2) and select **Build**. Once the build process has completed; right-click **Package.appxmanifest** and click **View Designer**.

Note: If you are prompted to close the first opened instance of Package.appxmanifest. Click **Yes**.

14. Within the **Package.appxmanifest** pane click the **Packaging** tab. Within this tab copy and paste the value for **Package family name** (PFN) to a notepad.



The information the system needs to deploy, display, or update your app is contained in the Package.appxmanifest file, and the information used for the Store listing is contained in the StoreManifest.xml file. You can use the Manifest Designer to modify the properties in these files.

Use this page to set the properties that identify and describe your package when it is deployed.

Package name: 15369MobilityServices.ACMEAppName

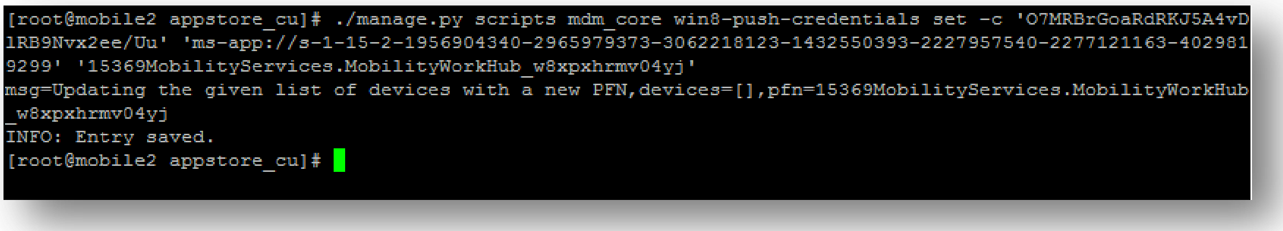
Package display name: App2

Version: Major: 1 Minor: 0 Build: 0 Revision: 0

Publisher display name: Adam_Burner

Package family name: [redacted]ervices.ACMEAppName[redacted]

15. Open an SSH shell to the Mobility server and access **/usr/local/nukona/appstore_cu/** by entering the following, as root:
    cd /usr/local/nukona/appstore_cu/
16. From within this directory enter following command entering the information saved from steps 9 and 14. Here is the **sintax: ./manage.py scripts mdm_core win8-push-credentials set -c '<client secret>' '<package_security_id>' '<pfn>'**



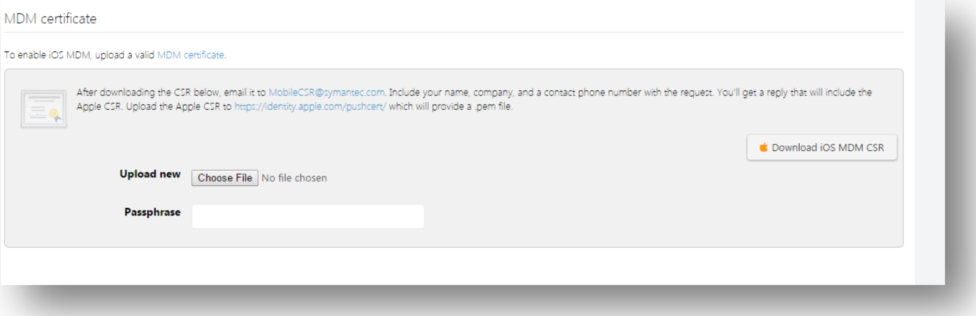
```
[root@mobile2 appstore_cu]# ./manage.py scripts mdm_core win8-push-credentials set -c 'O7MRBrGoaRdRKJ5A4vD
1RB9Nvx2ee/Uu' 'ms-app://s-1-15-2-1956904340-2965979373-3062218123-1432550393-2227957540-2277121163-402981
9299' '15369MobilityServices.MobilityWorkHub_w8xpxhrmv04yj'
msg=Updating the given list of devices with a new PFN,devices=[],pfn=15369MobilityServices.MobilityWorkHub
_w8xpxhrmv04yj
INFO: Entry saved.
[root@mobile2 appstore_cu]#
```

17. With the WPS configured, continue to Enrolling a Windows 8.1 Device

iOS MDM Certificate (HOWTO84066)

(Also known as a Mobile Device Management Push Certificate)

1. Download the Mobility Suite's CSR by going to **Settings > Certificates > iOS Certificates** from the Mobility Administrator Console and under MDM certificate, click **Download iOS CSR:**



MDM certificate

To enable iOS MDM, upload a valid MDM certificate.

After downloading the CSR below, email it to MobileCSR@symantec.com. Include your name, company, and a contact phone number with the request. You'll get a reply that will include the Apple CSR. Upload the Apple CSR to https://identity.apple.com/pushcert/ which will provide a .pem file.

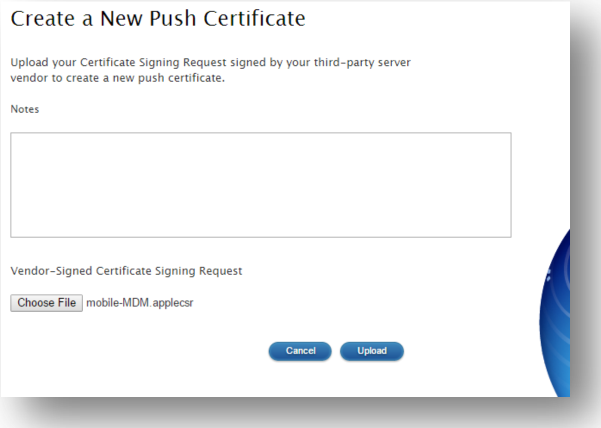
Upload new Choose File No file chosen

Passphrase

2. Email this CSR to mobilecsr@symantec.com. Once the signed CSR is returned, using a valid Apple ID, it may be submitted to: https://identity.apple.com/pushcert.

Note: SaaS users do not need to email the CSR to Symantec for signing.

3. Log into the Apple Push Certificate Portal using Chrome, Firefox or Safari and click **Create a Certificate.** Agreeing to the terms and conditions will allow the creation of a Mobile Device Management (MDM) certificate.
4. After agreeing to the terms and conditions click **Choose File** to select the signed CSR (ending in .applecsr) and click **Upload**:



Create a New Push Certificate

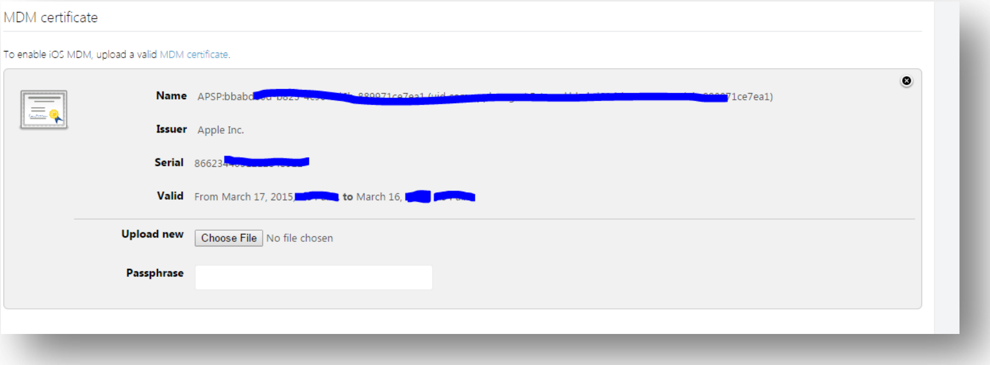
Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

Notes

Vendor-Signed Certificate Signing Request

Choose File mobile-MDM.applecsr

5. Click **Download** and upload the certificate (ending in .PEM) to **Settings** > **Certificates** > **Apple/iOS Certificates** under **MDM Certificate**…
6. Click **Choose File** and browse to the PEM certificate. Click **Upload,** the certificate details should now be displayed:



MDM certificate

To enable iOS MDM, upload a valid MDM certificate.

Name APSP:bbabd[redacted]1ce7ea1)

Issuer Apple Inc.

Serial 86623[redacted]

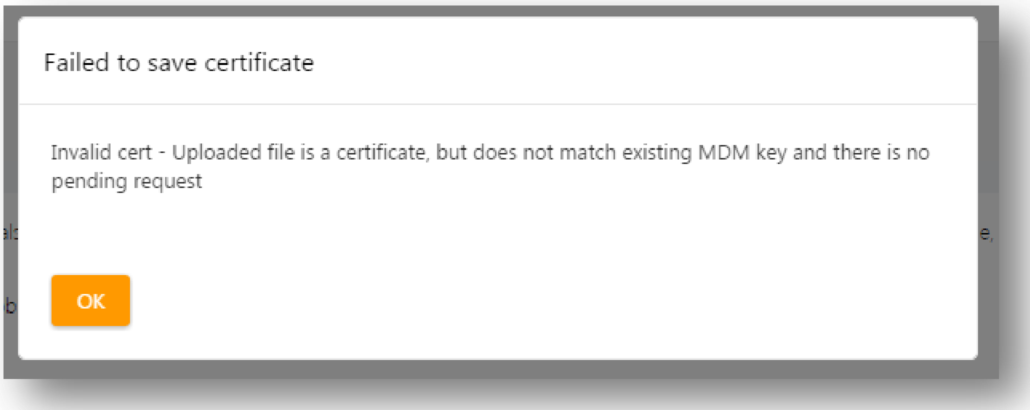
Valid From March 17, 2015[redacted] to March 16, [redacted]

Upload new Choose File No file chosen

Passphrase

IMPORTANT: It is vital to renew and not re-create this MDM Certificate on an annual basis. Take note of the Apple ID used to create this certificate so that it may be renewed 1 year from its creation.

Tip: If the below message is received. Repeate the **MDM Certificate** steps confirming that the correct certificate was emailed to Symantec for signing:



Failed to save certificate

Invalid cert - Uploaded file is a certificate, but does not match existing MDM key and there is no pending request

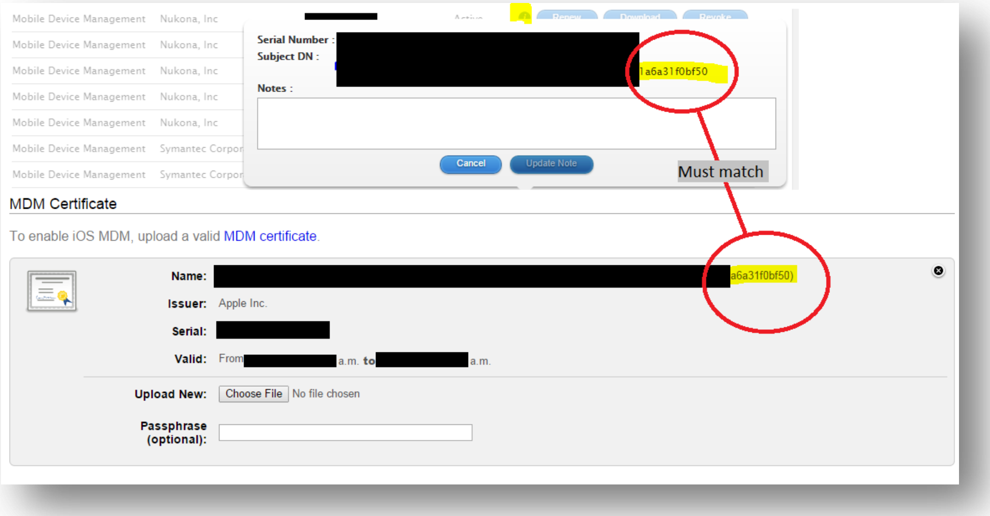
Renewing the iOS MDM Certificate (HOWTO110299)

Note: The following steps illustrate how to renew an expiring or expired MDM certificate. If this is a new installation, this part may be skipped and continue to Building the iOS Agent (HOWTO95463).

1. From the Mobility admin console, navigate to **Downloads** and click **Download iOS MDM CSR**. Save the certificate signing request (CSR) to the workstation. If using an on premise deployment of Mobility Suite email this CSR to mobilecsr@symantec.com. Do not continue until the signed CSR (ending in .applecsr) is returned.
2. Follow HOWTO109648 to match the mobile device management (MDM) certificate on https://identity.apple.com/pushcert/ with the mdm certificate in **Settings** > **Certificates** > **Apple/iOS certificates**.

Tip: Internet Explorer (IE) is not compatible with this Apple web portal.

3. Using Chrome, Firefox or Safari; navigate to https://identity.apple.com/pushcert/.
4. As stated in HOWTO109648 find the expiring MDM certificate and match its **Subject DN** with that of the MDM certificate **Name** in the Mobility **Admin console**.



Mobile Device Management Nukona, Inc [redacted] Active Renew Download Revoke
Mobile Device Management Nukona, Inc
Mobile Device Management Nukona, Inc
Mobile Device Management Nukona, Inc
Mobile Device Management Nukona, Inc
Mobile Device Management Symantec Corpor
Mobile Device Management Symantec Corpor

Serial Number : [redacted]
Subject DN : [redacted]1a6a31f0bf50

Notes :

Cancel Update Note

Must match

MDM Certificate

To enable iOS MDM, upload a valid MDM certificate.

Name: [redacted]a6a31f0bf50)
Issuer: Apple Inc.
Serial: [redacted]
Valid: From [redacted] a.m. to [redacted] a.m.

Upload New: Choose File No file chosen

Passphrase (optional):

Note: The above image is the Apple Signing portal page on the upper half and the iOS Certificates Admin Mobility page on the lower half.

5. Click Renew (**Renew**) and when the **Renew Push Certificate** page loads click **Choose File**.
6. Browse to the downloaded CSR (the certificate ending in **.applecsr**) from step 1 and click **Open**.
7. Click **upload** to renew the MDM certificate.
8. Once the confirmation page loads click **Download** and save the MDM_Nukona…pem certificate to the workstation.
9. Return to the Mobility **Admin console** > **Certificates** > **Apple/iOS certificates** and next to **Upload new** click **Choose File**.
10. Browse to the MDM_Nukona…pem certificate, from step 8, and click **Open**.
11. Now click Upload (**Upload**), in the upper-right, to save the new MDM certificate to the Mobility console.

Note: The devices will not immediately receive this new certificate. Users will need to either wait until their current MDM certificate expires, becomes invalid or is manually removed by going to Settings > General > Device Management. When removed any applications installed via MDM may be removed as well, this should only be done if the **Subject DN** of the old certificate does not match that of the new / replacement certificate. If they do match, there is no need to remove this certificate as the MDM certificate on the server will still be able to manage the device until it is gracefully replaced. Revoking the certificate from the Apple portal does not remove it from the device, if it needs to be removed, the user will have to do this manually. The Work Hub Agent will note that the certificate DN is not installed on the device and will prompt the user to install a new MDM certificate upon logging into the Agent. This installation will fail if the old MDM certificate (with a different DN) is not removed from the device.

How to replace an expiring SSL certificate
Re-sign the mobile device management (MDM) certificate

Note: To replace an expiring SSL certificate, replace the sign.crt, sign.key and gd_bundle.crt in the **/usr/local/nukona/certs/configurator/** with the new ones.

How to replace an expiring SSL certificate

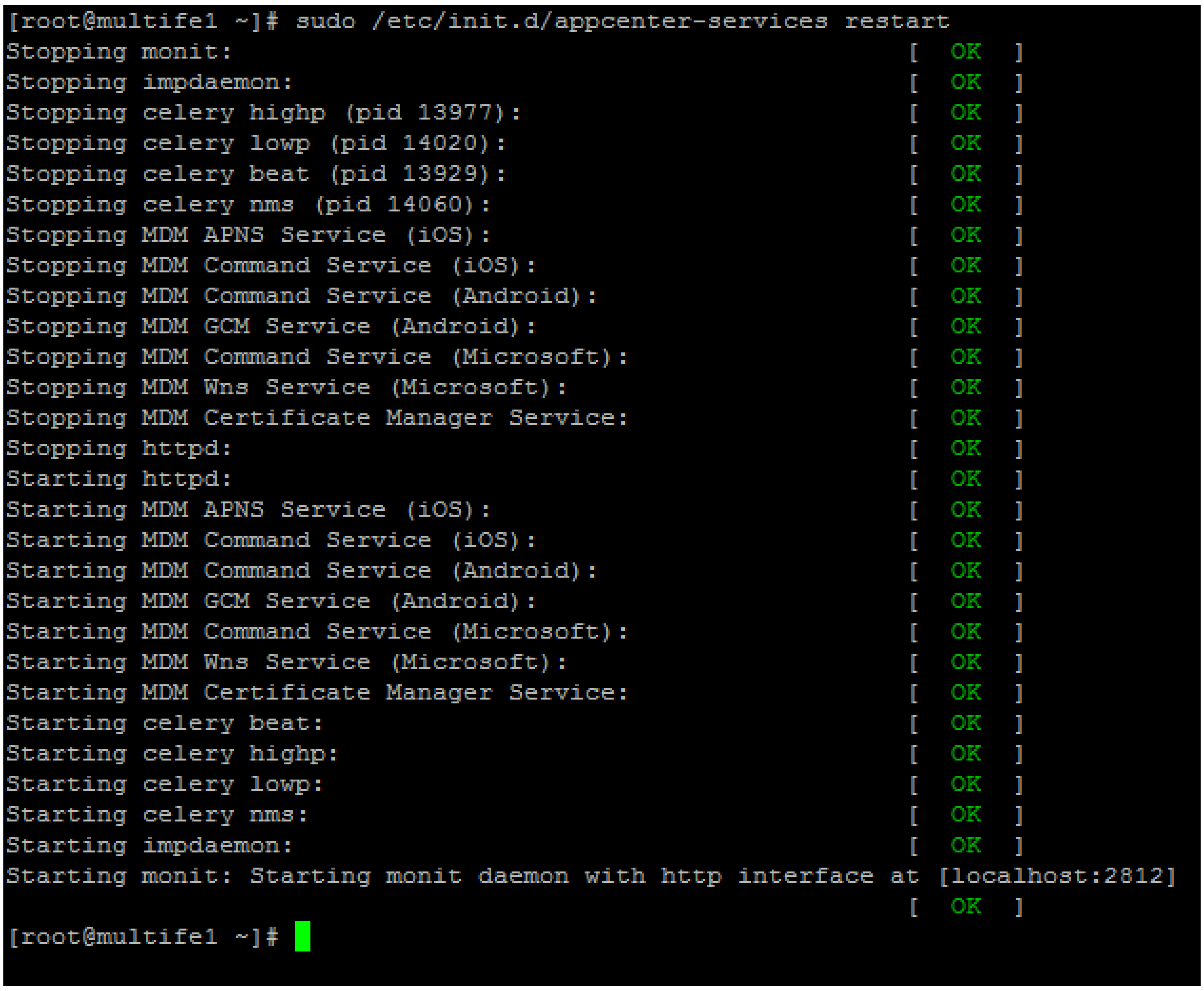
1. Follow HOWTO110248 to transfer the three new certificate files to each Mobility front end (FE); renaming them as necessary to match the names below. If the SSL certificate provided by the certificate authority (CA) is in PFX (PKCS personal exchange) follow HOWTO106999 to extract the three required certificates.

   /usr/local/nukona/certs/configurator/sign.crt
   Note: This is the PEM formatted public SSL certificate.

   /usr/local/nukona/certs/configurator/sign.key
   Note: This is the key file used to generate the certificate signing request (CSR) for the public SSL certificate.

   /usr/local/nukona/certs/configurator/gd_bundle.crt
   Note: This contains a PEM formatted certificate chain, most often is just the issuing CA certificate.

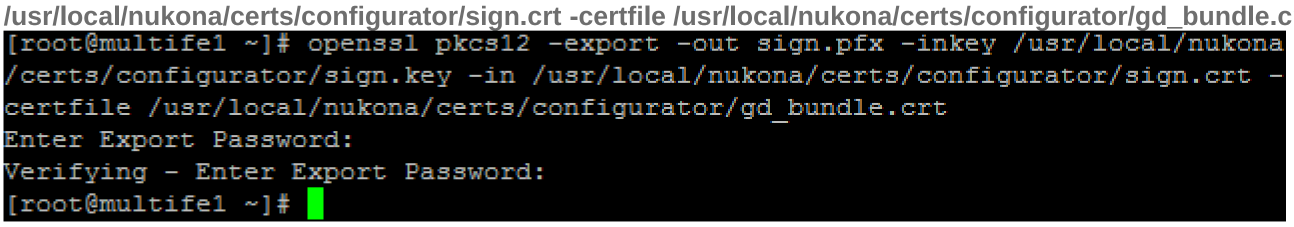
2. Enter the following, as root, from the FE:
   sudo /etc/init.d/appcenter-services restart



```
[root@multife1 ~]# sudo /etc/init.d/appcenter-services restart
Stopping monit:                                             [  OK  ]
Stopping impdaemon:                                         [  OK  ]
Stopping celery highp (pid 13977):                          [  OK  ]
Stopping celery lowp (pid 14020):                           [  OK  ]
Stopping celery beat (pid 13929):                           [  OK  ]
Stopping celery nms (pid 14060):                            [  OK  ]
Stopping MDM APNS Service (iOS):                            [  OK  ]
Stopping MDM Command Service (iOS):                         [  OK  ]
Stopping MDM Command Service (Android):                     [  OK  ]
Stopping MDM GCM Service (Android):                         [  OK  ]
Stopping MDM Command Service (Microsoft):                   [  OK  ]
Stopping MDM Wns Service (Microsoft):                       [  OK  ]
Stopping MDM Certificate Manager Service:                   [  OK  ]
Stopping httpd:                                             [  OK  ]
Starting httpd:                                             [  OK  ]
Starting MDM APNS Service (iOS):                            [  OK  ]
Starting MDM Command Service (iOS):                         [  OK  ]
Starting MDM Command Service (Android):                     [  OK  ]
Starting MDM GCM Service (Android):                         [  OK  ]
Starting MDM Command Service (Microsoft):                   [  OK  ]
Starting MDM Wns Service (Microsoft):                       [  OK  ]
Starting MDM Certificate Manager Service:                   [  OK  ]
Starting celery beat:                                       [  OK  ]
Starting celery highp:                                      [  OK  ]
Starting celery lowp:                                       [  OK  ]
Starting celery nms:                                        [  OK  ]
Starting impdaemon:                                         [  OK  ]
Starting monit: Starting monit daemon with http interface at [localhost:2812]
                                                            [  OK  ]

[root@multife1 ~]# 
```

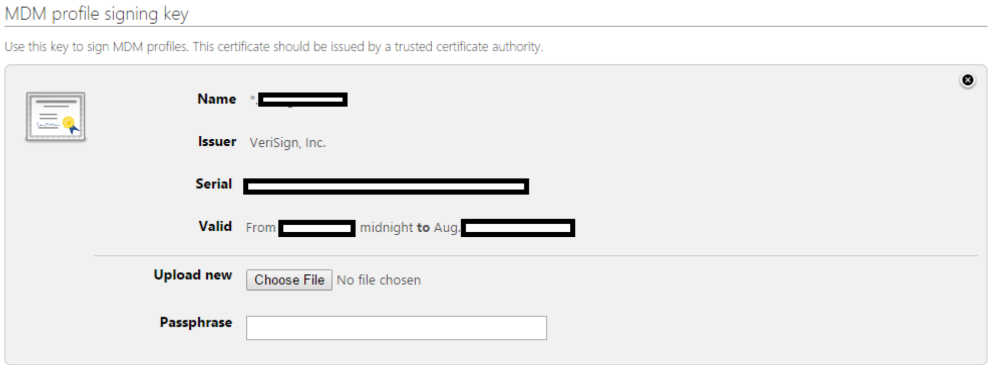
Re-sign the mobile device management (MDM) certificate

1. If the certificate is not already in PKCS format (from step 1 above) then run the following OpenSSL command, as root from the FE, to copy the sign.crt, sign.key and gd_bundle.crt files into a single PKCS file:
   openssl pkcs12 -export -out sign.pfx -inkey /usr/local/nukona/certs/configurator/sign.key -in /usr/local/nukona/certs/configurator/sign.crt -certfile /usr/local/nukona/certs/configurator/gd_bundle.crt



```
[root@multife1 ~]# openssl pkcs12 -export -out sign.pfx -inkey /usr/local/nukona
/certs/configurator/sign.key -in /usr/local/nukona/certs/configurator/sign.crt -
certfile /usr/local/nukona/certs/configurator/gd_bundle.crt
Enter Export Password:
Verifying - Enter Export Password:
[root@multife1 ~]# 
```

2. Transfer the **sign.pfx file** to the workstation following HOWTO110248.
3. Log into the tenant (https://<tenantFQDN>/admin/login) and navigate to **Admin console > Settings > Certificate > Apple / iOS certificates**
4. Scroll down to the bottom of the page, under **MDM profile signing key**, click **Choose File**, browse to the**sign.pfx** (or PKCS file provided by the CA) and click **Open**.
5. Scroll back to the top of the page and click Upload .



MDM profile signing key

Use this key to sign MDM profiles. This certificate should be issued by a trusted certificate authority.

Name [redacted]

Issuer VeriSign, Inc.

Serial [redacted]

Valid From [redacted] midnight to Aug [redacted]

Upload new Choose File No file chosen

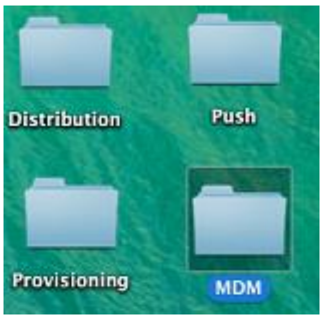
Passphrase

Important: For the following steps an Enterprise Apple Developer account is required. The enterprise level account is needed to distribute the iOS Work Hub Agent among multiple devices. The basic or free developer accounts cannot create **in-house** distribution profiles. As before, three methods will be shown: MAC, Linux and IIS. Choose the most familiar method.

Creating iOS certificates (HOWTO95463)

Note: Below are step-by-step instructions on how to create the series of certificates necessary to build the iOS Symantec Mobility Work Hub agent (client).

Tip: Create three folders named: Distribution, Push, Provisioning and MDM (to create iOS MDM, follow HOWTO84066); to keep track of each certificate with its associated CSR and P12/PFX.



How to create a distribution code-signing certificate

(Also referred to as an iOS Distribution certificate)

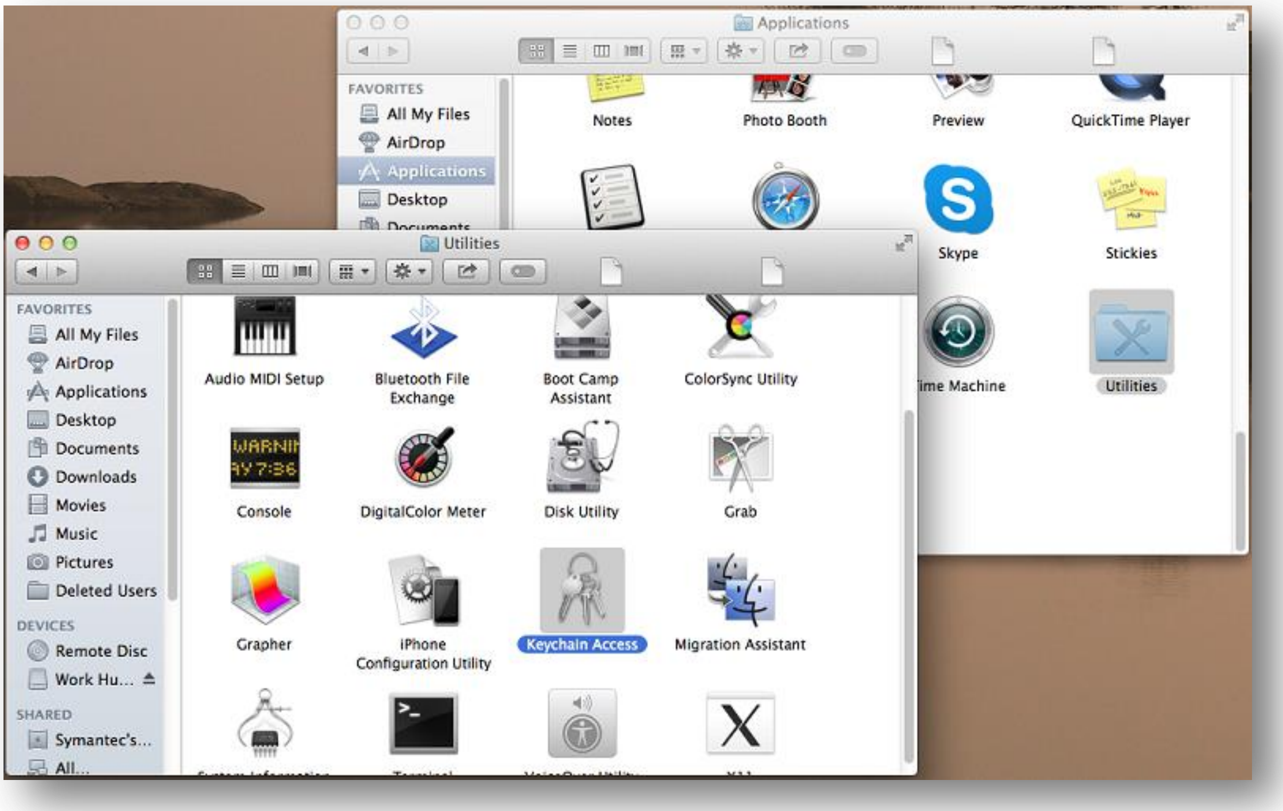
Create a CSR for Distribution:

Note: Use the developer's email address or leave the CN blank (not allowed in the IIS-Method). Choose from one of the three methods below:

OSX-Method
Linux-method
IIS-Method

OSX-Method:

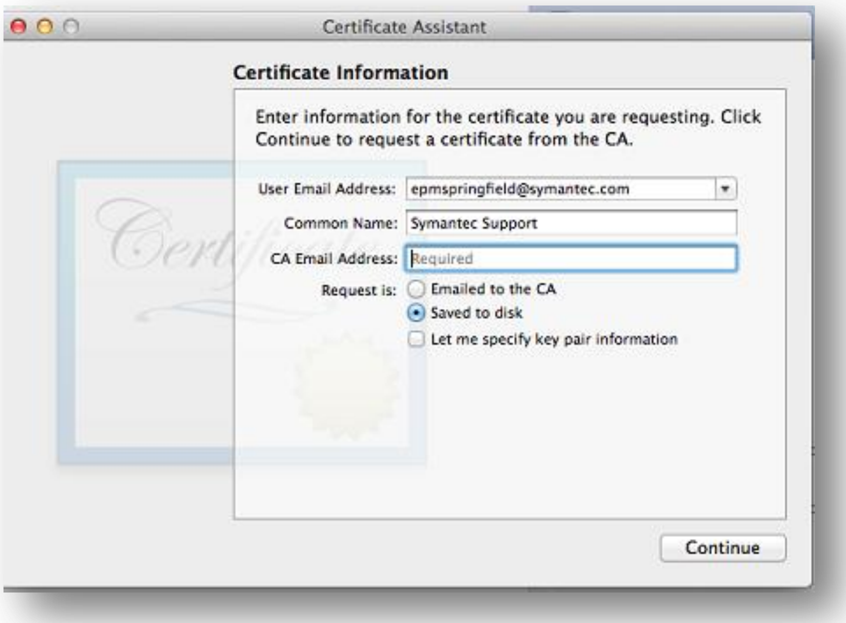
1. Open Keychain access in the Finder by browsing to **Applications** > **Utilities**.



2. Select the login keychain in the upper left-hand corner.

Note: All work will be done from the **login** keychain.

3. Select **Keychain Access** > **Certificate Assistant** at the top and select the **Request a Certificate from a Certificate Authority** option. Fill out the form with user information and select the **Save to disk** option and click continue.



Certificate Information

Enter information for the certificate you are requesting. Click Continue to request a certificate from the CA.

User Email Address: epmspringfield@symantec.com

Common Name: Symantec Support

CA Email Address: Required

Request is: ○ Emailed to the CA
● Saved to disk
□ Let me specify key pair information

4. Save this CSR to the Distribution folder (or to any ubiquitous location).
5. Once the CSR is created, continue to the In-House Distribution/Code-signing certificate portion of this guide.

Linux-method (**HOWTO123983**)

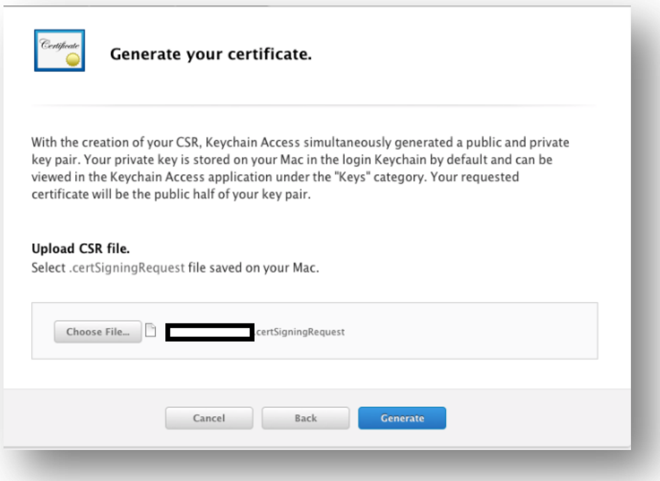
IIS-Method (**HOWTO59214**)

In-House Distribution/Code-signing certificate

1. Using Chrome, Firefox or Safari; open https://developer.apple.com and navigate to (**Account**) at the top.
2. Log in using the Enterprise Developer Account.
3. On the left, click **Certificates, IDs & Profiles**.
4. Select **Certificates** from the options and **Distribution**. Click the + symbol and select the **In-House and Ad Hoc** certificate option (see note below). Use the CSR created from Create a CSR for Distribution: click **Choose File…** and browse to the CSR file.
5. Click **Generate** and **Download** the **ios_distribution.cer** saving it to the **Distribution** folder.

Tip: Saving each CSR and certificate to their respective folders will greatly assist in gathering the required information to renew these certificates in the future.

Note: If the In-house Ad Hoc certificate option is greyed out, either the account is not an enterprise developer account or the maximum of two distribution certificates has already been created. In the second case, it will be necessary to obtain a P12 of this distribution certificate from whoever produced it. Revoking or deleting these certificates is not advisable as this will invalidate every app that has been distributed using the certificate.



Generate your certificate.

With the creation of your CSR, Keychain Access simultaneously generated a public and private key pair. Your private key is stored on your Mac in the login Keychain by default and can be viewed in the Keychain Access application under the "Keys" category. Your requested certificate will be the public half of your key pair.

Upload CSR file.
Select .certSigningRequest file saved on your Mac.

Choose File… [redacted] certSigningRequest

6. Once the certificate is created continue to the Import, convert and export certificates section, to convert the downloaded certificate to PFX/P12 format..

Import, convert and export the distribution certificate

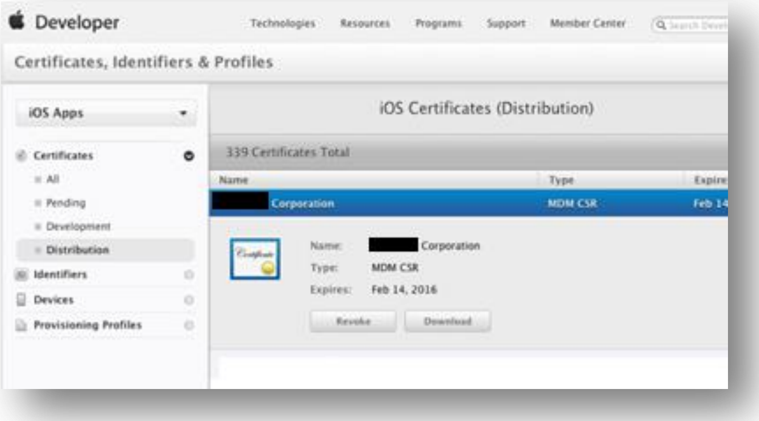
Note: For this step there are three options shown. Choose which option is most familiar:

OSX-Method:

[Linux-Method:](#)
[IIS-Method](#)

OSX-Method:

1. Download the newly created certificate (ios_distribution.cer) and install it to the keychain by opening the certificate with the Keychain application or manually importing the cert using the Keychain application:



iOS Certificates (Distribution)

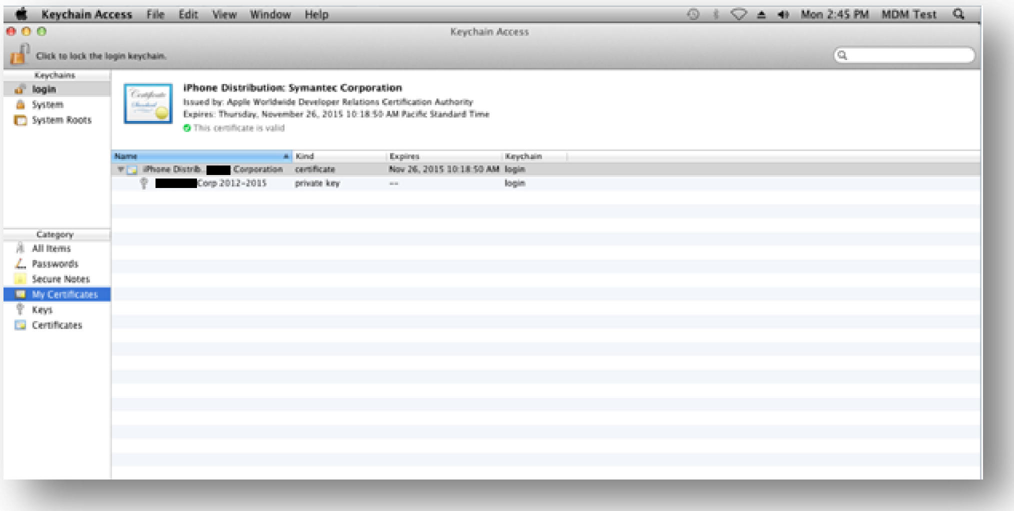
339 Certificates Total

Name	Type	Expire
[redacted] Corporation	MDM CSR	Feb 14

Name: [redacted] Corporation
Type: MDM CSR
Expires: Feb 14, 2016

Tip: To install or open any certificate in **Keychain**, simply click on the certificate, it will open in **Keychain**, by default.

2. The private key should be visible; associated with the certificate on the keychain as shown below:



iPhone Distribution: Symantec Corporation
Issued by: Apple Worldwide Developer Relations Certification Authority
Expires: Thursday, November 26, 2015 10:18:50 AM Pacific Standard Time
This certificate is valid

Name	Kind	Expires	Keychain
iPhone Distrib. [redacted] Corporation	certificate	Nov 26, 2015 10:18:50 AM	login
[redacted]Corp 2012-2015	private key	--	login

3. Right-click on the certificate and select **Export**. Save the exported Certificate as a **Personal Information Exchange (P12)** in the **Distribution** folder. Create a complex password to protect the P12.
4. Once the certificate has been successfully exported continue to the [Upload to Mobility](#) section.

*Linux-Method (**[HOWTO123984](#)**)*

*IIS-Method (**[HOWTO123984](#)**)*

Upload to Mobility

Upload the .p12/pfx certificate to the App Center Admin Console: **Settings** > **Certificates** > **Apple/iOS Certificates**; under the **Code-signing** section and click **Upload** in the upper-right of the page.

Once the certificate has been uploaded to the Mobility server, continue to the [Create a CSR for Push (HOWTO110247)](#) section of this guide.

How to create a Application Push Certificate (APN)

(Also known as the Apple Push Notification service SSL Certificate)

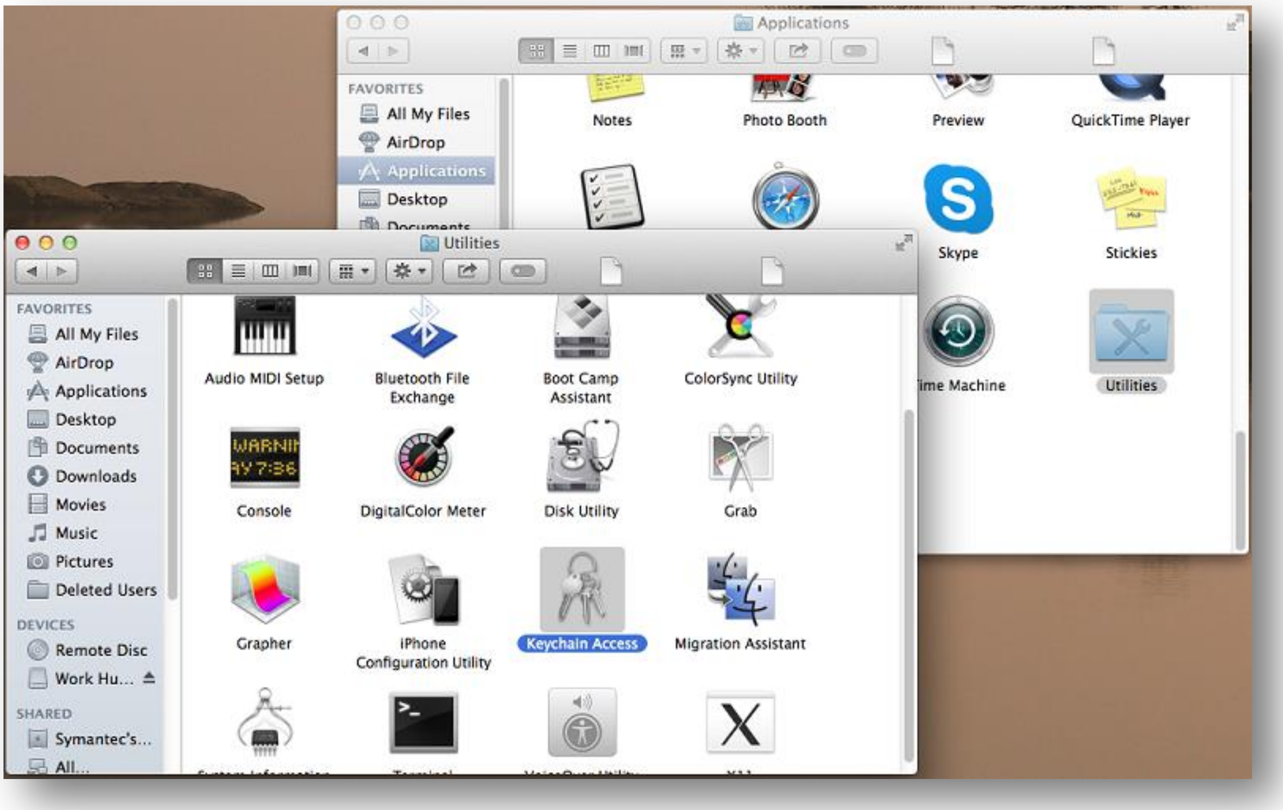
Create a CSR for Push:

Note: Use the developer's email address for Common Name (CN) or leave the CN blank (not allowed in the IIS-Method). Choose from one of the three methods below:

[OSX-Method](#)
[Linux-method](#)
[IIS-Method](#)

OSX-Method:

1. Open Keychain access in the Finder by browsing to **Applications and Utilities**

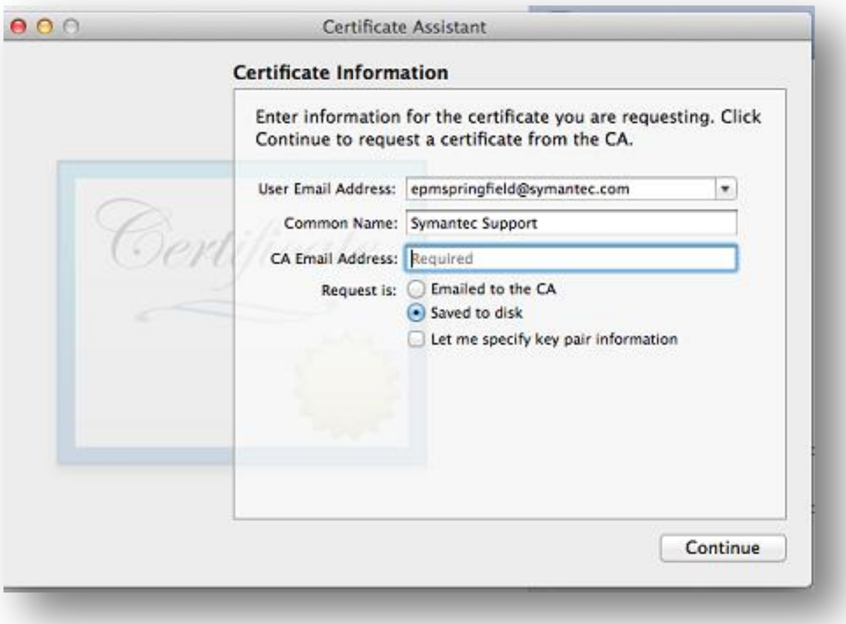


2. Select the login keychain in the upper left-hand corner.

Note: All work will be done from the **login** keychain.

3. Select **Keychain Access** > **Certificate Assistant** at the top and select the **Request a Certificate from a Certificate Authority** option. Fill out the form with user information and select the **Save to disk** option and click continue.

Note: The common name (CN) is arbitrary.



Certificate Assistant

Certificate Information

Enter information for the certificate you are requesting. Click Continue to request a certificate from the CA.

User Email Address: epmspringfield@symantec.com

Common Name: Symantec Support

CA Email Address: Required

Request is: ○ Emailed to the CA
● Saved to disk
□ Let me specify key pair information

Continue

4. Save this CSR to the Push folder (or to any ubiquitous location).
5. Once the CSR is created, continue to the Push Certificate section of this guide.

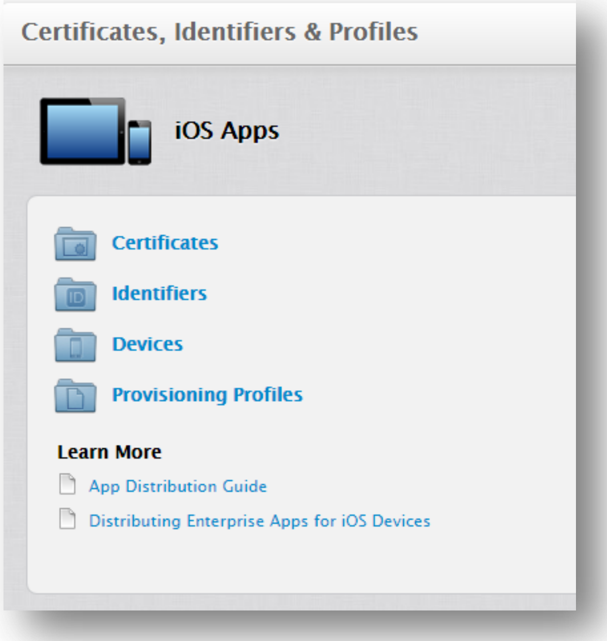
Linux-method (**HOWTO123985**)

IIS-Method (**HOWTO59214**)

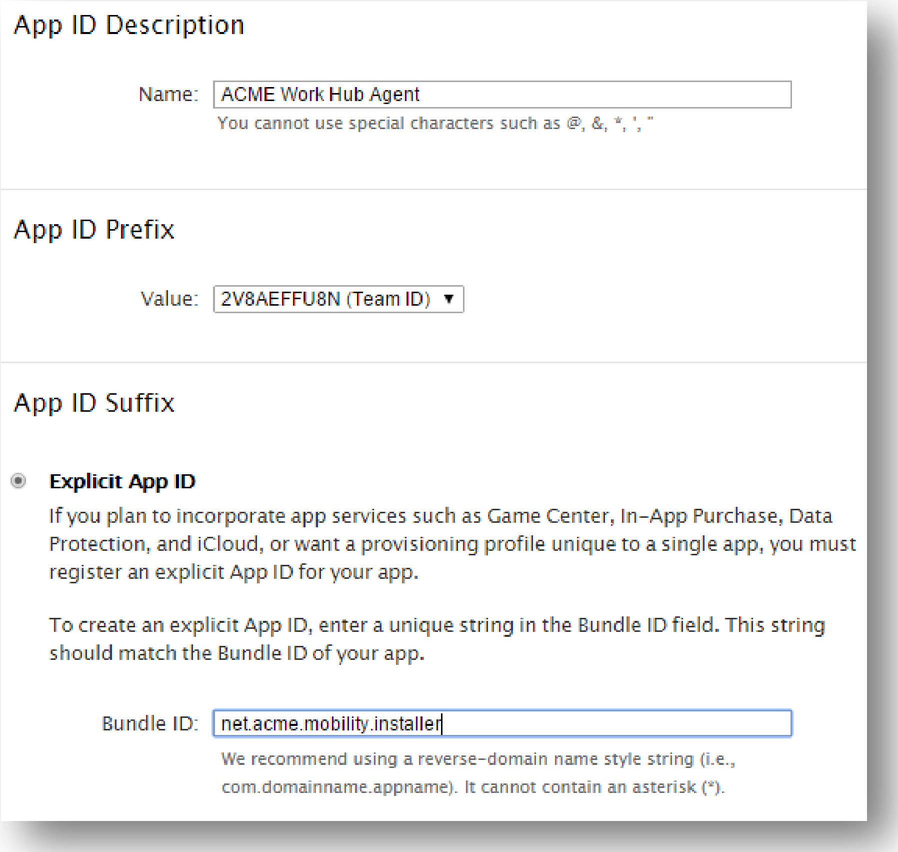
Push Certificate

1. Using Chrome, Firefox or Safari; open https://developer.apple.com and navigate to Member Center (**Account**) at the top.

2. Log in using the Enterprise Developer Account.
3. On the left, click **Certificates, IDs & Profiles**.
4. Select the **Identifiers** option from the list.



5. On the left under **Identifiers**, select **App IDs** and the + (+) symbol at the top:
6. Fill in the **App ID Description** Name field with something unique to identify the App ID from others, such as Your Company Mobile Agent.
7. **App Services** Select **Push Notifications or Services**
8. **App ID Prefix** should be the **Team ID**, if any, or the only option.
9. **Explicit App ID** is the domainSuffix.yourDomain.subDomain.installer For example if the App Center resides at: https://mobility.acme.com the Bundle ID would be: **com.acme.mobility.installer**.



App ID Description

Name: ACME Work Hub Agent

You cannot use special characters such as @, &, *, ', "

App ID Prefix

Value: 2V8AEFFU8N (Team ID) ▼

App ID Suffix

● **Explicit App ID**

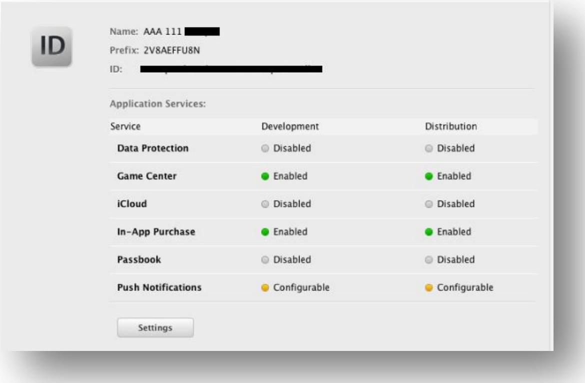
If you plan to incorporate app services such as Game Center, In-App Purchase, Data Protection, and iCloud, or want a provisioning profile unique to a single app, you must register an explicit App ID for your app.

To create an explicit App ID, enter a unique string in the Bundle ID field. This string should match the Bundle ID of your app.

Bundle ID: net.acme.mobility.installer

We recommend using a reverse-domain name style string (i.e., com.domainname.appname). It cannot contain an asterisk (*).

10. Reload the App ID's console by clicking on **App ID's** on the left; expand the newly created App ID and select the **Settings** button:



Name: AAA 111 [redacted]

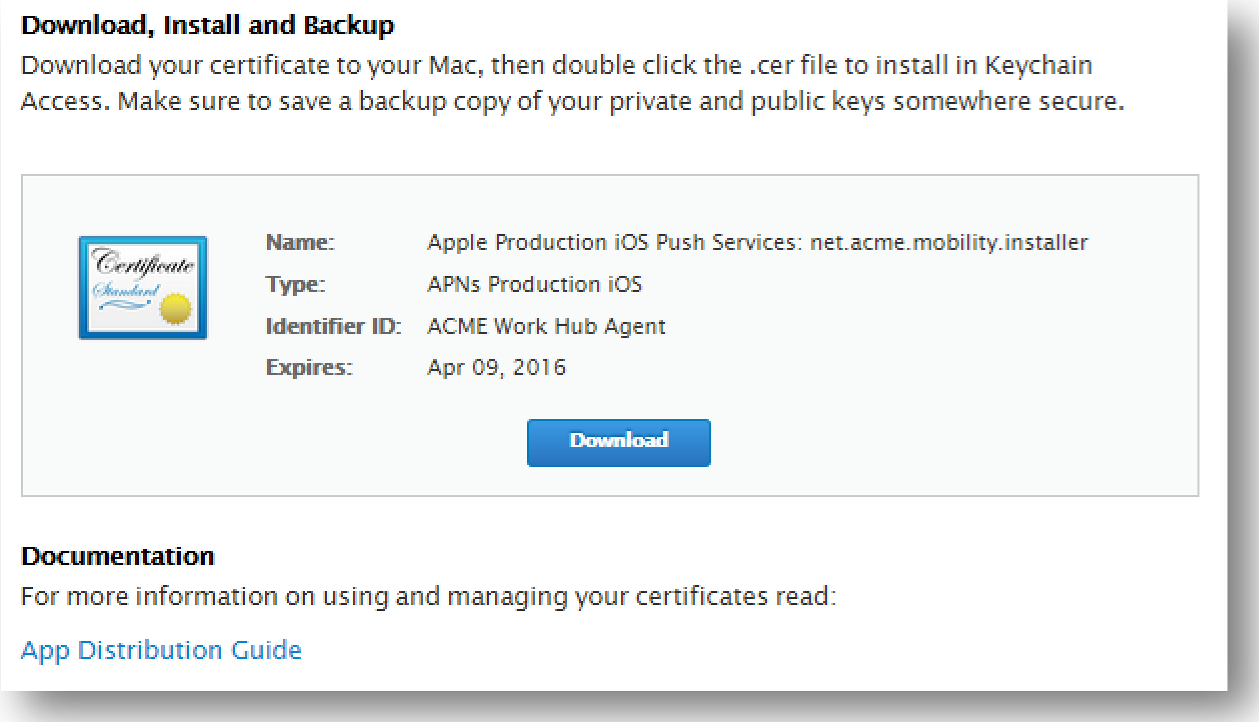
Prefix: 2V8AEFFU8N

ID: [redacted]

Application Services:

Service	Development	Distribution
Data Protection	○ Disabled	○ Disabled
Game Center	● Enabled	● Enabled
iCloud	○ Disabled	○ Disabled
In-App Purchase	● Enabled	● Enabled
Passbook	○ Disabled	○ Disabled
Push Notifications	● Configurable	● Configurable

11. Scroll down and under the Push Notifications options list select **Create Certificate** under the **Production SSL Certificate** section.
12. Upload the new CSR file created from [Create a CSR for Push]; click **Generate** and **Download**; save this file to the **Push** folder (to keep track of it).



Download, Install and Backup

Download your certificate to your Mac, then double click the .cer file to install in Keychain Access. Make sure to save a backup copy of your private and public keys somewhere secure.

Name: Apple Production iOS Push Services: net.acme.mobility.installer

Type: APNs Production iOS

Identifier ID: ACME Work Hub Agent

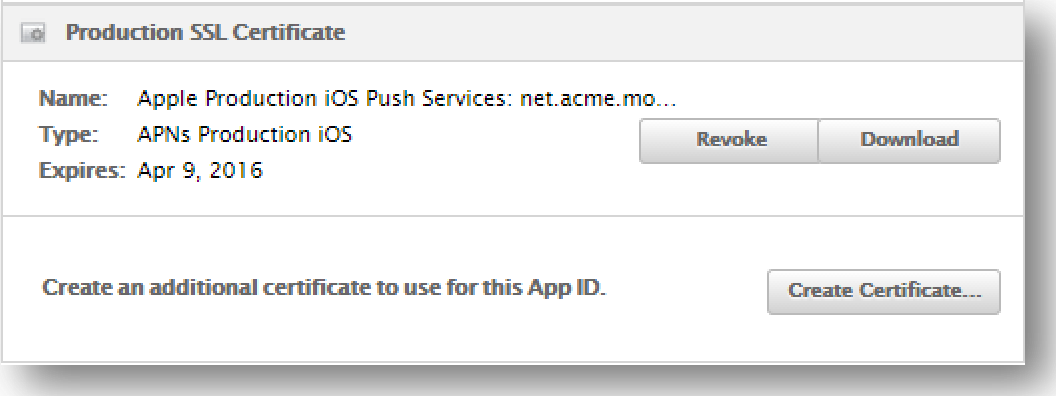
Expires: Apr 09, 2016

Documentation

For more information on using and managing your certificates read:

App Distribution Guide

13. Refresh the App ID console and expand the App ID and verify that a **Production SSL Certificate** has been created.



Production SSL Certificate

Name: Apple Production iOS Push Services: net.acme.mo...

Type: APNs Production iOS

Expires: Apr 9, 2016

Create an additional certificate to use for this App ID.

14. Once the aps_production.cer has been created, continue to the [Import, convert and export the push certificate] section of this guide.

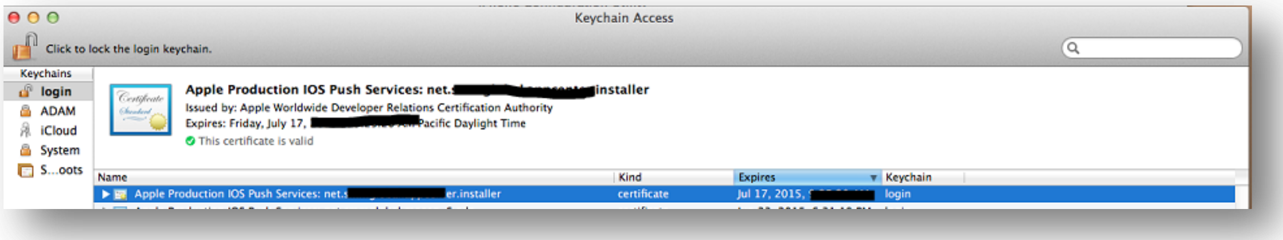
Import, convert and export the push certificate

Note: For this step there are three options shown. Choose which option is most familiar:

[OSX-Method:]
[Linux-Method:]
[IIS-Method]

OSX-Method:

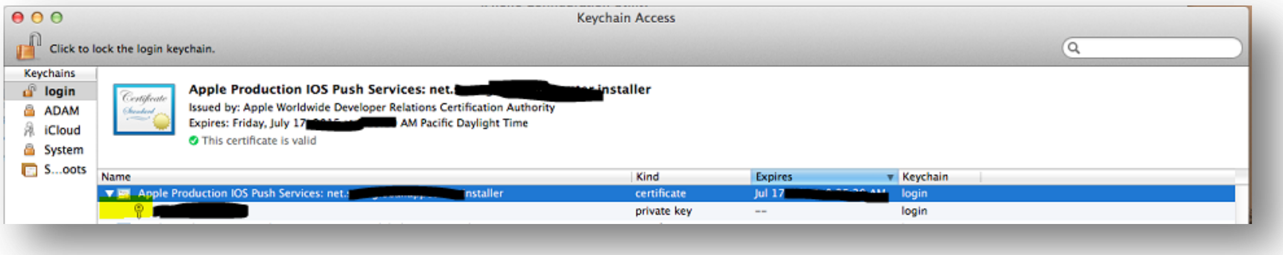
1. Take the downloaded certificate (apn_production.cer) and install it to the keychain by opening the certificate with the Keychain application or manually importing the cert using the Keychain application:



Apple Production IOS Push Services: net.[redacted]installer
Issued by: Apple Worldwide Developer Relations Certification Authority
Expires: Friday, July 17, [redacted]Pacific Daylight Time
This certificate is valid

Name	Kind	Expires	Keychain
Apple Production IOS Push Services: net.[redacted]er.installer	certificate	Jul 17, 2015, [redacted]	login

2. The private key should be visible; associated with the certificate on the keychain as shown below:



Apple Production IOS Push Services: net.[redacted]installer
Issued by: Apple Worldwide Developer Relations Certification Authority
Expires: Friday, July 17[redacted] AM Pacific Daylight Time
This certificate is valid

Name	Kind	Expires	Keychain
Apple Production IOS Push Services: net.[redacted]nstaller	certificate	Jul 17[redacted]	login
[redacted]	private key	--	login

3. Right-click on the certificate and select **Export**. Save the exported Cert as a **Personal Information Exchange (P12)** in the Code-Signing folder.
4. Once the certificate has been successfully exported continue to the Upload Push certificate to Mobility section of this guide.

*Linux-Method (**HOWTO123986**)*

*IIS-Method (**HOWTO123986**)*

Upload Push certificate to Mobility

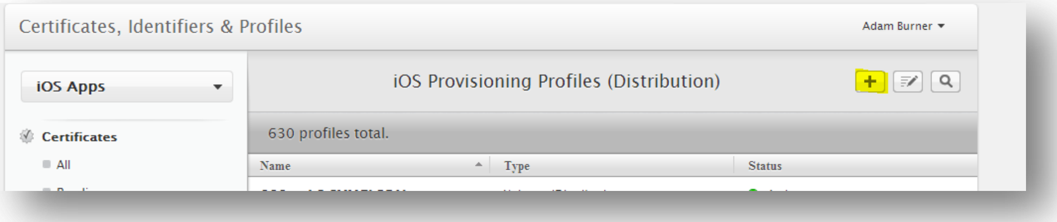
Upload the .p12/pfx push certificate to the App Center Admin Console: **Settings** > **Certificates** > **Apple/iOS Certificates**; under the **Push Certificate** section:

Once the certificate has been successfully uploaded to the console, continue to the Distribution Profile step.

Distribution Profile

(Also known as a iOS Distribution Provisioning Profile)

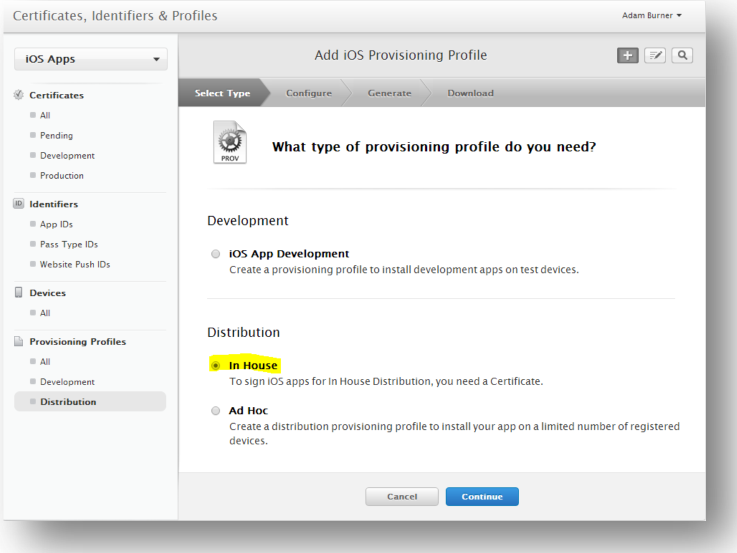
1. Using Chrome, Firefox or Safari; open https://developer.apple.com and navigate to Member Center (**Account**) at the top.
2. Log in using the Enterprise Developer Account.
3. On the left, click **Certificates, IDs & Profiles**.
4. Select **Provisioning Profiles**.
5. Click the + button at the top:


Certificates, Identifiers & Profiles
Adam Burner
iOS Apps
Certificates
All
iOS Provisioning Profiles (Distribution)
+

630 profiles total.

Name	Type	Status

6. Under the area labeled **Distribution** Select **In House** and click continue:



What type of provisioning profile do you need?

Development

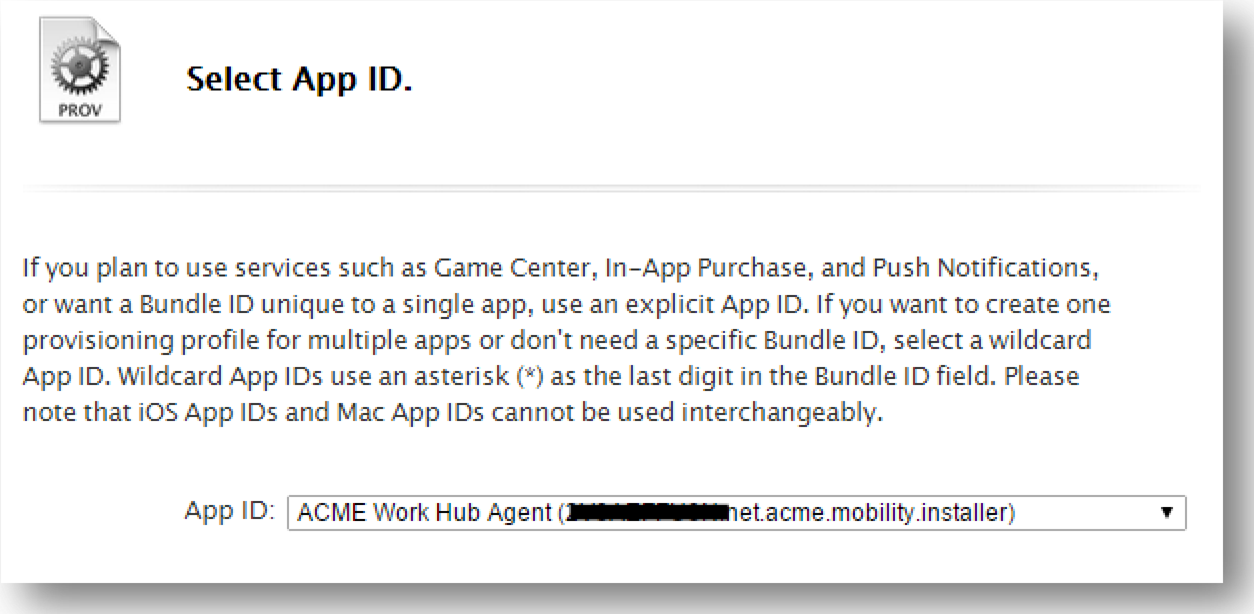
○ iOS App Development
Create a provisioning profile to install development apps on test devices.

Distribution

● In House
To sign iOS apps for In House Distribution, you need a Certificate.

○ Ad Hoc
Create a distribution provisioning profile to install your app on a limited number of registered devices.

7. Next, select the **App ID** that was created from the **Creating Certificates for App Center** section and select **Continue**:

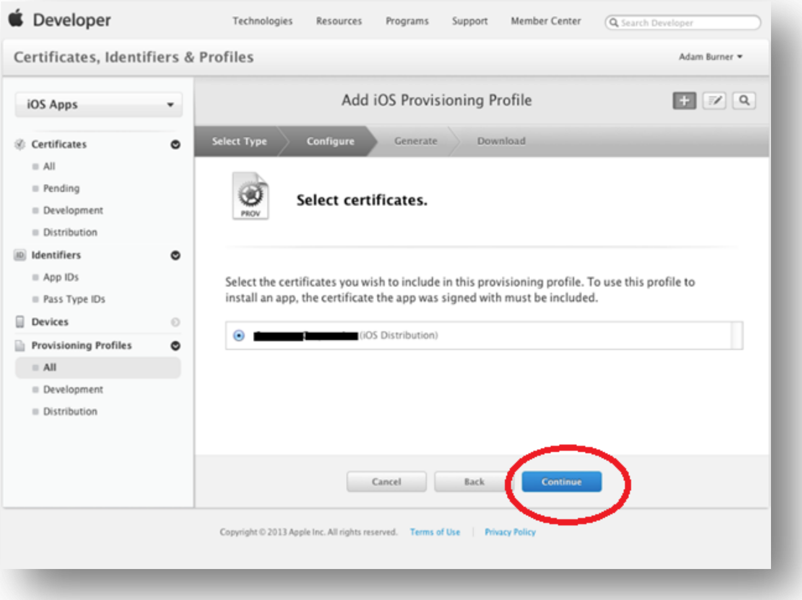


Select App ID.

If you plan to use services such as Game Center, In-App Purchase, and Push Notifications, or want a Bundle ID unique to a single app, use an explicit App ID. If you want to create one provisioning profile for multiple apps or don't need a specific Bundle ID, select a wildcard App ID. Wildcard App IDs use an asterisk (*) as the last digit in the Bundle ID field. Please note that iOS App IDs and Mac App IDs cannot be used interchangeably.

App ID: ACME Work Hub Agent ([redacted]net.acme.mobility.installer) ▼

8. Select the Distribution certificate by clicking the radio button to its left and click **Continue**:

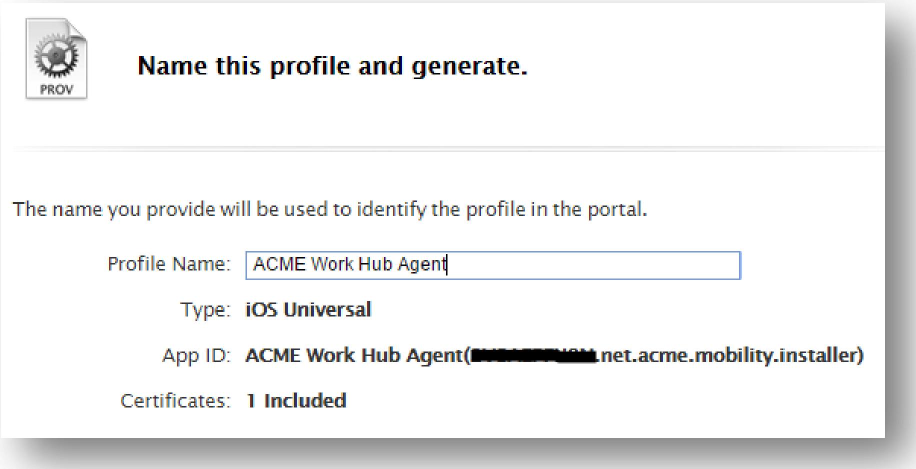


Select certificates.

Select the certificates you wish to include in this provisioning profile. To use this profile to install an app, the certificate the app was signed with must be included.

● [redacted](iOS Distribution)

9. Name the iOS Provisioning Profile with something unique. Advance to the next screen after verifying that the App ID and Developer Certificate are both included in the profile.



Name this profile and generate.

The name you provide will be used to identify the profile in the portal.

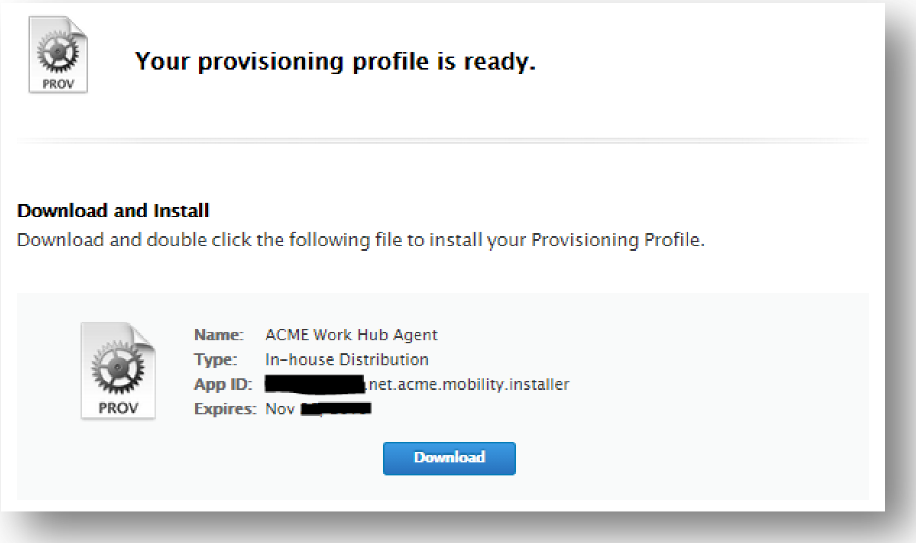
Profile Name: ACME Work Hub Agent

Type: iOS Universal

App ID: ACME Work Hub Agent([redacted].net.acme.mobility.installer)

Certificates: 1 Included

10. Download the Provisioning Profile to the workstation:



Your provisioning profile is ready.

Download and Install

Download and double click the following file to install your Provisioning Profile.

Name: ACME Work Hub Agent

Type: In-house Distribution

App ID: [redacted].net.acme.mobility.installer

Expires: Nov [redacted]

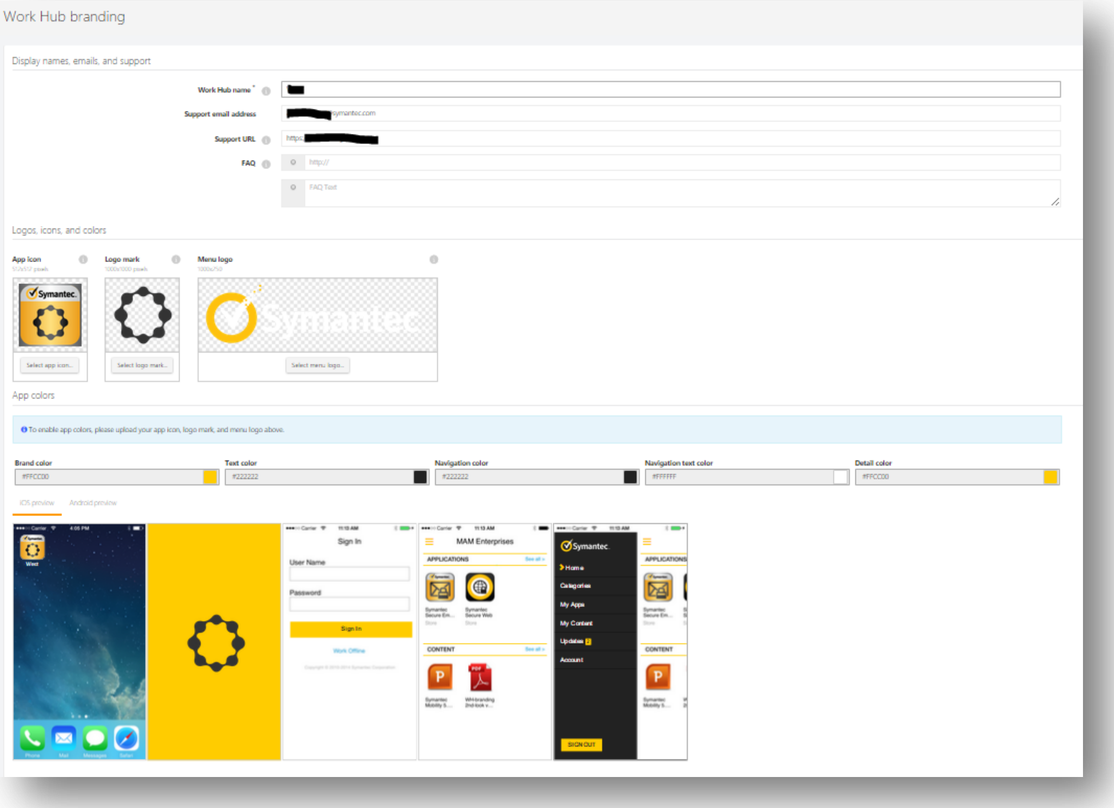
The below three certificates should now be created:

- iOS Distribution Certificate (also known as the code-signing certificate) (P12 or PFX)
- APNS (Push) Certificate (P12 or PFX)
- Mobile Provisioning Profile (for the above APNS: App-id).

11. Verify that the certificates are uploaded to Mobility by navigating to **Settings** > **Certificates** > **Apple/iOS Certificates**.
12. Once the Provisioning Profile is downloaded to the workstation, continue to the In-browser Work Hub Builder section of this guide, to build the iOS Work Hub agent / client.

In-browser Work Hub Builder

1. Before building the iOS client go to **Settings** > **Device Configuration** > **Work Hub branding**. Review the options available to further customize the Work Hub Agent:



Work Hub branding

Display names, emails, and support

Work Hub name * [redacted]

Support email address [redacted]symantec.com

Support URL https:[redacted]

FAQ http://

FAQ Text

Logos, icons, and colors

App icon 512x512 pixels — Select app icon...

Logo mark 1000x1000 pixels — Select logo mark...

Menu logo 1000x750 — Select menu logo...

App colors

To enable app colors, please upload your app icon, logo mark, and menu logo above.

Brand color #FFCC00

Text color #222222

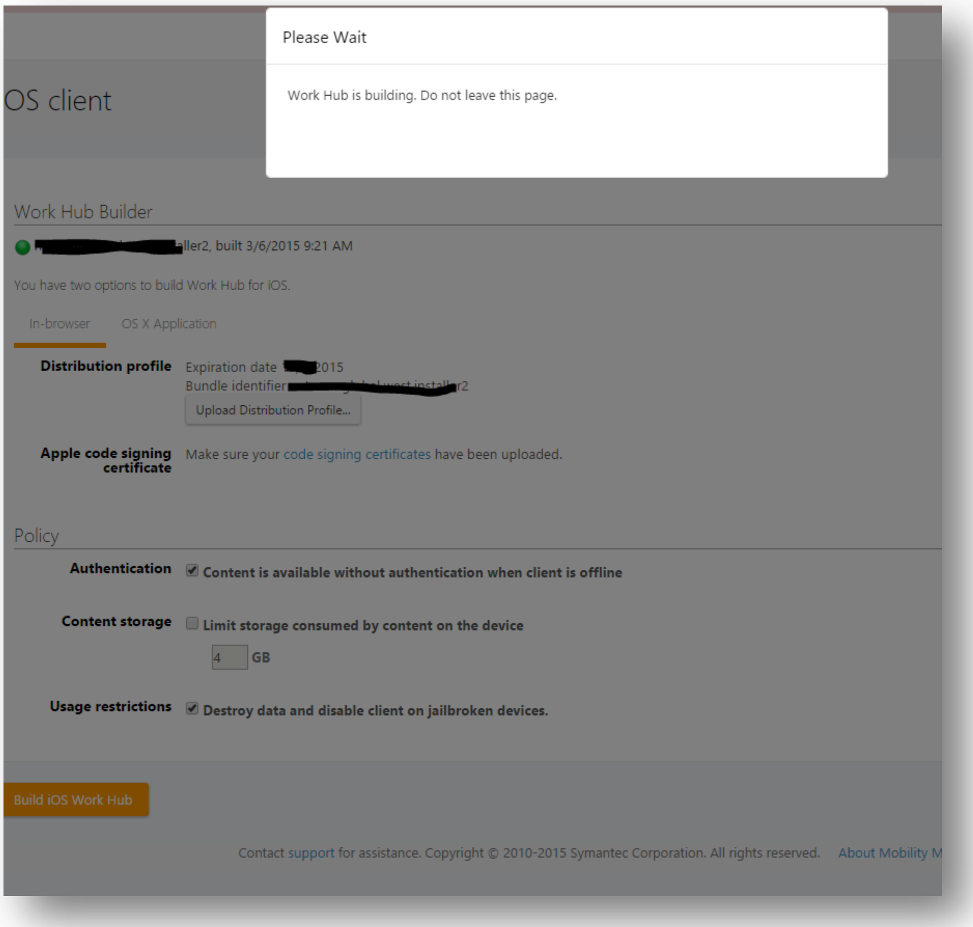
Navigation color #222222

Navigation text color #FFFFFF

Detail color #FFCC00

iOS preview | Android preview

2. Now go the Mobility Suite **Administrative Console** > **Settings > Device Configuration > iOS client**.
3. Upload the distribution certificate and click **Build iOS Work Hub:**



Please Wait

Work Hub is building. Do not leave this page.

OS client

Work Hub Builder

[redacted]ller2, built 3/6/2015 9:21 AM

You have two options to build Work Hub for iOS.

In-browser | OS X Application

Distribution profile Expiration date [redacted]2015
Bundle identifier [redacted]r2
Upload Distribution Profile...

Apple code signing certificate Make sure your code signing certificates have been uploaded.

Policy

Authentication ☑ Content is available without authentication when client is offline

Content storage □ Limit storage consumed by content on the device
4 GB

Usage restrictions ☑ Destroy data and disable client on jailbroken devices.

Build iOS Work Hub

Contact support for assistance. Copyright © 2010-2015 Symantec Corporation. All rights reserved. About Mobility M

4. Once the iOS Work Hub Agent is successfully built continue to the Work Mail section of this guide.

How to renew iOS certificates and profiles (HOWTO110304)

Note: The below steps outline how to renew and **not** replace the existing iOS certificates necessary to manage iOS devices and or applications. For Apple published documentation on these processes click here. To renew the MDM certificate see Renewing iOS MDM External: (HOWTO110299)

Important: If following the A to Z document, there is no need to complete these renewal steps; continue to the Building the Android Work Hub Agent, section of this guide.

Renewing the Apple Push Notification (APN) certificate

Note: As of December 17th 2015 the "APNs Production iOS" certificate name has been changed to "Apple Push Services." For On-Prem Customers on any version before 5.4.2, please see the note at the bottom before trying to upload a new Push Certificate. Please see http://www.symantec.com/docs/HOWTO95536 for more information.

1. Using Chrome, Firefox or Safari; open https://developer.apple.com and navigate to Member Center (**Account**) at the top.
2. Log in using the Enterprise Developer Account.
3. On the left, click **Certificates, IDs & Profiles**.
4. Once the new page loads, click **Identifiers**.
5. Next to the heading **iOS App IDs** click on the 🔍 (search icon) and enter the app id (bundle identifier) of the Mobility Work Hub Agent.

Tip: The app id of the Work Hub Agent may be found by opening the Mobility tenant **Admin console > Settings > Device Configuration > iOS client**; under the label **Bundle Identifier**.

6. Click on the App ID, in the search results.
7. Click **Edit** at the bottom.
8. Under the area labeled **Production SSL Certificate,** the expiring APN certificated will be shown.

Note: Two certificates may be created at one time. Revoke the certificate that is currently not in use. Match the certificate's expiration with the one found in the **Admin console > Settings > Apple/iOS certificates** under **Push Certificate**.

9. Click **Create Certificate…**
10. Select **Continue**.
11. See HOWTO110247 to create a new certificate signing request (CSR).
12. Click **Choose File…** and browse to the newly created CSR and click **Open**.
13. Click **Generate** and after the page reloads, **Download** the new APN certificate to the workstation.
14. Once the new APN certificate has been downloaded continue to the Import, convert and export certificates step.

Renewing the Apple iOS Distribution (code-signing) certificate

Note: The below steps outline how to renew the iOS Distribution certificate. Unlike the APN certificate, it is not advisable to revoke this certificate unless is has been compromised. Click here for more details.

1. Using Chrome, Firefox or Safari; open https://developer.apple.com and navigate to Member Center (**Account**) at the top.
2. Log in using the Enterprise Developer Account.
3. On the left, click **Certificates, IDs & Profiles**.
4. Click **Certificates**.
5. After the page loads, under **Certificates** select **Production**.
6. Search by the certificate name found in the Mobility **Admin console > Settings > Apple/iOS certificates** under the **Code Signing** section.
7. Search for expiring **iOS Distribution** certificate and confirm that this is indeed the code-signing certificate used by Mobility.

Tip: The certificate name is usually the company's name. To ID a certificate, download it to a workstation and open it using the **Certificate Viewer**. Or simply match the expiration dates.

8. Now that the certificate is identified as being managed by this iOS Developer Account, click the + (plus symbol) at the top.
9. Under the **Production** section select **In-House** and click **Continue** at the bottom.
15. Follow HOWTO110247 to create a new certificate signing request (CSR).
16. Click **Choose File…** and browse to the newly created CSR and click **Open**.
17. Click **Generate** and after the page reloads, **Download** the new Distribution certificate to the workstation.

18. Once the new distribution certificate has been downloaded, continue to the Import, convert and export certificates step.

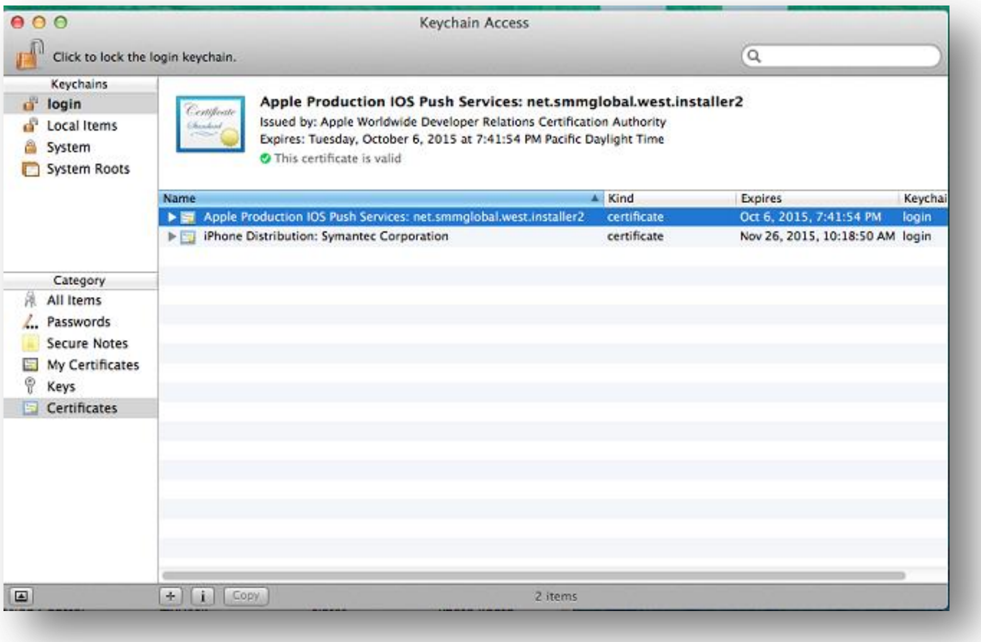
Import, convert and export certificates

Note: Repeat this section for both the Push and Distribution (code-signing) certificates. For this step there are three options shown. Choose which option is most familiar:

OSX-Method:
Linux-Method:
IIS-Method

OSX-Method:

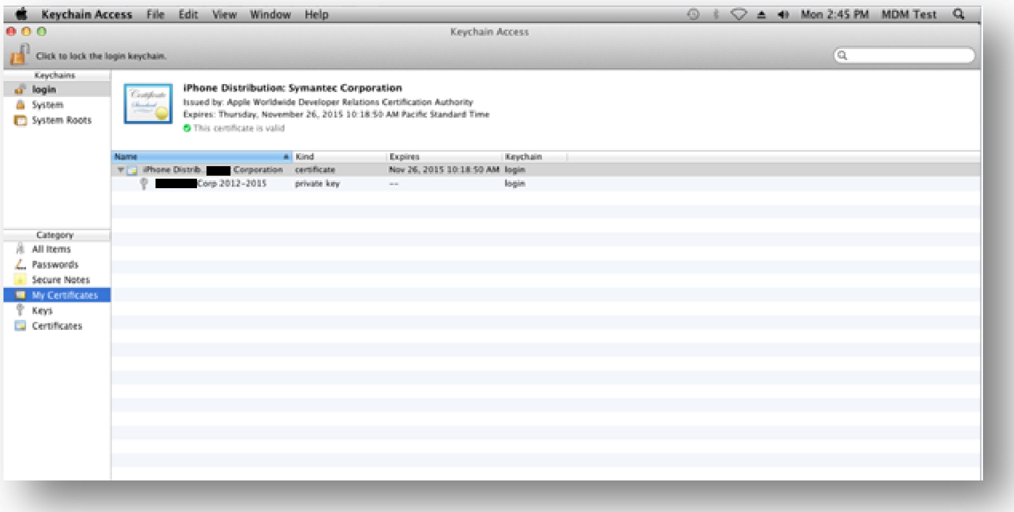
5. Download the newly created certificate (ios_distribution.cer or aps_distribution.cer) and install it to the keychain by opening the certificate with the Keychain application or manually importing the cert using the Keychain application:



Apple Production IOS Push Services: net.smmglobal.west.installer2
Issued by: Apple Worldwide Developer Relations Certification Authority
Expires: Tuesday, October 6, 2015 at 7:41:54 PM Pacific Daylight Time
This certificate is valid

Name	Kind	Expires	Keychai
Apple Production IOS Push Services: net.smmglobal.west.installer2	certificate	Oct 6, 2015, 7:41:54 PM	login
iPhone Distribution: Symantec Corporation	certificate	Nov 26, 2015, 10:18:50 AM	login

6. The private key should be visible; associated with the certificate on the keychain, see below:



iPhone Distribution: Symantec Corporation
Issued by: Apple Worldwide Developer Relations Certification Authority
Expires: Thursday, November 26, 2015 10:18:50 AM Pacific Standard Time
This certificate is valid

Name	Kind	Expires	Keychain
iPhone Distrib. [redacted] Corporation	certificate	Nov 26, 2015 10:18:50 AM	login
[redacted]Corp 2012-2015	private key	--	login

7. Right-click on the certificate and select **Export**. Save the exported Cert as a Personal Information Exchange (P12) in the Code-Signing folder. Protect the certificate with a complex password.
8. Once the certificate has been successfully exported continue to the Upload to Mobility step.

Linux-Method (HOWTO123987)

IIS-Method (HOWTO123987)

How to renew a Provisioning Profile

Note: The below steps outline how to regenerate iOS Distribution In-house Provisioning Profile. Click here for more information on maintaining in-house applications.

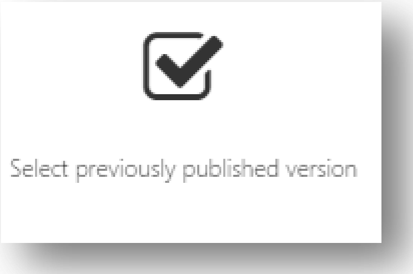
1. Using Chrome, Firefox or Safari; open https://developer.apple.com and navigate to Member Center (**Account**) at the top.
2. Log in using the Enterprise Developer Account.
3. On the left, click **Certificates, IDs & Profiles**.
4. Click **Provisioning Profiles**.
5. After the page loads, under **Provisioning Profiles** select **Production**.
6. Search by the provisioning profile name.
7. Click on the result to expand the preview.

Tip: Since iOS 8.0, profiles cannot be viewed from the device itself. X-Code may be used to view the profile installed on an iOS device. Click here for more detailed instructions on how to view provisioning profiles installed on a device using x-code. X-code requires a MAC.

8. At the bottom click **Edit**.
9. After the edit page loads, select the new Distribution Certificate created from HOWTO110304.
10. Click **Generate** and after the page reloads, click **Download**.
11. Use the newly downloaded provisioning profile to re-sign the in-house Application or rebuild the iOS Work Hub Agent.

How to replace the iOS provisioning profile used by a secure Web Application

1. If renewing the provisioning profile used by an iOS secure web app, navigate to the Mobility **Admin console > Apps** and select the app containing the expiring or invalid provisioning profile.
2. Click the ⬆ (upload symbol) next to the **Product Version** bar.
3. Click the option to use a **previously published version.**



4. Select the latest version (in most cases only one available version is shown).
5. Scroll down to **Provisioning** section and click **Browse**.
6. Browse to the downloaded profile and click **Open**.
7. Click Save and set version (**Save and set version**).

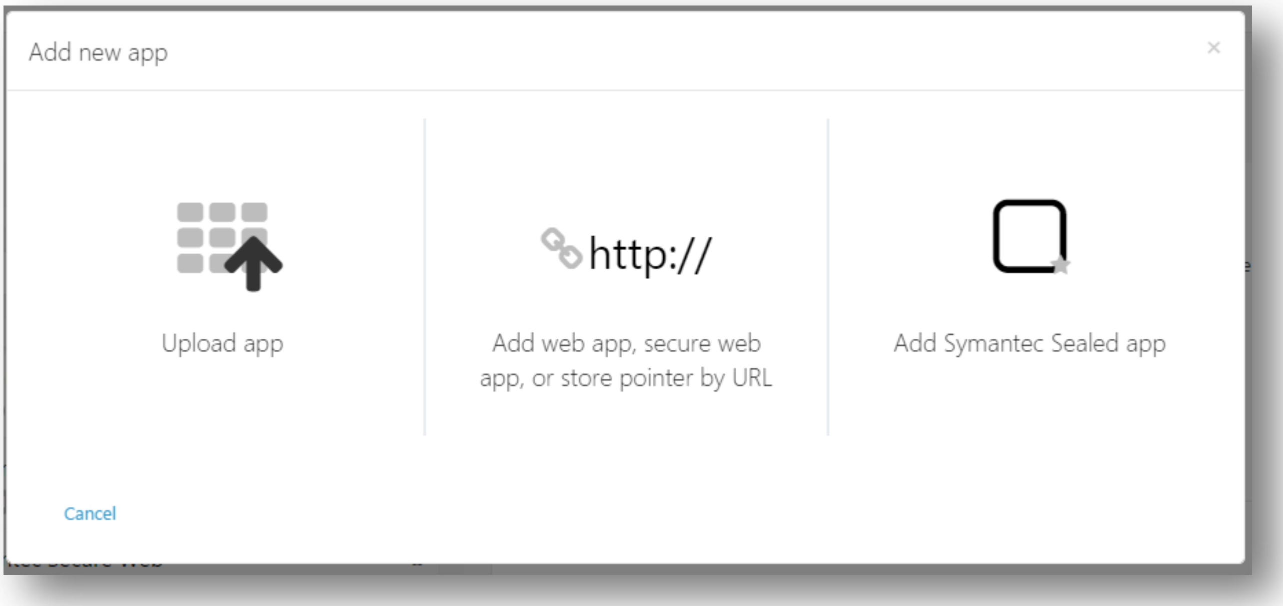
Building the Android Work Hub Agent

To build the Android work hub agent, first review the work hub branding options as described in In-browser Work Hub Builder. Once all the branding options are saved go to **settings > device configuration > Android client** and click **Build Android Work Hub**.

Note: All enrolled users may receive a notification that a new Work Hub Agent is available.

Work Mail (HOWTO83809)

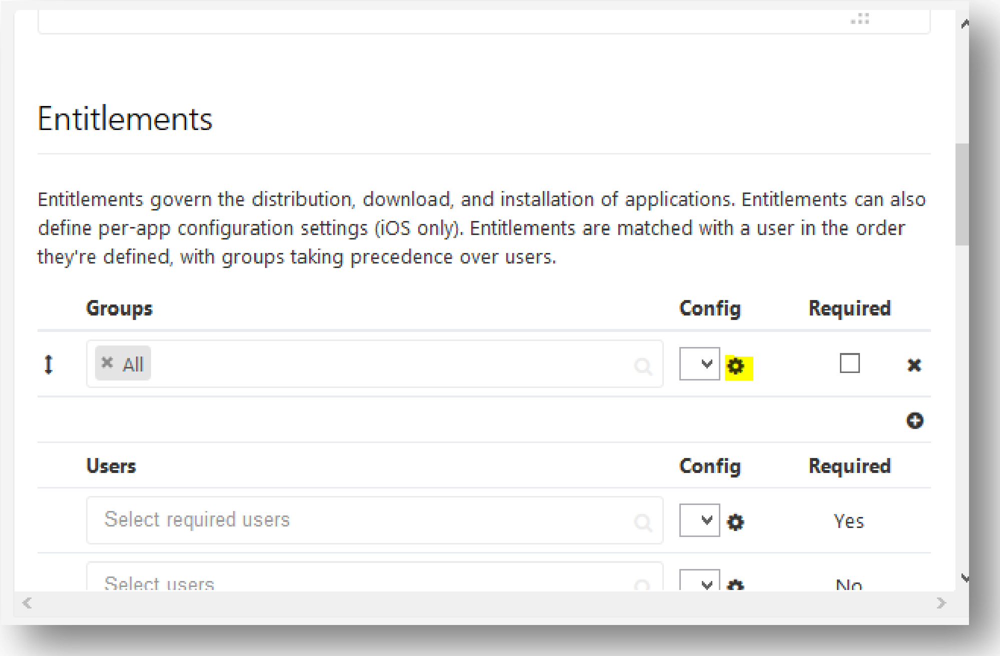
1. To add Work Mail to the tenant first go to the tenant **Admin console** > **Apps** and click **Add App** in the upper right of the page.
2. Click **Add Symantec Sealed app**.



3. Select the **Work Mail / Secure Email** for both iOS and Android.
4. Click **Add Sealed apps**.
5. Allow up to 5 minutes for all the app meta-data to load.

Tip: This is the point where outbound communication over port 80 to play.google.com and itunes.apple.com is important. If the app cannot be added refer to the **/var/log/nukona/appstore.log** file for details

6. Navigate to the Work Mail app for iOS and next to **Product Version** click the (edit icon).
7. Take note of the groups and users' entitlements options. Add or remove specific groups or users as needed.
8. Under the **Config** column click on the gear icon:



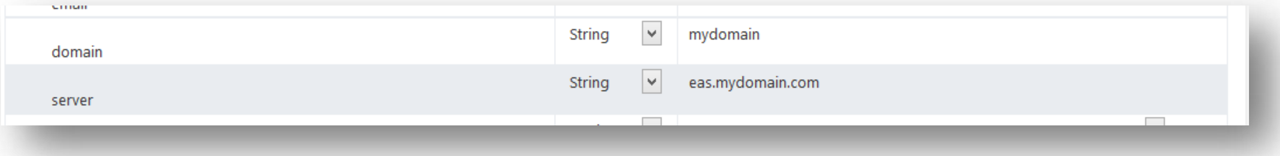
Entitlements

Entitlements govern the distribution, download, and installation of applications. Entitlements can also define per-app configuration settings (iOS only). Entitlements are matched with a user in the order they're defined, with groups taking precedence over users.

Groups	Config	Required
× All	⚙	□

Users	Config	Required
Select required users	⚙	Yes
Select users	⚙	No

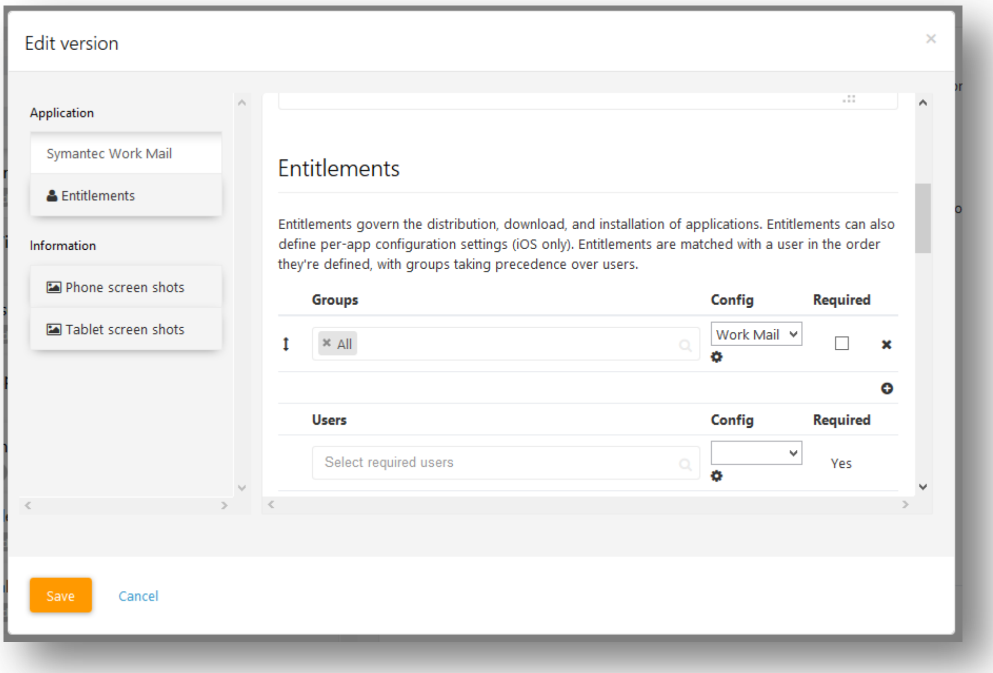
9. In the new window click **New**.
10. In a new tab, go to TECH226407 and download the **PermissiveSSEConfig.plist**.
11. Back to the original tab and click the (upload icon) and browse and upload the **PermissiveSSEConfig.plist** file.
12. Change the key values to reflect environment's Exchange Active Sync (EAS) server and domain settings:



domain	String	mydomain
server	String	eas.mydomain.com

13. Click (save icon) and **Close**.

14. Now select the newly created config from the list and click **Save:**



Entitlements

Entitlements govern the distribution, download, and installation of applications. Entitlements can also define per-app configuration settings (iOS only). Entitlements are matched with a user in the order they're defined, with groups taking precedence over users.

Groups	Config	Required
All	Work Mail	□

Users	Config	Required
Select required users		Yes

15. Repeat this process for the Android Work Mail Application.

Tip: By default Mobility Suite is set to install all iOS Applications via MDM. Until an MDM policy is created, the application installation will fail. To set install any application without MDM click on the very top edit icon of the application details page and uncheck these settings. To toggle this default setting go to **Settings** > **Device configuration** > **Device management**. Mobile Application Management (MAM) only deployments of Mobility Suite will need to have this setting turned off.

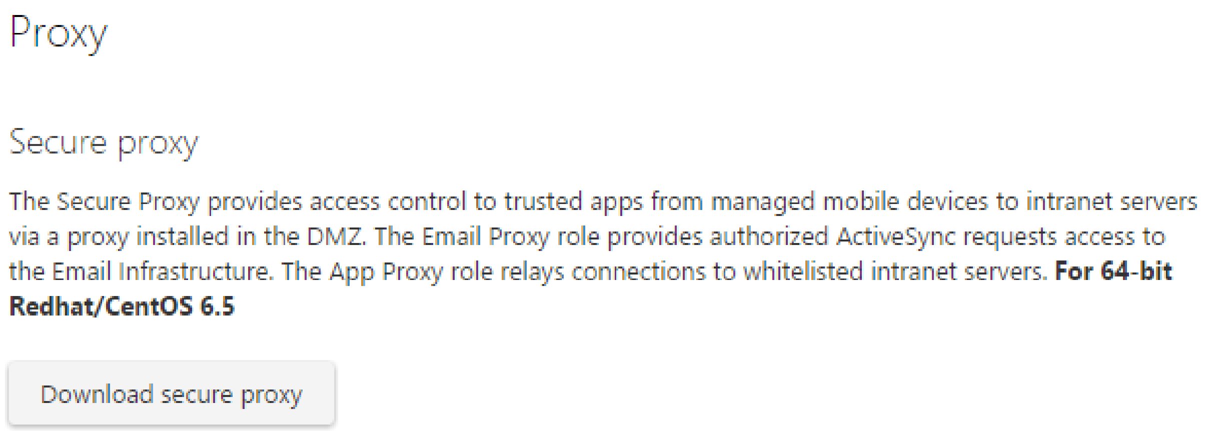
Email and App Proxy (HOWTO118669)

Note: If your environment is using in-house certificates on the Application or CAS front-end servers, their certificates must be trusted for Java to properly communicate with the resource. To add a certificate to the Java keystore see How to manually add a certificate to the Mobility Java keystore.

1. Deploy a cluster of VM's (Virtual Machines) matching the same number CAS/EAS server front-ends used by the organization.

Note: Follow HOWTO110252 to create these VM's. Each will require 8GB RAM and at least two dual core processors. Optionally configure two NICs per proxy, one for internal communication and the other for device communication. However, a single NIC can function to do both internal and external communication, with the proper routing.

2. From the **Mobility Admin Console > Downloads** click the **Download secure proxy** link:

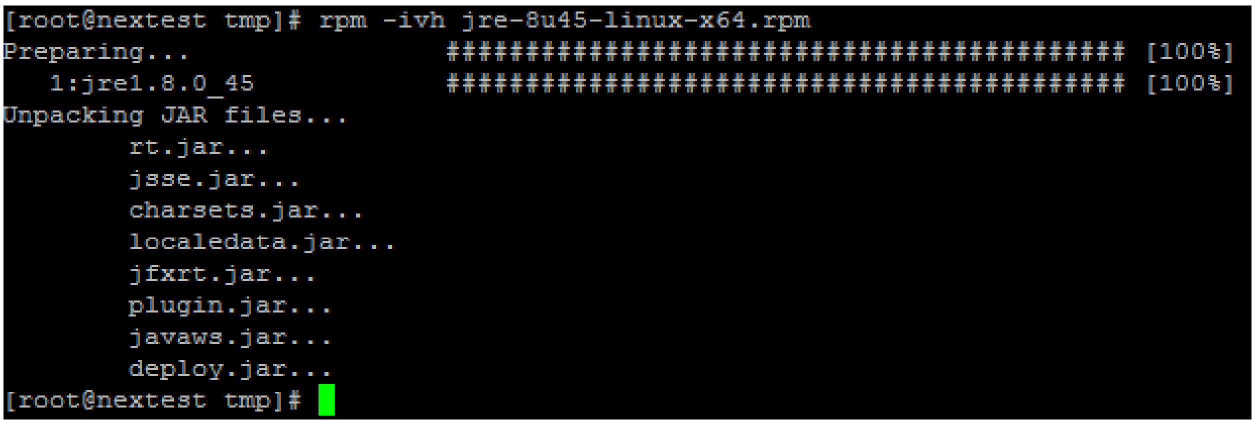


Proxy

Secure proxy

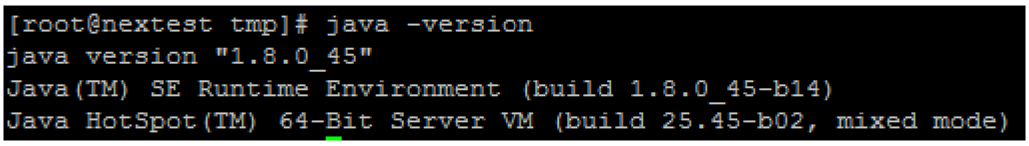
The Secure Proxy provides access control to trusted apps from managed mobile devices to intranet servers via a proxy installed in the DMZ. The Email Proxy role provides authorized ActiveSync requests access to the Email Infrastructure. The App Proxy role relays connections to whitelisted intranet servers. **For 64-bit Redhat/CentOS 6.5**

3. Follow HOWTO110248 to transfer the ISO file to each Secure Proxy front-end.
4. From the proxy's terminal, install libicu by entering the following as root:
   sudo yum -y install libicu perl-DBI
5. Download the JRE 1.7.51 RPM or later from the Oracle website and follow HOWTO110248 to transfer it to the proxy server.
6. Install the RPM, as root, using a command like:
   sudo rpm -ivh jre-8u45-linux-x64.rpm



```
[root@nextest tmp]# rpm -ivh jre-8u45-linux-x64.rpm
Preparing...                ########################################### [100%]
   1:jre1.8.0_45            ########################################### [100%]
Unpacking JAR files...
        rt.jar...
        jsse.jar...
        charsets.jar...
        localedata.jar...
        jfxrt.jar...
        plugin.jar...
        javaws.jar...
        deploy.jar...
[root@nextest tmp]#
```

7. Verify that java has successfully installed by entering the following:
   java -version

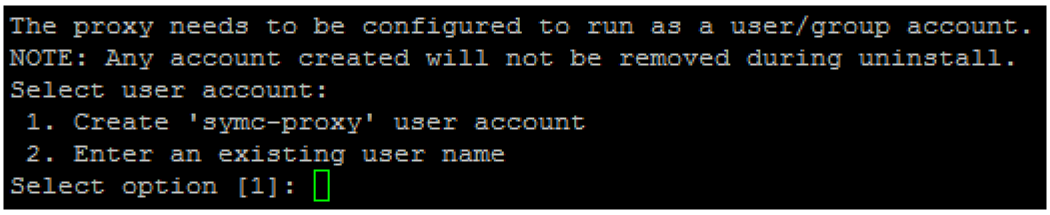


```
[root@nextest tmp]# java -version
java version "1.8.0_45"
Java(TM) SE Runtime Environment (build 1.8.0_45-b14)
Java HotSpot(TM) 64-Bit Server VM (build 25.45-b02, mixed mode)
```

8. Once libicu and Java Runtime Environment are installed create a mount point for the Secure Proxy ISO by entering, as root:
   mkdir /mnt/iso
9. Mount the Secure Proxy ISO using a command like:
   sudo mount -o loop /tmp/SecureProxy_x86_64_R5.3-17.iso /mnt/iso

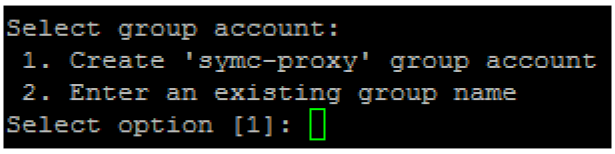
Note: The mount command syntax used above is: sudo mount -o loop <PathtoISO> <MountDirectory>

10. Change directories to **/mnt/iso** by entering:
    cd /mnt/iso
11. Execute the setup.sh script by entering the following, as root:
    sudo ./setup.sh --install
12. When prompted to create a user account hit **enter** to accept the default, as below:



```
The proxy needs to be configured to run as a user/group account.
NOTE: Any account created will not be removed during uninstall.
Select user account:
 1. Create 'symc-proxy' user account
 2. Enter an existing user name
Select option [1]:
```

13. Same for group-name, as above:



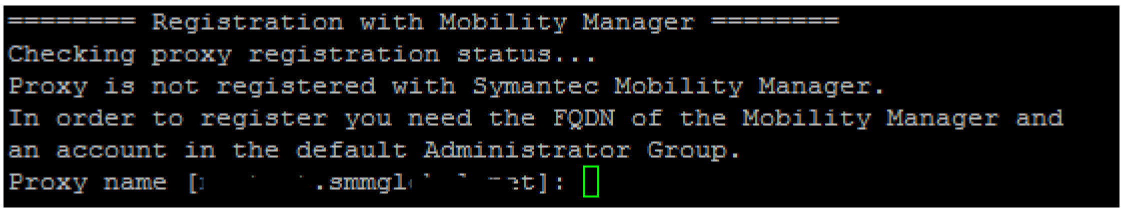
```
Select group account:
 1. Create 'symc-proxy' group account
 2. Enter an existing group name
Select option [1]:
```

Note: If an error occurs saying: **perl(DBI) is needed by squid-3.4.12-20151200914.x86_64** install perl-DBI using a command like: **sudo yum -y install perl-DBI**

14. Enter **y** to configure the proxy now.
15. Follow the prompts to configure the incoming and outgoing connections.

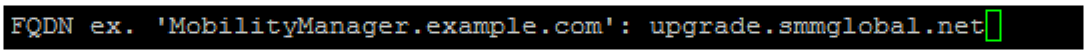
Tip: The incoming connection, from devices, should be 443 (default)

16. Optionally enter a unique name for your proxy server. This name is arbitrary but should be unique enough to identify this proxy within the Mobility Admin Console.



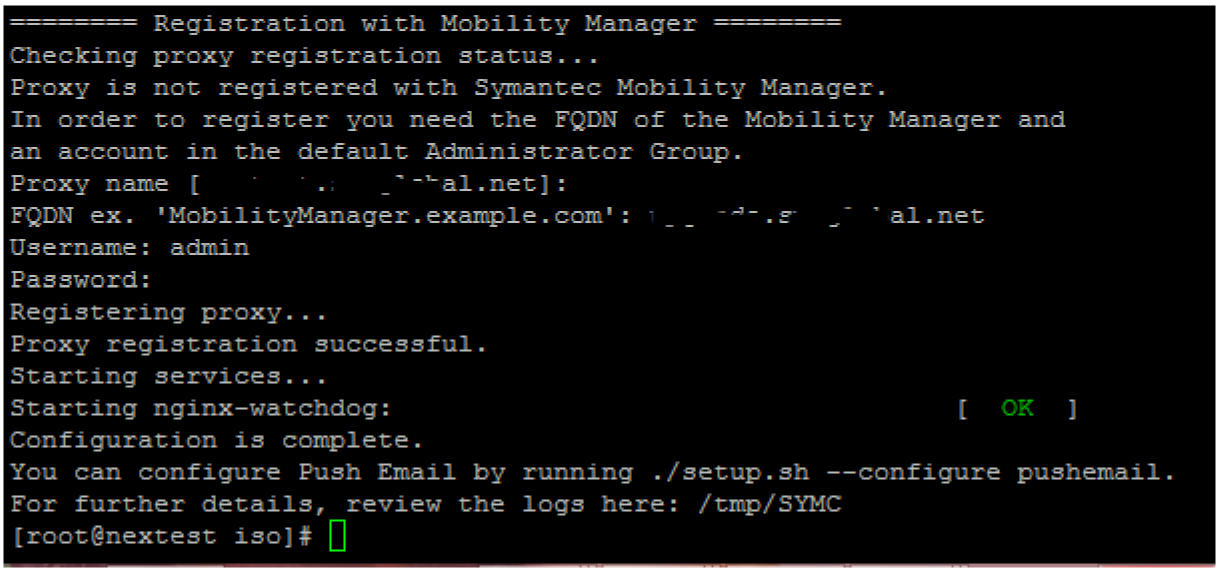
```
======== Registration with Mobility Manager ========
Checking proxy registration status...
Proxy is not registered with Symantec Mobility Manager.
In order to register you need the FQDN of the Mobility Manager and
an account in the default Administrator Group.
Proxy name [[redacted].smmgl[redacted]t]:
```

17. Register the proxy to a Mobility tenant by entering the FQDN of the Mobility server:



```
FQDN ex. 'MobilityManager.example.com': upgrade.smmglobal.net
```

18. Enter a local or LDAP/AD (if EIDP is used) administrative credential to register the proxy with Mobility:



```
======== Registration with Mobility Manager ========
Checking proxy registration status...
Proxy is not registered with Symantec Mobility Manager.
In order to register you need the FQDN of the Mobility Manager and
an account in the default Administrator Group.
Proxy name [[redacted]al.net]:
FQDN ex. 'MobilityManager.example.com': [redacted]al.net
Username: admin
Password:
Registering proxy...
Proxy registration successful.
Starting services...
Starting nginx-watchdog:                                    [  OK  ]
Configuration is complete.
You can configure Push Email by running ./setup.sh --configure pushemail.
For further details, review the logs here: /tmp/SYMC
[root@nextest iso]# 
```

Email Proxy Cluster Configuration

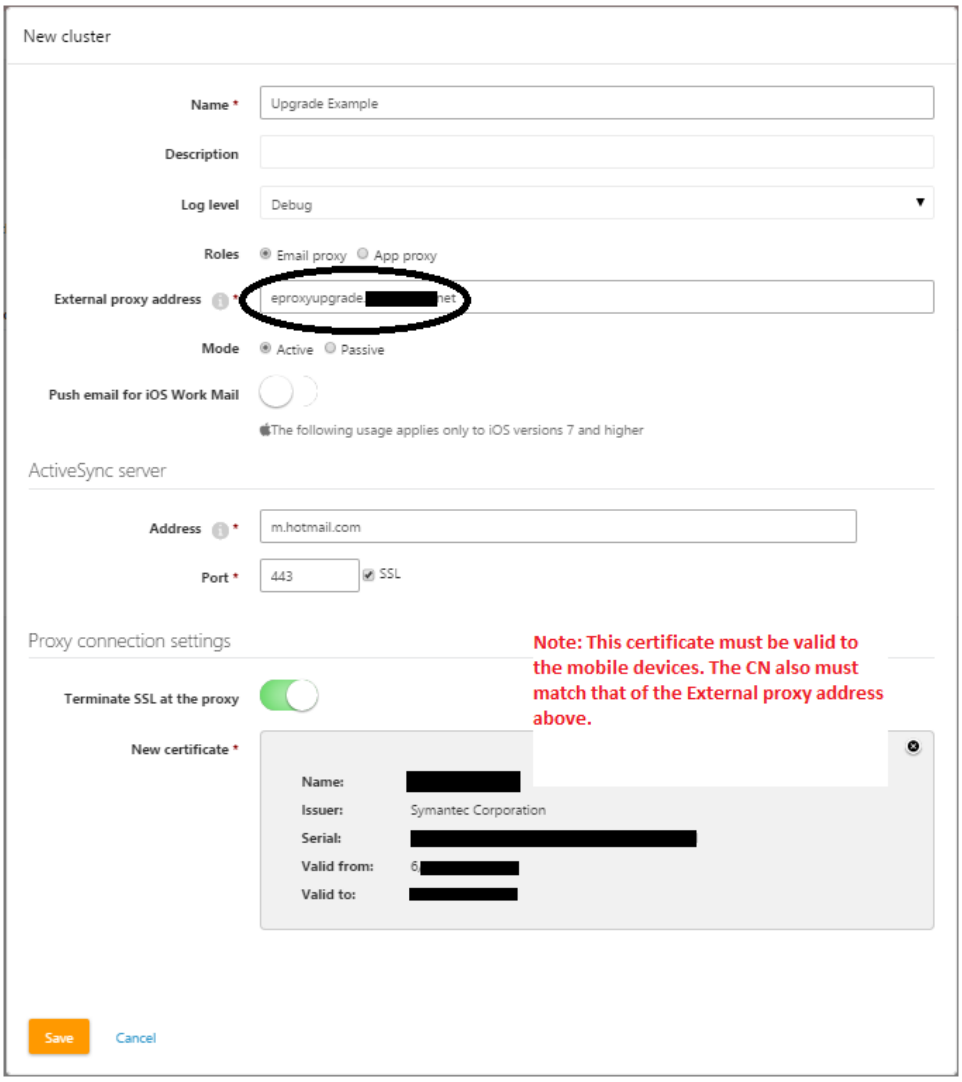
1. From the **Mobility Admin Console > Settings > Proxies** click + Add Cluster (**+Add Cluster**).
2. Fill in the name, description and set the logging level to Debug.
3. Ensure that **Email Proxy** is selected as the intended role.
4. Set an **external proxy address**.

Note: This address may be the address of the virtual application on the load balancer, if one is being used for multiple email proxies. Otherwise enter the published FQDN of the Email Proxy FE.

5. Set the **Mode** to **Passive** for testing purposes.
6. Keep push, deactivated; see documentation for detailed instructions for enabling Push for iOS 7 and later devices. Basic email proxy functionality will not be hindered by having this deactivated, for now.
7. Enter the routable address from the Email proxy to the EAS server or CAS front-end.

Tip: If the environment is already load-balancing between CAS FE's consider the number of hops between the device and the Email Proxy(s). You may want to consider pointing the proxy directly to the internal CAS FE rather than the load-balanced address to reduce latency, especially if an LB method is already being used between Secure Email Proxies.

8. Yes, terminate SSL at the proxy, unless it is going to be terminated at the load-balancer. In either scenario a valid SSL certificate is required for devices to trust the connection. Obtain a PKCS7 certificate with a matching CN (Common Name) and upload it to the cluster configuration:



New cluster

Name * Upgrade Example

Description

Log level Debug ▾

Roles ● Email proxy ○ App proxy

External proxy address * eproxyupgrade.[redacted]net

Mode ● Active ○ Passive

Push email for iOS Work Mail ○

The following usage applies only to iOS versions 7 and higher

ActiveSync server

Address * m.hotmail.com

Port * 443 ☑ SSL

Proxy connection settings

Terminate SSL at the proxy ●

New certificate *

Name: [redacted]

Issuer: Symantec Corporation

Serial: [redacted]

Valid from: 6[redacted]

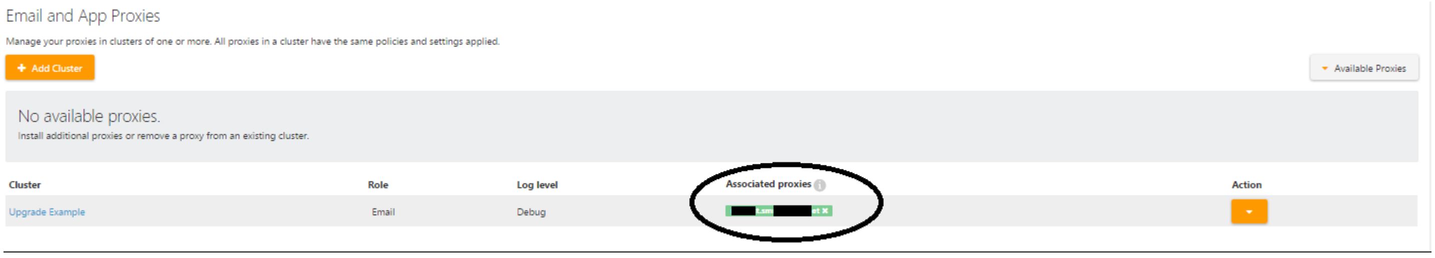
Valid to: [redacted]

Save Cancel

Note: This certificate must be valid to the mobile devices. The CN also must match that of the External proxy address above.

9. Click **Save.**

10. Click Available Proxies (**Available Proxies**) to expand and drag the newly registered proxy into the **Associated proxies** column:



Email and App Proxies

Manage your proxies in clusters of one or more. All proxies in a cluster have the same policies and settings applied.

+ Add Cluster

Available Proxies

No available proxies.

Install additional proxies or remove a proxy from an existing cluster.

Cluster	Role	Log level	Associated proxies	Action
Upgrade Example	Email	Debug	[redacted]	▾

11. Allow up to 5 minutes for the Proxy to receive its new configuration.

Tip: The proxy logs are located in **/usr/local/nginx/logs/** The controller.log file tends to contain the most useful information, at this stage.

12. Test the email proxy from an iOS device by manually configuring an exchange email setting.

Tip: Also confirm that the proxy is accessible from the Internet by browsing to the cluster FQDN in a browser. A 403 error will confirm connectivity. If no connectivity is established, consider firewall settings, for ex. Turn off iptables with a command like: **service iptables stop**. To insert an iptables-inbound-exception, the following commands should suffice:

```
/sbin/iptables --insert INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
/etc/init.d/iptables save
```

13. Now that the Email Proxy cluster contains an active proxy, the administrator may now set a device or app config to use this cluster's FQDN as the EAS server.

Note: Flip the cluster configuration from **Passive** to **Active** mode. This will require devices to be compliant and have a policy allowing email access via the proxy. Once preliminary testing is complete lower the cluster's logging level from **Debug**.

App Proxy Cluster Configuration

This subject is coming soon! The steps are nearly identical to Email Proxy.

How to replace an expiring Secure Proxy certificate (HOWTO118668)

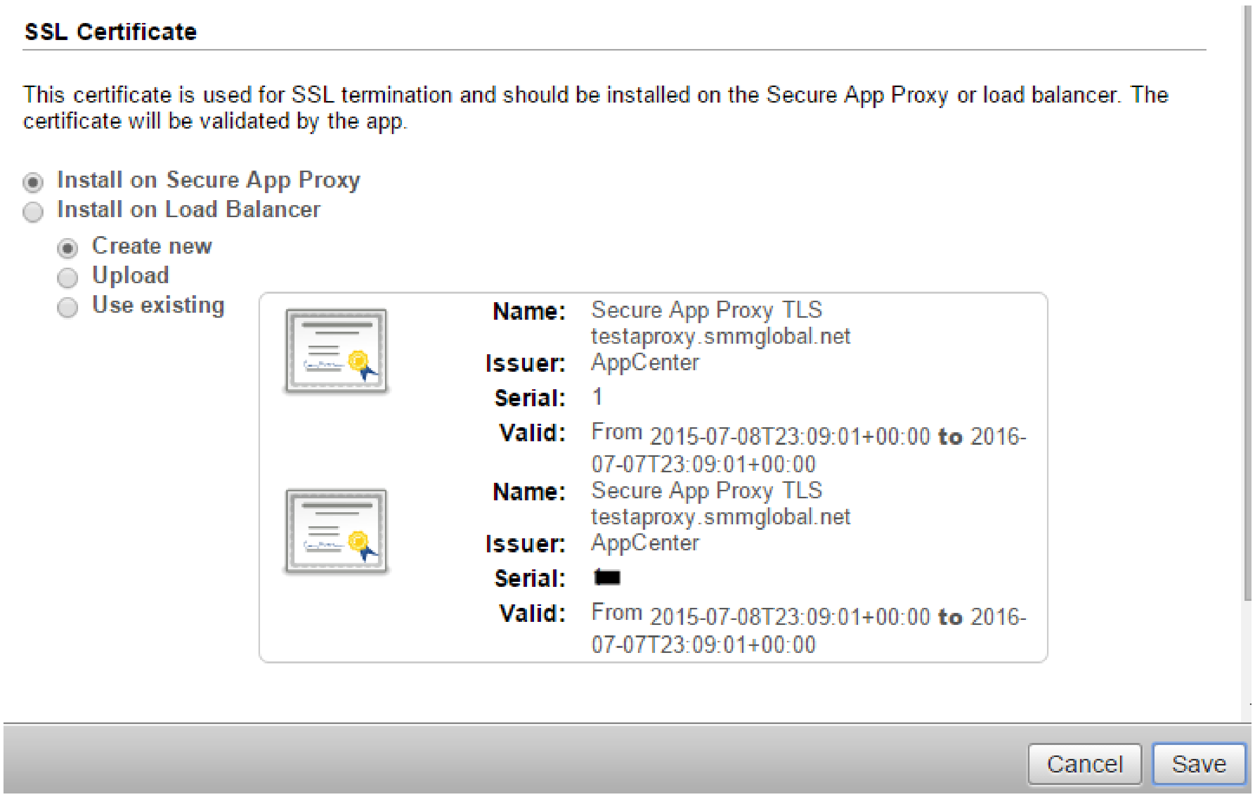
1. From the Mobility Admin Console > Settings > Proxies; find the cluster with the expiring SSL certificate, under **Action** click **Edit Cluster**.
2. Scroll down to the end of the page and remove the expiring or expired SSL certificate by clicking the **X** symbol.
3. **Browse** to the new PKSC7 certificate file and click **Open**.
4. Enter the password for the file and click **Upload**.
5. Finally click **Save.** The new SSL certificate will be installed onto every proxy within the cluster, momentarily.

Pre 5.3 Secure App Proxy and pre 5.0 Email Proxy certificate replacement

Note: This article applies to App Proxies used by Symantec Mobility 4.4 – 5.2.2

1. From the **Mobility Admin Console > Settings > App Proxy** click **Edit**.
2. Scroll down to the bottom of the page and select **Create new** and **Save**.

Note: If replacing a pre 5.0 email proxy certificate, select **Upload** and browse to the new PKCS7 certificate.



SSL Certificate

This certificate is used for SSL termination and should be installed on the Secure App Proxy or load balancer. The certificate will be validated by the app.

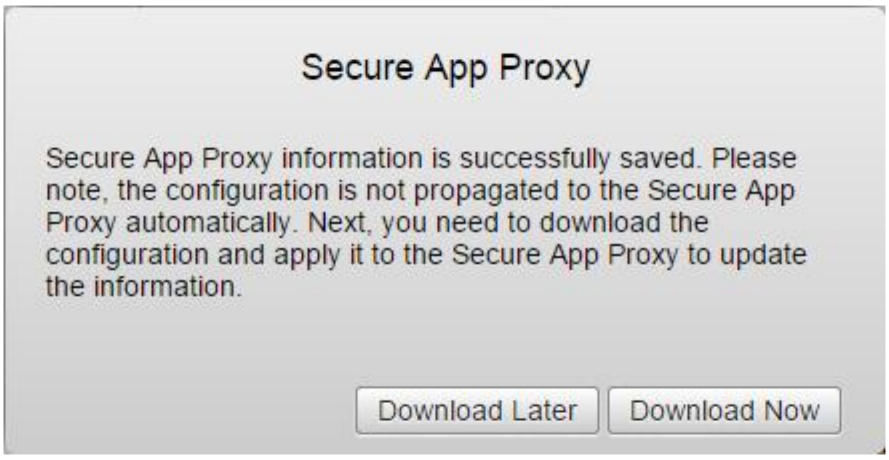
● Install on Secure App Proxy
○ Install on Load Balancer

● Create new
○ Upload
○ Use existing

Name: Secure App Proxy TLS testaproxy.smmglobal.net
Issuer: AppCenter
Serial: 1
Valid: From 2015-07-08T23:09:01+00:00 **to** 2016-07-07T23:09:01+00:00

Name: Secure App Proxy TLS testaproxy.smmglobal.net
Issuer: AppCenter
Serial: [redacted]
Valid: From 2015-07-08T23:09:01+00:00 **to** 2016-07-07T23:09:01+00:00

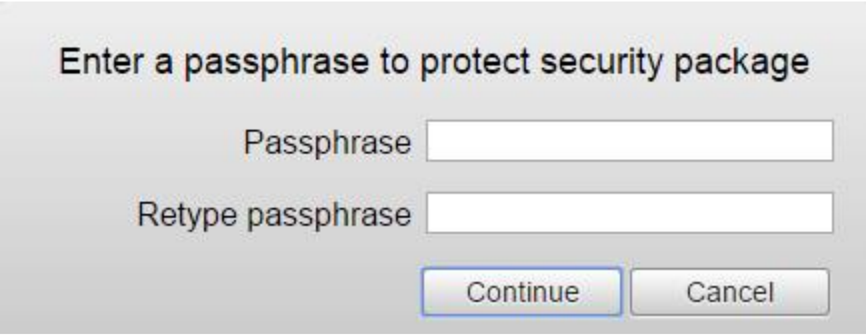
3. When prompted to download the configuration click **Download Now:**



Secure App Proxy

Secure App Proxy information is successfully saved. Please note, the configuration is not propagated to the Secure App Proxy automatically. Next, you need to download the configuration and apply it to the Secure App Proxy to update the information.

4. Enter a secure passphrase to encrypt this configuration file:



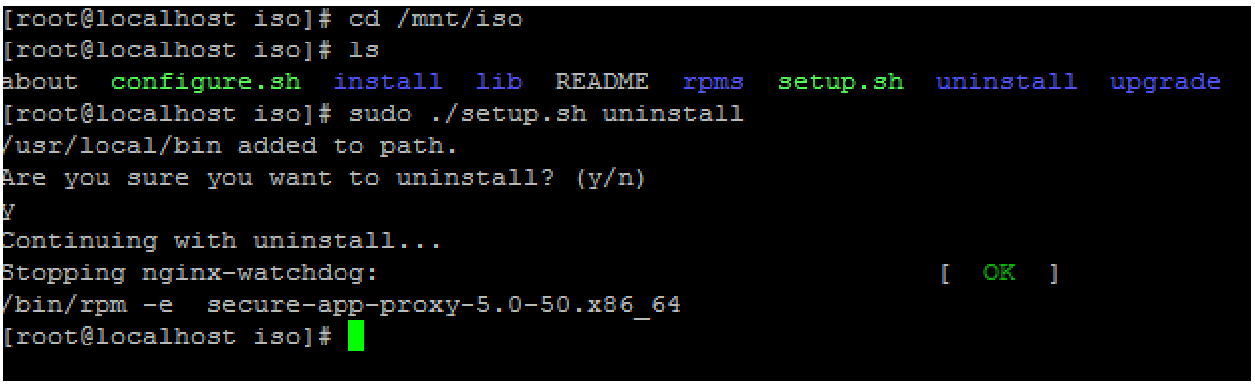
Enter a passphrase to protect security package

Passphrase

Retype passphrase

5. Follow HOWTO110248 to transfer the configuration file to each Secure App Proxy front-end.
6. Uninstall the Secure App Proxy by first mounting the App Proxy ISO, as root:
   #mount -o loop proxyisoname.iso /mnt/iso
   #cd /mnt/iso
   #./setup.sh uninstall

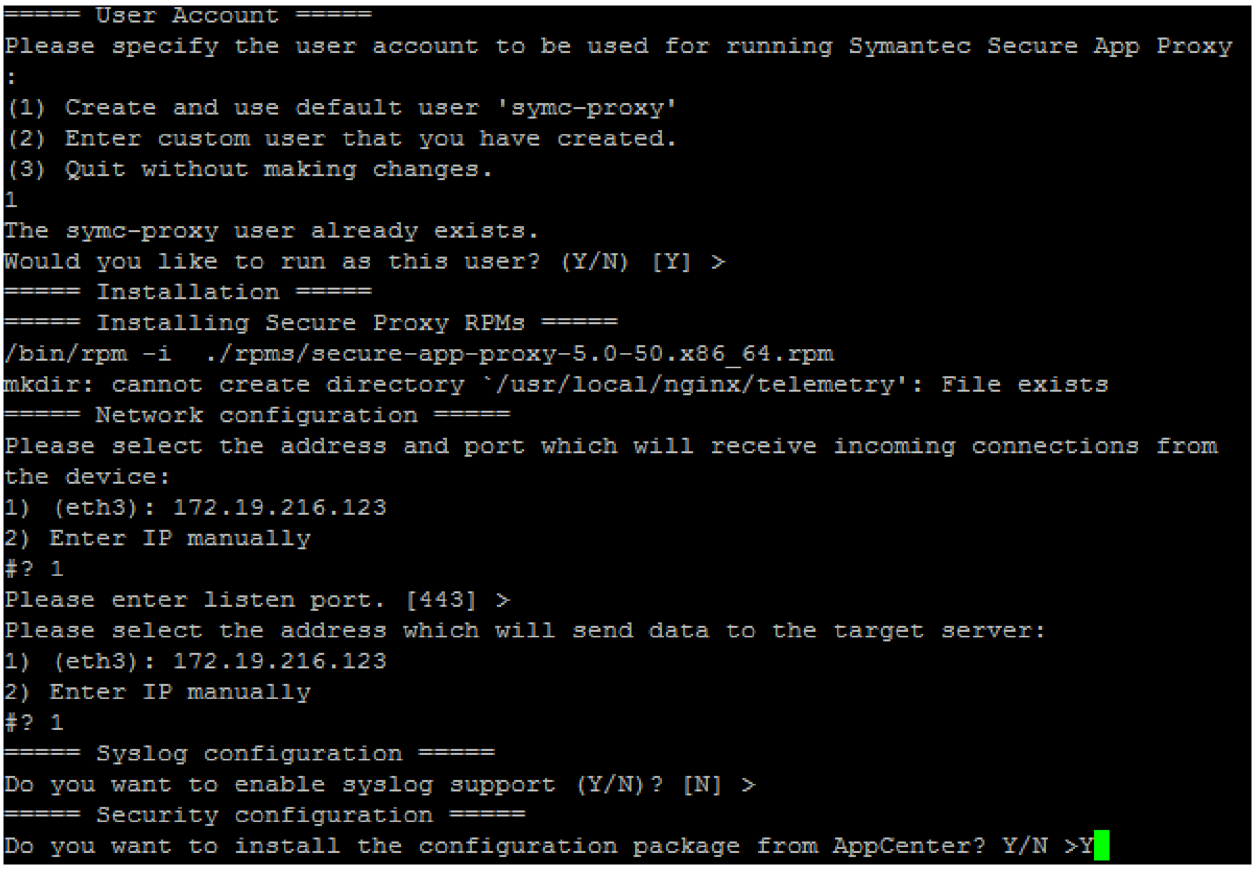
Note: If prompted to preserve logs hit **Y**. If using Email Proxy pre 5.0; use **./setup.sh --uninstall** instead of **./setup.sh uninstall**.



```
[root@localhost iso]# cd /mnt/iso
[root@localhost iso]# ls
about  configure.sh  install  lib  README  rpms  setup.sh  uninstall  upgrade
[root@localhost iso]# sudo ./setup.sh uninstall
/usr/local/bin added to path.
Are you sure you want to uninstall? (y/n)
y
Continuing with uninstall...
Stopping nginx-watchdog:                                   [  OK  ]
/bin/rpm -e  secure-app-proxy-5.0-50.x86_64
[root@localhost iso]#
```

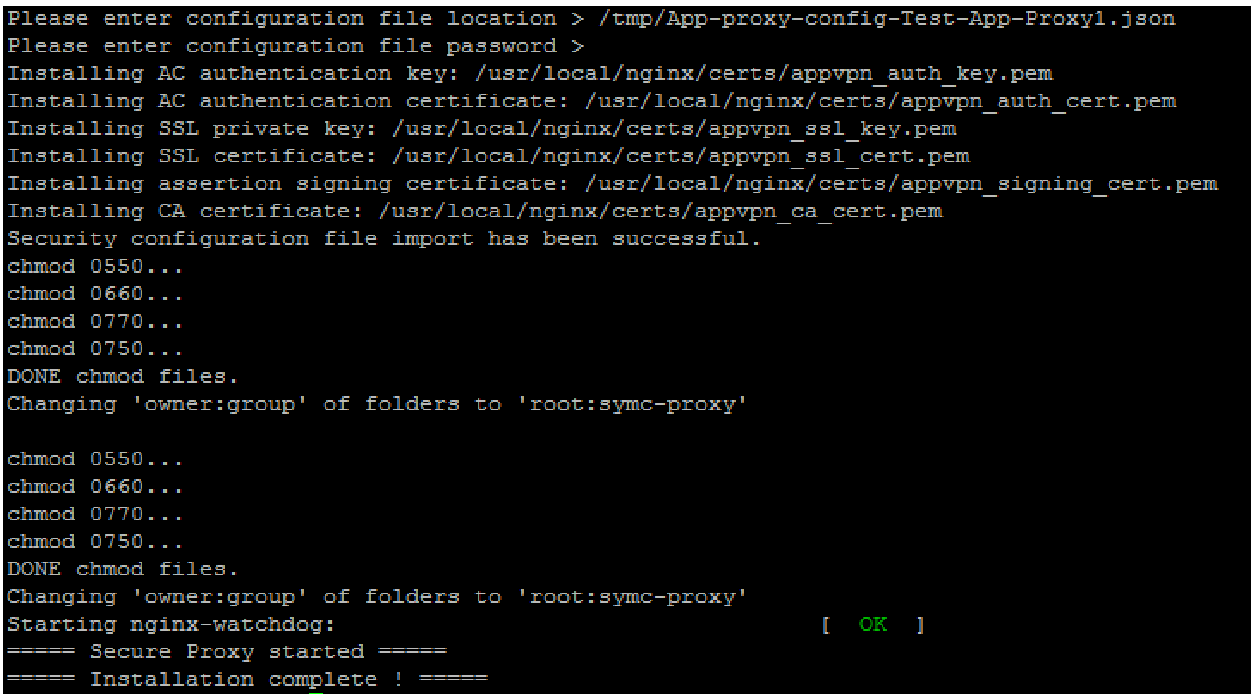
7. Once the uninstall is completed run the install by entering, as root:
   #./setup.sh install

8. Follow the prompts to re-install Secure Proxy, when prompted to install the configuration file now press **Y:**



```
===== User Account =====
Please specify the user account to be used for running Symantec Secure App Proxy
:
(1) Create and use default user 'symc-proxy'
(2) Enter custom user that you have created.
(3) Quit without making changes.
1
The symc-proxy user already exists.
Would you like to run as this user? (Y/N) [Y] >
===== Installation =====
===== Installing Secure Proxy RPMs =====
/bin/rpm -i  ./rpms/secure-app-proxy-5.0-50.x86_64.rpm
mkdir: cannot create directory `/usr/local/nginx/telemetry': File exists
===== Network configuration =====
Please select the address and port which will receive incoming connections from
the device:
1)  (eth3): 172.19.216.123
2)  Enter IP manually
#? 1
Please enter listen port. [443] >
Please select the address which will send data to the target server:
1)  (eth3): 172.19.216.123
2)  Enter IP manually
#? 1
===== Syslog configuration =====
Do you want to enable syslog support (Y/N)? [N] >
===== Security configuration =====
Do you want to install the configuration package from AppCenter? Y/N >Y
```

9. Enter the path for the configuration JSON file and hit **Enter**.
10. Enter the password created in step 4:



```
Please enter configuration file location > /tmp/App-proxy-config-Test-App-Proxy1.json
Please enter configuration file password >
Installing AC authentication key: /usr/local/nginx/certs/appvpn_auth_key.pem
Installing AC authentication certificate: /usr/local/nginx/certs/appvpn_auth_cert.pem
Installing SSL private key: /usr/local/nginx/certs/appvpn_ssl_key.pem
Installing SSL certificate: /usr/local/nginx/certs/appvpn_ssl_cert.pem
Installing assertion signing certificate: /usr/local/nginx/certs/appvpn_signing_cert.pem
Installing CA certificate: /usr/local/nginx/certs/appvpn_ca_cert.pem
Security configuration file import has been successful.
chmod 0550...
chmod 0660...
chmod 0770...
chmod 0750...
DONE chmod files.
Changing 'owner:group' of folders to 'root:symc-proxy'

chmod 0550...
chmod 0660...
chmod 0770...
chmod 0750...
DONE chmod files.
Changing 'owner:group' of folders to 'root:symc-proxy'
Starting nginx-watchdog:                                   [  OK  ]
===== Secure Proxy started =====
===== Installation complete ! =====
```

11. The installation should now be complete and the new SSL certificate(s) will be loaded into the **/usr/local/nginx/certs/**

Adding a license to Mobility

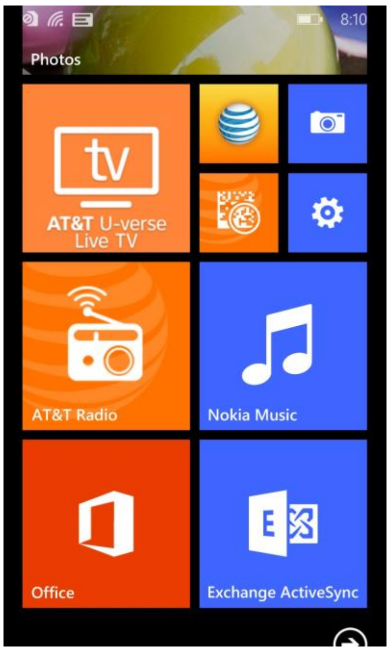
1. When logged into Mobility Suite as an administrator, click on the user name in the upper right of the window and **Licenses.**
2. To add an additional license click **Add License** and paste the license key into the form and **Add.**

Tip: If there is a problem loading the license, refer to the **/var/log/nukona/appstore.log** on the tenant. This most likely is due to a problem with outbound communication from the FE to the Symantec licensing server. Verify outbound communication and that the license serial number is valid.

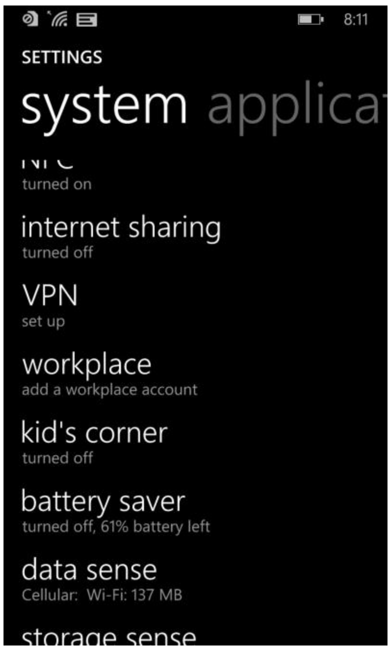
Windows 8.1: Enrollment (HOWTO110270)

Note: For Symantec Mobility Suite administrators: A device policy must be active with mobile device management (MDM) enabled for Windows Phone devices. MDM is supported on Windows Phones and allows a user to successfully enroll a Windows 8.1 Phone with Symantec Mobility Suite. Each device policy also includes a Targeted devices definition which defines the group that is associated with that device policy. To create a new device policy or access an existing device policy, click Policies and Rules and click the New/Edit icon located at the top right. Also, the user must be a member of a group that is defined in the target definition of the device policy. If there is no policy with the above parameters, Windows Phone enrollment will fail.

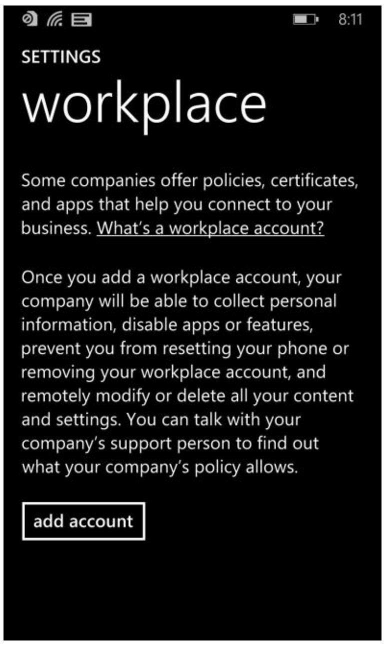
1. Go to **Settings :**



2. Under System tap **workplace:**



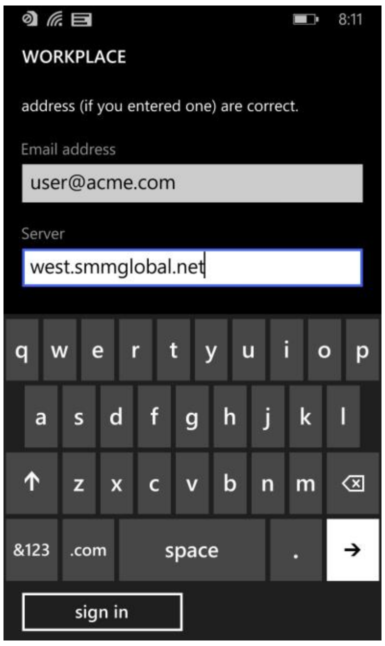
3. Tap **add account**:



Some companies offer policies, certificates, and apps that help you connect to your business. What's a workplace account?

Once you add a workplace account, your company will be able to collect personal information, disable apps or features, prevent you from resetting your phone or removing your workplace account, and remotely modify or delete all your content and settings. You can talk with your company's support person to find out what your company's policy allows.

4. Enter an email address. If no DNS record has been created for email resolution to the Mobility front-end (FE), an option to enter the server address will appear. Enter the fully qualified domain name (FQDN) of the Mobility FE and tap **sign in**:

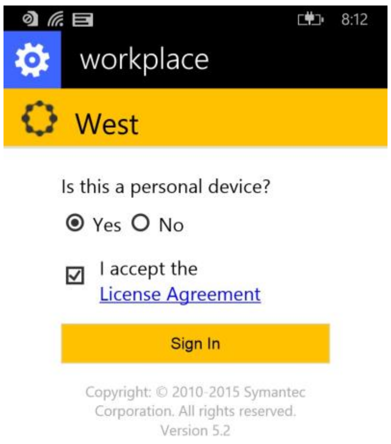


address (if you entered one) are correct.

Email address: user@acme.com

Server: west.smmglobal.net

5. Log into the Mobility FE using your company provided account.
6. Select device type (if shown), accept the terms and tap **Sign In**:



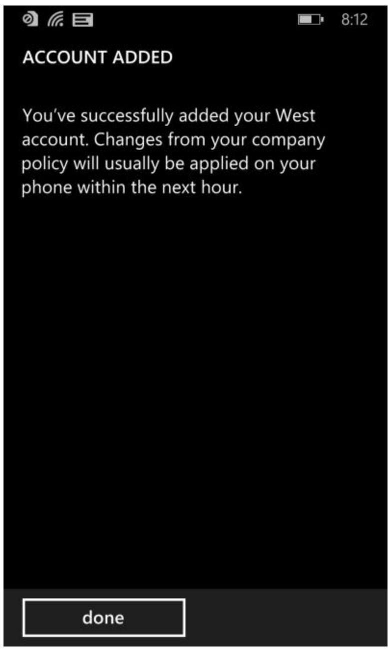
Is this a personal device?

● Yes ○ No

☑ I accept the License Agreement

Copyright: © 2010-2015 Symantec Corporation. All rights reserved.
Version 5.2

7. You are now enrolled into your company's workspace:



ACCOUNT ADDED

You've successfully added your West account. Changes from your company policy will usually be applied on your phone within the next hour.

Android: Enrollment (HOWTO94453)

Note: For Mobility administrators: A Google Cloud Messaging (API) key and project ID must be uploaded to the Mobility administrator console to send mobile device management (MDM) commands to Android devices. See Google Cloud Messaging for more details.

Follow HOWTO94453 to enroll your Android device.

iOS: Enrollment (HOWTO94449)

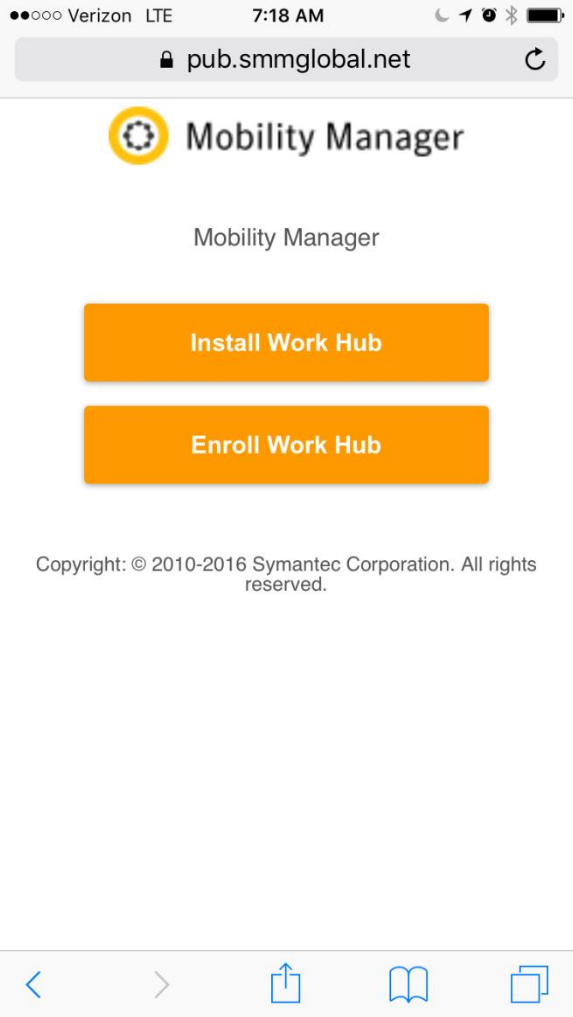
1. Open **Safari** and navigate to the fully qualified domain name (FQDN) of your organization's Mobility server.
2. Enter your company provided credentials (if prompted).
3. Tap **Install Work Hub** and when prompted tap **Install**.
4. After the Work Hub agent is installed, open the application. When prompted whether to trust the app developer, tap **trust**.
5. Log in using your provided credentials and follow the instructions provided in the app.

For more detailed instructions see HOWTO94449.

Public Work Hub Enrollment

Note: To Mobility administrators, the public work hub may be enabled from the **Admin console > Settings > Device management > iOS Client.** Switching between

1. Open Safari and navigate to the FQDN of the Mobility server, for example: https://exampletenant.appcenterhq.com
2. Click **Install Work Hub:**

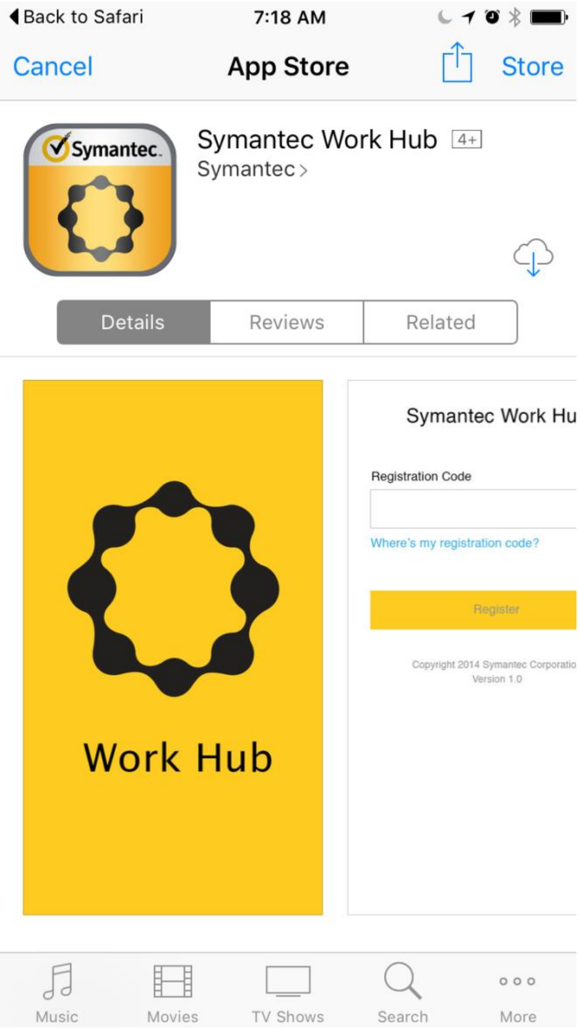


Mobility Manager

Mobility Manager

Copyright: © 2010-2016 Symantec Corporation. All rights reserved.

3. Download and install the **Symantec Work Hub** from the iTunes store.



Symantec Work Hub 4+
Symantec >

Symantec Work Hu

Registration Code

Where's my registration code?

Copyright 2014 Symantec Corporatio
Version 1.0

Select one of the two enrollment options below to complete the process…

Option 1: Open the App and enter the same URL from step 1 into the agent and click Enroll.

a. When prompted tap **Yes.**

b. Enter your enrollment credentials and follow the instructions provided in the app.

Option 2: After the installation is complete return to Safari and click Enroll Work Hub.

a. If prompted to open **Symantec Work Hub** tap **Open**.
b. When prompted tap **Yes.**
c. Enter your enrollment credentials and follow the instructions provided in the app.

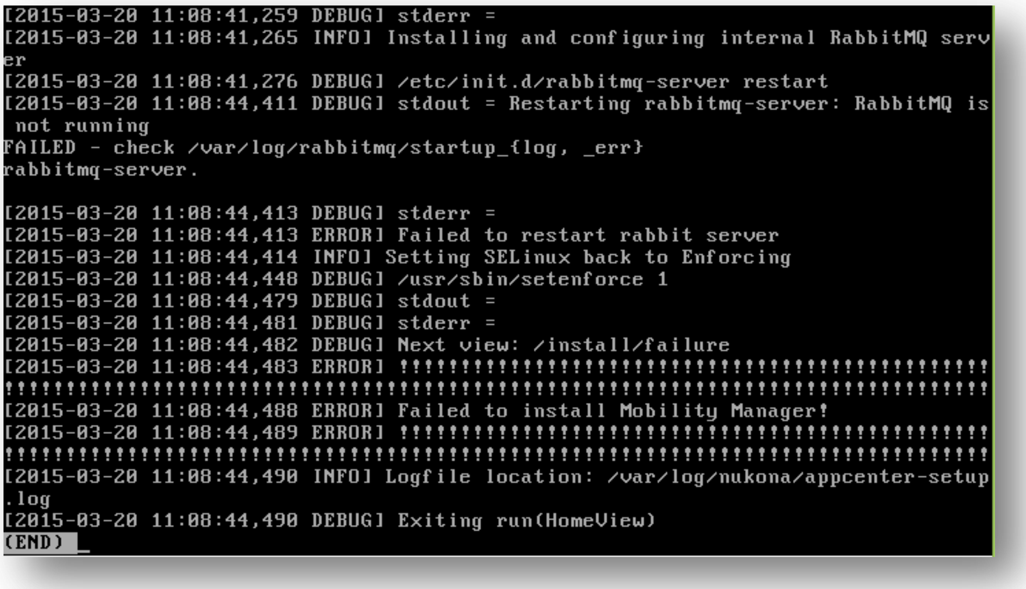
Optimize Symantec Mobility Suite FE (HOWTO109637)

To configure **monit** to run with the system and monitor Mobility Suite services see HOWTO109637.

Troubleshooting the pre configurator Symantec Mobility Suite installation

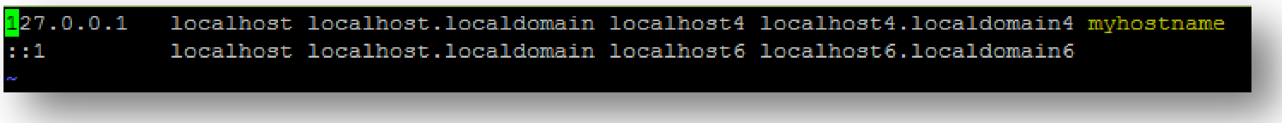
There are many things which can cause the pre configurator stage to fail. Below are some of the more common reasons.

The RabbitMQ service fails to start / restart (HOWTO109655 HOWTO110300):



```
[2015-03-20 11:08:41,259 DEBUG] stderr =
[2015-03-20 11:08:41,265 INFO] Installing and configuring internal RabbitMQ serv
er
[2015-03-20 11:08:41,276 DEBUG] /etc/init.d/rabbitmq-server restart
[2015-03-20 11:08:44,411 DEBUG] stdout = Restarting rabbitmq-server: RabbitMQ is
 not running
FAILED - check /var/log/rabbitmq/startup_{log, _err}
rabbitmq-server.

[2015-03-20 11:08:44,413 DEBUG] stderr =
[2015-03-20 11:08:44,413 ERROR] Failed to restart rabbit server
[2015-03-20 11:08:44,414 INFO] Setting SELinux back to Enforcing
[2015-03-20 11:08:44,448 DEBUG] /usr/sbin/setenforce 1
[2015-03-20 11:08:44,479 DEBUG] stdout =
[2015-03-20 11:08:44,481 DEBUG] stderr =
[2015-03-20 11:08:44,482 DEBUG] Next view: /install/failure
[2015-03-20 11:08:44,483 ERROR] !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[2015-03-20 11:08:44,488 ERROR] Failed to install Mobility Manager!
[2015-03-20 11:08:44,489 ERROR] !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[2015-03-20 11:08:44,490 INFO] Logfile location: /var/log/nukona/appcenter-setup
.log
[2015-03-20 11:08:44,490 DEBUG] Exiting run(HomeView)
(END)
```

1. Go to /var/log/rabbitmq/startup_log:
   less /var/log/rabbitmq/startus_log
2. Type **q** to exit **less**.
3. Verify that the server name resolves to 127.0.0.1 by entering the following where <hostname> is replaced with that of the machine:
   ping <hostname>
4. Edit **/etc/hosts** adding the hostname of the server to the IPV4 loop back (127.0.0.1):



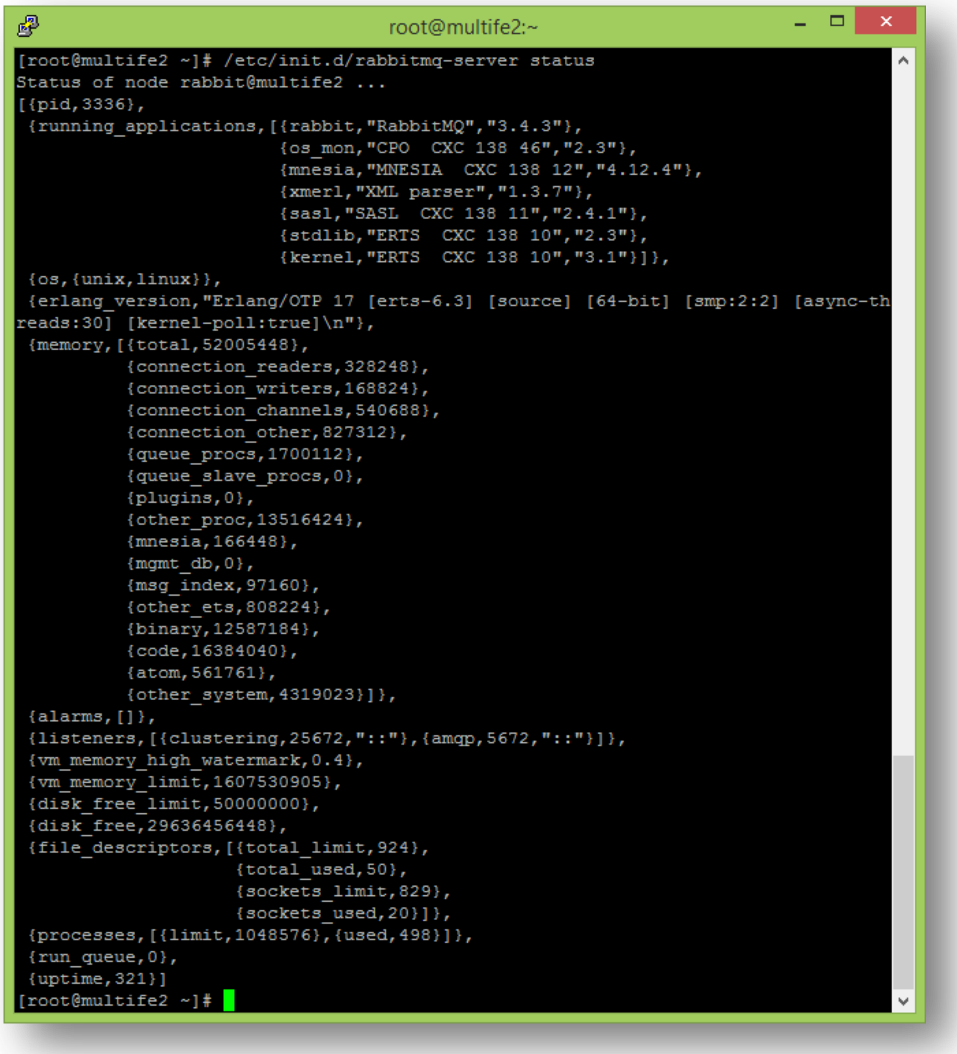
```
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4 myhostname
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
~
```

Tip: Quick guide to **vi**:
i → Insert
Esc key → End insert mode and returns to command mode which allows the below two commands:
:q! → Colon followed by **q!** quits without making any changes.
:wq → Colon followed by **wq** writes and quits, saving changes.

5. Also verify that /var/log/rabbitmq and /var/lib/rabbitmq is owned by the rabbitmq user by entering the below commands, as root:
   /etc/init.d/rabbitmq-server stop
   chown -R rabbitmq /var/log/rabbitmq
   chmod -R 755 /var/log/

6. Restart the rabbitMQ services with by entering the following command:
   /etc/init.d/rabbitmq-server restart
7. If the service still does not start, grep for any orphaned Rabbit services by entering the following:
   ps -Al | grep rabbit
8. Take note of any processes and enter the following, filling in the below syntax with the PID from the above command:
   kill <PID>
9. Restart rabbitmq-server:
   /etc/init.d/rabbitmq-server restart

10. Set the RabbitMQ service to start with the server:
    chkconfig --level 2345 rabbitmq-server on
11. If there is still an error, reboot the server:
    sudo reboot
12. During startup, verify that all the Mobility (appcenter) services have started by pressing the **F2** key. Once log back into the terminal, as root and type:
    /etc/init.d/rabbitmq-server status
13. If there is no status output then start the service with:
    /etc/init.d/rabbitmq-server restart
14. Re-check the status with:
    /etc/init.d/rabbitmq-server status

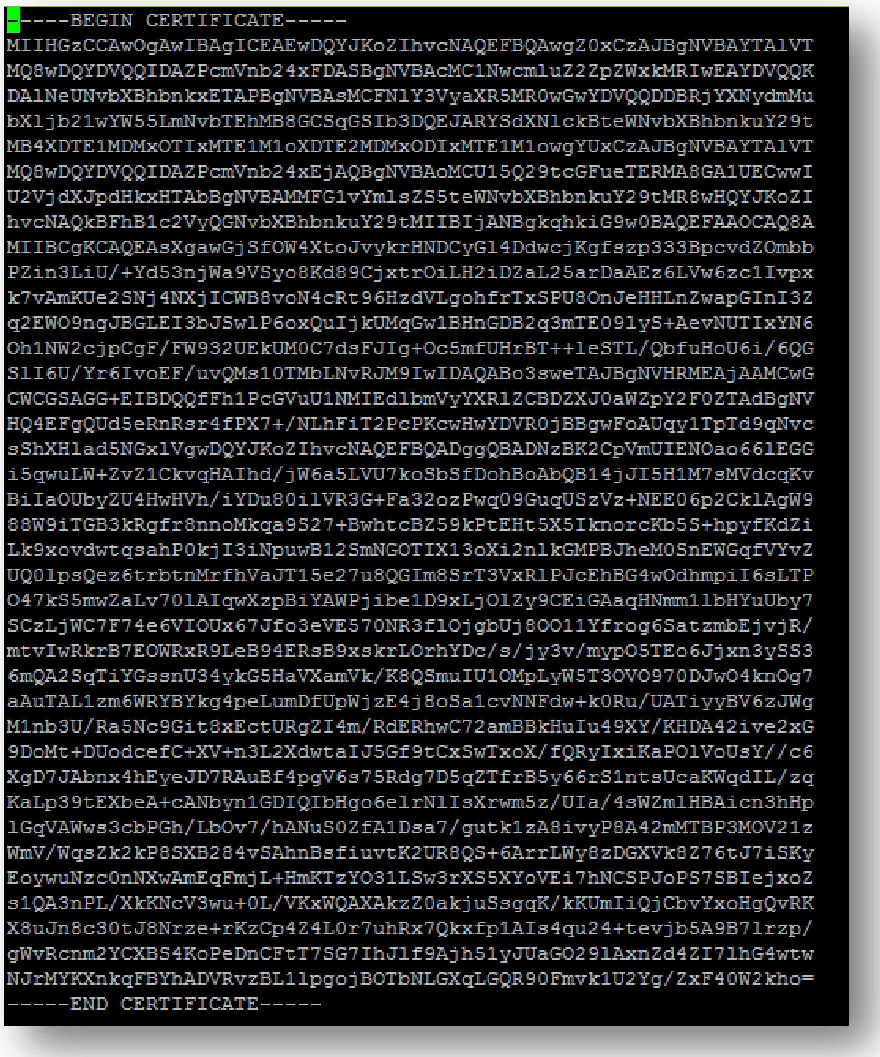


```
[root@multife2 ~]# /etc/init.d/rabbitmq-server status
Status of node rabbit@multife2 ...
[{pid,3336},
 {running_applications,[{rabbit,"RabbitMQ","3.4.3"},
                        {os_mon,"CPO  CXC 138 46","2.3"},
                        {mnesia,"MNESIA  CXC 138 12","4.12.4"},
                        {xmerl,"XML parser","1.3.7"},
                        {sasl,"SASL  CXC 138 11","2.4.1"},
                        {stdlib,"ERTS  CXC 138 10","2.3"},
                        {kernel,"ERTS  CXC 138 10","3.1"}]},
 {os,{unix,linux}},
 {erlang_version,"Erlang/OTP 17 [erts-6.3] [source] [64-bit] [smp:2:2] [async-th
reads:30] [kernel-poll:true]\n"},
 {memory,[{total,52005448},
          {connection_readers,328248},
          {connection_writers,168824},
          {connection_channels,540688},
          {connection_other,827312},
          {queue_procs,1700112},
          {queue_slave_procs,0},
          {plugins,0},
          {other_proc,13516424},
          {mnesia,166448},
          {mgmt_db,0},
          {msg_index,97160},
          {other_ets,808224},
          {binary,12587184},
          {code,16384040},
          {atom,561761},
          {other_system,4319023}]},
 {alarms,[]},
 {listeners,[{clustering,25672,"::"},{amqp,5672,"::"}]},
 {vm_memory_high_watermark,0.4},
 {vm_memory_limit,1607530905},
 {disk_free_limit,50000000},
 {disk_free,29636456448},
 {file_descriptors,[{total_limit,924},
                    {total_used,50},
                    {sockets_limit,829},
                    {sockets_used,20}]},
 {processes,[{limit,1048576},{used,498}]},
 {run_queue,0},
 {uptime,321}]
[root@multife2 ~]#
```

Note: The above is an example of a running RabbitMQ server from the **/etc/init.d/rabbitmq-server status** command.

How to remove extended properties from a PEM SSL certificate (HOWTO110259)

1. Open the certificate in a text editor and remove everything before and after the -----**BEGIN CERTIFICATE-----** and ------**END CERTIFICATE-----** lines.



```
-----BEGIN CERTIFICATE-----
MIIHGzCCAwOgAwIBAgICEAEwDQYJKoZIhvcNAQEFBQAwgZ0xCzAJBgNVBAYTAlVT
MQ8wDQYDVQQIDAZPcmVnb24xFDASBgNVBAcMC1NwcmluZ2ZpZWxkMRIwEAYDVQQK
DAlNeUNvbXBhbnkxETAPBgNVBAsMCFN1Y3VyaXR5MR0wGwYDVQQDDBRjYXNydmMu
bXljb21wYW55LmNvbTEhMB8GCSqGSIb3DQEJARYSdXN1ckBteWNvbXBhbnkuY29t
MB4XDTE1MDMxOTIxMTE1M1oXDTE2MDMxODIxMTE1M1owgYUxCzAJBgNVBAYTAlVT
MQ8wDQYDVQQIDAZPcmVnb24xEjAQBgNVBAoMCU15Q29tcGFueTERMA8GA1UECwwI
U2VjdXJpdHkxHTAbBgNVBAMMFG1vYmlsZS5teWNvbXBhbnkuY29tMR8wHQYJKoZI
hvcNAQkBFhB1c2VyQGNvbXBhbnkuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAsXgawGjSfOW4XtoJvykrHNDCyGl4DdwcjKgfszp333BpcvdZOmbb
PZin3LiU/+Yd53njWa9VSyo8Kd89CjxtrOiLH2iDZaL25arDaAEz6LVw6zc1Ivpx
k7vAmKUe2SNj4NXjICWB8voN4cRt96HzdVLgohfrTxSPU8OnJeHHLnZwapGInI3Z
q2EWO9ngJBGLEI3bJSwlP6oxQuIjkUMqGw1BHnGDB2q3mTE09lyS+AevNUTIxYN6
Oh1NW2cjpCgF/FW932UEkUM0C7dsFJIg+Oc5mfUHrBT++leSTL/QbfuHoU6i/6QG
SlI6U/Yr6IvoEF/uvQMs10TMbLNvRJM9IwIDAQABo3sweTAJBgNVHRMEAjAAMCwG
CWCGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAdBgNV
HQ4EFgQUd5eRnRsr4fPX7+/NLhFiT2PcPKcwHwYDVR0jBBgwFoAUqy1TpTd9qNvc
sShXHlad5NGxlVgwDQYJKoZIhvcNAQEFBQADggQBADNzBK2CpVmUIENOao66lEGG
i5qwuLW+ZvZ1CkvqHAIhd/jW6a5LVU7koSbSfDohBoAbQB14jJI5H1M7sMVdcqKv
BiIaOUbyZU4HwHVh/iYDu80ilVR3G+Fa32ozPwq09GuqUSzVz+NEE06p2CklAgW9
88W9iTGB3kRgfr8nnoMkqa9S27+BwhtcBZ59kPtEHt5X5IknorcKb5S+hpyfKdZi
Lk9xovdwtqsahP0kjI3iNpuwB12SmNGOTIX13oXi2nlkGMPBJheM0SnEWGqfVYvZ
UQ0lpsQez6trbtnMrfhVaJT15e27u8QGIm8SrT3VxRlPJcEhBG4wOdhmpiI6sLTP
O47kS5mwZaLv70lAIqwXzpBiYAWPjibe1D9xLjOlZy9CEiGAaqHNmm1lbHYuUby7
SCzLjWC7F74e6VIOUx67Jfo3eVE570NR3flOjgbUj8OO11Yfrog6SatzmbEjvjR/
mtvIwRkrB7EOWRxR9LeB94ERsB9xskrLOrhYDc/s/jy3v/mypO5TEo6Jjxn3ySS3
6mQA2SqTiYGssnU34ykG5HaVXamVk/K8QSmuIU1OMpLyW5T3OVO970DJwO4knOg7
aAuTAL1zm6WRYBYkg4peLumDfUpWjzE4j8oSa1cvNNFdw+k0Ru/UATiyyBV6zJWg
M1nb3U/Ra5Nc9Git8xEctURgZI4m/RdERhwC72amBBkHuIu49XY/KHDA42ive2xG
9DoMt+DUodcefC+XV+n3L2XdwtaIJ5Gf9tCxSwTxoX/fQRyIxiKaPO1VoUsY//c6
XgD7JAbnx4hEyeJD7RAuBf4pgV6s75Rdg7D5qZTfrB5y66rS1ntsUcaKWqdIL/zq
KaLp39tEXbeA+cANbyn1GDIQIbHgo6elrN1IsXrwm5z/UIa/4sWZmlHBAicn3hHp
lGqVAWws3cbPGh/LbOv7/hANuS0ZfA1Dsa7/gutk1zA8ivyP8A42mMTBP3MOV21z
WmV/WqsZk2kP8SXB284vSAhnBsfiuvtK2UR8QS+6ArrLWy8zDGXVk8Z76tJ7iSKy
EoywuNzc0nNXwAmEqFmjL+HmKTzYO31LSw3rXS5XYoVEi7hNCSPJoPS7SBIejxoZ
s1QA3nPL/XkKNcV3wu+0L/VKxWQAXAkzZ0akjuSsgqK/kKUmIiQjCbvYxoHgQvRK
X8uJn8c30tJ8Nrze+rKzCp4Z4L0r7uhRx7Qkxfp1AIs4qu24+tevjb5A9B7lrzp/
gWvRcnm2YCXBS4KoPeDnCFtT7SG7IhJlf9Ajh51yJUaGO29lAxnZd4ZI7lhG4wtw
NJrMYKXnkqFBYhADVRvzBL1lpgojBOTbNLGXqLGQR90Fmvk1U2Yg/ZxF40W2kho=
-----END CERTIFICATE-----
```

2. Save the file.

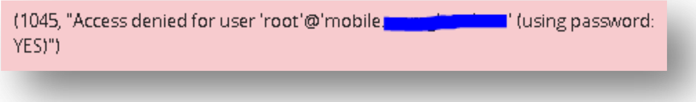
Return to Upload SSL Certificates to Configurator.

Troubleshooting MySQL Connectivity (HOWTO110250)

(During the Symantec Mobility Suite Configurator Installation)

Tip: If there is a problem connecting to the database take note of the following errors and example remedies:

Error:

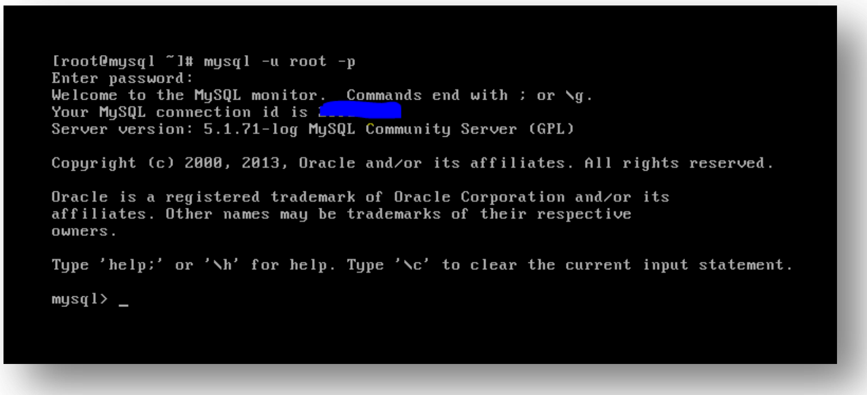


(1045, "Access denied for user 'root'@'mobile[redacted]' (using password: YES)")

Remedy: Verify the password, username and database information. If access is still denied, go to the MySQL host and log into the MySQL console with the following:

mysql –u root

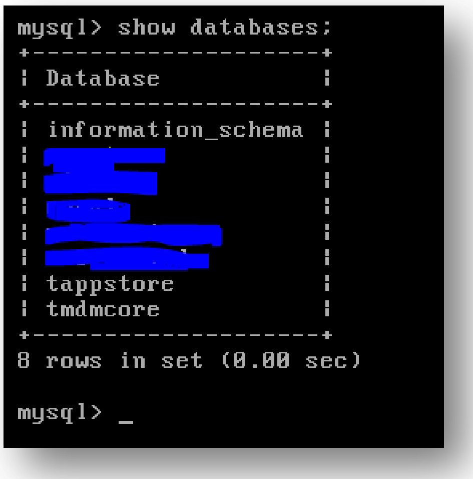
For example:



```
[root@mysql ~]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is [redacted]
Server version: 5.1.71-log MySQL Community Server (GPL)

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> _
```

Once a connection is established to the MySQL database the enter the following to show databases:

show databases;
For example:

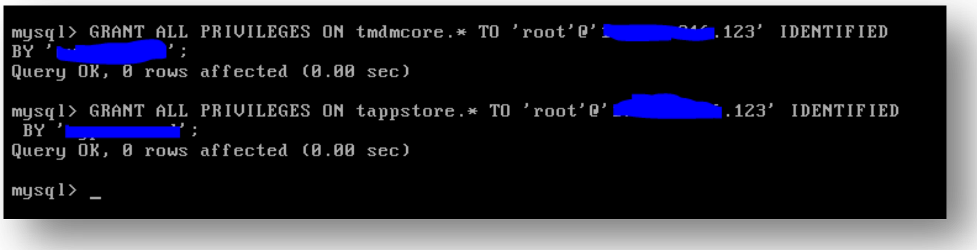


```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
[redacted]
| tappstore          |
| tmdmcore           |
+--------------------+
8 rows in set (0.00 sec)

mysql> _
```

Note: If there are no appstore and mdmcore databases, they may be created by entering the following two commands into the mysql console:
create database mdmcore;
create database appstore;

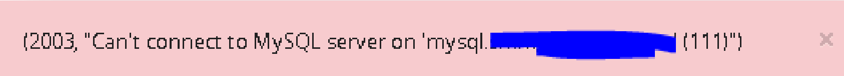
Make note of the two created databases and run the following two commands, into the mysql shell:
GRANT ALL PRIVILEGES ON <database1>.* TO 'username'@'<tenantIP>' IDENTIFIED BY '<password>';
GRANT ALL PRIVILEGES ON <database2>.* TO 'username'@'<tenantIP>' IDENTIFIED BY '<password>';

For example:



```
mysql> GRANT ALL PRIVILEGES ON tmdmcore.* TO 'root'@'[redacted].123' IDENTIFIED
BY '[redacted]';
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON tappstore.* TO 'root'@'[redacted].123' IDENTIFIED
 BY '[redacted]';
Query OK, 0 rows affected (0.00 sec)

mysql> _
```

Error:



(2003, "Can't connect to MySQL server on 'mysql.[redacted] (111)") ×

Remedy:
Confirm that the MySQL hostname is entered into the environment's domain name servers (DNS).
Verify that there is network communication between the Mobility FE and the MySQL host.

Once connectivity is confirmed continue to the Enter MySQL Connection Information section of this guide.

Temporary Email Option (HOWTO110251)

Important: Although this can be edited at a later time, email functionality is vital for password resets. A temporary relay using Gmail can be deployed using a valid Google email account. Enable POP3 access on the Google account and enter the following into the configurator:
host →smtp.gmail.com
port →587
username →<Google Email address>
password →<Gmail Password>
TLS Enabled →Yes

Important: The Gmail relay is only meant to be a **temporary** solution.

Click here to return to continue the Mail Relay Configuration.

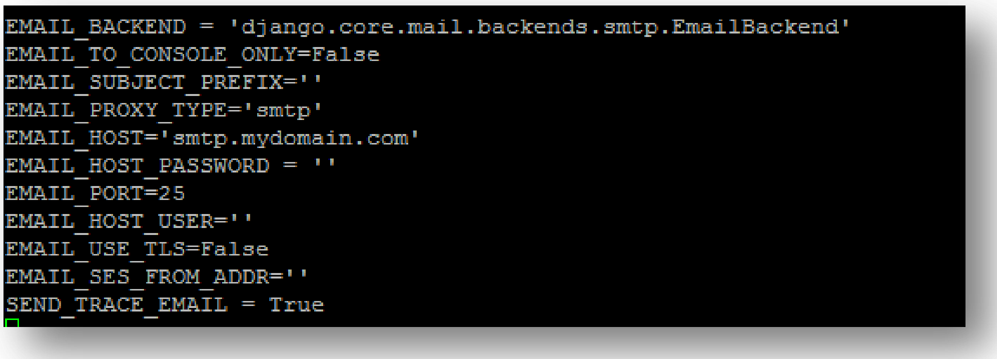
Changing the Mail-relay Post Configurator (HOWTO110249)

(Return to this step as needed)

To change the SMTP mail relay after completing the **bootstrapping** process: open a terminal to the FE. As root edit **/usr/local/nukona/appstore_cu/appstore_cu/settings_local.py**:
vi /usr/local/nukona/appstore_cu/appstore_cu/settings_local.py

The below lines can be changed and the following entries are accepted:
EMAIL_PROXY_TYPE='<smtp or localhost>'
EMAIL_HOST='<SMTPFQDN or localhost>'
EMAIL_HOST_PASSWORD = '<password or blank>'
EMAIL_PORT=<any port>
EMAIL_HOST_USER='<user or blank>'
EMAIL_USE_TLS=<True or False>

For example:



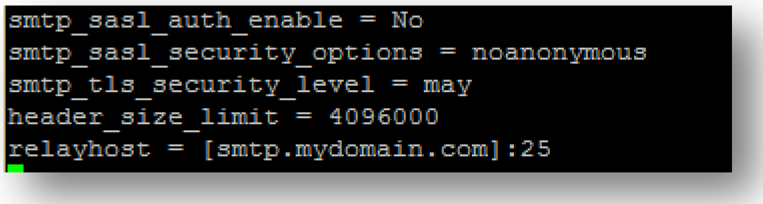
```
EMAIL_BACKEND = 'django.core.mail.backends.smtp.EmailBackend'
EMAIL_TO_CONSOLE_ONLY=False
EMAIL_SUBJECT_PREFIX=''
EMAIL_PROXY_TYPE='smtp'
EMAIL_HOST='smtp.mydomain.com'
EMAIL_HOST_PASSWORD = ''
EMAIL_PORT=25
EMAIL_HOST_USER=''
EMAIL_USE_TLS=False
EMAIL_SES_FROM_ADDR=''
SEND_TRACE_EMAIL = True
```

Restart Mobility Services:
sudo /etc/init.d/appcenter-services restart

If the **EMAIL_PROXY_TYPE='localhost'** and the **EMAIL_HOST='localhost'** the Mobility Suite FE will use postfix to proxy messages to the relay. Edit the postfix configuration file located at the end of the **/etc/postfix/main.cf** file:
vi /etc/postfix/main.cf

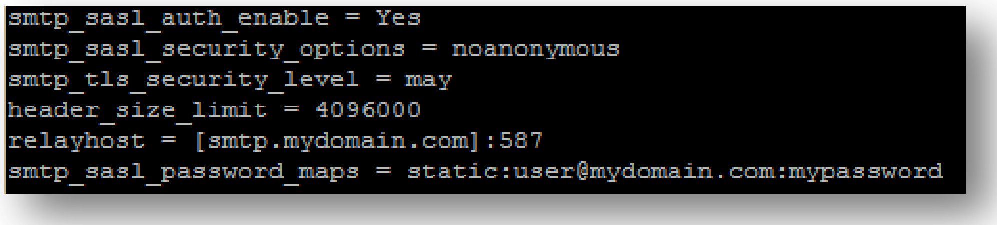
The below lines can be changed and the following entries are accepted:
smtp_sasl_auth_enable = <Yes or No>
smtp_sasl_security_options = noanonymous
smtp_tls_security_level = may
header_size_limit = 4096000
relayhost = [<SMTPFQDN or IP>]:<any port>
smtp_sasl_password_maps = static:<user>:<password>

For example:
Without Authentication:



```
smtp_sasl_auth_enable = No
smtp_sasl_security_options = noanonymous
smtp_tls_security_level = may
header_size_limit = 4096000
relayhost = [smtp.mydomain.com]:25
```

With authentication:



```
smtp_sasl_auth_enable = Yes
smtp_sasl_security_options = noanonymous
smtp_tls_security_level = may
header_size_limit = 4096000
relayhost = [smtp.mydomain.com]:587
smtp_sasl_password_maps = static:user@mydomain.com:mypassword
```

Restart postfix:
sudo service postfix restart

Tip: Postfix mail logs are stored in **/var/log/maillog** if the mail log contains messages regarding an **untrusted issuer** follow TECH209709 to build troubleshoot TLS failures.

Troubleshooting the Bootstrap / Configurator Process (HOWTO110301)

Tip: If there are any errors preventing this from completing review the following common errors with their remedies:

Error: Configurator has been hung on Configurator is running… for over 1 hour.
Remedy: The most likely cause of this is due to there being a failure in the HTTP connection between the workstation and the Configurator. The installation may have completed successfully. Go back to the Mobility Suite Server Console and type: **less /var/log/nukona/load_settings.log** while holding down the **Shift** key press **g**. This will bring the view to the end of the file. Successful completion of configurator will show a series of errors attempting to stop the Mobility Suite services followed by a series of successful service-starts. Use the **b** key and **spacebar** to page-up and down. **/** followed by a search string will search from the current view down.

Error: Configuration was unsuccessful.
Remedy: Review the load_settings.log file as described above. If there was any issues starting the Mobility Suite services take note of the service and run the following, as root:
sudo /etc/init.d/appcenter-services restart

Take note of any errors and messages and follow accordingly.

Tip: Log in and out of the linux terminal. This will allow the root bash profile to reload.

Error: Configuration was unsuccessful**.**
Remedy: If there are any entries in the **/var/log/nukona/load_settings.log** file for:
django.db.utils.OperationalError: (1298, Unknown or incorrect time zone: 'America/Los_Angeles') follow KB TECH217108. And restart the configurator by repeating Part IV: Installation and Part V: Bootstrapping.

Tip: Now is a good time to take a snapshot of the current hard drive state of the FE and most importantly of the Database host.

Return to Installation Part I or Installation Part II: Bootstrapping

Untrusted / In-house Certificates (HOWTO110246)

Important: In-house and self-signed certificates cannot be validated from iOS devices. This method should only be used to get past the Configurator step of the Mobility Suite installation. If an in-house certificate is used, the issuing CA certificate would need to be installed onto the mobile device (iOS8 no longer allows trusting in-house CA's). This usually can be accomplished by hosting the certificate on a website or file share and downloading it onto each device.

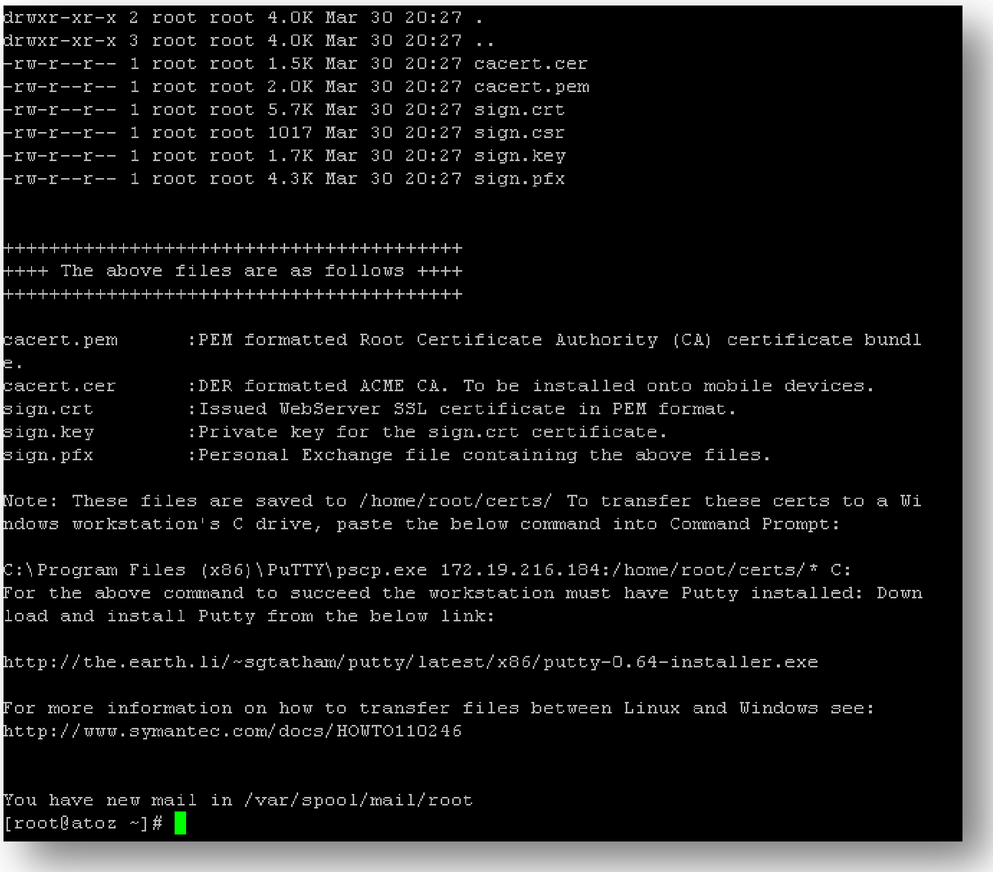
Option 1: Temporary Verisign Trial Certificate

For a temporary trial Verisign certificate click here. To generate a CSR for this request see: Create a CSR for iOS Development.

Option 2: Create an In-house Certificate Authority (HOWTO110246)

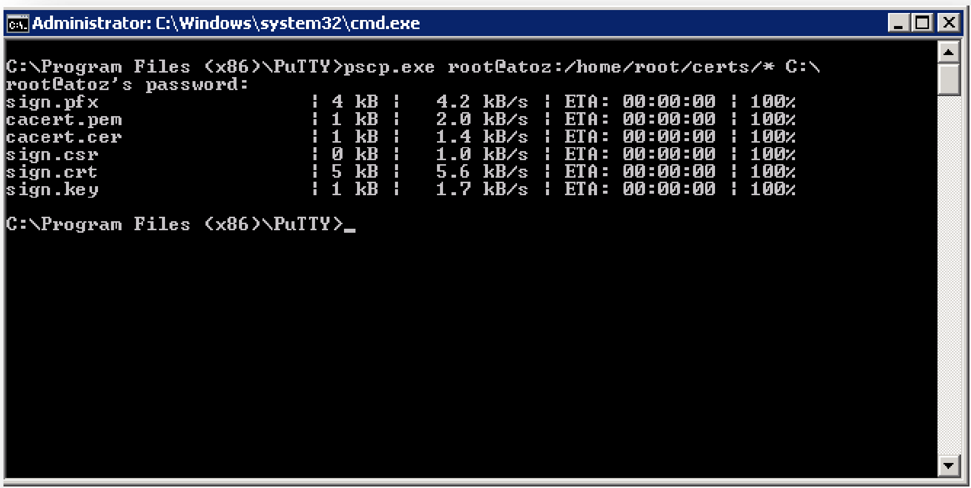
Run the **openca.sh** script from HOWTO110246, to deploy an in-house CA and issue an SSL certificate for the Mobility server (RHEL/CentOS 6). See HOWTO110248 to transfer the attached script to the CentOS 6 the enter the following two lines, as root:
chmod +x openca.sh
./openca.sh

The script will prompt for a common name (CN) for the webserver certificate. This must be the FQDN of the Mobility FE:



```
drwxr-xr-x 2 root root 4.0K Mar 30 20:27 .
drwxr-xr-x 3 root root 4.0K Mar 30 20:27 ..
-rw-r--r-- 1 root root 1.5K Mar 30 20:27 cacert.cer
-rw-r--r-- 1 root root 2.0K Mar 30 20:27 cacert.pem
-rw-r--r-- 1 root root 5.7K Mar 30 20:27 sign.crt
-rw-r--r-- 1 root root 1017 Mar 30 20:27 sign.csr
-rw-r--r-- 1 root root 1.7K Mar 30 20:27 sign.key
-rw-r--r-- 1 root root 4.3K Mar 30 20:27 sign.pfx


++++++++++++++++++++++++++++++++++++++++
++++ The above files are as follows ++++
++++++++++++++++++++++++++++++++++++++++

cacert.pem      :PEM formatted Root Certificate Authority (CA) certificate bundl
e.
cacert.cer      :DER formatted ACME CA. To be installed onto mobile devices.
sign.crt        :Issued WebServer SSL certificate in PEM format.
sign.key        :Private key for the sign.crt certificate.
sign.pfx        :Personal Exchange file containing the above files.

Note: These files are saved to /home/root/certs/ To transfer these certs to a Wi
ndows workstation's C drive, paste the below command into Command Prompt:

C:\Program Files (x86)\PuTTY\pscp.exe 172.19.216.184:/home/root/certs/* C:
For the above command to succeed the workstation must have Putty installed: Down
load and install Putty from the below link:

http://the.earth.li/~sgtatham/putty/latest/x86/putty-0.64-installer.exe

For more information on how to transfer files between Linux and Windows see:
http://www.symantec.com/docs/HOWTO110246


You have new mail in /var/spool/mail/root
[root@atoz ~]#
```

Copying files to PC from Linux using PSCP (Putty):



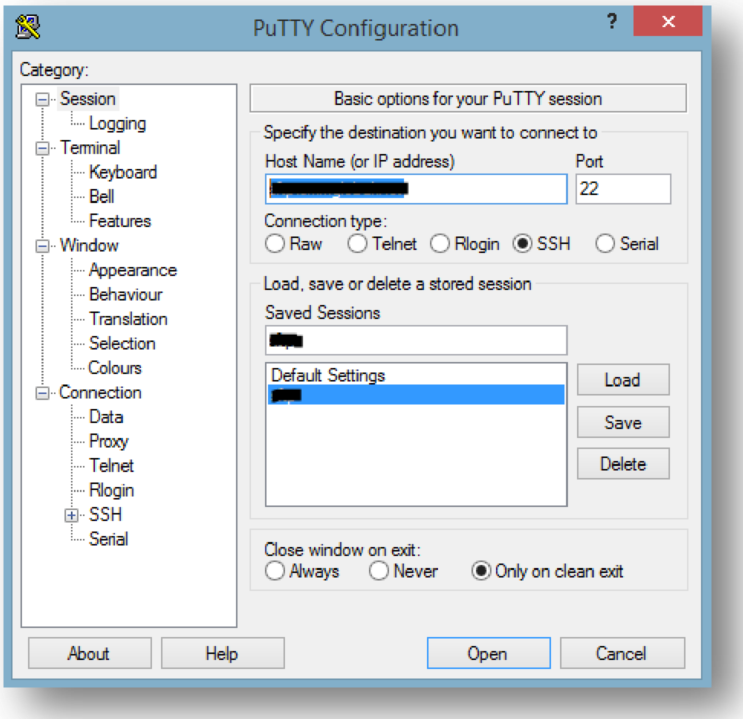
Administrator: C:\Windows\system32\cmd.exe

```
C:\Program Files (x86)\PuTTY>pscp.exe root@atoz:/home/root/certs/* C:\
root@atoz's password:
sign.pfx                  | 4 kB |   4.2 kB/s | ETA: 00:00:00 | 100%
cacert.pem                | 1 kB |   2.0 kB/s | ETA: 00:00:00 | 100%
cacert.cer                | 1 kB |   1.4 kB/s | ETA: 00:00:00 | 100%
sign.csr                  | 0 kB |   1.0 kB/s | ETA: 00:00:00 | 100%
sign.crt                  | 5 kB |   5.6 kB/s | ETA: 00:00:00 | 100%
sign.key                  | 1 kB |   1.7 kB/s | ETA: 00:00:00 | 100%

C:\Program Files (x86)\PuTTY>_
```

Instead of running the script, manually create the in-house CA and SSL certificates by completing the following steps.

Note: If the **openca.sh** script has already run, there is no need to continue with this manual method. Return to Upload SSL Certificates to Configurator.

1. To manually create the CA and issue a webserver SSL certificate use Putty to obtain root shell access to the Mobility Suite FE:



Specify the destination you want to connect to

Host Name (or IP address): [redacted]

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

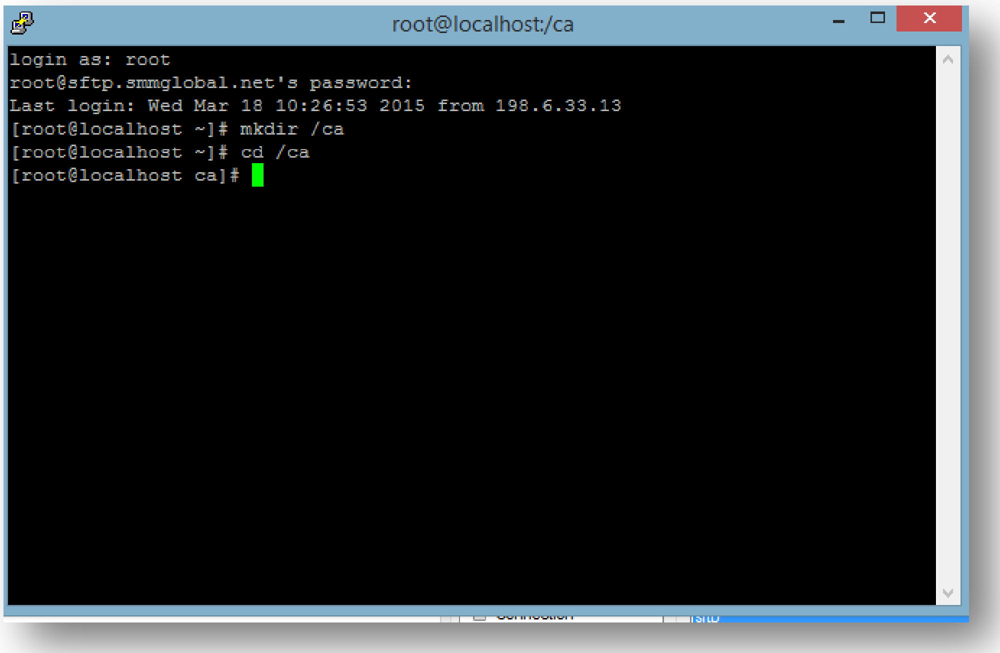
Load, save or delete a stored session

Saved Sessions: [redacted]

Default Settings
[redacted]

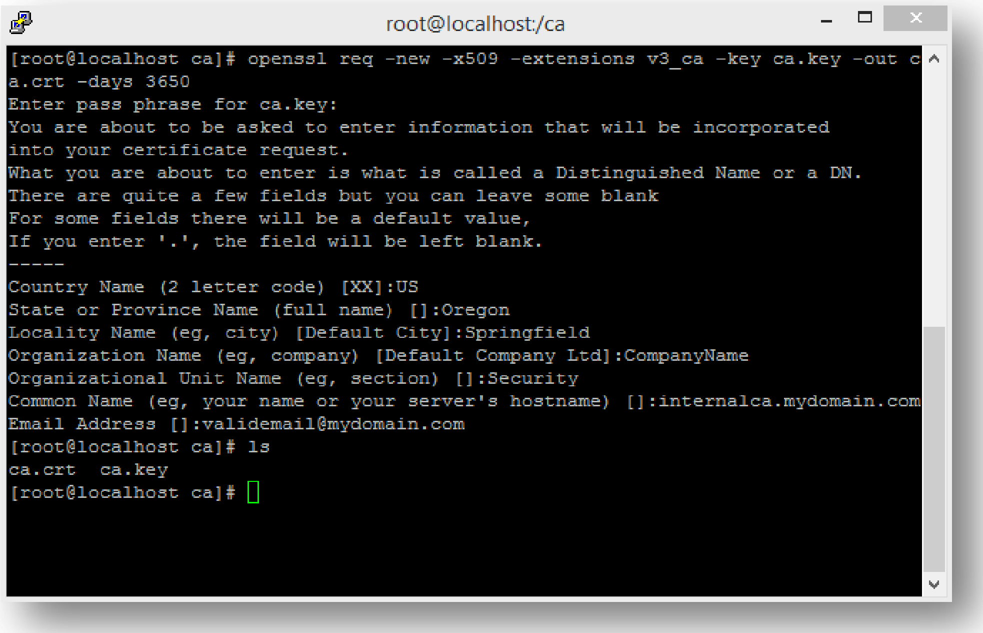
Close window on exit: ○ Always ○ Never ● Only on clean exit

2. Once root shell access is obtained type:
   mkdir /ca/
3. Change directories to **/ca**:
   cd /ca/



```
login as: root
root@sftp.smmglobal.net's password:
Last login: Wed Mar 18 10:26:53 2015 from 198.6.33.13
[root@localhost ~]# mkdir /ca
[root@localhost ~]# cd /ca
[root@localhost ca]# 
```

4. Enter the following to create a CA key, when prompted enter a complex password for the **key**:
   openssl genrsa -aes256 -out cakey.pem 4096
5. Enter the following to create a CA certificate from the newly created **CA Key**:
   openssl req -new -x509 -extensions v3_ca -key cakey.pem -out cacert.pem -days 3650
6. When prompted enter the key's password and all of the form data as requested:

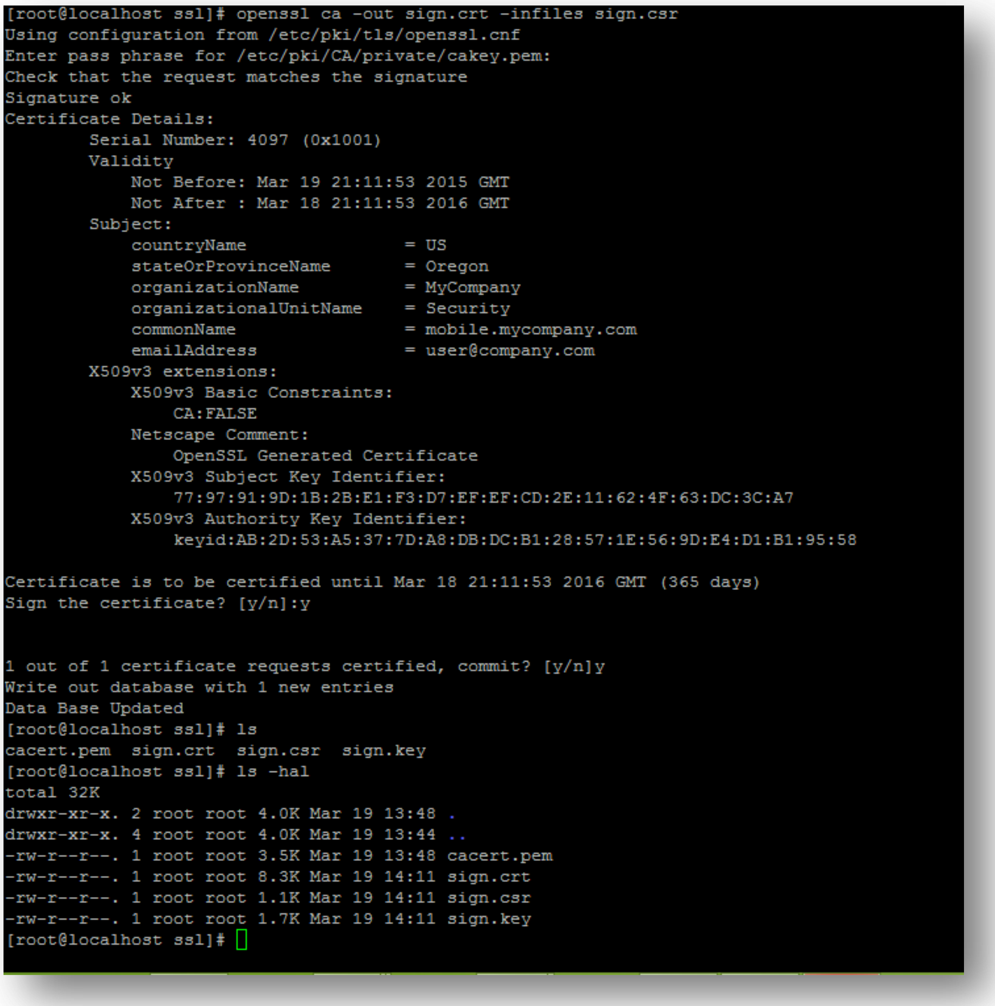


```
[root@localhost ca]# openssl req -new -x509 -extensions v3_ca -key ca.key -out c
a.crt -days 3650
Enter pass phrase for ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:Oregon
Locality Name (eg, city) [Default City]:Springfield
Organization Name (eg, company) [Default Company Ltd]:CompanyName
Organizational Unit Name (eg, section) []:Security
Common Name (eg, your name or your server's hostname) []:internalca.mydomain.com
Email Address []:validemail@mydomain.com
[root@localhost ca]# ls
ca.crt  ca.key
[root@localhost ca]#
```

7. Copy the ca.key file to /etc/pki/CA/private:
   cp /ca/cakey.pem /etc/pki/CA/private/
8. Copy the ca.crt to /etc/pki/CA/certs:
   cp /ca/cacert.pem /etc/pki/CA/
9. Create some required files inside the CA directory structure by entering the following two lines:
   touch /etc/pki/CA/index.txt
   echo 1000 >> /etc/pki/CA/serial
10. Secure the private key with:
    chmod 0400 /etc/pki/CA/private/cakey.pem
11. Now that the CA is created, create a new directory, generate a CSR and submit that to the CA (do not secure the key & CSR with a password) by entering the below three lines:
    mkdir /ca/ssl/
    cd /ca/ssl/
    openssl req -new -nodes -newkey rsa:2048 -keyout sign.key -out sign.csr -days 365

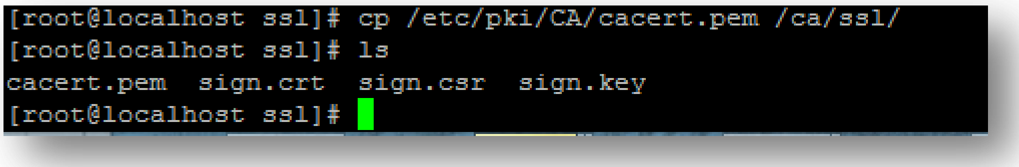
Important: The Common name must be the FQDN of the Mobility Suite FE. The organizational name, Country and State must match those of the CA. Recreate the CSR until the names/entries match.

12. Issue a domain certificate using the CA by entering the following command, enter the password created for the CA key and follow the prompts:
    openssl ca -out sign.crt -infiles sign.csr



```
[root@localhost ssl]# openssl ca -out sign.crt -infiles sign.csr
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for /etc/pki/CA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4097 (0x1001)
        Validity
            Not Before: Mar 19 21:11:53 2015 GMT
            Not After : Mar 18 21:11:53 2016 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = Oregon
            organizationName          = MyCompany
            organizationalUnitName    = Security
            commonName                = mobile.mycompany.com
            emailAddress              = user@company.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                77:97:91:9D:1B:2B:E1:F3:D7:EF:EF:CD:2E:11:62:4F:63:DC:3C:A7
            X509v3 Authority Key Identifier:
                keyid:AB:2D:53:A5:37:7D:A8:DB:DC:B1:28:57:1E:56:9D:E4:D1:B1:95:58

Certificate is to be certified until Mar 18 21:11:53 2016 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
[root@localhost ssl]# ls
cacert.pem  sign.crt  sign.csr  sign.key
[root@localhost ssl]# ls -hal
total 32K
drwxr-xr-x. 2 root root 4.0K Mar 19 13:48 .
drwxr-xr-x. 4 root root 4.0K Mar 19 13:44 ..
-rw-r--r--. 1 root root 3.5K Mar 19 13:48 cacert.pem
-rw-r--r--. 1 root root 8.3K Mar 19 14:11 sign.crt
-rw-r--r--. 1 root root 1.1K Mar 19 14:11 sign.csr
-rw-r--r--. 1 root root 1.7K Mar 19 14:11 sign.key
[root@localhost ssl]#
```

13. Copy the cacert.pem to the same directory:
    cp /etc/pki/CA/cacert.pem /ca/ssl/



```
[root@localhost ssl]# cp /etc/pki/CA/cacert.pem /ca/ssl/
[root@localhost ssl]# ls
cacert.pem  sign.crt  sign.csr  sign.key
[root@localhost ssl]#
```

14. Since this is an untrusted CA the **cacert.pem** must be installed onto each Mobile device prior to enrollment. The quickest way to accomplish this is to upload and share the certificate using a static HTTP link. This can be done using the direct link option “Anyone with the link” for the following share solutions: Google Drive, Box and Dropbox. Windows Phone requires that the cert be in DER format. Use the following openssl command to copy and conver this into DER format:
    openssl x509 -in cacert.pem -inform PEM -out cacert.crt -outform DER

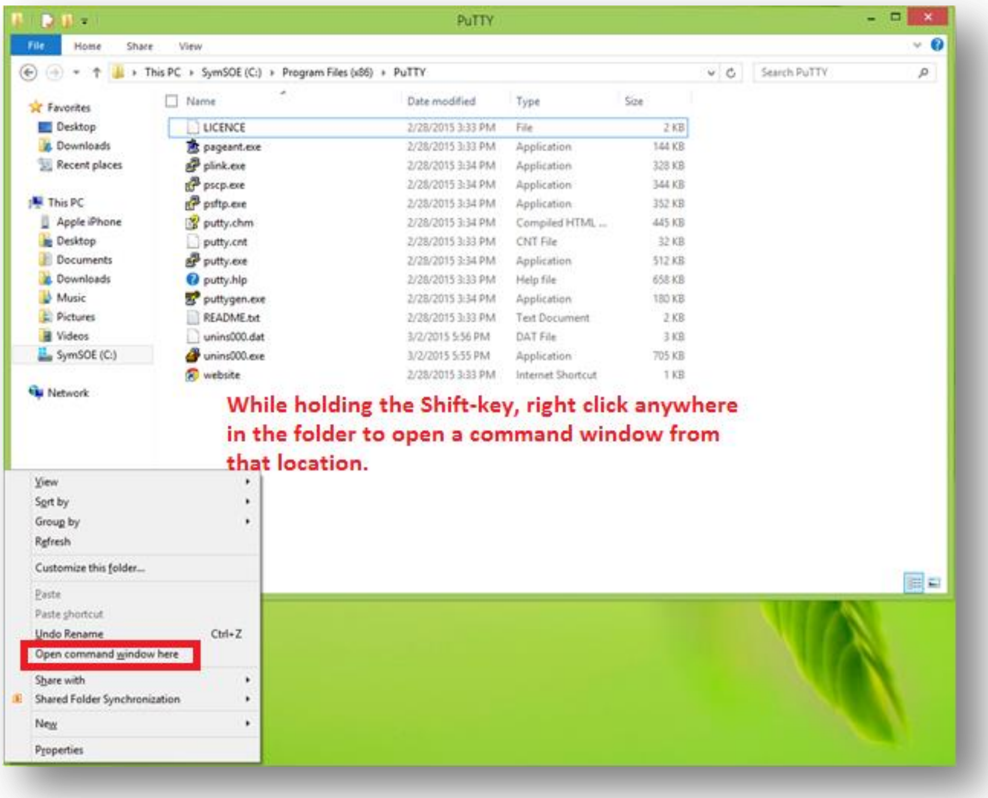
15. Continue to the How to transfer files from a Linux machine section below.

How to transfer files from a Linux machine (HOWTO110248)

Note: WinCP or Putty may be used, the below example, PSCP (Putty) will be used.

1. Download and install Putty onto the workstation.
2. Open a Command Prompt terminal and change directories to the Putty-installation-path.

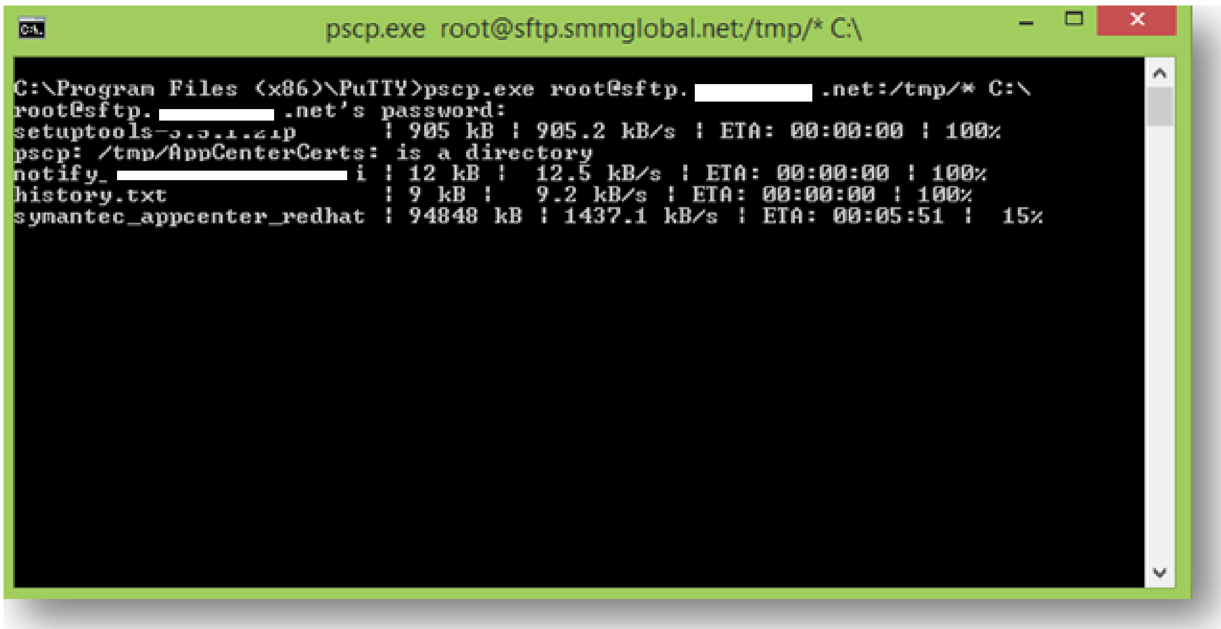
Tip: Browse to the Putty installation path **C:\Program Files (x86)\Putty\** using the Windows Explorer. Once in the directory, while holding the **shift**-key **right-click** anywhere in the window and select **Open command window here**. WinCP and Filezilla offer a graphical user interfaces (GUI) to transfer files between Linux and Windows.



Name	Date modified	Type	Size
LICENCE	2/28/2015 3:33 PM	File	2 KB
pageant.exe	2/28/2015 3:33 PM	Application	144 KB
plink.exe	2/28/2015 3:34 PM	Application	328 KB
pscp.exe	2/28/2015 3:34 PM	Application	344 KB
psftp.exe	2/28/2015 3:34 PM	Application	352 KB
putty.chm	2/28/2015 3:34 PM	Compiled HTML ...	445 KB
putty.cnt	2/28/2015 3:33 PM	CNT File	32 KB
putty.exe	2/28/2015 3:34 PM	Application	512 KB
putty.hlp	2/28/2015 3:33 PM	Help file	658 KB
puttygen.exe	2/28/2015 3:34 PM	Application	180 KB
README.txt	2/28/2015 3:33 PM	Text Document	2 KB
unins000.dat	3/2/2015 5:56 PM	DAT File	3 KB
unins000.exe	3/2/2015 5:55 PM	Application	705 KB
website	2/28/2015 3:33 PM	Internet Shortcut	1 KB

While holding the Shift-key, right click anywhere in the folder to open a command window from that location.

3. Enter the following line, replacing the <variable> items:
   pscp.exe root@<RemoteHost>:<RemoteDirectory>/* C:\



pscp.exe root@sftp.smmglobal.net:/tmp/* C:\

```
C:\Program Files (x86)\PuTTY>pscp.exe root@sftp.[redacted].net:/tmp/* C:\
root@sftp.[redacted].net's password:
setuptools-[redacted]p        | 905 kB | 905.2 kB/s | ETA: 00:00:00 | 100%
pscp: /tmp/AppCenterCerts: is a directory
notify_[redacted]i | 12 kB |  12.5 kB/s | ETA: 00:00:00 | 100%
history.txt                | 9 kB |   9.2 kB/s | ETA: 00:00:00 | 100%
symantec_appcenter_redhat | 94848 kB | 1437.1 kB/s | ETA: 00:05:51 |  15%
```

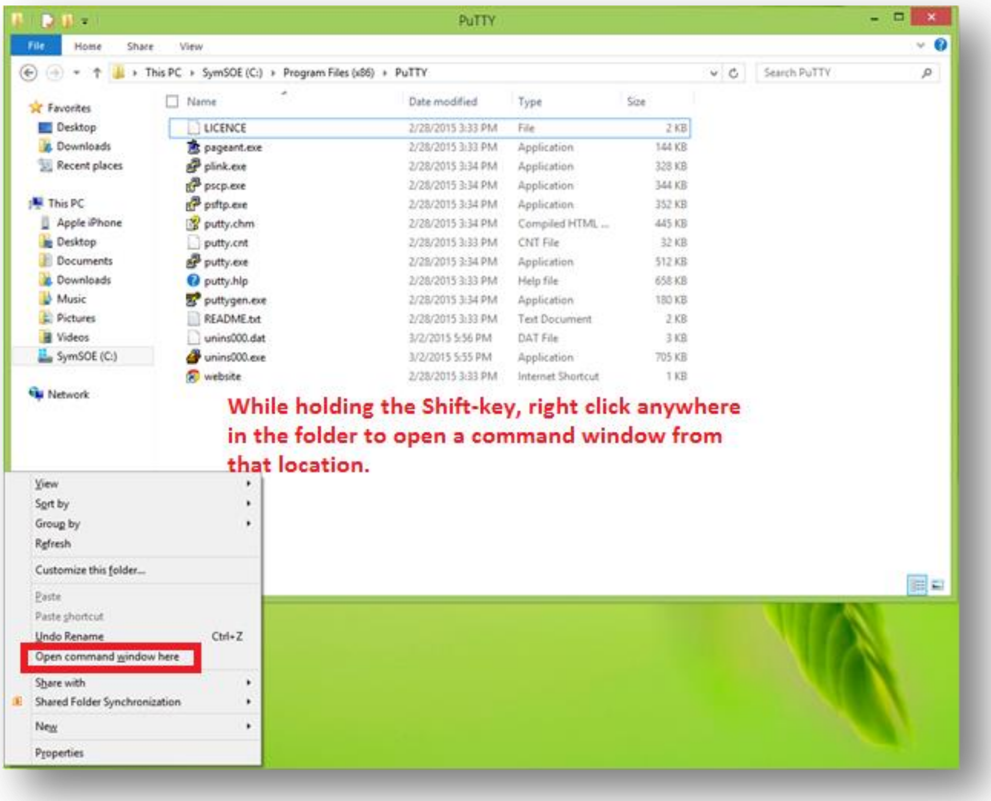
4. If following the installation of Mobility Suite: return to Upload SSL Certificates to Configurator.

How to transfer files to a Linux machine (HOWTO110248)

Note: WinCP or Putty may be used, the below example, PSCP (Putty) will be used.

1. Download and install Putty onto the workstation.
2. Open a Command Prompt terminal and change directories to the Putty-installation-path.

Tip: Browse to the Putty installation path **C:\Program Files (x86)\Putty\** using the Windows Explorer. Once in the directory, while holding the **shift**-key **right-click** anywhere in the window and select **Open command window here**. WinCP and Filezilla offer a graphical user interfaces (GUI) to transfer files between Linux and Windows.

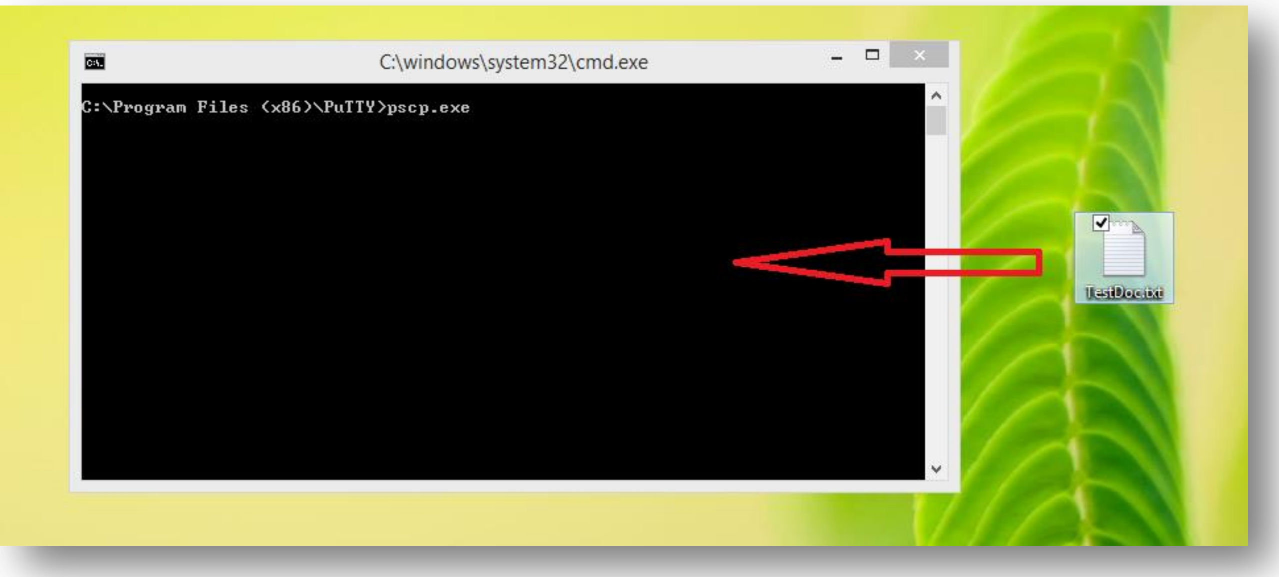


Name	Date modified	Type	Size
LICENCE	2/28/2015 3:33 PM	File	2 KB
pageant.exe	2/28/2015 3:33 PM	Application	144 KB
plink.exe	2/28/2015 3:34 PM	Application	328 KB
pscp.exe	2/28/2015 3:34 PM	Application	344 KB
psftp.exe	2/28/2015 3:34 PM	Application	352 KB
putty.chm	2/28/2015 3:34 PM	Compiled HTML ...	445 KB
putty.cnt	2/28/2015 3:33 PM	CNT File	32 KB
putty.exe	2/28/2015 3:34 PM	Application	512 KB
putty.hlp	2/28/2015 3:33 PM	Help file	658 KB
puttygen.exe	2/28/2015 3:34 PM	Application	180 KB
README.txt	2/28/2015 3:33 PM	Text Document	2 KB
unins000.dat	3/2/2015 5:56 PM	DAT File	3 KB
unins000.exe	3/2/2015 5:55 PM	Application	705 KB
website	2/28/2015 3:33 PM	Internet Shortcut	1 KB

While holding the Shift-key, right click anywhere in the folder to open a command window from that location.

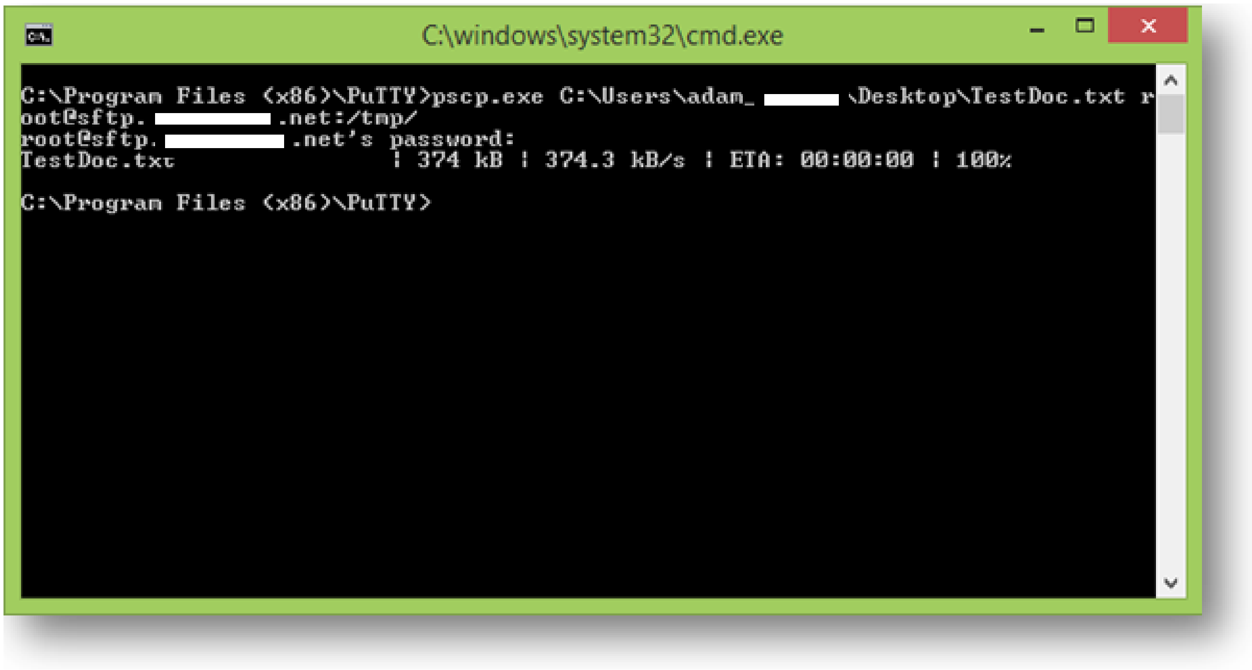
3. Enter the following line, replacing the <variable> items:
   pscp.exe <LocalFilePath> <user>@<RemoteHost>:<RemoteDirectory>

Tip: Simply drag the file, to be transferred, into the Command Prompt window after typing pscp.exe; this will automatically populated the <LocalFilePath>.



```
C:\Program Files (x86)\PuTTY>pscp.exe
```

For example:



```
C:\Program Files (x86)\PuTTY>pscp.exe C:\Users\adam_[redacted]\Desktop\TestDoc.txt r
oot@sftp.[redacted].net:/tmp/
root@sftp.[redacted].net's password:
TestDoc.txt               | 374 kB | 374.3 kB/s | ETA: 00:00:00 | 100%

C:\Program Files (x86)\PuTTY>
```

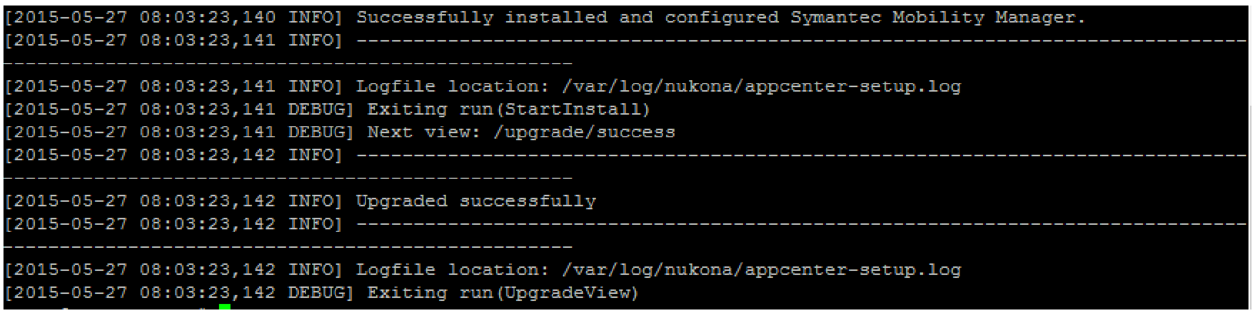
To return to Obtain the Symantec Mobility ISO.

Logging

Logging locations:

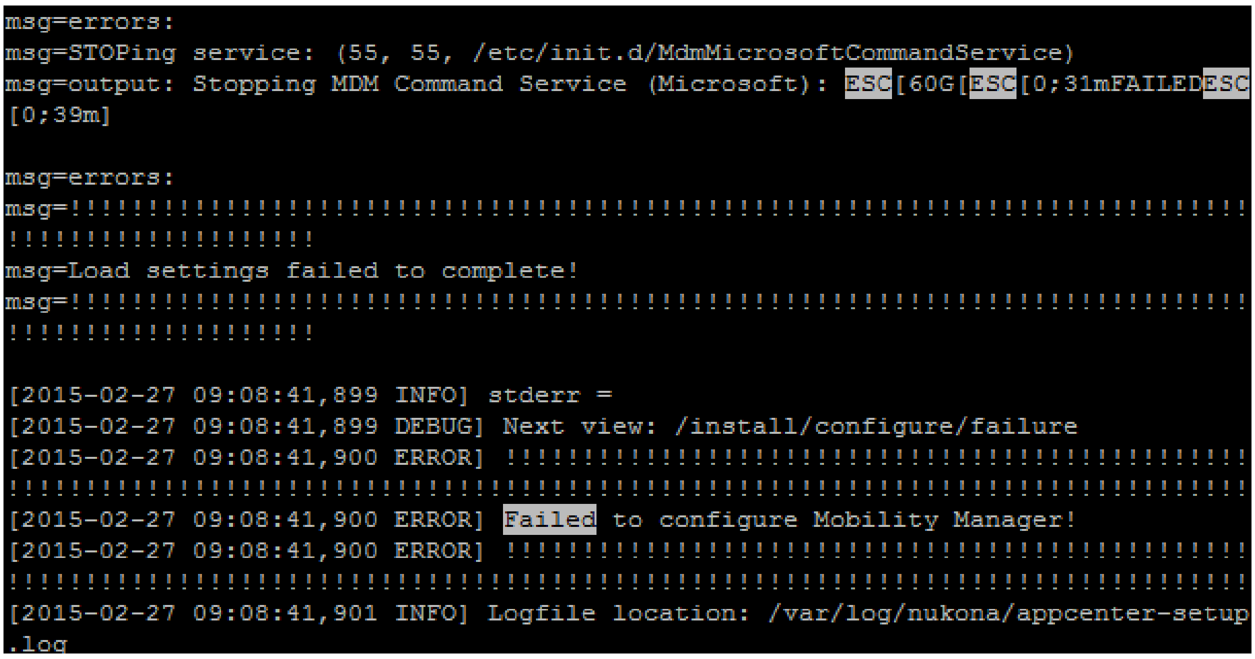
Install:

/var/log/nukona/appcenter-setup.log



```
[2015-05-27 08:03:23,140 INFO] Successfully installed and configured Symantec Mobility Manager.
[2015-05-27 08:03:23,141 INFO] -------------------------------------------------------------------------------
--------------------------------------------------
[2015-05-27 08:03:23,141 INFO] Logfile location: /var/log/nukona/appcenter-setup.log
[2015-05-27 08:03:23,141 DEBUG] Exiting run(StartInstall)
[2015-05-27 08:03:23,141 DEBUG] Next view: /upgrade/success
[2015-05-27 08:03:23,142 INFO] -------------------------------------------------------------------------------
--------------------------------------------------
[2015-05-27 08:03:23,142 INFO] Upgraded successfully
[2015-05-27 08:03:23,142 INFO] -------------------------------------------------------------------------------
--------------------------------------------------
[2015-05-27 08:03:23,142 INFO] Logfile location: /var/log/nukona/appcenter-setup.log
[2015-05-27 08:03:23,142 DEBUG] Exiting run(UpgradeView)
```

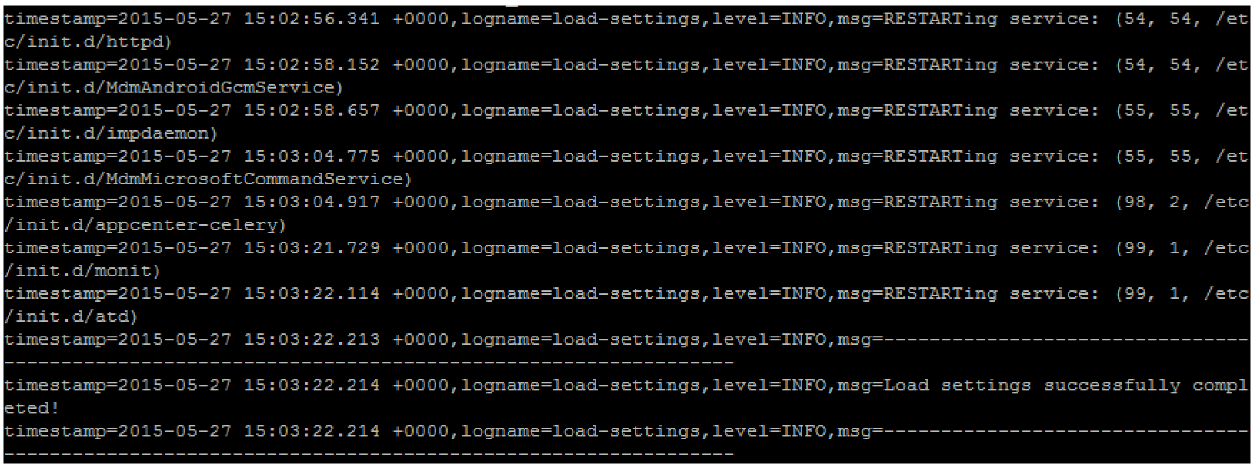
Error example:



```
msg=errors:
msg=STOPing service: (55, 55, /etc/init.d/MdmMicrosoftCommandService)
msg=output: Stopping MDM Command Service (Microsoft): ESC[60G[ESC[0;31mFAILEDESC
[0;39m]

msg=errors:
msg=!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
msg=Load settings failed to complete!
msg=!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!

[2015-02-27 09:08:41,899 INFO] stderr =
[2015-02-27 09:08:41,899 DEBUG] Next view: /install/configure/failure
[2015-02-27 09:08:41,900 ERROR] !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[2015-02-27 09:08:41,900 ERROR] Failed to configure Mobility Manager!
[2015-02-27 09:08:41,900 ERROR] !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[2015-02-27 09:08:41,901 INFO] Logfile location: /var/log/nukona/appcenter-setup
.log
```

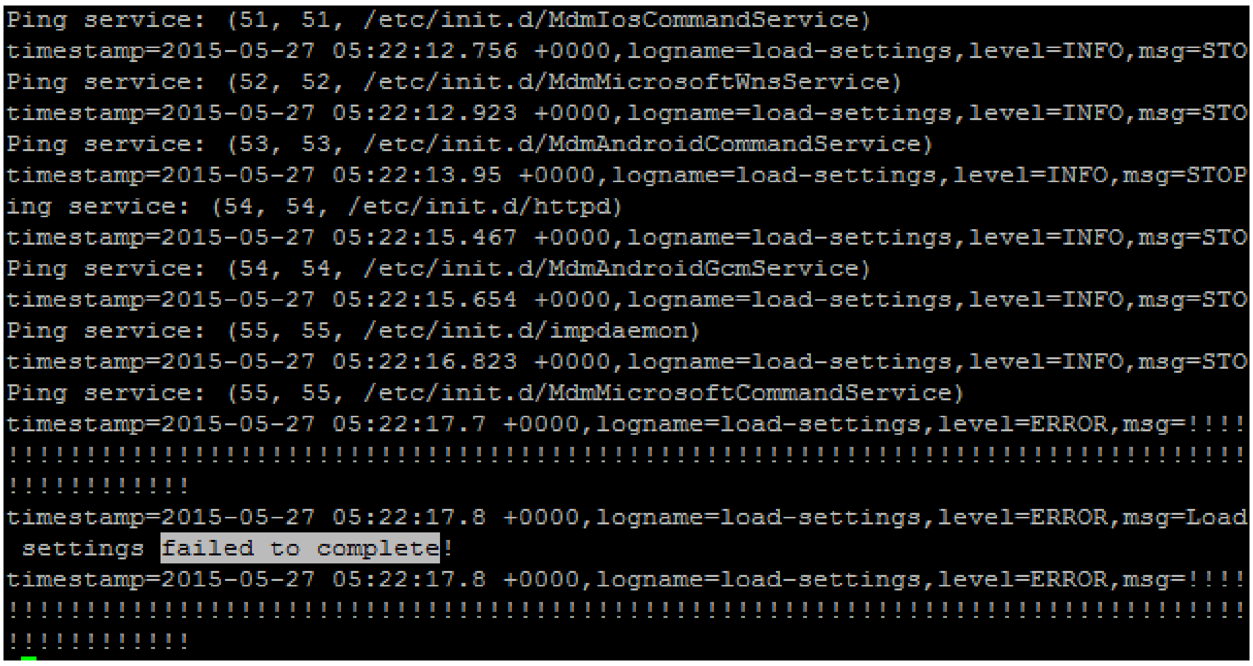
Bootstrap (provisioning):

/var/log/nukona/load_settings.log



```
timestamp=2015-05-27 15:02:56.341 +0000,logname=load-settings,level=INFO,msg=RESTARTing service: (54, 54, /et
c/init.d/httpd)
timestamp=2015-05-27 15:02:58.152 +0000,logname=load-settings,level=INFO,msg=RESTARTing service: (54, 54, /et
c/init.d/MdmAndroidGcmService)
timestamp=2015-05-27 15:02:58.657 +0000,logname=load-settings,level=INFO,msg=RESTARTing service: (55, 55, /et
c/init.d/impdaemon)
timestamp=2015-05-27 15:03:04.775 +0000,logname=load-settings,level=INFO,msg=RESTARTing service: (55, 55, /et
c/init.d/MdmMicrosoftCommandService)
timestamp=2015-05-27 15:03:04.917 +0000,logname=load-settings,level=INFO,msg=RESTARTing service: (98, 2, /etc
/init.d/appcenter-celery)
timestamp=2015-05-27 15:03:21.729 +0000,logname=load-settings,level=INFO,msg=RESTARTing service: (99, 1, /etc
/init.d/monit)
timestamp=2015-05-27 15:03:22.114 +0000,logname=load-settings,level=INFO,msg=RESTARTing service: (99, 1, /etc
/init.d/atd)
timestamp=2015-05-27 15:03:22.213 +0000,logname=load-settings,level=INFO,msg=--------------------------------
----------------------------------------------------------------
timestamp=2015-05-27 15:03:22.214 +0000,logname=load-settings,level=INFO,msg=Load settings successfully compl
eted!
timestamp=2015-05-27 15:03:22.214 +0000,logname=load-settings,level=INFO,msg=--------------------------------
----------------------------------------------------------------
```

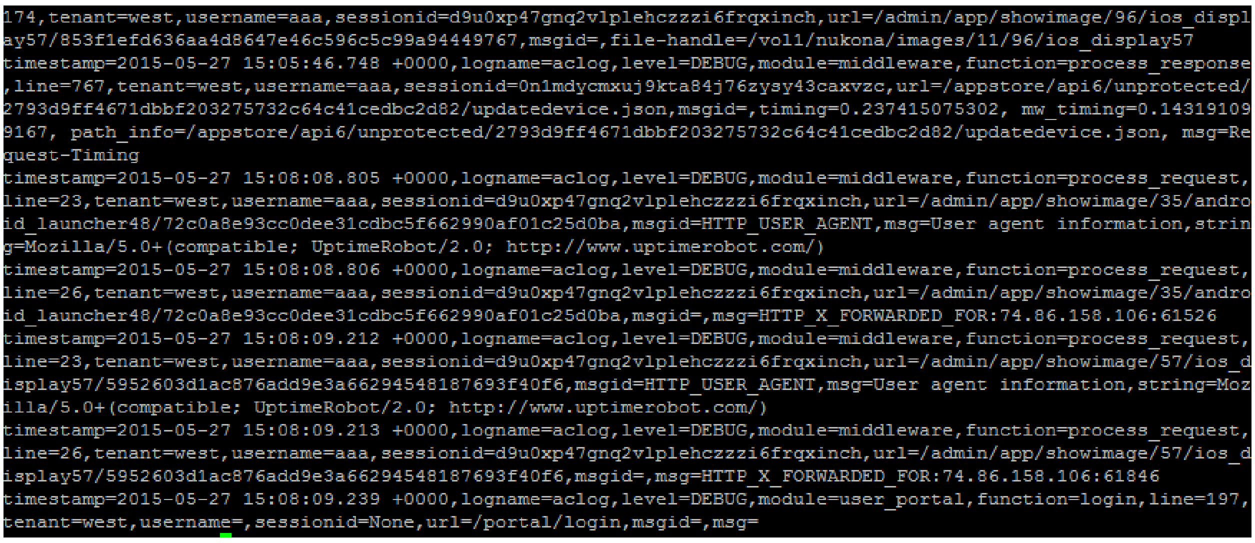
Error:



```
Ping service: (51, 51, /etc/init.d/MdmIosCommandService)
timestamp=2015-05-27 05:22:12.756 +0000,logname=load-settings,level=INFO,msg=STO
Ping service: (52, 52, /etc/init.d/MdmMicrosoftWnsService)
timestamp=2015-05-27 05:22:12.923 +0000,logname=load-settings,level=INFO,msg=STO
Ping service: (53, 53, /etc/init.d/MdmAndroidCommandService)
timestamp=2015-05-27 05:22:13.95 +0000,logname=load-settings,level=INFO,msg=STOP
ing service: (54, 54, /etc/init.d/httpd)
timestamp=2015-05-27 05:22:15.467 +0000,logname=load-settings,level=INFO,msg=STO
Ping service: (54, 54, /etc/init.d/MdmAndroidGcmService)
timestamp=2015-05-27 05:22:15.654 +0000,logname=load-settings,level=INFO,msg=STO
Ping service: (55, 55, /etc/init.d/impdaemon)
timestamp=2015-05-27 05:22:16.823 +0000,logname=load-settings,level=INFO,msg=STO
Ping service: (55, 55, /etc/init.d/MdmMicrosoftCommandService)
timestamp=2015-05-27 05:22:17.7 +0000,logname=load-settings,level=ERROR,msg=!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!
timestamp=2015-05-27 05:22:17.8 +0000,logname=load-settings,level=ERROR,msg=Load
 settings failed to complete!
timestamp=2015-05-27 05:22:17.8 +0000,logname=load-settings,level=ERROR,msg=!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!
```

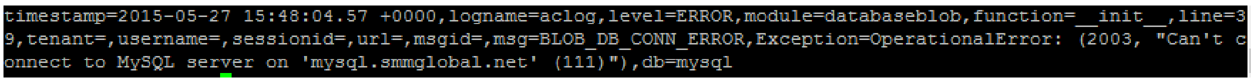
Appstore:

/var/log/nukona/appstore.log



```
174,tenant=west,username=aaa,sessionid=d9u0xp47gnq2vlplehczzzi6frqxinch,url=/admin/app/showimage/96/ios_displ
ay57/853f1efd636aa4d8647e46c596c5c99a94449767,msgid=,file-handle=/vol1/nukona/images/11/96/ios_display57
timestamp=2015-05-27 15:05:46.748 +0000,logname=aclog,level=DEBUG,module=middleware,function=process_response
,line=767,tenant=west,username=aaa,sessionid=0n1mdycmxuj9kta84j76zysy43caxvzc,url=/appstore/api6/unprotected/
2793d9ff4671dbbf203275732c64c41cedbc2d82/updatedevice.json,msgid=,timing=0.237415075302, mw_timing=0.14319109
9167, path_info=/appstore/api6/unprotected/2793d9ff4671dbbf203275732c64c41cedbc2d82/updatedevice.json, msg=Re
quest-Timing
timestamp=2015-05-27 15:08:08.805 +0000,logname=aclog,level=DEBUG,module=middleware,function=process_request,
line=23,tenant=west,username=aaa,sessionid=d9u0xp47gnq2vlplehczzzi6frqxinch,url=/admin/app/showimage/35/andro
id_launcher48/72c0a8e93cc0dee31cdbc5f662990af01c25d0ba,msgid=HTTP_USER_AGENT,msg=User agent information,strin
g=Mozilla/5.0+(compatible; UptimeRobot/2.0; http://www.uptimerobot.com/)
timestamp=2015-05-27 15:08:08.806 +0000,logname=aclog,level=DEBUG,module=middleware,function=process_request,
line=26,tenant=west,username=aaa,sessionid=d9u0xp47gnq2vlplehczzzi6frqxinch,url=/admin/app/showimage/35/andro
id_launcher48/72c0a8e93cc0dee31cdbc5f662990af01c25d0ba,msgid=,msg=HTTP_X_FORWARDED_FOR:74.86.158.106:61526
timestamp=2015-05-27 15:08:09.212 +0000,logname=aclog,level=DEBUG,module=middleware,function=process_request,
line=23,tenant=west,username=aaa,sessionid=d9u0xp47gnq2vlplehczzzi6frqxinch,url=/admin/app/showimage/57/ios_d
isplay57/5952603d1ac876add9e3a66294548187693f40f6,msgid=HTTP_USER_AGENT,msg=User agent information,string=Moz
illa/5.0+(compatible; UptimeRobot/2.0; http://www.uptimerobot.com/)
timestamp=2015-05-27 15:08:09.213 +0000,logname=aclog,level=DEBUG,module=middleware,function=process_request,
line=26,tenant=west,username=aaa,sessionid=d9u0xp47gnq2vlplehczzzi6frqxinch,url=/admin/app/showimage/57/ios_d
isplay57/5952603d1ac876add9e3a66294548187693f40f6,msgid=,msg=HTTP_X_FORWARDED_FOR:74.86.158.106:61846
timestamp=2015-05-27 15:08:09.239 +0000,logname=aclog,level=DEBUG,module=user_portal,function=login,line=197,
tenant=west,username=,sessionid=None,url=/portal/login,msgid=,msg=
```

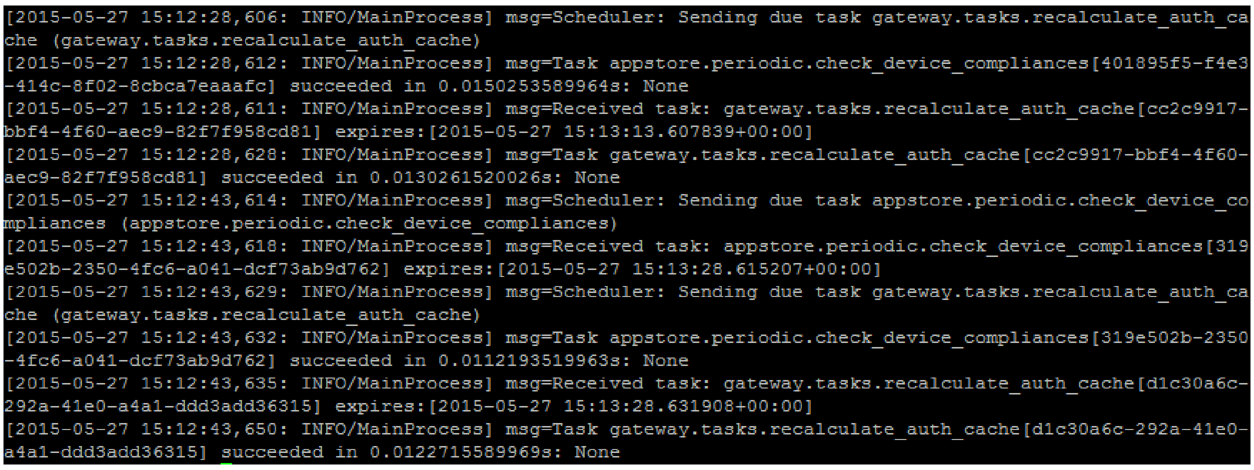
Error:



```
timestamp=2015-05-27 15:48:04.57 +0000,logname=aclog,level=ERROR,module=databaseblob,function=__init__,line=3
9,tenant=,username=,sessionid=,url=,msgid=,msg=BLOB_DB_CONN_ERROR,Exception=OperationalError: (2003, "Can't c
onnect to MySQL server on 'mysql.smmglobal.net' (111)"),db=mysql
```

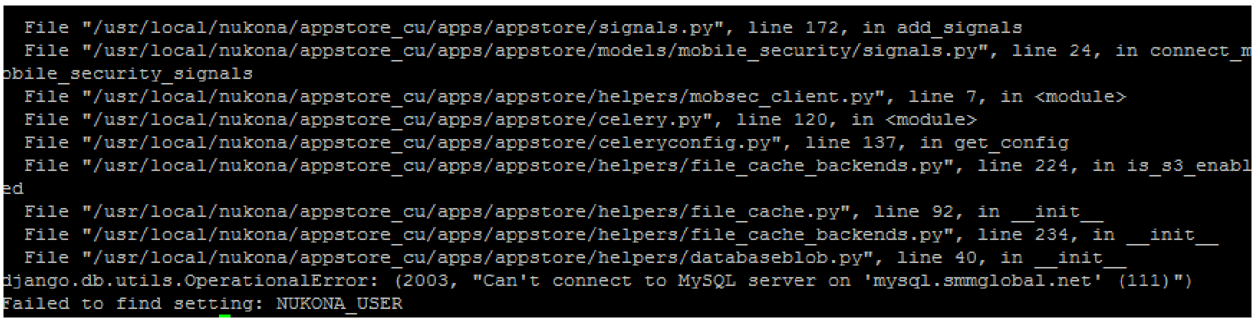
Celery:

/var/log/nukona/celery.log



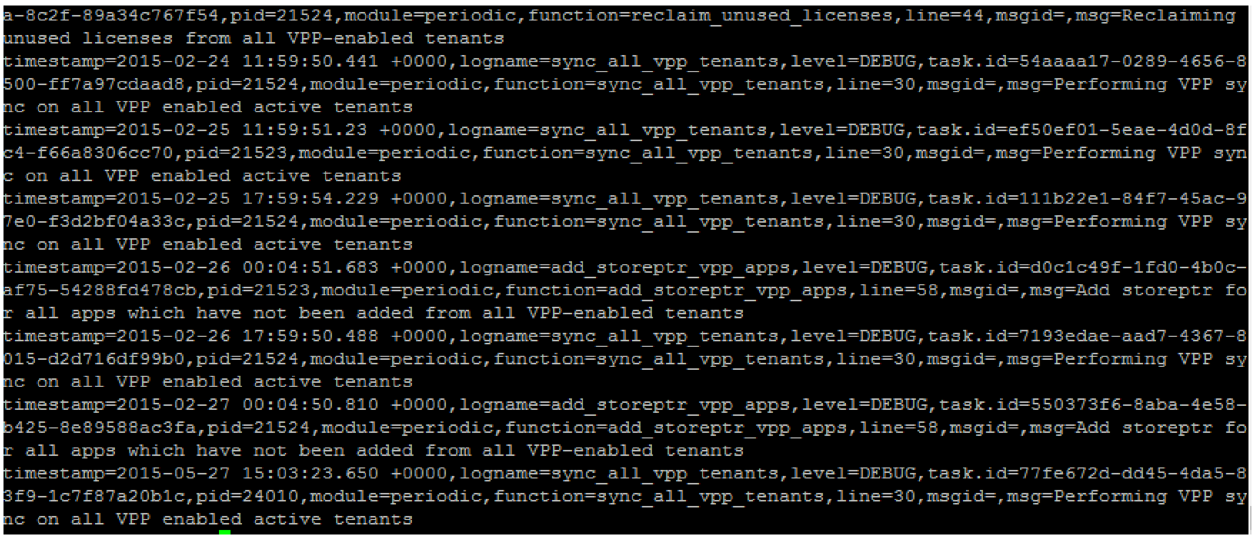
```
[2015-05-27 15:12:28,606: INFO/MainProcess] msg=Scheduler: Sending due task gateway.tasks.recalculate_auth_ca
che (gateway.tasks.recalculate_auth_cache)
[2015-05-27 15:12:28,612: INFO/MainProcess] msg=Task appstore.periodic.check_device_compliances[401895f5-f4e3
-414c-8f02-8cbca7eaaafc] succeeded in 0.0150253589964s: None
[2015-05-27 15:12:28,611: INFO/MainProcess] msg=Received task: gateway.tasks.recalculate_auth_cache[cc2c9917-
bbf4-4f60-aec9-82f7f958cd81] expires:[2015-05-27 15:13:13.607839+00:00]
[2015-05-27 15:12:28,628: INFO/MainProcess] msg=Task gateway.tasks.recalculate_auth_cache[cc2c9917-bbf4-4f60-
aec9-82f7f958cd81] succeeded in 0.0130261520026s: None
[2015-05-27 15:12:43,614: INFO/MainProcess] msg=Scheduler: Sending due task appstore.periodic.check_device_co
mpliances (appstore.periodic.check_device_compliances)
[2015-05-27 15:12:43,618: INFO/MainProcess] msg=Received task: appstore.periodic.check_device_compliances[319
e502b-2350-4fc6-a041-dcf73ab9d762] expires:[2015-05-27 15:13:28.615207+00:00]
[2015-05-27 15:12:43,629: INFO/MainProcess] msg=Scheduler: Sending due task gateway.tasks.recalculate_auth_ca
che (gateway.tasks.recalculate_auth_cache)
[2015-05-27 15:12:43,632: INFO/MainProcess] msg=Task appstore.periodic.check_device_compliances[319e502b-2350
-4fc6-a041-dcf73ab9d762] succeeded in 0.0112193519963s: None
[2015-05-27 15:12:43,635: INFO/MainProcess] msg=Received task: gateway.tasks.recalculate_auth_cache[d1c30a6c-
292a-41e0-a4a1-ddd3add36315] expires:[2015-05-27 15:13:28.631908+00:00]
[2015-05-27 15:12:43,650: INFO/MainProcess] msg=Task gateway.tasks.recalculate_auth_cache[d1c30a6c-292a-41e0-
a4a1-ddd3add36315] succeeded in 0.0122715589969s: None
```

Error:



```
  File "/usr/local/nukona/appstore_cu/apps/appstore/signals.py", line 172, in add_signals
  File "/usr/local/nukona/appstore_cu/apps/appstore/models/mobile_security/signals.py", line 24, in connect_m
obile_security_signals
  File "/usr/local/nukona/appstore_cu/apps/appstore/helpers/mobsec_client.py", line 7, in <module>
  File "/usr/local/nukona/appstore_cu/apps/appstore/celery.py", line 120, in <module>
  File "/usr/local/nukona/appstore_cu/apps/appstore/celeryconfig.py", line 137, in get_config
  File "/usr/local/nukona/appstore_cu/apps/appstore/helpers/file_cache_backends.py", line 224, in is_s3_enabl
ed
  File "/usr/local/nukona/appstore_cu/apps/appstore/helpers/file_cache.py", line 92, in __init__
  File "/usr/local/nukona/appstore_cu/apps/appstore/helpers/file_cache_backends.py", line 234, in __init__
  File "/usr/local/nukona/appstore_cu/apps/appstore/helpers/databaseblob.py", line 40, in __init__
django.db.utils.OperationalError: (2003, "Can't connect to MySQL server on 'mysql.smmglobal.net' (111)")
Failed to find setting: NUKONA_USER
```

/var/log/nukona/*tasks*.log

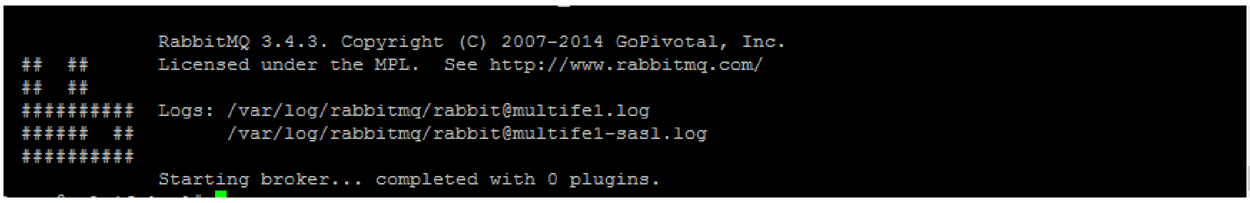


```
a-8c2f-89a34c767f54,pid=21524,module=periodic,function=reclaim_unused_licenses,line=44,msgid=,msg=Reclaiming
unused licenses from all VPP-enabled tenants
timestamp=2015-02-24 11:59:50.441 +0000,logname=sync_all_vpp_tenants,level=DEBUG,task.id=54aaaa17-0289-4656-8
500-ff7a97cdaad8,pid=21524,module=periodic,function=sync_all_vpp_tenants,line=30,msgid=,msg=Performing VPP sy
nc on all VPP enabled active tenants
timestamp=2015-02-25 11:59:51.23 +0000,logname=sync_all_vpp_tenants,level=DEBUG,task.id=ef50ef01-5eae-4d0d-8f
c4-f66a8306cc70,pid=21523,module=periodic,function=sync_all_vpp_tenants,line=30,msgid=,msg=Performing VPP syn
c on all VPP enabled active tenants
timestamp=2015-02-25 17:59:54.229 +0000,logname=sync_all_vpp_tenants,level=DEBUG,task.id=111b22e1-84f7-45ac-9
7e0-f3d2bf04a33c,pid=21524,module=periodic,function=sync_all_vpp_tenants,line=30,msgid=,msg=Performing VPP sy
nc on all VPP enabled active tenants
timestamp=2015-02-26 00:04:51.683 +0000,logname=add_storeptr_vpp_apps,level=DEBUG,task.id=d0c1c49f-1fd0-4b0c-
af75-54288fd478cb,pid=21523,module=periodic,function=add_storeptr_vpp_apps,line=58,msgid=,msg=Add storeptr fo
r all apps which have not been added from all VPP-enabled tenants
timestamp=2015-02-26 17:59:50.488 +0000,logname=sync_all_vpp_tenants,level=DEBUG,task.id=7193edae-aad7-4367-8
015-d2d716df99b0,pid=21524,module=periodic,function=sync_all_vpp_tenants,line=30,msgid=,msg=Performing VPP sy
nc on all VPP enabled active tenants
timestamp=2015-02-27 00:04:50.810 +0000,logname=add_storeptr_vpp_apps,level=DEBUG,task.id=550373f6-8aba-4e58-
b425-8e89588ac3fa,pid=21524,module=periodic,function=add_storeptr_vpp_apps,line=58,msgid=,msg=Add storeptr fo
r all apps which have not been added from all VPP-enabled tenants
timestamp=2015-05-27 15:03:23.650 +0000,logname=sync_all_vpp_tenants,level=DEBUG,task.id=77fe672d-dd45-4da5-8
3f9-1c7f87a20b1c,pid=24010,module=periodic,function=sync_all_vpp_tenants,line=30,msgid=,msg=Performing VPP sy
nc on all VPP enabled active tenants
```

RabbitMQ:

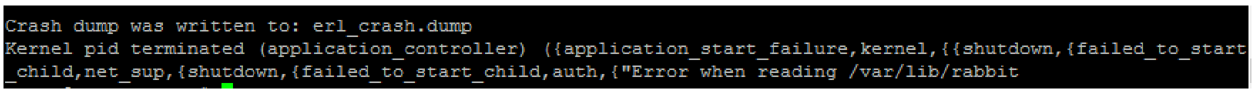
/var/log/rabbitmq

startup_log



```
            RabbitMQ 3.4.3. Copyright (C) 2007-2014 GoPivotal, Inc.
 ##  ##      Licensed under the MPL.  See http://www.rabbitmq.com/
 ##  ##
 ##########  Logs: /var/log/rabbitmq/rabbit@multife1.log
 ######  ##        /var/log/rabbitmq/rabbit@multife1-sasl.log
 ##########
            Starting broker... completed with 0 plugins.
```

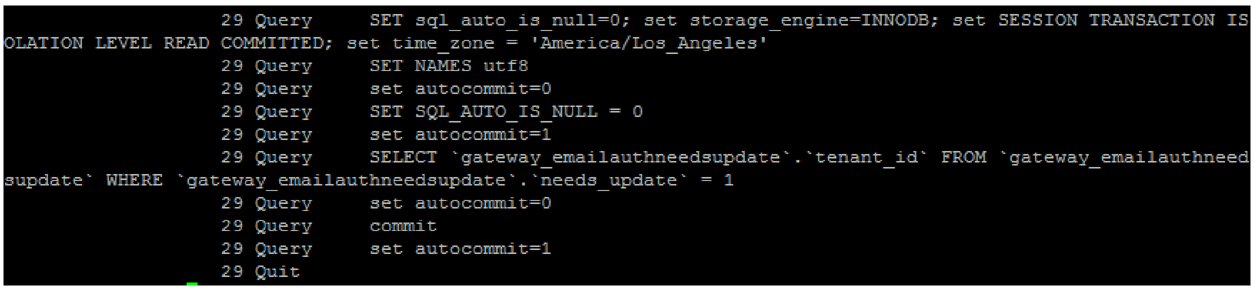
startup_err



```
Crash dump was written to: erl_crash.dump
Kernel pid terminated (application_controller) ({application_start_failure,kernel,{{shutdown,{failed_to_start
_child,net_sup,{shutdown,{failed_to_start_child,auth,{"Error when reading /var/lib/rabbit
```

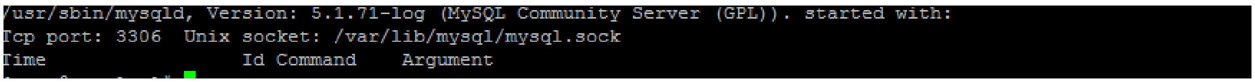
MySQL:

/var/log/mysql.log



```
                  29 Query     SET sql_auto_is_null=0; set storage_engine=INNODB; set SESSION TRANSACTION IS
OLATION LEVEL READ COMMITTED; set time_zone = 'America/Los_Angeles'
                  29 Query     SET NAMES utf8
                  29 Query     set autocommit=0
                  29 Query     SET SQL_AUTO_IS_NULL = 0
                  29 Query     set autocommit=1
                  29 Query     SELECT `gateway_emailauthneedsupdate`.`tenant_id` FROM `gateway_emailauthneed
supdate` WHERE `gateway_emailauthneedsupdate`.`needs_update` = 1
                  29 Query     set autocommit=0
                  29 Query     commit
                  29 Query     set autocommit=1
                  29 Quit
```

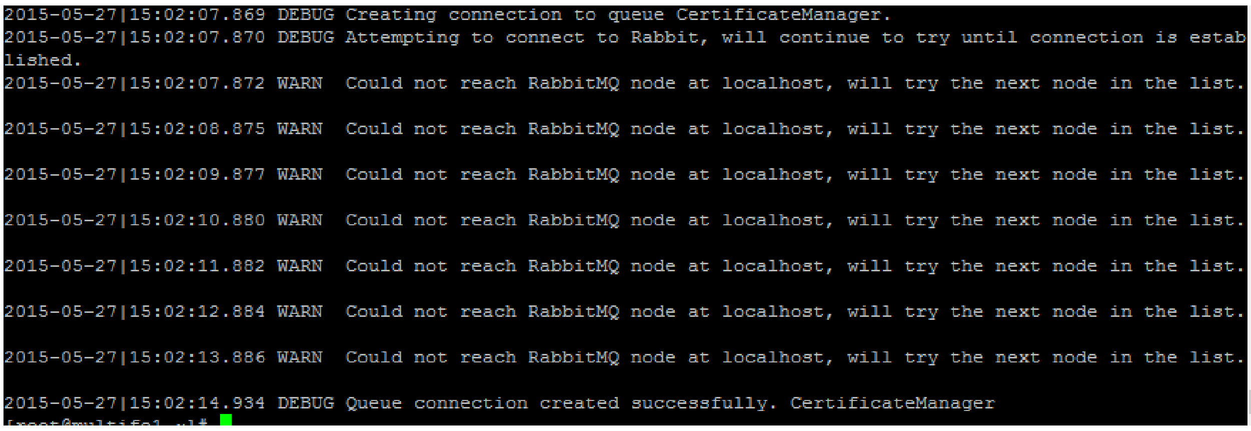
/var/log/mysql-slow.log



```
/usr/sbin/mysqld, Version: 5.1.71-log (MySQL Community Server (GPL)). started with:
Tcp port: 3306  Unix socket: /var/lib/mysql/mysql.sock
Time                 Id Command    Argument
```

MDMCore:

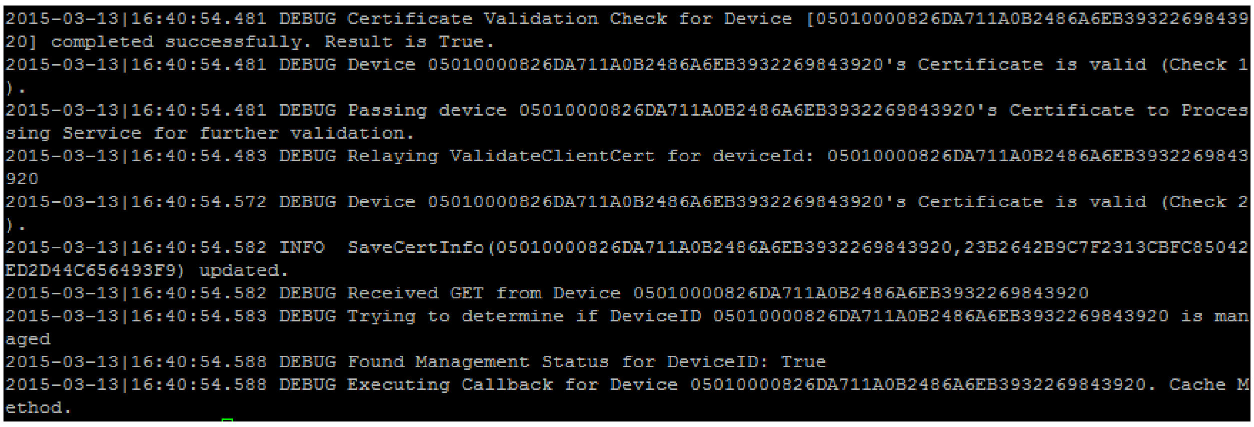
/var/log/symantec-mdm/CertificateManager.log



```
2015-05-27|15:02:07.869 DEBUG Creating connection to queue CertificateManager.
2015-05-27|15:02:07.870 DEBUG Attempting to connect to Rabbit, will continue to try until connection is estab
lished.
2015-05-27|15:02:07.872 WARN  Could not reach RabbitMQ node at localhost, will try the next node in the list.

2015-05-27|15:02:08.875 WARN  Could not reach RabbitMQ node at localhost, will try the next node in the list.

2015-05-27|15:02:09.877 WARN  Could not reach RabbitMQ node at localhost, will try the next node in the list.

2015-05-27|15:02:10.880 WARN  Could not reach RabbitMQ node at localhost, will try the next node in the list.

2015-05-27|15:02:11.882 WARN  Could not reach RabbitMQ node at localhost, will try the next node in the list.

2015-05-27|15:02:12.884 WARN  Could not reach RabbitMQ node at localhost, will try the next node in the list.

2015-05-27|15:02:13.886 WARN  Could not reach RabbitMQ node at localhost, will try the next node in the list.

2015-05-27|15:02:14.934 DEBUG Queue connection created successfully. CertificateManager
```

Error messages are shown in the above screen capture followed by a successful connection to ***RabbitMQ.***

/var/log/Symantec-mdm/Android/

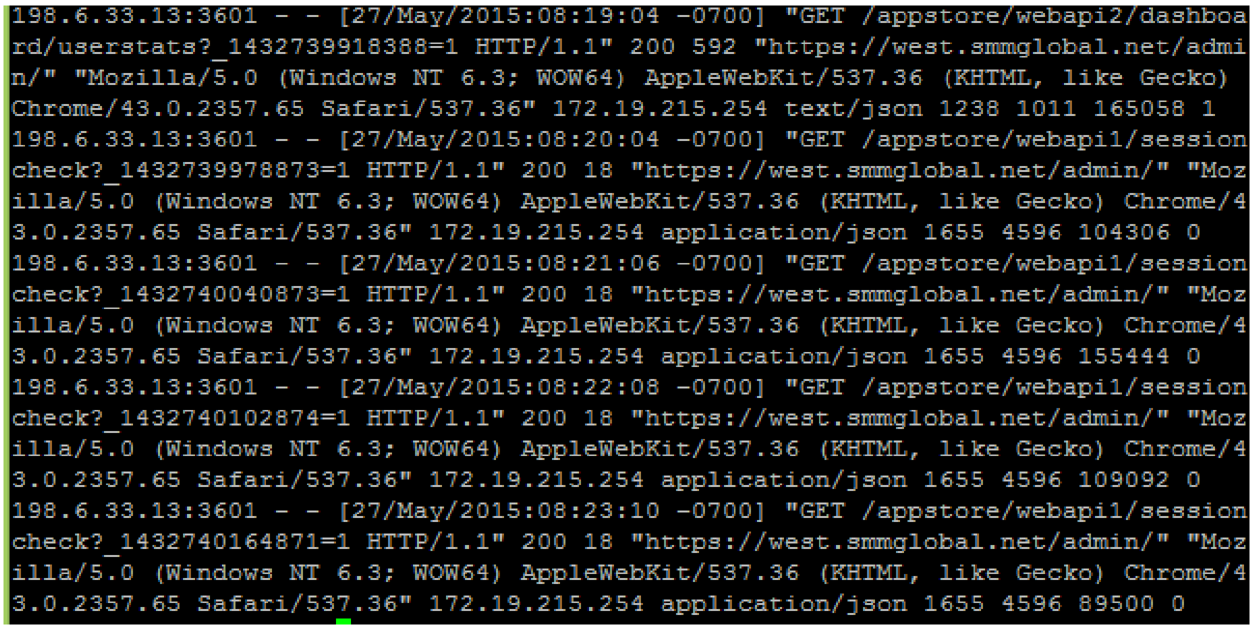


```
2015-03-13|16:40:54.481 DEBUG Certificate Validation Check for Device [05010000826DA711A0B2486A6EB39322698439
20] completed successfully. Result is True.
2015-03-13|16:40:54.481 DEBUG Device 05010000826DA711A0B2486A6EB3932269843920's Certificate is valid (Check 1
).
2015-03-13|16:40:54.481 DEBUG Passing device 05010000826DA711A0B2486A6EB3932269843920's Certificate to Proces
sing Service for further validation.
2015-03-13|16:40:54.483 DEBUG Relaying ValidateClientCert for deviceId: 05010000826DA711A0B2486A6EB3932269843
920
2015-03-13|16:40:54.572 DEBUG Device 05010000826DA711A0B2486A6EB3932269843920's Certificate is valid (Check 2
).
2015-03-13|16:40:54.582 INFO  SaveCertInfo(05010000826DA711A0B2486A6EB3932269843920,23B2642B9C7F2313CBFC85042
ED2D44C656493F9) updated.
2015-03-13|16:40:54.582 DEBUG Received GET from Device 05010000826DA711A0B2486A6EB3932269843920
2015-03-13|16:40:54.583 DEBUG Trying to determine if DeviceID 05010000826DA711A0B2486A6EB3932269843920 is man
aged
2015-03-13|16:40:54.588 DEBUG Found Management Status for DeviceID: True
2015-03-13|16:40:54.588 DEBUG Executing Callback for Device 05010000826DA711A0B2486A6EB3932269843920. Cache M
ethod.
```

Apache:

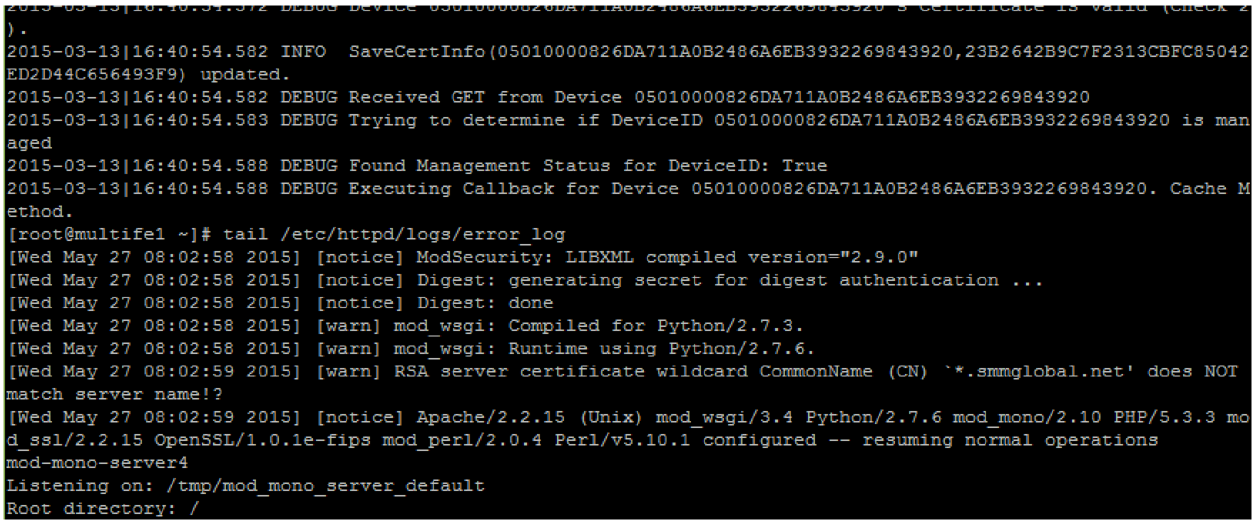
/etc/httpd/logs/

access_log



```
198.6.33.13:3601 - - [27/May/2015:08:19:04 -0700] "GET /appstore/webapi2/dashboa
rd/userstats?_1432739918388=1 HTTP/1.1" 200 592 "https://west.smmglobal.net/admi
n/" "Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/43.0.2357.65 Safari/537.36" 172.19.215.254 text/json 1238 1011 165058 1
198.6.33.13:3601 - - [27/May/2015:08:20:04 -0700] "GET /appstore/webapi1/session
check?_1432739978873=1 HTTP/1.1" 200 18 "https://west.smmglobal.net/admin/" "Moz
illa/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/4
3.0.2357.65 Safari/537.36" 172.19.215.254 application/json 1655 4596 104306 0
198.6.33.13:3601 - - [27/May/2015:08:21:06 -0700] "GET /appstore/webapi1/session
check?_1432740040873=1 HTTP/1.1" 200 18 "https://west.smmglobal.net/admin/" "Moz
illa/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/4
3.0.2357.65 Safari/537.36" 172.19.215.254 application/json 1655 4596 155444 0
198.6.33.13:3601 - - [27/May/2015:08:22:08 -0700] "GET /appstore/webapi1/session
check?_1432740102874=1 HTTP/1.1" 200 18 "https://west.smmglobal.net/admin/" "Moz
illa/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/4
3.0.2357.65 Safari/537.36" 172.19.215.254 application/json 1655 4596 109092 0
198.6.33.13:3601 - - [27/May/2015:08:23:10 -0700] "GET /appstore/webapi1/session
check?_1432740164871=1 HTTP/1.1" 200 18 "https://west.smmglobal.net/admin/" "Moz
illa/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/4
3.0.2357.65 Safari/537.36" 172.19.215.254 application/json 1655 4596 89500 0
```

error_log

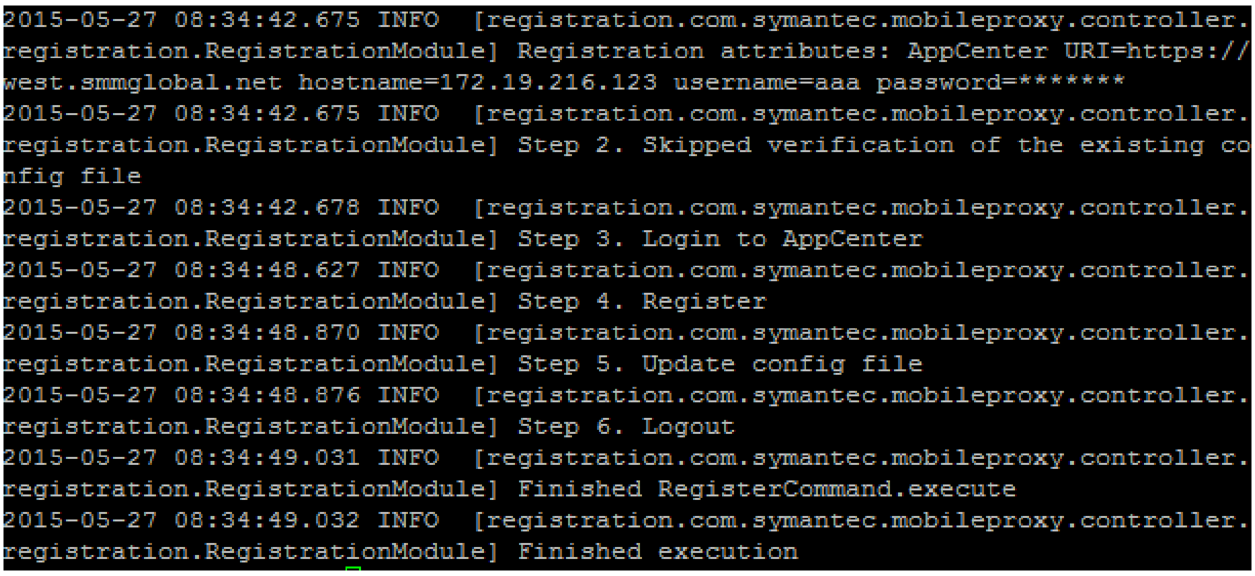


```
2015-03-13|16:40:54.572 DEBUG Device 05010000826DA711A0B2486A6EB3932269843920's Certificate is valid (check 2
).
2015-03-13|16:40:54.582 INFO  SaveCertInfo(05010000826DA711A0B2486A6EB3932269843920,23B2642B9C7F2313CBFC85042
ED2D44C656493F9) updated.
2015-03-13|16:40:54.582 DEBUG Received GET from Device 05010000826DA711A0B2486A6EB3932269843920
2015-03-13|16:40:54.583 DEBUG Trying to determine if DeviceID 05010000826DA711A0B2486A6EB3932269843920 is man
aged
2015-03-13|16:40:54.588 DEBUG Found Management Status for DeviceID: True
2015-03-13|16:40:54.588 DEBUG Executing Callback for Device 05010000826DA711A0B2486A6EB3932269843920. Cache M
ethod.
[root@multife1 ~]# tail /etc/httpd/logs/error_log
[Wed May 27 08:02:58 2015] [notice] ModSecurity: LIBXML compiled version="2.9.0"
[Wed May 27 08:02:58 2015] [notice] Digest: generating secret for digest authentication ...
[Wed May 27 08:02:58 2015] [notice] Digest: done
[Wed May 27 08:02:58 2015] [warn] mod_wsgi: Compiled for Python/2.7.3.
[Wed May 27 08:02:58 2015] [warn] mod_wsgi: Runtime using Python/2.7.6.
[Wed May 27 08:02:59 2015] [warn] RSA server certificate wildcard CommonName (CN) `*.smmglobal.net' does NOT
match server name!?
[Wed May 27 08:02:59 2015] [notice] Apache/2.2.15 (Unix) mod_wsgi/3.4 Python/2.7.6 mod_mono/2.10 PHP/5.3.3 mo
d_ssl/2.2.15 OpenSSL/1.0.1e-fips mod_perl/2.0.4 Perl/v5.10.1 configured -- resuming normal operations
mod-mono-server4
Listening on: /tmp/mod_mono_server_default
Root directory: /
```

NGINX:

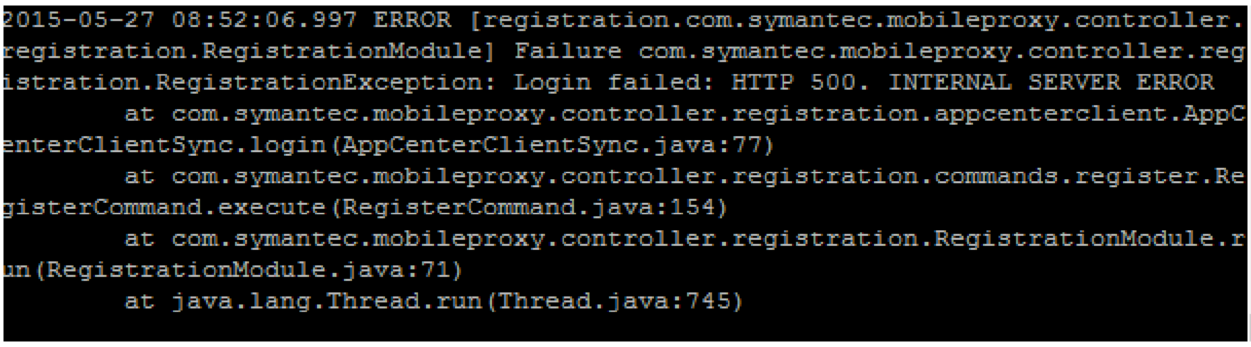
/usr/local/nginx/logs

registration.log



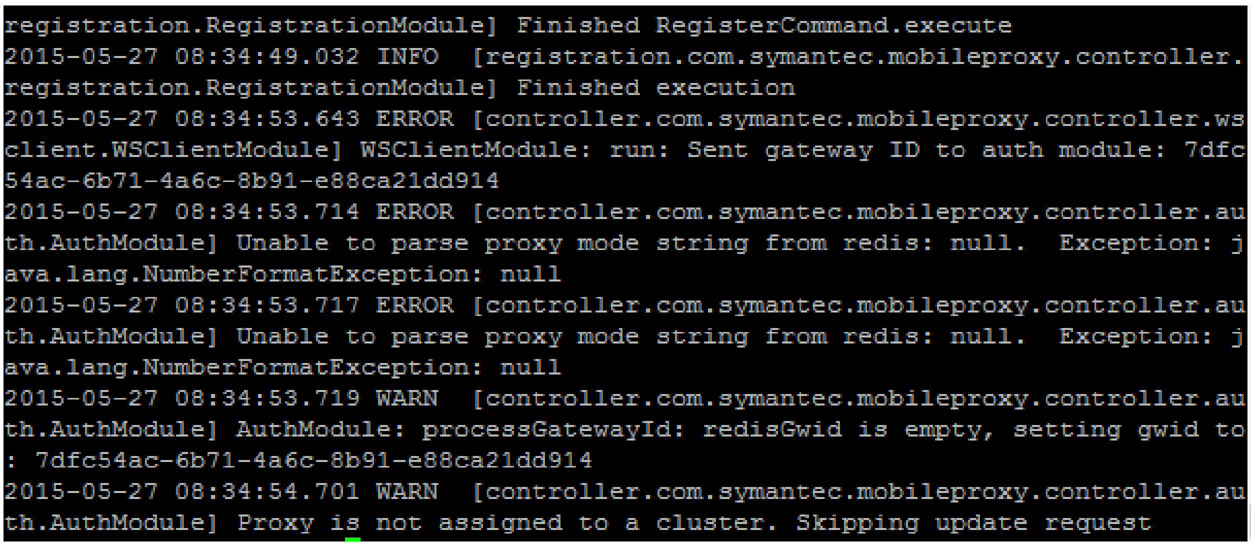
```
2015-05-27 08:34:42.675 INFO  [registration.com.symantec.mobileproxy.controller.
registration.RegistrationModule] Registration attributes: AppCenter URI=https://
west.smmglobal.net hostname=172.19.216.123 username=aaa password=*******
2015-05-27 08:34:42.675 INFO  [registration.com.symantec.mobileproxy.controller.
registration.RegistrationModule] Step 2. Skipped verification of the existing co
nfig file
2015-05-27 08:34:42.678 INFO  [registration.com.symantec.mobileproxy.controller.
registration.RegistrationModule] Step 3. Login to AppCenter
2015-05-27 08:34:48.627 INFO  [registration.com.symantec.mobileproxy.controller.
registration.RegistrationModule] Step 4. Register
2015-05-27 08:34:48.870 INFO  [registration.com.symantec.mobileproxy.controller.
registration.RegistrationModule] Step 5. Update config file
2015-05-27 08:34:48.876 INFO  [registration.com.symantec.mobileproxy.controller.
registration.RegistrationModule] Step 6. Logout
2015-05-27 08:34:49.031 INFO  [registration.com.symantec.mobileproxy.controller.
registration.RegistrationModule] Finished RegisterCommand.execute
2015-05-27 08:34:49.032 INFO  [registration.com.symantec.mobileproxy.controller.
registration.RegistrationModule] Finished execution
```

Error:



```
2015-05-27 08:52:06.997 ERROR [registration.com.symantec.mobileproxy.controller.
registration.RegistrationModule] Failure com.symantec.mobileproxy.controller.reg
istration.RegistrationException: Login failed: HTTP 500. INTERNAL SERVER ERROR
        at com.symantec.mobileproxy.controller.registration.appcenterclient.AppC
enterClientSync.login(AppCenterClientSync.java:77)
        at com.symantec.mobileproxy.controller.registration.commands.register.Re
gisterCommand.execute(RegisterCommand.java:154)
        at com.symantec.mobileproxy.controller.registration.RegistrationModule.r
un(RegistrationModule.java:71)
        at java.lang.Thread.run(Thread.java:745)
```

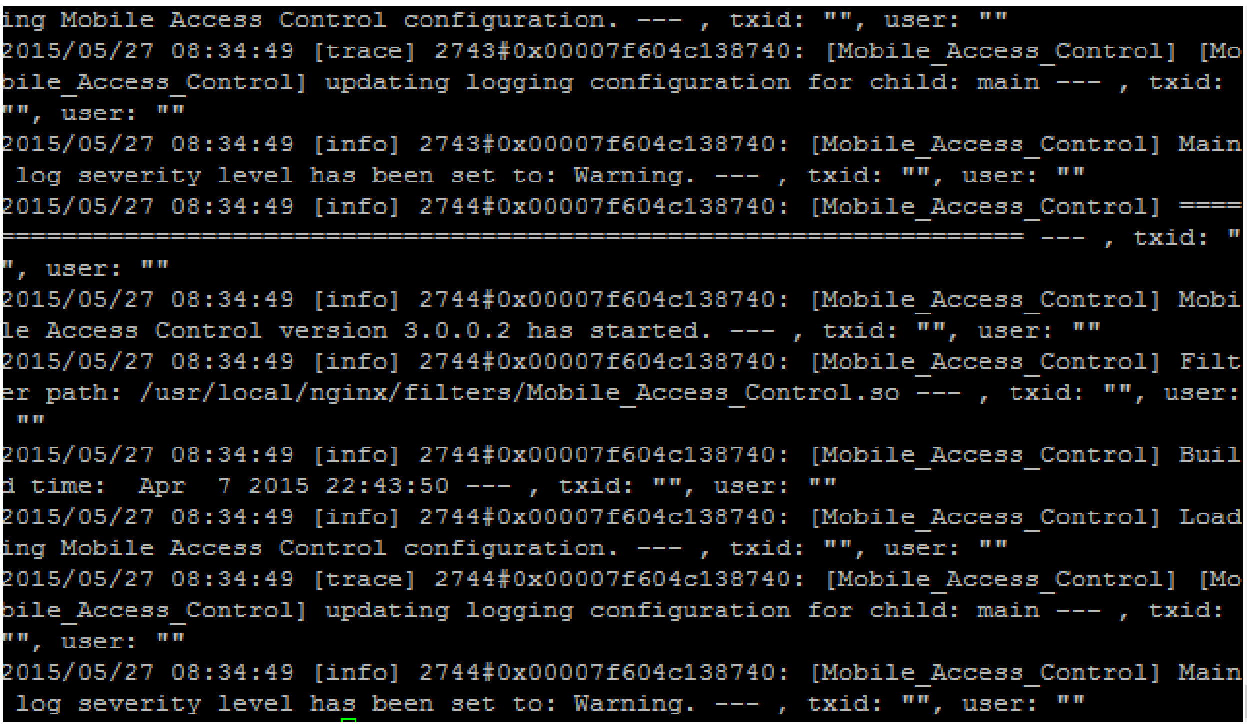
controller.log



```
registration.RegistrationModule] Finished RegisterCommand.execute
2015-05-27 08:34:49.032 INFO  [registration.com.symantec.mobileproxy.controller.
registration.RegistrationModule] Finished execution
2015-05-27 08:34:53.643 ERROR [controller.com.symantec.mobileproxy.controller.ws
client.WSClientModule] WSClientModule: run: Sent gateway ID to auth module: 7dfc
54ac-6b71-4a6c-8b91-e88ca21dd914
2015-05-27 08:34:53.714 ERROR [controller.com.symantec.mobileproxy.controller.au
th.AuthModule] Unable to parse proxy mode string from redis: null.  Exception: j
ava.lang.NumberFormatException: null
2015-05-27 08:34:53.717 ERROR [controller.com.symantec.mobileproxy.controller.au
th.AuthModule] Unable to parse proxy mode string from redis: null.  Exception: j
ava.lang.NumberFormatException: null
2015-05-27 08:34:53.719 WARN  [controller.com.symantec.mobileproxy.controller.au
th.AuthModule] AuthModule: processGatewayId: redisGwid is empty, setting gwid to
: 7dfc54ac-6b71-4a6c-8b91-e88ca21dd914
2015-05-27 08:34:54.701 WARN  [controller.com.symantec.mobileproxy.controller.au
th.AuthModule] Proxy is not assigned to a cluster. Skipping update request
```

Error messages are shown above.

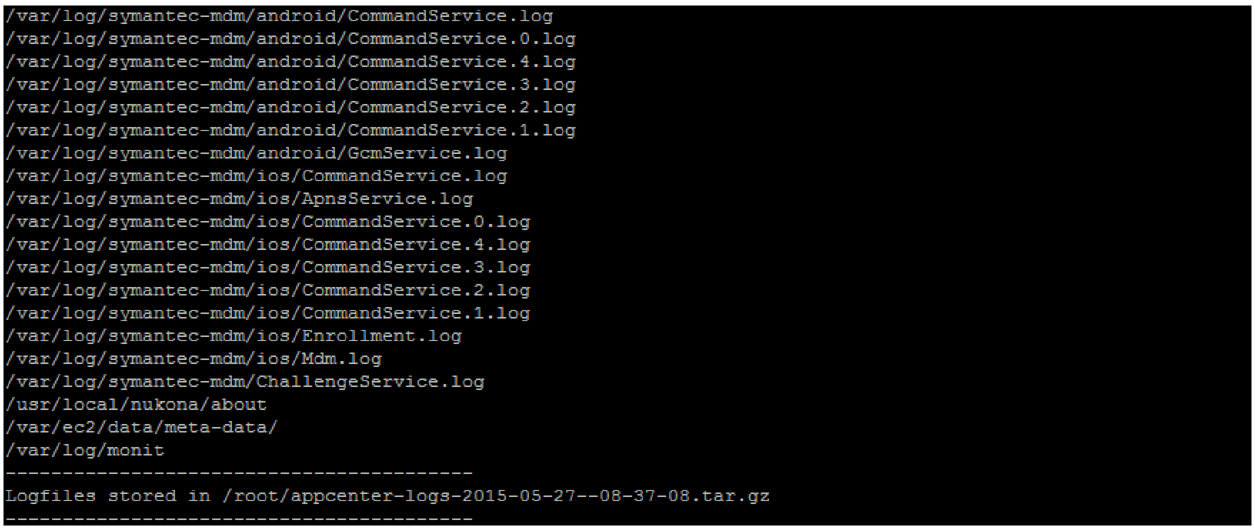
error.log



```
ing Mobile Access Control configuration. --- , txid: "", user: ""
2015/05/27 08:34:49 [trace] 2743#0x00007f604c138740: [Mobile_Access_Control] [Mo
bile_Access_Control] updating logging configuration for child: main --- , txid:
"", user: ""
2015/05/27 08:34:49 [info] 2743#0x00007f604c138740: [Mobile_Access_Control] Main
 log severity level has been set to: Warning. --- , txid: "", user: ""
2015/05/27 08:34:49 [info] 2744#0x00007f604c138740: [Mobile_Access_Control] ====
================================================================ --- , txid: "
", user: ""
2015/05/27 08:34:49 [info] 2744#0x00007f604c138740: [Mobile_Access_Control] Mobi
le Access Control version 3.0.0.2 has started. --- , txid: "", user: ""
2015/05/27 08:34:49 [info] 2744#0x00007f604c138740: [Mobile_Access_Control] Filt
er path: /usr/local/nginx/filters/Mobile_Access_Control.so --- , txid: "", user:
 ""
2015/05/27 08:34:49 [info] 2744#0x00007f604c138740: [Mobile_Access_Control] Buil
d time:  Apr  7 2015 22:43:50 --- , txid: "", user: ""
2015/05/27 08:34:49 [info] 2744#0x00007f604c138740: [Mobile_Access_Control] Load
ing Mobile Access Control configuration. --- , txid: "", user: ""
2015/05/27 08:34:49 [trace] 2744#0x00007f604c138740: [Mobile_Access_Control] [Mo
bile_Access_Control] updating logging configuration for child: main --- , txid:
"", user: ""
2015/05/27 08:34:49 [info] 2744#0x00007f604c138740: [Mobile_Access_Control] Main
 log severity level has been set to: Warning. --- , txid: "", user: ""
```

Gather logs script:

/usr/local/nukona/bin/gather_logs.sh

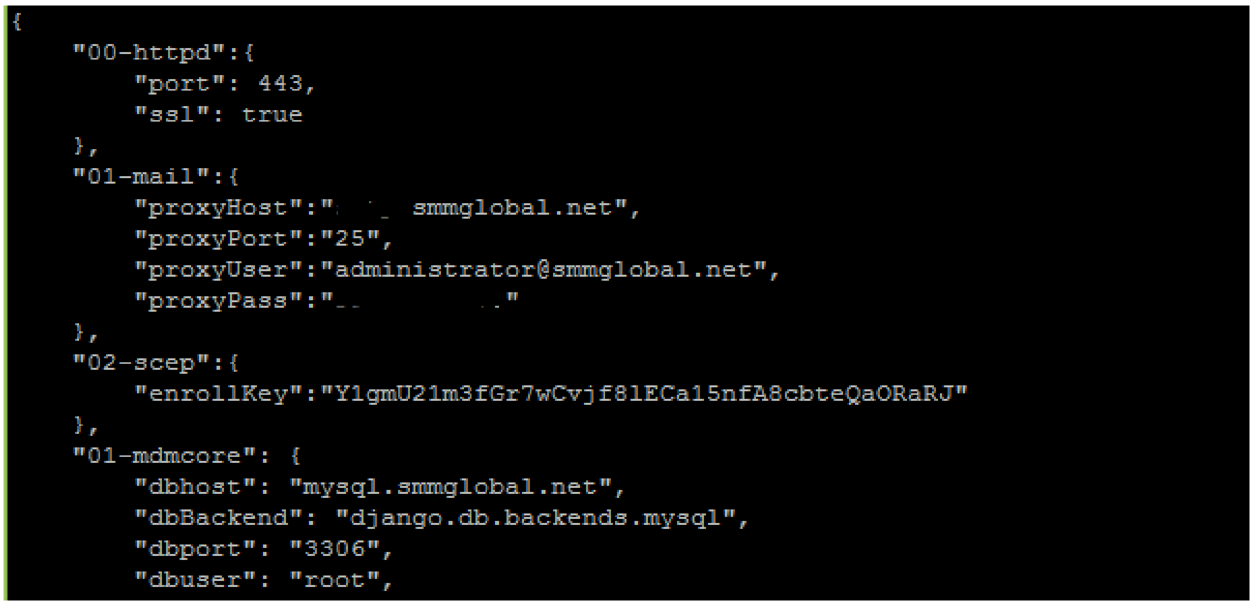


```
/var/log/symantec-mdm/android/CommandService.log
/var/log/symantec-mdm/android/CommandService.0.log
/var/log/symantec-mdm/android/CommandService.4.log
/var/log/symantec-mdm/android/CommandService.3.log
/var/log/symantec-mdm/android/CommandService.2.log
/var/log/symantec-mdm/android/CommandService.1.log
/var/log/symantec-mdm/android/GcmService.log
/var/log/symantec-mdm/ios/CommandService.log
/var/log/symantec-mdm/ios/ApnsService.log
/var/log/symantec-mdm/ios/CommandService.0.log
/var/log/symantec-mdm/ios/CommandService.4.log
/var/log/symantec-mdm/ios/CommandService.3.log
/var/log/symantec-mdm/ios/CommandService.2.log
/var/log/symantec-mdm/ios/CommandService.1.log
/var/log/symantec-mdm/ios/Enrollment.log
/var/log/symantec-mdm/ios/Mdm.log
/var/log/symantec-mdm/ChallengeService.log
/usr/local/nukona/about
/var/ec2/data/meta-data/
/var/log/monit
-----------------------------------------
Logfiles stored in /root/appcenter-logs-2015-05-27--08-37-08.tar.gz
-----------------------------------------
```

Note: The gather logs script does not take into account custom directories.

Configuration:

/usr/local/nukona/etc/settings.cfg



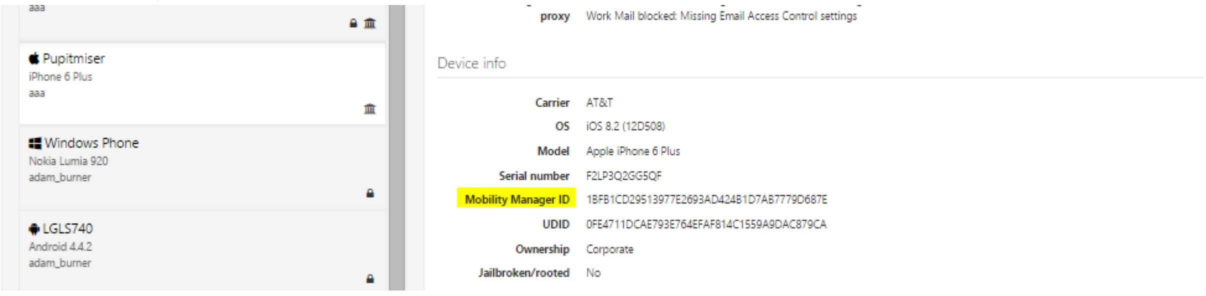
```
{
    "00-httpd":{
        "port": 443,
        "ssl": true
    },
    "01-mail":{
        "proxyHost":"[redacted]smmglobal.net",
        "proxyPort":"25",
        "proxyUser":"administrator@smmglobal.net",
        "proxyPass":"[redacted]"
    },
    "02-scep":{
        "enrollKey":"Y1gmU21m3fGr7wCvjf81ECa15nfA8cbteQaORaRJ"
    },
    "01-mdmcore": {
        "dbhost": "mysql.smmglobal.net",
        "dbBackend": "django.db.backends.mysql",
        "dbport": "3306",
        "dbuser": "root",
```

Tools:

- less
- tail

Searchable terms examples:

Mobility Manager ID



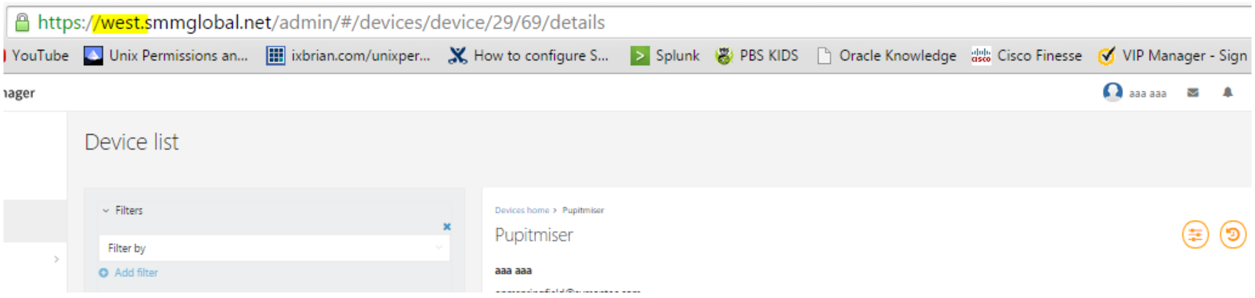
proxy Work Mail blocked: Missing Email Access Control settings

Device info

Carrier AT&T
OS iOS 8.2 (12D508)
Model Apple iPhone 6 Plus
Serial number F2LP3Q2GG5QF
Mobility Manager ID 1BFB1CD29513977E2693AD424B1D7AB7779D687E
UDID 0FE4711DCAE793E764EFAF814C1559A9DAC879CA
Ownership Corporate
Jailbroken/rooted No

Tenant name

grep -i ‘tenant=west’ /var/log/nukona/appstore.log|less



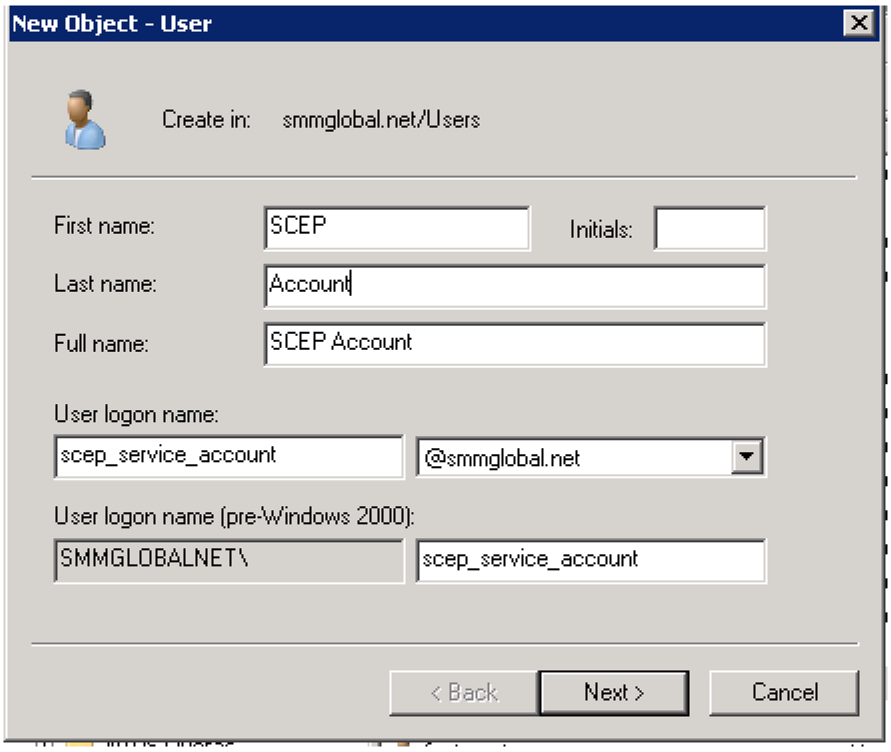
https://west.smmglobal.net/admin/#/devices/device/29/69/details

How to setup MSCA with Symantec Mobility | iOS

Deploy a MSCA (Microsoft Certificate Authority) Server:

Before you begin: The 'Enterprise Windows Server 2008 R2 machine' must be a member of an Active Directory domain. A production off-box RabbitMQ server is required. To deploy a HA (High Availability) RabbitMQ server see HOWTO110356. This document assumes that the admin has already created an MDM, Code-signing, Provisioning profile and APNS certificates. See the Mobility A to Z document and relevant sections for step-by-step instructions on creating these certificates prior to continuing with this article.

1. From AD create a new user:



New Object - User

Create in: smmglobal.net/Users

First name: SCEP

Initials:

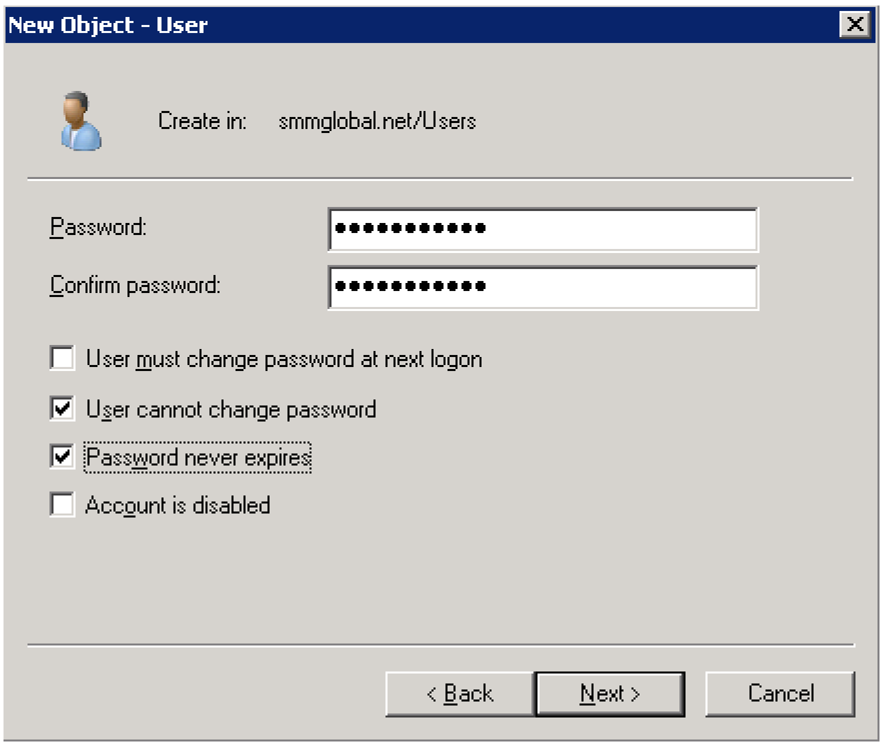
Last name: Account

Full name: SCEP Account

User logon name: scep_service_account @smmglobal.net

User logon name (pre-Windows 2000): SMMGLOBALNET\ scep_service_account

2. Set a static password for this user account as the NDES (Network Device Enrollment Service) will use this account to enroll users:



New Object - User

Create in: smmglobal.net/Users

Password: ●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●

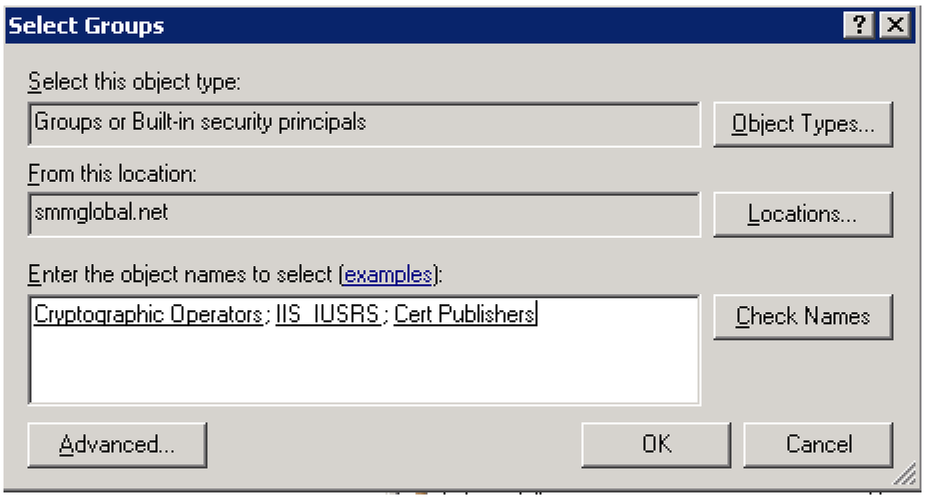
□ User must change password at next logon

☑ User cannot change password

☑ Password never expires

□ Account is disabled

3. Click **Next** and **Finish**.
4. Add the user to the Cryptographic_Operators, Cert Publishers and IIS_USERS groups; by right-clicking on the user and selecting **Add to group**:



Select Groups

Select this object type:
Groups or Built-in security principals

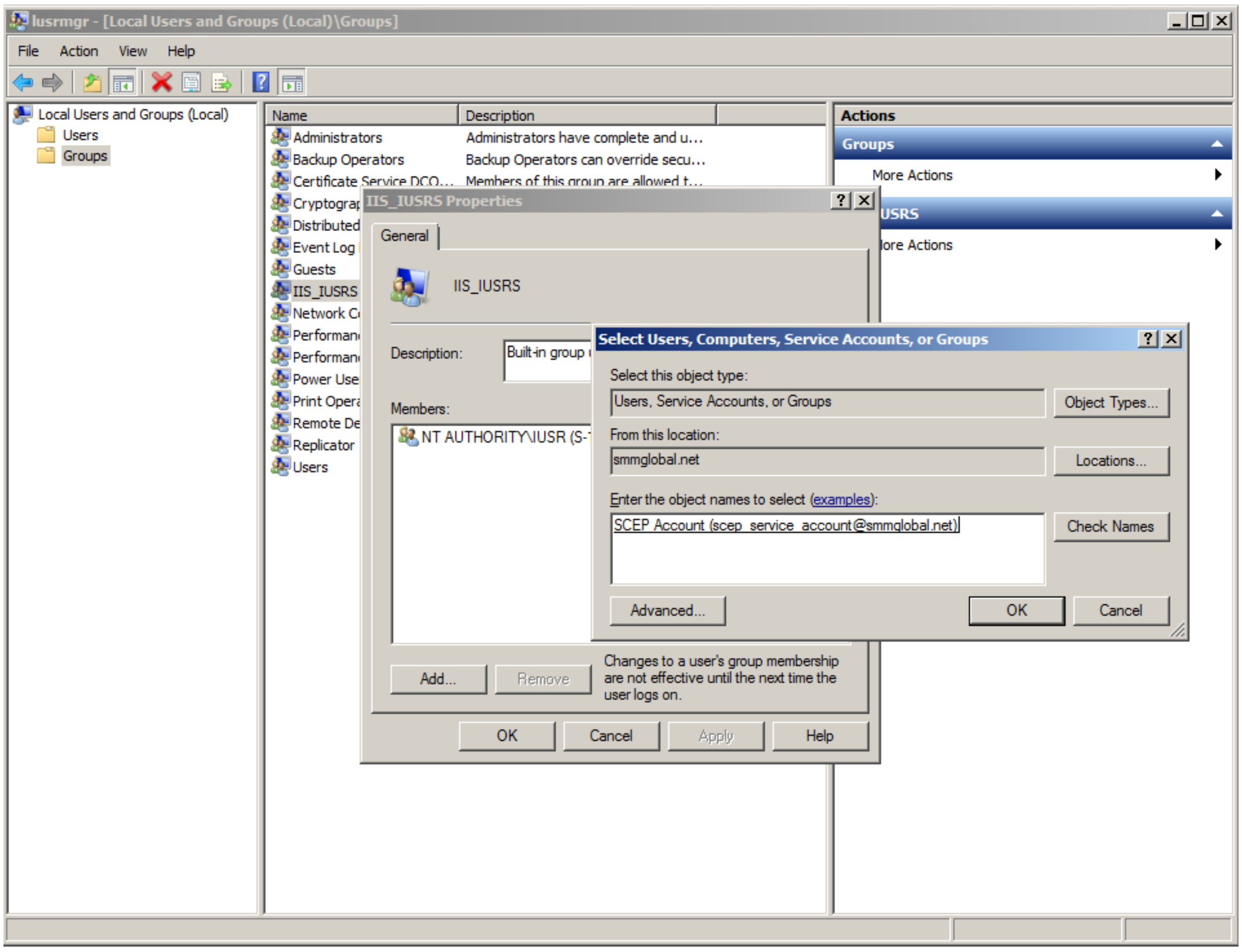
From this location:
smmglobal.net

Enter the object names to select (examples):
Cryptographic Operators; IIS_IUSRS; Cert Publishers

5. Log into the future MSCA server as a **Domain Administrator**.
6. From **Start > Run** enter:
   lusrmgr.msc

Adding a user to the machine's local IIS_USERS group

7. From the User Manager Console, add the SCEP user to that machine's local **IIS_USERS** group:



lusrmgr - [Local Users and Groups (Local)\Groups]

Name	Description
Administrators	Administrators have complete and u...
Backup Operators	Backup Operators can override secu...
Certificate Service DCO...	Members of this group are allowed t...
Cryptograp	
Distributed	
Event Log	
Guests	
IIS_IUSRS	
Network C	
Performan	
Performan	
Power Use	
Print Opera	
Remote De	
Replicator	
Users	

IIS_IUSRS Properties

IIS_IUSRS

Description: Built-in group

Members:
NT AUTHORITY\IUSR (S-

Changes to a user's group membership are not effective until the next time the user logs on.

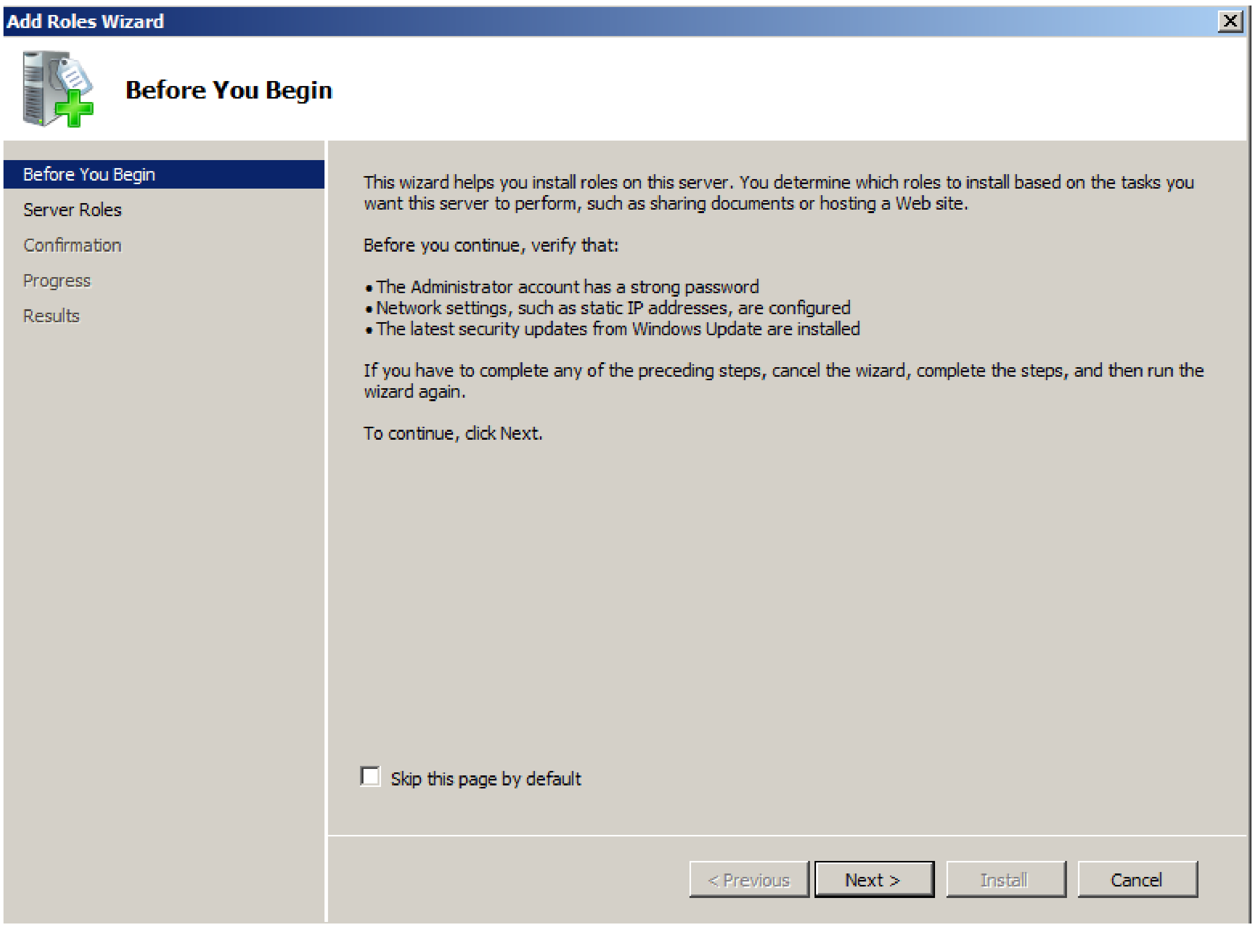
Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users, Service Accounts, or Groups

From this location:
smmglobal.net

Enter the object names to select (examples):
SCEP Account (scep_service_account@smmglobal.net)

8. Click **OK** to apply the settings.
9. Open the **Server Management Console** from **Start > Run** by entering:
   servermanager.msc
10. Under Server Manager right-click on **Roles** and select **Add Roles:**



This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

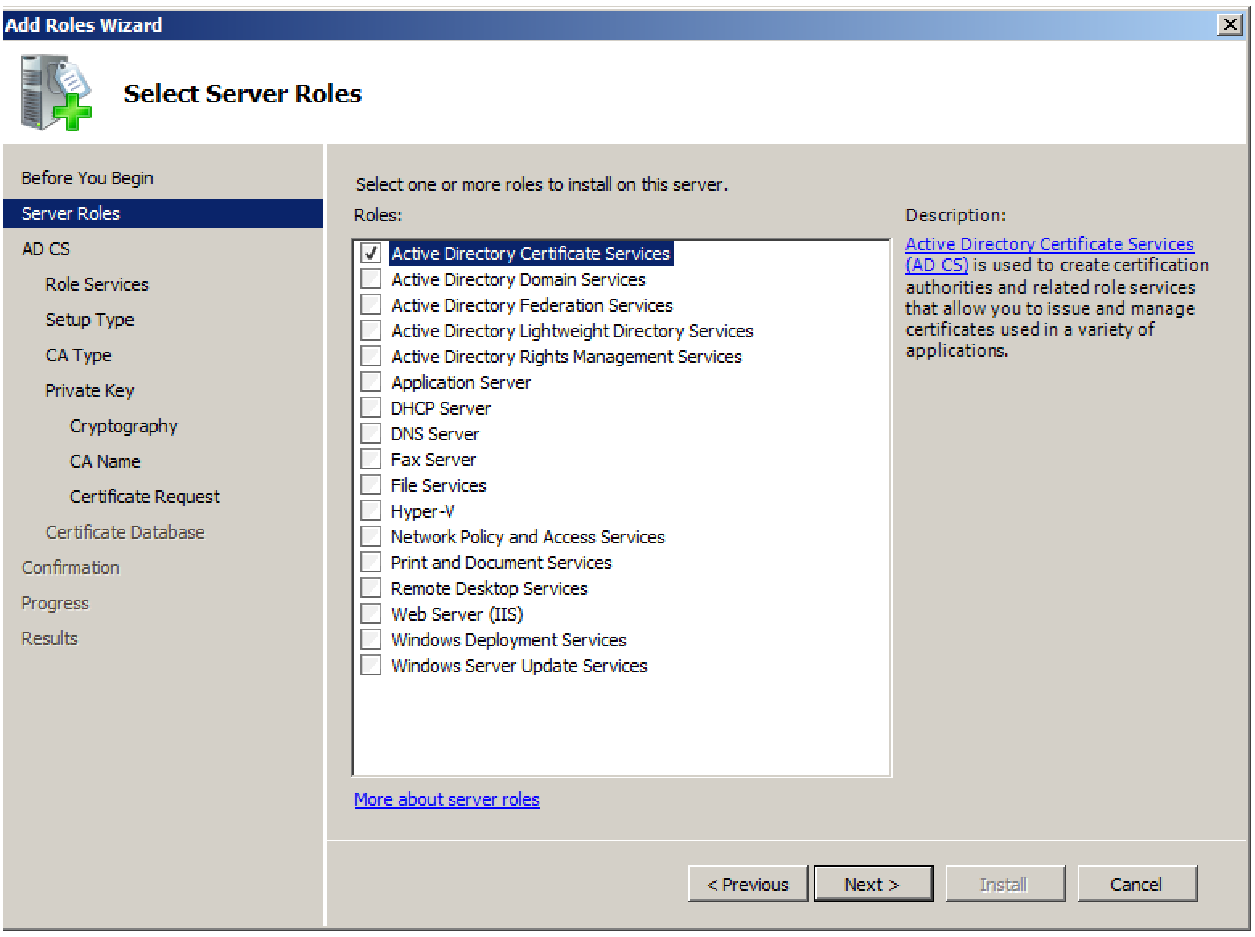
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

11. Click **Next**, from the next window check **Active Directory Certificate Services** and **Next** to continue.



Select one or more roles to install on this server.

Roles:

☑ Active Directory Certificate Services
□ Active Directory Domain Services
□ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Application Server
□ DHCP Server
□ DNS Server
□ Fax Server
□ File Services
□ Hyper-V
□ Network Policy and Access Services
□ Print and Document Services
□ Remote Desktop Services
□ Web Server (IIS)
□ Windows Deployment Services
□ Windows Server Update Services

Description:

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

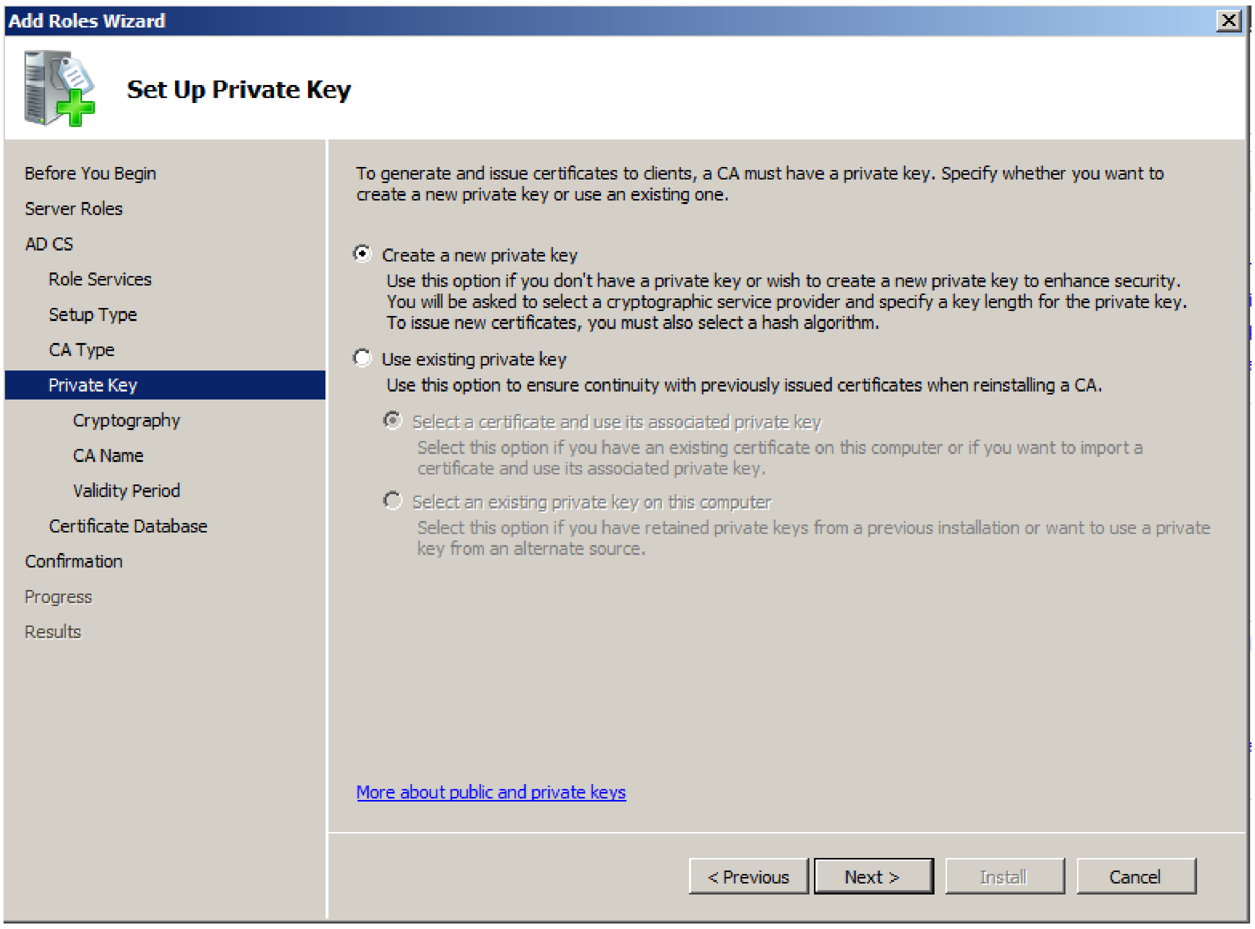
12. **Next** through the Introduction page and on the Select Role Services page ensure that only **Certificate Authority** is checked and **Next**.
13. Select **Enterprise** and **Next** to continue.

Note: If the enterprise option is greyed out, this machine is either not a member of the domain, the user account is a local account or this is not an Enterprise version of Windows 2008 R2.

14. The CA type is important, if there is an existing MSCA in the environment, it is recommended to set this up as a Subordinate CA. If there is no CA in the environment the Root CA option is acceptable. Follow below whether Root or Subordinate is selected.

Root CA Option:

15. Select **Root CA** and **Next.** From the Private Key section select **Create a new private key** and **Next** to continue:



Add Roles Wizard

Set Up Private Key

To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.

● Create a new private key

Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key. To issue new certificates, you must also select a hash algorithm.

○ Use existing private key

Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

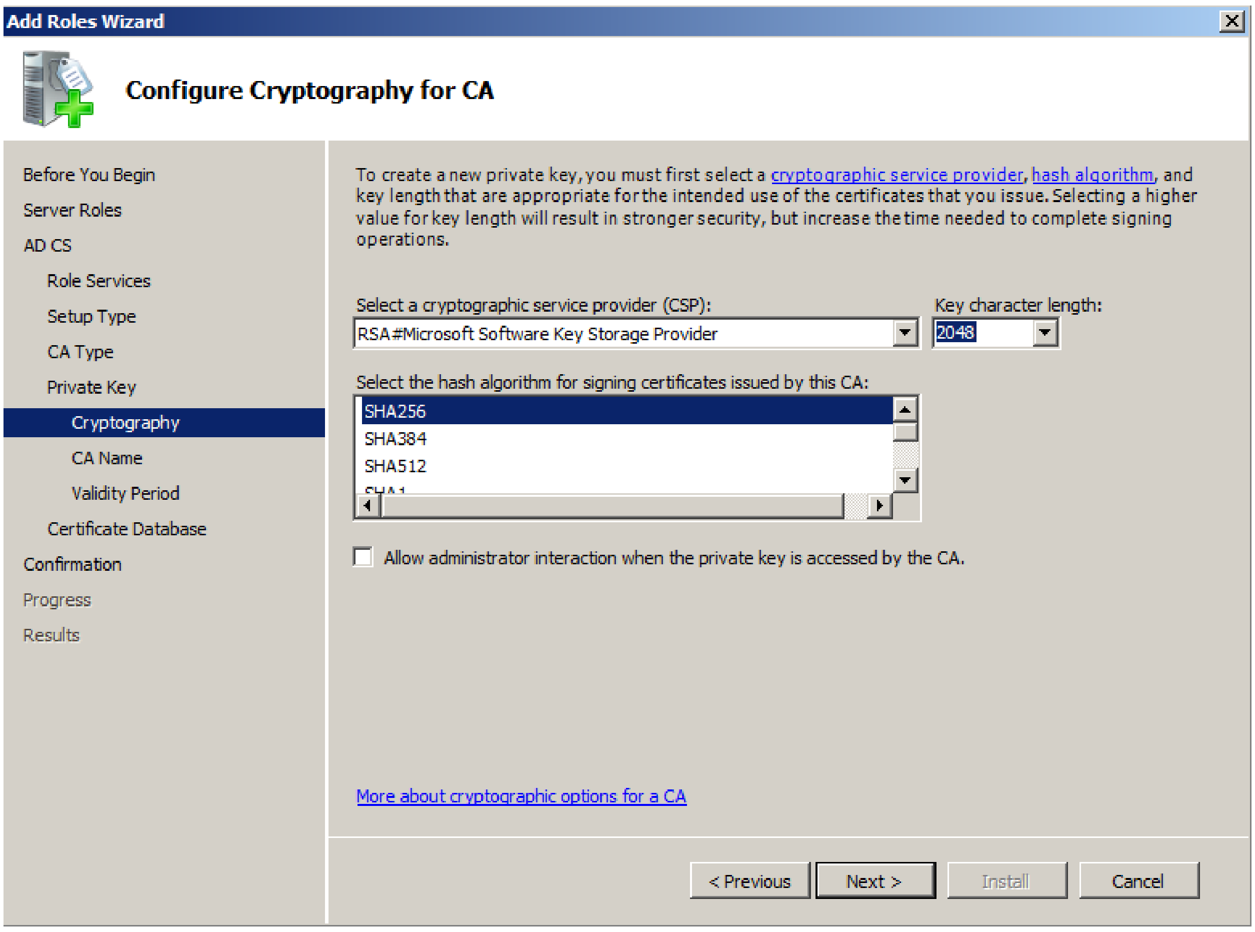
● Select a certificate and use its associated private key

Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer

Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

16. Select **SHA256** for the key's signing algorithm and **2048** or **4092** for the character length.



Add Roles Wizard

Configure Cryptography for CA

To create a new private key, you must first select a cryptographic service provider, hash algorithm, and key length that are appropriate for the intended use of the certificates that you issue. Selecting a higher value for key length will result in stronger security, but increase the time needed to complete signing operations.

Select a cryptographic service provider (CSP): RSA#Microsoft Software Key Storage Provider

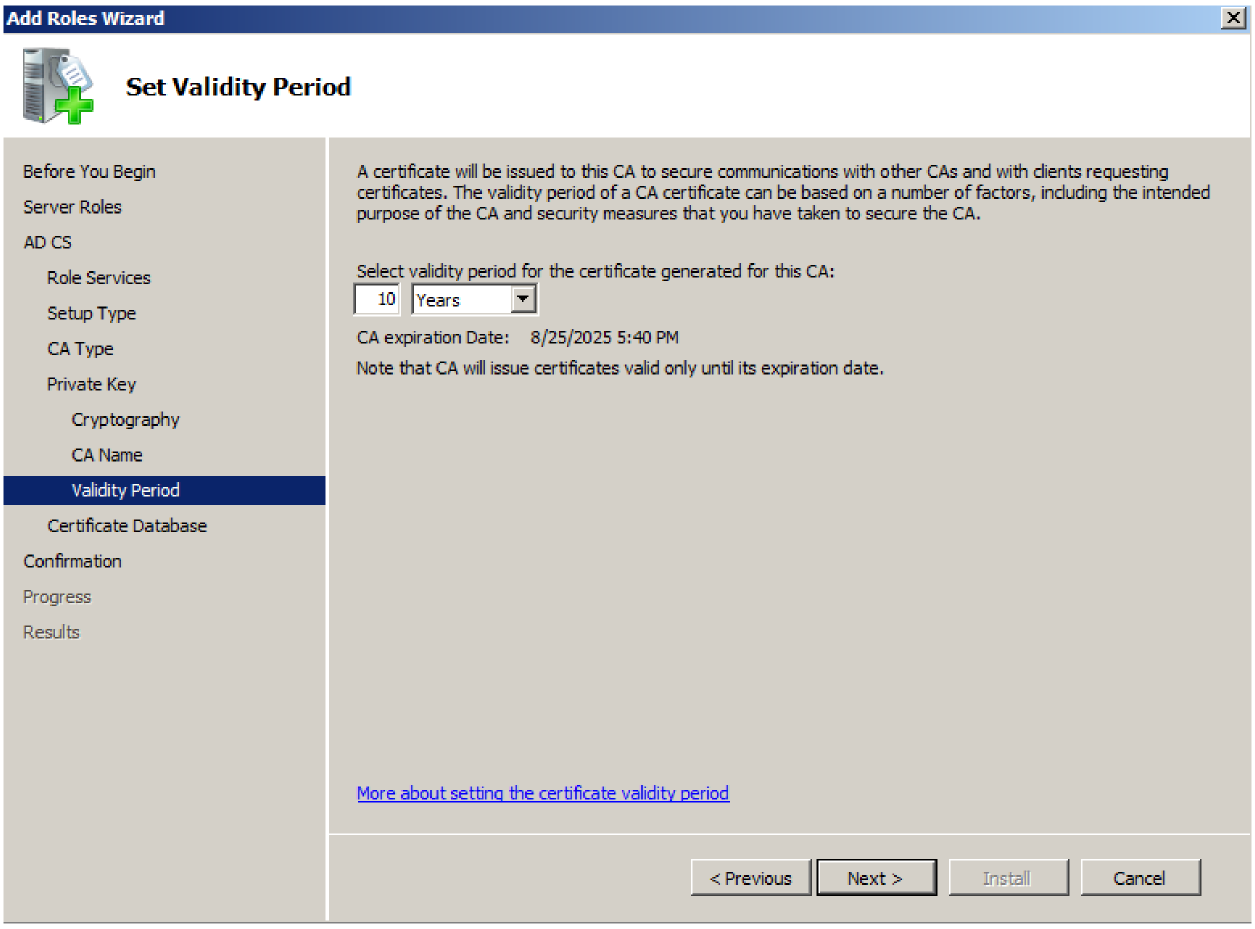
Key character length: 2048

Select the hash algorithm for signing certificates issued by this CA: SHA256

□ Allow administrator interaction when the private key is accessed by the CA.

Note: iOS does not validate CA/RA certificates which are greater than 4096.

17. Accept the default common name and DN for the CA and **Next**.
18. Set the validity period to **10 years** and **Next**:



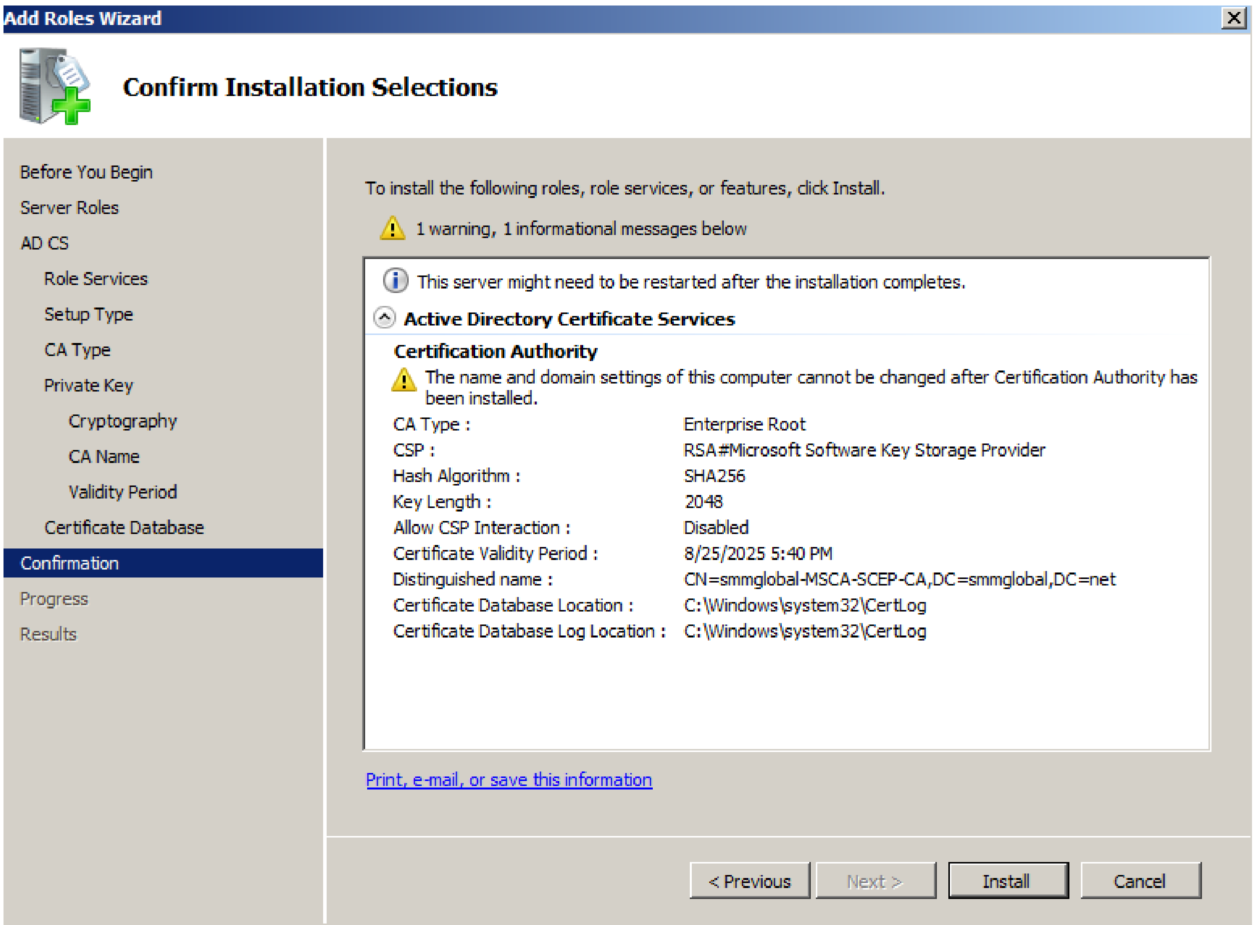
A certificate will be issued to this CA to secure communications with other CAs and with clients requesting certificates. The validity period of a CA certificate can be based on a number of factors, including the intended purpose of the CA and security measures that you have taken to secure the CA.

Select validity period for the certificate generated for this CA:
10 Years

CA expiration Date: 8/25/2025 5:40 PM

Note that CA will issue certificates valid only until its expiration date.

19. Accept the default database locations and **Next**.
20. Review the configurations and click **Install**:



To install the following roles, role services, or features, click Install.

⚠ 1 warning, 1 informational messages below

ⓘ This server might need to be restarted after the installation completes.

Active Directory Certificate Services

Certification Authority

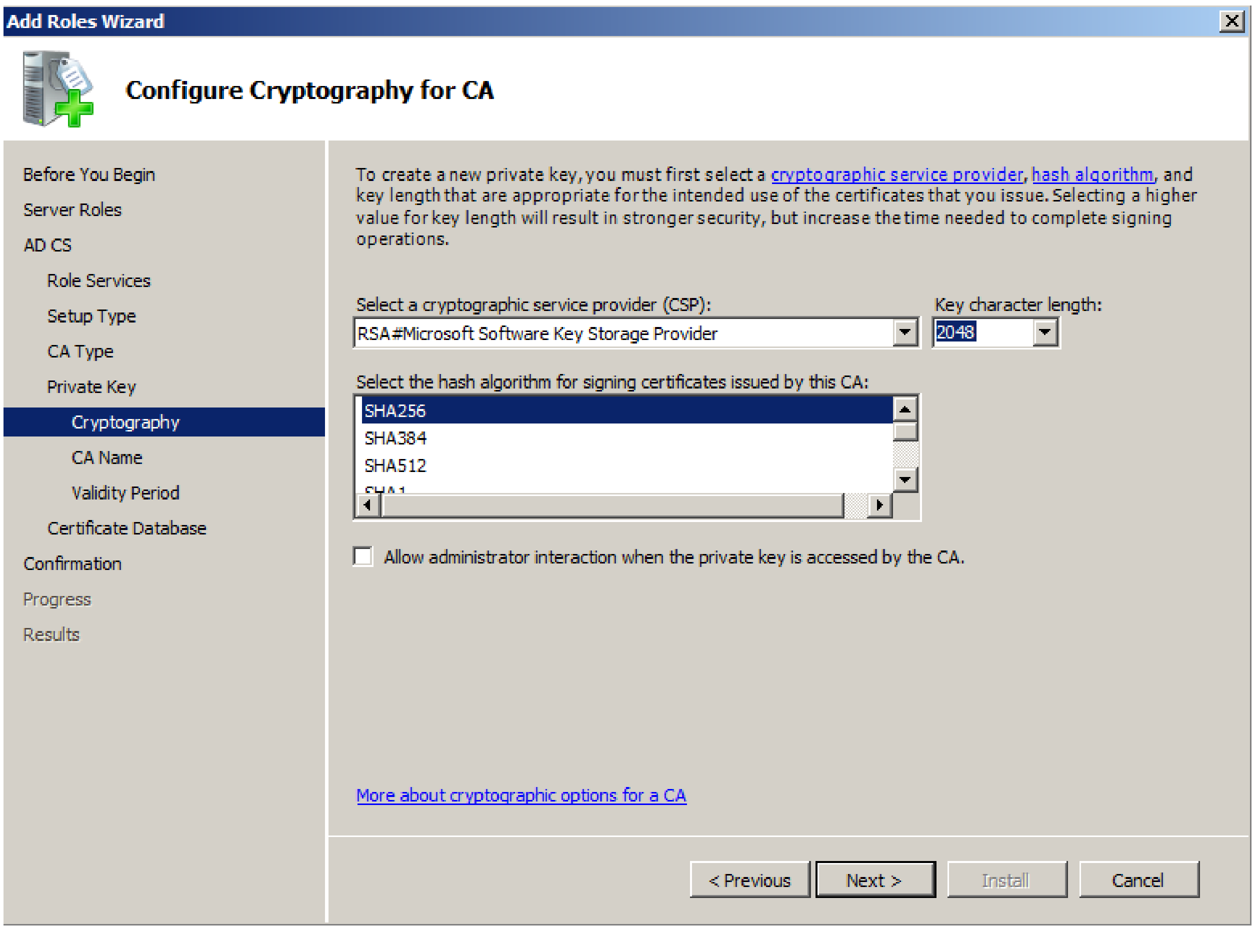
⚠ The name and domain settings of this computer cannot be changed after Certification Authority has been installed.

```
CA Type :                          Enterprise Root
CSP :                              RSA#Microsoft Software Key Storage Provider
Hash Algorithm :                   SHA256
Key Length :                       2048
Allow CSP Interaction :            Disabled
Certificate Validity Period :      8/25/2025 5:40 PM
Distinguished name :               CN=smmglobal-MSCA-SCEP-CA,DC=smmglobal,DC=net
Certificate Database Location :    C:\Windows\system32\CertLog
Certificate Database Log Location : C:\Windows\system32\CertLog
```

Note: The service role usually takes about 10 minutes to install. Skip the below **Subordinate CA Option** and continue to Install the DNES service role.

Subordinate CA Option

21. Select **Subordinate CA** and **Next**.
22. Ensure that **Create a new private key** is selected and **Next**.
23. Select **SHA256** for the key's signing algorithm and **2048** or **4092** for the character length.



Add Roles Wizard

Configure Cryptography for CA

To create a new private key, you must first select a cryptographic service provider, hash algorithm, and key length that are appropriate for the intended use of the certificates that you issue. Selecting a higher value for key length will result in stronger security, but increase the time needed to complete signing operations.

Select a cryptographic service provider (CSP): RSA#Microsoft Software Key Storage Provider

Key character length: 2048

Select the hash algorithm for signing certificates issued by this CA:

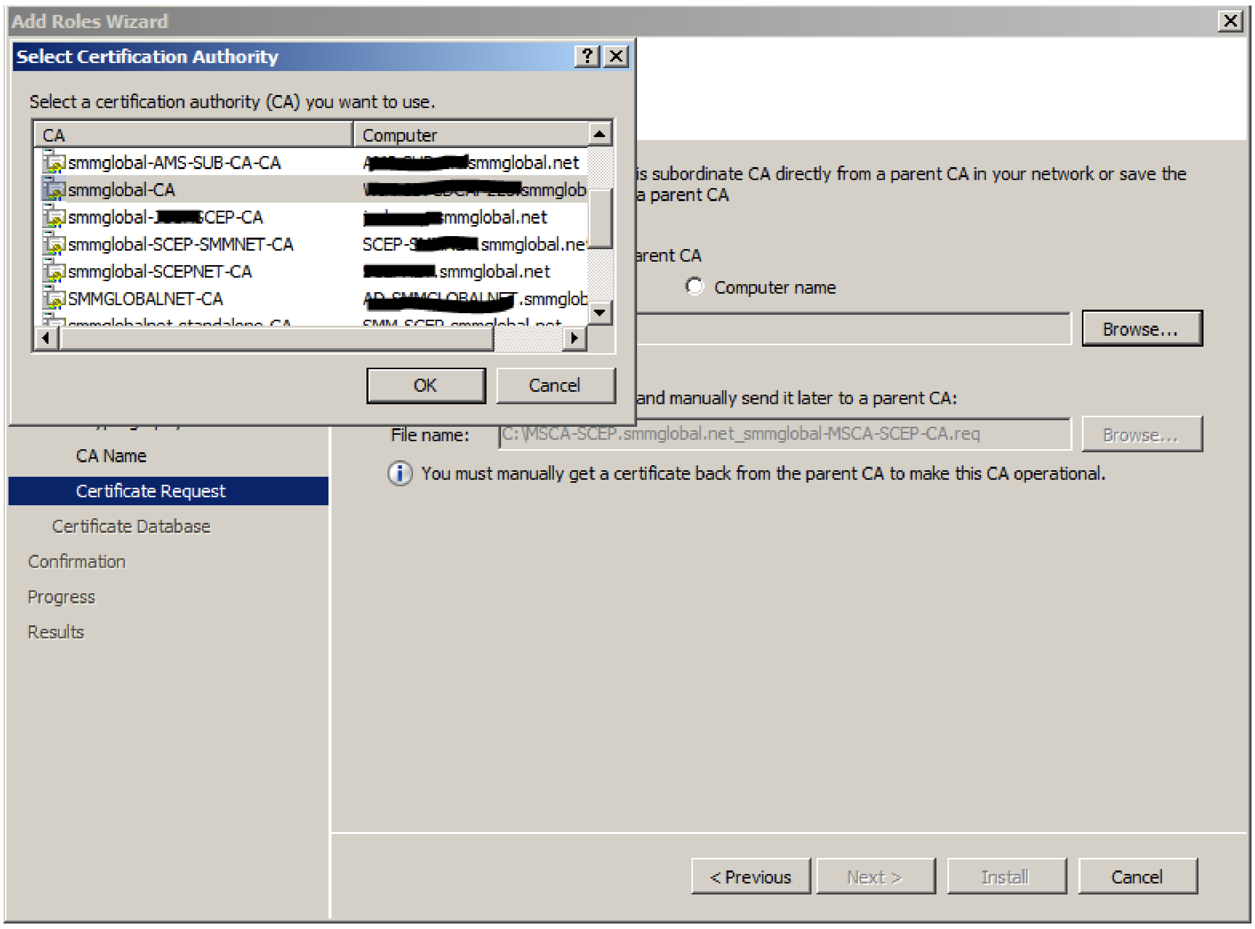
- SHA256
- SHA384
- SHA512
- SHA1

□ Allow administrator interaction when the private key is accessed by the CA.

More about cryptographic options for a CA

Note: iOS does not validate CA/RA certificates which are greater than 4096.

24. Accept the default common name and DN for the CA and **Next**.
25. Select **Send a certificate request to a parent CA** and click **Browse…**



Add Roles Wizard

Select Certification Authority

Select a certification authority (CA) you want to use.

CA	Computer
smmglobal-AMS-SUB-CA-CA	[redacted]smmglobal.net
smmglobal-CA	[redacted]smmglob
smmglobal-[redacted]CEP-CA	[redacted]mmglobal.net
smmglobal-SCEP-SMMNET-CA	SCEP-[redacted]smmglobal.ne
smmglobal-SCEPNET-CA	[redacted].smmglobal.net
SMMGLOBALNET-CA	[redacted].smmglob

is subordinate CA directly from a parent CA in your network or save the a parent CA

arent CA

○ Computer name

and manually send it later to a parent CA:

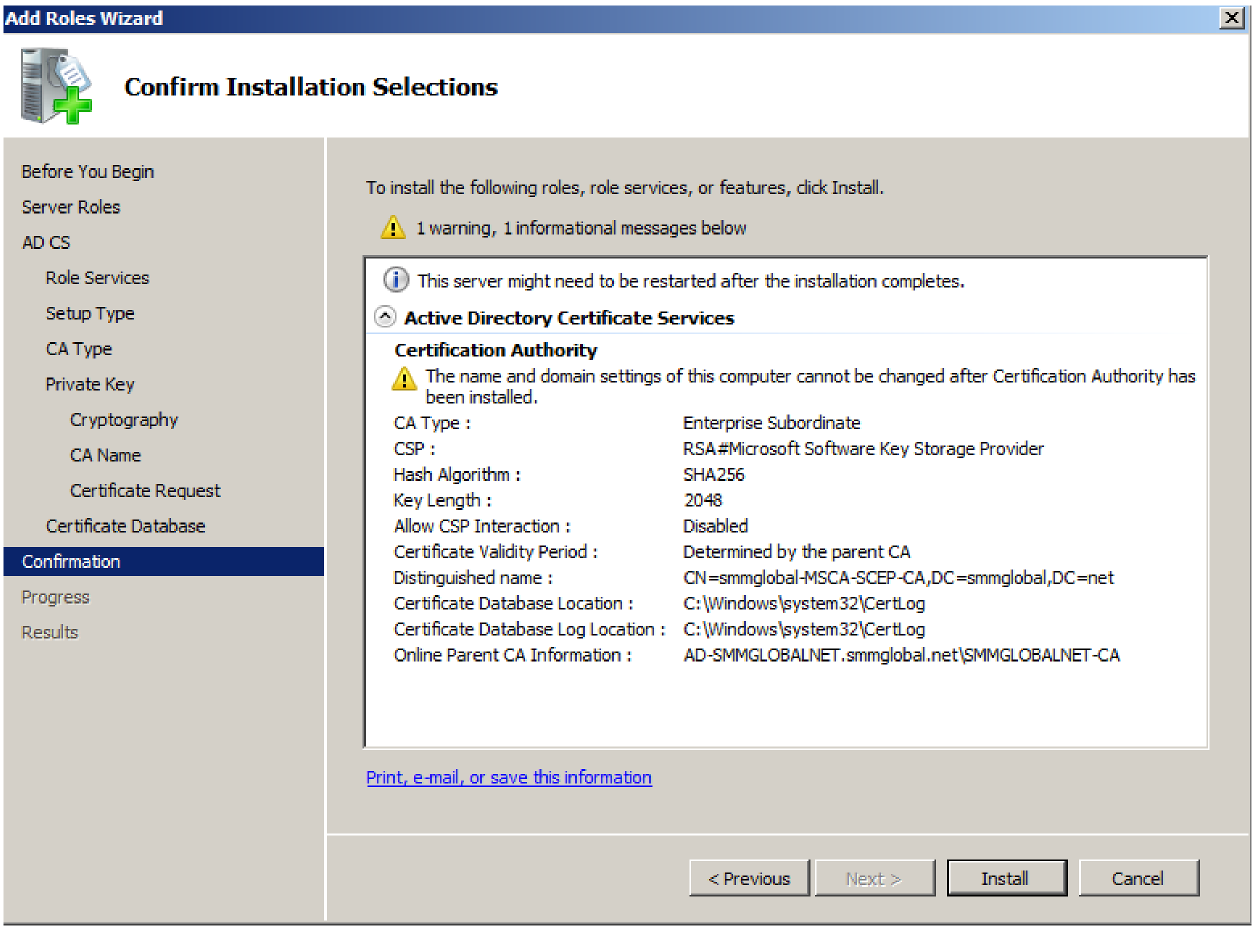
File name: C:\MSCA-SCEP.smmglobal.net_smmglobal-MSCA-SCEP-CA.req

You must manually get a certificate back from the parent CA to make this CA operational.

26. Select the CA from the list and **OK** from the selection window and click **Next**.

Note: If no CA is displayed the Root CA Option is recommended.

27. Review the default database directories and **Next**.
28. Review the subordinate CA's configuration and click **Install**:



To install the following roles, role services, or features, click Install.

1 warning, 1 informational messages below

This server might need to be restarted after the installation completes.

Active Directory Certificate Services

Certification Authority

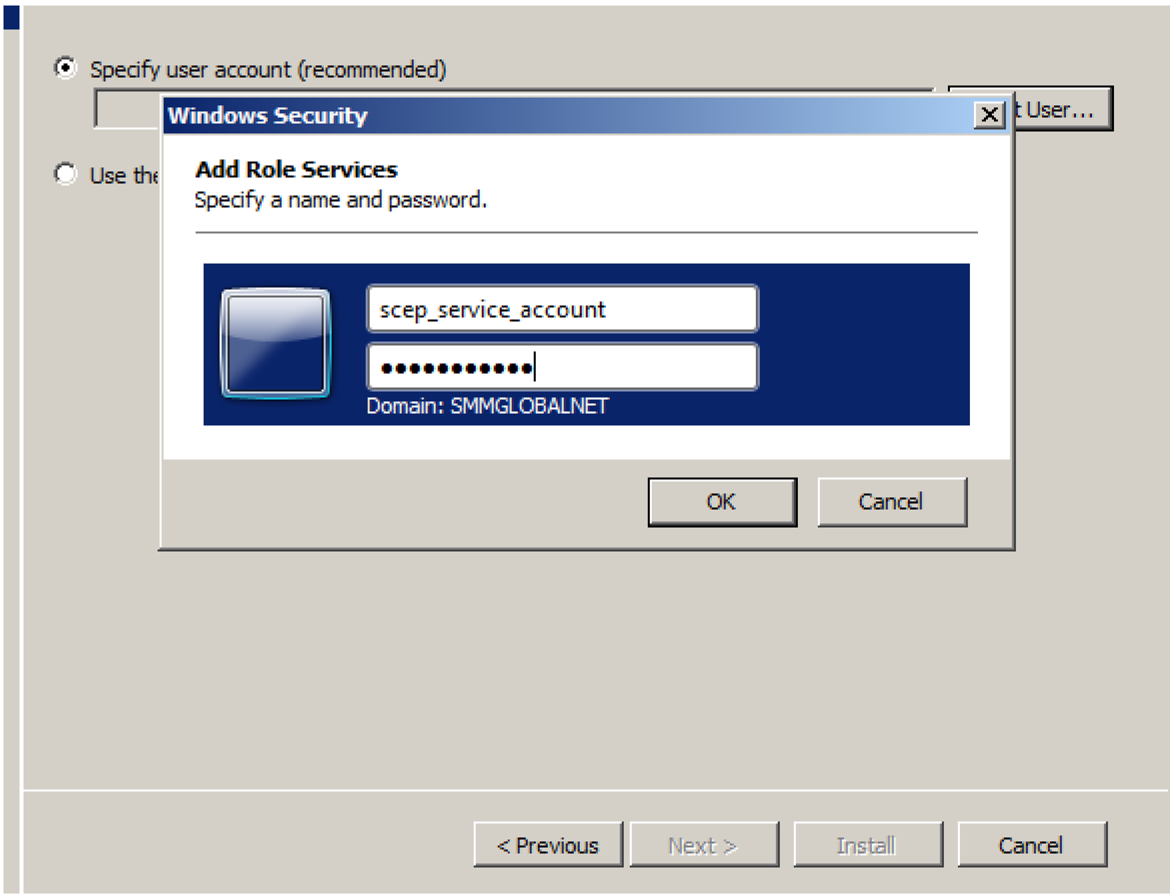
The name and domain settings of this computer cannot be changed after Certification Authority has been installed.

CA Type :	Enterprise Subordinate
CSP :	RSA#Microsoft Software Key Storage Provider
Hash Algorithm :	SHA256
Key Length :	2048
Allow CSP Interaction :	Disabled
Certificate Validity Period :	Determined by the parent CA
Distinguished name :	CN=smmglobal-MSCA-SCEP-CA,DC=smmglobal,DC=net
Certificate Database Location :	C:\Windows\system32\CertLog
Certificate Database Log Location :	C:\Windows\system32\CertLog
Online Parent CA Information :	AD-SMMGLOBALNET.smmglobal.net\SMMGLOBALNET-CA

Note: The installation can take up to 10 minutes.

Install the DNES service role

29. From the Server Manager console, expand **Roles** right-click on the **Active Directory Certificate Services** and click **Add Role Services.**
30. Check the **Network Device Enrollment Service**, when prompted click **Add Required Role Services** and **Next** to continue.
31. Click **Select User…** and add the SCEP user account created earlier:



Add Role Services

Specify a name and password.

scep_service_account

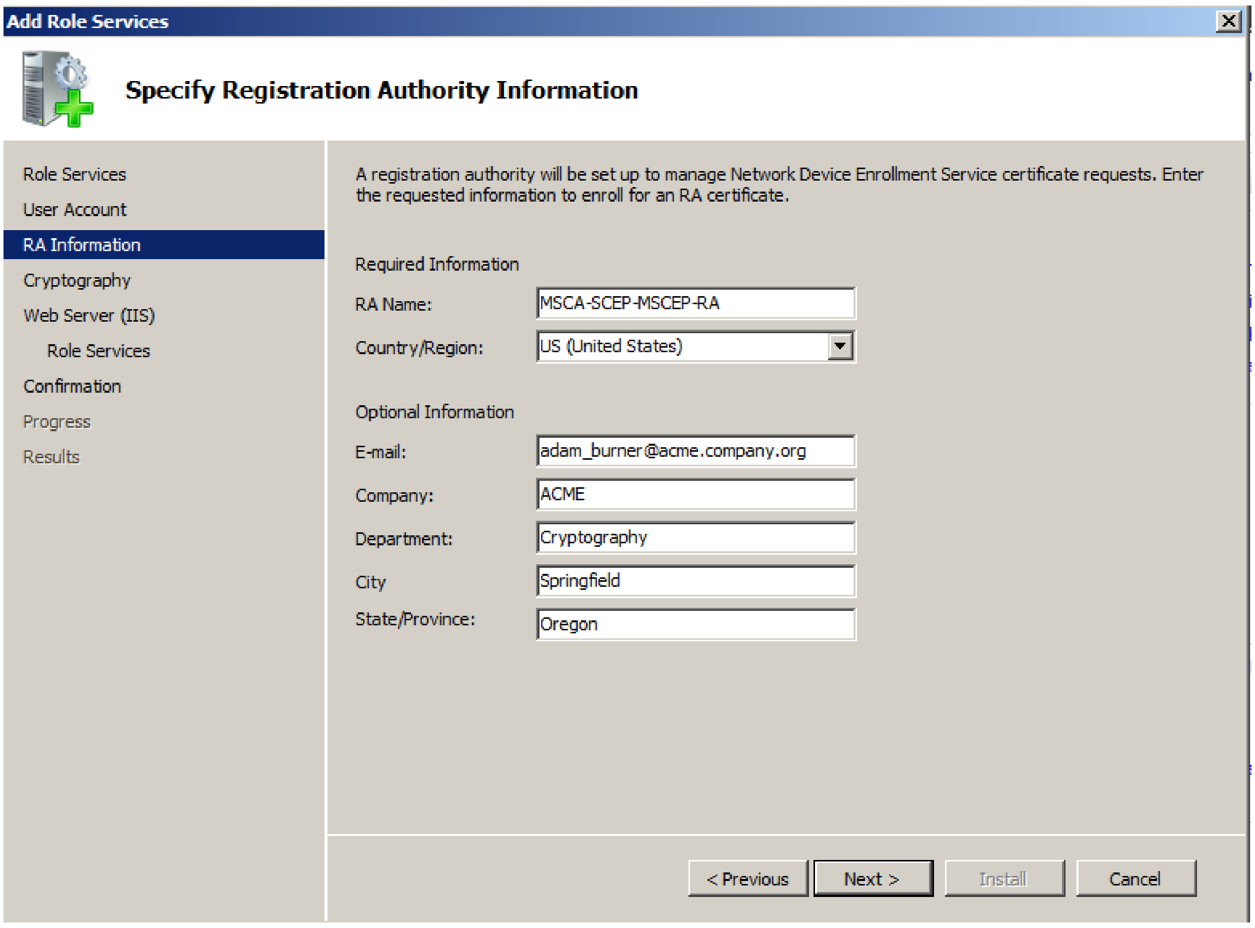
●●●●●●●●●●●

Domain: SMMGLOBALNET

Note: If a notification appears that the user is not a member of the IIS_USERS group on the local machine repeat Adding a user to the machine's local IIS_USERS group.

32. **Next** to continue to the RA (Registration Authority) Information section.

33. Optionally enter the certificate administrator's contact information. Ensure to not abbreviate the State/Province name:



Specify Registration Authority Information

A registration authority will be set up to manage Network Device Enrollment Service certificate requests. Enter the requested information to enroll for an RA certificate.

Required Information

RA Name: MSCA-SCEP-MSCEP-RA

Country/Region: US (United States)

Optional Information

E-mail: adam_burner@acme.company.org

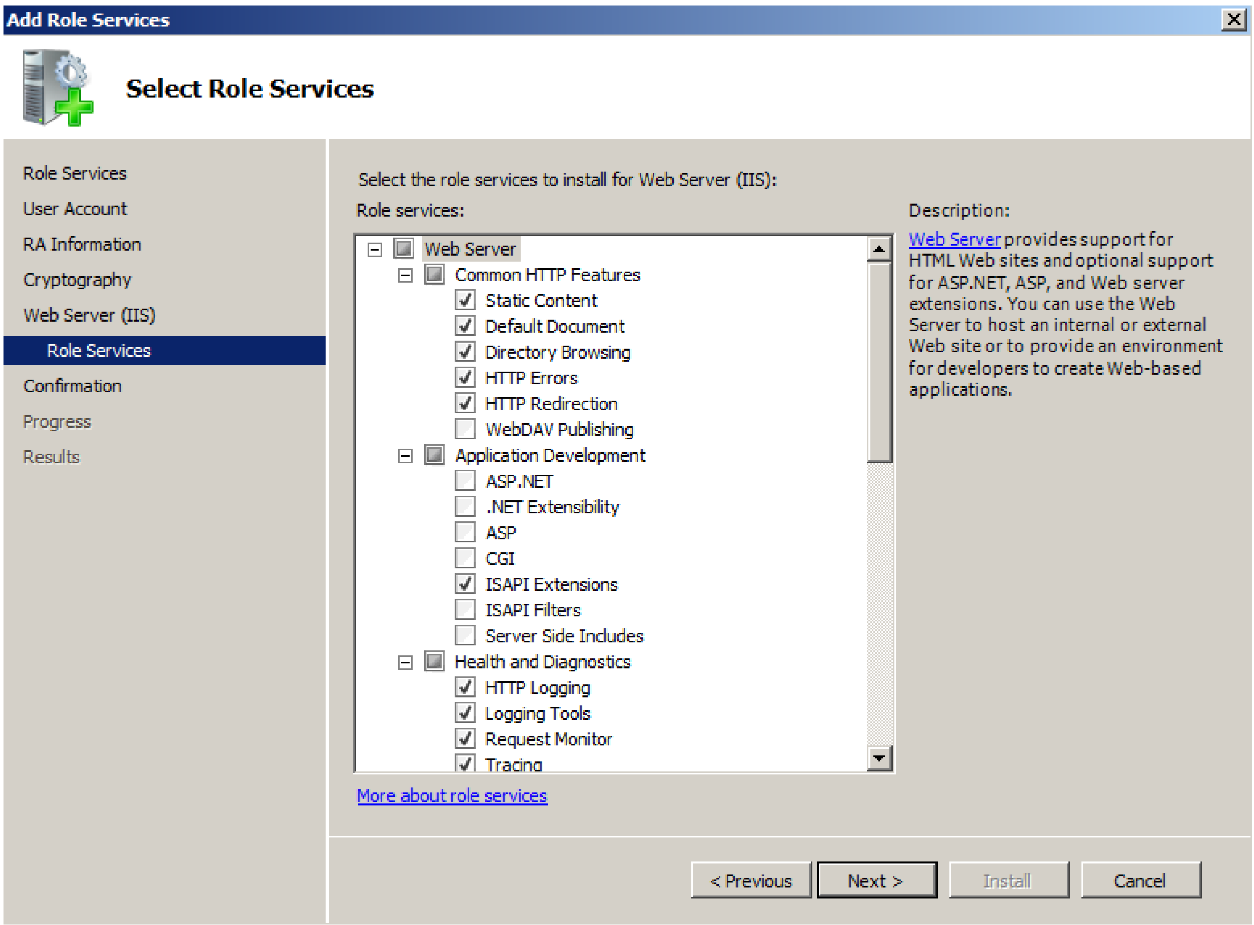
Company: ACME

Department: Cryptography

City Springfield

State/Province: Oregon

34. Click **Next** and ensure that 2048 or 4096 are selected for the key character lengths and **Next** .
35. **Next** through the Web Server (IIS) Introduction page.
36. Accept the default features and **Next**:



Select Role Services

Select the role services to install for Web Server (IIS):

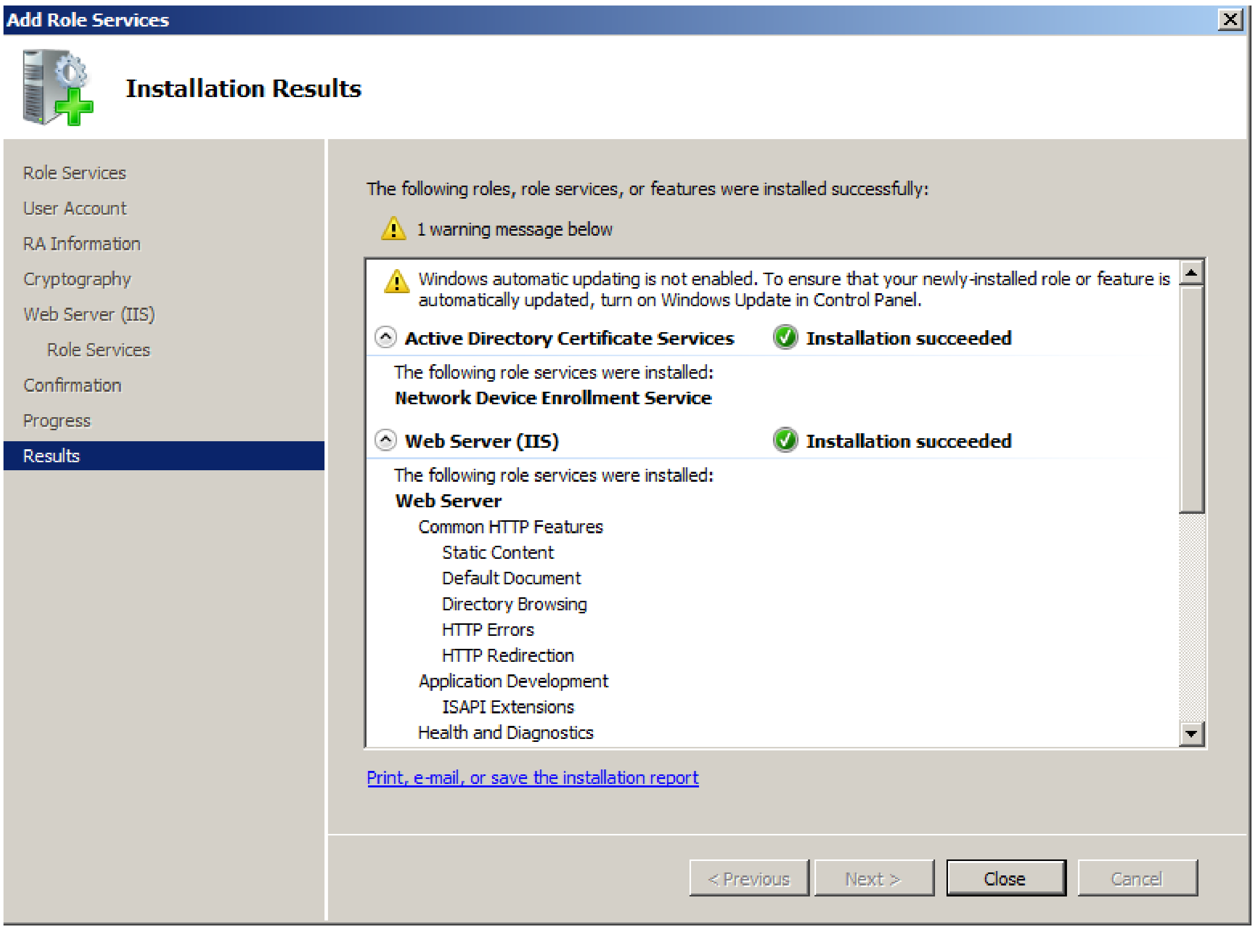
Role services:

- Web Server
  - Common HTTP Features
    - ☑ Static Content
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ HTTP Redirection
    - □ WebDAV Publishing
  - Application Development
    - □ ASP.NET
    - □ .NET Extensibility
    - □ ASP
    - □ CGI
    - ☑ ISAPI Extensions
    - □ ISAPI Filters
    - □ Server Side Includes
  - Health and Diagnostics
    - ☑ HTTP Logging
    - ☑ Logging Tools
    - ☑ Request Monitor
    - ☑ Tracing

Description:

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

37. Review the configuration and click **Install**:



The following roles, role services, or features were installed successfully:

1 warning message below

Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update in Control Panel.

Active Directory Certificate Services **Installation succeeded**

The following role services were installed:
Network Device Enrollment Service

Web Server (IIS) **Installation succeeded**

The following role services were installed:
Web Server
Common HTTP Features
Static Content
Default Document
Directory Browsing
HTTP Errors
HTTP Redirection
Application Development
ISAPI Extensions
Health and Diagnostics

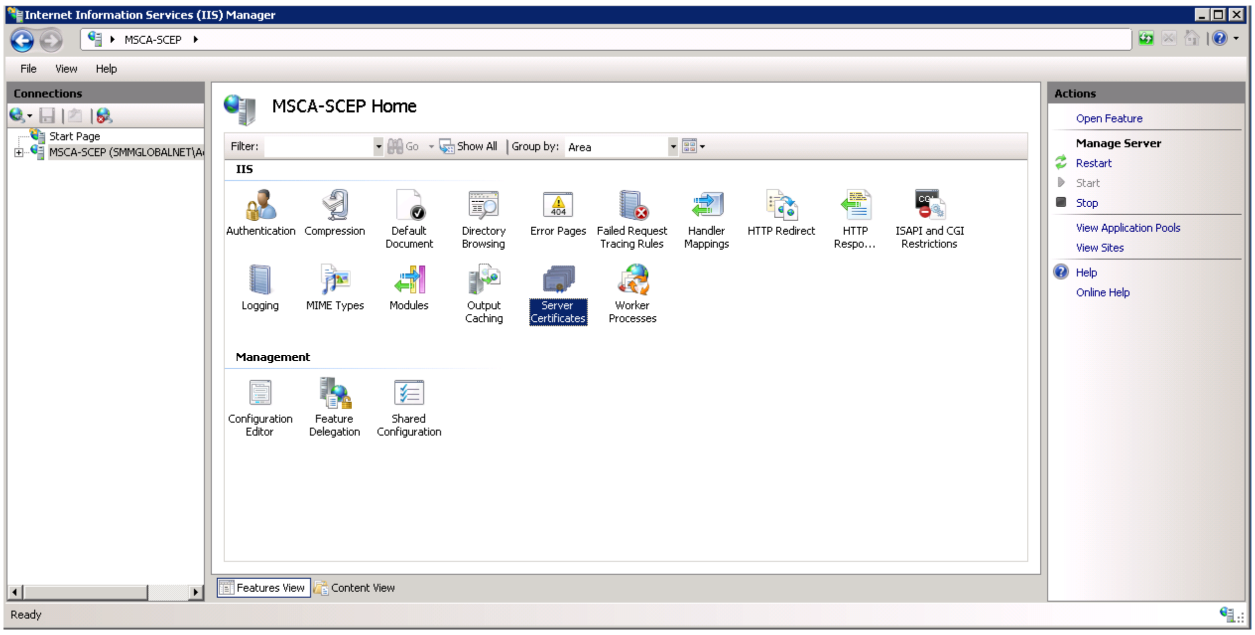
Print, e-mail, or save the installation report

Adding a Certificate to the IIS

38. **Start > Run**:

    inetmgr

39. From the IIS Manager console select the SCEP server's name on the left and open **Server Certificates** from the **Features View** on the right:



40. If an SSL certificate is already issued to this machine, it will be displayed along with the CA certificate. Select one of the three options below to bind an SSL certificate to this machine.

Temporary Self-Signed Certificate

41. On the right, click **Create Self-Signed Certificate…**
42. Enter a friendly name for this certificate to identify it and OK.

Import a PKCS Certificate

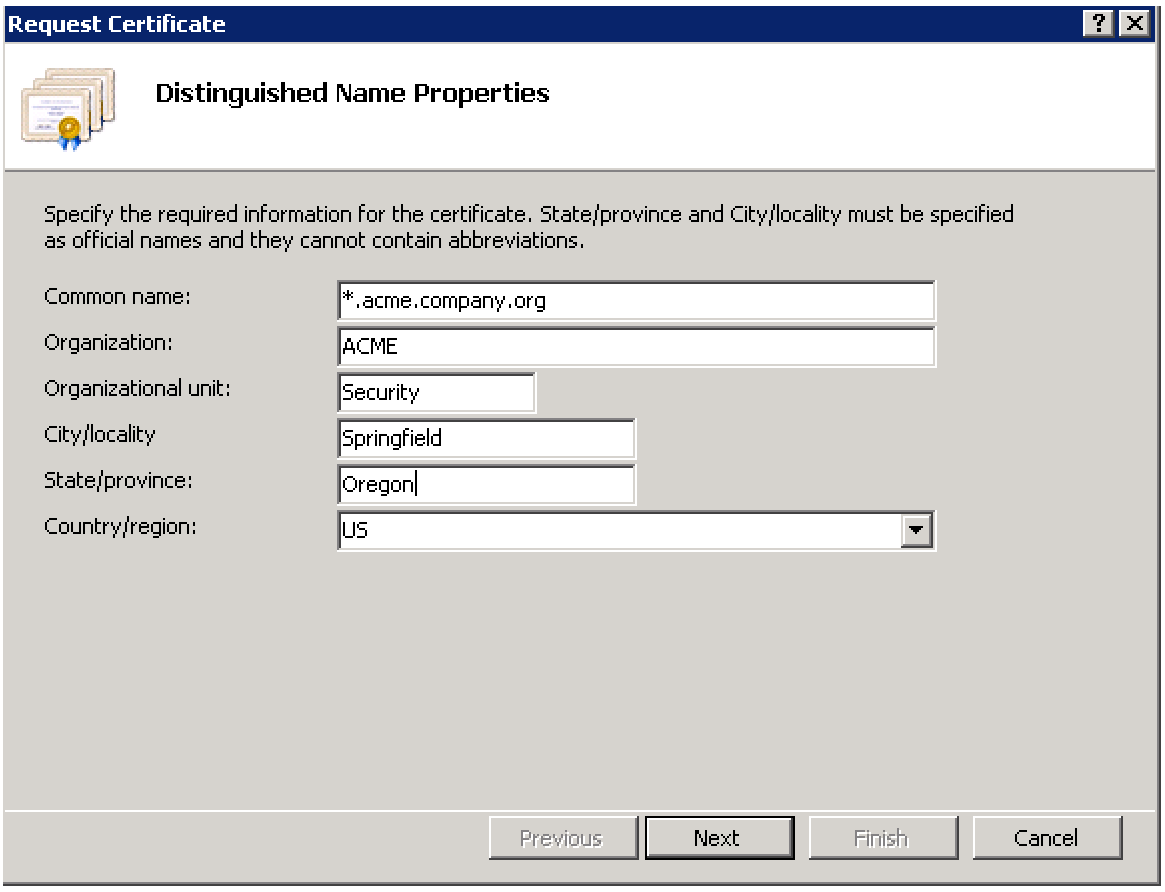
43. Transfer the PKCS certificate to the machine.
44. From the IIS **Manager > Server Certificates** click **Import…** on the right.
45. Browse to the certificate file and click **OK**.
46. Enter the passphrase for the certificate file.

Request a Certificate from a Certificate Authority

47. From the IIS **Manager > Server Certificates** click **Create Certificate Request…** on the right.

48. Enter the server information into the request.

Note: The Common Name must match the published domain name of the server. Do not abbreviate the State/Province field. Contact your public certificate authority for how to fill in this request:



Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name: *.acme.company.org

Organization: ACME

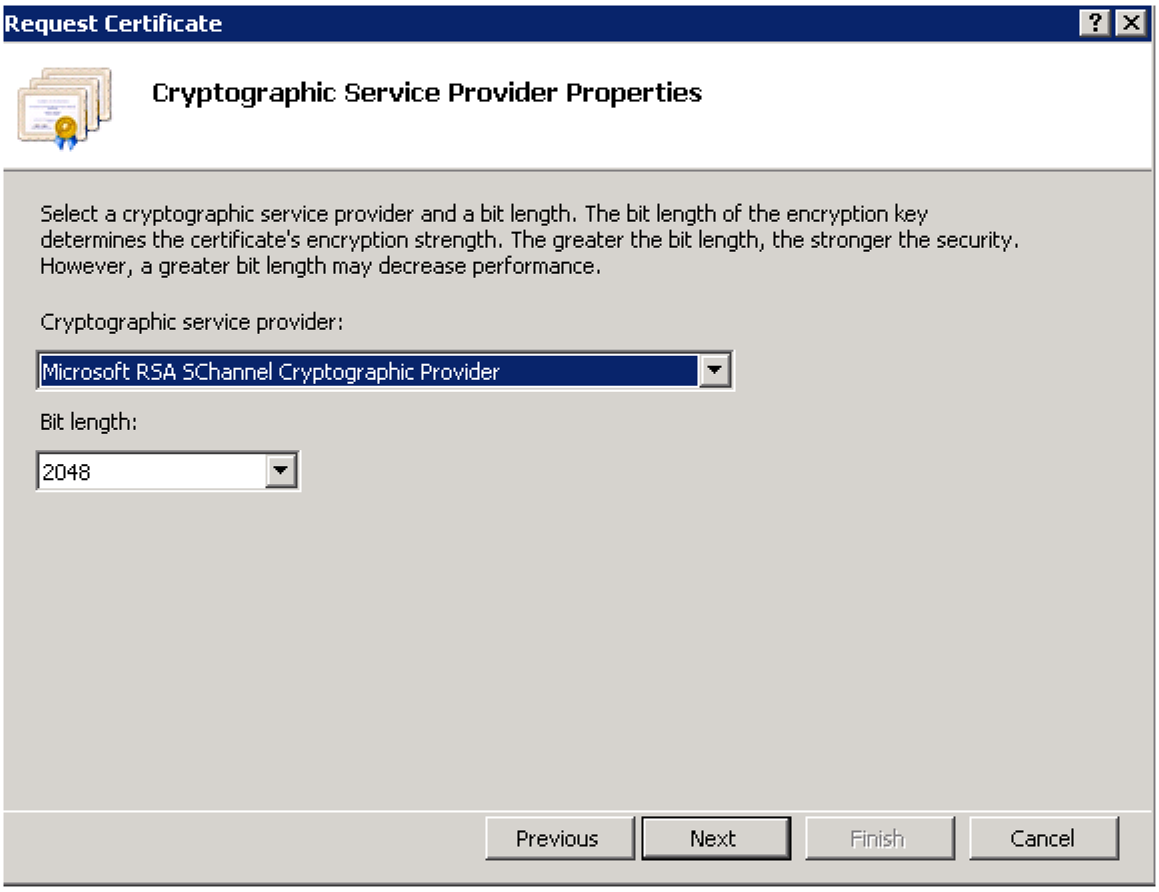
Organizational unit: Security

City/locality: Springfield

State/province: Oregon

Country/region: US

49. **Next** to the Cryptographic properties and ensure that 2048 or 4096 are selected for the **Bit Length** and **Next**.



Cryptographic Service Provider Properties

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider

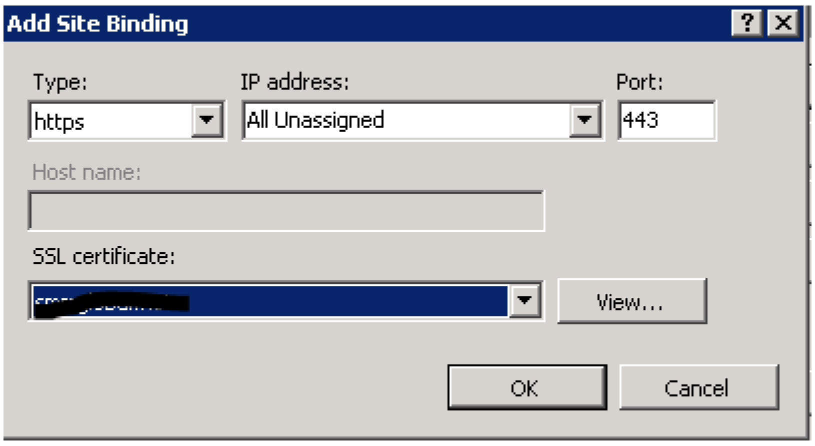
Bit length: 2048

50. Save the CSR (Certificate Signing Request) file and **Finish**.
51. Send the CSR to the CA, following their instructions.
52. Once a certificate is issue click **Complete Certificate Request…** from the IIS Manager > Certificates console and follow the wizard to import the new certificate.

HTTPS Bindings

53. From within the IIS Manager, expand the **Sites** and right-click on the **Default Web Site** and select **Edit Bindings**.

54. Click **Add** and select **HTTPS** for the **type** and the **new SSL certificate**:



Type: https

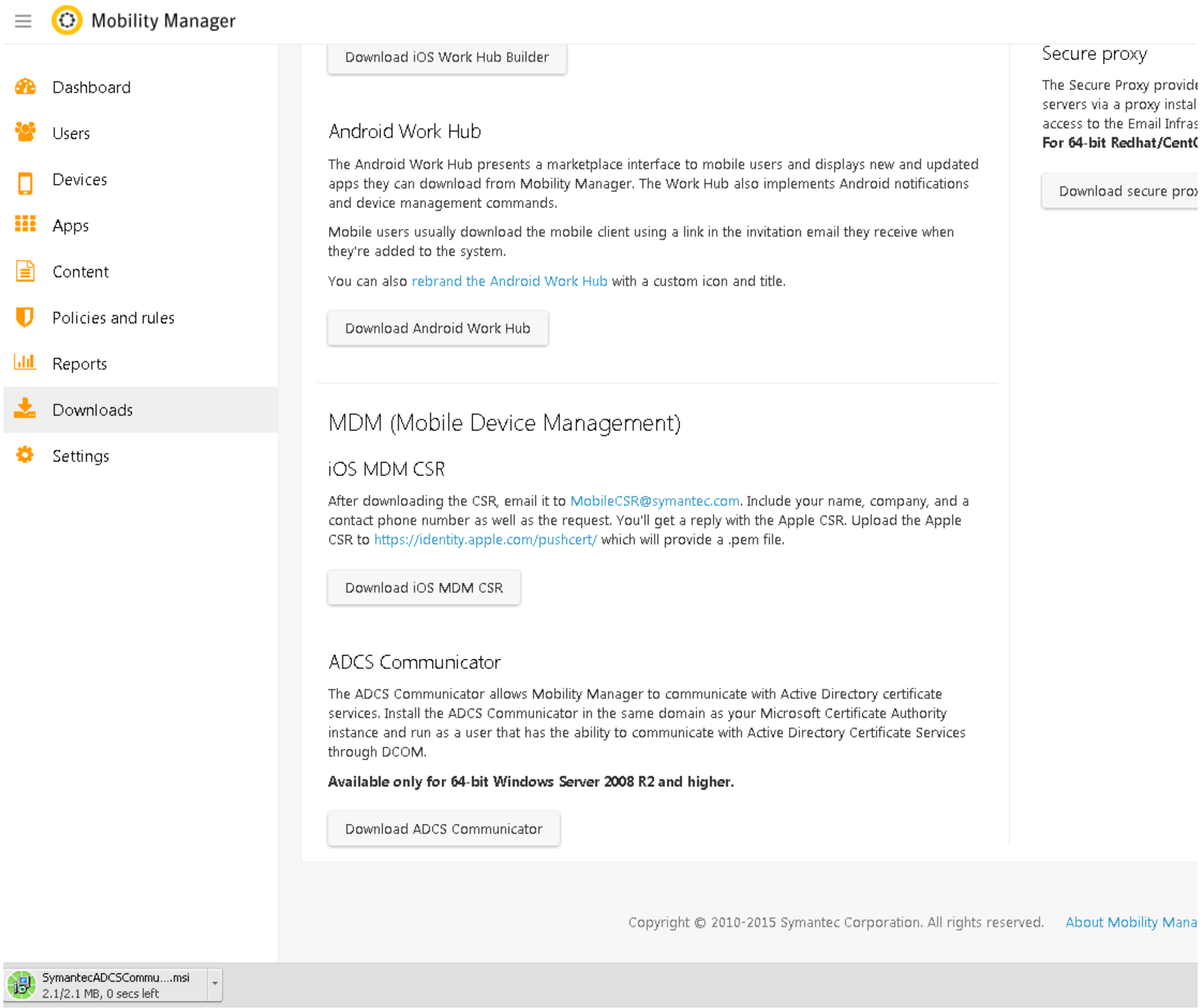
IP address: All Unassigned

Port: 443

Host name:

SSL certificate: [redacted]

55. Click **OK** and **Close** out of the Site Bindings window.
56. Download and transfer the ADSC Communicator installer to the MSCA server:



Android Work Hub

The Android Work Hub presents a marketplace interface to mobile users and displays new and updated apps they can download from Mobility Manager. The Work Hub also implements Android notifications and device management commands.

Mobile users usually download the mobile client using a link in the invitation email they receive when they're added to the system.

You can also rebrand the Android Work Hub with a custom icon and title.

MDM (Mobile Device Management)

iOS MDM CSR

After downloading the CSR, email it to MobileCSR@symantec.com. Include your name, company, and a contact phone number as well as the request. You'll get a reply with the Apple CSR. Upload the Apple CSR to https://identity.apple.com/pushcert/ which will provide a .pem file.

ADCS Communicator

The ADCS Communicator allows Mobility Manager to communicate with Active Directory certificate services. Install the ADCS Communicator in the same domain as your Microsoft Certificate Authority instance and run as a user that has the ability to communicate with Active Directory Certificate Services through DCOM.

Available only for 64-bit Windows Server 2008 R2 and higher.

Secure proxy

The Secure Proxy provid
servers via a proxy instal
access to the Email Infras
For 64-bit Redhat/Cent

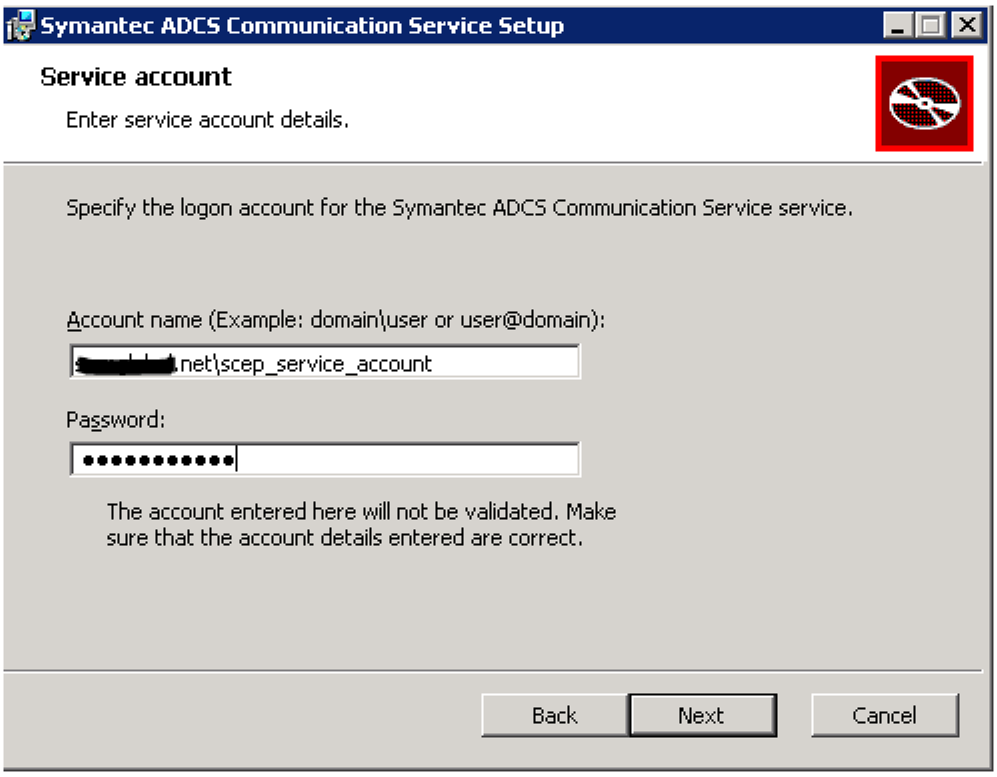
Copyright © 2010-2015 Symantec Corporation. All rights reserved.

57. Download and install the .NET Framework 4:

http://www.microsoft.com/en-us/download/details.aspx?id=17851

Note: A system reboot is required after installing .NET 4.

58. Run the SymantecADCSCommunicator.msi file, to begin, click **Next.**
59. Take note of the installation path, click **Next.**
60. Enter the scep user's credentials for the **Account name** and **Password;** click **Next**:



Symantec ADCS Communication Service Setup

Service account

Enter service account details.

Specify the logon account for the Symantec ADCS Communication Service service.

Account name (Example: domain\user or user@domain):

[redacted].net\scep_service_account

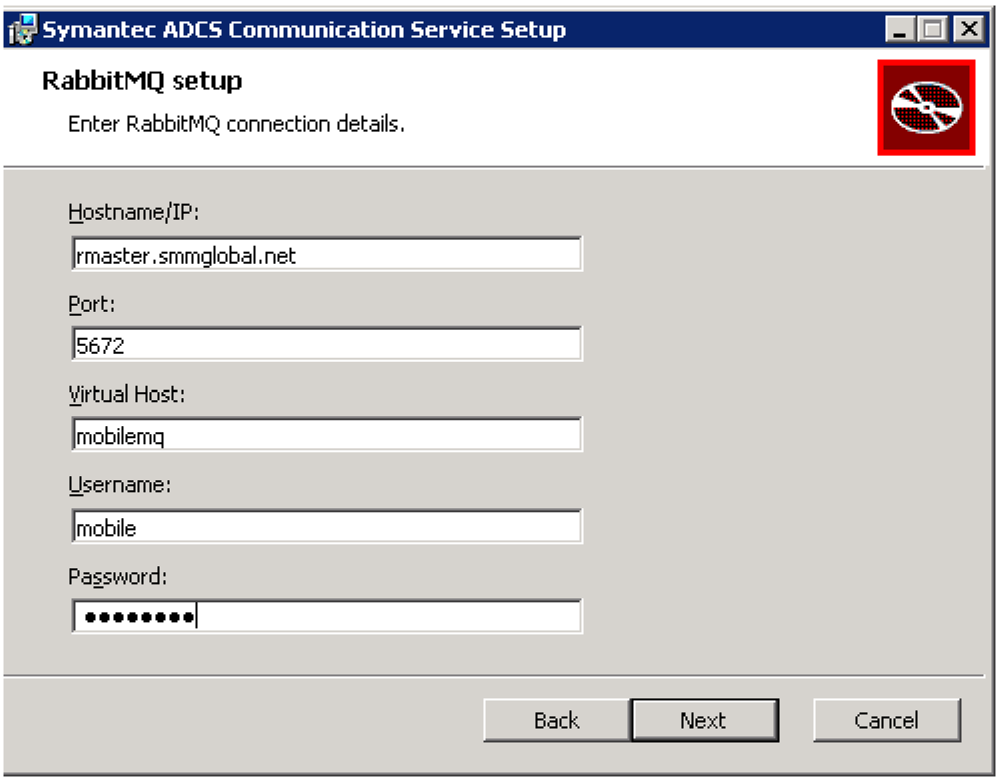
Password:

●●●●●●●●●●●●

The account entered here will not be validated. Make sure that the account details entered are correct.

61. Enter the RabbitMQ information for the Mobility server.

Important: If a local RabbitMQ service was used, STOP and read the beginning of this article. A production RabbitMQ service is required. See HOWTO110356 to deploy a production RabbitMQ cluster. If this article was followed, all this information is stored on the Rabbit server in /var/log/rabbit-install.log



Symantec ADCS Communication Service Setup

RabbitMQ setup

Enter RabbitMQ connection details.

Hostname/IP: rmaster.smmglobal.net

Port: 5672

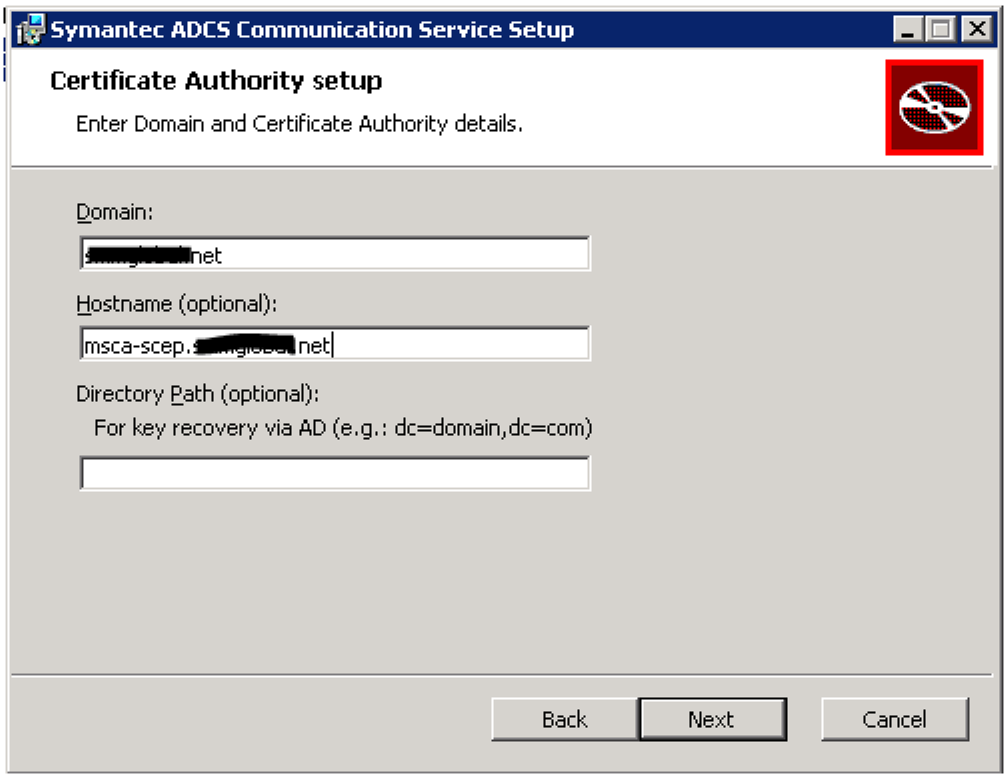
Virtual Host: mobilemq

Username: mobile

Password: ●●●●●●●●●

62. Verify that the domain information is correct and enter the server's published hostname, click **Next**.

Note: The server's hostname is the name used for the CN (Common Name) in the certificate, unless the certificate is wildcard. This hostname needs to be resolvable from the Mobility FE (front-end):



Certificate Authority setup

Enter Domain and Certificate Authority details.

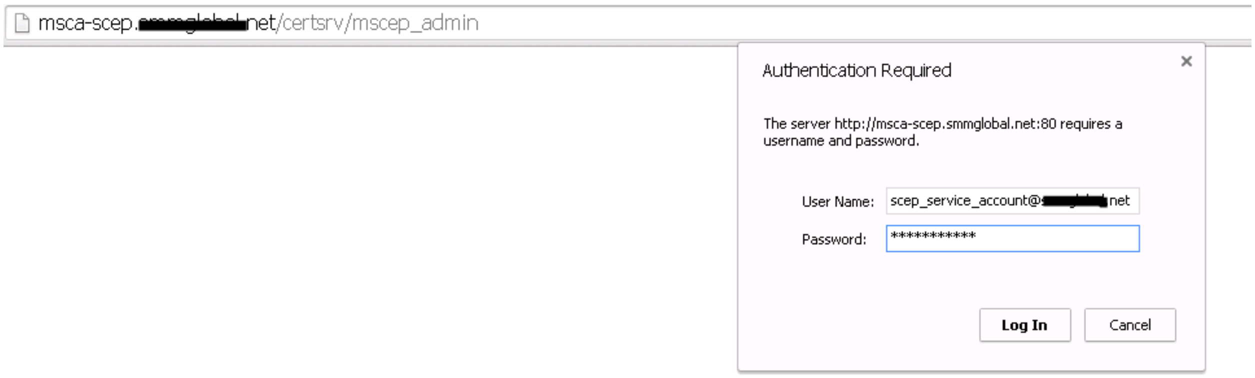
Domain: [redacted]net

Hostname (optional): msca-scep.[redacted]net

Directory Path (optional):
For key recovery via AD (e.g.: dc=domain,dc=com)

63. Enter the MSCA's SCEP/NDES admin URL and see the tip below…

Tip: To test this URL, enter it into a browser, enter the SCEP user's credentials, click **Log In**:



msca-scep.[redacted]net/certsrv/mscep_admin

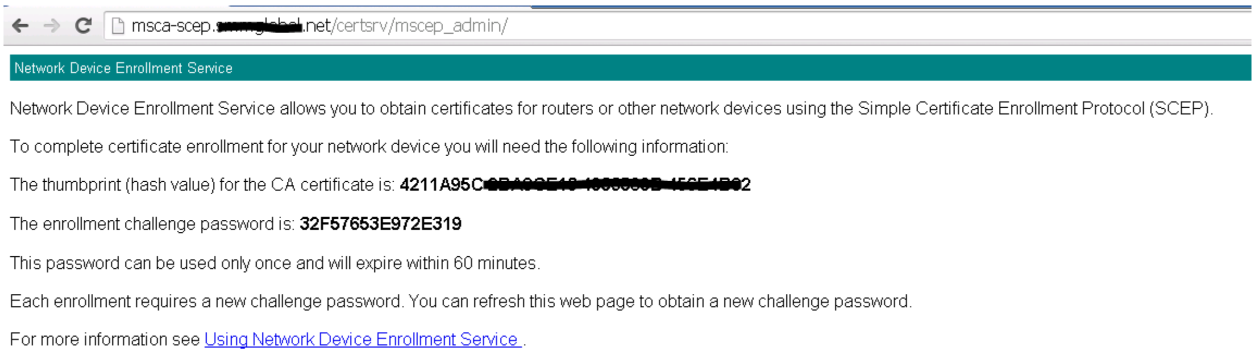
Authentication Required

The server http://msca-scep.smmglobal.net:80 requires a username and password.

User Name: scep_service_account@[redacted]net

Password: ************

After log in:



msca-scep.[redacted]net/certsrv/mscep_admin/

Network Device Enrollment Service

Network Device Enrollment Service allows you to obtain certificates for routers or other network devices using the Simple Certificate Enrollment Protocol (SCEP).

To complete certificate enrollment for your network device you will need the following information:

The thumbprint (hash value) for the CA certificate is: **4211A95C[redacted]**

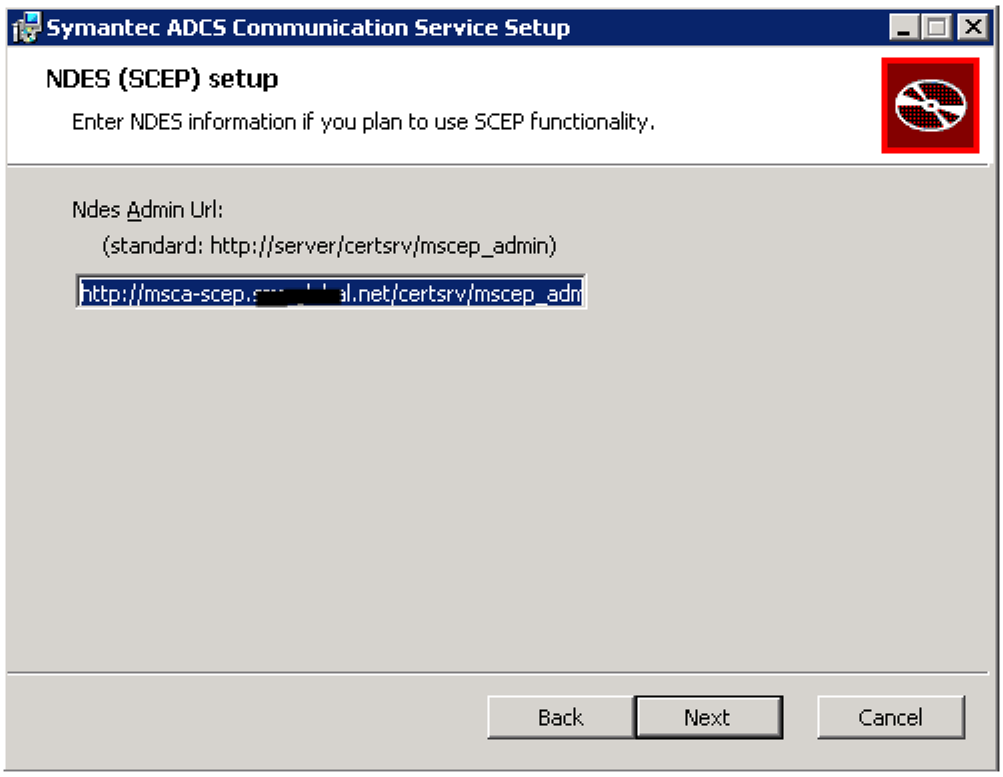
The enrollment challenge password is: **32F57653E972E319**

This password can be used only once and will expire within 60 minutes.

Each enrollment requires a new challenge password. You can refresh this web page to obtain a new challenge password.

For more information see Using Network Device Enrollment Service .

Once the URL is confirmed, click **Next**.


Symantec ADCS Communication Service Setup

NDES (SCEP) setup

Enter NDES information if you plan to use SCEP functionality.

Ndes Admin Url:

(standard: http://server/certsrv/mscep_admin)

http://msca-scep.[redacted]l.net/certsrv/mscep_adm

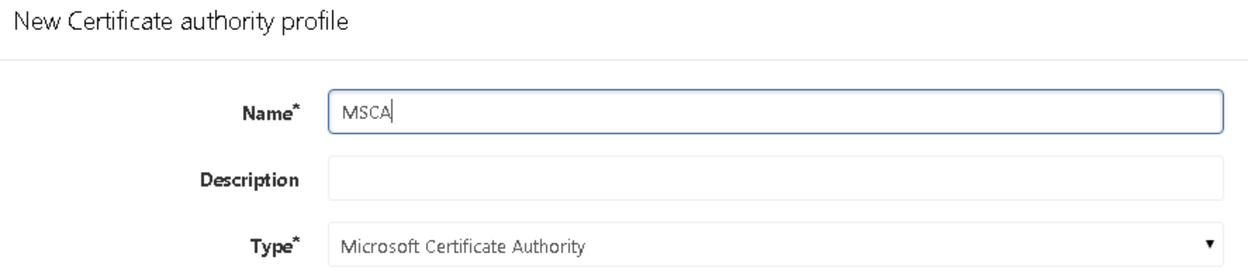
64. Click **Install**.

Add a Certificate Authority to Mobility

65. From the MSCA server, click **Start > Run** and enter **MMC**.
66. Click **File > Add remove snap-in,** select **Certificates** and click **Add.**
67. Select **Computer Account** and **Next.**
68. Ensure **Local computer** is selected and click **Finish**.
69. Click **OK.**
70. Expand the Certificates (Local computer) tree to **Personal Certificates**.
71. Right-click on the CA certificate and select **All tasks** > **Export**.
72. Click, **Next**; select **No, do not export the private key** and click **Next.**
73. Select **Base-64** and click **Next**.
74. Save the file as **CA_cert.cer** and click **Next**.

Note: This certificate needs to be accessible from the workstation accessing the Mobility admin console as it will be uploaded to the server.

75. From the Mobility **Admin console > Policies and rules > Device profiles,** click the + (plus) symbol next to **CERTIFICATE AUTHORITY**:
76. Name it, MSCA and select **Microsoft Certificate Authority** for **Type:**

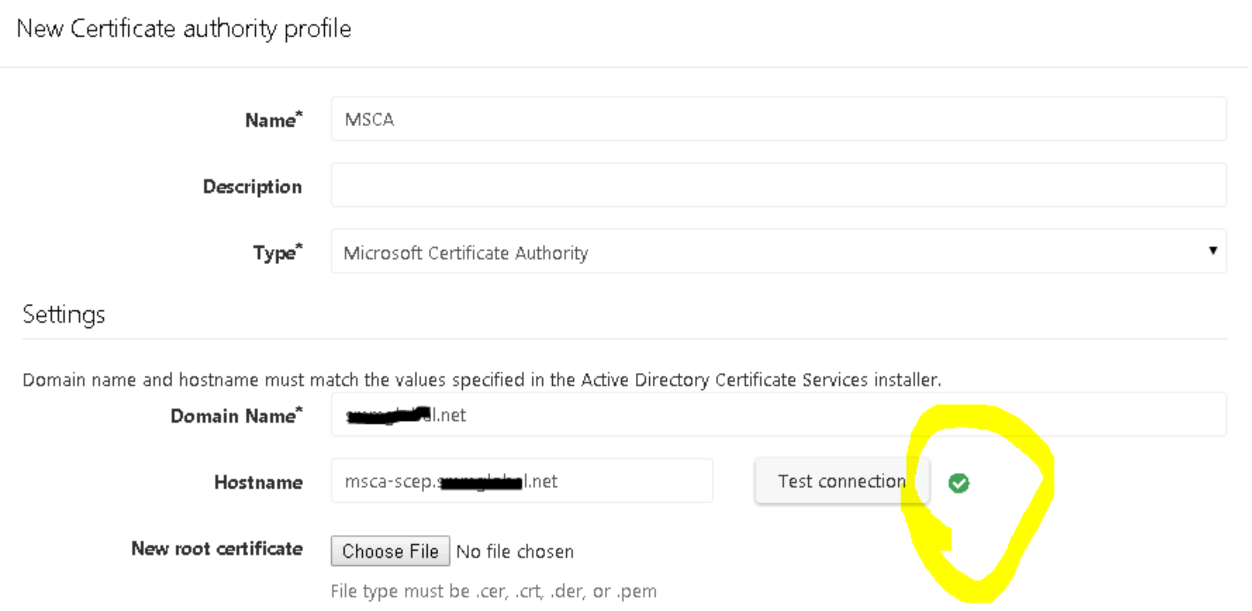

New Certificate authority profile

Name*: MSCA

Description:

Type*: Microsoft Certificate Authority

77. Under **Settings** enter the **Domain Name** and **Hostname** from step 62, click **Test connection**. A green checkbox is displayed. If after some time it errors, verify that the Mobility server can resolve this hostname. Add it to the DNS or modify the server's /etc/hosts file.



New Certificate authority profile

Name* MSCA

Description

Type* Microsoft Certificate Authority ▾

Settings

Domain name and hostname must match the values specified in the Active Directory Certificate Services installer.

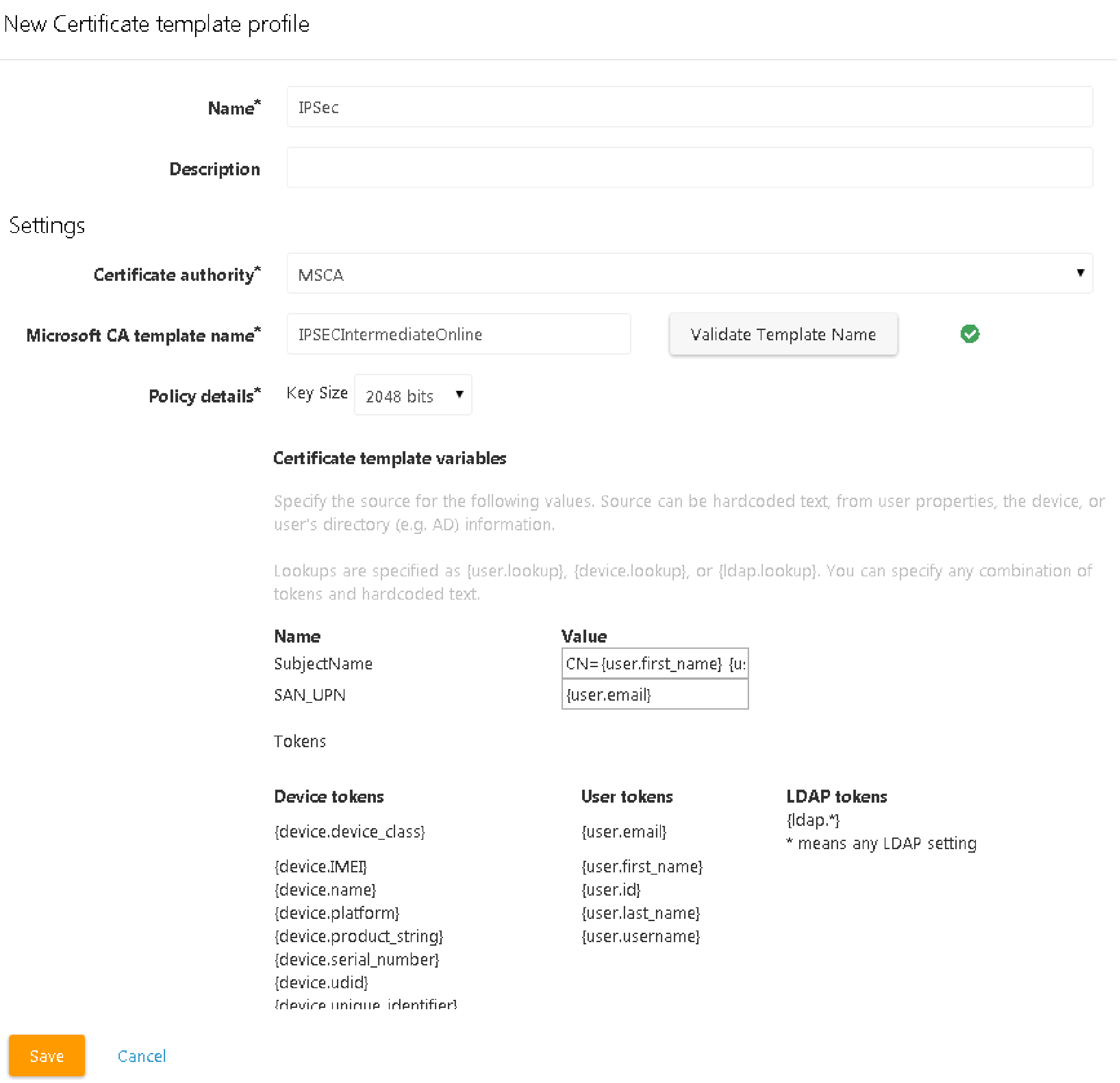
Domain Name* [redacted]l.net

Hostname msca-scep.[redacted]l.net

New root certificate

File type must be .cer, .crt, .der, or .pem

78. Finally, click **Choose File** and browse to the certificate exported /saved in step 74. Click **Save**.
79. Click the + (plus) symbol next to the **CERTIFICATE TEMPLATE** profile.
80. Name it, IPSec and select the MSCA as the **Certificate Authority**.
81. For the template name, enter **IPSECIntermediateOnline** and click **Validate Template Name:**



New Certificate template profile

Name* IPSec

Description

Settings

Certificate authority* MSCA ▾

Microsoft CA template name* IPSECIntermediateOnline

Policy details* Key Size 2048 bits ▾

Certificate template variables

Specify the source for the following values. Source can be hardcoded text, from user properties, the device, or user's directory (e.g. AD) information.

Lookups are specified as {user.lookup}, {device.lookup}, or {ldap.lookup}. You can specify any combination of tokens and hardcoded text.

Name	Value
SubjectName	CN={user.first_name} {u:
SAN_UPN	{user.email}

Tokens

Device tokens	User tokens	LDAP tokens
{device.device_class}	{user.email}	{ldap.*} * means any LDAP setting
{device.IMEI}	{user.first_name}	
{device.name}	{user.id}	
{device.platform}	{user.last_name}	
{device.product_string}	{user.username}	
{device.serial_number}		
{device.udid}		
{device.unique_identifier}		

82. Click **Save**.
83. Click the **+ (plus)** symbol next to **SCEP**.
84. Name the Profile **SCEP** and enter the URL of the MSCA enrollment service. The FQDN is this URL needs to be resolvable from the Mobile Devices. EG https://msca-scep.acme.company.org/certsrv/mscep/mscep.dll

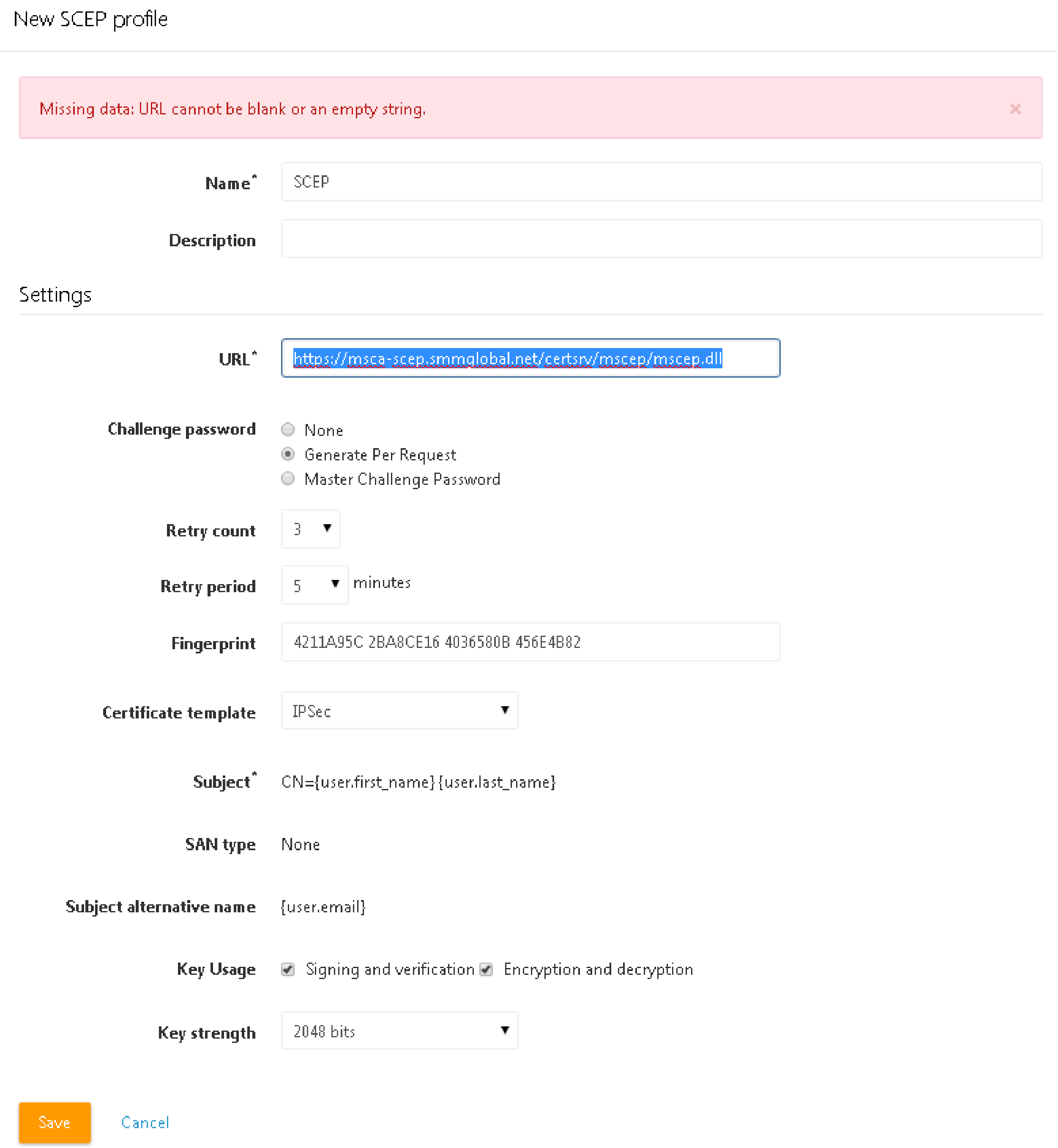
Tip: Test this URL in a workstation to ensure that it arrives at the device enrollment page of the MSCA/NDES server.

85. Select **Generate Per Request** for the **Challenge Password**.

86. Navigate, from the workstation, to the SCEP admin URL from step 63 and copy the CA's thumbprint as the **Fingerprint.**

Note: Spaces in the Fingerprint/Thumbprint are okay.

87. Select **IPSec** as the **Template** and 2048 as the **Key strength**; click **Save:**



New SCEP profile

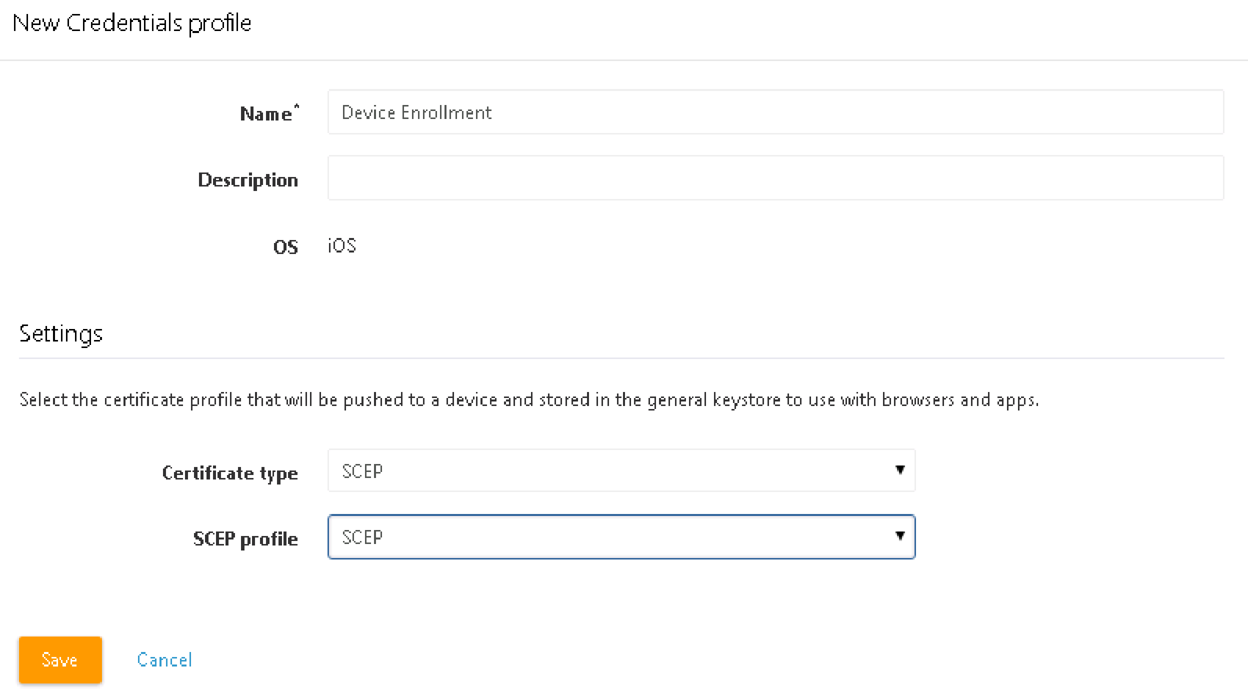
Missing data: URL cannot be blank or an empty string.

Name*	SCEP
Description	

Settings

URL*	https://msca-scep.smmglobal.net/certsrv/mscep/mscep.dll
Challenge password	○ None ● Generate Per Request ○ Master Challenge Password
Retry count	3 ▼
Retry period	5 ▼ minutes
Fingerprint	4211A95C 2BA8CE16 4036580B 456E4B82
Certificate template	IPSec ▼
Subject*	CN={user.first_name} {user.last_name}
SAN type	None
Subject alternative name	{user.email}
Key Usage	☑ Signing and verification ☑ Encryption and decryption
Key strength	2048 bits ▼

88. Click the + (plus) symbol next to **CREDENTIALS** and name the credential **Device Enrollment.**
89. For **Certificate type** select **SCEP.**
90. For the SCEP Profile select **SCEP**, and click **Save:**



New Credentials profile

Name* Device Enrollment

Description

OS iOS

Settings

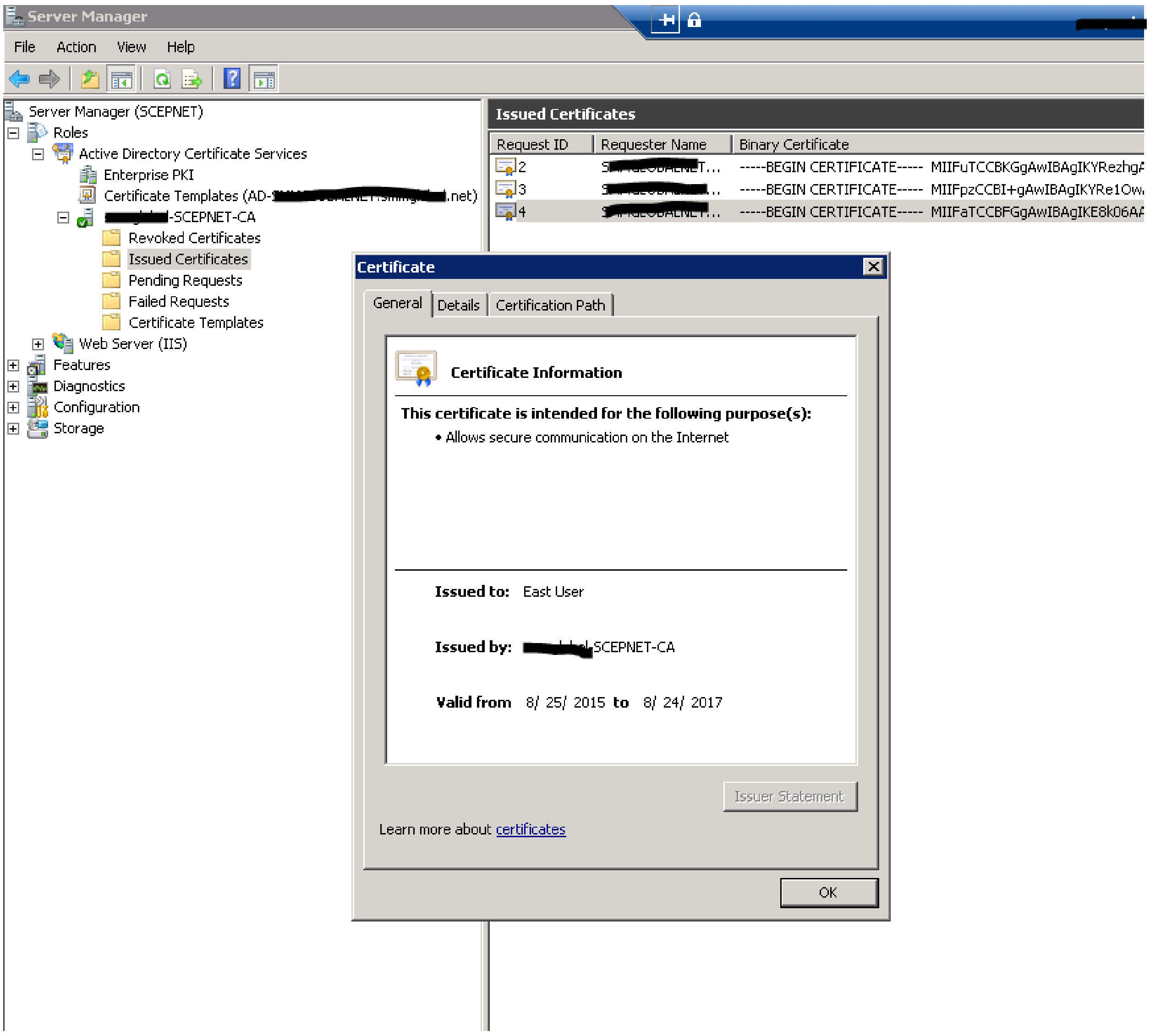
Select the certificate profile that will be pushed to a device and stored in the general keystore to use with browsers and apps.

Certificate type SCEP

SCEP profile SCEP

Add the SCEP Profile to a Device Policy

91. If not device profile has been created, create one.
92. Select the profile and click the edit symbol (Pencil).
93. Ensure enable MDM for iOS devices is checked and scroll down to the bottom of the edit window.
94. Under **Credentials** click **Add** and select **Device Enrollment.**
95. Save the profile and test it by enrolling a new iOS device that does not already have an MDM profile installed.
96. Verify that the server has issued a SCEP certificate by going to the Server Manager and expand **Active Directory Certificate Authority > Server_Name > Issued Certificates**. There should be a new certificate(s) issued to users by the First and Last names:



Issued Certificates

Request ID	Requester Name	Binary Certificate
2	[redacted]	-----BEGIN CERTIFICATE----- MIIFuTCCBKGgAwIBAgIKYRezhgA
3	[redacted]	-----BEGIN CERTIFICATE----- MIIFpzCCBI+gAwIBAgIKYRe1Ow
4	[redacted]	-----BEGIN CERTIFICATE----- MIIFaTCCBFGgAwIBAgIKE8k06AA

Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- Allows secure communication on the Internet

Issued to: East User

Issued by: [redacted]SCEPNET-CA

Valid from 8/ 25/ 2015 to 8/ 24/ 2017

Manual installation of an in-house certificate on Android and iOS

Important: The below article should only be used by technical professionals or when instructed by a trusted and qualified technician. It is divided into two main parts; the first is directed towards how to obtain and publish the certificate, making it available for the device. The second will add an in-house certificate to the devices' certificate store trust. This means that any certificate, application or website using a certificate by this source will be trusted to the device.

Terms of use for this information are found in Legal Notices.

Contents

Obtain the root/intermediate certificate

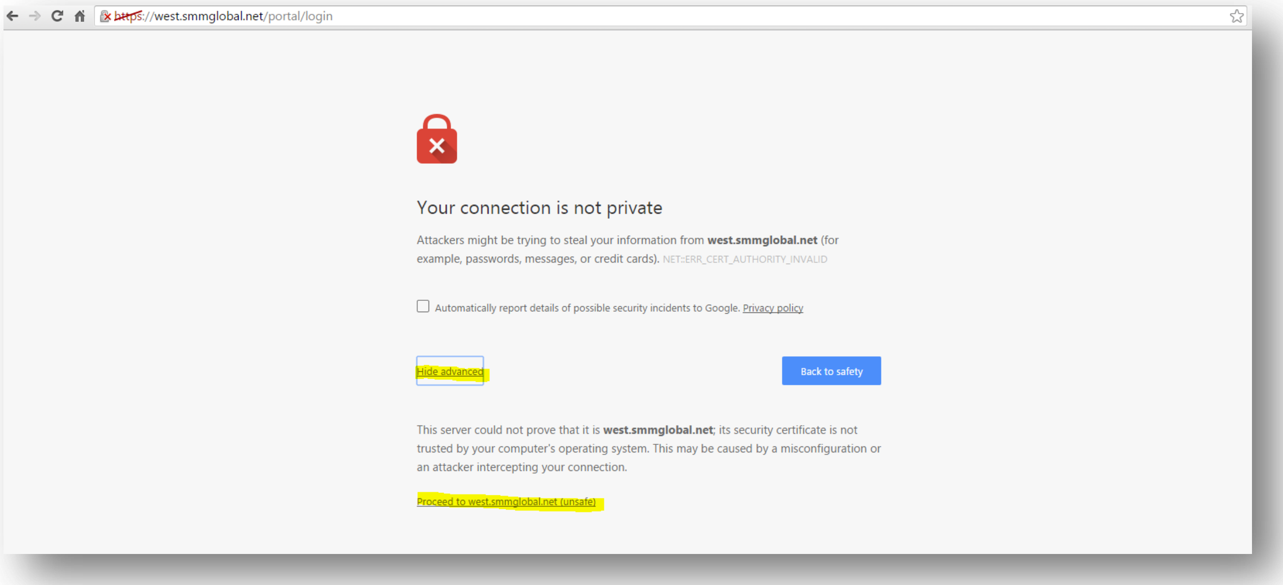
1. Use one of the following methods to obtain the root certificate which will be published to an internal site for devices to download.

Note: If the openca.sh script was used to create a temporary certificate to install Mobility as part of the Mobility A to Z guide the certificates are stored in the /home/<USERNAME>/certs/ directory on the server. Use the cacert.cer for device authentication.

Method 1: Using a PC

a. Open Chrome or Internet Explorer and navigate to any internal site hosting an in-house issued certificate.

Note: If prompted with a certificate warning, verify the URL and click proceed.



~~https~~://west.smmglobal.net/portal/login

Your connection is not private

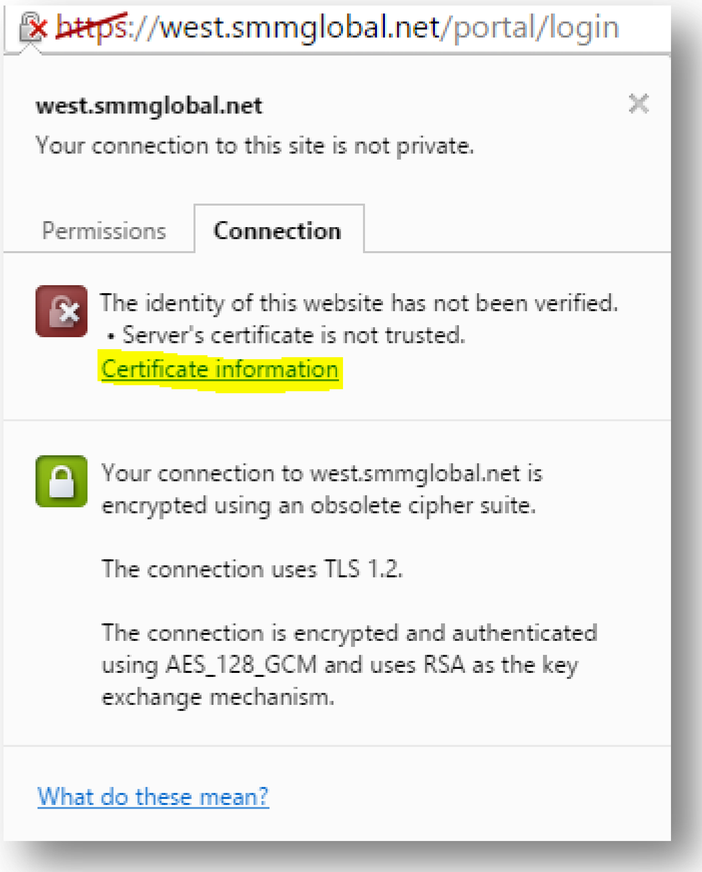
Attackers might be trying to steal your information from **west.smmglobal.net** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically report details of possible security incidents to Google. Privacy policy

This server could not prove that it is **west.smmglobal.net**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to west.smmglobal.net (unsafe)

b. Click on lock icon ~~https~~:/ preceding the URL in the address bar and view the Certificate information:



~~https~~://west.smmglobal.net/portal/login

west.smmglobal.net

Your connection to this site is not private.

The identity of this website has not been verified.
• Server's certificate is not trusted.
Certificate information

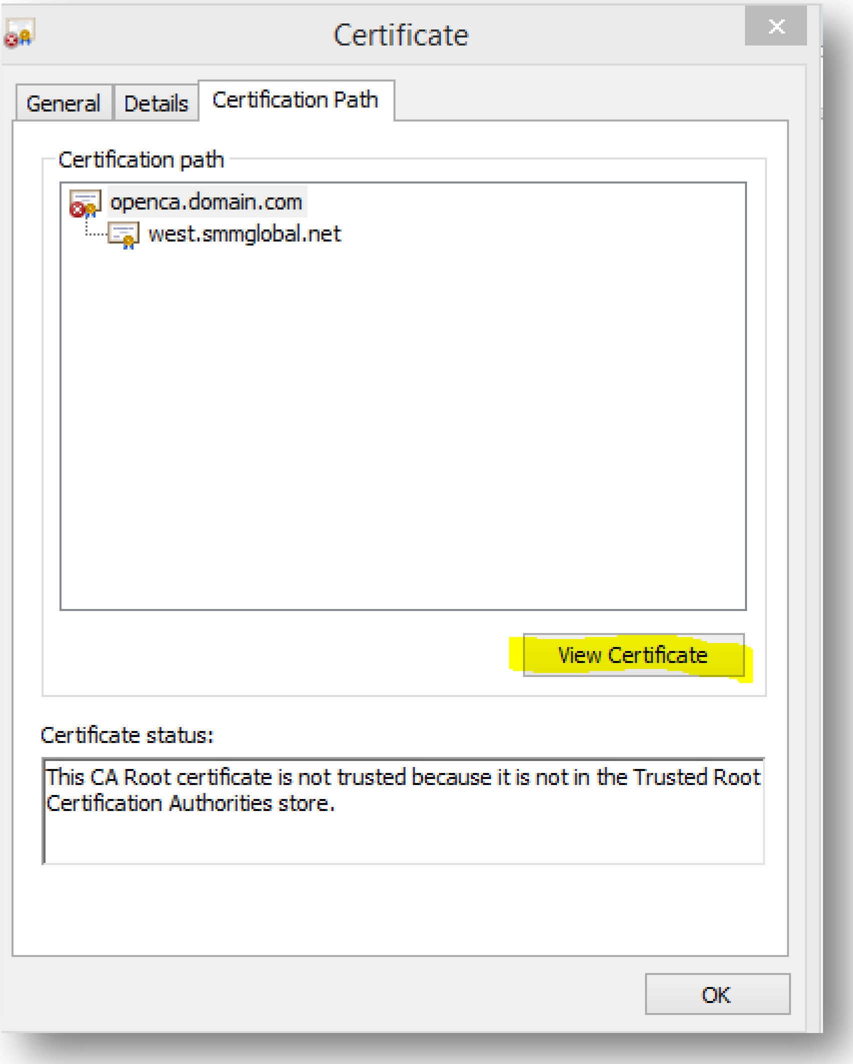
Your connection to west.smmglobal.net is encrypted using an obsolete cipher suite.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES_128_GCM and uses RSA as the key exchange mechanism.

What do these mean?

c. In the certificate viewer window click the "Certification Path" tab, select the certificate one level up from the bottom and click "View Certificate":



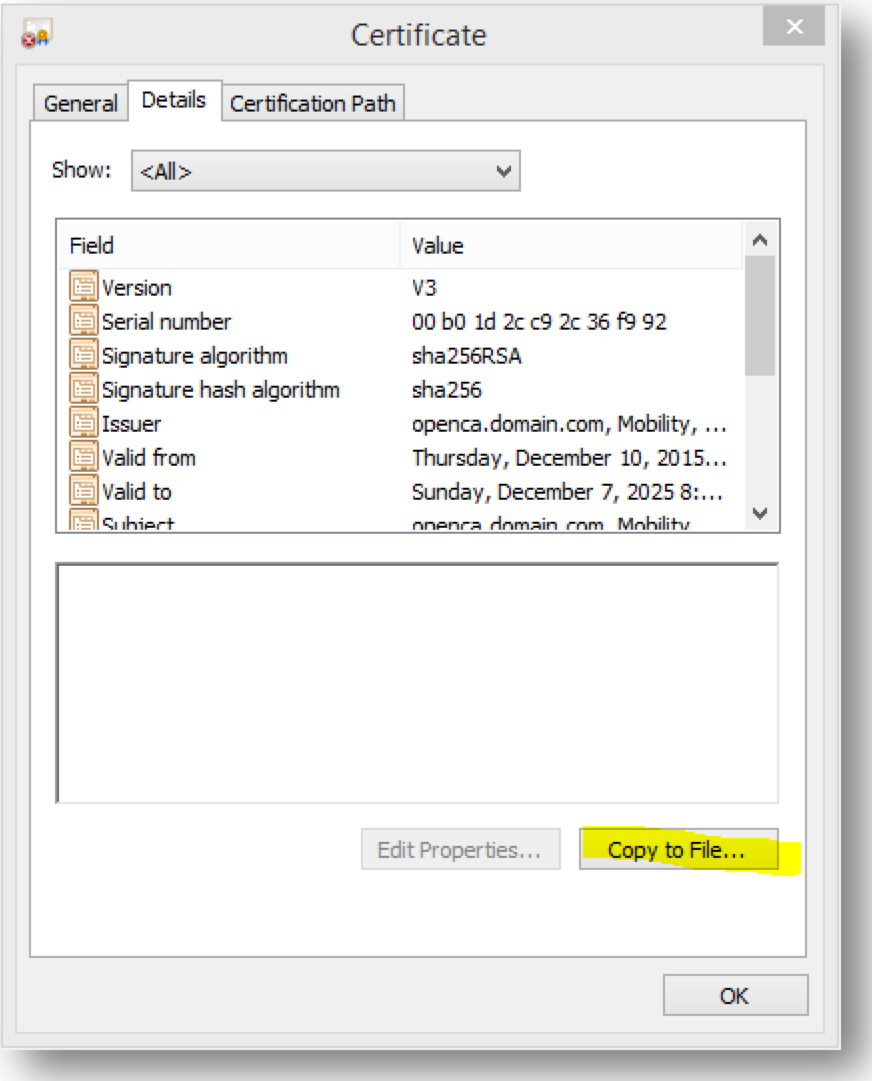
openca.domain.com
west.smmglobal.net

Certificate status:

This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store.

Note: If the root/intermediate certificate is not displayed use the Linux method to extract the CA certificate.

d. A new certificate viewer window will appear showing the details of the intermediate/root certificate. Select the "Details" tab and click "Copy to File":



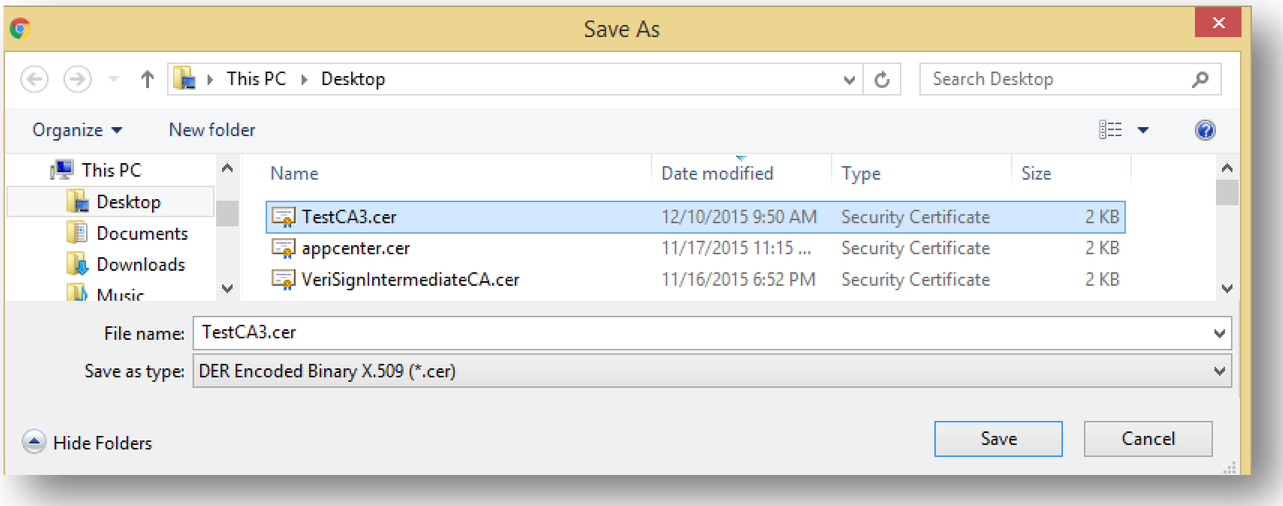
Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	00 b0 1d 2c c9 2c 36 f9 92
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	openca.domain.com, Mobility, ...
Valid from	Thursday, December 10, 2015...
Valid to	Sunday, December 7, 2025 8:...
Subject	openca.domain.com, Mobility

e. In the Certificate Export Wizard click **Next**, ensure DER is selected, click **Next**. Click “Browse” to name and save the certificate to the workstation:



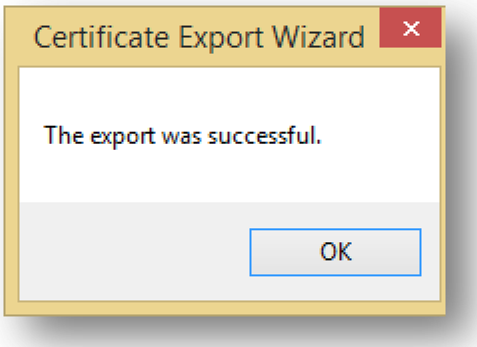
Save As

Name	Date modified	Type	Size
TestCA3.cer	12/10/2015 9:50 AM	Security Certificate	2 KB
appcenter.cer	11/17/2015 11:15 ...	Security Certificate	2 KB
VeriSignIntermediateCA.cer	11/16/2015 6:52 PM	Security Certificate	2 KB

File name: TestCA3.cer

Save as type: DER Encoded Binary X.509 (*.cer)

f. Finally click **Next**, review the certificate details and click **Finish**:



Certificate Export Wizard

The export was successful.

g. The file may now be uploaded to either a file Share site such as Box or an internal website for secure publishing.

Method 2: Using OpenSSL on Linux

a. From an Unix/Linux machine ensure that OpenSSL is installed and updated to the latest version with one of the following commands:

```
#sudo yum -y install openssl
```

Or

```
#apt-get install openssl
```

b. Enter the following command to obtain the issuer certificate and save it to a file named “mycertfile.pem”:

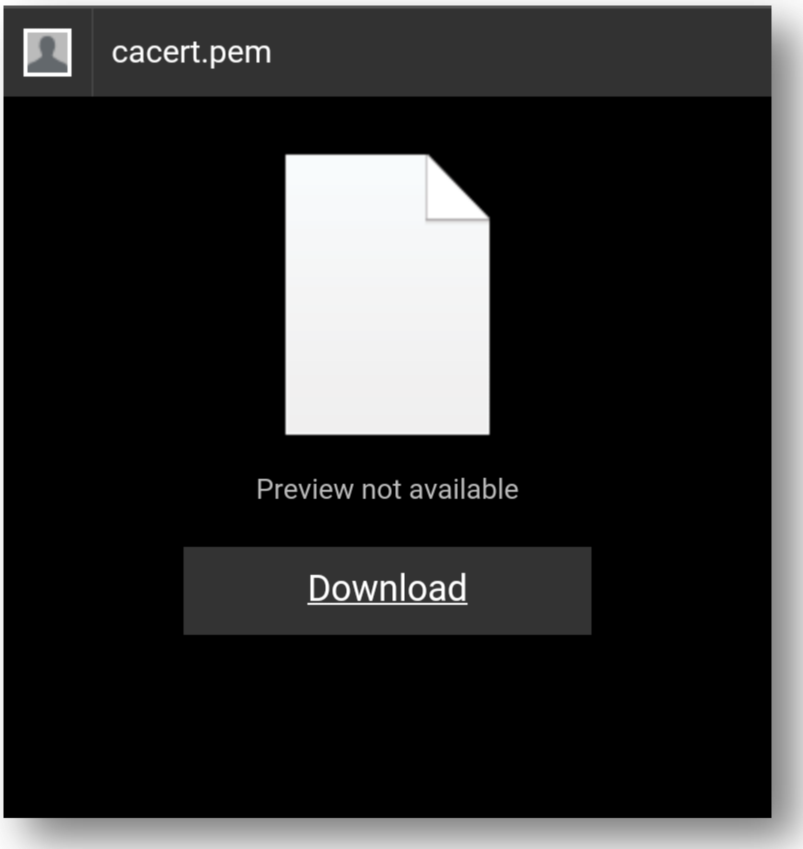
```
# openssl s_client -showcerts -connect <FQDNofMobilityFE>:443 </dev/null 2>/dev/null|openssl x509 -outform DER >mycertfile.pem
```

c. Publish this certificate to a file share service like Box or an internal site accessible by the end-user device.

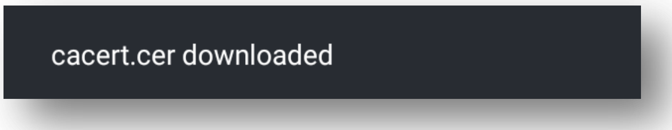
Installing the certificate

Android

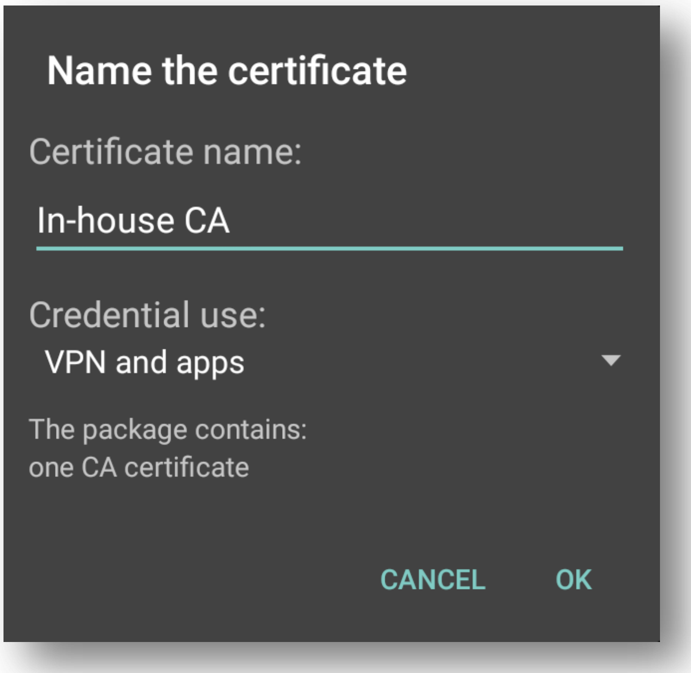
1. Navigate to the site hosting the certificate:



2. Download the certificate:


cacert.cer downloaded

3. Swipe down from the top and tap the download to open the Certificate.
4. Name the certificate and tap **ok**:


Name the certificate

Certificate name:

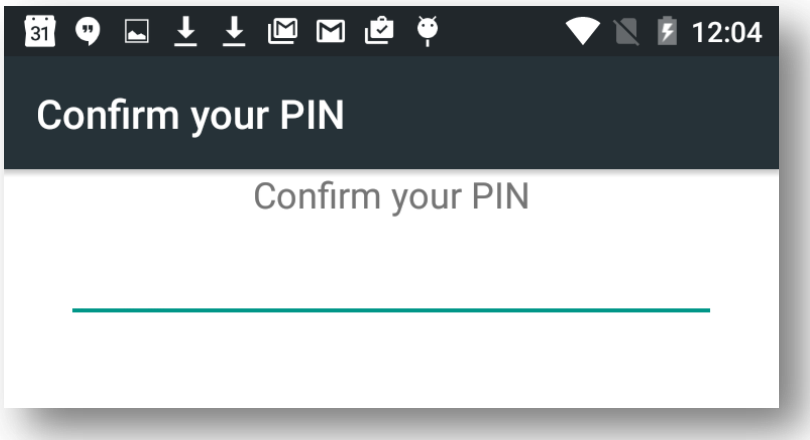
In-house CA

Credential use:

VPN and apps

The package contains:
one CA certificate

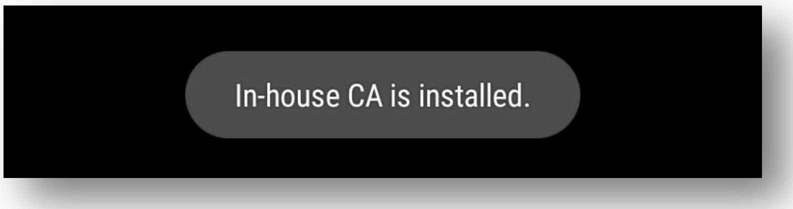
5. If prompted, enter the device PIN/Password:



Confirm your PIN

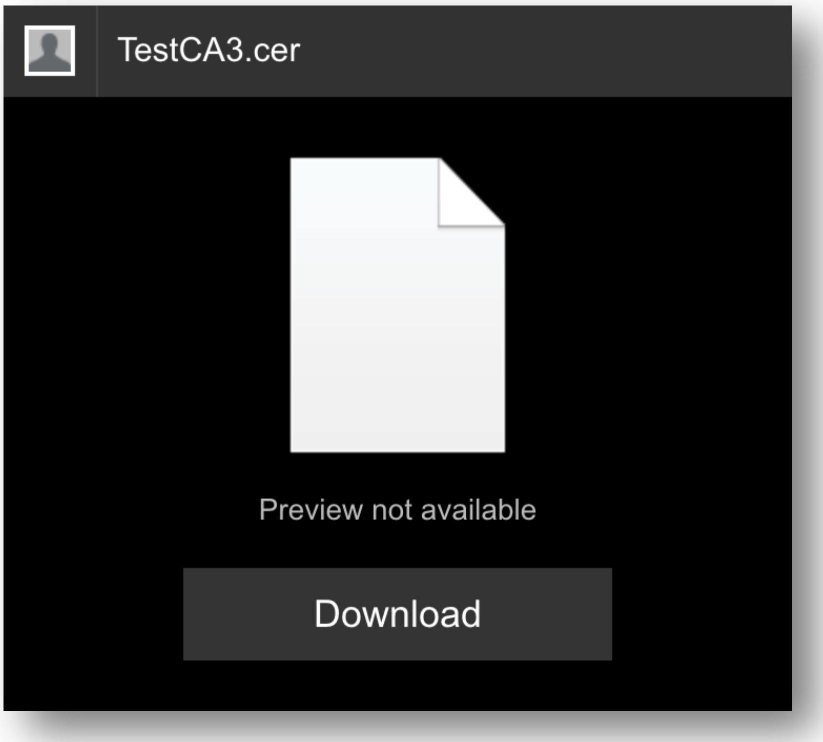
Confirm your PIN

6. A certificate installed message should be displayed:


In-house CA is installed.

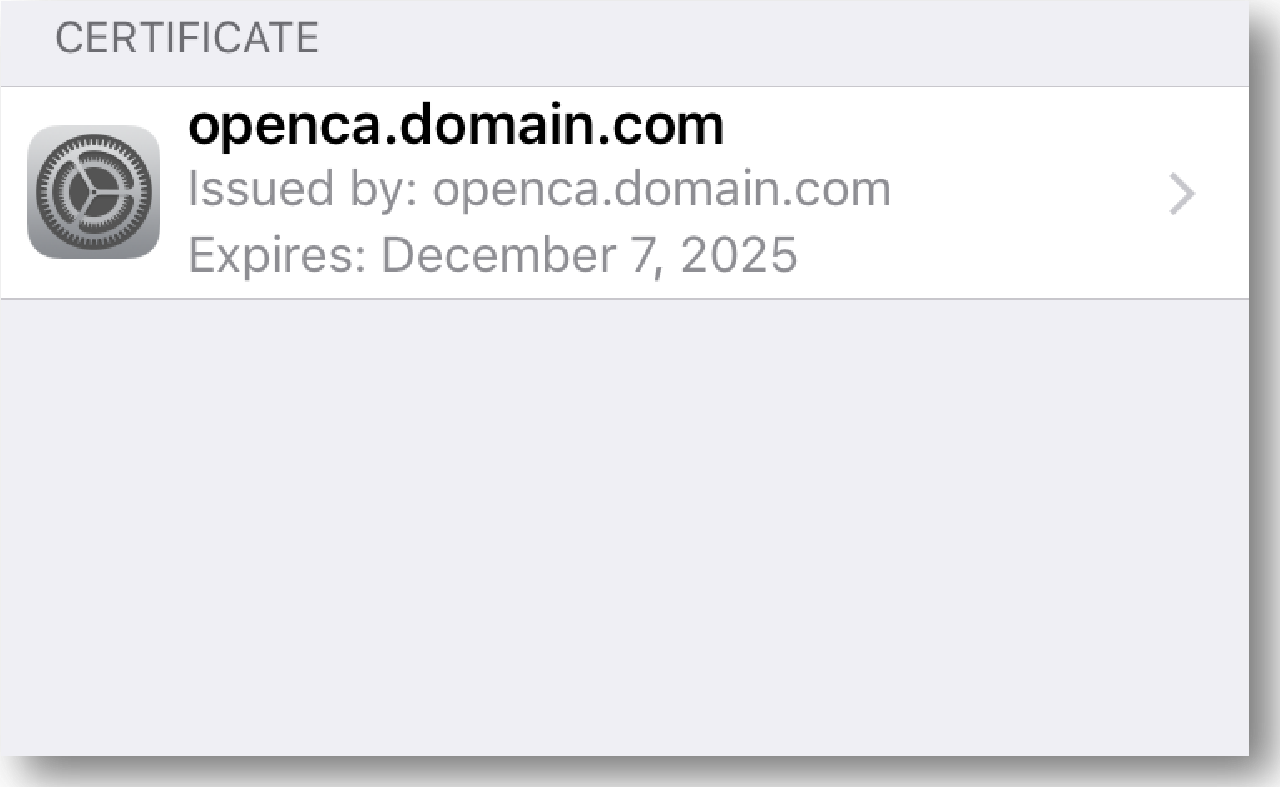
iOS

1. Open Safari and navigate to the company site hosting the certificate:



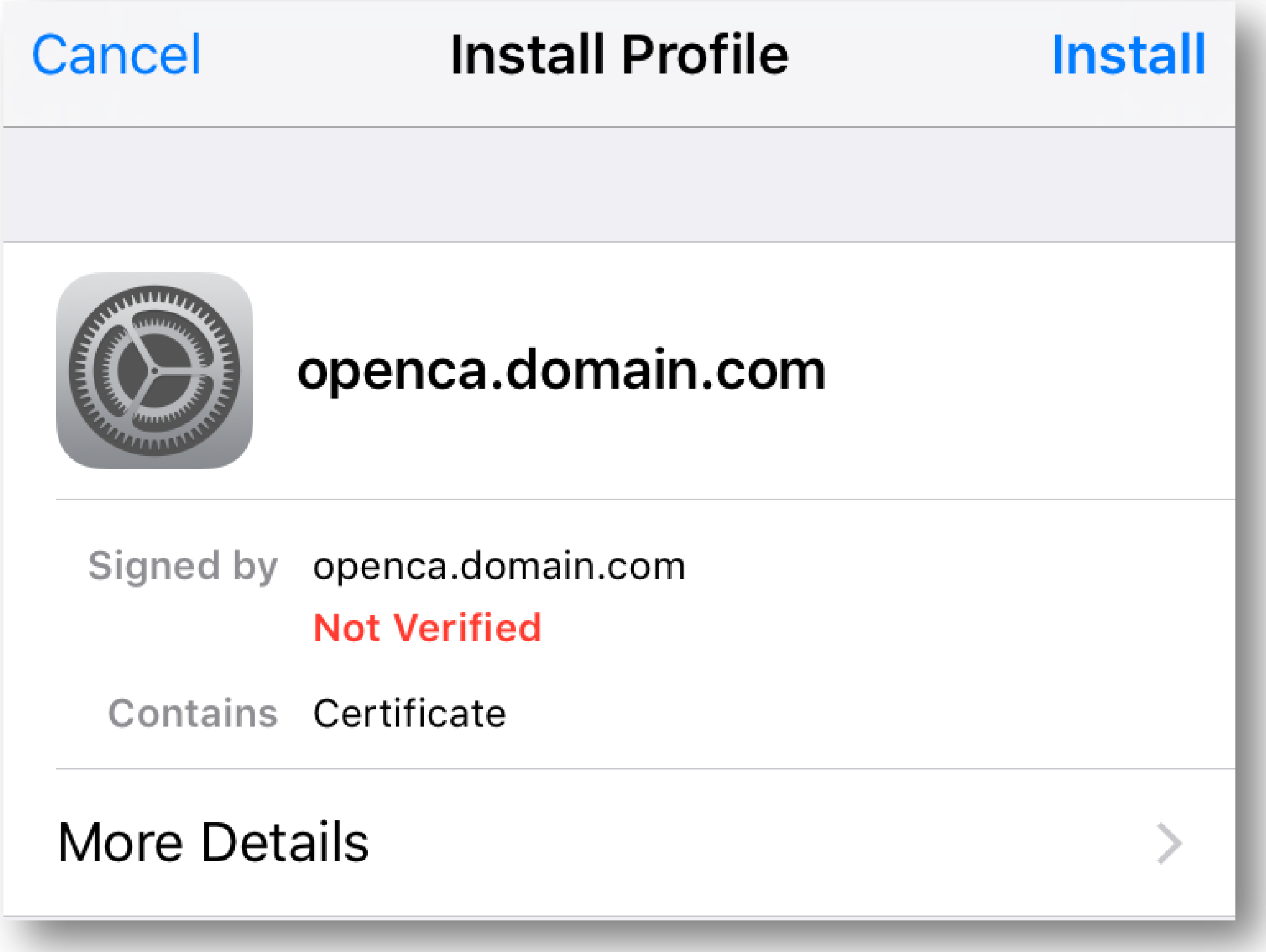
2. After tapping the download link iOS will direct the viewer to an Install Profile wizard. Tap **Install** and enter the device credentials, if prompted.

Important: Tap **More Details** to confirm that this is a **Certificate** and does not contain any management or restrictive profiles, if there any restrictive or device management profiles **STOP** and verify that that the certificate is being downloaded from a reputable source:



CERTIFICATE

openca.domain.com
Issued by: openca.domain.com
Expires: December 7, 2025

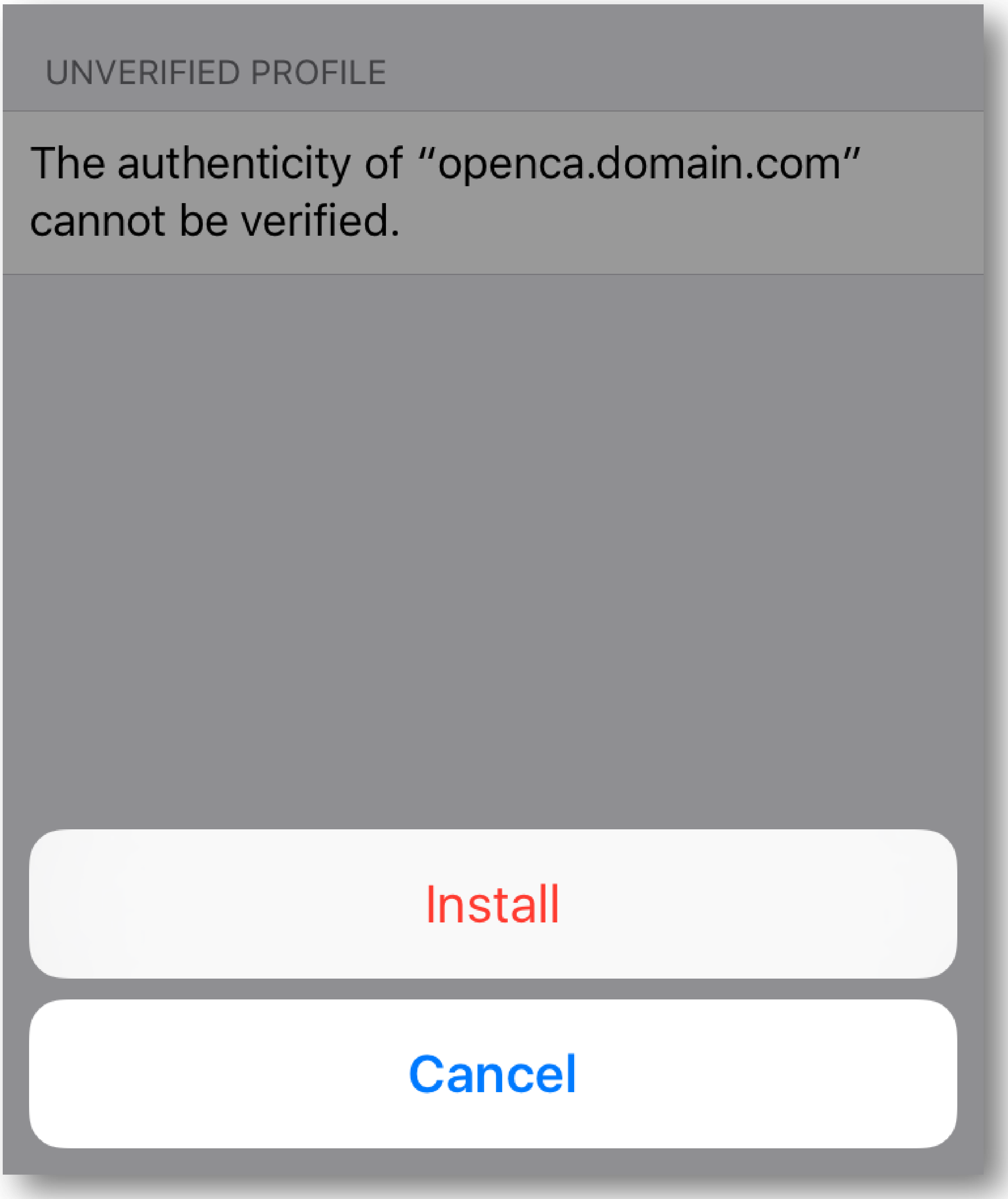


openca.domain.com

Signed by openca.domain.com
Not Verified

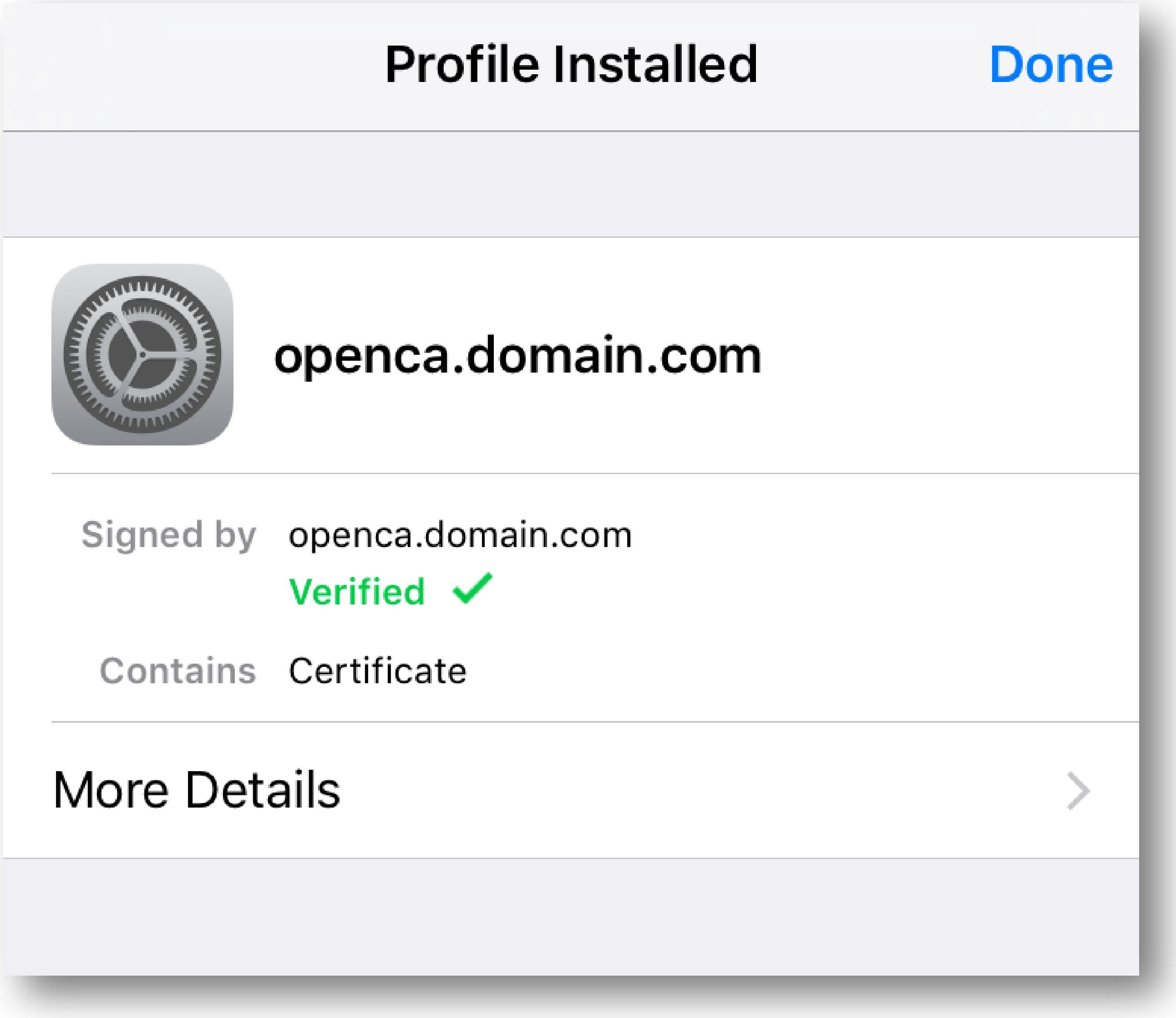
Contains Certificate

3. Tap **Install** from the warning page:


UNVERIFIED PROFILE

The authenticity of “openca.domain.com” cannot be verified.

4. Finally the certificate should show as “Verified”:



openca.domain.com

Signed by openca.domain.com
Verified ✓

Contains Certificate

How to administratively intercept an email sent by a Mobility server where there is no SMTP available

Contents

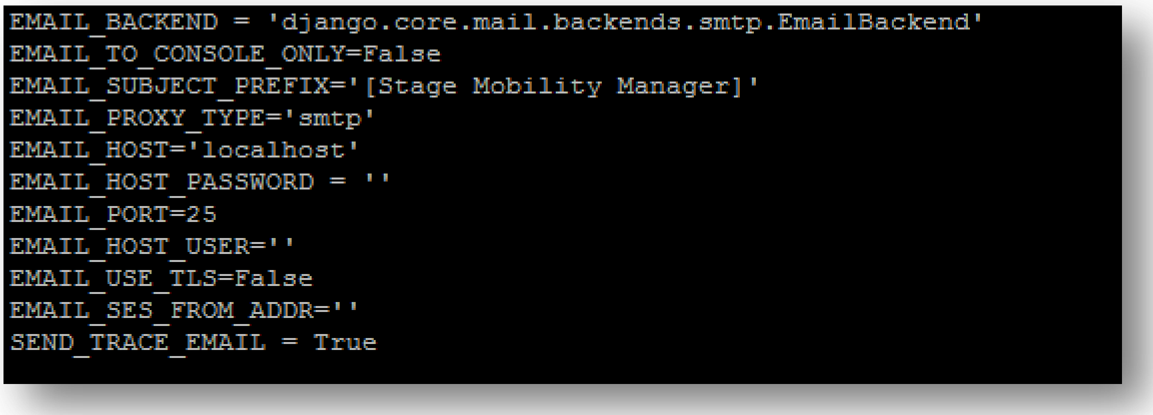
How to administratively intercept an email sent by a Mobility server where there is no SMTP available

Note: These steps are to be used if there is no working SMTP or outbound delivery method available in the environment. For steps on how to connect to an SMTP server see the appendix at the end of this article.

1. Backup the settings configurations found in **/usr/local/nukona/appstore_cu/appstore_cu/settings_local.py**:
   cp /usr/local/nukona/appstore_cu/appstore_cu/settings_local.py /usr/local/nukona/appstore_cu/appstore_cu/.backup_settings_local.py
2. Change the SMTP mail relay after completing the **bootstrapping** process: open a terminal to the FE. As root edit **/usr/local/nukona/appstore_cu/appstore_cu/settings_local.py**:
   vi /usr/local/nukona/appstore_cu/appstore_cu/settings_local.py

EMAIL_PROXY_TYPE='localhost'
EMAIL_HOST='localhost'
EMAIL_HOST_PASSWORD = ''
EMAIL_PORT=25
EMAIL_HOST_USER=''
EMAIL_USE_TLS = False

For example:

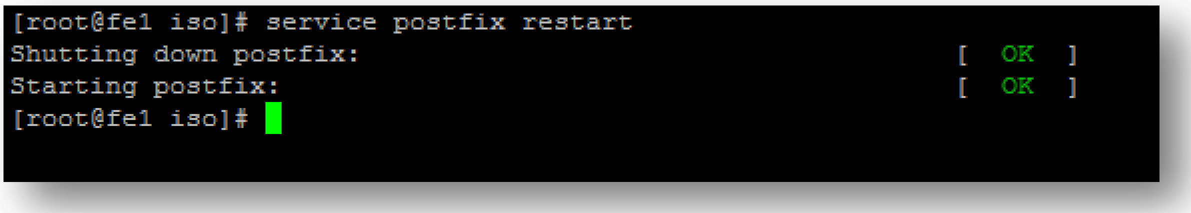


```
EMAIL_BACKEND = 'django.core.mail.backends.smtp.EmailBackend'
EMAIL_TO_CONSOLE_ONLY=False
EMAIL_SUBJECT_PREFIX='[Stage Mobility Manager]'
EMAIL_PROXY_TYPE='smtp'
EMAIL_HOST='localhost'
EMAIL_HOST_PASSWORD = ''
EMAIL_PORT=25
EMAIL_HOST_USER=''
EMAIL_USE_TLS=False
EMAIL_SES_FROM_ADDR=''
SEND_TRACE_EMAIL = True
```

Restart Mobility Services:
sudo /etc/init.d/appcenter-services restart

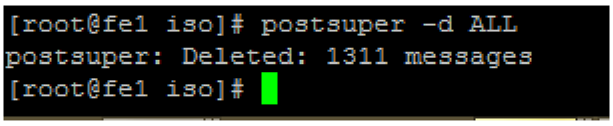
3. Backup the postfix configuration file:
   cp /etc/postfix/main.cf /etc/postfix/.backup_main.cf
4. Comment out any duplicate directives and add the following to the end of the file:

   smtp_sasl_auth_enable = No
   smtp_sasl_security_options = noanonymous
   smtp_tls_security_level = may
   header_size_limit = 4096000
   relayhost = [localhost]:25
5. Restart the postfix services:
   service postfix restart



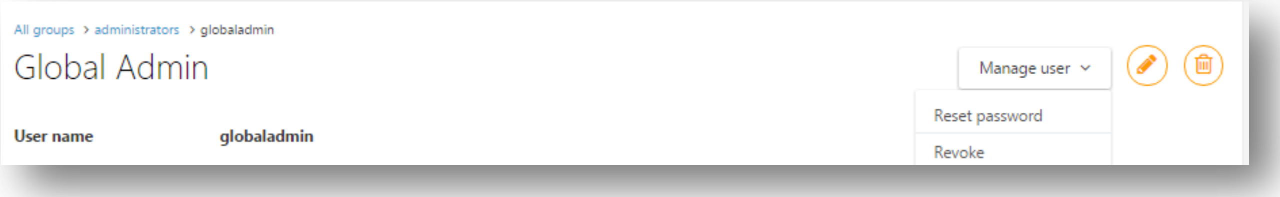
```
[root@fe1 iso]# service postfix restart
Shutting down postfix:                                     [  OK  ]
Starting postfix:                                          [  OK  ]
[root@fe1 iso]#
```

6. Clear the current mailq with the following command:
   postsuper -d ALL



```
[root@fe1 iso]# postsuper -d ALL
postsuper: Deleted: 1311 messages
[root@fe1 iso]#
```

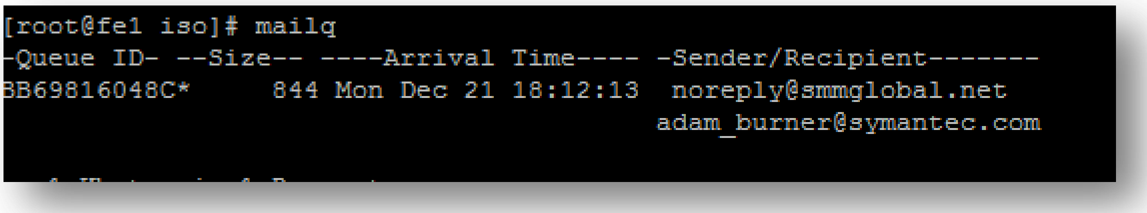
7. From the Mobility admin console, send a reset email to the administrative account:



User name globaladmin

8. View the queue with the following command:
   mailq

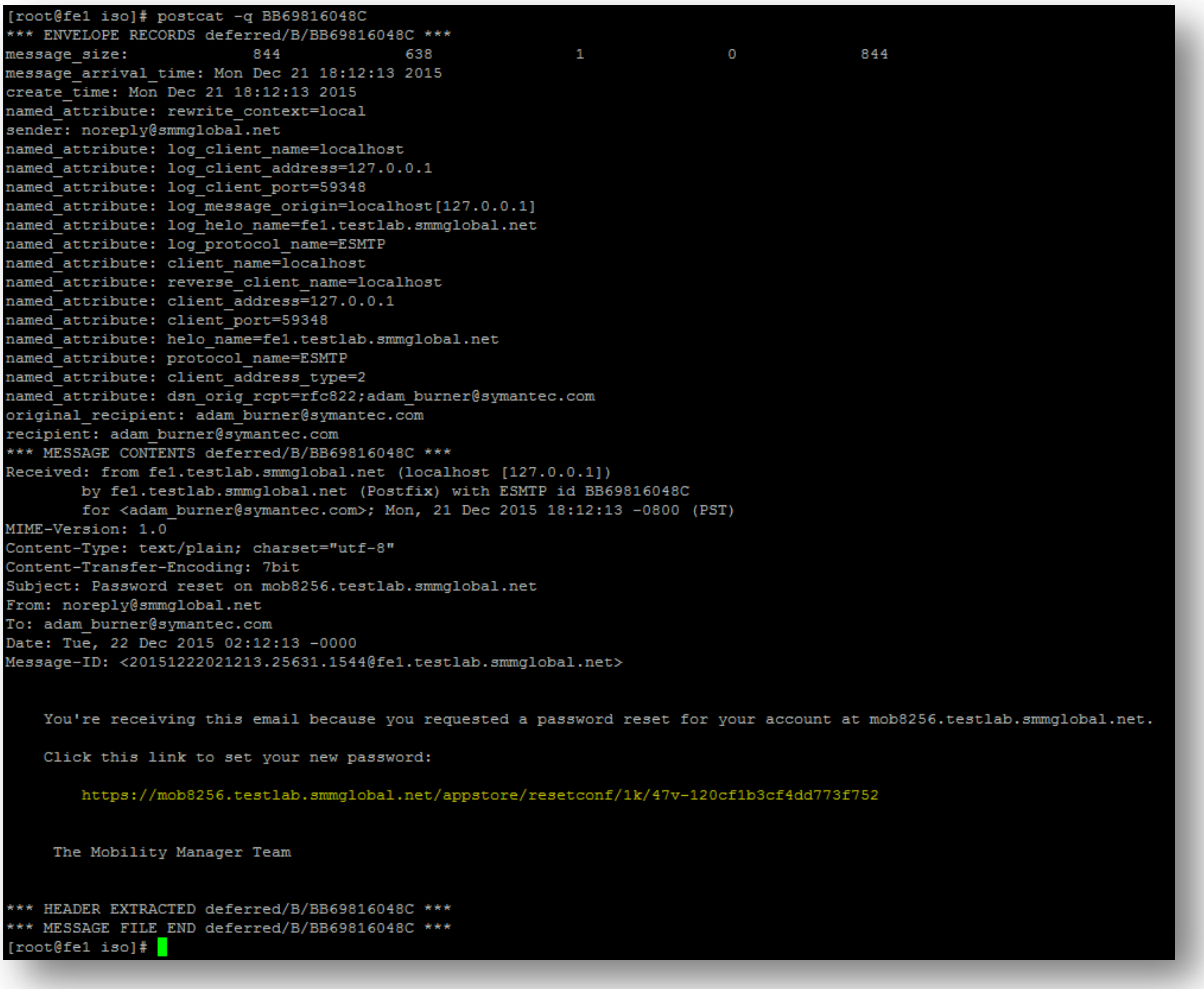
For example:



```
[root@fe1 iso]# mailq
-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient-------
BB69816048C*      844 Mon Dec 21 18:12:13  noreply@smmglobal.net
                                          adam_burner@symantec.com
```

9. Copy the **Queue ID** for the message to the clipboard and enter it into the following:
   postcat -q <QueueID>

   For example:



```
[root@fe1 iso]# postcat -q BB69816048C
*** ENVELOPE RECORDS deferred/B/BB69816048C ***
message_size:            844             638               1               0            844
message_arrival_time: Mon Dec 21 18:12:13 2015
create_time: Mon Dec 21 18:12:13 2015
named_attribute: rewrite_context=local
sender: noreply@smmglobal.net
named_attribute: log_client_name=localhost
named_attribute: log_client_address=127.0.0.1
named_attribute: log_client_port=59348
named_attribute: log_message_origin=localhost[127.0.0.1]
named_attribute: log_helo_name=fe1.testlab.smmglobal.net
named_attribute: log_protocol_name=ESMTP
named_attribute: client_name=localhost
named_attribute: reverse_client_name=localhost
named_attribute: client_address=127.0.0.1
named_attribute: client_port=59348
named_attribute: helo_name=fe1.testlab.smmglobal.net
named_attribute: protocol_name=ESMTP
named_attribute: client_address_type=2
named_attribute: dsn_orig_rcpt=rfc822;adam_burner@symantec.com
original_recipient: adam_burner@symantec.com
recipient: adam_burner@symantec.com
*** MESSAGE CONTENTS deferred/B/BB69816048C ***
Received: from fe1.testlab.smmglobal.net (localhost [127.0.0.1])
        by fe1.testlab.smmglobal.net (Postfix) with ESMTP id BB69816048C
        for <adam_burner@symantec.com>; Mon, 21 Dec 2015 18:12:13 -0800 (PST)
MIME-Version: 1.0
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 7bit
Subject: Password reset on mob8256.testlab.smmglobal.net
From: noreply@smmglobal.net
To: adam_burner@symantec.com
Date: Tue, 22 Dec 2015 02:12:13 -0000
Message-ID: <20151222021213.25631.1544@fe1.testlab.smmglobal.net>


    You're receiving this email because you requested a password reset for your account at mob8256.testlab.smmglobal.net.

    Click this link to set your new password:

        https://mob8256.testlab.smmglobal.net/appstore/resetconf/1k/47v-120cf1b3cf4dd773f752


     The Mobility Manager Team


*** HEADER EXTRACTED deferred/B/BB69816048C ***
*** MESSAGE FILE END deferred/B/BB69816048C ***
[root@fe1 iso]#
```

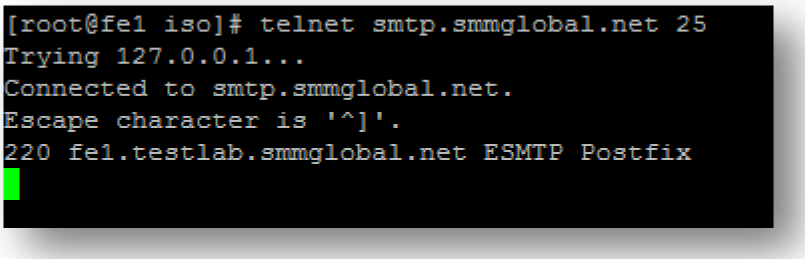
10. Finally enter the URL to reset the administrative password.

Tip: Postfix mail logs are stored in **/var/log/maillog**

Using telnet to confirm SMTP connectivity between the Mobility front-end (FE) and the SMTP server

1. Install telnet client:
   sudo yum -y install telnet
2. Enter the following syntax:
   telnet <FQDN> <PORT>

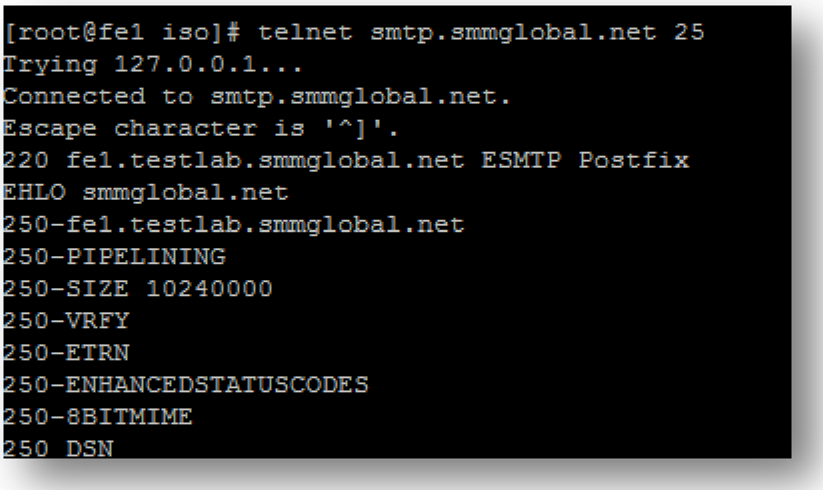
   For example:



```
[root@fe1 iso]# telnet smtp.smmglobal.net 25
Trying 127.0.0.1...
Connected to smtp.smmglobal.net.
Escape character is '^]'.
220 fe1.testlab.smmglobal.net ESMTP Postfix
```

3. Once the above or something like it is displayed, enter the following to manually send a message through the SMTP service.
4. Type the following followed by hitting <enter>:
   EHLO <domain>

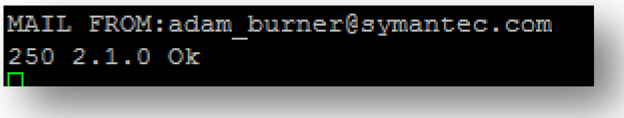
   For example:



```
[root@fe1 iso]# telnet smtp.smmglobal.net 25
Trying 127.0.0.1...
Connected to smtp.smmglobal.net.
Escape character is '^]'.
220 fe1.testlab.smmglobal.net ESMTP Postfix
EHLO smmglobal.net
250-fe1.testlab.smmglobal.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

5. Enter the following as the from address:
   MAIL FROM:<email>

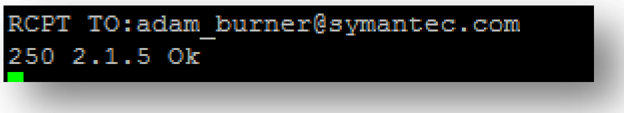
   For example:



```
MAIL FROM:adam_burner@symantec.com
250 2.1.0 Ok
```

6. Enter the recipient's email address:
   RCPT TO:<email>

   For example:

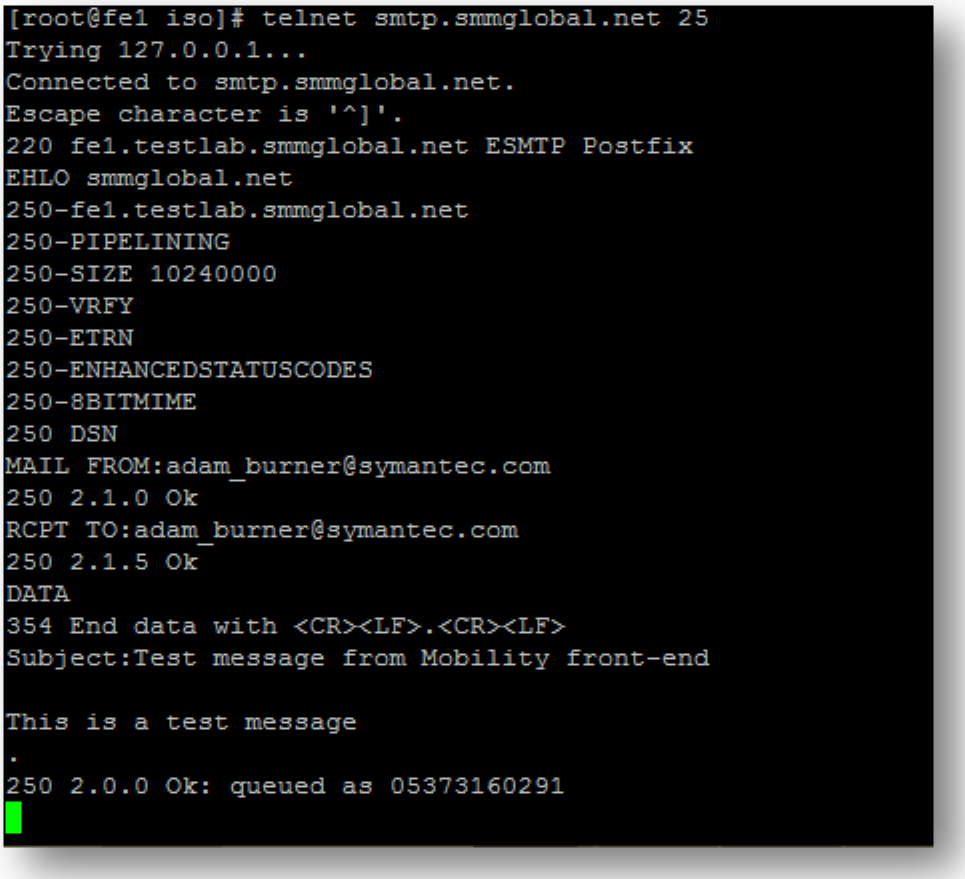


```
RCPT TO:adam_burner@symantec.com
250 2.1.5 Ok
```

7. Type the following command to tell the server that you are ready to send data:
   DATA
8. Type the following:
   Subject: test message from Mobility server

Press Enter twice (there is no response to this action).

9. Now enter the message body:
   This is a test message
10. Type a period at the end of a blank line to send the message:

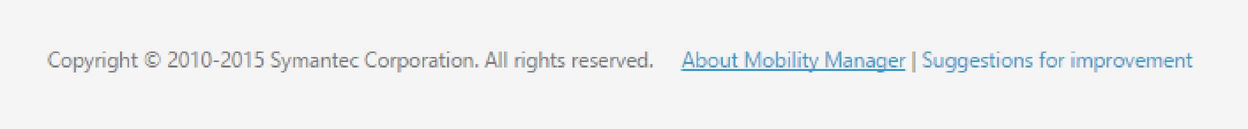


```
[root@fe1 iso]# telnet smtp.smmglobal.net 25
Trying 127.0.0.1...
Connected to smtp.smmglobal.net.
Escape character is '^]'.
220 fe1.testlab.smmglobal.net ESMTP Postfix
EHLO smmglobal.net
250-fe1.testlab.smmglobal.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM:adam_burner@symantec.com
250 2.1.0 Ok
RCPT TO:adam_burner@symantec.com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject:Test message from Mobility front-end

This is a test message
.
250 2.0.0 Ok: queued as 05373160291
```

Bootstrapping and repairing RabbitMQ configuration on a production Mobility front-end

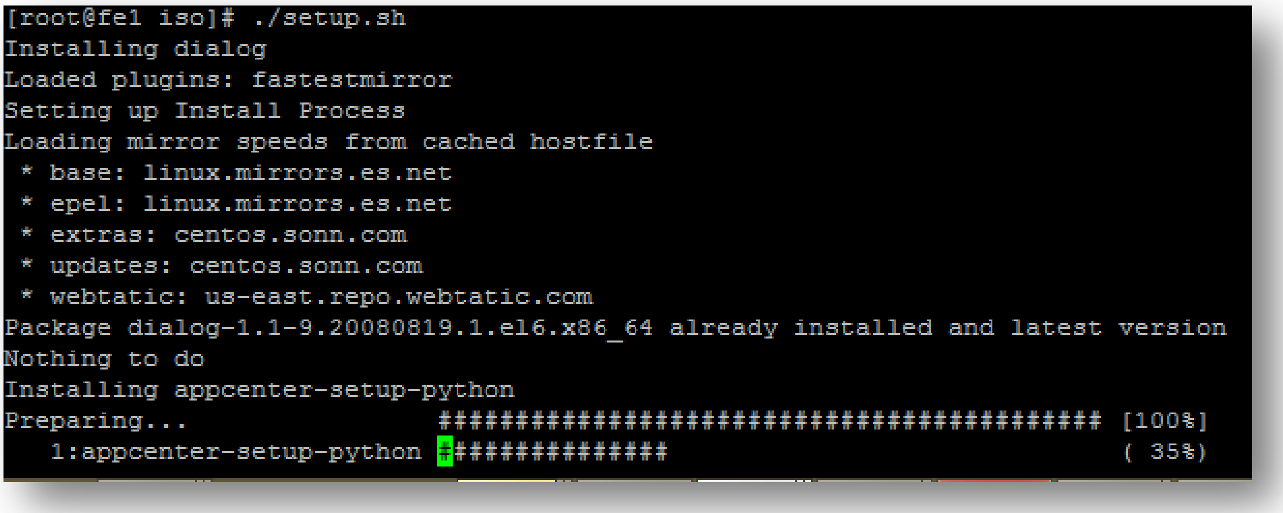
1. Mount the Mobility server's corresponding ISO (5.3 or later) to the system:
   mount -o loop /tmp/symantec_appcenter_5.4.1_Linux_ML.iso /mnt/iso

Note: To find the version, from the admin console select **About Mobility Manager** at the bottom.



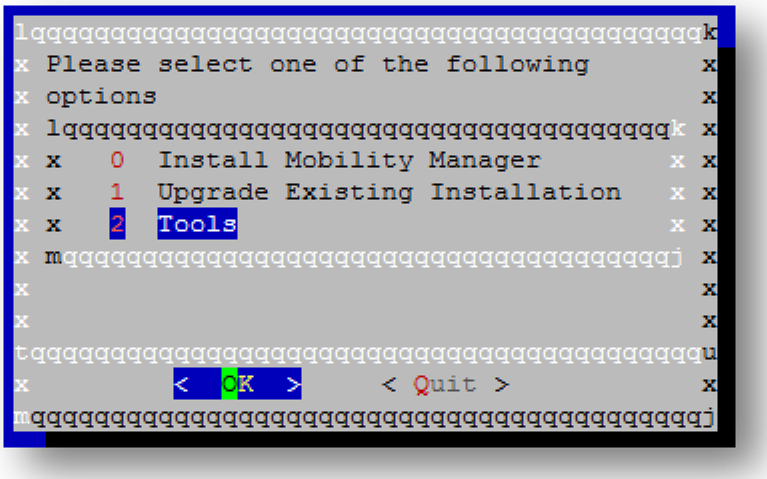
Copyright © 2010-2015 Symantec Corporation. All rights reserved. About Mobility Manager | Suggestions for improvement

2. Run the ./setup.sh utility, as root:
   ./setup.sh



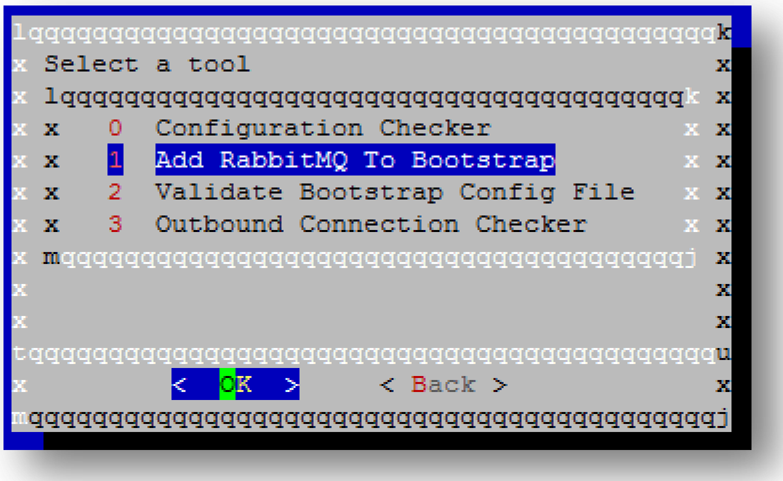
```
[root@fe1 iso]# ./setup.sh
Installing dialog
Loaded plugins: fastestmirror
Setting up Install Process
Loading mirror speeds from cached hostfile
 * base: linux.mirrors.es.net
 * epel: linux.mirrors.es.net
 * extras: centos.sonn.com
 * updates: centos.sonn.com
 * webtatic: us-east.repo.webtatic.com
Package dialog-1.1-9.20080819.1.el6.x86_64 already installed and latest version
Nothing to do
Installing appcenter-setup-python
Preparing...                ########################################### [100%]
   1:appcenter-setup-python ###############                             ( 35%)
```

3. Select **Tools** and <enter>



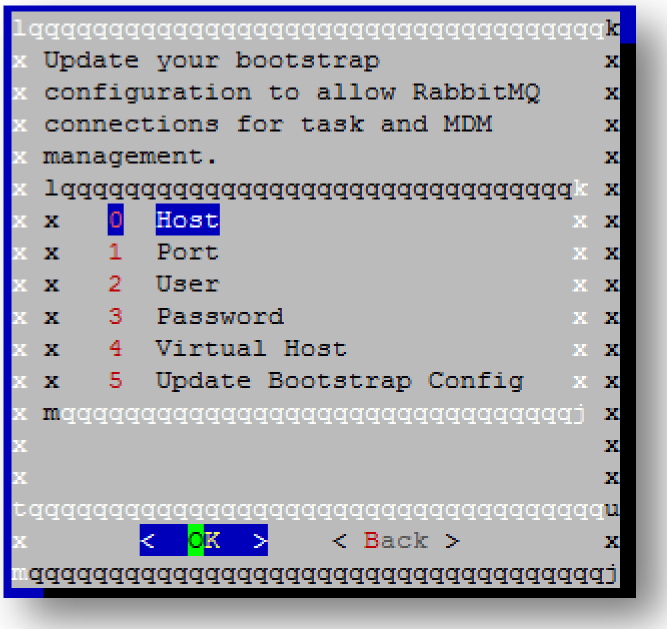
```
Please select one of the following
options
   0   Install Mobility Manager
   1   Upgrade Existing Installation
   2   Tools

           <  OK  >      < Quit >
```

4. Select **Add RabbitmQ To Bootstrap** and <enter>



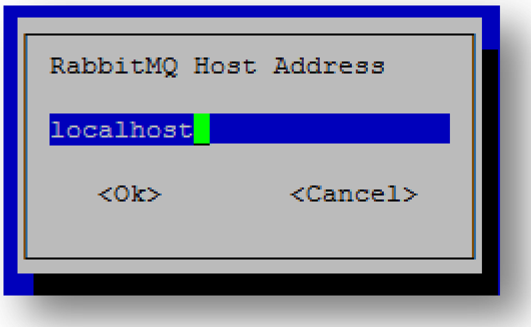
```
Select a tool
   0   Configuration Checker
   1   Add RabbitMQ To Bootstrap
   2   Validate Bootstrap Config File
   3   Outbound Connection Checker

           <  OK  >      < Back >
```

5. Select **Host** and <enter>



```
Update your bootstrap
configuration to allow RabbitMQ
connections for task and MDM
management.
   0   Host
   1   Port
   2   User
   3   Password
   4   Virtual Host
   5   Update Bootstrap Config

         <  OK  >      < Back >
```

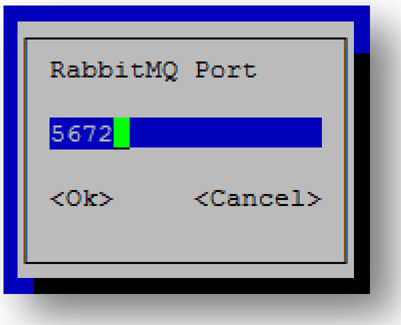
6. Enter the address of the RabbitMQ server. If using a local server, enter **localhost** otherwise use the hostname of the RabbitMQ master server. <enter>



RabbitMQ Host Address

localhost

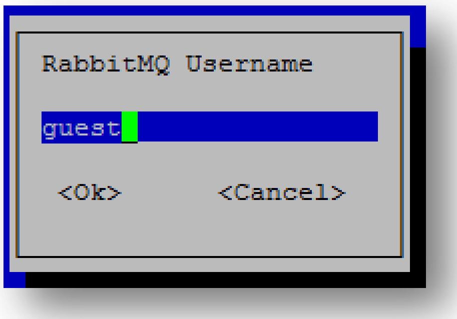
7. Select **Port** and use 5672:



RabbitMQ Port

5672

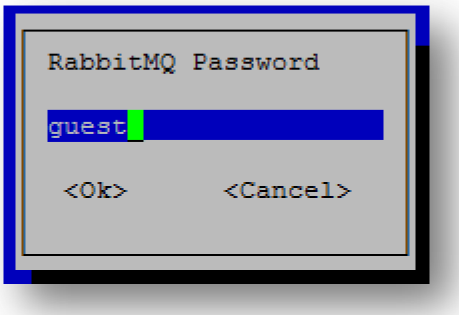
8. For the **User** enter **guest** if a local server is used, otherwise enter the username set during the RabbitMQ installation:



RabbitMQ Username

guest

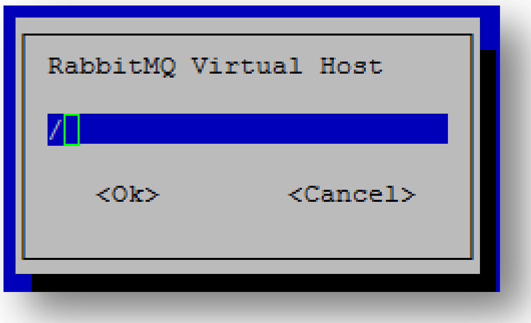
9. For the **Password** also enter **guest** if a local server is used, otherwise enter the password set during the RabbitMQ installation:



RabbitMQ Password

guest

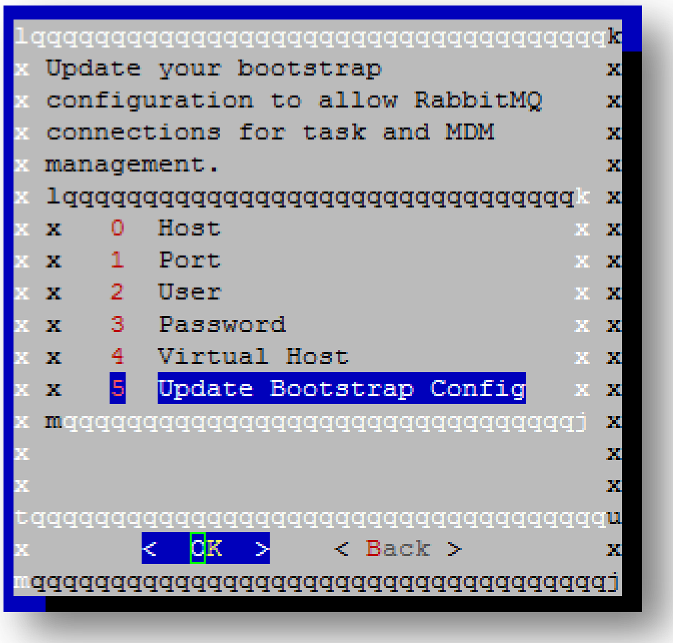
10. For the **Virtual Host** enter **/** if a local server is used, otherwise enter the virtual host as configured during installation:



RabbitMQ Virtual Host

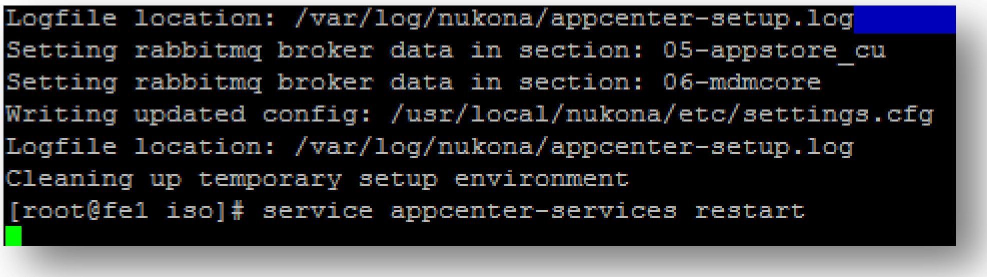
/

11. Select **Upgrade Bootstrap Configuration** and <enter>



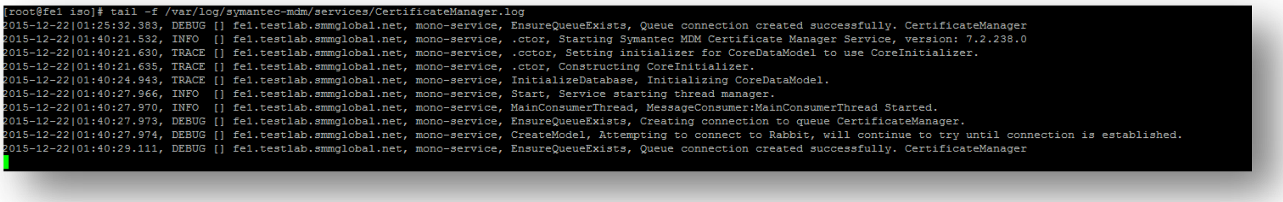
Update your bootstrap configuration to allow RabbitMQ connections for task and MDM management.

12. Restart the appcenter-services, as root:
    service appcenter-services restart



```
Logfile location: /var/log/nukona/appcenter-setup.log
Setting rabbitmq broker data in section: 05-appstore_cu
Setting rabbitmq broker data in section: 06-mdmcore
Writing updated config: /usr/local/nukona/etc/settings.cfg
Logfile location: /var/log/nukona/appcenter-setup.log
Cleaning up temporary setup environment
[root@fe1 iso]# service appcenter-services restart
```

13. Finally tail -f the following log file to determine whether a connection to rabbitMQ was successfully established:
    tail -f /var/log/symantec-mdm/services/CertificateManager.log



```
[root@fe1 iso]# tail -f /var/log/symantec-mdm/services/CertificateManager.log
2015-12-22|01:25:32.383, DEBUG [] fe1.testlab.smmglobal.net, mono-service, EnsureQueueExists, Queue connection created successfully. CertificateManager
2015-12-22|01:40:21.532, INFO  [] fe1.testlab.smmglobal.net, mono-service, .ctor, Starting Symantec MDM Certificate Manager Service, version: 7.2.238.0
2015-12-22|01:40:21.630, TRACE [] fe1.testlab.smmglobal.net, mono-service, .cctor, Setting initializer for CoreDataModel to use CoreInitializer.
2015-12-22|01:40:21.635, TRACE [] fe1.testlab.smmglobal.net, mono-service, .ctor, Constructing CoreInitializer.
2015-12-22|01:40:24.943, TRACE [] fe1.testlab.smmglobal.net, mono-service, InitializeDatabase, Initializing CoreDataModel.
2015-12-22|01:40:27.966, INFO  [] fe1.testlab.smmglobal.net, mono-service, Start, Service starting thread manager.
2015-12-22|01:40:27.970, INFO  [] fe1.testlab.smmglobal.net, mono-service, MainConsumerThread, MessageConsumer:MainConsumerThread Started.
2015-12-22|01:40:27.973, DEBUG [] fe1.testlab.smmglobal.net, mono-service, EnsureQueueExists, Creating connection to queue CertificateManager.
2015-12-22|01:40:27.974, DEBUG [] fe1.testlab.smmglobal.net, mono-service, CreateModel, Attempting to connect to Rabbit, will continue to try until connection is established.
2015-12-22|01:40:29.111, DEBUG [] fe1.testlab.smmglobal.net, mono-service, EnsureQueueExists, Queue connection created successfully. CertificateManager
```

How to uninstall Symantec Mobility Suite

https://www-secure.symantec.com/connect/articles/how-uninstall-mobility-suite-542-and-refresh-dependencies

How to manually add a certificate to the Mobility Java keystore

Problem

The Secure Proxy's NGINX /usr/local/nginx/logs/controller.log file has "Failed to create SSL Connection" on the javax.net.ssl.SSLHandshakeException. This SSL handshake error is preventing the Secure Proxy server from registering to the Symantec Mobility Front End.

This same error may also prevent email sync and push functionality while communicating between the EAS/EWS front ends. See the note below regarding how to use these same steps to resolve other SSL Java related connectivity issues.

Error Message

javax.net.ssl.SSLHandshakeException

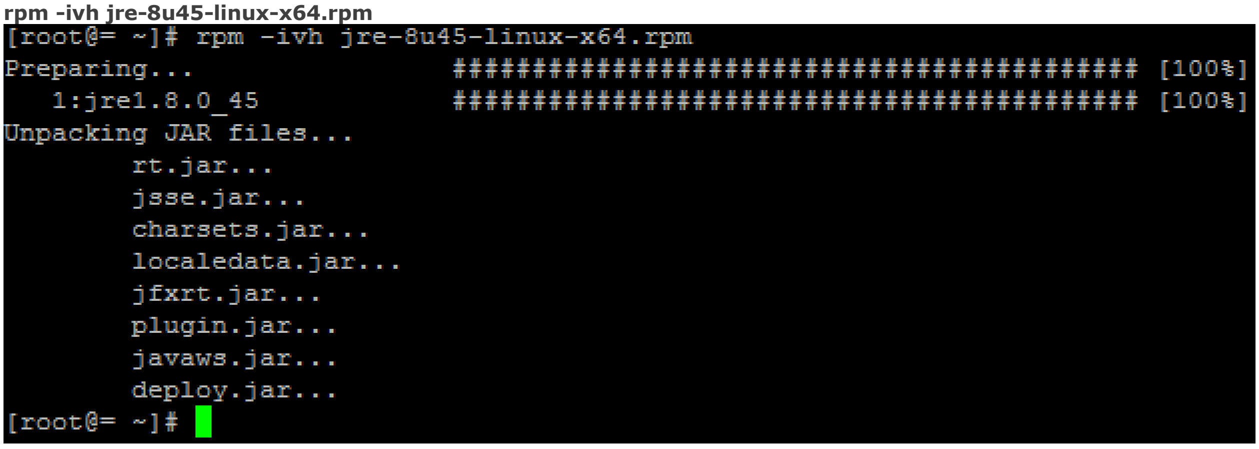
Cause

The SSL certificate installed on the network resource is not trusted by Java.

Solution

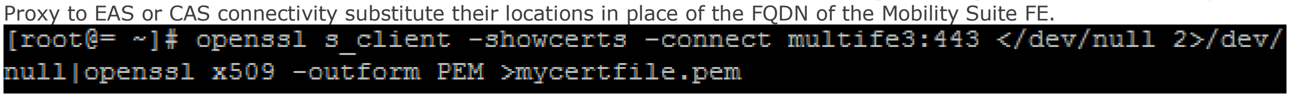
Note: Several things can cause an Secure Proxy server to not be able to register to a Mobility Suite Front End (FE) server or lose it's connectivity thereto. First verify that the server has direct outbound access over TCP 443 to the fully qualified domain name (FQDN) of the FE. Also confirm that a local administrative account is being used to register the Secure Proxy to the FE. Steps 5 and 6 may be repeated substituting the internal CAS/EAS/EWS server FQDN for the Mobility FQDN in the **keytool** command if having this connectivity issue while attempting to send/receive email or register the impersonation account.

1. Verify that Oracle JRE 1.8 or later is installed by entering the following, as root:
   java -version
2. If the output of the above command contains OpenJDK or an earlier JRE version, remove the OpenJRE package by entering the following, as root:
   sudo yum -y remove java
3. Download **find** for **Linux x64** by navigating to http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html
   Tip: For step by step guide on how to transfer files between a Linux and Windows see HOWTO110248.
4. Once the RPM, from step 3, has been transferred to the Secure Proxy server, run the following command, **as root** from the location of the **jre-8u45-linux-x64.rpm** file, to install Oracle JRE:
   rpm -ivh jre-8u45-linux-x64.rpm



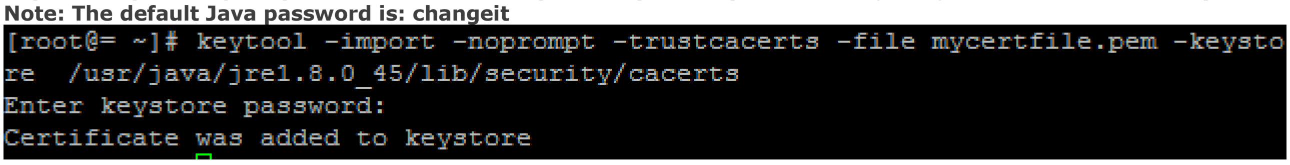
```
[root@= ~]# rpm -ivh jre-8u45-linux-x64.rpm
Preparing...                ########################################### [100%]
   1:jre1.8.0_45            ########################################### [100%]
Unpacking JAR files...
        rt.jar...
        jsse.jar...
        charsets.jar...
        localedata.jar...
        jfxrt.jar...
        plugin.jar...
        javaws.jar...
        deploy.jar...
[root@= ~]#
```

5. Once JRE is successfully installed transfer the SSL certificate, installed on the Mobility Suite FE to the Secure Proxy by entering a command like:
   openssl s_client -showcerts -connect <FQDNofMobilityFE>:443 </dev/null 2>/dev/null|openssl x509 -outform PEM >mycertfile.pem
   Note: The SSL certificate of the Mobility Suite FE has been stored into a file named **mycertfile.pem**. If troubleshooting Email Proxy to EAS or CAS connectivity substitute their locations in place of the FQDN of the Mobility Suite FE.



```
[root@= ~]# openssl s_client -showcerts -connect multife3:443 </dev/null 2>/dev/
null|openssl x509 -outform PEM >mycertfile.pem
```

6. Add the certificate file to the Java trust by entering the following, as root:
   keytool -import -noprompt -trustcacerts -file mycertfile.pem -keystore /usr/java/jre1.8.0_45/lib/security/cacerts
   Note: The default Java password is: changeit



```
[root@= ~]# keytool -import -noprompt -trustcacerts -file mycertfile.pem -keysto
re  /usr/java/jre1.8.0_45/lib/security/cacerts
Enter keystore password:
Certificate was added to keystore
```

   Note: If adding additional certificates for the EAS and CAS servers use the -alias tag to give the certificate a specific name. For example:
   keytool -import -noprompt -trustcacerts -file cascert.pem -alias cascert -keystore /usr/java/jre1.8.0_45/lib/security/cacert

7. Ensure that the latest Secure Email ISO has been downloaded from the Mobility Suite FE by navigating to the Mobility **Admin console > Downloads** and click (**Download secure email proxy**).
   Tip: To get to the Mobility admin console navigate to **https://<FQDNofMobility>/admin/login**

8. Transfer the ISO to the Secure Proxy server.
   Tip: For step by step guide on how to transfer files between a Linux and Windows see HOWTO110248.
9. Create a new mount point for the ISO by entering the following, as root:
   mkdir /mnt/iso
   Tip: If the /mnt/iso directory already has an ISO mounted, close any sessions accessing this location and type, **sudo umount /mnt/iso**
10. Mount the transferred ISO to the **/mnt/iso** directory by entering the following, as root:
    sudo mount -o loop <PathToSecureProxyISO> /mnt/iso
11. Change the terminal's directory to /mnt/iso:
    cd /mnt/iso
12. Remove any previous installation by entering the following, as root:
    sudo ./setup.sh --uninstall
13. After the un-installation completes, re-install by entering the following, as root:
    sudo ./setup.sh --install

14. Complete the installation by following the Mobility Suite Administration Guide