McAfee Install Guide

Mac OS X Installation

Desktop Services

INFORMATION TECHNOLOGY
6356 Agricultural Road, Vancouver, BC V6T 1Z2
www.it.ubc.ca

MNE (Management of Native Encryption)

About MNE:

MNE is a new tool introduced with the release of OS X 10.9. In past versions of McAfee WDE encryption was done on the Whole disk. Because the whole disk was encrypted using a third party program Apple updates had to be applied only when a supported version of McAfee encryption was made available. In most cases this would take anywhere between 3 – 6 months. With the new McAfee MNE, McAfee only acts as a management point. It has the ability to manage encryption state, key escrow and password policy. MNE runs over top of FileVault2 which means that you will not have to worry about updating your OS.

McAfee Agent Installation – Mac

Minimum System Requirements – Mac

Apple Mac Laptop Endpoints (McAfee Endpoint Encryption for Mac only)

- Operating systems
  - Mac OS Mountain Lion (10.8.2 and above)
- Hardware requirements
  - CPU: Intel-based Mac laptop with 64-bit EFI
  - RAM: 1 GB minimum
  - Hard disk: 200 MB minimum free disk space

Install Procedure – Mac OS X

Pre Install Steps:

Hardware Test:

Prior to installing McAfee Endpoint Encryption it is advised to run a full disk scan to confirm there are no bad sectors or general hard drive issues. To do a whole drive scan, follow these steps:

1. Launch Disk Utility, search for it via Spotlight or navigate your way to it via this trail: Finder > Applications > Utilities > Disk Utility.

2. Click on your hard drive from the left panel of the Disk Utility window.
   With your hard drive selected, click the Verify Disk Permissions button. Disk Utility will scan your hard drive.
   You have the Show details button checked, you'll see any irregularities as they're found during the scan.

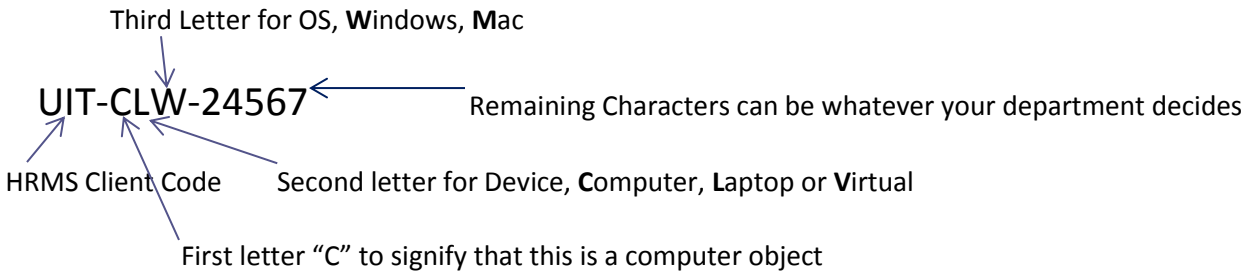
3. When the scan is complete, you can review any of the permissions issues it found in the window in the middle of the Disk Utility window. To repair these issues, click the Repair Disk Permissions button.

Change Host Name:

- Open Terminal Window
- Type the following without brackets (**sudo scutil --set HostName new_hostname**)
  - Note: for the set command there is a double dash. For the "new_hostname" enter in a descriptive hostname to match EAD naming standards.
- Enter your admin password when prompted
- Verify host name change is successful by typing **hostname** in the terminal window

Naming Convention

1. Naming Standard:



2. Reboot when renaming is complete

McAfee Agent Installation – Mac OS X

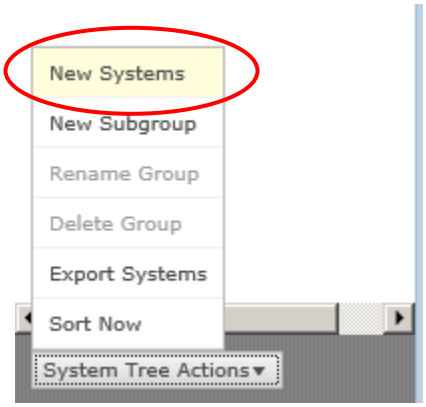
Smart Installer:

The smart installer will place any system into the group which was selected during the creation of the URL. Be sure to select the "Staging Area" group when creating the URL.

Downloading Agent

The installation of the Endpoint Encryption Agent is fairly straight forward.

1. Log onto the ePolicy orchestrator https://137.82.116.22:8443
2. Select System Tree
3. In the pane to the left select the "Staging Area" group
4. From the additional options found under "System tree Actions", Select "New Systems"



5. Select "Create url for client-side download"
6. Select under Agent version: MAC, choose Mcafee Agent for MAC…
7. Download Agent Deployment URL
8. **BEFORE you install the install the agent, rename the computer name**

Post Install Procedure – Mac OS X:

Once the McAfee Agent is installed on the client, the computer object will appear in the Staging Area group within your system tree. Assigning the computer object to a group will provide it with the correct policies. In the event your machine does not appear within the staging area check the Lost & Found group by following the steps below.

1. Log onto the ePO
2. Click **Menu** | **Systems** | **System Tree**
3. Find the group **Lost&Found** in the System Tree to the left.
4. Expand the **Lost&Found** group. The object will be in the group which is the same as the Domain of the computer.
5. Now simply drag-and-drop the computer object(s) in to the staging Area.

Note: When going through the lost and found container confirm that you are only moving Endpoints which you are working with. Once you move your Endpoint into the proper group delete the container in the Lost&Found to keep this area clean.

To move multiple objects at once, simply check the checkboxes to the left of the objects and drag-and-drop the objects in to the appropriate group.

Install and Encrypt

Installing the McAfee agent is only the first step to encrypting a machine. The McAfee agent setups communication between the server and the client. The install of encryption extensions and enablement of encryption will not take place until the machine has been moved into an "Install & Encrypt" Group.

1. Log onto the ePO https://encrypt.it.ubc.ca:8443
2. Click **Menu** | **Systems** | **System Tree**
3. Find the group **Staging Area** in the System Tree to the left.
4. Find the machine which you just installed the McAfee agent in the right hand side of the screen.
5. Once found simply drag-and-drop the computer object(s) in to the correct **Install & Encrypt** group.

Note: Once you have moved the systems into the correct group it may take some time to enable and install. To force the process along follow the instructions listed in the section below.

Forcing Agent Wake-Up

With McAfee endpoint encryption all tasks are completed through the ePO server but can be forced through **Wake Up Agents** and by manually running **Collect and Send Props** on windows or through **terminal commands** on Mac OS X. **Wake Up Agents** (through ePO) and **Terminal Commands** (manually on client machine) are generally used if you would like to either force policy and tasks to computer objects in the event of a policy update or agent update or if you want to force a machine to install encryption extensions while monitoring the endpoint.

Force Commands Mac OS X – Terminal Commands

This process is generally used to force communication with the ePO server as well as to pull down policy and tasks.

1. To monitor the McAfee Agent logs, run the command **sudo tail –fF /Library/McAfee/cma/scratch/etc/log** and provide the administrator password when prompted.
2. To force sending and collection of properties and polices run the following command in terminal **sudo /Library/McAfee/cma/bin/cmdagent –p –c –f** (run each switch separately)

User Management

Because McAfee only manages the enablement of FileVault2 all user management is done through the FileVault2 preferences page on within OS X.

For instruction on how to enable users in filevault2 follow the link below…

http://support.apple.com/kb/ht4790

FileVault2 Key Import

If you have a machine which was previously encrypted using FileVault2 you have 2 options for these systems.

1. Prior to installing and configuring the McAfee agent and MNE you will want to confirm that FileVault2 is enabled and that the user has a copy of the recovery key. If the user still has their recovery key then you can manually import the key to ePO.
2. If the user does not have the FileVault recovery key then you will need to first decrypt the machine and then follow the process above to install and encrypt.

Note: If at all possible you should always allow McAfee to enable FileVault2 encryption. This will make certain that the setup is correct and that the key has been properly sent to the server.