Issue Date: 2004-03-10
Last Updated: 2017-12-17
Updated By: Lisa Mildon
Revision: 1.3

INFORMATION TECHNOLOGY

ENDPOINT MANAGEMENT MANUAL

Table of Contents

Introduction

The following document details the processes and procedures followed by Tulsa IT staff in managing university-owned endpoints. This manual should enable IT staff to manage and configure an endpoint from the time it arrives on campus to the time it is removed from production and disposed. Included in the manual are the baseline standards for endpoints being placed on the OU-Tulsa network. Additionally, technical instructions and inventory management procedures are included for use by Tulsa IT staff. All Tulsa IT staff should conform to and abide by the information and instructions contained in this manual. Each procedure found in the manual is available on the OU-Tulsa IT team collaboration site https://share.ou.edu/sites/IT/tulsa/CS/default.aspx. The information contained here will be reviewed annually and updates will be made as they are needed.

Issue Date: 2015-07-27
Last Updated: 2016-12-06
Updated By: Lisa Mildon
Revision: 1.2

Endpoint Management Standards

The following controls are required for all endpoints deployed at OU-Tulsa and placed on the network:

- Client Management
  - Active Directory
    - Member of the university active directory
    - Subjected to all university global group policies (GPO)
    - Follows standard naming convention. (See page 15.)
  - Antivirus
    - Member of the university anti-virus solution (McAfee Antivirus)
    - Configured to provide automatic virus definition updates on at least a daily basis
    - Configured to provide centralized alerting and reporting of malware infections
  - Patch management
    - Member of OU-Tulsa patch management process
    - Enforce at least monthly patching of critical security vulnerabilities, which includes Microsoft updates
    - McAfee Antivirus will be updated automatically as updates are released
    - Palo Alto transmits patches as they are developed by company support team
  - Vulnerability management
    - Member of a university vulnerability scanning group (Tripwire)
    - Vulnerability scanning performed once monthly
    - IT staff will review reports and remediate all vulnerabilities based on the following schedule:

Vulnerability Rating	Time
Medium	1 month
High	1 week
Critical	ASAP

  - Inventory Management
    - All Endpoints must have an entry in the Service Now inventory
    - Records must meet minimum standard set by IT: see page 23

- Client Configuration
  - Secure baseline
    - Client must run a university- and vendor-supported operating system
    - Client configuration based on Microsoft baselines (preferably configured via GPO)
    - IT will create and utilize system images with built-in baseline configurations
    - Mobile devices (laptops) must be encrypted utilizing university approved encryption software (McAfee Endpoint Encryption): see page 16

Issue Date: 2015-07-27
Last Updated: 2016-12-06
Updated By: Lisa Mildon
Revision: 1.2

- Accounts
  - Users of endpoints will be granted local administration rights based on user's role. Faculty, Administrative staff, and laptop owners will be granted administration rights with the exception of residents
  - The domain administrators group must be a member of the local administrators group
  - The OUHSC\TULSA-DesktopAdmins account must be a part of the local administrators group. OUHSC\Tulsa-MedInfo Admins will be a part of the local administrators group on all clinical endpoints

- Logging
  - Local event logging enabled
    - Logging levels—system events

- Other
  - Customer must not install or use software of the following types:
    - P2P file sharing applications. See: http://it.ouhsc.edu/policies/Peer-to-peer.asp

  - The following security measures will apply to each endpoint:
    - Compromised or malware infected systems will have their network connections disabled immediately to prevent spread of infection or exfiltration of data
    - Sensitive university data should not be stored locally to the desktop hard drive
    - Endpoints must not access third party mail providers
    -

Additional Requirements to be placed on HSCACCESS wireless Network:

- Device must be encrypted
  - Laptops and tablets with a full OS with must have full disk encryption
  - Mobile devices will utilize Secure Mobile via email app
- Device must have an inventory record in ServiceNow
- Device must be whitelisted in InfoBlox
- Laptops and tablets with a full OS should have:
  - McAfee Agent
  - McAfee Antivirus (PC) or Endpoint Security (Mac)
  - GlobalProtect Client

Issue Date: 2009-10-06
Last Updated: 2016-06-15
Updated By: Lisa Mildon
Revision: 2.1

New PC Deployment Protocol

Purpose: To provide required steps and processes needed for the deployment of new computers.

Scope: This document covers the steps and processes related to Client Services configuration and deployment of new computers.

Definitions:

CS – Client Services

Procedure:

1. Upon arrival of order, work order becomes available for building, configuration and deployment
2. CS technician checks work order for any specific instructions.
3. Create computer account in AD (Tulsa or Sooner).
    a. Must use the following naming convention:
        i. For OUHSC PC's: OUT-dept-username (or may be location, something unique)
        ii. For College of Education PC's: EDUC-location
        iii. For Arts and Sciences
        iv. Tulsa Grad College TGC- location
    b. In the description line, enter the model, service tag\serial number and warranty expiration date.
4. Image PC with image off PXE (\\out-wds\REMINST\Images)
5. Change name of PC to match the new name in AD.
6. Put PC on domain.
7. Apply any Microsoft, McAfee or anti-spyware updates.
8. If PC is a laptop then encrypt laptop with McAfee Endpoint Encryption
9. Contact purchaser and\or end-user to get any specific installation instructions.
    a. Special software.
        i. New license or transfer of license.
    b. Printers installed.
    c. Other hardware.
    d. New or existing user.
        i. If existing user, either notify them to backup personal files or offer assistance.
    e. What date\time would be best for installation?
10. Input Inventory information into Service Now (see p. 23 Inventory Updating Procedure)

Enforcement: Failure to comply will be met with appropriate disciplinary action as determined by the OU standards for Positive Discipline included in *The University of Oklahoma Staff Handbook*

Issue Date: 2009-10-06
Last Updated: 2016-06-15
Updated By: Lisa Mildon
Revision: 2.1

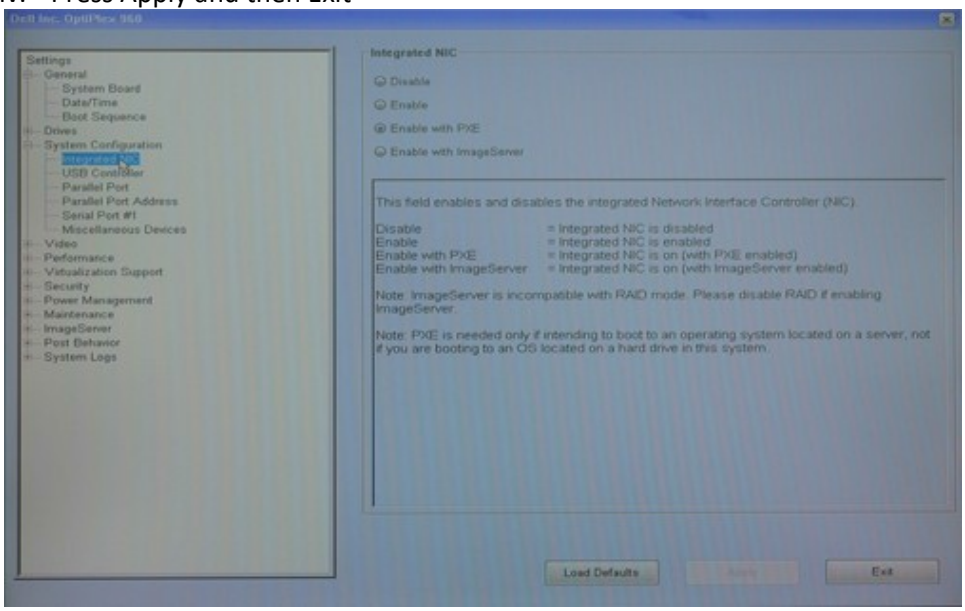
Upgrade a Computer by Use of PXE

1.0 Purpose
This document sets out to provide the steps needed to (re)image a computer to run Windows 7 via the use of PXE over the OU-Tulsa network

2.0 Scope
This document applies to any computer (desktop and laptop) owned by or operated by OU-Tulsa, associated departments, clinics, off-site clinics and affiliates that connect to the OU-Tulsa network

3.1 Policy
3.2 Steps for PC and Laptop

1. Log into PC and
    a. Record PC Name
    b. Record printers installed
    c. Record non-standard software installed
    d. Back-up user files in the following folders - Desktop, My Documents, Favorites
    e. Back-up Outlook .pst files (if Outlook is setup and in use)
        i. Reboot PC
2. On system boot, insure the NIC is bootable (image 1)
    a. Press F12 to bring up boot options.
        i. Go to System Config
        ii. Integrated NIC
        iii. Enable with PXE
        iv. Press Apply and then Exit

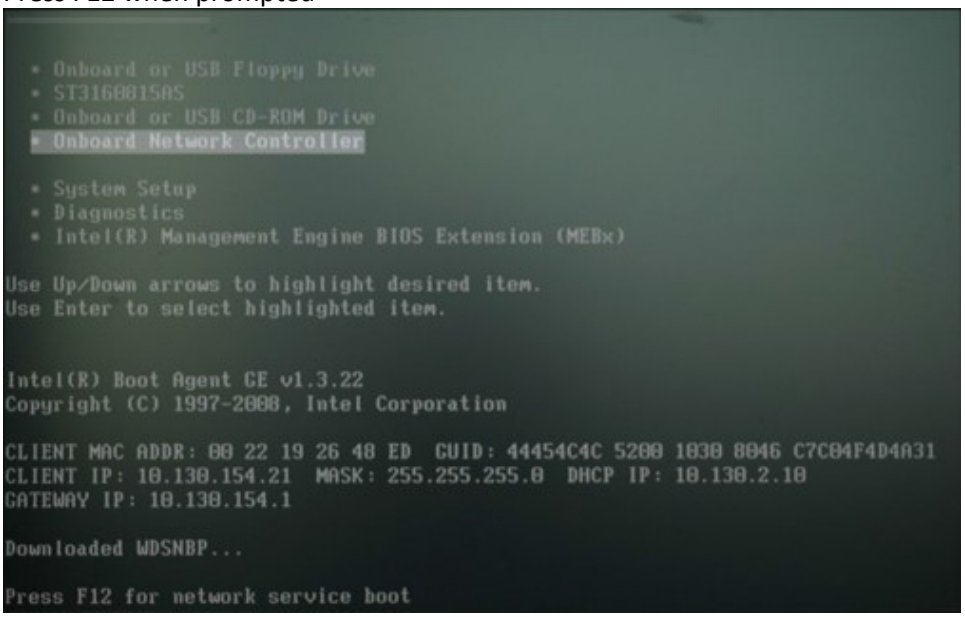


(image 1)

3. For older system SATA operation will need to be set.
    a. Under Drives-SATA Operation, select AHCI.
4. Press F12 to bring up boot options (image 2)
    a. Select Onboard Network Controller

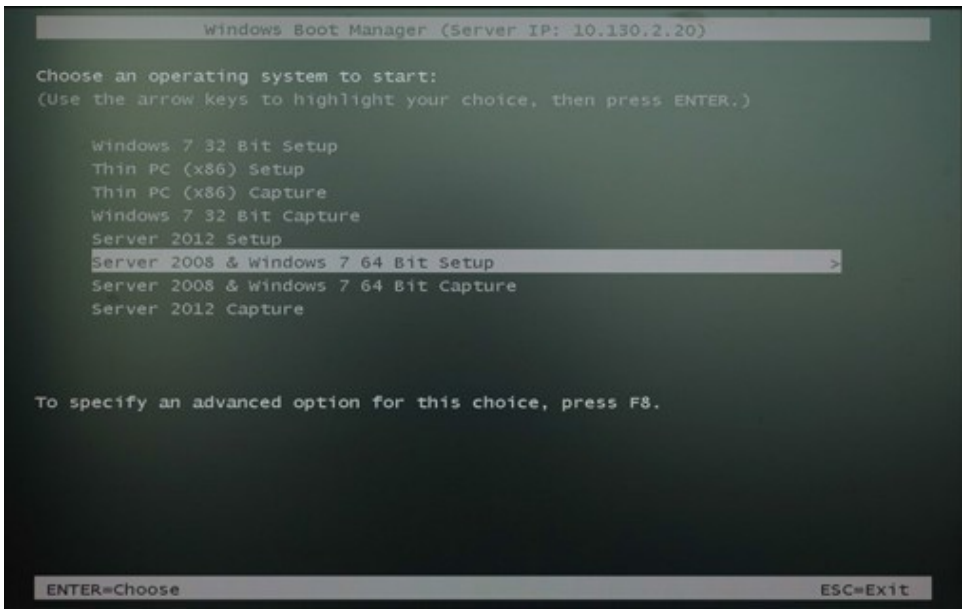
Issue Date: 2009-10-06
Last Updated: 2016-06-15
Updated By: Lisa Mildon
Revision: 2.1

b. Press Enter
c. Press F12 when prompted



(image 2)

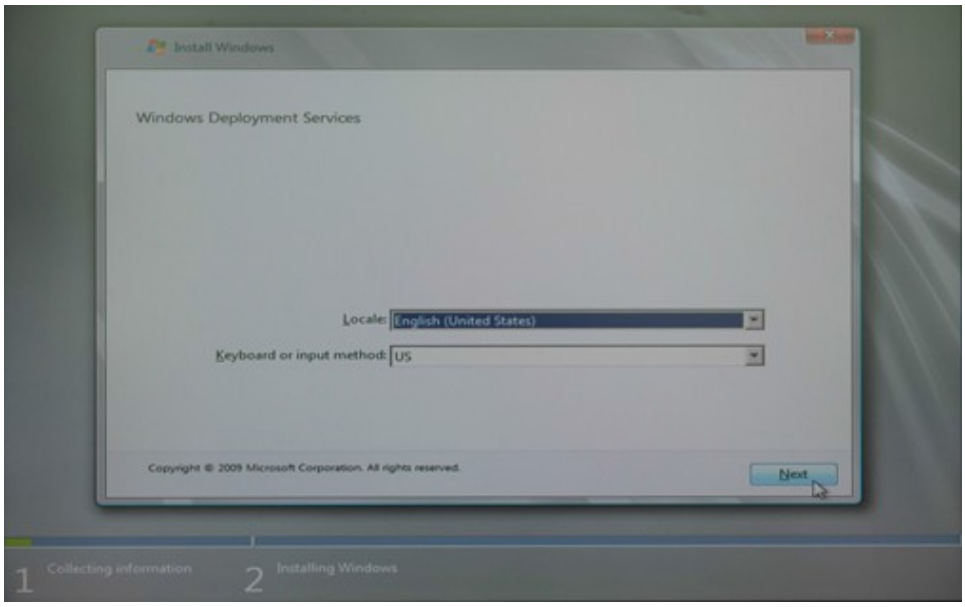
5. Select “Server 2008 & Windows 7 64bit setup” (image 3)
   a. Press Enter



(image 3)

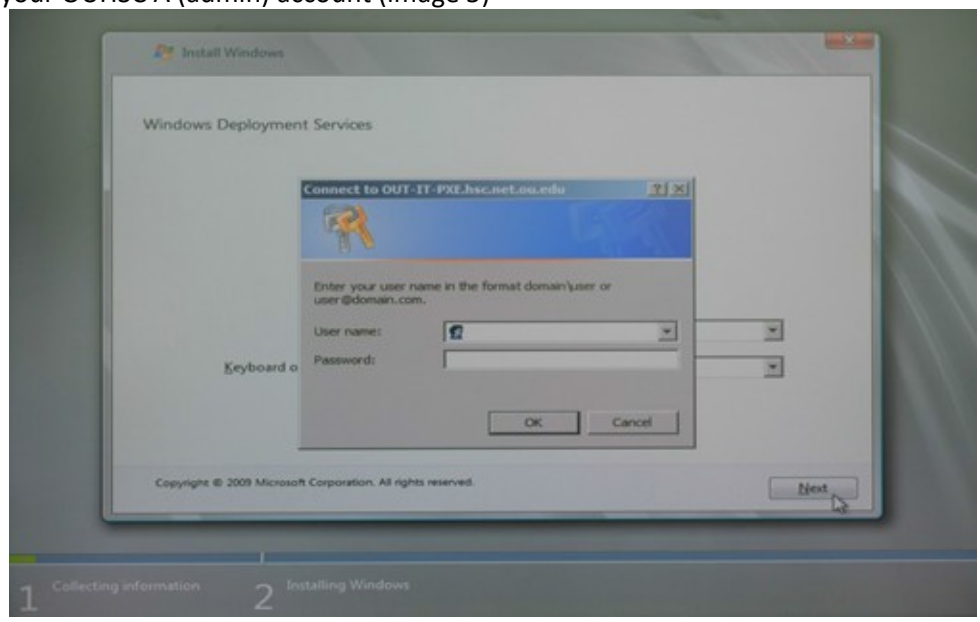
6. Leave as default and press Next (image 4)

Issue Date: 2009-10-06
Last Updated: 2016-06-15
Updated By: Lisa Mildon
Revision: 2.1



(image 4)

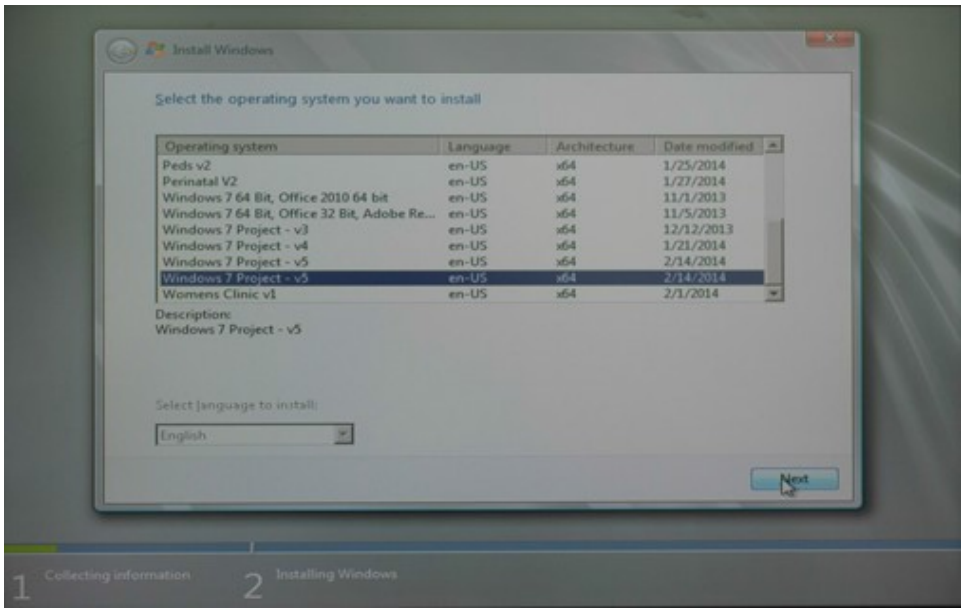
7. Log in with your OUHSC A (admin) account (image 5)



(image 5)

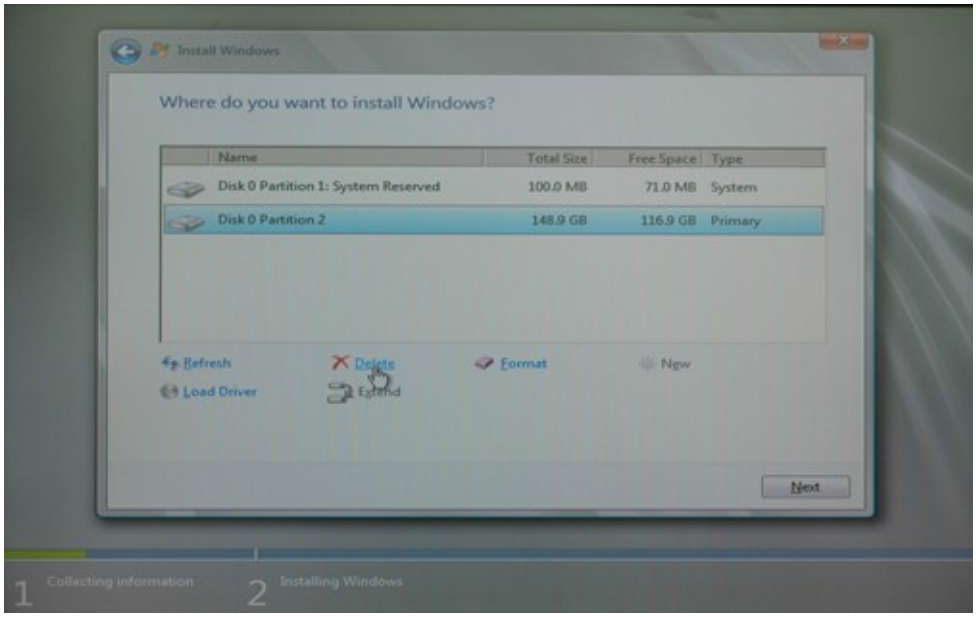
8. Select the appropriate image from the list. In this example it was “Windows 7 Project – v5” (image 6)
    a. Press Next

Issue Date: 2009-10-06
Last Updated: 2016-06-15
Updated By: Lisa Mildon
Revision: 2.1



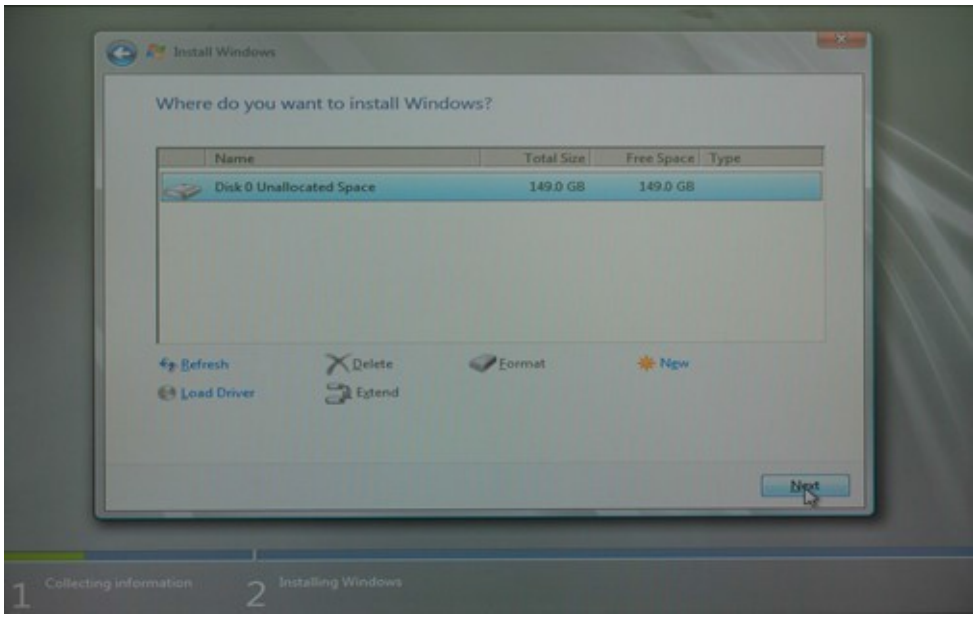
(image 6)

9. Delete any existing partitions until only unallocated space remains (images 7 & 8)
    a. Press Next



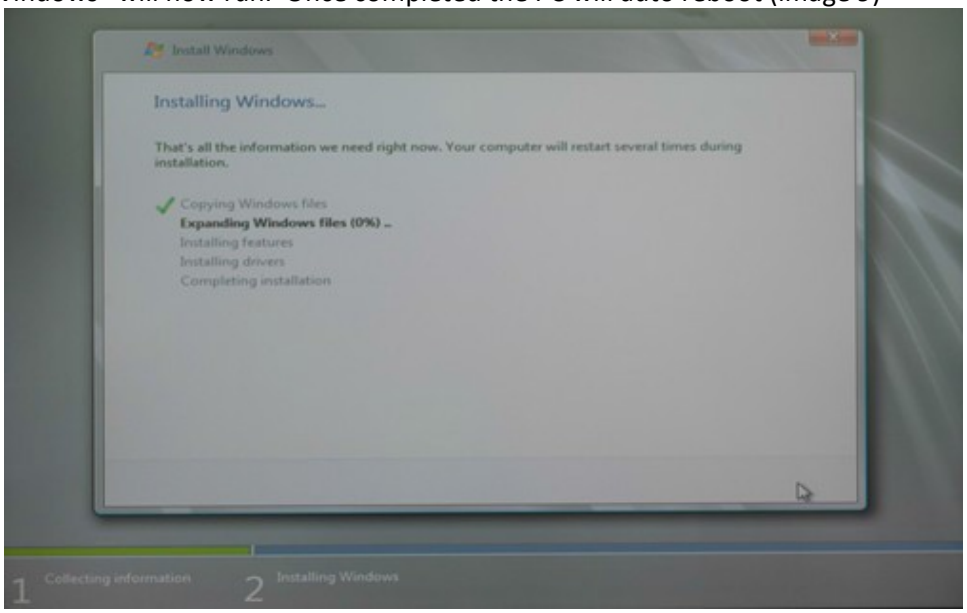
(image 7)

Issue Date: 2009-10-06
Last Updated: 2016-06-15
Updated By: Lisa Mildon
Revision: 2.1



(image 8)

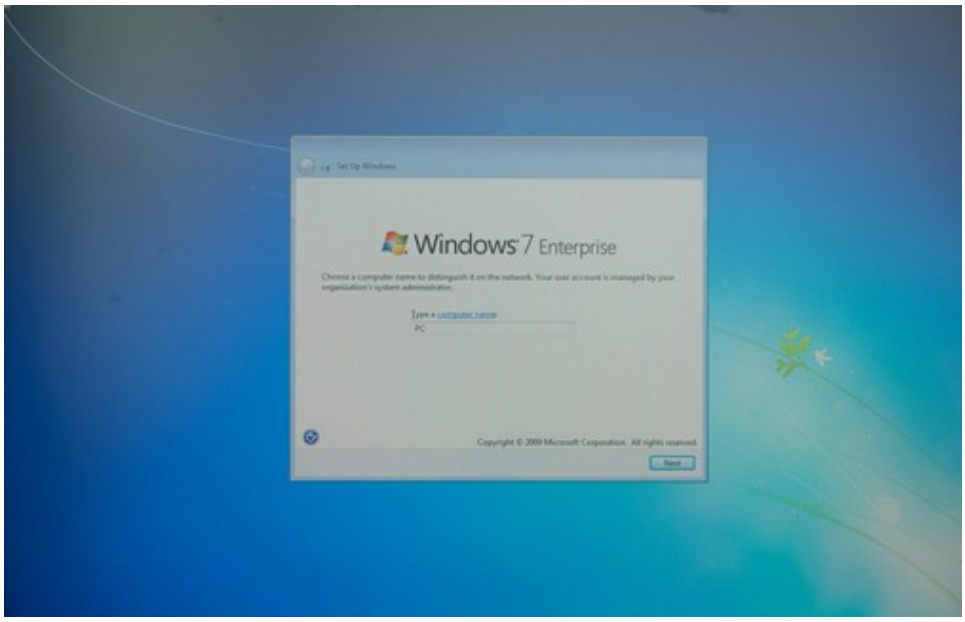
10. "Installing Windows" will now run. Once completed the PC will auto reboot (image 9)



(image 9)

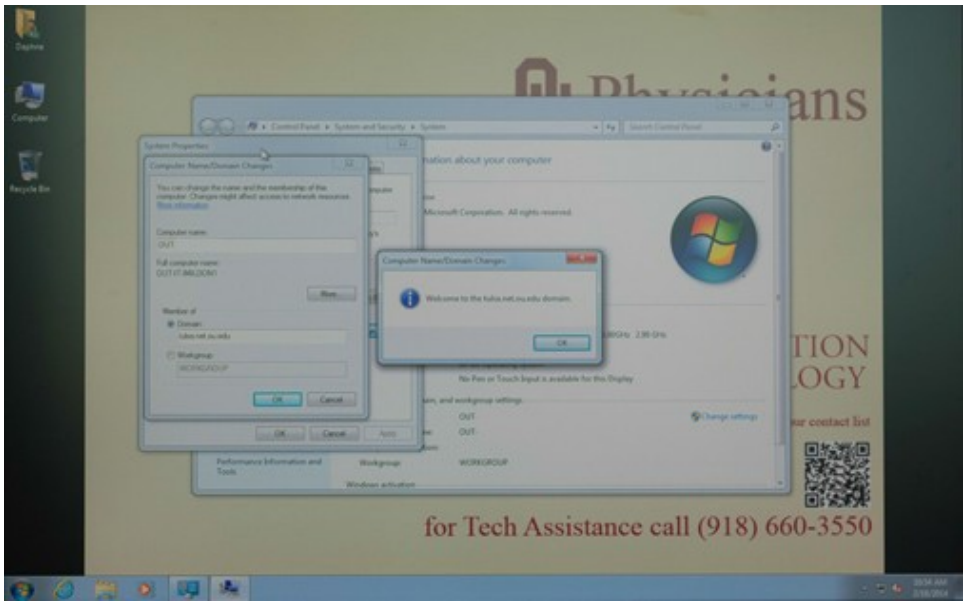
11. "Finish Setup/Driver Install" will run on reboot and once completed the PC will auto reboot again
12. Name the computer (image 10)
    a. Click the Next button
    b. Select Restart Later (restart after joining PC to the domain)

Issue Date: 2009-10-06
Last Updated: 2016-06-15
Updated By: Lisa Mildon
Revision: 2.1



(image 10)

13. From another PC, create a new computer account in the Tulsa AD
    a. Add PC to “tulsa.net.ou.edu” (remember to remove HSC AD account) (image 11)
    b. Reboot



(image 11)

14. Install McAfee ePO Agent from the following location/file
    a. \\out-file\public\McAfeeAgent\ePO_Agent_4. 8. 0. 1995.exe
    b. Run “all” Windows Updates
    c. Finish required software installs/setup
    d. Copy backed-up User files folder to root of C:\
        i. These can be returned to correct location once the user account has been created after they login for the first time
    e. Add user as a Local Admin if appropriate to role
    f. If a laptop, Setup Wi-Fi to use OUBASE
    g. Modify the ServiceNow entry for the PC/Laptop or create a new entry

Issue Date: 2009-10-06
Last Updated: 2016-06-15
Updated By: Lisa Mildon
Revision: 2.1

3.1 Additional steps for encrypted Laptops

1. Log into encrypted pre-boot environment
    a. If your account is not recognized, check with Lisa Mildon or Ben Tuttle
2. Boot laptop and follow ALL steps in 3.1 above, then add the following final steps
    a. Encrypt laptop (re-imaging “removed” encryption)
    b. Add user to the computer in McAfee ePO
    c. Check that user name is recognized by the encryption logon

4.0 Enforcement

Any employee found to have violated this procedure may be subject to disciplinary action within the appropriate existing University employment guideline

Issue Date: 2003-12-01
Last Updated: 2015-06-26
Updated By: Lisa Mildon
Revision: 3.0

Windows 7 Endpoint Checklist

Username: _____ **PC Name:** _____
Department: _____
Location: _____ **Service Tag#:** _____
Phone: _____

Needs	Done	
x		**Image computer using PXE**
x		Create computer account in AD + Model, Service Tag # and warranty expiration date in the description.
x		Add to Domain (Name PC, add to Tulsa domain)
x		Update group policies (gpudate /force)
x		Update BIOS as needed
x		Update ePo Agent if needed
x		Update McAfee AntiVirus
x		Check Device Manager and update drivers from support.dell.com
x		Microsoft Updates from Windows update (Control Panel)
x		Change Folder properties to show full path in address bar and don't hide extensions
x		Set Power to Never Sleep
x		Remove ability for Windows to turn off NIC power (Wireless and Hardline)
x		Update Java
x		Update Flash
x		Update Acrobat Reader
x		Install Printers: _____
		Update Citrix Receiver if needed
		Wireless devices
		Disable ad hoc wireless mode--restrict to infrastructure only
		Configure wireless Ethernet connection to disable when computer is attached to wired network
		Disable Bluetooth collaboration (if applicable)
x		Encrypt, if laptop
		Inventory
x		Input new install or transfer of PC into ServiceNow inventory
		End user setup
x		Setup Outlook
x		Set Default Printer
x		Map S & and any other network No backup.
x		Restore user's backup
		Additional Software

PU	Admin

Issue Date: 2003-12-01
Last Updated: 2016-06-17
Updated By: Lisa Mildon
Revision: 2.1

NAMING CONVENTION

abbrev.	Dept
CC	CallCenter
CAD	BedlamDept
ADM	AdminDept
CAD	CliAffDept
CB	CenBilDept
CAN	ChildAbuseNetwork
COM	DeansDept
PPC	DistanceED
EM	EmergencyDept
FMC	FamMedClinic
FMD	FamMedDept
HR	HumResDept
PACT	ImpactDept
IMC	IntMedClinic
IIC	IntegratedImmunologyCenter
IMD	IntMedDept
LIB	LibraDept
LC	LearningCenter
MI	MedicalInformatics
MRD	MedicalRecordsDept
NEU	NeurologyDept
OBD	OBDept
OPS	OperaDept
PC	PedsClinic
PD	PedsDept
PDC	PedsDiabDept
PSC	PsychClinic
PSD	PsychDept
RAM	Ramona
RSA	ResStuAff
SA	StudentAff
SC	SurgClinic
SD	SurgDept
SEC	SecurDept
STU	StuSer
IT	ItDept
WC	WomenClinic
TGC	Grad College
PRES	PresOff

Issue Date: 2004-03-10
Last Updated: 2017-12-17
Updated By: Lisa Mildon
Revision: 1.3

Installing McAfee Endpoint Encryption

1.0 Purpose
This document sets out to provide the steps needed to install and setup McAfee Endpoint Encryption on a computer

2.0 Scope
This document applies to any computer (desktop and laptop) owned by or operated by OU-Tulsa, associated departments, clinics, offsite clinics and affiliates that connect to the OU-Tulsa network

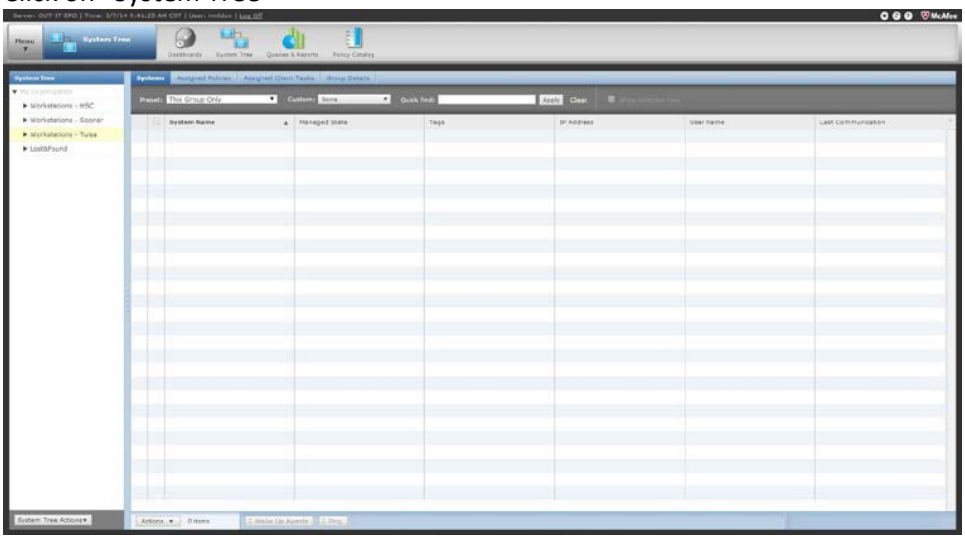
3.1 Policy

3.2 Agent Deployment

1. Log into ePO Server

(Fig. 1)

2. Click on “System Tree”

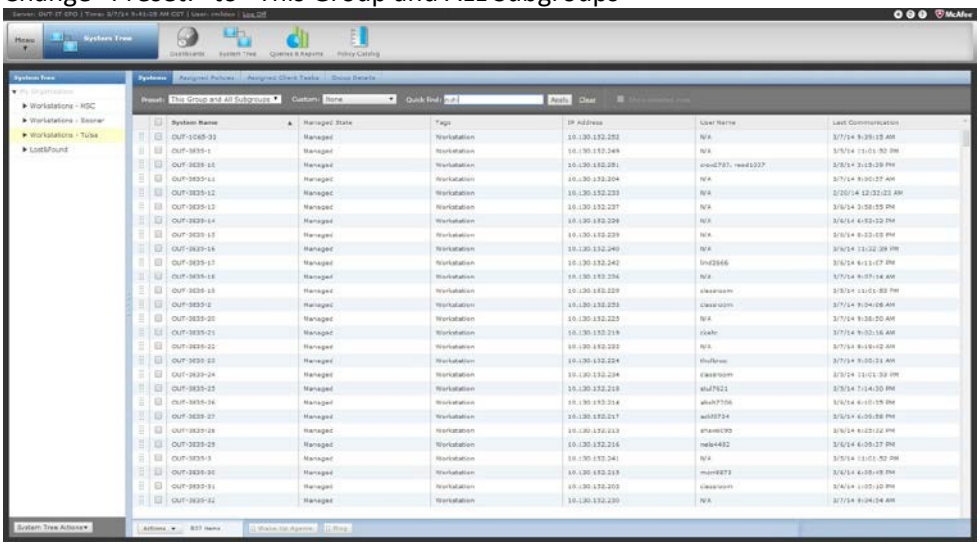


(Fig. 2)

3. Select “Workstations – Tulsa”

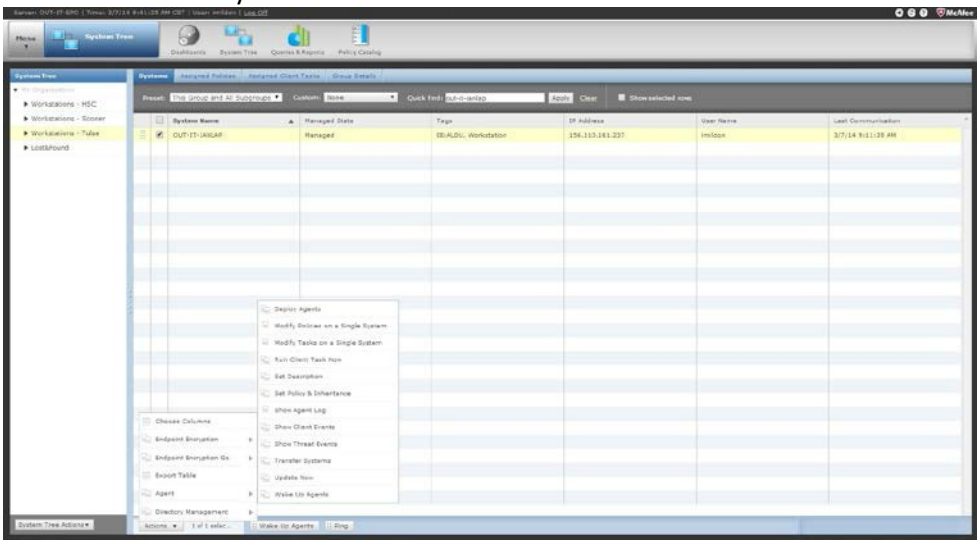
Issue Date: 2003-12-01
Last Updated: 2016-06-17
Updated By: Lisa Mildon
Revision: 2.1

4. Change “Preset:” to “This Group and ALL Subgroups”



(Fig. 3)

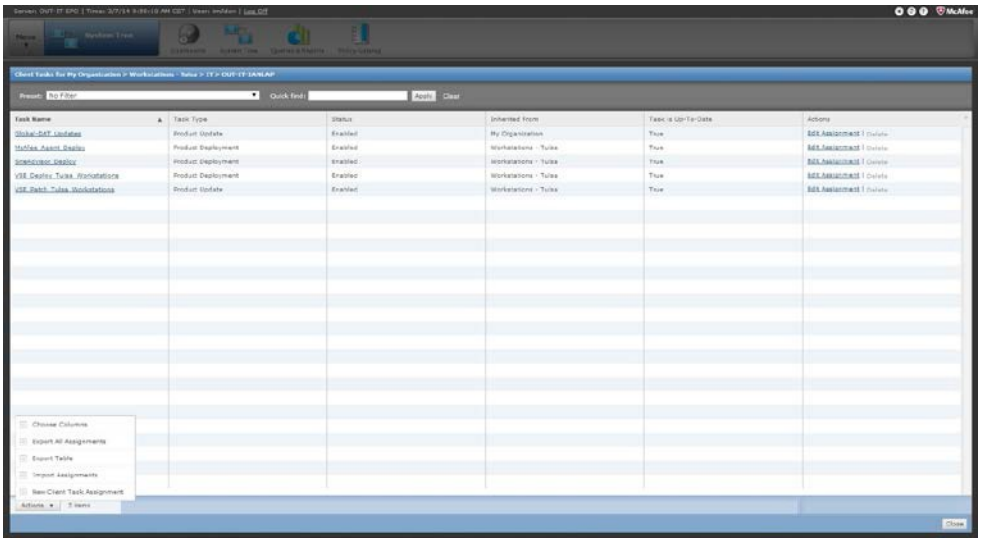
5. Enter system name in “Quick Find”
    a. Click Apply
6. Check box next to system name



(Fig. 4)

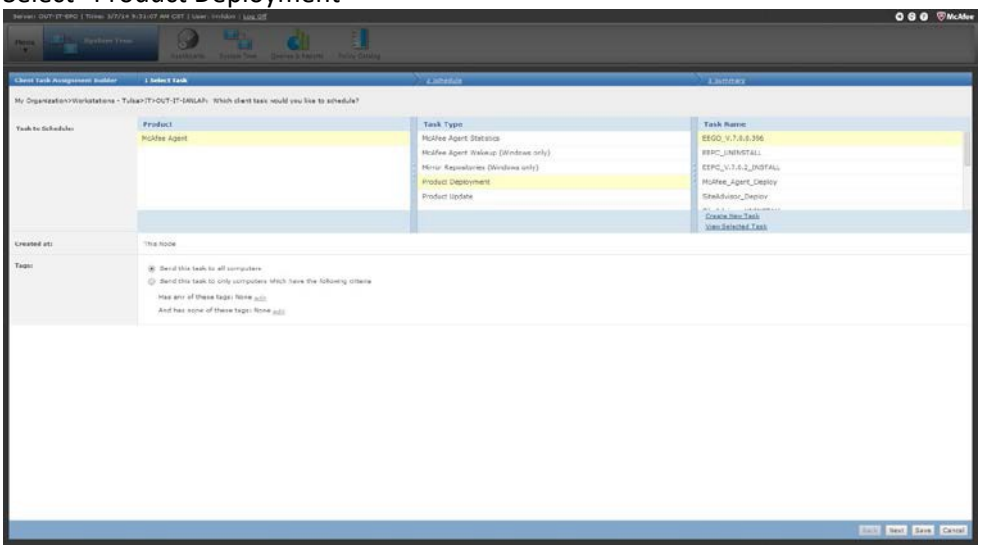
7. Click "Actions"
    a. Select "Agent", “Modify Tasks on Single System”
8. Click "Actions"
    a. Select "Actions", “New Client Task Assignment”

Issue Date: 2003-12-01
Last Updated: 2016-06-17
Updated By: Lisa Mildon
Revision: 2.1



(Fig. 5)

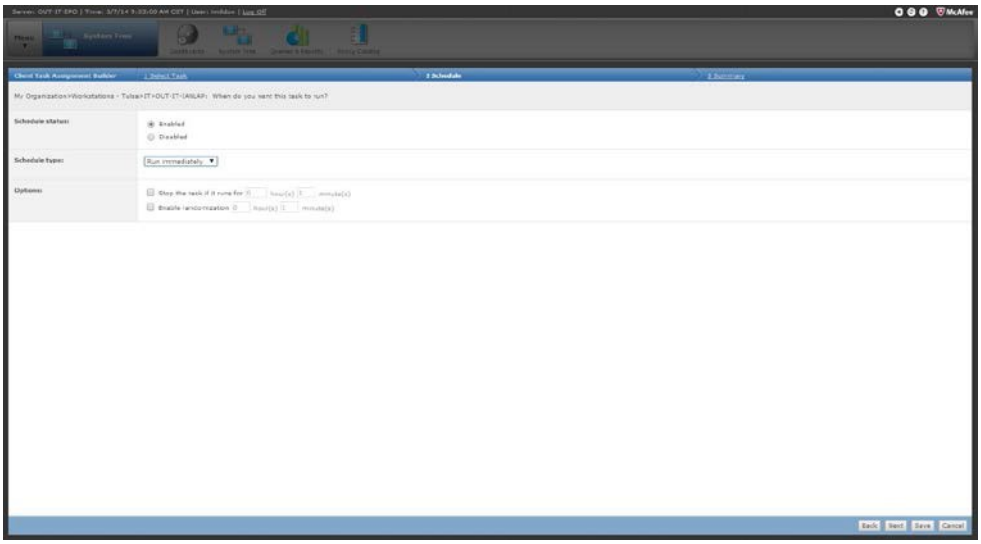
9. Under “Task Type”
10. Select “Product Deployment”



(Fig. 6)

11. Under “Task Name”
    a. Select “Drive_Encryption_GO_Windows_Install” (the default)
    b. Click Next
12. Change “Schedule Type” to “Run Immediately”
    a. Click Next

Issue Date: 2003-12-01
Last Updated: 2016-06-17
Updated By: Lisa Mildon
Revision: 2.1



(Fig. 7)

13. Click Save to deploy the agent
14. On the PC to be encrypted, Right-click the McAfee shield icon and select “McAfee Agent Status Monitor”
    a. Click “Collect and Save Props”, then “Check New Policies”
        i. You should see a message for both the download and the install of the agent

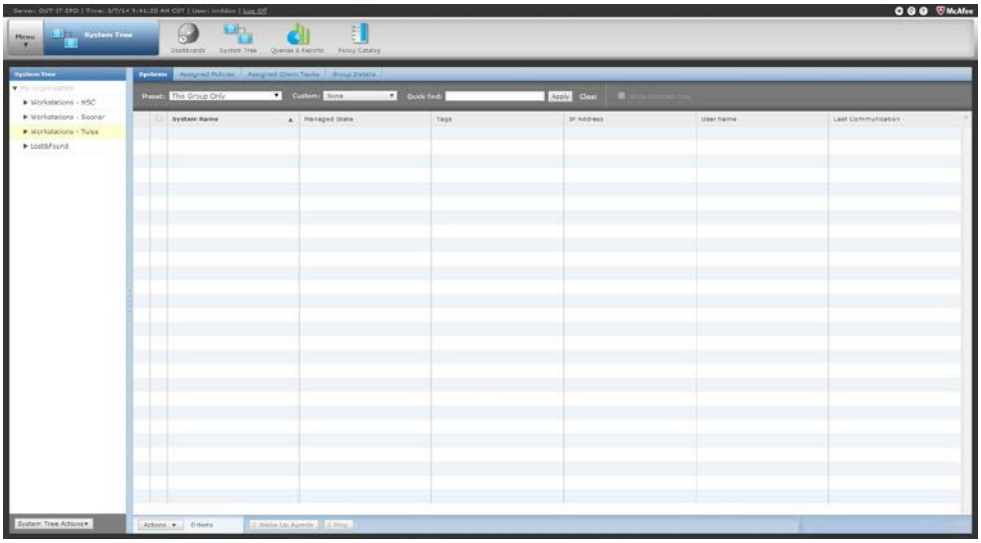
3.3 Client Deployment (Refer to section 3.2, Fig. 1)

1. Return to or Log into ePO Server
2. Delete the “EEGO” task
3. Complete steps 1 through 7 from Agent Deployment
4. Select "Actions", “New Client Task Assignment”
5. Under “Task Type”
    a. Select "Product Deployment"
6. Under “Task Name”
    a. Select “Drive_Encryption_install”
    b. Click Next
7. Change “Schedule Type” to “Run Immediately”
    a. Click Next
8. Check all the settings on this screen is correct
    a. Click Save
9. On the PC to be encrypted
    a. Right-click the McAfee shield icon and select “McAfee Agent Status Monitor”
    b. Click “Collect and Save Props”, then “Check New Policies”
    c. When the client has been installed you will see a message that the system needs to log off and a timer will start until it automatically logs off
10. The pre-boot encryption logon process is now in place
    a. Login as normal for an encrypted computer
11. Once back at the desktop
    a. Right-click the McAfee shield icon and select “McAfee Agent Status Monitor”
    b. Click “Collect and Save Props”, then “Check New Policies”
    c. Check on the encryption status
        i. Right-click the McAfee shield icon
        ii. Select “Quick Settings”
        iii. “Show Endpoint Encryption Status”

Issue Date: 2003-12-01
Last Updated: 2016-06-17
Updated By: Lisa Mildon
Revision: 2.1

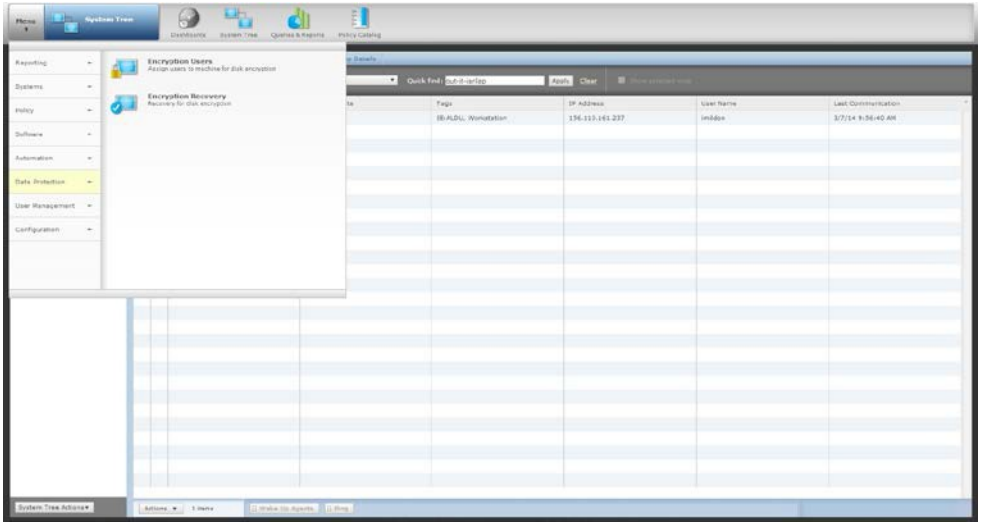
3.4 Adding a User to an Encrypted Computer

1. Log into ePO Server
2. Click on “System Tree”
3. Select “Workstations – Tulsa”



(Fig. 8)

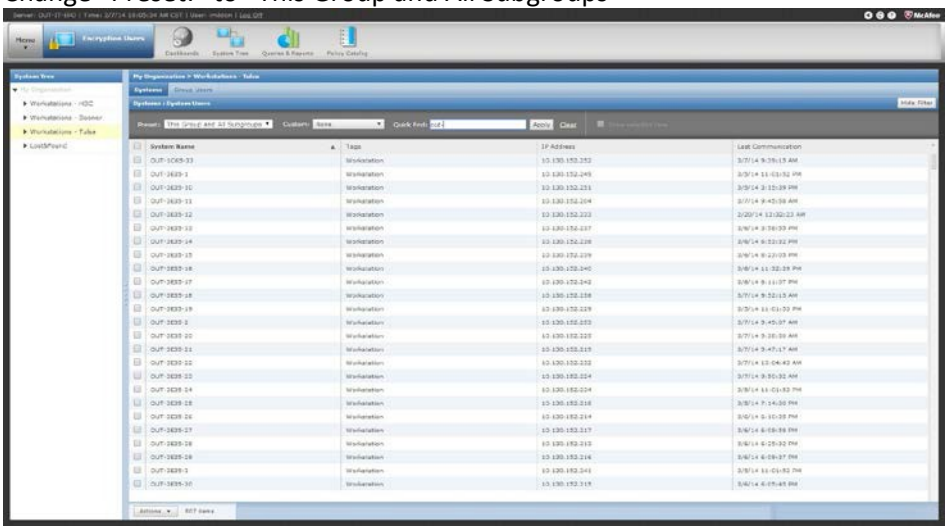
4. Click “Menu”
    a. Select “Data Protection”
    b. Select “Encryption Users”



(Fig. 9)

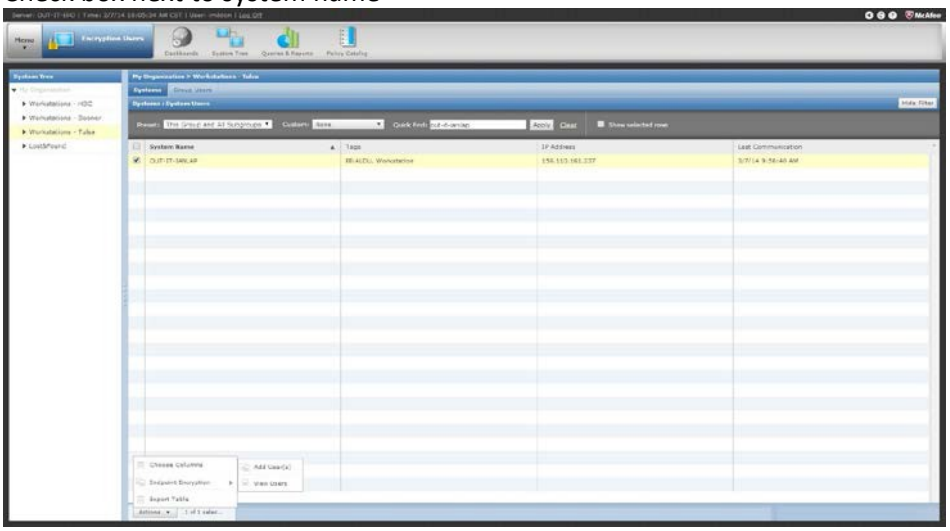
Issue Date: 2003-12-01
Last Updated: 2016-06-17
Updated By: Lisa Mildon
Revision: 2.1

5. Change “Preset:” to “This Group and All Subgroups”



(Fig. 10)

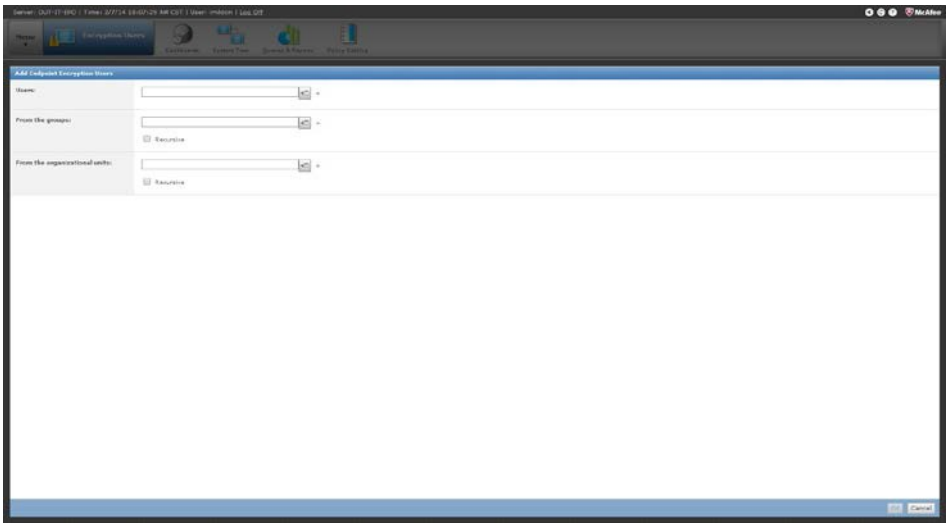
6. Enter system name in “Quick Find”
    a. Click Apply
7. Check box next to system name



(Fig. 11)

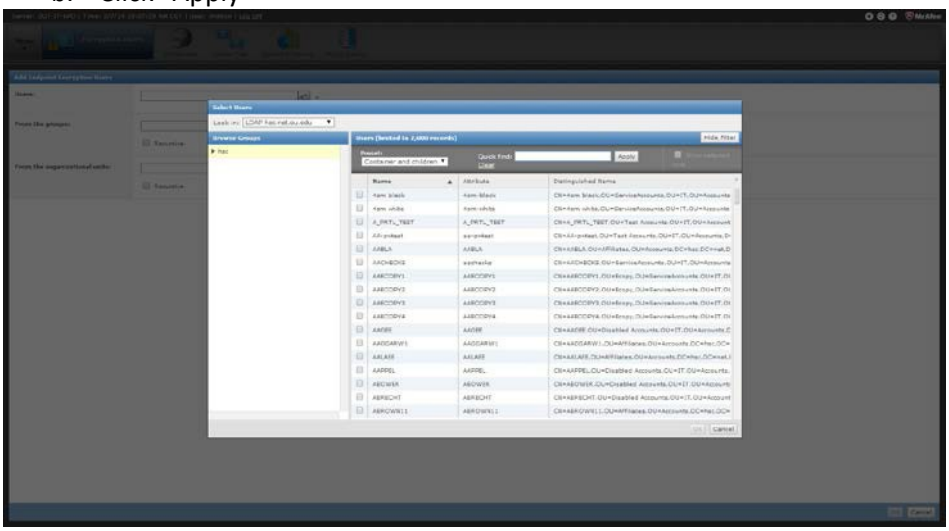
8. Click “Actions”
    a. Select “Endpoint Encryption”
    b. Select “Add Users”
9. Click the “+” box next to the Users field

Issue Date: 2003-12-01
Last Updated: 2016-06-17
Updated By: Lisa Mildon
Revision: 2.1



(Fig. 12)

10. Change “Preset to “Container and Children”
    a. Enter the user name in the “Quick Find” field
    b. Click “Apply”



(Fig. 13)

11. Check box next to user name you want to add to system
    a. Click OK
    b. Click OK again
12. Add Tulsa-DesktopAdmins and if clinical PC, add Tulsa-MedInfoAdmins
    a. See step 8, but click on the “+” next to the field labeled “From the groups” (See Fig. 11)
13. On the encrypted PC
    a. Right-click the McAfee shield icon and select “McAfee Agent Status Monitor”
    b. Click “Collect and Save Props”, then “Check New Policies”
14. Enter the new user name at the Encryption logon to test that they are recognized by the Encryption Agent
    a. The end user will need to reset their security questions when they first logon

4.0 Enforcement

Any employee found to have violated this procedure may be subject to disciplinary action within the appropriate existing University employment guidelines.

Issue Date:	2003-12-01
Last Updated:	2016-06-17
Updated By:	Lisa Mildon
Revision:	2.1

5.0 Definitions

Term Definition

6.0 Revision History

Issue Date: 2013-01-14
Last Updated: 2013-03-07
Updated By: Lisa Mildon
Revision: 1.1

Inventory Updating Procedure

1.0 Purpose
To provide the required steps and guidelines required to update the inventory records within Service Now

2.0 Scope
To achieve and maintain consistency in recording when any hardware or software is deployed, re-deployed or sent to surplus. Also, to record additional features such as warranty status and software licensing

3.1 Policy
3.2 Applies to

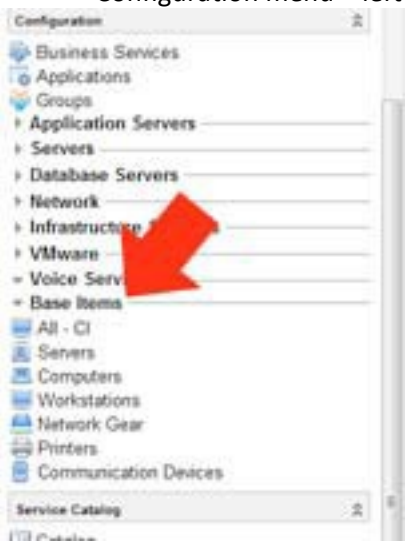
- All OU-Tulsa Information Technology employees

3.3 When to record/update

- When new hardware or software is deployed
- When hardware or software is re-deployed to different users and/or locations
- When hardware is sent for surplus
- When licensed software is installed or removed from a computer
- When a warranty (or service contract) is renewed/extended
- After working on a particular endpoint.

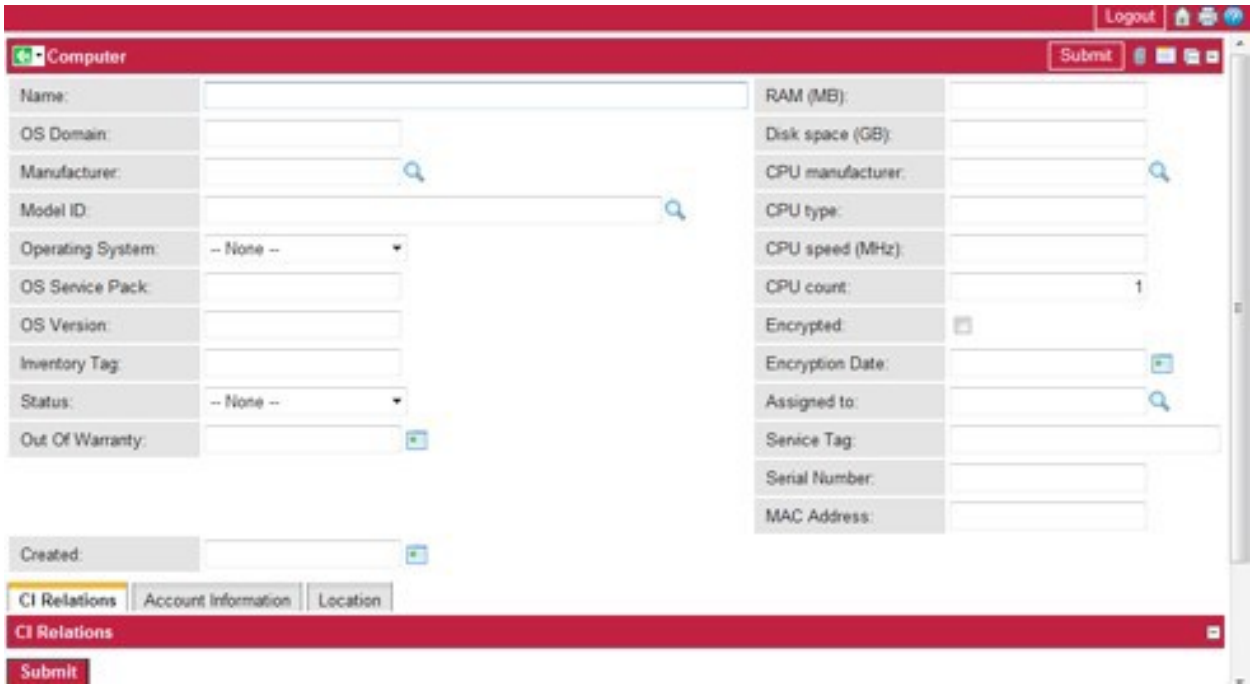
3.4 What to record/update

- The information will vary depending on what item(s) are being recorded into Service Now
- To enter or update information within Service Now, first locate the Base Items section of the Configuration menu – left side of your screen when looking at the Service Now window



- For this example, to show the required fields, I have opened the Computer option and selected New from the toolbar
    - Fill out as much information as you can for the item being added or updated
    - Click the Submit button when you have filled out or updated the relevant sections

Issue Date: 2013-01-14
Last Updated: 2013-03-07
Updated By: Lisa Mildon
Revision: 1.1



4.0 Enforcement

Any employee found to have violated this procedure may be subject to disciplinary action within the appropriate existing University employment guidelines

5.0 Definitions

Term Definition

6.1 Revision History

Issue Date: 2011-01-07
Last Updated: 2016-06-17
Updated By: Lisa Mildon
Revision: 1.8

Inventory Surplus Procedure

Purpose: This procedure provides the rules and guidelines for proper surplus of equipment.

Scope: To achieve and maintain consistent standards for inventory surplus.

Definitions:

Data Device – Designation for any item that has data storage (PC hard drive, networked printer, etc.)

Procedure:

1. **Collection** – IT staff will remove surplus items from support departments, colleges, and/or clinics as requested. A ServiceNow request must be submitted and approved by user prior to removal of surplus items from owner's location.
    a. Change of inventory will be noted in Service Now when the item is removed from its owner's location.
    b. Remove computer object from Active Directory, when applicable.
    c. All items must be logged on the Inventory Surplus Form when they are brought to desktop staff in the Tech East area. The form can be found: here
    d. For items with a university asset tag, the IT Business Office must be notified in order to complete a change of inventory form.
2. **Data Collection** – If hardware has a hard drive, system information must be recorded and placed in secure storage by CS staff. All data devices can be delivered to CS staff for inventory and storage.
    a. CS staff will remove hard drive from surplus items and bring to inventory station located at the north end of tech area next to data center.
    b. Open Hard drive inventory spreadsheet found here
    c. Scan hard drive serial number with barcode scanner.
    d. Place host name, reason for disposal, service tag, date and time of disposal and technician's name in spreadsheet fields. If item has an Asset tag that should be noted also.
    e. Hard drive will be placed in secured HiTech Assets container. The combination for the container is on file in the Business Office.
3. **Sorting** – CS tech will store all non-data equipment in room 4WB120. When designated surplus shelves have been filled, equipment will be moved to pallets located in south end of garage (with a number color sticker on it) to be shrink wrapped and stored until removal.
    a. Off-site techs will store non-data storing equipment in their offices until a surplus day is designated.
    b. Storage media must be brought to East Tech area at Schusterman. (See step 2)

4. **Removal** – CS tech will notify Client Services Manager when 6 or more pallets have been created or data device container is full. Client Services Manager will coordinate removal of assets with IT Business Office. Prior to removal of any equipment, IT Business Office must have a copy of surplus inventory information. This information will be stored on the Tulsa IT SharePoint Site located here .
    a. **For data device** – IT Business Office will contact HiTech Assets (rmooring@htassets.com) for pick-up of container (HiTech Assets Gaylord box) to have data devices shredded. A new container will be left to replace the full container.
    b. **For non-data surplus** – IT Business Office will contact HiTech Assets to pick up the pallets of surplus.

Compliance:

The Client Services Manager will randomly review inventory database status, the current status of the surplus processes, reports, and activities to ensure that they meet the support standards set in this protocol. Since any hardware that is unaccounted for is a potential breach, accountability of each step in this procedure will be consistently monitored before surplus is removed from central IT area. Anyone responsible for skipping any of these steps will be held accountable with potential disciplinary actions taken.

ANY changes to this protocol should result in a copy being sent to the OU- Tulsa Risk Management office.

Issue Date: 2015-07-20
Last Updated: 2016-06-17
Updated By: Lisa Mildon
Revision: 2.0

Tripwire Procedure

I. On Fridays, CS Security Tech receives weekly vulnerability report.

II. ServiceNow automatically generates incident for vulnerability remediation
   A. Request: Request
   B. Category: Security
   C. Subcategory: Risk Assessment
   D. Service: Vulnerability Scan\Remediation
   E. ITIL Watch list: IT-Security Team

III. CS Security Tech attaches weekly report.

IV. CS Security Tech looks at Risk Matrix for a Host Score of 1000 or higher.
   A. Are there vulnerabilities?
      1. If no, then step **g.**
      2. If yes, follow steps below:
         a. Click on top right corner of Risk Matrix.
         b. Click on the highest score, on the Affected Hosts number.
         c. Export vulnerabilities for the current category and attach to SN ticket.
         d. Determine which items are endpoints.
            i. Within Tripwire, look at NetBIOS Name or Operating System.
            ii. Or with NSLOOKUP, NBTSTAT or NMAP via IP address.
            iii. Compile, export and attach list of endpoints to SN ticket.
         e. Click on each DNS Name for endpoint vulnerability list.
            i. Look at Score of each vulnerability, focusing on scores of 1000 or more.
            ii. Click on each individual Remediation to get definition, instructions and possible download for fix.
               1. Research via NIST, US-CERT, TechNET or other pertinent vendor knowledge bases.
               2. Paste any research links into SN incident.
            iii. CS Security Tech downloads any necessary patches or updates for CS Techs to utilize in remediation.
               1. If found on non-IT supported systems, contact will be made via SN email to their respective POC support person detailing vulnerabilities.
         f. CS Security Tech sorts report by NetBIOS Name and creates separate reports to CS Techs for their respective coverage areas.
         g. CS Security Tech creates new incident per vulnerability and support area based on reports from step e.
            i. Request Type: Incident
            ii. Category: Endpoints
            iii. Subcategory: Security
            iv. Service: Vulnerability Remediation

v. Short Description: Vulnerability ID: CVE-#### (pertinent ID issued by Mitre.org.)
vi. Add CS Security Tech and their respective backup to ITIL Watchlist.
vii. CS Security Tech attaches report and gives instructions on vulnerability remediation in SN incident.
viii. In original ticket, CS Security Tech makes note of new Incident numbers.

h. CS Security Tech notes any new exceptions in original SN incident.

B. CS Tech performs vulnerability remediation per SN incident.
1. Updates incident and notifies CS Security Tech.
2. CS Security Tech will confirm in the next new scan.
a. New scans occur every Thursday; results available on every Friday.
b. If all clear, step C.
c. If vulnerability still exists, repeat step B.
i. If after 2nd scan endpoint vulnerability still remains, system will be re-imaged.

C. CS Tech closes their assigned SN incident.
D. CS Security Tech closes their SN incident.

For full diagram and details, procedure can be found here.