

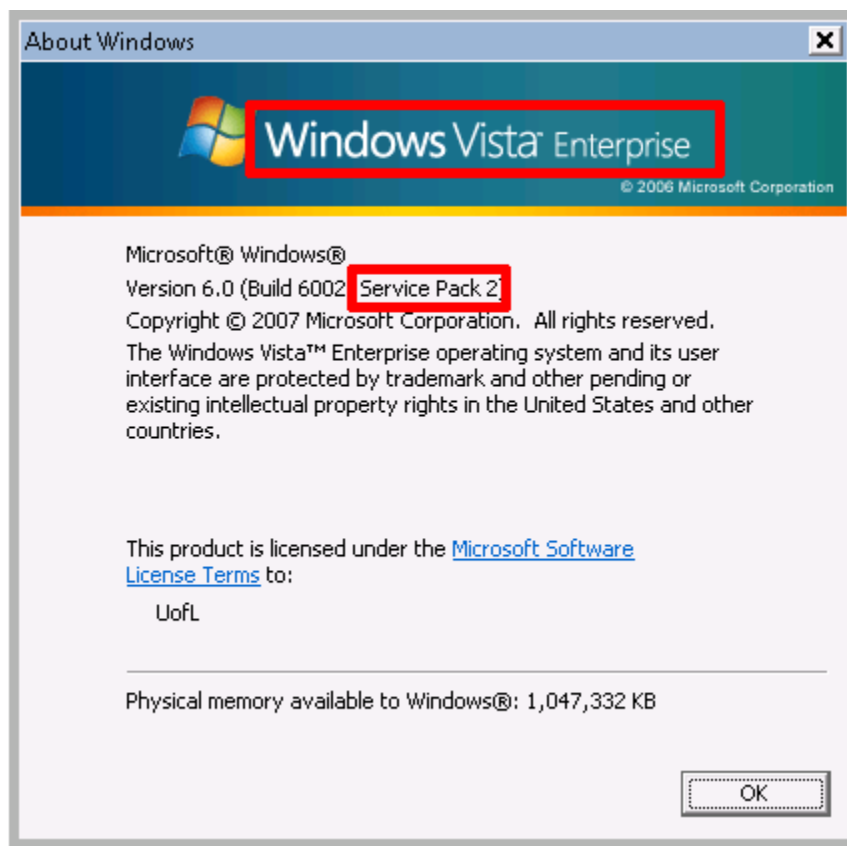
SCCM Client Checklist for Vista

1. The client workstation must have a supported [operating system](#).

Supported operating systems include Windows Vista.

To view information about the operating system version:

- a. Open a [Command Shell](#)
- b. Enter **winver** at the [command prompt](#)

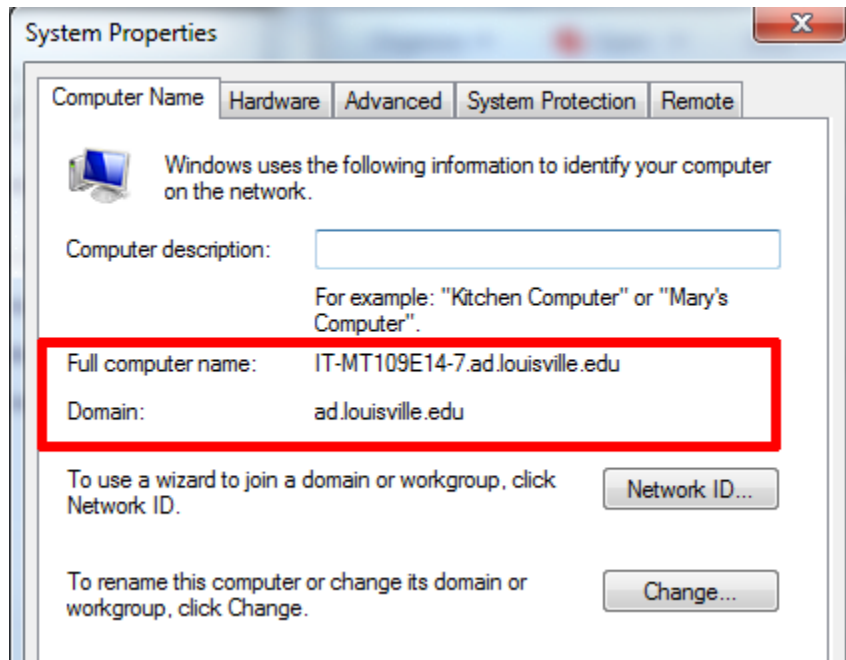


2. The client workstation must be joined to the enterprise Active Directory “ad.louisville.edu”

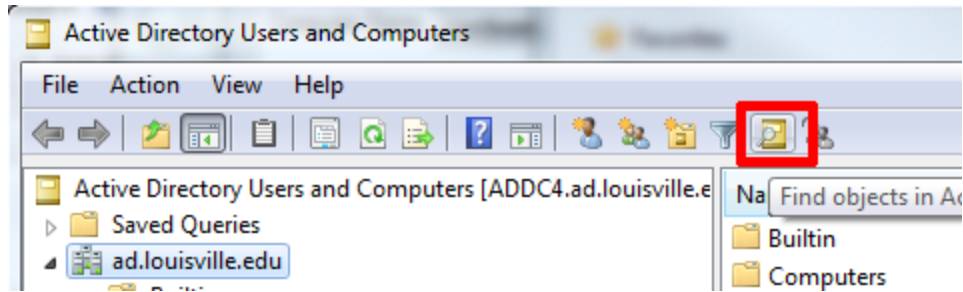
To view information about the domain:

- a. Click on **Start**
- b. Right-click on **Computer**
- c. Click on **Properties**
- d. Click the link in the left navigation panel

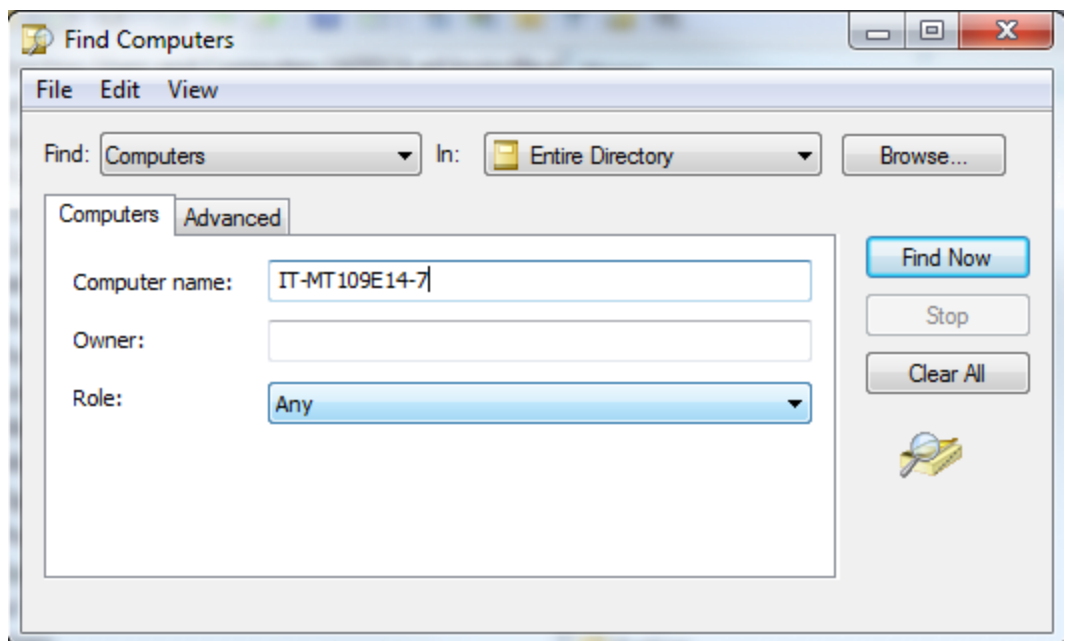
- e. Click on the **Computer Name** tab



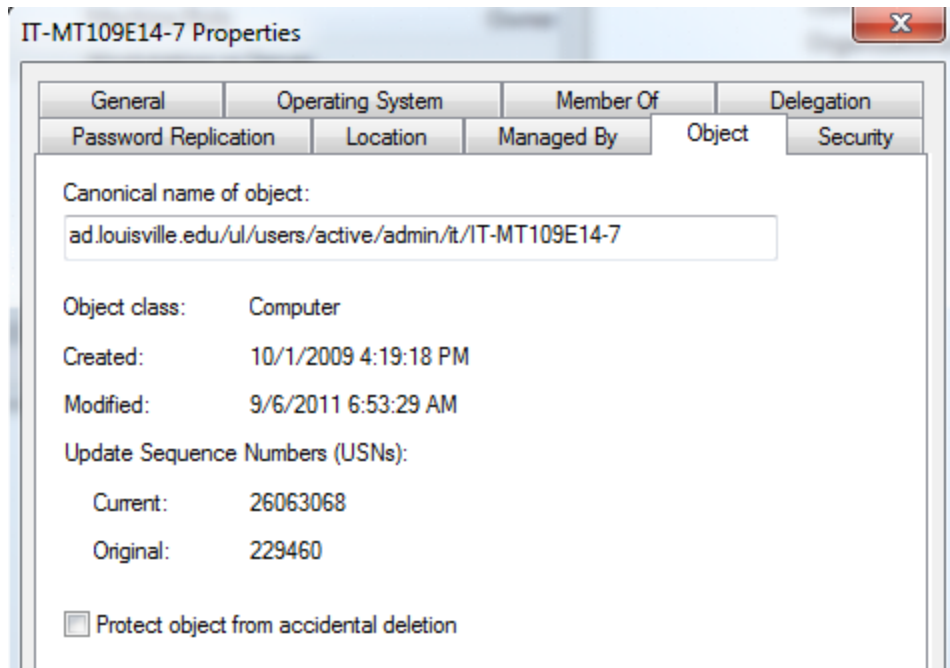
3. The client workstation account in Active Directory must be in a departmental OU. Computers in the default "Computers" OU are not targeted for the client push.
 - a. Review the [recommended workstation naming convention](#).
 - b. Install the Remote Server Administration Tools
 - i. Supported Operating Systems: Windows Vista Business, Windows Vista Enterprise, Windows Vista Ultimate
 - ii. Support for Windows Vista with Service Pack 1 ends on July 12, 2011. Update to Service Pack 2.
 - iii. <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=21090>
 - c. See [Appendix 2 : Enable ADUC Advanced Features](#)
 - d. Use the **Active Directory Users and Computers** (ADUC) administrative [tool](#) to search for the computer name and view the Object tab.
 - i. Click on **Start**
 - ii. Click on **Control Panel**
 - iii. Double-click on **Administrative Tools**
 - iv. Double-click on **Active Directory Users and Computer**
 - v. Click on the **Find** icon in the [toolbar](#)



- vi. Select **Computers** in the “Find” [drop-down list](#).
- vii. Select **Entire Directory** in the “In” [drop-down list](#).
- viii. Enter the name of the computer in the “Computer Name” [text box](#).



- ix. Click the **Find Now** button.
- x. Right-click on the computer in the results pane and select **Properties**.
- xi. Click on the **Object** tab



The **Canonical name of object** should:

- Begin with "ad.louisville.edu/ul/users/active/"
- End with the name of the computer.
- Contain your departmental path in the middle. In this example, the departmental path is "/admin/it", which is correct.

4. The client workstation must successfully register the fully qualified domain name (FQDN) with the Active Directory DNS servers.

From a [command shell](#), enter: `ping computername -4`

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\UofL>ping it-mt109e14-7 -4

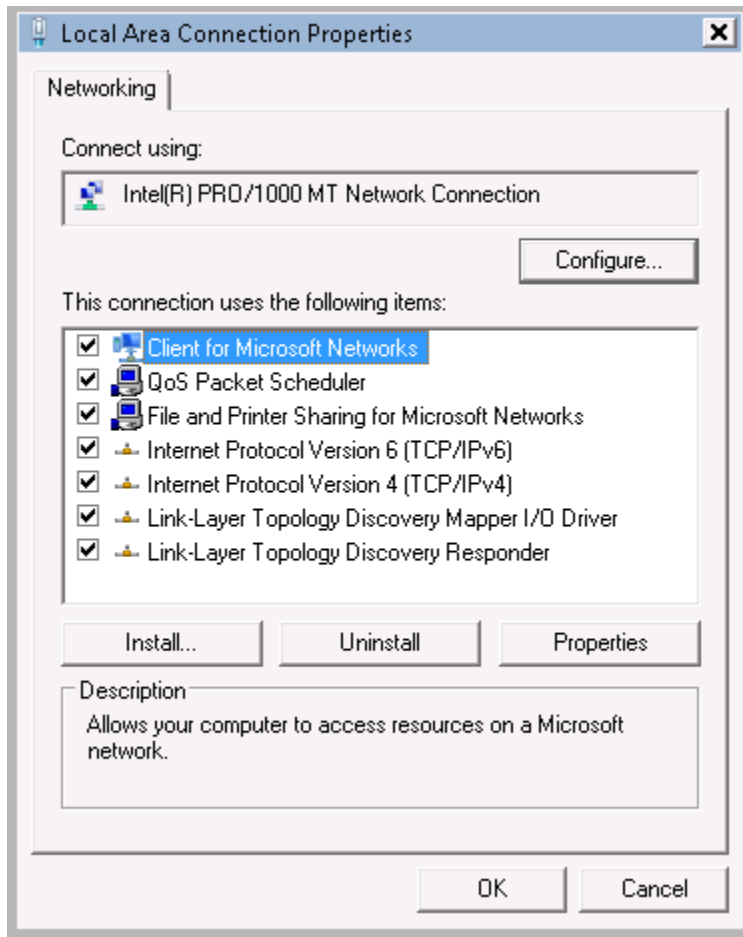
Pinging it-mt109e14-7.ad.louisville.edu [136.165.99.204] with 32 bytes of data:
Reply from 136.165.99.204: bytes=32 time<1ms TTL=126
Reply from 136.165.99.204: bytes=32 time<1ms TTL=126
Reply from 136.165.99.204: bytes=32 time<1ms TTL=126
Reply from 136.165.99.204: bytes=32 time=2ms TTL=126

Ping statistics for 136.165.99.204:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\UofL>_
```

Verify that the computer name resolves to the correct FQDN and to the correct IP address. In the above example, it-mt109E14-7 correctly resolves to IT-MT109E14-7.ad.louisville.edu and 136.165.99.204.

5. **The client workstation must have the “File and Printer Sharing for Microsoft Networks” service installed for the active network adapter.**
 - a. Click on **Start**
 - b. Click on **Control Panel**
 - c. Double-click on **Network and Sharing Center**
 - d. Click on **Manage network connections** in the left navigation panel
 - e. Right-click on **Local Area Connection** and select Properties
 - f. Verify that the **File and Printer Sharing for Microsoft Networks** service is installed:



6. If the Windows firewall is turned on, the client workstation must have firewall exceptions to allow the SCCM servers to access the workstation's admin shares. Access should include the 136.165.230.0/24 range.
 - a. From a [command shell](#), enter: `gresult /R /SCOPE COMPUTER| more`

```
Administrator: C:\Windows\system32\cmd.exe
Group Policy slow link threshold: 500 kbps
Domain Name: AD
Domain Type: Windows 2000

Applied Group Policy Objects
-----
IT-Add Admin
IT-TrustedSites
IT-Sharepoint-Windows 7
IT-Guardian Edge
IT-Open SCCM Ports
IT-Autoenroll Certificates
IT-GPCSE Install
UofL Group Policy
Local Group Policy

The following GPOs were not applied because they were filtered out
-----
IT-Sharepoint-XP
Filtering: Denied (WMI Filter)
WMI Filter: XP Workstations

IT-Sharepoint-Vista
Filtering: Denied (WMI Filter)

-- More --
```

Verify that the “IP-OPEN SCCM Ports” GPO has been applied.

7. The client workstation must have the group “AD\Domain Admins” as a member of the local administrators group. SCCM needs access to \\computer\admin\$.
 - a. From a [command shell](#), enter: `net localgroup “Administrators”`
 - b. Verify that **AD\Admin Admins** is a member

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\sysmop>net localgroup "Administrators"
Alias name      Administrators
Comment

Members
-----
AD\Domain Admins
AD\IT_DesktopSupport
AD\IT-EntDev
AD\sysmop
Administrator
godzilla
The command completed successfully.
```

8. The client workstation must allow “Remote Administration” for the SCCM subnet 136.165.230.0/24. SCCM needs to be able to use RPC, WMI, and/or DCOM remotely.
 - a. Click on **Start**
 - b. Click on **Control Panel**

- c. Double-click **Administrative Tools**
- d. Double-click on **Windows Firewall with Advanced Security**
- e. Click on **Advanced settings** in the left navigation panel
- f. Click on **Inbound Rules**
- g. Scroll to the **Remote Administration** rules

Inbound Rules								
Name	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	
Performance Logs and Alerts (TCP-In)	Domain	No	Allow	No	%system...	Any	Any	
Performance Logs and Alerts (TCP-In)	Private...	No	Allow	No	%system...	Any	Local subnet	
Remote Administration (NP-In)	Domain	Yes	Allow	No	System	Any	136.165.224.0/20	
Remote Administration (RPC)	Domain	Yes	Allow	No	%System...	Any	136.165.224.0/20	
Remote Administration (RPC-EPMAP)	Domain	Yes	Allow	No	%System...	Any	136.165.224.0/20	
Remote Assistance (DCOM-In)	Domain	No	Allow	No	%System...	Any	Any	
Remote Assistance (PNRP-In)	Public	No	Allow	No	%system...	Any	Any	
Remote Assistance (PNRP-In)	Domai...	No	Allow	No	%system...	Any	Any	

- h. Ensure that the domain profiles include 136.165.230.0/24. The remote address could include Any (All IP addresses), 136.165.224.0/20 (the IT datacenter), or 136.165.230/24 (the SCCM servers)

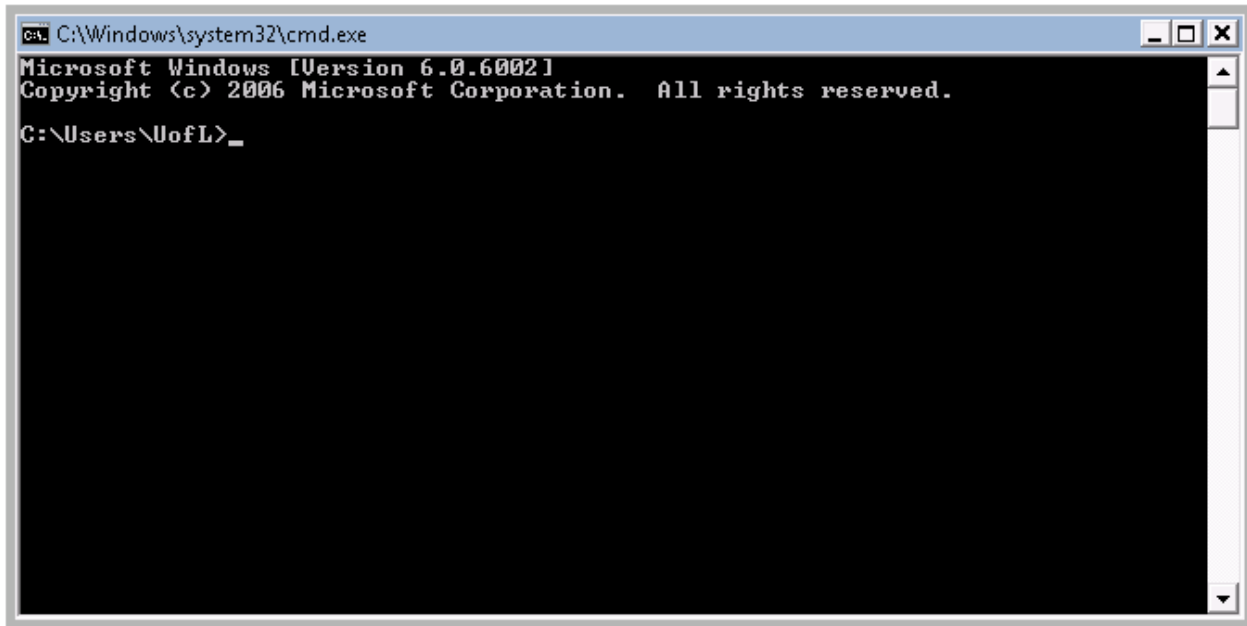
9. The client workstation must be able to autoenroll “ConfigMgr Client Certificate” certificates.

- a. On the **Start** menu, type **mmc** in the “Start Search” [text box](#) and **Enter**. This starts the Microsoft Management Console (MMC).
- b. In the console, click the **File** menu and then click **Add/Remove Snap-in**.
- c. In the **Add/Remove Snap-ins** window, click **Certificates** and then click the **Add** button.
- d. In the **Certificates Snap-in** window, select **Computer account**, and then click **Next**.
- e. In the **Select Computer** window, select **Local computer**, and then click **Finish**. This adds the Certificates Snap-in to the list.
- f. In the **Add/Remove snap-ins** window, click **OK**. This adds the Certificates snap-in to the mmc console.
- g. Expand **Certificates (Local Computer) | Personal | Certificates**
- h. Verify that a certificate has been issued to the client workstation, that it is not expired, and that it uses the “ConfigMgr Client Certificate” certificate template.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Template
IT-MT109G14-2.ad.louisville.edu	ADDC2	8/17/2012	Client Authentication	<None>		Computer
IT-MT109G14-2.ad.louisville.edu	ADDC2	8/17/2012	Client Authentication	<None>		ConfigMgr Client Certificate

Appendix 1: Open a Command Shell

1. Click on **Start**
2. Enter **CMD** in the [text box](#) labeled "Start Search"
3. Press the Enter key



Appendix 2: Enable ADUC Advanced Features

1. Click on **Start**
2. Click on **Control Panel**
3. Double-click on **Administrative Tools**
4. Double-click on **Active Directory Users and Computer**
5. Click on **View** in the [menu bar](#)

6. Make sure **Advanced Features** is checked.

