



# MS14-068 Out of Band Update

AKA KB3011780

**A TRADITION OF  
INDEPENDENT  
THINKING**

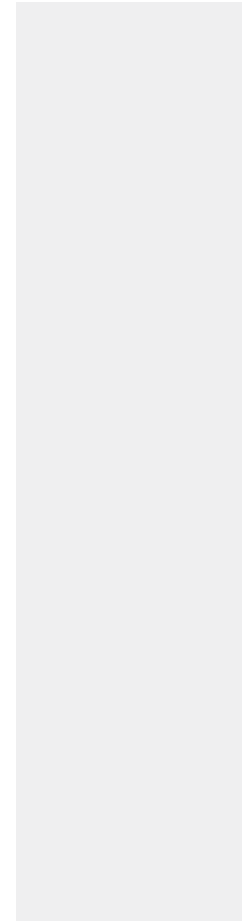


**UCC**

University College Cork, Ireland  
Coláiste na hOllscoile Corcaigh

# Agenda

- Who am I
- Microsoft Windows Patching technologies used by UCC
- Out of Band release timeline



# Who Am I

- Technical Lead for Microsoft Infrastructure in I.T. Services (central I.T.)
- Main areas of responsibility
  - Microsoft Server Infrastructure
  - System Center Infrastructure
- MSc Student in CIT
- Vendor Certifications
  - Microsoft - MCP, MCSA, MCSE, MCITP, MCSE
  - Cisco - CCNA

**Microsoft**  
**CERTIFIED**  
Professional

Microsoft Certified  
Professional

**Microsoft**  
**CERTIFIED**  
Systems Administrator

Messaging on Windows Server 2003  
Windows Server 2003

**Microsoft**  
**CERTIFIED**  
Systems Engineer

Windows Server 2003

**Microsoft**  
**CERTIFIED**  
IT Professional

Enterprise Administrator  
on Windows Server 2008

Server Administrator on  
Windows Server 2008

Virtualization  
Administrator on  
Windows Server 2008 R2

**Microsoft**  
**CERTIFIED**  
Solutions Expert

Private Cloud

Server Infrastructure



# Microsoft Windows Patching Technologies used by UCC

# Patching Technologies used in UCC

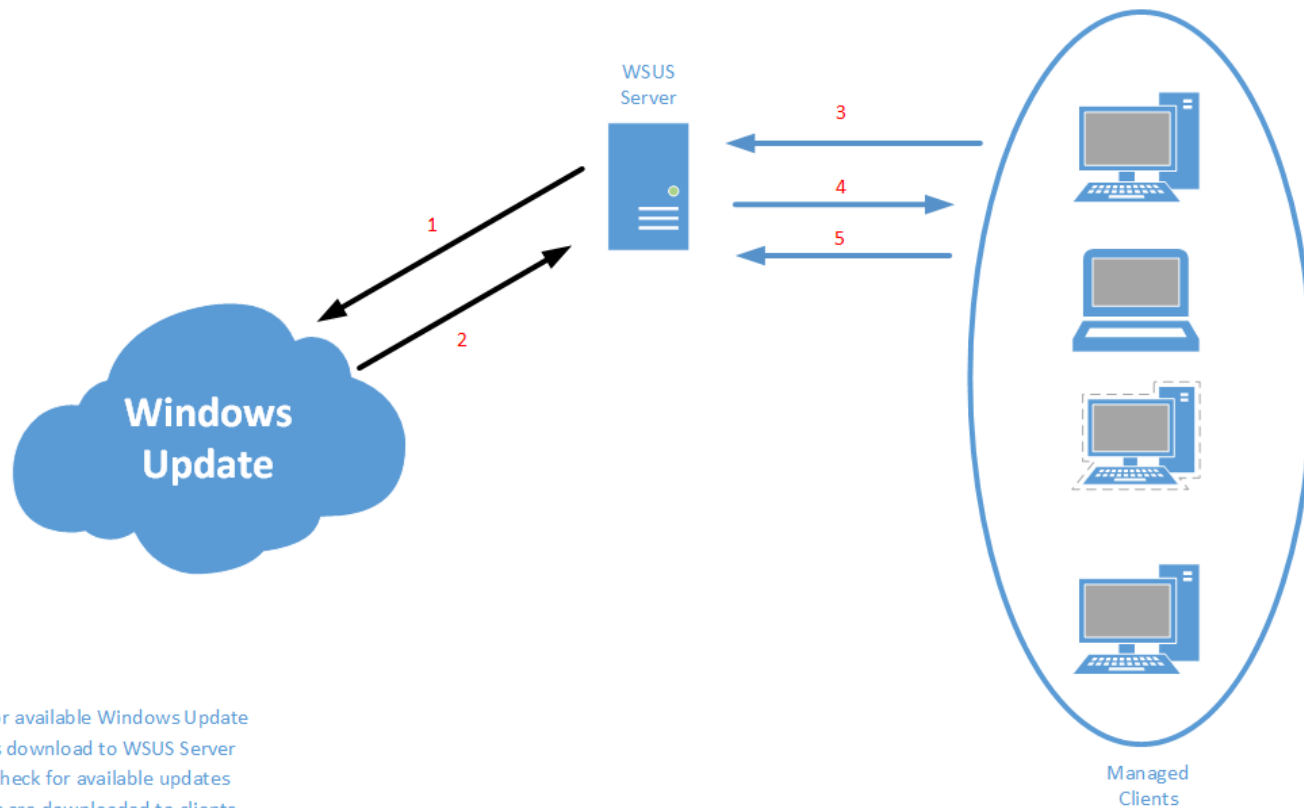
- Windows Update
- WSUS – Windows Server Update Services
- SCCM – System Center Configuration Manager
- Under evaluation
  - Microsoft Intune (Cloud Service)  
<http://www.microsoft.com/sam/en/us/intune.aspx>

# WSUS - Windows Server Update Services

- An onsite copy of Windows Update (Microsoft Updates)
- Available as a download or included as a Server Role since Windows Server 2012
- Saves bandwidth. Download once, distribute to many clients
- WSUS administrator controls when and what updates are deployed to WSUS clients
- Group Policy is used to manage WSUS
  - Specify the WSUS Server to be used
  - Apply updates at a time and on a day specified
  - Configure the behaviour of Windows Update on the client

<http://technet.microsoft.com/en-us/windowsserver/bb332157.aspx>

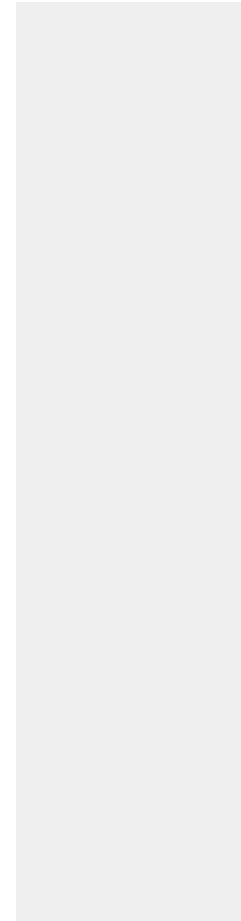
# Simplified WSUS Update Architecture



- 1 – Check for available Windows Update
- 2 – Updates download to WSUS Server
- 3 – Clients check for available updates
- 4 – Updates are downloaded to clients
- 5 – Clients report back their status

# SCCM – System Center Configuration Manager

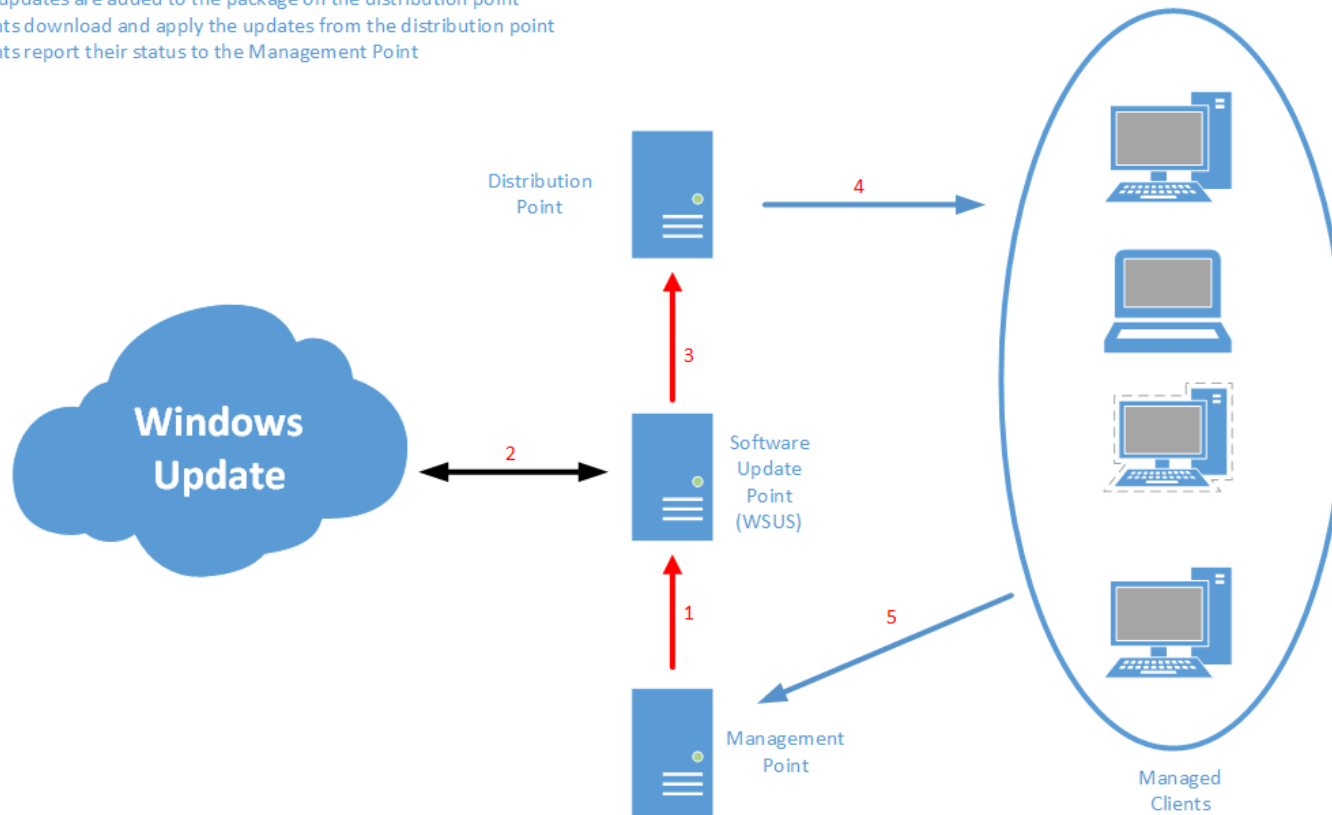
- Can be used to manage and deploy
  - Software & Software Updates
    - Windows Updates
    - Java
    - Non Microsoft applications
  - Operating Systems
  - Desired State Configuration
- Agent installed on managed clients
- Updates can be applied in a maintenance window
- <http://technet.microsoft.com/en-us/library/gg682129.aspx>



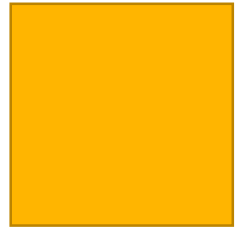


# Simplified SCCM Update Release

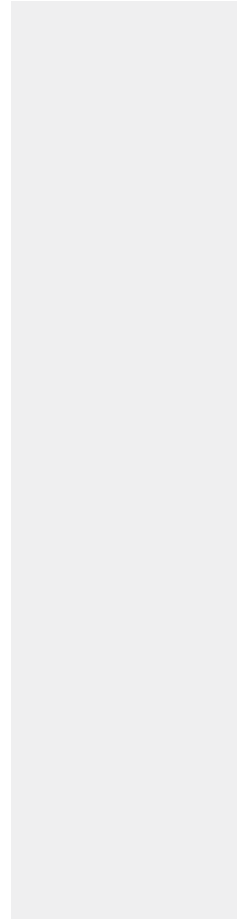
- 1 – When a Software Update Package is created, the Management Point requests the updates from the Software Update Point
- 2 – The SUP downloads the updates
- 3 – The updates are added to the package on the distribution point
- 4 – Clients download and apply the updates from the distribution point
- 5 – Clients report their status to the Management Point



# UCC Windows Server Update Process



- Microsoft releases updates (2<sup>nd</sup> Tuesday of the month)
- Updates evaluated for criticality
- Updates released via WSUS (Wednesday or Thursday)
- Tested in test environment (Thursday or Friday)
- Updates released via SCCM with a Friday 21:00 deadline
- Updates apply and systems reboot in the appropriate maintenance window the following week
  - Spread over 4 days Mon – Thurs
  - Starting at 00:00 – 07:59 in two hour intervals
  - Total of 16 automated Server Maintenance Windows



# Out of Band Update timeline



University College Cork, Ireland  
Coláiste na hOllscoile Corcaigh

# Managed Clients

- WSUS

Windows 7	1659
Windows 8	0
Windows 8.1	3
Window Server	124

- SCCM

Windows 7	2335
Windows 8	32
Windows 8.1	740
Window Server	165


# Tuesday 18/11/2014 - Advance Notification

Tuesday 18/11/2014 14:08

Tue 18/11/2014 14:08

Microsoft <securitynotifications@e-mail.microsoft.com>  
Microsoft Security Bulletin Advance Notification for November 2014

To: Crotty, Anthony

 We removed extra line breaks from this message.

-----BEGIN PGP SIGNED MESSAGE-----  
Hash: SHA256

\*\*\*\*\*  
Microsoft Security Bulletin Advance Notification for November 2014  
Issued: November 18, 2014  
\*\*\*\*\*

This is an advance notification for one out-of-band security bulletin that Microsoft will release on November 18, 2014.

The full version of the Microsoft Security Bulletin Advance Notification for November 18, 2014 can be found at <<https://technet.microsoft.com/library/security/ms14-nov>>.

This bulletin advance notification will be replaced with the November bulletin summary on November 18, 2014. For more information about the bulletin advance notification service, see <<http://technet.microsoft.com/security/gg309152>>.

Critical Security Bulletins  
=====


MS14-068

- Affected Software:


- Windows Server 2003 Service Pack 2
- Windows Server 2003 x64 Edition Service Pack 2
- Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Vista Service Pack 2
- Windows Vista x64 Edition Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2  
(Windows Server 2008 Server Core installation affected)
- Windows Server 2008 for x64-based Systems Service Pack 2  
(Windows Server 2008 Server Core installation affected)
- Windows Server 2008 for Itanium-based Systems Service Pack 2
- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1  
(Windows Server 2008 R2 Server Core installation affected)
- Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
- Windows 8 for 32-bit Systems
- Windows 8 for x64-based Systems
- Windows 8.1 for 32-bit Systems
- Windows 8.1 for x64-based Systems

# Tuesday 18/11/2014 - Notification

Tuesday 18/11/2014 18:11

 Tue 18/11/2014 18:11  
Microsoft <securitynotifications@e-mail.microsoft.com>  
Microsoft Security Bulletin Releases

To: Crotty, Anthony

 You forwarded this message on 18/11/2014 18:12.  
We removed extra line breaks from this message.

-----BEGIN PGP SIGNED MESSAGE-----  
Hash: SHA256

\*\*\*\*\*  
Title: Microsoft Security Bulletin Releases  
Issued: November 18, 2014  
\*\*\*\*\*

Summary  
=====

The following bulletin has been released.

- \* MS14-068 - Critical

The following bulletins have undergone a major revision increment.

- \* MS14-066 - Critical
- \* MS14-NOV

Bulletin Information:  
=====

MS14-068 - Critical

- <https://technet.microsoft.com/library/security/ms14-068>
- Reason for Revision: V1.0 (November 18, 2014): Bulletin published.
- Originally posted: November 18, 2014
- Updated: November 18, 2014
- Bulletin Severity Rating: Critical
- Version: 1.0

MS14-066 - Critical

- <https://technet.microsoft.com/library/security/ms14-066>
- Reason for Revision: V2.0 (November 18, 2014): Bulletin revised to announce the reoffering of the 2992611 update to systems running Windows Server 2008 R2 and Windows Server 2012. The reoffering addresses known issues that a small number of customers experienced with the new TLS cipher suites that were

# Tuesday 18/11/2014 - Security Bulletin

## Microsoft Security Bulletin MS14-068 - Critical

This topic has not yet been rated - [Rate this topic](#)

### Vulnerability in Kerberos Could Allow Elevation of Privilege (3011780)

Published: November 18, 2014

Version: 1.0

#### Executive Summary

This security update resolves a privately reported vulnerability in Microsoft Windows [Kerberos KDC](#) that could allow an attacker to elevate unprivileged domain user account privileges to those of the domain administrator account. An attacker could use these elevated privileges to compromise any computer in the domain, including domain controllers. An attacker must have valid domain credentials to exploit this vulnerability. The affected component is available remotely to users who have standard user accounts with domain credentials; this is not the case for users with local account credentials only. When this security bulletin was issued, Microsoft was aware of limited, targeted attacks that attempt to exploit this vulnerability.

This security update is rated Critical for all supported editions of Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. The update is also being provided on a [defense-in-depth](#) basis for all supported editions of Windows Vista, Windows 7, Windows 8, and Windows 8.1. For more information, see the **Affected Software** section.

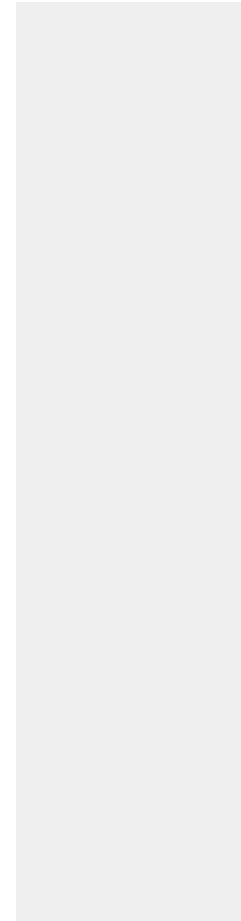
The security update addresses the vulnerability by correcting signature verification behavior in Windows implementations of Kerberos. For more information about the vulnerability, see the **Frequently Asked Questions (FAQ)** subsection for the specific vulnerability.

For more information about this update, see [Microsoft Knowledge Base Article 3011780](#).

<https://technet.microsoft.com/en-us/library/security/ms14-068.aspx>

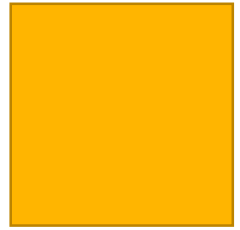
# Tuesday Night 18/11/2014

- After reviewing notification decision to patch everything is made
- Email WSUS Admin to confirm release to test environment
- Check if test environment running (Done Remotely)
- WSUS Admin syncs WSUS server with Microsoft (Done Remotely)
- WSUS Admin releases the updates in WSUS (Done remotely)

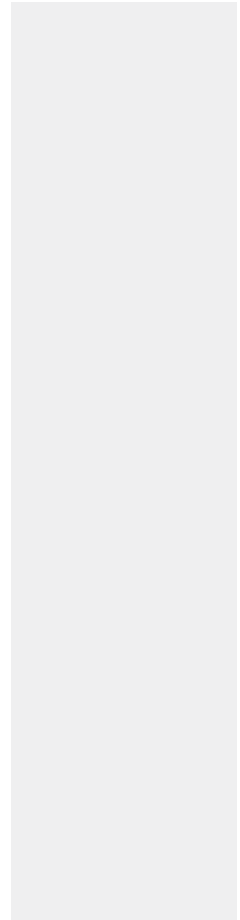




# Wednesday 19/11/2014



- Wednesday 10:00
  - Escalate the requirement for immediate patching to management to notify business owners of impending patching and reboots.
  - IT Services website news article published
- Wednesday 10:30 – 13:00
  - Test updates in test environment (updates delivered via WSUS)
- Wednesday 10:30 – 13:30
  - Create software update packages for client and server operating systems that will be deployed via SCCM
  - Create two new server collections that are divided based on server name A-L and M-Z
    - Separate resilient services into the different groups
    - Two new maintenance windows at 18:00 to 20:00 for Wed & Thurs



# Wednesday 19/11/2014

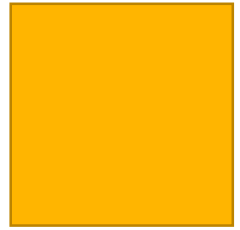
- Wednesday 15:00 – 17:30
  - Manually update domain controllers (updates delivered via SCCM)
- Wednesday 18:00 – 20:00
  - 1<sup>st</sup> Server Collection Maintenance Window in SCCM
  - Some manual intervention required on some W2k8R2 machines
- Wednesday 21:00
  - Deadline for updates delivered via SCCM for client OS machines
- Thursday 00:00 – 01:00
  - Deadline for updates to virtualization hosts that host 1<sup>st</sup> Server collection VM's and reboot

# Thursday 20/11/2014



- Thursday Morning
  - Verify status of the updates from previous day and resilient services ok after patch installation
- Thursday 18:00 – 20:00
  - 2<sup>nd</sup> Server Collection Maintenance Window in SCCM
- Friday 00:00 – 01:00
  - Deadline for updates to virtualization hosts that host 2nd Server Collection VM's and reboot

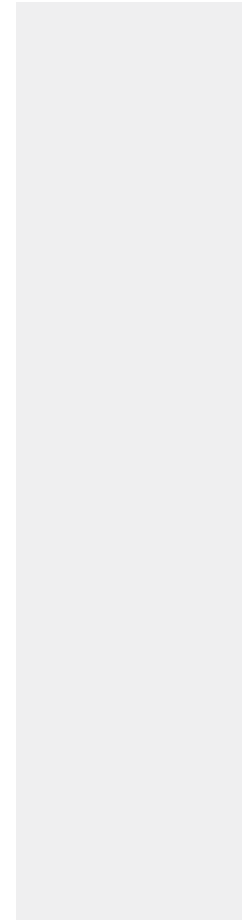
# Friday 21/11/2014



- Check compliance of machines

Available	↕	Deadline	↕	Last State	↕	Count of Computers	↕	% of Total
19/11/2014 13:27:00		20/11/2014 18:00:00		Compliant		68		91.89
19/11/2014 13:27:00		20/11/2014 18:00:00		Enforcement state unknown		6		8.11

- Close out update process for servers



# Post update review

- Change the configuration of SCCM agent profile on Servers
  - The poll interval for the Software Updates is to be shortened
- Maintenance window for client operating systems needed
  - All machines are not equal e.g. a PC connected to an incubator needs to be restarted in a controlled manner vs an admin user
- Document how to update Windows Server Minimal Shell systems
- Review how to do updates in the middle of an update cycle
  - Some issues with the updates were as a result of the fact we were in the middle of an update cycle

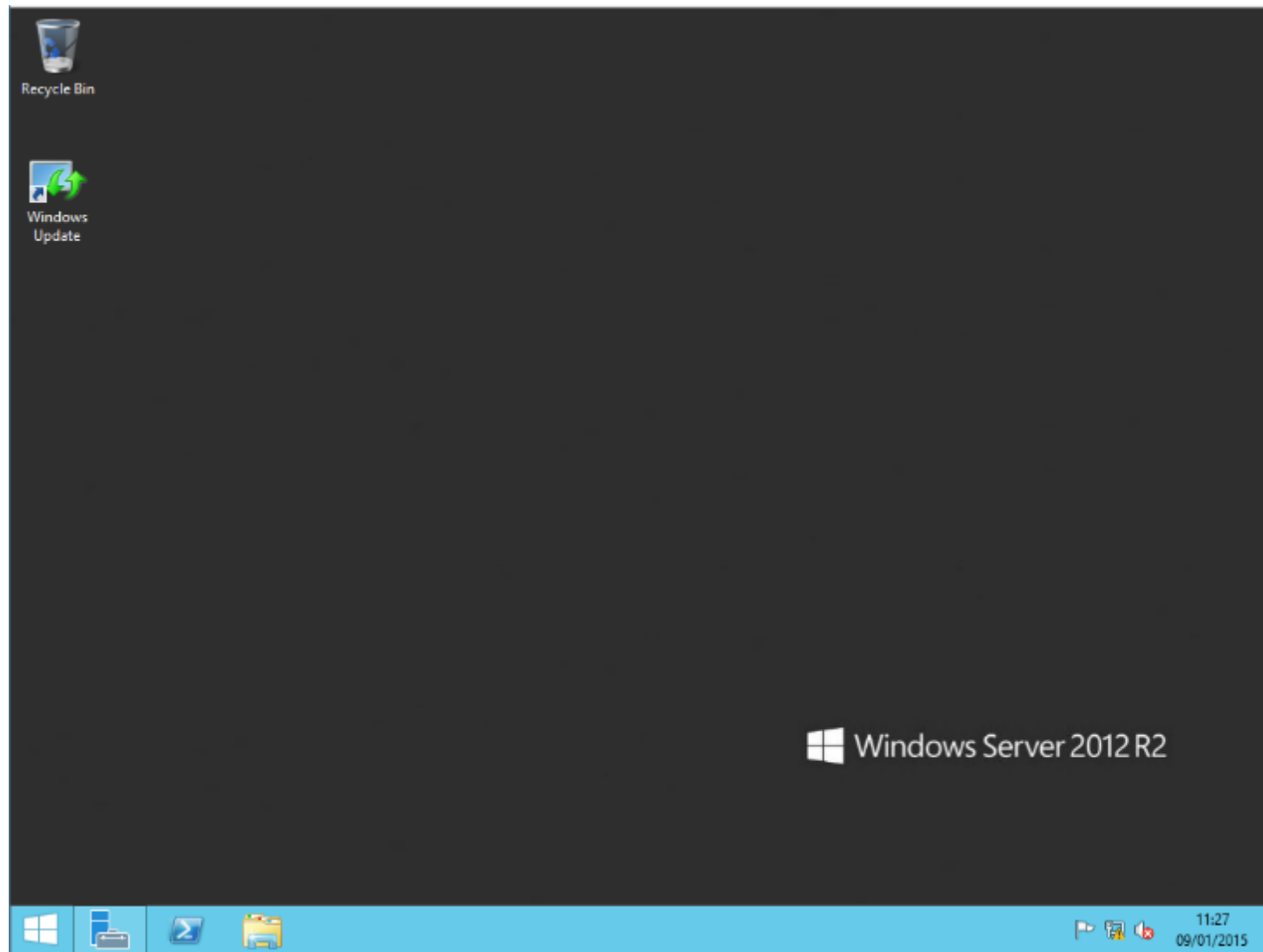
# Administrative Effort involved

- How many people does it take to deploy the updates to the windows environment?
  - 2 people. WSUS/SCCM administrator manages the release of updates and has responsibility for Windows Client machines. A Windows Server Administrator to test and apply updates on servers
- How many hours were put in to releasing this update?
  - Approximately 14 man hours between evaluation, testing, release of updates (between 2 people)
- What was the latest time that the update team worked until?
  - Apart from the initial WSUS release which was done remotely, the Wednesday was a 19.30 finish and the Thursday was a 18.30 finish
- How long to patch the Windows Client OS?
  - After 48 hours the majority of the switched on client computers on the campus network are patched

Thanks for listening.  
Any Questions?

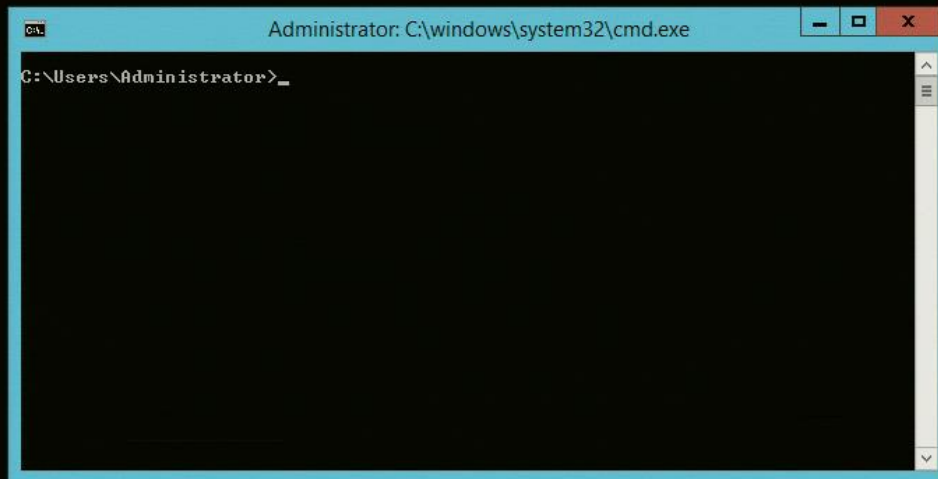


# Windows Server GUI

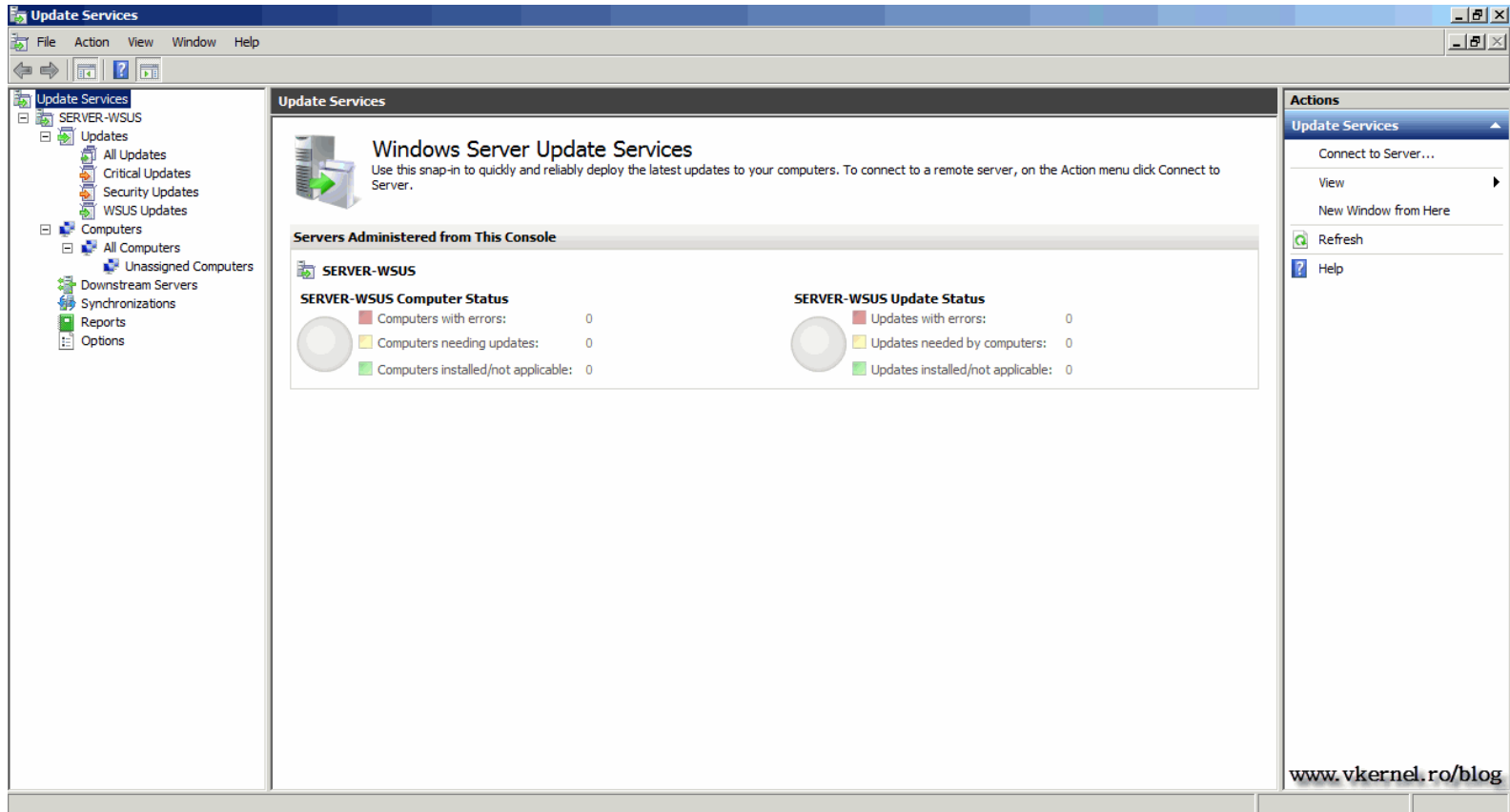




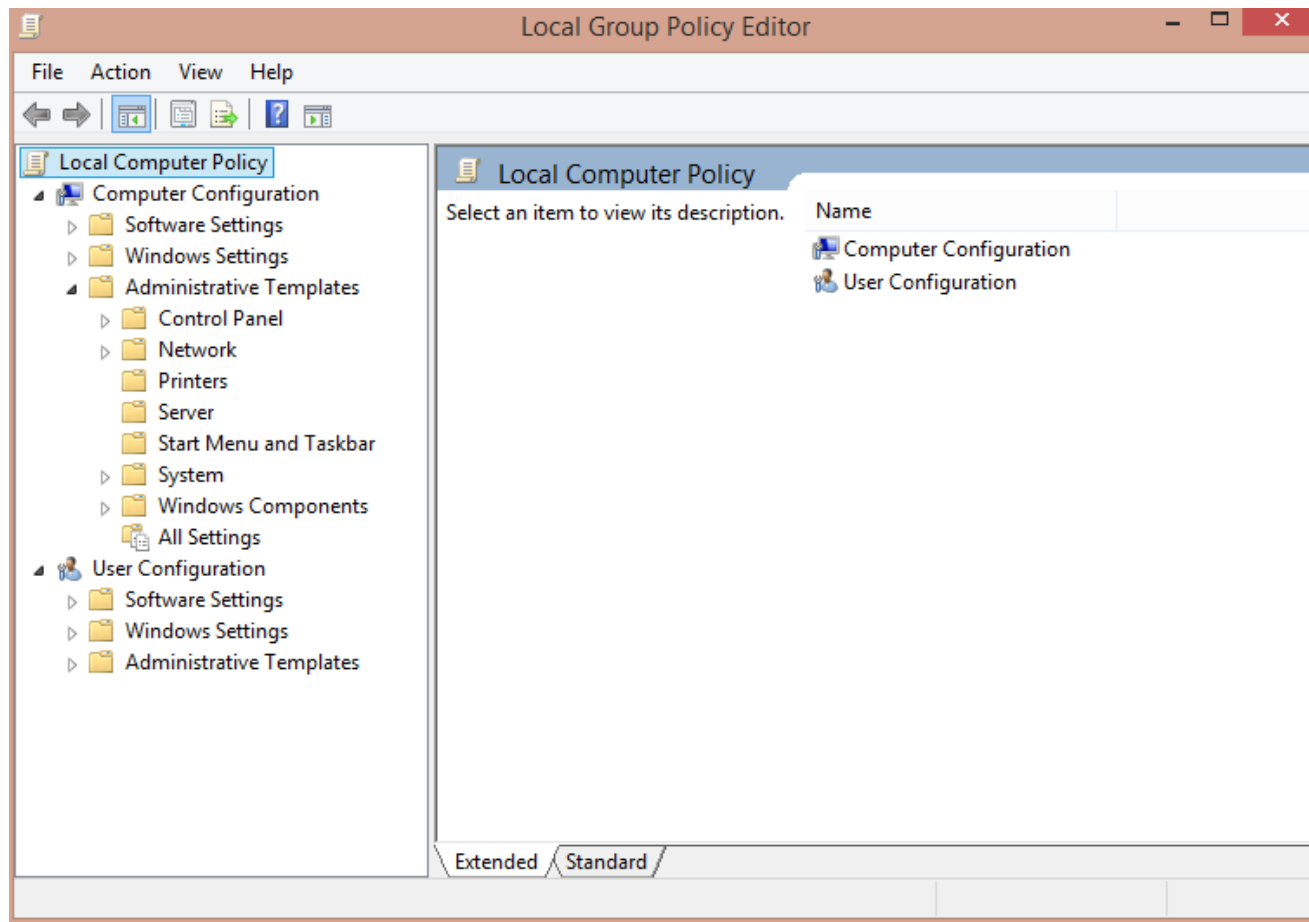
# Windows Server Core



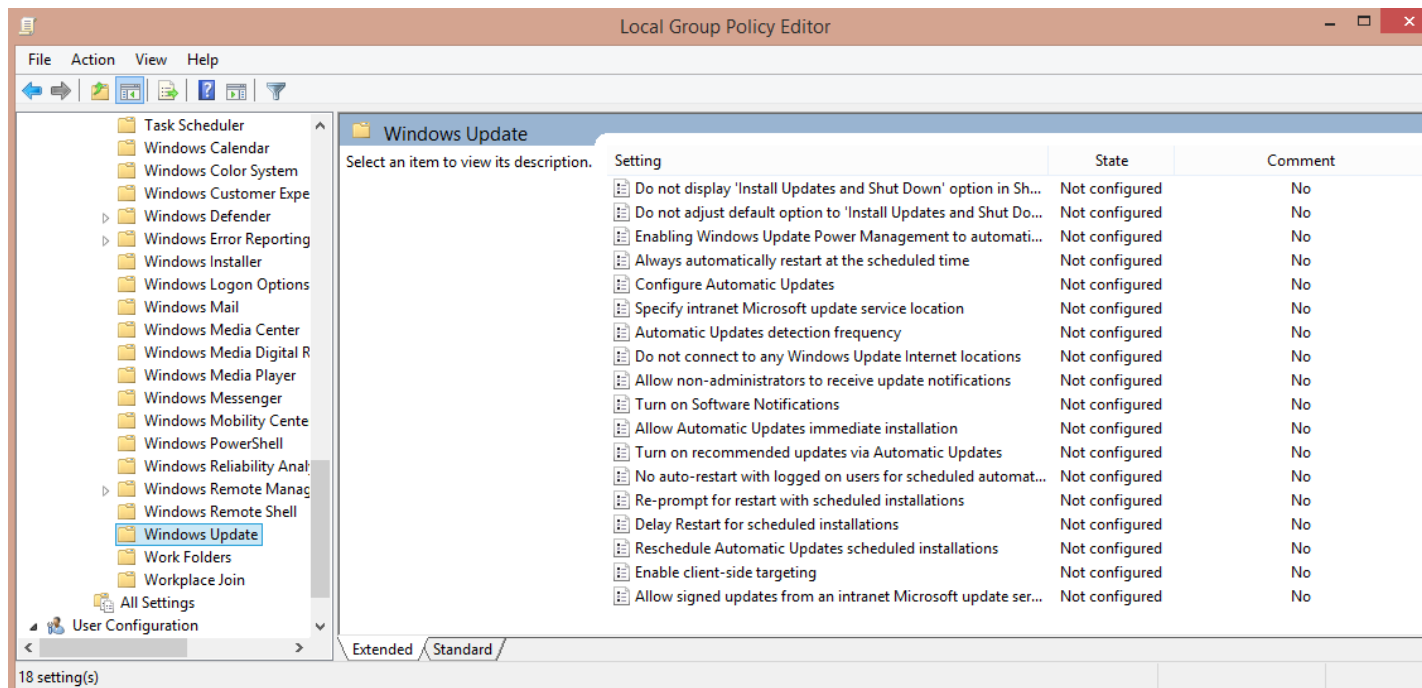
# WSUS Console



# Local Group Policy



# Local Group Policy – Windows Update Settings



# Local Group Policy – Configure Automatic Updates

Configure Automatic Updates

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on: Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3

Options:

Configure automatic updating:  
3 - Auto download and notify for install

The following settings are only required and applicable if 4 is selected.

☐ Install during automatic maintenance

Scheduled install day:  
0 - Every day

Scheduled install time: 03:00

Help:

Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

Note: This policy does not apply to Windows RT.

This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:

2 = Notify before downloading and installing any updates.

When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any available updates.

3 = (Default setting) Download the updates automatically and notify when they are ready to be installed

Windows finds updates that apply to the computer and

OK Cancel Apply

# Local Group Policy – update service location

Specify intranet Microsoft update service location

Specify intranet Microsoft update service location Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on: At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, excluding Windows RT

Options:

Set the intranet update service for detecting updates:

Set the intranet statistics server:

(example: http://IntranetUpd01)

Help:

Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network.

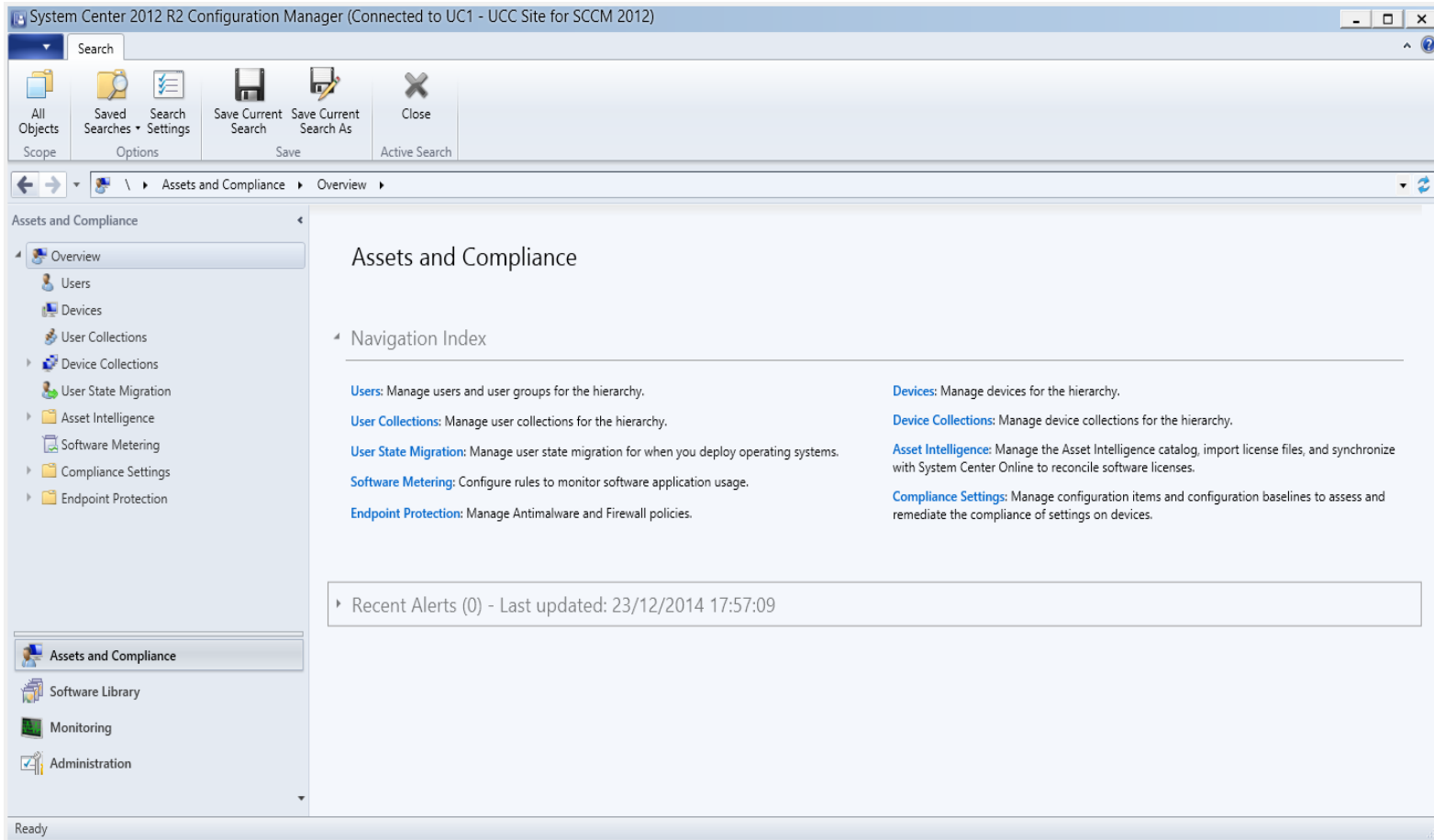
This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network.

To use this setting, you must set two servername values: the server from which the Automatic Updates client detects and downloads updates, and the server to which updated workstations upload statistics. You can set both values to be the same server.

If the status is set to Enabled, the Automatic Updates client connects to the specified intranet Microsoft update service, instead of Windows Update, to search for and download updates. Enabling this setting means that end users in your organization don't have to go through a firewall to get updates, and it gives you the opportunity to test updates before deploying

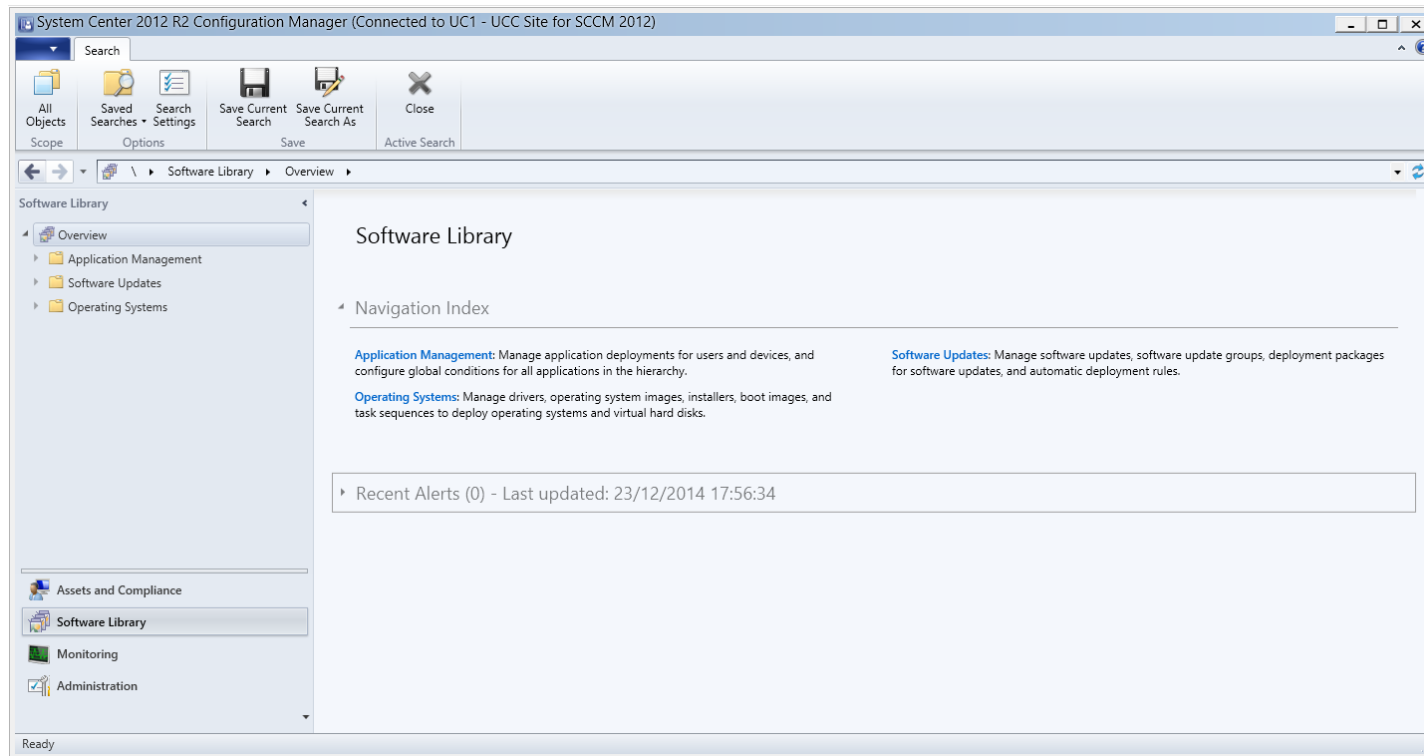
OK Cancel Apply

# SCCM Management Console - Assets and Compliance



# SCCM Management Console

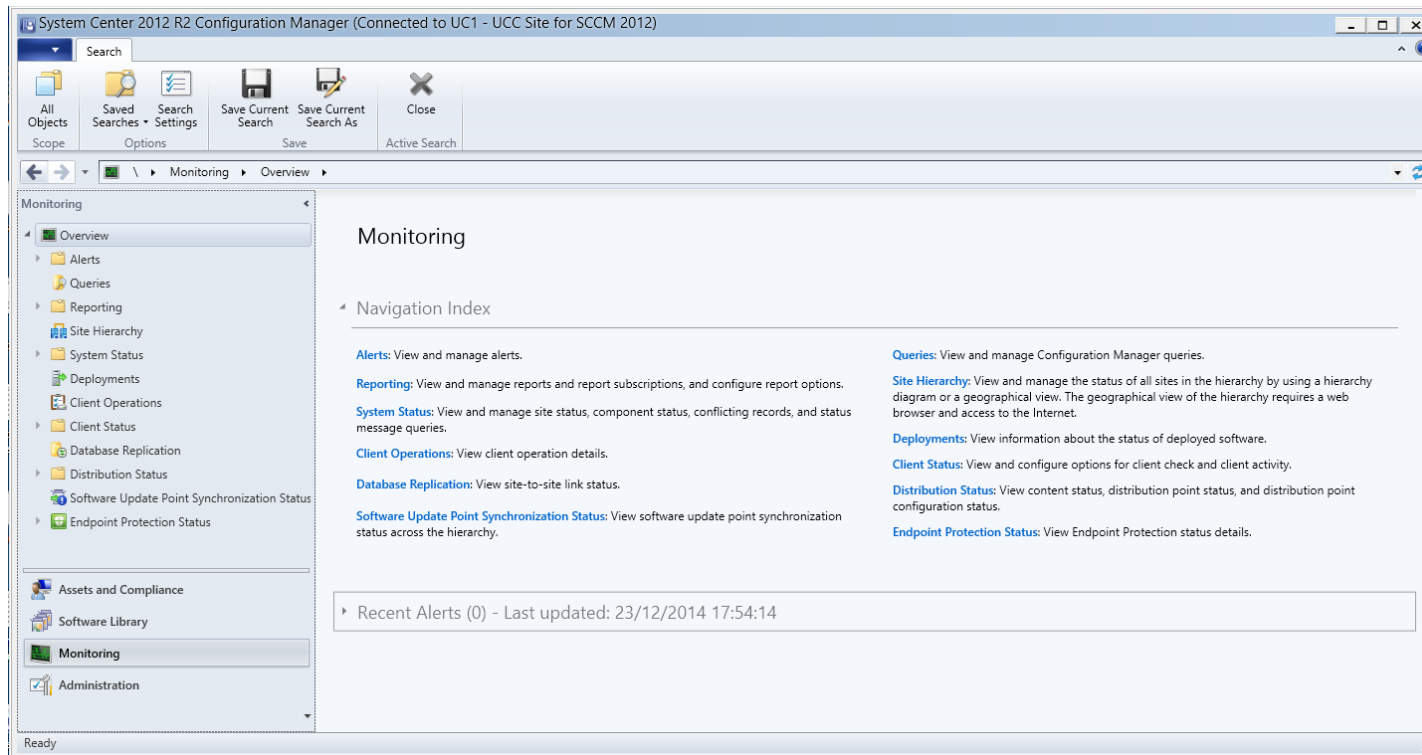
## - Software Library





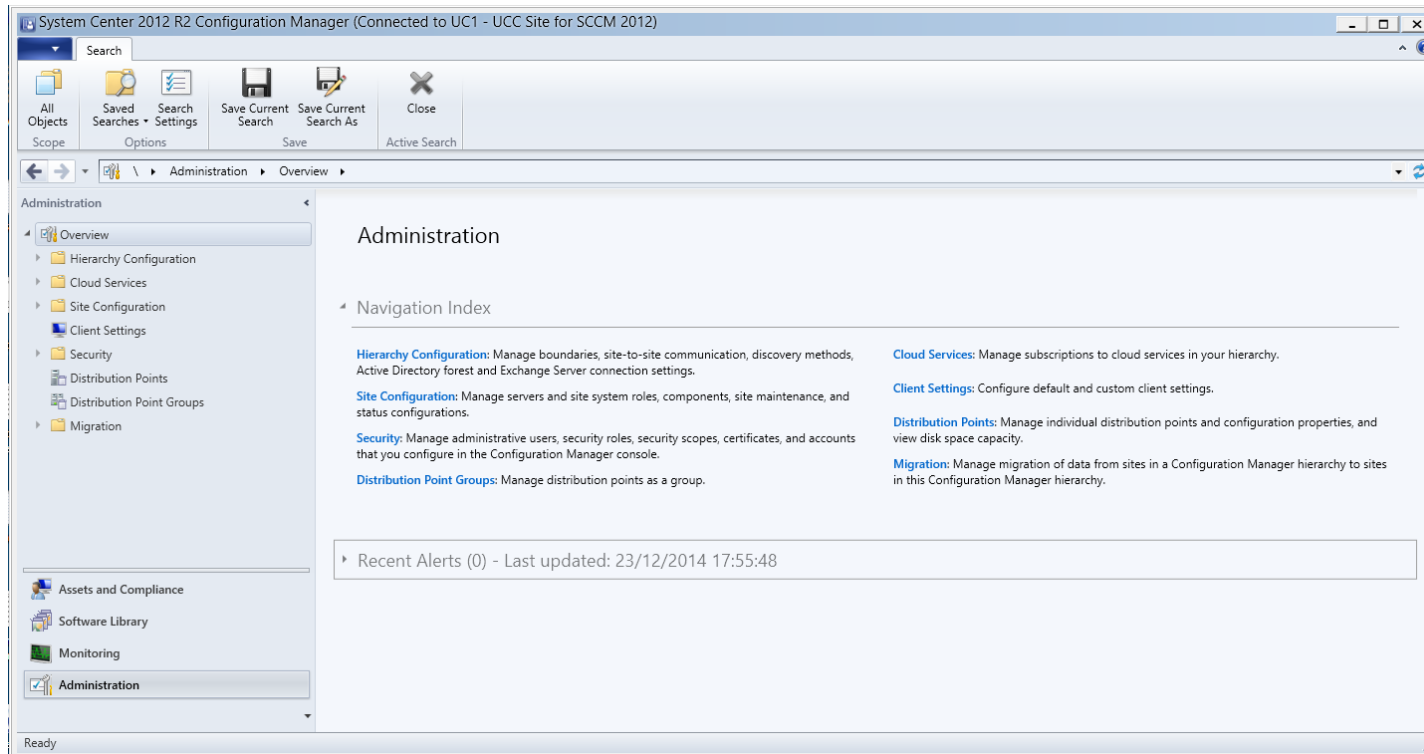
# SCCM Management Console

## - Monitoring



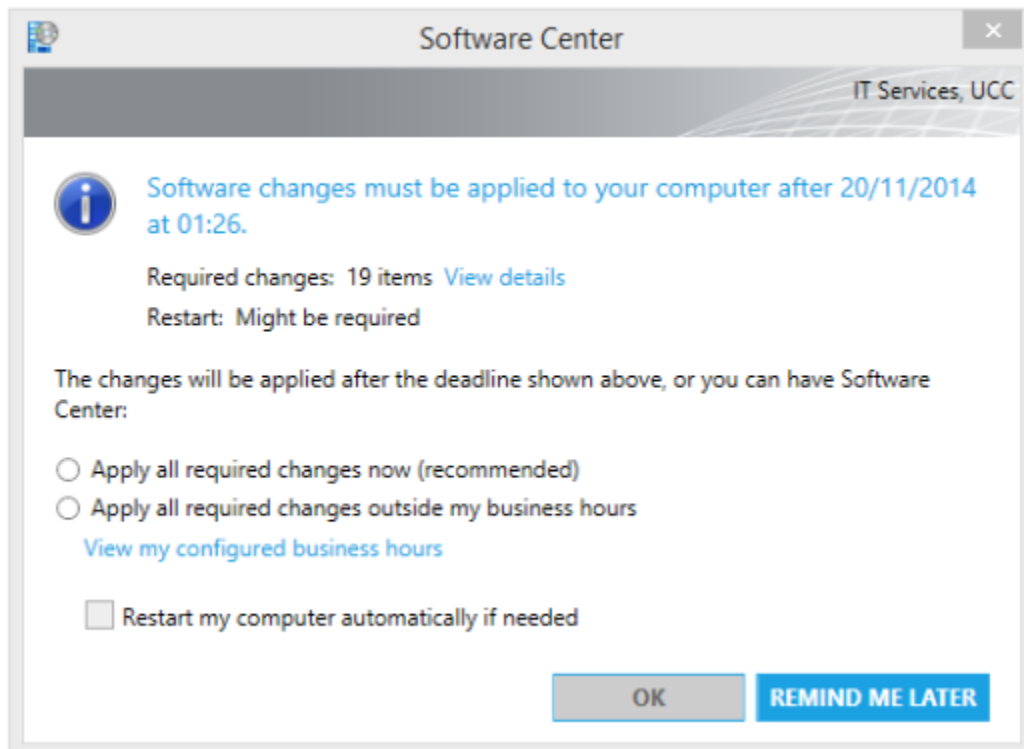
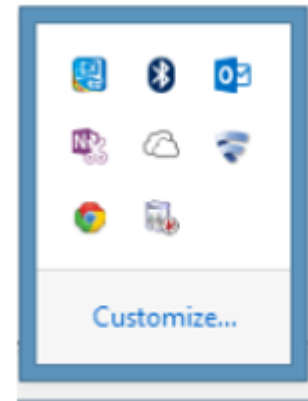
# SCCM Management Console

## - Administration



# SCCM Download Icons

Downloading and installing software  
Click to view progress.



# Software Centre – View Details

Software Center

IT Services, UCC

Available Software

Installation Status

Installed Software

Options

SHOW

Updates

☐ Show optional software

SEARCH

Find additional applications from the Application Catalog

<input type="checkbox"/>	NAME	TYPE	PUBLISHER	AVAILABLE AFTER	STATUS
<input type="checkbox"/>	Cumulative Security Update for Internet Explorer 11 for Windows 8.1 for x...	Update	Microsoft	13/11/2014	Past due - will be installed
<input type="checkbox"/>	Security Update for Internet Explorer Flash Player for Windows 8.1 for x...	Update	Microsoft	13/11/2014	Past due - will be installed
<input type="checkbox"/>	Security Update for Microsoft .NET Framework 3.5 on Windows 8.1 and...	Update	Microsoft	13/11/2014	Past due - will be installed
<input type="checkbox"/>	Security Update for Microsoft .NET Framework 4.5.1 and 4.5.2 on Windo...	Update	Microsoft	13/11/2014	Past due - will be installed
<input type="checkbox"/>	Security Update for Windows 8.1 for x64-based Systems (KB2992611)	Update	Microsoft	13/11/2014	Past due - will be installed
<input type="checkbox"/>	Security Update for Windows 8.1 for x64-based Systems (KB2993958)	Update	Microsoft	13/11/2014	Past due - will be installed
<input type="checkbox"/>	Security Update for Windows 8.1 for x64-based Systems (KB3002885)	Update	Microsoft	13/11/2014	Past due - will be installed
<input type="checkbox"/>	Security Update for Windows 8.1 for x64-based Systems (KB3003743)	Update	Microsoft	13/11/2014	Past due - will be installed
<input type="checkbox"/>	Security Update for Windows 8.1 for x64-based Systems (KB3005607)	Update	Microsoft	13/11/2014	Past due - will be installed
<input type="checkbox"/>	Security Update for Windows 8.1 for x64-based Systems (KB3006226)	Update	Microsoft	13/11/2014	Past due - will be installed
<input type="checkbox"/>	Security Update for Windows 8.1 for x64-based Systems (KB3010788)	Update	Microsoft	13/11/2014	Past due - will be installed
<input type="checkbox"/>	Security Update for Windows 8.1 for x64-based Systems (KB3011780)	Update	Microsoft	13/11/2014	Past due - will be installed
<input checked="" type="checkbox"/>	Update for Windows 8.1 for x64-based Systems (KB2976536)	Update	Microsoft	13/11/2014	Past due - will be installed
<input type="checkbox"/>	Update for Windows 8.1 for x64-based Systems (KB2976978)	Update	Microsoft	13/11/2014	Past due - will be installed
<input type="checkbox"/>	Update for Windows 8.1 for x64-based Systems (KB3003667)	Update	Microsoft	13/11/2014	Past due - will be installed
<input type="checkbox"/>	Update for Windows 8.1 for x64-based Systems (KB3006178)	Update	Microsoft	13/11/2014	Past due - will be installed
<input type="checkbox"/>	Update for Windows 8.1 for x64-based Systems (KB3008188)	Update	Microsoft	13/11/2014	Past due - will be installed
<input type="checkbox"/>	Update for Windows 8.1 for x64-based Systems (KB3008627)	Update	Microsoft	13/11/2014	Past due - will be installed
<input type="checkbox"/>	Windows Malicious Software Removal Tool for Windows 8, 8.1 and Win...	Update	Microsoft	13/11/2014	Past due - will be installed

Update for Windows 8.1 for x64-based Systems (KB2976536)

OVERVIEW

Status: Past due - will be installed  
Help document: [Click here](#)  
Bulletin ID: None  
Article ID: 2976536

REQUIREMENTS

Restart required: Might be required

DESCRIPTION

Install this update to improve protection functionality in Windows Defender. See the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

SCHEDULE

INSTALL

# Application Catalog

[Application Catalog](#) [My Application Requests](#) [My Devices](#)

Welcome,





Search Application Catalog


BROWSE BY

Category [Publisher](#)

All

Showing 1 - 4 of 4 results

NAME	VERSION	PUBLISHER	CATEGORY	REQUIRES APPROVAL
 Adobe Reader 11.0.07 (PS)				No
 Java 6 Update 45				No
 Microsoft Office Professional Plus 2013	2013	Microsoft		No
 Panopto Recorder 4.6				No

 **Adobe Reader 11.0.07 (PS)**  
No description available  
[More Details](#)

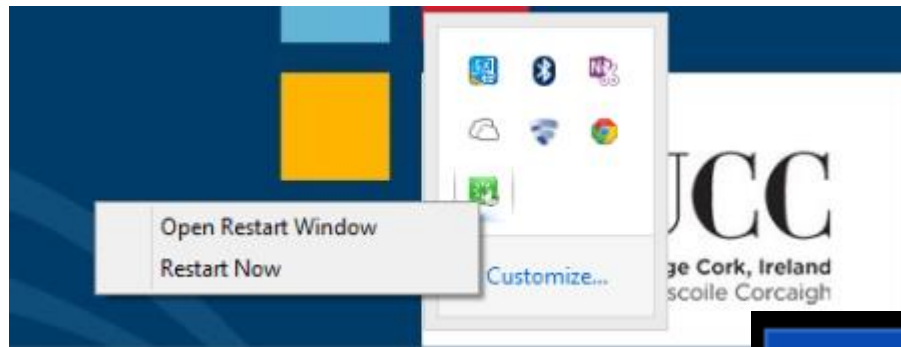
INSTALL

ITS - University College Cork

First Prev 1 Next Last

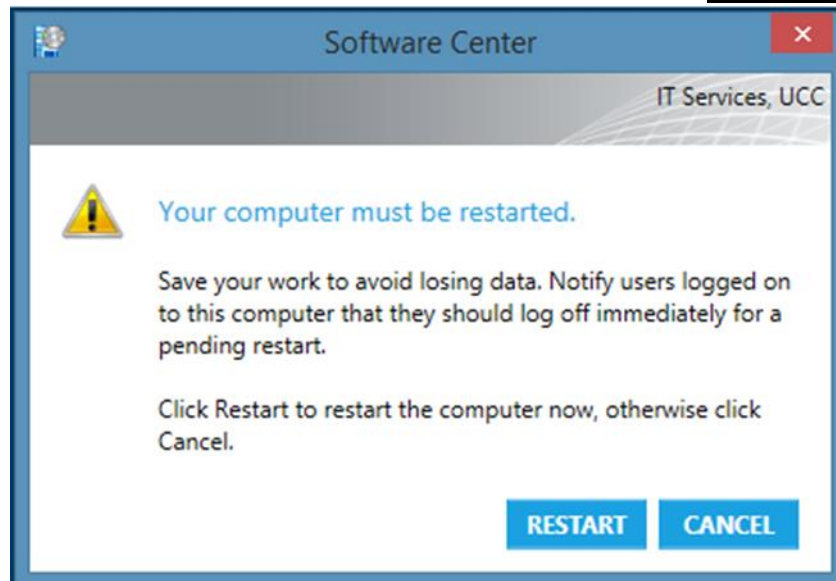
Microsoft System Center 2012 R2 Configuration Manager

# SCCM Restart Icons



## Restart required

Recently installed software requires your computer to restart to complete the...



You have really reached  
the end now 😊