ARIZONA WESTERN COLLEGE – ITSS

**Windows Patch Management**

**Version 1.000**

# **Disclaimers**

The information contained in this document is the proprietary and exclusive property of Arizona Western College except as otherwise indicated. No part of this document, in whole or in part, may be reproduced, stored, transmitted, or used for design purposes without the prior written permission of Arizona Western College.

The information contained in this document is subject to change without notice.

The information in this document is provided for informational purposes only. Arizona Western College specifically disclaims all warranties, express or limited, including, but not limited, to the implied warranties of merchantability and fitness for a particular purpose, except as provided for in a separate software license agreement.

# **Privacy Information**

This document may contain information of a sensitive nature. This information should not be given to persons other than those who are involved in the Windows Patch Management project or who will become involved during the lifecycle.

# **Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| REVISION CHART | | | |
| Version | Author(s) | Description of Version | Date Completed |
| 1.0 | Robert Schroeder | Created document | 10-12-2020 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# **Document Owner**

The primary contact for questions regarding this document is:

Author: Academic & Administrative Technology Coordinator

Windows Patch Management

# **Document Approval**

Document Name: Windows Patch Management

Publication Date:

Prepared by:

Approval: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

***Name and Organization***

Concurrence: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

***Name and Organization***

Table of Contents

1. **Introduction**
   1. Purpose of this document
   2. Scope
   3. Overview
   4. References
2. **System Overview**
   1. **System Overview**
3. **System Architecture**
   1. **Product Components**
   2. **Decomposition Description**
   3. **Design Rationale**
4. **Human Interface Design**
   1. **Overview of the User Interface**
   2. **Screen Images**
   3. **Screen Objects and Actions**
5. **Requirements Matrix**
   1. **Site Systems**
   2. **Clients**
6. **Arizona Western College Patch Management Configuration**
   1. **Group Policy (GPO)**
   2. **Initial Update**
   3. **Scanning Schedule**
   4. **Patch Policy Membership**
      1. **Patch Policy Approvals**
   5. **Automatic Patch Updates**
   6. **Reboot Action Policy**

1 Introduction

* 1. **Purpose of this document**

**The purpose of this document is to describe the implementation of the Windows Patch Management and serve as an overall guidance to the architecture of Windows Patch Management.**

* 1. **Scope**

**Patch Management is the process of distributing and applying updates to software. These patches are often necessary to correct errors (or vulnerabilities) in the software. This process can prevent software from being vulnerable to bugs, malware, and major issues. Successful implementation of Patch Management can help ensure every Arizona Western College managed and owned device on the AWC network is up to date.**

* 1. **Overview**

**This document is divided into 5 sections with various subsections. The sections of the document are:**

* **Introduction**
* **System Overview**
* **System Architecture**
* **Human Interface Design**
* **Requirements Matrix**
  1. **References**

*Kaseya - Patch Management Documentation*, 19 Dec. 2019, help.kaseya.com/webhelp/EN/KPATCH/9050000/EN\_kpatchguide\_R95.pdf.

2 System Overview

**2.1 System Overview**

Arizona Western College currently uses the Kaseya system platform for distributing and applying patches to Windows OS systems.

When Kaseya VSA is used for Windows Patch Management, it provides a comprehensive enterprise management solution that allows Arizona Western College ITSS department to:

* Keep software patching up to date to maintain security of IT infrastructure and remediate critical software vulnerabilities.
* Gain full control over patching including the ability to skip problematic patches by automating the process with scripts.
* Set up patch reports to see compliance across entire environment and identify endpoints that need attention.
* Gain visibility into CVEs by aggregating the patch status of IT environment into one dashboard.
  1. System Architecture

**3.1 Product Components**

**Table – Main components**

|  |  |
| --- | --- |
| **Component** | **Description** |
| **Kaseya Server** | **Kaseya VSA is a server used for Remote Monitoring and Management (RMM), Endpoint Management, and Network Monitoring in a single console. Major components of the Kaseya VSA are:**   * **High Powered Automation.** * **Remote Control.** * **Discovery & Inventory.** * **Patch Management** * **Monitoring & Alerts** |
| **Supported Operating Systems** | **Patch Management supports all OSs supported by Windows Update which includes:**  **-Microsoft Windows Server 2012, 2012 R2, 2016, 2019**  **-Microsoft Windows 8, 8.1, 10** |

**3.2 Decomposition Description**

**Kaseya VSA Patch Management architecture uses five methods of applying Microsoft patches to managed Windows machines:**

* **Initial Update**
  + ***One-time* processing of all approved Microsoft patches applicable to a managed machine based on Patch Policy. Initial Update ignores the Reboot Action policy and reboots the managed device without warning to the user as often as necessary until the machine has been brought up to the latest patch level. Initial Update should only be performed during non-business hours and is typically performed on newly added machines.**
* **Automatic Update**
  + **This is the preferred method of updating managed devices on a recurring basis. Automatic Update obeys both the Patch Policy and Reboot Action policy.**
* **Patch Update**
  + **Patch Update is used on an exception basis to apply individual patches to multiple machines or for patches that originally failed on certain machines. Patch Update overrides the Patch Policy but obeys the Reboot Action policy.**
* **Machine Update**
  + **Machine Update is used on an exception basis to apply patches to individual machines. Machine Update overrides the Patch Policy but obeys Reboot Action policy. Machine Update could be used to test a new patch prior to approving it for general release to all machines.**
* **Patch Deploy**
  + **A user defined procedure to install Microsoft patches can be used using Agent Procedures > Patch Deploy. The Patch Management module in the VSA uses Microsoft Update Catalog and the Office Detection Tool as it’s data sources for Patch Management. Patch Deploy enables Arizona Western College ITSS Department to create a patch installation procedure for hot fixes, via a wizard, to be can be used to schedule the installation on any desired machine that are not included in the Microsoft Update Catalog or the Office Detection Tool.**

**3.3 Design Rationale**

* **Cost – Arizona Western College has purchased licensing for the use of Kaseya VSA. The patch management model was included in this licensing.**
* **Usability – Every Arizona Western College owned and managed Windows device will receive a Kaseya endpoint agent installed. This agent checks in with the Kaseya VSA server frequently. With the agent already installed on each device, it makes the integration with the patch management module simple to use.**
* **Efficiency – Kaseya VSA allows Arizona Western College ITSS Department to manage endpoints including remote management and patch management from one console.** 
  1. Human Interface Design

**4.1 Overview of the User Interface**

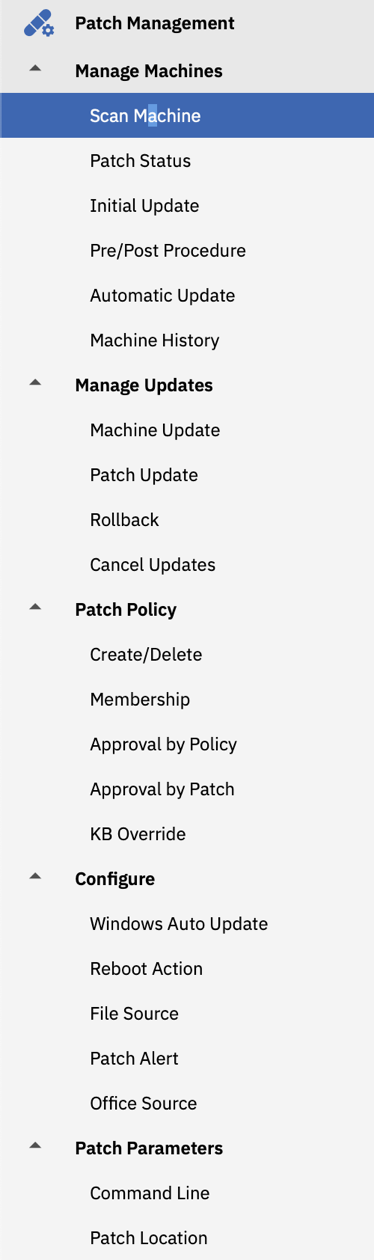
**Windows**

**The Kaseya VSA shows up on a user’s computer as an icon in the system tray. There is no other UI provided for the user.**

**For administrators of Kaseya VSA, the UI for management of packages will be done via the web interface. Currently the web address for the Kaseya VSA is:** <https://pcmgmt.azwestern.edu>

**4.2 Screen Images**

**Patch Management Module via Kaseya VSA:**

****

**4.3 Screen Objects and Actions**

**Patch Management Module via Kaseya VSA:**

**The Patch Management module of Kaseya VSA is divided into five main sections which can be accessed by the tab structures inside the module.**

**The following is a description of options within the tab structure:**

* **Manage Machines – Used for scanning, looking at Patch Status, Initial Updates, Automatic Update management, and Machine History**
* **Manage Updates – Used for Machine Updates, Patch Updates, Rollbacks, and Cancelling Updates**
* **Patch Policy – Allows for creation of policies, managing membership to policies, managing approvals by policy or patch, and KB Overrides.**
* **Configure – Allows for configuration of Auto Update, Reboot Actions, Patch Alerts, and File Sources**
* **Patch Parameters – Used to view specific information related to each patch such as KB Article, products, and installation switches.** 
  1. Requirements Matrix

The following recommendations are guidelines to help you scale your System Center Configuration Manager environment to support more than a very basic deployment of sites, site systems, and clients. They are not intended to cover all possible site and hierarchy configurations.

Use the information in the following sections as a guide to help you plan for hardware that can meet the processing loads for clients and sites that use the available Configuration Manager features with the default configurations.

**5.1 Server Systems**

Patch Management Module Minimum Server Requirements

1. The Patch Management R95 module requires VSA R95

**5.2 Clients**

Patch Management Module Minimum Client Requirements

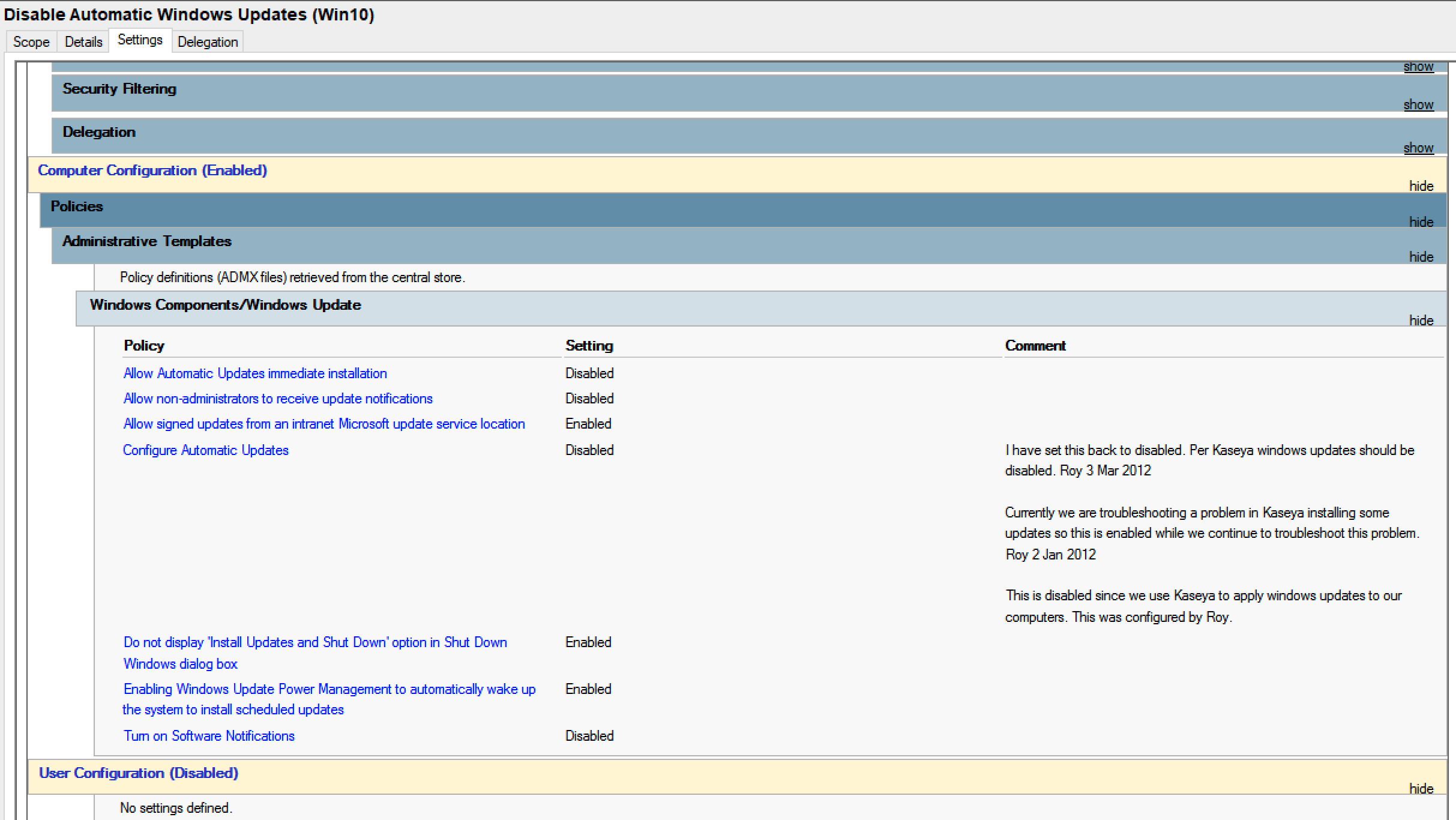
1. Microsoft Server 2012, 2012 R2, 2016, 2019
2. Microsoft Windows 8, 8.1, 10
   1. Arizona Western College Patch Management Configuration

**The following represents the current configuration of Windows Patch Management solution via Kaseya VSA for Arizona Western College.**

**6.1 Group Policy (GPO)**

**For the purpose of allowing the Kaseya VSA Patch Management module to distribute and apply patch updates, built in Windows Update needs to be disabled. There is a Group Policy Object (GPO) created and deployed in the AWC environment. The current GPO is linked to the adroot > AZW > Computers OU in Active Directory. The object is named ‘Disable Automatic Windows Updates (Win 10)’.**

**The settings that are being defined in the GPO are in Computer Configuration > Policies > Administrative Templates > Windows Components/Windows Update. Below is a snapshot of the settings that are being defined.**



**6.2 Initial Update**

**Initial Update is a one-time processing of all approved Microsoft patches applicable to a managed machine based on Patch Policy. This method of applying updates ignores any configured Reboot Action. Policy and will reboot the managed device without warning to the user as often as necessary until the machine has been brought up to the latest patch level.**

**For use in the Arizona Western College ITSS Department, Initial Update should only be used on newly deployed devices before given to the end user.**

**6.3 Scanning Schedule**

**The purpose of scanning a machine is to search for missing patches on each managed machine. Scanning takes very little resources and can be safely scheduled to run at any time of day. The scanning operation does not impact users at all.**

**Arizona Western College ITSS Department currently uses a reoccurring scan schedule for all managed devices. Scanning is conducted in the following configuration:**

* **Recurrence: Weekly**
* **Time Preference: Schedule will be based on timezone of the agent (rather than server)**
* **Weekly Schedule Options:** 
  + **Run at 8:00 AM**
  + **Distribution Window: 2 Day**
  + **Every: 1 week(s)**
  + **On: Monday**
* **Start/End**
  + **Ending after: No end date**
* **Execution Options**
  + **Exclude the following time range**
    - **From: 7:00 am**
    - **Through 11:30 am**

**6.4 Patch Policy Membership**

**The Membership page assigns devices to one or more patch policies. Patch policies contain all active patches for the purpose of approving or denying patches. An active patch is defined as a patch that has been reported by a patch scan by at least one machine in the VSA. Any machine can be made a member of one or more patch polices. Note:**

* **Patches of machines that are not a member of any patch policy are treated as if they were automatically approved.**
* **When a new patch policy is created the default approval status is pending approval for all patch categories.**
* **The default approval status for each category of patches and for each product can be individually set.**
* **If a machine is a member of multiple patch policies and those polices have conflicting approval statuses, the most restrictive approval status is used.**
* **Initial Update and Automatic Update require patches be approved before these patches are installed.**
* **Approval by Policy approves or denies patch by policy**
* **Approval by Patch approves or denies a patch and sets the approval status for that patch in all patch polices.**
* **KB Override overrides the default approval status by KB Article for al patch polices and sets the approval status for patches associated with the KB Article in all patch polices.**
* **Patch Update and Machine Update can install denied patches.**
* **Non-Master role users can only see patch polices they have created or patch policies that have machine IDs the user is authorized to see based on their scope.**

**Arizona Western College ITSS Department uses a 3 ring patch management membership policy. For Windows 10 updates, these memberships include Windows 10 – Ring 1, Windows 10 – Ring 2, and Windows 10 – Ring 3.**

**Windows 10 – Ring 1: This ring is used for first round of patch policy application. This is a small set of devices that receive the first round of patches.**

**Windows 10 – Ring 2: This ring is used for selected power users as a secondary test phase of patches.**

**Windows 10 – Ring 3: This ring is for general availability for all approved patches.**

**6.4.1 Patch Policy Approvals**

**Patch Policy approvals for Arizona Western College for each ring are currently being approved by the Arizona Western College System Administrator.**

**6.5 Automatic Patch Updates**

**Automatic Update is the preferred method of updating managed devices with Microsoft patches on a recurring basis. Automatic Update obeys both the Patch Approval Policy and the Reboot Action policy.**

**Arizona Western College ITSS Department Automatic Update Windows 10 – Ring 3 scheduling configuration listed below:**

* **Recurrence: Monthly**
* **Time Preference: Schedule will be based on timezone of the agent (rather than server)**
* **Monthly Schedule Options:** 
  + **Run at 8:00 AM**
  + **Distribution Window: 1 Day**
  + **Every: 1 month(s)**
  + **On the: Last Thursday**
* **Start/End**
  + **Ending after: No end date**
* **Execution Options**
  + **Exclude the following time range**
    - **From: 7:00 am**
    - **Through 11:30 am**

**6.6 Reboot Action Policy**

**The Reboot Action defines how reboots are performed after a patch install. Patch installs do not take effect until after a machine is rebooted. If the device that requires a reboot for completion of the patch installation, the reboot action is configured as ‘Skip reboot if user logged in’. All other computers are configured as ‘If user logged in ask to reboot every 60 minutes until the reboot occurs. Reboot if the user not logged in’.**