Technical Guide



Configuration Manager 1610

Prepared for

[Type Customer Name Here]

9/22/2017

Version 1 Draft

Prepared by

**Janusz Gal**

[Type Author Position Here]

[Type Author Email Here]

Contributors

**[Type Contributors Here]**

Revision and Signoff Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
|  |  | 1 | Initial draft for review/discussion |
|  |  |  |  |
|  |  |  |  |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version Approved | Position | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Overview 7](#_Toc474852465)

[2 Technical Design 8](#_Toc474852466)

[2.1 Core Infrastructure Dependencies 10](#_Toc474852467)

[2.2 Environment Prerequisites 11](#_Toc474852468)

[2.3 Software Update Delivery 12](#_Toc474852469)

[2.4 Current Branch 15](#_Toc474852470)

[2.5 Current Branch for Business 17](#_Toc474852471)

[2.6 Long Term Servicing Branch 18](#_Toc474852472)

[3 Technical Implementation 20](#_Toc474852473)

[3.1 Implementation Activities and Tasks 21](#_Toc474852474)

[3.2 Prepare Environment 21](#_Toc474852475)

[3.3 Service System Center Configuration Manager 24](#_Toc474852476)

[3.4 Configure Software Update Delivery 26](#_Toc474852477)

[3.5 Configure & Deploy Group Policy Objects 29](#_Toc474852478)

[3.6 Service Windows 10 Devices 30](#_Toc474852479)

[4 Test Plan 31](#_Toc474852480)

[4.1 System Center Configuration Manager Upgrade Testing 32](#_Toc474852481)

[4.2 Software Update Delivery 32](#_Toc474852482)

[4.3 Current Branch 33](#_Toc474852483)

[4.4 Current Branch for Business 34](#_Toc474852484)

[4.5 Move Between Rings & Branches 35](#_Toc474852485)

[4.6 Long Term Servicing Branch 36](#_Toc474852486)

[4.7 Windows 10 Quality Update Testing 37](#_Toc474852487)

[4.8 Windows 10 Feature Update Testing 38](#_Toc474852488)

[5 Component Operation 39](#_Toc474852489)

[Appendix A Windows as a Service Implementation 40](#_Toc474852490)

[Appendix B Group Policy Configuration 42](#_Toc474852491)

[Appendix C Long Term Servicing Branch 43](#_Toc474852492)

We are very interested in your input!  If you have comments or would like to request an update to this document, please provide your feedback to the [SDM Suggestions alias](mailto:msdmods@microsoft.com).   Attach the document and clearly describe the changes you would like and explain why the changes are needed.

**Spell/grammar check is turned ON within all SDM Word templates -** Remember to turn off spell/grammar check before sending out the document if you want to avoid showing spelling and grammar red mark-ups. To turn this feature off, do the following:

1. Click on File
2. Click on the Options on the left
3. Click on Proofing
4. Scroll to bottom and check the two boxes shown below:



**To remove all the Visible Guidance (Hot Pink text with Grey Background) all at once:**

1. Click Ctrl H to open the Find and Replace box
2. Make sure your cursor is in the ‘Find what’ box.
3. Click on the More button at the bottom left
4. Click on the Format Button at the bottom left and select Style
5. Scroll down, locate select the “Visible Guidance”
6. Make sure the ‘Replace with’ box is empty:
7. Click ‘Replace All”
8. If not empty - click on the format button in the lower left hand corner. Scroll down and chose ‘(no style)’then replace all.

**IMPORTANT – Finalize This Document**

**REMOVE** all pink text, guidance, comments, changes, and hidden text in this document before submitting it to the customer. You can do this in two ways:

* **Save as PDF** and send the PDF version to the customer.   
  ~ OR ~
* **Inspect document and remove comments, revisions, any document properties you do not want included, personal information, and hidden text.** For guidance on how to do this, see [Remove hidden data and personal information from Office documents](http://office.microsoft.com/client/helppreview.aspx?AssetID=HA100375931033&QueryID=ALdFua2no0&respos=6&rt=2&ns=WINWORD&lcid=1033&pid=CH100487501033#3).

1. Overview

The purpose of this document is to detail all aspects of the Servicing design and implementation as it relates to the <CUSTOMERNAME> - <PROJECTNAME> project. This document is for use by the <PROJECTNAME> project manager, <DELIVERYORG> technical specialists and <CUSTOMERNAME> IS and IT teams.

This document includes the design of features to support the Servicing design including:

* Software Updates Approach
* Current Branch
* Current Branch for Business
* Long Term Servicing Branch

1. Technical Design

This section outlines design options, customer decisions and configuration for the capability.

The design will identify the appropriate Windows as a Service branches, feature and quality update approach and external services that are required to successfully implement a Servicing capability.

The design comprises three key areas:

* Core infrastructure dependencies – all dependent services required for the capability to operate.
* External prerequisites – all external prerequisites in the System Center Configuration Manager pilot.
* Design – details each of the features of the capability, including decisions and configuration parameters as discussed and captured through the design workshop for this capability.

The table below identifies key decisions that impact the overall implementation and ownership of the capability:

|  |  |  |
| --- | --- | --- |
| Decision | Justification | Impact |
| A servicing capability will be designed to support Windows 10 | System Center Configuration Manager can perform servicing of Windows devices using an in-console dashboard, reducing administrative effort to manage Operating System updates | Existing update infrastructure may require an upgrade to support Windows 10 servicing. Refer to Section 2.3 – Software Update Delivery for further information |
| The capability will support updates to the following Operating Systems:   * Windows 7 * Windows 10 | Operating Systems are present in the production environment | Existing devices require the installation or upgrade of a System Center Configuration Manager agent to be managed by the solution |
| Current Branch will be implemented for a controlled set of devices involved in validation prior to deployment to the organization | Early adopters will perform feature and configuration validation of feature updates. | Group policy must be updated to restrict the configuration of the current branch to only approved devices |
| Current Branch for Business will be implemented in the production environment | All systems, except early adopters and mission-critical systems, will be configured for the Current Branch for Business. | Group policy must be updated to enforce the configuration of the current branch for business on devices, by default |
| The Current Branch will use three servicing rings (Ring A, B, C) to control the release cadence of Windows 10 quality updates | Servicing of Windows 10 devices can be controlled to meet business and technical requirements, whilst minimizing the impact of updates to the environment | Administrative effort will be required identify and to place devices into each servicing ring |
| The Current Branch for Business will use three servicing rings (Ring 0, 1, 2) to control the release cadence of Windows 10 quality & feature updates | Servicing of Windows 10 devices can be controlled to meet business and technical requirements, whilst minimizing the impact of feature and quality updates to the environment | Administrative effort will be required identify and to place devices into each servicing ring |
| The default servicing approach for all devices will be to leverage Ring 2 of the Current Branch for Business for feature updates and quality updates | Devices that have not been selected for the Current Branch or a specific Current Branch for Business Ring must be accommodated in the design.  All devices are configured to point to Configuration Manager to receive updates, using Ring 2 ensures that ’non-configured’ devices will use the same servicing tool and provides assurance that all Windows 10 will remain supported. | All Windows 10 devices must be connected to Configuration Manager to receive updates  Administrative effort required to confirm all Windows 10 devices in the estate are updated |
| Long-Term Servicing Branch will not be deployed | No mission critical devices exist in the customer estate. | No impact to the production environment. |
| The capability will be implemented by <PROJECT TEAM NAME> | All defect resolution must be completed by the project team prior to transition to the operational team. | The project team will implement all initial services to a production level prior to transition to production. |
| The capability will be owned by the <TEAM NAME> | Production quality services must be owned by an operational team. | The <TEAM NAME> is responsible for all image development after the pilot project. |

Table 1: Servicing Core Design Decisions

* 1. Core Infrastructure Dependencies

This section identifies services required for the capability to operate. This includes the following mandatory services:

| Component | Description |
| --- | --- |
| Group Policy | The refers to the Group Policy environment in which the Windows as a Service Branch configuration will be applied to Windows 10 devices. Windows 10 Group Policy Administrative Templates are required to configure the Windows as a Service branches. |
| Servicing Infrastructure | The Servicing Infrastructure refers to the server(s) that contain the Servicing environment. This environment will support the quality and feature updating of Windows 10 devices where the infrastructure and Windows as a Service branch permits this to occur. |
| Windows 10 Devices | This refers to the devices in the production environment that will have Windows as a Service configuration applied to them. |
| Image Creation Service | The refers to the environment in which the image will be created. This environment consists of the infrastructure, software, tools, applications, and source files that will be used to successfully develop images to support Windows as a Service branches. |

Table 2: Infrastructure Dependencies

The following service map illustrates the infrastructure dependencies required for the Servicing capability:

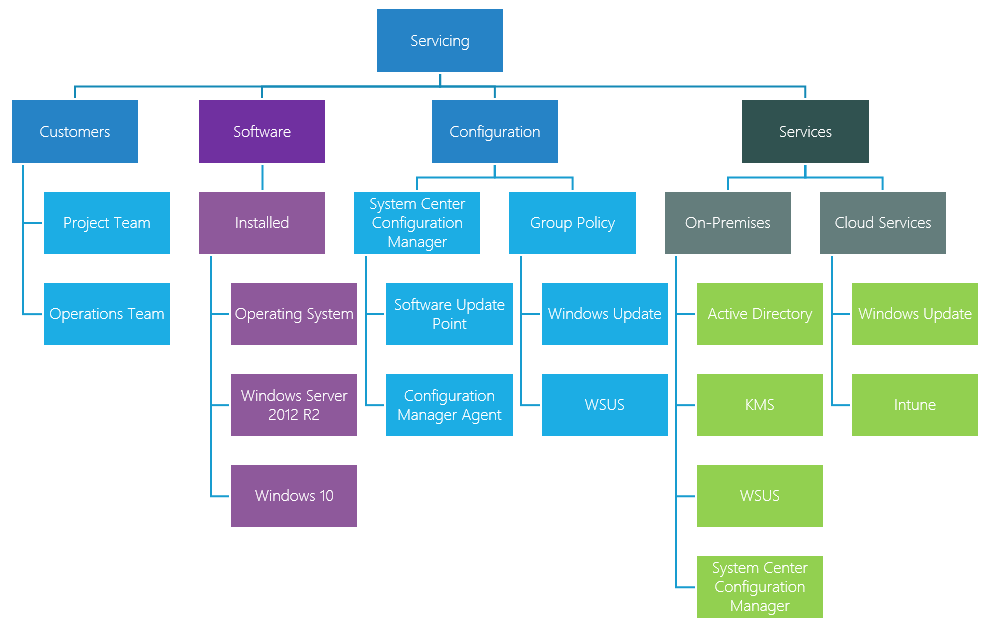


Figure 1: Service Map for Servicing

* 1. Environment Prerequisites

This section details environment prerequisites for Servicing in the production environment and provides context for the design decisions documented in subsequent sections.

|  |  |
| --- | --- |
| Item | Description |
| Operating System Media | Access to the Volume Licensing Service Center is required to obtain Operating System Media to ensure the chosen Windows as a Service branches can be supported in the environment. |
| KMS Server | If Windows 10 devices are activated by a KMS server, it must be patched to support Windows 10. This will ensure when KMS activated Windows 10 devices receive feature updates, Windows 10 can activate them. |
| Internet Connectivity | Internet access is required to download feature and quality updates, to one or multiple devices dependent on the servicing tool chosen. |

Table 3: Environment Prerequisites of Servicing.

This section should be changed and/or completed to detail the Servicing prerequisites design decisions specified by the customer.

The following table describes how the infrastructure considerations and prerequisites are addressed:

|  |  |  |
| --- | --- | --- |
| Component | Prerequisite Met | Description of service required |
| Operating System Media | <YES/NO> | The volume licensing administrator must download and provide media to support feature updates for Servicing for KMS activated devices. |
| KMS Server | <YES/NO> | The KMS server must be patched to support Windows 10 |
| Internet connectivity | <YES/NO> | Internet access, including access to Windows Update is required. |

Table 4: Servicing Infrastructure Considerations and Prerequisites

* 1. Software Update Delivery

This section details decisions related to the software updates that will be delivered to client devices in the production environment. The scope of the project provides support for software update delivery as supported by the System Center Configuration Manager platform.

The table below provides a list of all design decisions related to the implementation in the customer environment.

|  |  |  |  |
| --- | --- | --- | --- |
| Design Decision | Design Options | Decision | Justification |
| Update Classification | * Critical Updates **(Default)** * Security Updates **(Default)** * Definition Updates **(Default)** | * **Critical Updates** * **Security Updates** * **Definition Updates** | Production devices must have all critical and security updates installed to ensure compliance in the environment |
| Products | * Office 2013 / 2016 / ProPlus **(Default)** * Windows 7/8.1/10 **(Default)** * Windows Server 2012 R2 * Custom | * **Office 2013 / 2016 / ProPlus** * **Windows 7/8.1/10** | This approach reduces the number of updates downloaded into the environment and reduces administrative overhead |
| Supported Update Groups | * Software Updates - <Product Name>, <Deployment Cycle> - <Device Group> **(Default)** | * **Software Updates - <Product Name>, <Deployment Cycle> - <Device Group>** | To provide flexibility in the deployment of updates, software updates will be targeted to different products, different groups of devices and in different deployment cycles. |
| Deployment Cycles | * Monthly **(Default)** * Baseline **(Default)** * Expedited **(Default)** * Custom | * **Monthly** * **Baseline** * **Expedited** | The corporate security strategy requires Software Update deployments in 3 categories/scenarios for New workstation, monthly updates, and Critical software updates per product. |
| Device Groups | * Test **(Default)** * Pilot **(Default)** * Production **(Default)** | * **Test** * **Pilot** * **Production** | This approach allows phases of rollout to validate updates. |
| Maintenance Window | * Custom **(Default)** | * **Custom** | This approach helps ensure that client configuration changes occur during periods that do not affect the productivity of the organization. |
| Software Update Synchronization | * Patch existing WSUS instance **(Default)** * Synchronize directly with Microsoft Update | * **Patch Existing WSUS instance** | An existing version of WSUS is present and secured in the environment. Refer to the CORE\_CAPBILITY sheet of the Technical Design planning workbook for further information |
| Synchronization Schedule | * Monthly **(Default)** * Daily * Custom | * **Monthly** | The capability will synchronize monthly to support the monthly release cadence of feature and quality updates by Microsoft |
| Software Update Point Resilience | * Multiple Software Update Points **(Default)** * Single Software Update Point | * **Multiple Software Update Points** | Fault tolerance is a required feature of the design |
| Service Connection Point Configuration | * Online **(Default)** * Offline | * **Online** | The Windows 10 servicing capability provided by System Center Configuration Manager requires usage data to be sent to Microsoft, which requires an online connection to be configured |

Table 5 - Design decisions for Application Delivery Mechanisms

For a detailed view of all design settings implemented as part of this section, refer to the Technical Design Planning spreadsheet that is included as part of this document set.

* 1. Current Branch

This section details decisions related to the use and adoption of the Current Branch. The project scope provides for the use of the Current Branch to provide testing of new features and functionality prior to release as the Current Branch for Business. This branch choice is optional and may be omitted from the design. If included, it is recommended that users or groups are selected as part of a managed internal early adopter program.

The default corporate configuration for Windows 10 systems is the current branch for business. Hence, systems that are opted into a validation program on the current branch must be managed as exceptions. The group of devices in the program will be initially configured using the following computer group policy setting:

|  |  |  |  |
| --- | --- | --- | --- |
| Setting | Registry key | Description | Value |
| Windows Components\ Windows Update\ Defer Upgrades and Updates | HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\DeferUpgrades and Updates | If enabled, this policy setting in Pro and Enterprise SKUs, can defer quality updates for up to 4 weeks and feature updates (*previously upgrades*) for up to 8 months.  If disabled, feature and quality updates will not be deferred. | Disabled |

Table 6. Current Branch GPO setting.

This setting has no effect when devices in the environment are configured to use Windows Server Update Services (WSUS) or System Center Configuration Manager, however it will be set to ensure that if a device is removed from WSUS or System Center Configuration Manager, it will continue to receive updates from Windows Update if connected to the internet. using the current branch configuration.

The following table provides a list of all design decisions related to the implementation in the environment.

|  |  |  |  |
| --- | --- | --- | --- |
| Design Decision | Design Options | Decision | Justification |
| Branch Implementation | * Branch Included **(Default)** * Branch Excluded | **Branch Included** | The Current Branch provides the ability to test new Windows 10 features and functionality. |
| System Targeting Approach | * Target by group **(Default)** * Target by location * Target individual devices * Target all devices to receive Current Branch configuration | **Target by group** | This approach ensures that group membership to the current branch can be administratively controlled  Refer to **Appendix A –Windows as a Service Implementation** for further configuration information |
| Branch Coexistence | * Include Current Branch and Current Branch for Business devices in the same Windows 10 OU **(Default)** * Separate Current Branch devices into a unique OU | **Include Current Branch and Current Branch for Business devices in the same Windows 10 OU** | The selective use of Current Branch in the environment reduces risk and impact when performing tests of hardware and application compatibility.  Refer to **Appendix B –Group Policy Configuration** for further configuration information |

Table 7. Design decisions for Current Branch Servicing

* 1. Current Branch for Business

The Current Branch for Business is a deferred installation of the Windows 10 Current Branch. The scope of the project provides for the use the Current Branch for Business to accommodate validation of new features and functionality prior to scale deployment. An assessment of a feature update release can be conducted by devices with the Current Branch applied. During the deferral period, quality updates or hotfixes may also be released based on the adoption by Windows 10 Current Branch configured systems. This will improve the level of assurance that businesses have of a feature update validated by a very large adoption base.

Current Branch for Business will be configured differently based on the concept of servicing ‘Rings’. using Group Policy. The following table shows the settings that must be configured to assign Windows Devices to Current Branch for Business:

|  |  |  |  |
| --- | --- | --- | --- |
| Setting | Registry key | Description | Value |
| Windows Components\Windows Update\Defer Upgrades and Updates | HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\DeferUpgrades and Updates | If enabled, this policy setting in Pro and Enterprise SKUs, can defer quality updates for up to 4 weeks and feature updates (*previously upgrades*) for up to 8 months.  If disabled, feature or quality updates will not be deferred. | Enabled |

Table 8. Current Branch GPO setting

The following table provides a list of all design decisions related to the implementation in the environment.

|  |  |  |  |
| --- | --- | --- | --- |
| Design Decision | Design Options | Decision | Justification |
| Branch Implementation | * Branch Included **(Default)** * Branch Excluded | **Branch Included** | The Current Branch for Business provides the ability to apply new Windows 10 features and functionality in a quicker release cadence than traditional update methods |
| System Targeting Approach | * Target by group **(Default)** * Target by location * Target individual devices (manual) | **Target by group** | Deploying to business groups minimizes risk for the deployment of feature and quality updates.  Refer to **Appendix A – Windows as a Service Implementation** for further information |
| Branch Coexistence | * Include Current Branch and Current Branch for Business devices in the same Windows 10 OU **(Default)** * Separate Current Branch for Business devices into a unique OU | **Include Current Branch and Current Branch for Business devices in the same Windows 10 OU** | This approach reduces administrative effort to manage domain joined Windows 10 devices  **Refer to Appendix B – Group Policy Configuration** for further information |

Table 9. Current Branch for Business Design Decisions

* 1. Long Term Servicing Branch

For systems that are mission critical and require longer term stability, Microsoft has released the Long-Term Servicing Branch. Long-Term Servicing Branch is a specific media edition of Windows 10 Enterprise. To preserve stability of mission-critical systems, Long-Term Servicing Branch will have longer release cadence than any of the branches. Since there is a long cadence of innovation and a need for stability in mission critical systems, some innovative features of Windows 10 will not be available on Long-Term Servicing Branch systems, including the use of Universal Applications (such as Microsoft Edge). This branch choice is optional and may be omitted from the design. If included, it is recommended that only mission critical devices are selected for inclusion.

The following table provides a list of all design decisions related to the implementation in the customer environment.

|  |  |  |  |
| --- | --- | --- | --- |
| Design Decision | Design Options | Decision | Justification |
| Branch Implementation | * Branch Excluded **(Default)** * Branch Included | **Branch Excluded** | No mission critical devices exist in the customer estate. |
| System Targeting Approach | * Target individual devices (manual) **(Default)** * Target by group * Target by location | **Target individual devices (manual)** | Targeting individual devices on the Long-Term Servicing branch allows for the deployment of feature and quality updates to be customized per device and application requirements. Refer to **Appendix A – Windows as a Service Implementation** for further information. |
| Branch Coexistence | * Place Long Term Servicing Branch devices into OU separate from other Windows 10 devices **(Default)** * Include Long Term Servicing Branch devices in common Windows 10 OU with Current Branch and Current Branch for Business devices | **Place Long Term Servicing Branch devices into OU separate from other Windows 10 devices** | The use of separate OU’s to store Windows 10 Long Term Servicing branch devices reduces risk to these mission-critical systems. Refer to **Appendix C –Long Term Servicing Branch** for further information. |

Table 10. Design decisions for Long Term Servicing Branch Servicing.

1. Technical Implementation

This section details the implementation of Servicing developed for the production environment and the steps to install, configure, and operate the required component that will deliver the Servicing capability.

The following high-level activities are needed:

|  |  |
| --- | --- |
| Section | Activity |
| 3.2 | Prepare Environment |
| 3.3 | Service System Center Configuration Manager |
| 3.4 | Configure Software Update Delivery |
| 3.5 | Configure & Deploy Group Policy Objects |
| 3.6 | Service Windows 10 Devices |

Table 11: List of tasks to prepare for Servicing implementation

* 1. Implementation Activities and Tasks

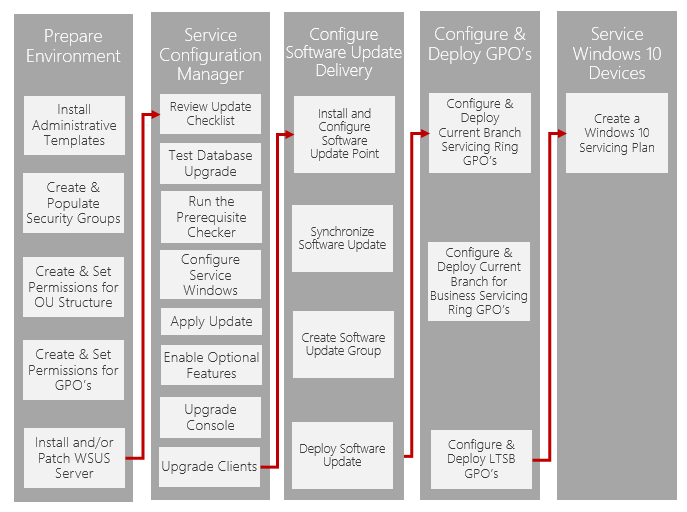


Figure 2: Servicing capability implementation steps

* 1. Prepare Environment

The environment must be prepared to accommodate the servicing model defined as part of the design. This section lists the preparation activities to support the configuration of the Current Branch, Current Branch for Business, and the Long-Term Servicing Branch.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Install Windows 10 Group Policy Administrative Templates | Windows 10 Administrative templates are required to ensure Windows 10 group policy settings can be configured on a single device, or group of devices by implementing a Group Policy Central Store. | Refer to: [Managing Group Policy ADMX Files Step-by-Step Guide](https://msdn.microsoft.com/en-us/library/bb530196.aspx#manageadmxfiles_topic6) for instructions to add Group Policy administrative templates to a central store. The Windows 10 Administrative Templates can be found [here](https://www.microsoft.com/en-us/download/details.aspx?id=48257) |
| Create & Populate Security Groups | Devices configured for servicing rings in the Current Branch & Current Branch for Business will be managed as using security groups. | * Refer to: [Create a new Group](https://technet.microsoft.com/en-us/library/cc783256(v=ws.10).aspx) to add a group in Active Directory Users and Computers. * Refer to **Appendix A – Windows as a Service Implementation** and **Appendix B – Group Policy Configuration** for design information for the servicing ring Active Directory group implementation in the production environment. |
| Create & set permissions for Organizational Unit structure | An Organizational Unit (OU) is required to apply group policy (including update policy) to Windows 10 devices separate from the existing production systems. The following OU structure is recommended in the target domain:   * OU=Windows 10 * OU=LTSB,OU=Windows 10   The LTSB OU will only contain mission-critical systems, and must have policy inheritance blocked. | * Refer to: [Create a New Organizational Unit](https://technet.microsoft.com/en-us/library/cc771564.aspx) to create an OU in Active Directory Users and Computers. * Refer to: [Block Inheritance](https://technet.microsoft.com/en-us/library/cc731076.aspx) to block inheritance in Group Policy Management Console * Refer to **Appendix B – Group Policy Configuration** for design information for the implementation of Windows as a Service in the production environment. |
| Create and set permissions for Group Policy Object Structure | Permissions must be set on each servicing ring Group Policy Object to ensure design objectives are met. User configuration settings must be disabled to ensure that recommended practice is followed when applying computer group policy settings. | * Refer to: [Create a new Group Policy object](https://technet.microsoft.com/en-us/library/cc738830(v=ws.10).aspx) to create Group Policy Objects for all in scope Windows as a Service Branches * Refer to: [Filter using security groups](https://technet.microsoft.com/en-us/library/cc779291(v=ws.10).aspx) to modify security settings to the in the Windows as a Service Group Policy Objects. * Refer to: [Disable the User or Computer settings in a Group Policy object using GPMC](https://technet.microsoft.com/en-us/library/cc778238(v=ws.10).aspx) to disable user policy for all implemented GPO’s. * Refer to **Appendix B – Group Policy Configuration** for GPO design information for the implementation of Windows as a Service in the production environment. |
| Install and/or Patch WSUS Server | The KB3095113 hotfix enables Windows Server Update Services (WSUS) on a Windows Server 2012-based or a Windows Server 2012 R2-based server to synchronize and distribute feature updates for Windows 10. This hotfix is not required to enable WSUS to synchronize and distribute servicing updates for Windows 10. | * Refer to [Deploy Windows Server Update Services in Your Organization](https://technet.microsoft.com/en-us/library/hh852340.aspx) to install WSIS * Refer to [Update to enable WSUS support for Windows 10 feature upgrades](https://support.microsoft.com/en-us/kb/3095113) to patch WSUS |

Table 12. Prepare Environment Implementation Steps.

* 1. Service System Center Configuration Manager

The environment must be prepared to support the System Center Configuration Manager Service component in the production environment, which can be performed using the steps below.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Review the update checklist | To confirm suitability of the site ahead of performing an upgrade | For an upgrade from 1511, 1602, or 1606, to 1610 review the [Checklist for installing update 1610 for System Center Configuration Manager](https://docs.microsoft.com/en-us/sccm/core/servers/manage/checklist-for-installing-update-1610)  For an upgrade from System Center 2012 Configuration Manager, refer to the migration capability of the offering |
| Test the database upgrade | While the test upgrade of the database is less critical than in past product versions it remains a recommended step. | Refer to [Install in-console updates for System Center Configuration Manager](https://technet.microsoft.com/en-us/library/mt652102.aspx) for more information |
| Run the prerequisite checker | The update files are replicated to other sites in advance of installing the update  The prerequisite check will automatically run again when you choose to install the update | Refer to [Install in-console updates for System Center Configuration Manager](https://technet.microsoft.com/en-us/library/mt652102.aspx) for more information |
| Configure Service Windows to control when site servers install updates | Child primary sites start the update automatically after the central administration site completes installation of the update.  This approach helps control when sites in the hierarchy install the update. | Use [Service Windows for site servers](https://technet.microsoft.com/en-us/library/mt652102.aspx#bkmk_ServiceWindow) to control when a site installs updates |
| Apply update at top-tier site | The update approach requires the top-level site is upgraded first.  Apply the update to take advantage of feature improvements and supportability status of the System Center Configuration Manager upgrade | Plan to install the update outside of normal business hours for each site when the process of installing the update and its actions to reinstall site components and site system roles will have the least effect on business operations  Refer to [Install in-console updates for System Center Configuration Manager](https://technet.microsoft.com/en-us/library/mt652102.aspx) for more information |
| Apply update at secondary site | Automatic update of secondary site servers is not supported.  Manually update secondary sites from within the Configuration Manager console after the primary parent site update is complete | Refer to [Install in-console updates for System Center Configuration Manager](https://technet.microsoft.com/en-us/library/mt652102.aspx) for more information |
| Enable optional features from updates | Leverage optional features that provide business or technical benefits to the environment | To view available features and their status, in the console navigate to Administration > Cloud Services > Updates and Servicing > Features.  When a feature is not optional, it installs automatically and does not appear in the Features node.  Beginning with 1606, you must give consent to use Pre-release features before you can enable their use.  Refer to [Install in-console updates for System Center Configuration Manager](https://technet.microsoft.com/en-us/library/mt652102.aspx) and [Use pre-release features from updates](https://docs.microsoft.com/en-us/sccm/core/servers/manage/install-in-console-updates#bkmk_prerelease) for more information |
| Upgrade stand-alone consoles | Ensure administration of the environment is performed on a supported console | Refer to [Install System Center Configuration Manager sites](https://technet.microsoft.com/en-US/library/mt590197.aspx) for more information |
| Upgrade clients | Ensure client devices can be managed using a supported version of the System Center Configuration Manager client | Refer to [Upgrade clients in System Center Configuration Manager](https://technet.microsoft.com/en-US/library/mt627876.aspx) for more information |

* 1. Configure Software Update Delivery

The environment must be prepared to support the Software Update Delivery Service component in the production environment, which can be performed using the steps below.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Install Windows Server Update Service | WSUS is necessary for software updates synchronization and for the software updates compliance assessment scan on clients. The WSUS server must be installed before you create the software update point site system role. | Refer to TechNet article for configuration instructions  <https://technet.microsoft.com/en-us/library/hh852340.aspx> |
| Install and Configure Software Update Point | When you have a Configuration Manager hierarchy, install, and configure the software update point at the central administration site first, and then install and configure the software update points on other sites. Some settings are only available when you configure the software update point on the top-level site, which is the central administration site or the stand-alone primary site. Refer Section 2.3.15 for design decision. | Refer to TechNet article for configuration instructions  <https://docs.microsoft.com/en-us/sccm/sum/get-started/install-a-software-update-point> |
| Synchronize Software Update | The synchronization of software updates is the process of retrieving software updates metadata from the Microsoft Update site and the replication of the metadata to all sites that are enabled for software updates in the Configuration Manager hierarchy. | Refer to TechNet article for configuration instructions  <https://docs.microsoft.com/en-us/sccm/sum/get-started/synchronize-software-updates> |
| Configure Classifications and Products to Synchronize | Every software update is defined with an update classification that helps to organize the different types of updates. During the synchronization process, the software updates metadata for the specified classifications will be synchronized. | Refer to TechNet article for configuration instructions  <https://docs.microsoft.com/en-us/sccm/sum/get-started/configure-classifications-and-products> |
| Verify Software Updates Client Settings and Group Policy Configurations | There are Configuration Manager client settings and group policy configurations that impact software update functionality that must be verified before software updates are deployed. | Refer to TechNet article for configuration instructions  <https://docs.microsoft.com/en-us/sccm/sum/get-started/manage-settings-for-software-updates>  *Optional -* Configure a grace period for required application and software update deployments  <https://docs.microsoft.com/en-us/sccm/core/plan-design/changes/whats-new-in-version-1610#enforcement-grace-period-for-required-application-and-software-update-deployments> |
| Implement Group policy on Clients | There are specific Group Policy settings that are used by Windows Update Agent (WUA) on client computers to connect to WSUS that runs on the software updates point. These Group Policy settings are also used to successfully scan for software update compliance, and to automatically update the software updates and the WUA. | Refer to TechNet article for configuration instructions  <https://docs.microsoft.com/en-us/sccm/sum/get-started/manage-settings-for-software-updates> |
| Add Software Updates to Groups | Software update groups provide you with an effective method to organize software updates in your environment. You can manually add software updates to a software update group or automatically add software updates to a software update group by using an automatic deployment rule. | Refer to TechNet article for configuration instructions  <https://docs.microsoft.com/en-us/sccm/sum/deploy-use/add-software-updates-to-an-update-group> <https://technet.microsoft.com/en-us/library/mt629383.aspx>  [https://technet.microsoft.com/en-us/library/gg712304.aspx - BKMK\_AddUpdatesToGroup](https://technet.microsoft.com/en-us/library/gg712304.aspx#BKMK_AddUpdatesToGroup) |
| Deploy Software Updates | The software update deployment phase is the process of deploying the software updates. Typically, you add software updates to a software update group and then deploy the software update group to clients. | Refer to TechNet article for configuration instructions  <https://technet.microsoft.com/en-us/library/mt629383.aspx> |

* 1. Configure & Deploy Group Policy Objects

The following tasks must be completed to configure access, for selected devices, to the Current Branch for Business.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Configure and Deploy Current Branch Servicing Ring GPO’s | Centralized control of settings requires a group policy to be configured appropriately | * Refer to the [Azure Group Policy Search](http://gpsearch.azurewebsites.net/) to find the Defer Upgrade & Update setting and apply it to the Current Branch GPO as defined in **Appendix B – Group Policy Configuration** * Refer to [Link a group policy object using GPMC](https://technet.microsoft.com/en-us/library/cc778387(v=ws.10).aspx) to link the GPO to the Windows 10 OU * Refer [to Add a computer account to a group](https://technet.microsoft.com/en-us/library/cc780108(v=ws.10).aspx) to add Current Branch devices to a security group if Security Filtering of the GPO is required. |
| Configure and Deploy Current Branch for Business Servicing Ring GPO’s | Centralized control of settings requires a group policy to be configured appropriately | * Refer to the [Azure Group Policy Search](http://gpsearch.azurewebsites.net/) to find the Defer Upgrade & Update setting and apply it to the Current Branch for Business GPO as defined in **Appendix B – Group Policy Configuration** * Refer to [Link a group policy object using GPMC](https://technet.microsoft.com/en-us/library/cc778387(v=ws.10).aspx) to link the GPO to the Windows 10 OU * Refer [to Add a computer account to a group](https://technet.microsoft.com/en-us/library/cc780108(v=ws.10).aspx) to add Current Branch for Business devices to a security group if Security Filtering of the GPO is required. |
| Configure and Deploy Long Term Servicing Branch GPO | Centralized control of settings requires a group policy to be configured appropriately | * Refer to [Link a group policy object using GPMC](https://technet.microsoft.com/en-us/library/cc778387(v=ws.10).aspx) to link the GPO to the Long-Term Servicing Branch OU |

Table 13. Current Branch for Business configuration steps.

* 1. Service Windows 10 Devices

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Create a Windows 10 Servicing Plan | Windows 10 devices to be updated in-console by System Center Configuration Manager must have a servicing plan. | Refer to the Technical Planning Spreadsheet (SERVICING) for configuration settings to create a Windows 10 Servicing Plan.  For more information, see [Manage Windows as a service using System Center Configuration Manager](https://technet.microsoft.com/en-us/library/mt627931.aspx) |

1. Test Plan

This section details the test plan for the Servicing component developed for the production environment.

The following high-level tests are needed:

|  |  |
| --- | --- |
| Section | Description |
| 4.1 | System Center Configuration Manager Upgrade Testing |
| 4.2 | Software Update Delivery Testing |
| 4.3 | Current Branch Scenario Testing |
| 4.4 | Current Branch for Business Scenario Testing |
| 4.5 | Move Between Rings & Branches |
| 4.6 | Long Term Servicing Branch Testing |
| 4.7 | Windows 10 Quality Update Testing |
| 4.8 | Windows 10 Feature Update Testing |

Table 14: List of tests for Servicing

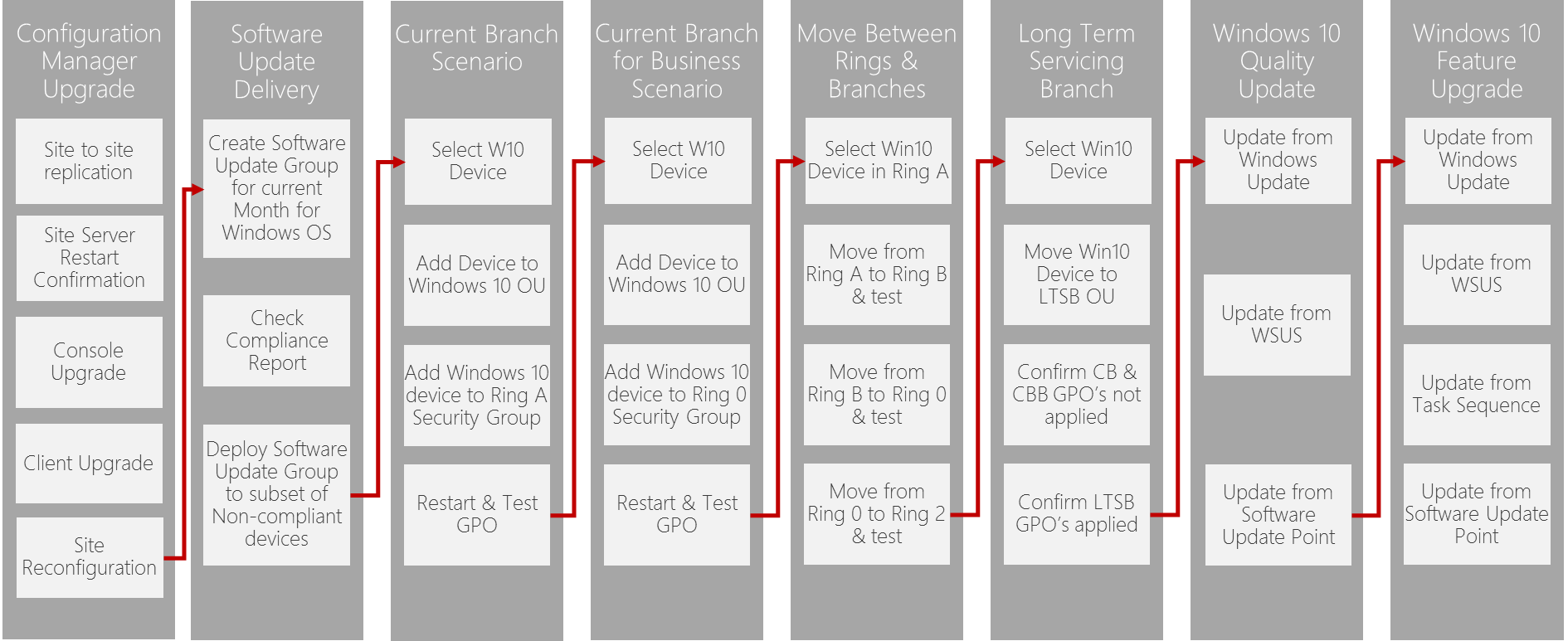


Figure 3: Servicing Test Scenarios

* 1. System Center Configuration Manager Upgrade Testing

The following section defines the description of how testing should start, pause, and stop for each test criteria. These are key quality metrics to be used in ensuring the items under test are ready to progress to the next stage in the testing process. Refer to the following [link](https://technet.microsoft.com/en-us/library/mt652102.aspx) for additional information to test the upgrade process for System Center Configuration Manager

|  |  |  |
| --- | --- | --- |
| **Task ID** | **Description** | **Pass / Fail** |
| 1 | Confirm site to site replication is active | Choose an item. |
| 2 | Confirm site servers and remote site system servers have restarted (if required) | Choose an item. |
| 3 | Confirm stand-alone configuration manager consoles have been updated | Choose an item. |
| 4 | Confirm Configuration Manager clients have been updated | Choose an item. |
| 5 | Confirm database replicas are reconfigured for management points at primary sites | Choose an item. |

Table 15: List of tasks for Upgrade Scenario

* 1. Software Update Delivery

The following section defines the description of how testing should start, pause, and stop for each test criteria. These are key quality metrics to be used in ensuring the items under test are ready to progress to the next stage in the testing process.

List of tasks to be performed.

|  |  |  |
| --- | --- | --- |
| **Task ID** | **Description** | **Pass / Fail** |
| 1 | Create and deploy Software Update Group with all security updates for current month for a <Windows 8.1/10 OS> | Choose an item. |
| 2 | Check compliance report/view Software Updates Compliance Dashboard for recently created software update group compliance | Choose an item. |
| 3 | Deploy Software Update Group to Subset of non-compliant Test machines and verify updates install | Choose an item. |

Table 16: Test Criteria for Automated Software Update Deployment

* 1. Current Branch

The following section defines the description of how testing should start, pause, and stop for each test criteria. These are key quality metrics to be used in ensuring the items under test are ready to progress to the next stage in the testing process.

|  |  |  |
| --- | --- | --- |
| **Task ID** | **Description** | **Pass / Fail** |
| 1 | Introduce a vanilla Windows 10 device to the production environment and join it to the domain. Using Active Directory Users and computers, locate the Windows 10 device in Active Directory. | Choose an item. |
| 2 | Move the computer object to the organizational unit where Windows 10 devices are located, and Current Branch/ Current Branch for Business GPO’s are applied. | Choose an item. |
| 3 | Add the Windows 10 Device to a Current Branch servicing ring A security group. Restart the Windows 10 Device | Choose an item. |
| 4 | Logon to the Windows 10 device and using and Run “**GPResult /h *<PathToHTMLOutput>***” to confirm Current Branch GPO policy applies, and the configuration is consistent with the servicing ring settings specified in **Appendix A – Windows as a Service Implementation** | Choose an item. |

Table 17: List of tasks for Current Branch

* 1. Current Branch for Business

The following section defines the description of how testing should start, pause, and stop for each test criteria. These are key quality metrics to be used in ensuring the items under test are ready to progress to the next stage in the testing process.

|  |  |  |
| --- | --- | --- |
| **Task ID** | **Description** | **Pass / Fail** |
| 1 | Introduce a vanilla Windows 10 device to the production environment and join it to the domain. Using Active Directory Users and computers, locate the Windows 10 device in Active Directory. | Choose an item. |
| 2 | Move the computer object to the organizational unit where Windows 10 devices are located, and Current Branch/ Current Branch for Business GPO’s are applied. | Choose an item. |
| 3 | Add the Windows 10 Device to a Current Branch for Business servicing ring 0 security group. Restart the Windows 10 Device | Choose an item. |
| 4 | Logon to the Windows 10 device and using and Run “**GPResult /h *<PathToHTMLOutput>***” to confirm the relevant Current Branch for Business GPO servicing ring policy applies, and the configuration is consistent with the servicing ring settings specified in **Appendix A – Windows as a Service Implementation** | Choose an item. |

Table 18: List of tasks for Current Branch for Business

* 1. Move Between Rings & Branches

The following section defines the description of how testing should start, pause, and stop for each test criteria. These are key quality metrics to be used in ensuring the items under test are ready to progress to the next stage in the testing process.

|  |  |  |
| --- | --- | --- |
| **Task ID** | **Description** | **Pass / Fail** |
| 1 | Locate a Windows 10 device on the production network that resides in the Windows 10 OU with Current Branch GPO and Current Branch for Business GPO applied, and is a member of the Current Branch Ring A Security Group | Choose an item. |
| 2 | Logon to the Windows 10 device and using and Run “**GPResult /h *<PathToHTMLOutput>***” to confirm Current Branch GPO policy applies, and “Defer Upgrade” setting is disabled | Choose an item. |
| 3 | Move the Windows 10 Device from the Current Branch Ring A security group to the Current Branch Ring B security group and restart the device. | Choose an item. |
| 4 | Logon to the Windows 10 device and using and Run “**GPResult /h *<PathToHTMLOutput>***” to confirm Current Branch GPO policy applies, and “Defer Upgrades and Updates” setting is enabled and the update setting is set to 1 week | Choose an item. |
| 5 | Move the Windows 10 Device from the Current Branch Ring B security group to the Current Branch for Business Ring 0 security group and restart the device. | Choose an item. |
| 6 | Logon to the Windows 10 device and using and Run “**GPResult /h *<PathToHTMLOutput>***” to confirm Current Branch for Business GPO policy applies, and “Defer Upgrades and Updates” setting is enabled, the upgrade setting is configured to 2 months and the update setting is set to 0 weeks | Choose an item. |
| 7 | Move the Windows 10 Device from the Current Branch for Business Ring 0 security group to the Current Branch for Business Ring 2 security group and restart the device. | Choose an item. |
| 8 | Logon to the Windows 10 device and using and Run “**GPResult /h *<PathToHTMLOutput>***” to confirm Current Branch for Business GPO policy applies, and “Defer Upgrades and Updates” setting is enabled, the upgrade setting is configured to 6 months and the update setting is set to 2 weeks | Choose an item. |

Table 19: List of tasks for Move from Current Branch to Current Branch for Business

* 1. Long Term Servicing Branch

The following section defines the description of how testing should start, pause, and stop for each test criteria. These are key quality metrics to be used in ensuring the items under test are ready to progress to the next stage in the testing process.

|  |  |  |
| --- | --- | --- |
| **Task ID** | **Description** | **Pass / Fail** |
| 1 | Build or select a Windows 10 Enterprise LTSB device on the production network and confirm it resides in the Windows 10 OU. | Choose an item. |
| 2 | Move the Windows 10 Enterprise LTSB device to the Windows 10 LTSB OU. Restart Windows 10 Device. | Choose an item. |
| 4 | Confirm Current Branch GPO and Current Branch for Business GPO are not applied to Windows 10 Enterprise LTSB Device | Choose an item. |
| 5 | Confirm GPO’s marked as ‘Enforced’ are applied to Windows 10 Enterprise LTSB Device | Choose an item. |

Table 20: List of tasks for Long Term Servicing Branch

* 1. Windows 10 Quality Update Testing

The following section defines the description of how testing should start, pause, and stop for each test criteria. These are key quality metrics to be used in ensuring the items under test are ready to progress to the next stage in the testing process.

|  |  |  |
| --- | --- | --- |
| **Task ID** | **Description** | **Pass / Fail** |
| 1 | Select a Windows 10 device that is connected to System Center Configuration Manager infrastructure and is configured to receive updates from a software update point.  When an update to Windows 10 is administratively approved to a collection where the device resides, confirm the device receives the update from the Software Update Point. | Choose an item. |

Table 21: List of tasks for Quality Update Scenario

* 1. Windows 10 Feature Update Testing

The following section defines the description of how testing should start, pause, and stop for each test criteria. These are key quality metrics to be used in ensuring the items under test are ready to progress to the next stage in the testing process.

|  |  |  |
| --- | --- | --- |
| **Task ID** | **Description** | **Pass / Fail** |
| 1 | Select a Windows 10 device that is connected to System Center Configuration Manager infrastructure and is configured for Windows 10 servicing.  Update Windows 10 using the servicing component of System Center Configuration Manager and confirm the feature update is applied successfully. | Choose an item. |

Table 22: List of tasks for Feature Update Scenario

1. Component Operation

This section details the operation of the service as implemented in the production environment.

The environment must be prepared to support the Servicing component in the production environment, which can be performed using the steps below.

|  |  |
| --- | --- |
| **Scenario** | **Outcome** |
| Monitor Software Updates | Ensure software updates objects, processes, and compliance information is available and operational. Refer to TechNet Article for more information: <https://technet.microsoft.com/en-us/library/mt629383.aspx> |
| Add Software Updates to Existing Software Update Group. | After you deploy a software update group, you can add new software updates to the group and Configuration Manager will automatically deploy them. Refer to TechNet Article for more information:  <https://technet.microsoft.com/en-us/library/mt629383.aspx> |
| Move Windows 10 Enterprise Device into Windows 10 OU | Device receives Current Branch for Business configuration upon reboot. |
| Add Device to Current Branch Security Group | Device receives Current Branch configuration upon reboot. |
| Remove Device from Current Branch Security Group | Device receives Current Branch for Business configuration upon reboot. |
| Move Windows 10 Enterprise LTSB Device into the LTSB OU | Device receives appropriate GPO configuration for the OU upon reboot |

Table 23. Component Operation for Servicing.

1. Windows as a Service Implementation

This table determines what servicing tools and configuration will be required for each applicable branch, ring (if applicable) and group.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Branch | | Servicing Tool | Configuration Method | Quality Update Deferral | Feature Update Deferral | Group | Number of Devices | Group Membership |
| **Current Branch** | **Ring\_A** | Windows Update | Group Policy | 0 weeks | 0 months | Sales\_Group | 10 | <CBRingA> |
| **Ring\_B** | 1 week | 15 | <CBRingB> |
| **Ring\_C** | 2 weeks | 20 | <CBRingC> |
| **Current Branch for Business** | **Ring\_0** | Windows Update | Group Policy | 0 weeks | 2 months | IT\_Group | 225 | <CBBRing0> |
| **Ring\_1** | Windows Server Update Services | Group Policy  WSUS Console | 1 week | 4 months | Marketing\_Group | 150 | <CBBRing1> |
| **Ring\_2** | 2 weeks | 6 months | Domain Computers | 75 | <CBBRing2> |
| **Long Term Servicing Branch** | | Task Sequence | Manual | Custom | Custom | ScaleComp\_Group | TBC | TBC |

1. Group Policy Configuration

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | | CB Ring A | CB Ring B | CB Ring C | CBB Ring 0 | CBB Ring 1 | CBB Ring 2 |
| **Group Policy Name** | | <CBRingA> | <CBRingB> | <CBRingC> | <CBBRing0> | <CBBRing1> | <CBBRing2> |
| **Targeted OU** | | <OUPATH> | <OUPATH> | <OUPATH> | <OUPATH> | <OUPATH> | <OUPATH> |
| **GPO Priority** | | 1 | 2 | 3 | 4 | 5 | 6 |
| **Group Membership Mechanism** | | AD Group <W10CBRingA> | AD Group <W10CBRingB> | AD Group <W10CBRingC> | AD Group <W10CBBRing0> | AD Group <W10CBBRing1> | AD Group <W10CBBRing2> |
| **GPO Filtering** | | <W10CBRingA> | <W10CBRingB> | <W10CBBRingB> | <W10CBBRing0> | <W10CBBRing1> | Authenticated Users |
| **Defer Upgrades & Updates GPO** | **State** | Disabled | Enabled | Enabled | Enabled | Enabled | Enabled |
| **Defer Upgrade** | 0 months | 0 months | 0 months | 2 months | 4 months | 6 months |
| **Defer Update** | 0 months | 1 week | 2 weeks | 0 weeks | 1 week | 2 weeks |
| **Specify intranet Microsoft update service location** | **State** | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled |
| **Path** | N/A | N/A | N/A | N/A | N/A | N/A |

1. Long Term Servicing Branch

The Long-Term Servicing Branch will be configured manually. The devices that are included in the current branch can be determined by reviewing the Organizational Unit listed below:

|  |  |
| --- | --- |
| Setting | Description |
| **Selection Approach** | Device manually added to Group Policy OU  <OUName>  <OUPath> |
| **Additional Configuration** | OU Permission = Block Inheritance  Group Policy Enforced |