Document Identification

Document	Procedure for preparing Workstations and Printers in the Company's IT Infrastructure.
Involved Areas	Security Division; IT Service Desk Division; IT Networking Division.
Objective	To establish the standard configurations for workstations and printers within Company's IT Infrastructure.
References	Standardization of workstations in Company's IT Infrastructure.

Version and Revision Control

Document	Version	Date	Responsibles	Reviewers
Initial Check-List	1.1	July 21, 2022	@brazilianscriptguy	All of You
Approval	2.2	July 21, 2023	@brazilianscriptguy	All of You
Last Update	**22.22**	**June 19, 2025**	@brazilianscriptguy	All of You

Classification of this Document

RESTRICTED	For internal use only, regarding configurations of Company's institutional workstations. Access is restricted to those responsible for the configurations.

Justifications

STRATEGIC OBJECTIVES **(ISO/ IEC 20000 International Standard for IT Service Management)**	Improve Service Quality; Enhance Customer Satisfaction; Increase Operational Efficiency; Ensure Service Continuity; Drive Continuous Improvement; Enhance Risk Management; Foster IT Governance.

Summary

UNIT I – Prerequisites for Executing the ITSM-Templates-WKS Standard

All procedures must be executed in the sequence outlined in this document. No subsequent step should be performed without confirming the compliance of the preceding steps:

1) Deploy the standard **ITSM-Templates-WKS** image to the workstation, system root **'C:\'** and set the default local Administrator password.

2) Ensure you possess credentials with permissions to join workstations to the domain.

3) When cloning the operating system, verify that the clone followed the **Sysprep standard**, since each system's **Security Identifier (SID)** must be unique. This step is mandatory to avoid duplicated SIDs across the network.

4) Submit in advance to the **IT Managed Services Provider** a complete list of workstation and printer accounts to be created in the Active Directory object structure, including the **MAC addresses of printers**, bio-metric terminals, and any workstations that require **persistent network services** (e.g., online broadcasting terminals, plenary session workstations). This submission is required to allow for **IP address reservation within the service address range**, rather than from the dynamic distribution pool.

5) Ensure you have access credentials for **Antivirus Software** management (update/configuration/removal) and **administrator-level credentials** for managing printers.

6) Notify the **IT Infrastructure Division** in advance regarding any **VLAN configuration changes** required for the migration unit.

7) Always use the most recent version of the **ITSM-Templates-WKS** configuration folder and this checklist document.

8) Establish standardized naming conventions for all **workstations and printers** in the unit undergoing migration.

9) Any errors or blockers identified before or during the migration process must be logged and reported via the **IT Service Desk platform** for escalation to the appropriate support level.

10) Send the list of workstation and printer names (preferably via email) in advance to the **User and Service Management Section**, which is responsible for creating the necessary Active Directory accounts and confirming completion with the requesting unit.

11) Any account naming issues detected during workstation preparation must be communicated immediately to the responsible section for prompt correction.

12) Reports of **non-compliance** with the requirements in this document must be submitted:

- **a) Weekly to** the **L1 / L2 Service Desk Support Coordinators** and the **IT Service Desk Manager;**
- **b) Monthly** to the **IT Department CIO.**

13) Confirm that the initial stage of this process – **deploying the ITSM-Templates-WKS image** – was completed. If unsure, consult the **L1 / L2 Service Desk Support Coordinator**.

14) Confirm with the **L1 / L2 Service Desk Support Coordinator** that **operating system cloning procedures followed the unique SID requirement**. This step prevents duplication of security identifiers across the domain.

15) Verify that all **setup and validated configuration files** are stored in the network share informed by the **IT Managed Services Provider**:

`\\DML\IT-Service-Desk-Repository\`

This is the authoritative repository for all officially sanctioned software (DML - Definitive Media Library).

16) Confirm with the **L1 / L2 Service Desk Support Coordinator** that the following have been submitted to the **IT Managed Services Provider**:

c) The **Standard Migration Form** for the unit.

d) **MAC address mappings** for printers, bio-metric devices, and workstations requiring continuous service. This enables proper **IP address allocation** from the static services pool.

17) Confirm with the **L1 / L2 Service Desk Support Coordinator** and the **IT Infrastructure Division** any **switch or VLAN modifications** required in the target unit.

18) Confirm the configuration or adjustment of the following network and directory service items with the **L1 / L2 Service Desk Support Coordinator**:

e) **DHCP** scopes

f) **VLAN** entries in DNS

g) **VLAN** entries in Active Directory Sites and Services

h) Creation of **OU structures** in Active Directory

19) Ensure the **most current version** of the **ITSM-Templates-WKS** folder has been **copied to your removable media**, and that you have the **latest edition of the official Check-List Manual** for applying ITSM-Templates-WKS in institutional workstations.

20) If you encounter issues or doubts that are **beyond your scope of knowledge or authorization**, immediately consult the **L1 / L2 Service Desk Support Coordinator** for guidance or escalation.

21) You must commit to executing the procedures outlined in this document, as they ensure the **workstation OS adheres to domain authentication policies and Active Directory forest requirements**.

22) All **scripts must be executed** in the order presented in this Check-List and in accordance with instructions in the Check-List Manual. This guarantees compliance and correct sequencing.

23) All features, commands, and functions used in this Check-List rely exclusively on built-in features of the **Microsoft Windows operating system**—no third-party or non-standard tools are involved.

24) **L1 Service Desk Teams** are the official executors of the Check-List. To maintain **maturity, accountability, and compliance**, any suggested improvements or changes to scripts must be submitted to the **L1 / L2 Service Desk Support Coordinator**, who will formally report them to the **IT Managed Services Provider** via the administrative process.

25) The structure and contents of each folder within the ITSM-Templates-WKS repository are as follows:

a) At the root directory: **`C:\ITSM-Templates-WKS\`**

- **BeforeJoinDomain** – Contains the `ITSM-BeforeJoinDomain.hta` script, which must be executed **before domain join**. This script applies **10 registry settings** (`.REG`) and **10 script-based configurations** (`.VBS`).
- **AfterJoinDomain** – Contains the `ITSM-AfterJoinDomain.hta` script, which must be executed **immediately after joining the domain**. This script resets network settings, clears DNS cache, and resynchronizes Group Policy Objects (GPOs).

b) In **`C:\ITSM-Templates-WKS\Assets\`**

The function of each script is **described in Unit III and Unit IV** of this Check-List.

AdditionalSupportScripts – Contains auxiliary tools for addressing previously identified configuration inconsistencies:

- **`ActivateAllAdminShare`** – Enables Admin shares, enables RDP, disables Windows Firewall, and disables Windows Defender.
- **`ExportCustomThemesFiles`** – Exports Windows custom theme elements.
- **`FixPrinterDriverIssues`** – Resets the print spooler and clears printer driver conflicts.
- **`GetSID`** – Includes Sysinternals tool to retrieve the OS security identifier (SID).
- **`InventoryInstalledSoftwareList`** – Gathers a list of all installed applications.
- **`LegacyWorkstationIngress`** – Allows older OSes to join modern Active Directory domains.
- **`RenameDiskVolumes`** – Renames the C: drive to the workstation hostname and D: drive to "UserData" or similar.
- **`SystemMaintenanceWorkstations`** – Runs system health tasks: SFC, DISM, GPO reset, WSUS resync, and optional reboot with GUI.
- **`UnjoinADComputer-and-Cleanup`** – Unjoins the computer from the domain and cleans legacy AD artifacts.
- **`Update-KasperskyAgent`** – Redirects the agent to the current antivirus server and updates certificates.

- **`WorkStationConfigReport`** – Collects BIOS, OS, and network configuration into a `.CSV` file.
- **`WorkstationTimeSync`** – Syncs time, time zone, and NTP configuration using GUI-assisted logic.

Certificates – Contains the institutional Certificate Authority (CA) certificates required during the initial workstation configuration:

- **`ADCS-Server`** – Certificate for the organization's internal **Active Directory Certificate Services (ADCS)** infrastructure.
- **`RDS-Server`** – Certificate used to establish trust for **Remote Desktop Services (RDS)** within the enterprise network.
- **`WSUS-Server`** – Certificate required for secure communication with the organization's **Windows Server Update Services (WSUS)** platform.

CustomImages – Institutional user and desktop theme images used in the local profile.

MainDocs – Contains the source documents for this Check-List and default visual templates:

- **`CheckListOrigin`** – Editable version of this document.
- **`DefaultUsersAccountImages`** – Includes default institutional profile images and a **`hosts`** file that protects against malicious sites (from Safer-Networking Ltd). These will be replaced upon domain join.

ModifyReg – Contains folders for initial registry modifications and desktop personalization:

- **`AllGeneralConfigs`** – General-purpose system configuration scripts.
- **`DefaultBackground`** – Scripts for desktop and login screen backgrounds, plus `hosts` file setup.
- **`UserDesktopFolders`** – Institutional shortcuts and links copied to each user's profile.
- **`UserDesktopTheme`** – Applies institutional desktop theme, including classic mode configuration and wallpaper replacement.

26) **Note:** The role and execution order of each script used for workstation setup are detailed in **Unit III** and **Unit IV** of this document.

UNIT II – Preparing and Updating the Workstation

1) Proceed with operating system customization, referred to as the **Out-of-Box Experience (OOBE)**, using the **`sysprep`** command and specifying an initial account to access the operating system:

   a) Remove any additional accounts with administrative privileges, enable the built-in Administrator account, and define the new default password;

   Use the **`netplwiz`** command to verify that only one account holds administrative rights;

   b) Remove all local printers from the workstation, except for **Microsoft Print to PDF**;

   c) Enable automatic network configuration by setting the **IP address and DNS settings to obtain automatically via DHCP**, and ensure **IPv6** is enabled.

Note: In cases where the workstation does not acquire an IP address via DHCP, the network environment settings should be reset. Navigate to the directory:

`C:\ITSM-Templates-WKS\Assets\ModifyReg\AllGeneralConfigs\`

   a) `Renew-all-IP-Connections.vbs` – Resets TCP/IP connections and forces network reconfiguration via DHCP;

   b) Alternatively, open **Device Manager**, uninstall the network adapter, choose to remove the driver, and then **restart the workstation** to reinstall it automatically.

2) Perform **operating system updates** using the **WSUS Offline** tool for Windows 10 and 11 workstations, following the steps below:

   a) From the network share:

   `\DML\IT-Service-Desk-Repository\WSUS_Offline-Win10x11-WinSvr\client\UpdateInstaller.exe`, launch the update application. Alternatively, use a removable media source prepared with the same update package.

   b) Under the **Updating – Installation** section, **check all options** for installation. Under the **Control** section, **leave all options unchecked**.

   c) **Restart** the system when prompted with the message: `“Installation successful. Please reboot your system”` After rebooting, repeat steps **2.a** and **2.b**.

   d) Continue this cycle **until no additional updates are found**, and the message `"No missing update found. Nothing to do."` is displayed.

   e) Once updates are complete, **reboot the workstation** again and confirm via **Control Panel > Windows Update** that no further updates are pending.

UNIT III – Standardizing the Workstation for Domain Join

1) While signed in with the workstation's **local Administrator account**, proceed with the following steps. These steps apply **exclusively to Windows 10 and Windows 11 systems**. Two scripts will be executed that apply the complete set of configurations defined in the **ITSM-Templates-WKS** standard.

a. Copy the entire folder: \ITSM-Templates-WKS, to the root of the **C:** drive on the workstation being configured.

b. Open the folder:

C:\ITSM-Templates-WKS\BeforeJoinDomain

and run the script below, which consolidates **20 individual configurations** that must be applied **before the workstation joins the Domain**.

Run as Administrator by right-clicking the script and selecting **"Open"**:

ITSM-BeforeJoinDomain.hta

c) Configuration Overview

The tables below detail the actions performed by the script, including both **`.VBS`** and **`.REG`** configuration files, for better traceability and operational awareness.

VBS-Based Configuration Scripts

Script Name	Description
Disable-Windows-Firewall.vbs	Disables the Windows Firewall
Grant-Full-Access-Legacy-App.vbs	Grants full access for legacy apps, running on workstations
Renew-all-IP-Connections.vbs	Resets and renews all TCP/IP network connections
WSUS-Certificate-Install.vbs	Installs the WSUS certificate
WSUS-Clean-SID.vbs	Cleans previous WSUS SID registration to avoid conflicts
CopyDefaultFolders.vbs	Copies default desktop folders and the Start Menu appearance profile
CopyHosts.vbs	Secures network access before antivirus installation
CopyLogonBackground.vbs	Copies the institutional lock screen images
CopyUserLogo.vbs	Copies institutional user profile pictures
CopyWallPaperDefault.vbs	Copies the default desktop wallpapers

REG-Based Registry Configurations

Registry File Name	Description
AddStartPageADM.reg	Sets the default homepage in supported browsers
DisableUAC-LUA.reg	Disables User Account Control (UAC) prompts
Enable-AutoShareAdmin.reg	Enables administrative share access
Register-Owner.reg	Adds Company's ownership metadata to Windows registration
Win10_Domain-Ingress.reg	Applies secure settings for domain sharing
WSUS-App-Intranet.reg	Points the system to the institutional WSUS server
DesktopCurrent.reg	Applies UI configuration for the current user
DesktopDefault.reg	Applies UI configuration for the default user profile
EnableCustomLogonBackgrounds.reg	Enables support for custom logon backgrounds
ITSM-Templates.deskthemepack	Applies the company's desktop theme

Important Notes:

- All **20 configurations** are integrated into a single automated script.
- Any errors encountered during execution **must be reviewed carefully**.
- The technician responsible must validate which configurations were successfully applied and verify compliance with the **`ITSM-Templates-WKS`** standard.

Note: During execution, pay close attention to on-screen messages and validate configuration results. This ensures full compliance with the defined standards.

Troubleshooting

After execution, check the following log file for possible errors:

C:\ITSM-Logs\ITSM-BeforeJoinDomain.log

If any errors are encountered that **cannot be resolved immediately**, they must be documented and reported to the **appropriate support level** through the **IT Service Desk System**.

UNIT IV – Institutionalizing the Microsoft Windows Workstation

Note: To ensure standardized identification of each workstation – allowing asset management and monitoring tools to accurately recognize each device on the network – it is **critical** to enforce consistency across naming and identification configurations.

Follow the procedures below precisely. In the event of any doubts or technical issues, consult the **L1/L2 Service Desk Support Coordinator**.

1) Renaming the Network Connection

- **Location:**
  Control Panel → Network and Internet → Network Connections
- **Procedure:**
  Rename the active network connection to reflect the building or physical location using the standardized naming convention (e.g., **`BOSNet`**, **`MIANet`**, **`NYCNet`**, **`AUSNet`**, etc.), according to the designated Remote Office (see Appendix – **UNIT VIII**).

2) Standardizing Workstation Identification

a) Hostname Format:

- Construct the hostname using the following elements:
  - 03 letter from abbreviation of the Office name = **`MIA`** for Miami office;
  - Abbreviation of the Equipment Type = **`D`** for Desktop
  - Abbreviation of the Division = **`SALESO`** for Sales office
  - Asset Control Number = **`11704`**
- Example for Hostnames: **`MIADSALESO11704`**

e.g.: **`BOSDHUMANR27706; AUSLITSUPT21772; NYCLACCOUN37890`**

b) Drive C Volume Label:

- The label must match the hostname exactly.

c) Drive D Volume Label:

- Label the volume as: **`Personal-Files`**
- If the second partition is not assigned the letter `D:`, adjust the drive letter accordingly.

d) Computer Description:

- Define the system description to reflect the associated unit. Examples: `Workstation – L2 Service Desk`, `Workstation – L2SERVDESK`

3) Confirmation and Validation

- **Verification:** Confirm all configurations with the **L1/L2 Service Desk Support Coordinator**, referring also to the **Host Naming Table** and **Appendix – UNIT VIII** of this Check-List.
- **Application to Other Devices:** These naming standards also apply to other networked assets, such as:
    - Laptops
    - Printers
    - Multifunction devices
    - Scanners

Note: This procedure ensures that all equipment is correctly and consistently identified, enabling asset tracking and monitoring systems to function in compliance with the **ITSM-Templates-WKS** standard.

4) Special Cases for IP address reservation

- Bio-metric Attendance Terminal;
- Continuous Service Workstations;
- Community Kiosk Workstations;
- Online Transmission Workstations
- Special IP address Workstations

For workstations used for **daily time tracking** or requiring **continuous service availability**, the **L1/L2 Support Team** must submit the corresponding **MAC addresses** to the **IT Managed Services Provider**.

This enables the proper reservation of IP addresses within the **designated service IP range**, separate from the **dynamic distribution pool**.

All special-case configurations requiring IP address reservation must be clearly communicated to the **IT Managed Services Division** to ensure accurate allocation and network compliance.

UNIT V – Configuration of Printers and Multifunction Devices

Note: Printers are also domain objects. To join the domain, they must meet specific configuration requirements and have up-to-date firmware.

- **Enforce DHCP Configuration Acquisition**

  Use the printer's physical control panel to initiate automatic acquisition of network settings via DHCP.

- **Access Configuration via Web Interface**

  Access the printer's Embedded Web Server (EWS) using its assigned IP address to perform necessary configurations.

- **Firmware Update**

  Ensure the printer firmware is up to date with the latest approved version.

- **Admin Credential Customization**

  Change the default administrator (SNMP) credentials in accordance with guidance from the **IT Managed Services Provider** and the **IT Infrastructure Division**.

- **Configure Hostname**

  Set the printer hostname according to the organizational naming conventions and **Organizational Unit (OU)** standards.

- **Disable Unused Protocols**

  Disable all unnecessary announcement and wireless protocols. Only the following must remain enabled:

  - `RAW TCP/IP on port 9100 / SMB`
  - `HTTP on port 80`
  - `LPD Service`

- **Configure SNMP Protocols (v2/v3)**

  Set up SNMP credentials following the specifications provided by the **IT Managed Services Provider** and **IT Infrastructure Division**.

- **Time Synchronization**

  Configure the printer to synchronize date and time using the NTP server: `ntp1.Company's`.

- **Enable Internal Memory and Storage**

  Ensure the internal RAM and storage disk modules are active and functioning properly.

- **Configure Network Scan Login Credentials**

  Set the appropriate login account for multifunction devices to enable network-based document scanning.

- **DHCP Assignment and IP Reservation**

  Submit printer MAC addresses to the **IT Managed Services Provider** so static IP addresses can be assigned within the service address range.

  Define which protocols should be blocked or allowed to ensure security compliance. This step prevents the assignment of dynamic (distribution-range) IP addresses.

- **Procedure for Acquiring Reserved IP Address**

  After the static IP reservation is completed by the **IT Managed Services Provider**, follow these steps to ensure the printer receives the correct address:

  - Disconnect the network cable from the printer;
  - Power off the printer;
  - Wait a few seconds and power it back on;
  - Once the printer completes startup, reconnect the network cable;
  - Confirm the printer has acquired the new static IP address.

- **Set the Friendly Printer Name**

  Define a user-friendly name that will be displayed in the users' printer list.

Examples:
`PRINTER-HQ-ND4020, PRINTER-ATL-L14510, PRINTER-TPA-HPCOLOR.`

Ensure these names are aligned with the **IT Managed Services Provider** and included in the **`L1/L2 Service` support report** to facilitate identification across all support levels.

UNIT VI – Joining MS-Windows Workstations to the Active Directory Domain

Note: A workstation should only be joined to the domain after **all previous procedures have been executed and verified**.

Proceeding without proper validation may compromise the operating system configuration and invalidate the setup process.

1) Configure Domain Membership

Access **System Properties > Advanced System Settings**, click on **Change**, and in the **"Member of"** section:

- Define the **hostname** for the workstation;
- Enter the name of the **domain** to which the workstation will be joined (e.g., `Company's`).

2) Authenticate the Domain Join

Use the domain join credential (usually a delegated account named `INGDOMAIN`), as provided by the **L1/ L2 Service Desk Support Coordinator**.

3) Restart the Workstation

After successful domain join, allow the system to **restart automatically** to complete the integration.

4) Execute Post-Domain Join Script

Once restarted and logged in as a domain user, navigate to the following directory:

`C:\ITSM-Templates-WKS\AfterJoinDomain\`

Run the script below:

`ITSM-AfterJoinDomain.hta`

Right-click and select "Open".

This script performs the following tasks:

- Registers the **new DNS data** of the workstation into the domain **DNS Servers**;
- Applies domain profile adjustments required by the **ITSM-Templates-WKS** standard.

5) Perform Mandatory Logon Cycles

To ensure proper domain integration and offline profile provisioning:

- Log in with the domain user;
- Perform the following sequence **three times**: **Logon → Logoff → Reboot**

This process:

- Enforces domain-based GPO policies;
- Creates the cached user profile for offline access;
- Validates the full application of the workstation's configuration in the domain.

Reminder:
This step applies to **all workstations**, whether operating within the Company's network or at remote locations.

6) Post-Join Verification Tasks

After executing the post-join procedures, the technician must validate the following **under the logged-in domain user profile**:

a) Network Drive Mapping

- Ensure the `T:\` drive is mapped and properly displays the user's assigned network storage.

b) Data Storage Volume

- Confirm that `D:\` is the default data volume for the user's local profile.

c) Printer Mapping

- Verify that the workstation has the designated **user-friendly printer name** mapped correctly.

d) Browser Functionality

- Launch supported web browsers and test access to institutional portals, confirming layout integrity and loading behavior.

e) Script Log Validation – GPO-based domain's rules

Check the following log files under: `C:\Scripts-LOGS\`

Expected files:

```
disks-volumes-wks-rename.log
expired-certificates-purge.log
forticlient-vpn-install.log
fusioninventory-agent-remove.log
glpi-agent-install.log
gpos-synch-and-sysmaint.log
itsm-templates-wks-folder-copy.log
kes-antivirus-install.log
libreoffice-fullpackage-install.log
logon-post-message.log
remove-drive-letter-adminshares.log
softwares-non-comp-remove.log
wingetapps-update.log
zoom-workplace-install.log
```

f) Script Log Validation – ITSM Templates

Confirm that the following script logs are present in: `C:\ITSM-Logs\`

Expected files:

`ITSM-BeforeJoinDomain.log`

`ITSM-AfterJoinDomain.log`

Additional Notes

- Scripts provide visual confirmation and status messages during execution.
- Lightweight operations are performed silently to ensure performance while reducing unnecessary prompts.
- The technician must monitor all interactive messages, execution durations, and output validations.

If any errors occur that cannot be resolved during configuration, report them immediately via the **IT Service Desk System** for escalation to the appropriate support tier.

UNIT VII – Joining MacOS Workstations to the Active Directory Domain

Note: This procedure applies exclusively to MacOS workstations intended for use within the COMPANY network. These devices must comply with the policies established for workstations joined to the Active Directory Domain.

1. **Verify Network Connectivity:**
    - Ensure the workstation is connected to the network and can automatically obtain an `IP address` via DHCP.

2. **Open Directory Utility:**
    - Navigate to **System Preferences > Users & Groups > Login Options**.
    - Click **Join** next to the **Network Account Server**, and then select **Open Directory Utility**.

3. **Configure Directory Utility for Active Directory:** a) In the Directory Utility, enable the **Active Directory** plugin.

   Click **Edit** to specify the following:
    - **Active Directory Domain:** `headq.company.`
    - **Computer ID:** Enter the unique hostname of the workstation, adhering to the naming standard outlined in **Appendix – Unit IX**.

4. **Provide Administrative Credentials:**
    - Use the domain `Administrator` credentials provided by the `L1/L2 Service Desk Support Coordinator` to join the workstation to the Active Directory Domain.

5. **Verify Domain Join:**
    - Restart the workstation after joining the domain, and confirm the login screen displays an option to log in with Active Directory `credentials`

6. **Update DNS Settings:**
    - Open **System Preferences > Network**, and verify that the DNS settings point to the Company's primary and secondary DNS servers:
        - Primary: `dns1.headq.company`
        - Secondary: `dns2.headq.company`

7. **Install Security Certificates:**
    - Download the Company's trusted root certificates from the shared directory: `C:\ITSM-Templates-WKS\Assets\Certificates`.

- Install these certificates into the MacOS **System** and **Login** keychains to ensure compatibility with Company's secured resources.

8. **Configure File and Printer Access:**
    - Map network drives to the Company's file server using **Finder > Go > Connect to Server**, and enter the file server address provided by the `L1/L2 Service Desk Support Coordinator`.
    - Add printers via **System Preferences > Printers & Scanners**, using the `IP address` or `hostname` defined in the **Appendix – Unit IX**.

9. **Verify Compliance:**
    - Ensure the following configurations are applied:
        - Access to Company's internal network resources.
        - Synchronization of user profiles for both offline and online usage.
        - Proper mapping of network drives and printers.
        - Updated DNS and NTP settings.

10. **Report Completion:**
    - Submit a detailed report to the `L1/L2 Service Desk Support Coordinator`, including confirmation of the successful domain join, configuration status, and any issues encountered during the process.

UNIT VIII – Removing MS-Windows Workstations from the Domain Forest

Note: Situations such as workstation replacement, decommissioning, or asset reassignment require the workstation to be properly removed from the Domain Controllers within the entire forest.

The removal process ensures the de-registration of the computer account in Active Directory and the clean disassociation of DNS records, maintaining directory integrity and preventing conflicts.

A) Manual Domain Removal Procedure

1. **Access Advanced System Settings**
    - Navigate to: `System Properties > Computer Name > Change`
    - Under the **Member of** section, select **Workgroup**, and enter a generic group name (e.g., `WORKGROUP`) to leave the domain.
2. **Authenticate with Domain Credentials**
    - When prompted, use the domain-based credential provided by the `L1/ L2 Service Desk Support Coordinator`.
3. **Reboot the Workstation**
    - After confirmation, the system will automatically restart to complete the domain removal process.
4. **Clear DNS Registration**
    - After reboot, run the following command to flush and de-register the DNS records:

      ```
      ipconfig /flushdns && ipconfig /registerdns
      ```

B) Script-Based Domain Removal Procedure

1. **Navigate to Script Directory**

   Path:`C:\ITSM-Templates-WKS\Assets\AdditionalSupportScipts\UnjoinADComputer-and-Cleanup`
2. **Execute the Script**
    - Right-click on `Unjoin-ADComputer-and-Cleanup.ps1`
    - Select **Run with PowerShell**
    - This GUI-based script provides a two-step process:

   Step 1 – Domain Unjoin
    - Click **Leave Domain**
    - The workstation will automatically restart after successful unjoin.

Step 2 – Post-Unjoin Cleanup

- After reboot, re-run the same script.
- Click **Cleanup After Unjoin**
- This will remove cached domain metadata, clear DNS entries, and reboot the system again.

Post-Unjoin Validation

After performing either method:

- Ensure the system is no longer associated with a domain.
- Verify that the hostname is no longer resolvable through the Company's DNS.
- Confirm readiness for:
  - Renaming the device.
  - Reassignment to a new unit.
  - Re-imaging, if necessary.

Note: Always report the completion of workstation removal to the `IT Managed Services Provider`, and update asset status in the Service Desk or Asset Management System.

UNIT IX – Appendix: Standard Hosts Naming

Standardized Hosts Naming for Headquarters and Regional Branches

For example, “NEW YORK BRANCH” would be:

Workstations Desktops

BRANCH			HOST	OFFICE-DIVISION-SECTION						EQUIPMENT ASSET NUMBER				
N	**Y**	**C**	**D**											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Workstations Laptops

BRANCH			HOST	OFFICE-DIVISION-SECTION						EQUIPMENT ASSET NUMBER				
N	**Y**	**C**	**L**											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Printers and Multifunction Printers (MFP) (Printers)

BRANCH			HOST	OFFICE-DIVISION-SECTION						EQUIPMENT ASSET NUMBER				
N	**Y**	**C**	**P**											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Network Scanners (not attached to multifuncion devices)

BRANCH			HOST	OFFICE-DIVISION-SECTION						EQUIPMENT ASSET NUMBER				
N	**Y**	**C**	**P**											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Standardized Naming Convention for Hosts, Sites, and Services Across the IT Infrastructure

This table defines the official three-letter location codes used for naming conventions in hosts, Active Directory Sites, and infrastructure services across all regional divisions.

Region	City / Location	Code
Northeast	Boston, MA	BOS
	New York City, NY	NYC
	Philadelphia, PA	PHL
	Washington, D.C.	DCA
	Hartford, CT	HFD
	Buffalo, NY	BUF
	Pittsburgh, PA	PIT
	Wilmington, DE	ILG
	Richmond, VA	RIC
Southeast	Atlanta, GA	ATL
	Charlotte, NC	CLT
	Miami, FL	MIA
	Orlando, FL	MCO
	Jacksonville, FL	JAX
	Tampa, FL	TPA
	Nashville, TN	BNA
	Raleigh, NC	RDU
	Birmingham, AL	BHM
	Mobile, AL	MOB
	Jackson, MS	JAN
	New Orleans, LA	MSY
Midwest	Chicago, IL	ORD
	Detroit, MI	DTW
	Minneapolis, MN	MSP

Region	City / Location	Code
	Indianapolis, IN	IND
	Kansas City, MO	MCI
	Cleveland, OH	CLE
	Milwaukee, WI	MKE
	Columbus, OH	CMH
	Omaha, NE	OMA
	Fargo, ND	FAR
South	Dallas, TX	DFW
	Houston, TX	HOU
	Austin, TX	AUS
	San Antonio, TX	SAT
	Oklahoma City, OK	OKC
	Memphis, TN	MEM
	Louisville, KY	SDF
	El Paso, TX	ELP
West	Las Vegas, NV	LAS
	Los Angeles, CA	LAX
	San Diego, CA	SAN
	San Francisco, CA	SFO
	Seattle, WA	SEA
	Portland, OR	PDX
	Spokane, WA	GEG
	Salt Lake City, UT	SLC
	Long Beach, CA	LGB
	Eugene, OR	EUG

Region	City / Location	Code
Mountain	Denver, CO	DEN
Pacific Islands	Albuquerque, NM	ABQ
	Boise, ID	BOI
	Colorado Springs, CO	COS
	Billings, MT	BIL
	Rapid City, SD	RAP
	Honolulu, HI	HNL
Alaska	Anchorage, AK	ANC
	Fairbanks, AK	FAI
Border Gateways	San Ysidro, CA (MX Border)	SYS
	Nogales, AZ (MX Border)	NOG
	Buffalo, NY (Canada Border)	BUF
	Detroit, MI (Canada Border)	DTW

Usage Note:

These standardized codes should be used consistently in naming conventions for hostnames, AD Sites/ Subnets, GPO targeting, printer mappings, and deployment scripts to maintain clarity and compliance with infrastructure policies.