

### 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	<a href="#">@brazilianscriptguy</a>	All of You
Approval	2.2	July 21, 2023	<a href="#">@brazilianscriptguy</a>	All of You
Last Update	12.12	Nov 30, 2024	<a href="#">@brazilianscriptguy</a>	All of You

### Classification of this Document

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

### Justifications

<b>STRATEGIC OBJECTIVES</b> (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 – Premises for Executing the ITSM-Templates-WKS Standard.....	2
UNIT II – Preparing and Updating the Workstation.....	7
UNIT III – Standardizing the Workstation for Active Directory Domain Join.....	8
UNIT IV – Institutionalizing the MS-Windows Workstation.....	10
UNIT V – Configuring Printers and Multi-functional Devices.....	11
UNIT VI – Joining MS-Windows Workstations to the Active Directory Domain.....	13
UNIT VII – Joining MacOS Workstations to the Active Directory Domain.....	15
UNIT VIII – Removing MS-Windows Workstations from the Domain Forest.....	17
UNIT IX – Appendix: Standard Host Naming Table.....	18

## **UNIT I – Premises for Executing the ITSM-Templates-WKS Standard**

The procedures must be performed in the sequence outlined in this document, and subsequent steps should not be executed without confirming compliance with the previous steps:

1. Deploy the ITSM-Templates-WKS standard O.S. image on the workstation, setting the default local Administrator password.
2. Ensure you have credentials with the necessary permissions to join workstations to the Domain.
3. When cloning the operating system, verify that the clone followed the sysprep standard, as each operating system's security identifiers (SIDs) must be unique. This step is necessary to avoid duplicate identifiers on the network.
4. Submit in advance to the IT Security Division the list of workstation and printer accounts to be created within the AD object structure, including the MAC addresses of printers, biometric workstations, and workstations requiring continuous services (e.g., online transmission stations, conference workstations). This ensures the IT Security Division can allocate specific IP addresses within the service IP address range and not the distribution range.
5. Ensure knowledge of the credentials for updating/configuring/removing Antivirus and the printer Administrator credentials
6. Notify the IT Infrastructure Division in advance of the need for VLAN changes at the unit where migration is being carried out.
7. Use the latest version of the ITSM-Templates-WKS configuration folder and the most recent version of this Check-List.
8. Define the standardized names for workstations and printers in the unit being migrated.
9. Any errors or obstacles identified beforehand or during the process must be documented and submitted through the IT Service Desk System for resolution by the responsible support level.
10. Send the list of workstation and printer names (preferably via email) in advance to the User and Service Management Section, which will create the domain accounts and confirm them with the requesting unit.
11. Any naming errors detected during the workstation preparation process must be reported to the responsible section for immediate correction.
12. Nonconformity reports regarding the definitions in this document must be submitted weekly to the L1 Service Support Coordinators and the IT Service Desk Head and monthly to the Company's IT Officer.
13. Confirm whether the first stage of this process, deploying the ITSM-Templates-WKS standard O.S. image on the workstation, has been completed, or request information from the L1 Service Support Coordinator.

14. Confirm with the L1 Service Support Coordinator that the operating system clones followed the premise of having unique security identifiers (SIDs). This action is critical to prevent duplicate security identifiers on the network.
15. Verify that the location containing all setup and approved configuration files is the network share provided by the IT Security Division: ...\\DML\\IT-Service-Desk\\, which contains all software (DML - Definitive Media Library).
16. Confirm with the L1 Service Support Coordinator the submission of the following:
  - Standard Migration Form for the Unit.
  - Standard MAC address configurations for printers and biometric workstations, and workstations requiring continuous services (e.g., online transmission stations, Conference workstations). This ensures the IT Security Division can allocate specific IP addresses within the service IP address range and not the distribution range.
17. Confirm with the L1 Service Support Coordinator regarding the configurations and changes to switches and VLANs at the unit where the migration is being carried out, as coordinated by the IT Infrastructure Division.
18. Confirm with the L1 Service Support Coordinator the configuration or adjustments for the following:
  - DHCP Scope;
  - VLAN inclusion in DNS;
  - VLAN inclusion in Sites and Services;
  - Creation of OU structures in Active Directory (AD).
19. Confirm with the L1 Service Support Coordinator that you have copied the latest version of the ITSM-Templates-WKS configuration folder to your removable media and that you possess the latest version of the Check-List Manual for applying ITSM-Templates-WKS to Company's institutional workstations.
20. Confirm that in case of doubts, errors, or issues beyond your scope of management or knowledge, you consult the L1 Service Support Coordinator for clarifications or escalation to the appropriate support level.
21. Commit to executing the following procedures, as they ensure the workstation operating system's compliance with the policies on the domain authentication server and the Domain Forest.
22. Execute the scripts according to the instructions in this Check-List Manual, following the sequence outlined in each chapter. This ensures compliance and adherence to the proper order of configuration execution.
23. All functionalities, commands, and functions executed in this Check-List are features present in the Windows operating system, without the intervention of non-standard commands or external software unrelated to Microsoft operating systems.

24. L1 Service Support teams are the operators and executors of the Check-List. To ensure the maturity and compliance of the execution and communication of incidents described in these procedures, they must report potential script modifications to the L1 Service Support Coordinator. The Coordinators must then communicate these modifications to the IT Security Division via an administrative process.
25. Below is a detailed description of each folder and its contents from the ... \DML\IT-Service-Desk\ directory, noting that the function of each script is described in Unit III and Unit IV of this Check-List:
- **Certificates:** Folder containing Company's certificates to be installed during the workstation's initial configuration.
    - **ADCS-Server:** Contains the certificate for Company's AC Services;
    - **RDS-Server:** Contains the certificate for Company's RDS Services;
    - **WSUS-Server:** Contains the Company's WSUS Services.
  - **CustomImages:** Folder containing standardized Company's images for the machine's local user profile and desktop environment.
  - **MainDocs** – Folder containing the original and editable files for this ITSM-Templates-WKS Manual and the standard system operation figure templates.
    - **Check-ListOrigin** – Folder containing the original and editable file of this Check-List.
    - **DefaultUsersAccountImages** – Folder containing institutional user profile image files and a hosts file with protections against malicious websites, based on the Safer-Networking Ltd. blacklist. These will be replaced once the workstation joins the Domain and is protected by institutional Antivirus and Firewall.
  - **ModifyReg** – Folder containing the initial execution script folders.
    - **AllGeneralConfigs** – Folder containing general configuration scripts.
    - **DefaultBackground** – Folder containing scripts for desktop and logon screen configurations.
    - **UserDesktopFolders** – Contains folders that will be copied to each user's desktop upon logging into the workstation, including institutional shortcuts and links.
    - **UserDesktopTheme** – Contains scripts that apply the Company's institutional theme, replacing default images and configuring the Windows environment for the classic desktop mode.
  - **PostIngress** – Folder containing scripts to be executed after the workstation is joined to the domain.
  - **ScriptsAdditionalSupport** – Folder containing additional support scripts for addressing configuration inconsistencies identified by L1 Service Support:
    - **ActivateAllAdminShare** – Script to activate administrative shares; enable RDP, disable Windows Firewall, and turn off Windows Defender.
    - **ExportCustomThemesFiles** – Script to export customized system themes.

- **FixPrinterDriverIssues** – Script to clear the print spooler and reset all printer drivers on the workstation.
- **GetSID** – Folder with the Microsoft Internals tool to identify the SID (Security Identifier).
- **InventoryInstalledSoftwareList** – Script to inventory the list of installed software on the workstation.
- **LegacyWorkstationIngress** – Script to enable legacy operating system workstations to join new domains.
- **RecallKESCert** – Script to point to the Antivirus server and renew the certificate.
- **RenameDiskVolumes** – Script to locally rename the disk volumes C: and D:.
- **ResyncGPOsDataStore** – Script to reset all GPOs on the workstation and initiate a new synchronization.
- **UnjoinADComputer-and-Cleanup** – Script to unjoin workstations from a domain and clear old domain data.
- **WorkStationConfigReport** – Script for generating configuration reports for each workstation and recording them in a spreadsheet.
- **WorkstationTimeSync** – Script to synchronize the workstation's time, date, and time zone.
- **Uniquescripts** – Folder containing two unified scripts for executing registry (.REG) configurations and script-based (.VBS) configurations.

26. Emphasizing that the function of each script for workstation preparation and their execution order are described in **Unit III** and **Unit IV** of this Check - List.

## UNIT II – Preparing and Updating the Workstation

1. Customize the operating system, referred to as Out-of-Box Experience (OOBE), using the configurations from the sysprep command and providing an initial account to log into the operating system:

a) Remove any other accounts with Administrator privileges, enable the built-in Administrator account, and set a new default password. Use the netplwiz command to confirm that only one account has administrative privileges.

b) Remove all local printers from the workstation, except “Print to PDF.”

c) Enable the Network Properties configuration (IP and DNS address) so the workstation retrieves network settings automatically via DHCP and verify/enable the IPv6 protocol.

**Note:** If the workstation fails to acquire an IP address via DHCP, reset the network environment settings as follows:

- Navigate to:  
C:\ITSM-Templates-WKS\ModifyReg\AllGeneralConfigs\
- Use the Renew-all-IP-Connections.vbs script to reset the TCP/IP connections and enforce the DHCP configuration for the network environment.
- Alternatively, in the Device Manager, remove the network adapter and choose to delete the driver, then restart the workstation.

2. Perform system updates using the WSUS Offline tool for Windows 10 and 11, following these steps:

a) From the network share in the DML, run the update application located in: \WSUS\_Offline-Win10x11-WinSvr\client\UpdateInstaller.exe or use the removable media provided for operating system updates.

b) Select all installation options in the Updating - Installation section. Do not select any options in the Control section.

c) Restart the operating system after receiving the message: "Installation successful. Please reboot your system." Then repeat steps 2.a and 2.b.

d) Continue until there are no more pending updates and the message: "No missing updates found. Nothing to do" is displayed.

e) After completing all updates, restart the system and check the **Control Panel > Windows Update** for any remaining updates.

## UNIT III – Standardizing the Workstation for Active Directory Domain Join

1. Now, logged in with the workstation's local Administrator account, proceed with the following steps, applicable exclusively to Windows 10 and 11 systems. Execute two scripts that consolidate the complete workstation configuration under the ITSM-Templates-WKS standard:

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

b) Open the folder C:\ITSM-Templates-WKS\Uniquescripts\ and execute the script for applying standardized configurations for:

- Desktop layout,
- Themes,
- User desktop folders.

Execute the script:

- ITSM-DefaultVBSing.vbs  
(Note: Right-click the script and select "Run with Command Prompt").

This script includes the following ten (10) configurations:

- Disable-Windows-Firewall.vbs – Disables Windows Firewall.
- Grant-Full-Access-Gestor.vbs – Grants access to the Manager.
- Renew-all-IP-Connections.vbs – Renews TCP/IP connections.
- WSUS-Certificate-Install.vbs – Installs the WSUS certificate.
- WSUS-Clean-SID.vbs – Cleans previous WSUS connections.
- CopyDefaultFolders.vbs – Copies default desktop folders and XML profiles for the desktop and Start menu appearance.
- CopyHosts.vbs – Protects network connections before Antivirus installation.
- CopyUserLogo.vbs – Copies standardized user profile images.
- CopyWallPaperDefault.vbs – Copies default desktop wallpaper images.
- CopyLogonBackground.vbs – Copies default lock screen images.

**Note:** As all ten (10) configurations are encapsulated in a single script, closely monitor any error messages. After execution, the operator must verify which configurations were successfully applied and confirm compliance with the ITSM-Templates-WKS standard.

c) Execute the registry configuration script, standardized for all versions of MS-Windows:

- ITSM-ModifyREGing.vbs  
(Note: Right-click the script and select "Run with Command Prompt").

This script includes the following ten (10) configurations:

- AddStartPageADM.reg – Configures the browser's start page.
- DisableUAC-LUA.reg – Disables User Account Control (UAC).



- `Enable-AutoShareAdmin.reg` – Enables administrative sharing.
- `Register-Owner.reg` – Customizes COMPANY information in the Windows license.
- `Win10_Domain-Ingress.reg` – Secures domain-sharing configurations.
- `WSUS-App-Intranet.reg` – Points to the corporate WSUS server.
- `DesktopCurrent.reg` – Configures the current user's graphical appearance.
- `DesktopDefault.reg` – Configures the default graphical appearance.
- `EnableCustomLogonBackgrounds.reg` – Customizes wallpapers.
- `ITSM-GSTI-Templates.deskthemepack` – Applies the COMPANY standard desktop theme.

**Note:** It is critical that the operator verifies each configuration applied and confirms adherence to the ITSM-Templates-WKS standard.

2. Check for log files generated in the folder `C:\ITSM-Logs-WKS\` to confirm script execution results:
  - `ITSM-DefaultVBSing.log`
  - `ITSM-ModifyREGing.log`
3. If any errors occur that cannot be immediately resolved, report the incidents to the appropriate support level through the IT Service Desk System.

## UNIT IV – Institutionalizing the MS-Windows Workstation

**Note:** To standardize the information of each workstation and ensure that monitoring and asset management software can correctly identify each workstation on the network, it is essential to follow the procedures below.

In case of doubts or issues, always consult the L1 Service Support Coordinator.

1. In the module **Control Panel > Network and Internet > Network Connections**, rename the active network connection to reflect the building or site configuration, such as:
  - COMPANYNet, HQBNet, ATLNet, etc., following the naming conventions for the office or advanced post (see **Appendix – Unit IX**).
2. Standardize the **workstation name**, **disk volume names (C: and D:)**, and **computer description**:
  - **Workstation name example:** CIADMINHQB54890, ATLDSUPPOR67890  
Consult the **Standard Standard Host Naming Table** in **Appendix – Unit IX** or the L1 Service Support Coordinator.
  - **C: drive volume label:** The same as the workstation hostname.
  - **D: drive volume label:** User-Files.

**Note:** Ensure the following:

- The C: drive label matches the workstation hostname.
  - The D: drive label is set to User-Files.
  - **Computer description:** Align with the workstation's assigned unit, for example: Workstation – IT Service Support.
3. For workstations where daily attendance systems or continuous services are installed (e.g., online transmission stations, Conference workstations), provide the **MAC addresses** of these workstations to the **IT Security Division**. This ensures the workstation receives a reserved IP address. Notify the L1 Service Support Coordinator for configuration of the daily attendance system.
  4. If the second partition of the disk is not assigned the letter D:, adjust the settings to make this change.

## UNIT V – Configuring Printers and Multi-functional Devices

**Note:** Printers are also considered domain objects and require specific configurations and firmware updates to join the domain.

1. **Force DHCP Configuration Acquisition:** Use the physical control panel of the printer to enforce network configuration acquisition via DHCP.
2. **Access Embedded Web Server Settings:** Access the printer's Embedded Web Server (EWS) using its assigned IP address to apply the necessary configurations.
3. **Firmware Update:** Ensure the printer firmware is updated to the latest version.
4. **Customize Administrator Credentials:** Modify the default SNMP Administrator credentials following the guidelines provided by the IT Security Division and the IT Infrastructure Division.
5. **Configure Hostname:** Assign the hostname to the printer, following the naming standard outlined in the **Standard Host Naming Table** in **Appendix – Unit IX**.
6. **Disable Unnecessary Protocols:** Turn off all broadcast protocols and WiFi settings, keeping only the following protocols enabled:
  - RAW TCP/IP on port 9100/SMB.
  - HTTP on port 80.
  - LPD service.
7. **Set SNMPv3 and SNMPv2 Protocols:** Configure SNMP credentials as per the guidelines provided by the IT Security Division and the IT Infrastructure Division.
8. **Synchronize Date and Time:** Set up the time synchronization service using the NTP server: `ntp1.headq.company`.
9. **Enable Internal Memory and Storage:** Ensure that the printer's RAM module and internal storage disk are activated.
10. **Configure Network Scanning Login:** Set up the login account for multifunction printers for network scanning.
11. **Acquire Static IP address via DHCP Reservation:** Provide the printer's MAC address to the IT Security Division so that specific IP addresses can be reserved. Define the protocols to be blocked or allowed. This ensures the IP is allocated within the service address range, avoiding assignment in the distribution range.
12. **Procedure for Acquiring a Static IP:** After the IT Security Division reserves the IP address, follow these steps to ensure the printer acquires the IP:

- a) Disconnect the network cable from the printer;
- b) Turn off the printer;

- c) Wait a few seconds, then turn the printer back on;
- d) Once the printer finishes initializing, reconnect the network cable;
- e) Confirm the printer's new IP address.

- 13. Set a Friendly Name for the Printer:** Assign a user-friendly name for display in users' printer lists. **Examples:** PRINTER-HQ-Laser4020, PRINTER-ATL-L14510, PRINTER-TPA-HPCOLOR.
- 14.** Align these names with the IT Security Division and include them in the service report for easier identification across all support levels.

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

**Note:** Joining the workstation to the domain server can only occur after all previous procedures have been completed and verified.

Do not proceed to the following steps without validating all prior procedures and configurations, as this could compromise the operating system's compliance and invalidate the work performed.

1. In **Advanced System Settings > System Properties**, select the **Change** button. Then, in the **Member of** section, specify the computer name and the domain to which the workstation will belong.
2. Confirm the workstation's domain join using the **DOMAIN INGRESS** credential provided by the **L1 Service Support Coordinator**.
3. Confirm that the workstation reboots after being joined to the domain.
4. After rebooting, execute the DNS registration for the workstation to update its **hostname** and new domain information. So, navigate to:

**C:\ITSM-Templates-WKS\PostIngress\**

And execute the script:

- **ITSM-NewDNSRegistering.vbs**  
(Note: Right-click the script and select "Run with Command Prompt").

This script will register the workstation's new information in the **DNS Servers** of the Company's Active Directory forest.

5. Once the workstation is joined to the domain, for all workstations - whether used within a Company's unit or outside the Company's network - the following steps must be performed for each user login (three cycles of login, logoff, and restart):
  - This process enforces the network environment, domain configurations, and user profile registration on the workstation, ensuring proper functionality both within and outside the Company's network. So, navigate to:

**C:\ITSM-Templates-WKS\PostIngress\**

And execute the script:

- **ITSM-ProfileImprinting.vbs**  
(Note: Right-click the script and select "Run with Command Prompt").

This script registers the user's domain profile on the workstation after three logins, enabling usage outside the Company's network.

**Note:** The operator must verify that all configurations have been applied successfully and confirm compliance with the **ITSM-Templates-WKS** standard.

6. Check the logs generated in the folder `C:\ITSM-Logs-WKS\` for error reports related to script execution:

- `ITSM-NewDNSRegistering.log`
- `ITSM-ProfileImprinting.log`

7. After completing the above procedures, verify the configurations within the user's workstation profile:

a) Confirm that the **T: drive is mapped in Windows Explorer**, and its contents align with the user's role (this must be configured by a Domain GPO).

b) Confirm that the **D:** drive stores the user's profile.

c) Verify that the printer is mapped to the user's profile with the assigned friendly name.

d) Launch all browsers and ensure correct access to required portals.

e) Check for logs of installations or updates in the folder `C:\Scripts-LOGS`, which are created automatically by domain rules:

- `disks-volumes-wks-rename.log`
- `expired-certificates-purge.log`
- `forticlient-vpn-install.log`
- `gsti-templates-folder-copy.log`
- `kes-antivirus-install.log`
- `logon-post-message.log`
- `powershell-env-install.log`
- `shared-folders-remove.log`
- `softwares-non-comp-remove.log`
- `wingetapps-update.log`
- `zoom-workplace-install.log`

f) Check logs in the folder `C:\ITSM-Logs-WKS\` for any errors related to the execution of this Check-List:

- `ITSM-DefaultVBSing.log`
- `ITSM-ModifyREGing.log`
- `ITSM-NewDNSRegistering.log`
- `ITSM-ProfileImprinting.log`

**Note:** Script interactions include confirmation messages for the operator, ensuring awareness of wait times and transitions between executions. Minimal interactions are omitted to streamline the process.

## 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:

1. Ensure the workstation is connected to the network and can automatically obtain an IP address via DHCP.

### 2. Open Directory Utility:

1. Navigate to **System Preferences > Users & Groups > Login Options**.
2. 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.

b) Click **Edit** to specify the following:

1. **Active Directory Domain:** headq.company.
2. **Computer ID:** Enter the unique hostname of the workstation, adhering to the naming standard outlined in **Appendix – Unit IX**.

### 4. Provide Administrative Credentials:

1. Use the domain Administrator credentials provided by the L1 Service Support Coordinator to join the workstation to the Active Directory Domain.

### 5. Verify Domain Join:

1. 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:

1. Open **System Preferences > Network**, and verify that the DNS settings point to the Company's primary and secondary DNS servers:
  1. Primary: dns1.Headq.company
  2. Secondary: dns2.Headq.company

### 7. Install Security Certificates:

1. Download the Company's trusted root certificates from the shared directory: C:\ITSM-Templates-WKS\Certificates\.
2. Install these certificates into the MacOS **System** and **Login** keychains to ensure compatibility with Company's secured resources.

## **8. Configure File and Printer Access:**

1. 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 Service Support Coordinator.
2. Add printers via **System Preferences > Printers & Scanners**, using the IP address or hostname defined in the **Appendix – Unit IX**.

## **9. Verify Compliance:**

1. Ensure the following configurations are applied:
  1. Access to Company's internal network resources.
  2. Synchronization of user profiles for both offline and online usage.
  3. Proper mapping of network drives and printers.
  4. Updated DNS and NTP settings.

## **10. Report Completion:**

1. Submit a detailed report to the IT Service Desk System, 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:** In certain situations, such as replacing a workstation, decommissioning equipment, or other events, it becomes necessary to unjoin/remove the workstation from the Domain Servers. Thus, there is a specific procedure to follow before replacing the equipment to remove the current computer account.

### 1. Manual Procedure to Unjoin/Remove a Workstation from the Domain:

- a) In **Advanced System Settings > System Properties**, click the **Change** button. Then, in the **Member of:** section, specify the **Workgroup** to which the workstation will be downgraded/unjoined (e.g., **WORKGROUP**).
- b) Confirm the unjoining/removal of the workstation using the **DOMAIN INGRESS** credentials provided by the Support Coordinator (L1 Service Support).
- c) Ensure the workstation restarts after being unjoined/removed from the Domain.
- d) After the workstation restarts, remove its DNS records to delete the hostname information from the DNS Server of the HEADQ . COMPANY Forest by executing the following command at CMD:

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

### 2. Script-Based Procedure to Unjoin/Remove a Workstation from the Domain

- a) Navigate to the folder:

```
C:\ITSM-Templates-WKS\ScriptsAdditionalSupport\UnjoinADComputer-and-Cleanup
```

Execute the script: `Unjoin-ADComputer-and-Cleanup.ps1`

*(Note: Right-click the script and select “Run with Command Prompt”).*

This script performs two operations in a single execution:

- b) Click the button **LEAVE DOMAIN**, and after the process is complete, the workstation will restart.
- c) Once the workstation restarts, run the script again and click the button **POST-REMOVAL CLEANUP**. The workstation will restart again and will then be ready to receive a new hostname or be reallocated.

## UNIT IX – Appendix: Standard Host Naming Table

### Standardized Host Naming for Headquarters and Regional Branches

For example, "NEW YORK BRANCH" would be:

#### Workstations **D**esktops

BRANCH			HOST	OFFICE-DIVISION-SECTION						EQUIPAMENT ASSET NUMBER				
<b>N</b>	<b>Y</b>	<b>C</b>	<b>D</b>											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

#### Workstations **N**otebooks

BRANCH			HOST	OFFICE-DIVISION-SECTION						EQUIPAMENT ASSET NUMBER				
<b>N</b>	<b>Y</b>	<b>C</b>	<b>N</b>											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

#### Printers and Multifunction printers (MFP) (**P**rinters)

BRANCH			HOST	OFFICE-DIVISION-SECTION						EQUIPAMENT ASSET NUMBER				
<b>N</b>	<b>Y</b>	<b>C</b>	<b>P</b>											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

#### Network **S**canners (not attached to multifunction devices)

BRANCH			HOST	OFFICE-DIVISION-SECTION						EQUIPAMENT ASSET NUMBER				
<b>N</b>	<b>Y</b>	<b>C</b>	<b>S</b>											
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 Entire IT Infrastructure

Region	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
	Chicago, IL	ORD
Midwest	Detroit, MI	DTW
	Minneapolis, MN	MSP
	Indianapolis, IN	IND

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

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