==========

==========

CATEGORY: UserProfiles

==========

==========

User profile operations directly affect login behavior, data storage, troubleshooting, and de-provisioning workflows. These SOPs ensure every user-profile-related action performed through RDAM Script Wizard is **controlled**, **auditable**, and aligned with **enterprise operational and security standards**.

SOP 1 – List User Profiles

Script Name: List User Profiles **Category:** UserProfiles **Version:** 1.0 **Approved By:** IT Operations / Security

1. Purpose==========

CATEGORY: WindowsUpdates

==========

==========

Windows Update operations directly affect system security, stability, compliance, and lifecycle management. These SOPs ensure every update-related action performed through RDAM Script Wizard is **controlled**, **auditable**, and aligned with **enterprise patch-management standards**.

SOP 1 – Check for Available Updates

Script Name: Check for Available Updates **Category:** WindowsUpdates **Version:** 1.0 **Approved By:** IT Operations / Security**

1. Purpose

This script checks for available Windows updates, supporting patch compliance, vulnerability management, and maintenance planning.

2. Scope

- Windows servers and workstations
- Windows Update, WSUS, or Microsoft Update sources

3. Definitions

- **Update Scan:** Querying update sources for applicable patches.

4. Preconditions

- Operator must have permission to query update status.
- Windows Update service must be running.
- System must have internet or WSUS connectivity.

5. Required Inputs

- None

6. Procedure Steps

1. Initialize Update Scan
    - Trigger Windows Update detection.
2. Retrieve Available Updates
    - Extract:
        - KB numbers
        - Update titles
        - Categories (Security, Critical, Feature)
        - Download size
3. Output Formatting
    - Present structured list of available updates.
4. Logging
    - Log operator and timestamp.

7. Expected Output

- List of updates available for installation.

8. Post-Execution Validation

- Operator may verify via Windows Update GUI.

9. Error Handling

- Update service disabled
- Connectivity failure
- Access denied

10. Security Considerations

- Update metadata may reveal vulnerability exposure.

11. Audit Logging Requirements

- Operator ID
- Timestamp

12. Organizational Benefit Statement

This script provides a consistent, auditable method for identifying pending updates, supporting compliance and security.

SOP 2 – Install Available Updates

Script Name: Install Available Updates **Category:** WindowsUpdates**

1. Purpose

This script installs all applicable Windows updates, supporting patch compliance, vulnerability mitigation, and system maintenance.

2. Scope

- Windows servers and workstations
- Windows Update, WSUS, or Microsoft Update

3. Definitions

- **Update Installation:** Downloading and applying patches.

4. Preconditions

- Operator must have administrative rights.
- System must be allowed to install updates.
- Reboot may be required.

5. Required Inputs

- Optional: Install only security updates
- Optional: Install only specific KB numbers

6. Procedure Steps

1. Input Collection
    - Wizard prompts for optional filters.
2. Update Scan
    - Retrieve applicable updates.
3. Filtering
    - Apply KB or category filters.
4. Installation Operation
    - Download updates.
    - Install updates.
    - Capture installation results.
5. Reboot Handling
    - If reboot required, notify operator.
6. Logging
    - Log updates installed, operator, timestamp.

7. Expected Output

- Confirmation of installed updates.

8. Post-Execution Validation

- Operator may verify via Windows Update history.

9. Error Handling

- Installation failure

- Access denied
- Update conflict
- Reboot pending

10. Security Considerations

- Installing updates may temporarily impact performance.

11. Audit Logging Requirements

- Operator ID
- KB numbers installed
- Timestamp

12. Organizational Benefit Statement

This script ensures updates are installed safely and consistently, supporting security and compliance.

SOP 3 – Get Windows Update History

Script Name: Get Windows Update History **Category:** WindowsUpdates**

1. Purpose

This script retrieves the update installation history, supporting compliance audits, troubleshooting, and forensic analysis.

2. Scope

- Windows servers and workstations
- Windows Update, WSUS, and manual installs

3. Definitions

- **Update History:** Log of installed patches and results.

4. Preconditions

- Operator must have permission to query update history.

5. Required Inputs

- Optional: KB filter
- Optional: Date range

6. Procedure Steps

1. Input Collection
    - Wizard prompts for optional filters.
2. History Enumeration
    - Retrieve installed updates.
3. Filtering
    - Apply KB or date filters.
4. Output Formatting
    - Present structured update history.
5. Logging
    - Log filters, operator, timestamp.

7. Expected Output

- List of installed updates with metadata.

8. Post-Execution Validation

- Operator may verify via Windows Update GUI.

9. Error Handling

- Access denied
- History unavailable
- Invalid filter

10. Security Considerations

- Patch history may reveal vulnerability exposure.

11. Audit Logging Requirements

- Operator ID
- Filters used
- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for retrieving update history, supporting compliance and troubleshooting.

SOP 4 – Pause Windows Updates

Script Name: Pause Windows Updates **Category:** WindowsUpdates**

1. Purpose

This script pauses Windows Updates for a defined period, supporting maintenance windows, troubleshooting, and stability control.

2. Scope

- Windows 10/11
- Windows Update service

3. Definitions

- **Pause:** Temporarily prevents update installation.

4. Preconditions

- Operator must have administrative rights.
- System must support update pausing.

5. Required Inputs

- Pause duration (days)

6. Procedure Steps

1. Input Collection
    - Wizard prompts for pause duration.
2. Apply Pause
    - Configure Windows Update pause settings.
3. Post-Change Verification
    - Confirm pause is active.
4. Logging
    - Log duration, operator, timestamp.

7. Expected Output

- Confirmation that updates are paused.

8. Post-Execution Validation

- Operator may verify via Windows Update GUI.

9. Error Handling

- Unsupported OS
- Access denied
- Invalid duration

10. Security Considerations

- Pausing updates increases vulnerability exposure.

11. Audit Logging Requirements

- Operator ID
- Duration
- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for pausing updates, supporting maintenance and troubleshooting.

SOP 5 – Resume Windows Updates

Script Name: Resume Windows Updates **Category:** WindowsUpdates**

1. Purpose

This script resumes Windows Updates after a pause period, supporting patch compliance and security posture restoration.

2. Scope

- Windows 10/11
- Windows Update service

3. Definitions

- **Resume:** Re-enable update scanning and installation.

4. Preconditions

- Operator must have administrative rights.

5. Required Inputs

- None

6. Procedure Steps

1. Clear Pause Settings
    - Remove pause configuration.
2. Trigger Update Scan
    - Initiate detection cycle.
3. Output Formatting
    - Present confirmation.
4. Logging
    - Log operator and timestamp.

7. Expected Output

- Confirmation that updates are resumed.

8. Post-Execution Validation

- Operator may verify via Windows Update GUI.

9. Error Handling

- Access denied
- Update service disabled

10. Security Considerations

- Resuming updates may trigger immediate downloads.

11. Audit Logging Requirements

- Operator ID

- Timestamp

12. Organizational Benefit Statement

This script ensures update resumption is performed safely and consistently, supporting compliance and security.

SOP 6 – Force Windows Update Detection Cycle

Script Name: Force Windows Update Detection Cycle **Category:** WindowsUpdates**

1. Purpose

This script forces Windows to immediately check for updates, supporting troubleshooting, compliance, and patch validation.

2. Scope

- Windows servers and workstations
- Windows Update, WSUS

3. Definitions

- **Detection Cycle:** Immediate update scan.

4. Preconditions

- Operator must have administrative rights.
- Update service must be running.

5. Required Inputs

- None

6. Procedure Steps

1. Trigger Detection
    - Force Windows Update to scan immediately.
2. Monitor Status
    - Capture detection results.
3. Output Formatting
    - Present detection summary.
4. Logging

- Log operator and timestamp.

7. Expected Output

- Confirmation that detection cycle was triggered.

8. Post-Execution Validation

- Operator may verify via Windows Update GUI.

9. Error Handling

- Access denied
- Update service disabled

10. Security Considerations

- Frequent scans may increase network load.

11. Audit Logging Requirements

- Operator ID
- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for forcing update detection, supporting troubleshooting and compliance.

This script enumerates all local user profiles on the system, supporting troubleshooting, cleanup, and inventory.

2. Scope

- Windows servers and workstations
- Local user profiles stored under `C:\Users`

3. Definitions

- **User Profile:** A directory containing user-specific data and configuration.
- **Profile State:** Loaded, unloaded, temporary, or corrupted.

4. Preconditions

- Operator must have permission to query profile information.

5. Required Inputs

- Optional: Username filter

6. Procedure Steps

1. Input Collection
    - Wizard prompts for optional filter.
2. Profile Enumeration
    - Retrieve all local profiles.
3. Attribute Retrieval
    - Extract:
        - Username
        - Profile path
        - SID
        - Last modified time
        - Profile state
4. Output Formatting
    - Present structured profile list.
5. Logging
    - Log filter, operator, timestamp.

7. Expected Output

- List of user profiles with key attributes.

8. Post-Execution Validation

- Operator may verify via `wmic userprofile`.

9. Error Handling

- Access denied
- Invalid filter

10. Security Considerations

- Profile data may reveal sensitive user information.

11. Audit Logging Requirements

- Operator ID
- Filter used
- Timestamp

12. Organizational Benefit Statement

This script provides a consistent, auditable method for enumerating user profiles, supporting troubleshooting and cleanup workflows.

SOP 2 – Get User Profile Details

Script Name: Get User Profile Details **Category:** UserProfiles

1. Purpose

This script retrieves detailed information about a specific user profile, supporting troubleshooting, forensic analysis, and configuration validation.

2. Scope

- Windows servers and workstations
- Local user profiles

3. Definitions

- **Profile Details:** Includes path, SID, size, state, and timestamps.

4. Preconditions

- Operator must have permission to query profile details.
- Profile must exist.

5. Required Inputs

- Username or profile path

6. Procedure Steps

1. Input Collection
    - Wizard prompts for username or path.
2. Profile Resolution
    - Identify matching profile.

3. Attribute Retrieval
    - Extract:
        - SID
        - Profile path
        - State
        - Last use time
        - Profile size (optional)
4. Output Formatting
    - Present structured profile details.
5. Logging
    - Log username/path, operator, timestamp.

7. Expected Output

- Detailed user profile information.

8. Post-Execution Validation

- Operator may verify via `wmic userprofile`.

9. Error Handling

- Profile not found
- Access denied

10. Security Considerations

- Profile paths may contain sensitive data.

11. Audit Logging Requirements

- Operator ID
- Username/path
- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for retrieving user profile details, supporting troubleshooting and forensic workflows.

SOP 3 – Remove User Profile

Script Name: Remove User Profile **Category:** UserProfiles

1. Purpose

This script deletes a user profile from the system, supporting de-provisioning, cleanup, and troubleshooting.

2. Scope

- Windows servers and workstations
- Local user profiles

3. Definitions

- **Profile Removal:** Deletes profile directory and registry references.

4. Preconditions

- Operator must have administrative rights.
- Profile must not be currently loaded.
- Removal must be authorized.

5. Required Inputs

- Username or profile path

6. Procedure Steps

1. Input Collection
    - Wizard prompts for username or path.
2. Profile Resolution
    - Identify matching profile.
3. Safety Check
    - Confirm profile is not in use.
    - Prevent deletion of system or service profiles.
4. Removal Operation
    - Delete profile directory.
    - Remove registry references.

5. Post-Removal Verification
    - Confirm profile no longer exists.
6. Logging
    - Log username/path, operator, timestamp.

7. Expected Output

- Confirmation of profile removal.

8. Post-Execution Validation

- Operator may verify via `wmic userprofile`.

9. Error Handling

- Profile in use
- Access denied
- Profile not found

10. Security Considerations

- Deleting profiles permanently removes user data; ensure approvals.

11. Audit Logging Requirements

- Operator ID
- Username/path
- Timestamp

12. Organizational Benefit Statement

This script ensures profile removal is performed safely and with full accountability, supporting de-provisioning and cleanup.

SOP 4 – Set User Profile Path

Script Name: Set User Profile Path **Category:** UserProfiles

1. Purpose

This script updates the profile path for a user account, supporting profile migrations, storage changes, and troubleshooting.

2. Scope

- Windows servers and workstations
- Local user accounts

3. Definitions

- **Profile Path:** Directory where user data is stored.

4. Preconditions

- Operator must have administrative rights.
- New path must exist or be creatable.
- User must not be logged in.

5. Required Inputs

- Username
- New profile path

6. Procedure Steps

1. Input Collection
    - Wizard prompts for username and new path.
2. Validation
    - Confirm user exists.
    - Confirm path validity.
3. Update Operation
    - Modify registry profile path.
4. Optional Migration
    - Copy existing profile data to new path (if supported).
5. Post-Update Verification
    - Confirm registry and file system alignment.
6. Logging
    - Log username, new path, operator, timestamp.

7. Expected Output

- Confirmation of profile path update.

8. Post-Execution Validation

- Operator may verify via registry and file system.

9. Error Handling

- Access denied
- Invalid path
- User logged in

10. Security Considerations

- Profile path changes may affect application behavior.

11. Audit Logging Requirements

- Operator ID
- Username
- New path
- Timestamp

12. Organizational Benefit Statement

This script ensures profile path changes are performed safely and consistently, supporting migrations and troubleshooting.

SOP 5 – Get User Profile Size

Script Name: Get User Profile Size **Category:** UserProfiles

1. Purpose

This script calculates the total size of a user profile, supporting storage analysis, cleanup planning, and troubleshooting.

2. Scope

- Windows servers and workstations
- Local user profiles

3. Definitions

- **Profile Size:** Total size of all files and subfolders.

4. Preconditions

- Operator must have read access to the profile directory.

5. Required Inputs

- Username or profile path

6. Procedure Steps

1. Input Collection
    - Wizard prompts for username or path.
2. Profile Resolution
    - Identify matching profile.
3. Recursive Enumeration
    - Traverse profile directory.
    - Sum file sizes.
4. Output Formatting
    - Present total size in MB/GB.
5. Logging
    - Log username/path, operator, timestamp.

7. Expected Output

- Total profile size.

8. Post-Execution Validation

- Operator may verify via File Explorer.

9. Error Handling

- Access denied
- Profile not found
- Large directory performance issues

10. Security Considerations

- Profile contents may include sensitive data.

11. Audit Logging Requirements

- Operator ID
- Username/path
- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for calculating profile size, supporting storage planning and cleanup.