

=====

=====

CATEGORY: WindowsFeatures

=====

=====

Windows feature operations directly affect system capabilities, application support, security posture, and server roles. These SOPs ensure every feature-related action performed through RDAM Script Wizard is **controlled**, **auditable**, and aligned with **enterprise operational and security standards**.

SOP 1 – List Windows Features

Script Name: List Windows Features **Category:** WindowsFeatures **Version:** 1.0 **Approved By:** IT Operations / Engineering

1. Purpose

This script enumerates all Windows features and their installation states, supporting troubleshooting, compliance, and system configuration reviews.

2. Scope

- Windows servers and workstations
- Optional features, roles, and role services

3. Definitions

- **Windows Feature:** A modular component that can be enabled or disabled.
- **State:** Enabled, Disabled, or Disabled with Payload Removed.

4. Preconditions

- Operator must have permission to query system features.

5. Required Inputs

- Optional: Feature name filter

6. Procedure Steps

1. Input Collection
 - Wizard prompts for optional filter.
2. Feature Enumeration
 - Retrieve all features and states.
3. Filtering
 - Apply name filter if provided.
4. Output Formatting
 - Present structured feature list.
5. Logging
 - Log filter, operator, timestamp.

7. Expected Output

- List of Windows features with installation states.

8. Post-Execution Validation

- Operator may verify via `Get-WindowsOptionalFeature` or Server Manager.

9. Error Handling

- Access denied
- Invalid filter
- Feature list unavailable

10. Security Considerations

- Feature data may reveal system capabilities.

11. Audit Logging Requirements

- Operator ID
- Filter used
- Timestamp

12. Organizational Benefit Statement

This script provides a consistent, auditable method for enumerating Windows features, supporting troubleshooting and configuration management.

SOP 2 – Enable Windows Feature

Script Name: Enable Windows Feature **Category:** WindowsFeatures

1. Purpose

This script enables a Windows feature, supporting application requirements, system configuration, and server role deployment.

2. Scope

- Windows servers and workstations
- Optional features and server roles

3. Definitions

- **Enable Feature:** Install and activate a Windows component.

4. Preconditions

- Operator must have administrative rights.
- Feature must exist.
- Action must be authorized.
- System may require reboot.

5. Required Inputs

- Feature name
- Optional: Source path (for payload-removed features)

6. Procedure Steps

1. Input Collection

- Wizard prompts for feature name and optional source.

2. Validation

- Confirm feature exists.
- Confirm source path if required.

3. Enable Operation

- Install and enable feature.

4. Reboot Handling

- Notify operator if reboot required.

5. Post-Enable Verification

- Confirm feature state is Enabled.

6. Logging

- Log feature name, operator, timestamp.

7. Expected Output

- Confirmation that feature was enabled.

8. Post-Execution Validation

- Operator may verify via Server Manager or PowerShell.

9. Error Handling

- Feature not found
- Access denied
- Payload missing
- Reboot pending

10. Security Considerations

- Enabling features may expand attack surface.

11. Audit Logging Requirements

- Operator ID
- Feature name
- Timestamp

12. Organizational Benefit Statement

This script ensures feature enablement is performed safely and consistently, supporting system configuration and application readiness.

SOP 3 – Disable Windows Feature

Script Name: Disable Windows Feature **Category:** WindowsFeatures

1. Purpose

This script disables a Windows feature, supporting hardening, cleanup, and configuration rollback.

2. Scope

- Windows servers and workstations
- Optional features and server roles

3. Definitions

- **Disable Feature:** Remove or deactivate a Windows component.

4. Preconditions

- Operator must have administrative rights.
- Feature must exist.
- Action must be authorized.

5. Required Inputs

- Feature name
- Optional: Remove payload flag

6. Procedure Steps

1. Input Collection
 - Wizard prompts for feature name and options.
2. Validation
 - Confirm feature exists.
3. Disable Operation
 - Disable feature.
 - Optionally remove payload.
4. Reboot Handling
 - Notify operator if reboot required.
5. Post-Disable Verification

- Confirm feature state is Disabled.

6. Logging

- Log feature name, operator, timestamp.

7. Expected Output

- Confirmation that feature was disabled.

8. Post-Execution Validation

- Operator may verify via Server Manager or PowerShell.

9. Error Handling

- Feature not found
- Access denied
- Dependency conflict

10. Security Considerations

- Removing features may impact applications or services.

11. Audit Logging Requirements

- Operator ID
- Feature name
- Timestamp

12. Organizational Benefit Statement

This script ensures feature disablement is performed safely and with full accountability, supporting hardening and configuration management.

SOP 4 – Get Installed Roles and Features (Server)

Script Name: Get Installed Roles and Features (Server) **Category:** WindowsFeatures

1. Purpose

This script retrieves installed server roles and features, supporting configuration audits, compliance, and troubleshooting.

2. Scope

- Windows Server systems
- Roles, role services, and features

3. Definitions

- **Server Role:** Major functional component (e.g., AD DS, IIS).
- **Role Service:** Sub-component of a server role.

4. Preconditions

- Operator must have permission to query server roles.
- System must be running Windows Server.

5. Required Inputs

- None

6. Procedure Steps

1. Role Enumeration
 - Retrieve installed roles and role services.
2. Feature Enumeration
 - Retrieve installed features.
3. Output Formatting
 - Present structured role/feature summary.
4. Logging
 - Log operator and timestamp.

7. Expected Output

- List of installed roles and features.

8. Post-Execution Validation

- Operator may verify via Server Manager.

9. Error Handling

- Access denied
- Unsupported OS

10. Security Considerations

- Role data may reveal system purpose and exposure.

11. Audit Logging Requirements

- Operator ID
- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for retrieving server roles and features, supporting compliance and configuration management.

SOP 5 – Install Windows Capability (Optional Features)

Script Name: Install Windows Capability **Category:** WindowsFeatures

1. Purpose

This script installs Windows capabilities (e.g., RSAT tools, language packs), supporting administrative workflows and application requirements.

2. Scope

- Windows 10/11
- Windows capabilities via DISM or PowerShell

3. Definitions

- **Capability:** Optional component delivered via Windows Update or local source.

4. Preconditions

- Operator must have administrative rights.
- Capability must exist.
- System must have access to capability source.

5. Required Inputs

- Capability name
- Optional: Source path

6. Procedure Steps

1. Input Collection
 - Wizard prompts for capability name and optional source.
2. Validation
 - Confirm capability availability.
3. Installation Operation
 - Install capability via DISM or PowerShell.
4. Reboot Handling
 - Notify operator if reboot required.
5. Post-Install Verification
 - Confirm capability installed.
6. Logging
 - Log capability name, operator, timestamp.

7. Expected Output

- Confirmation of capability installation.

8. Post-Execution Validation

- Operator may verify via `Get-WindowsCapability`.

9. Error Handling

- Capability not found
- Access denied
- Source unavailable

10. Security Considerations

- Installing capabilities may introduce new administrative tools.

11. Audit Logging Requirements

- Operator ID
- Capability name
- Timestamp

12. Organizational Benefit Statement

This script ensures capability installation is performed safely and consistently, supporting administrative workflows and system configuration.