

=====

=====

## CATEGORY: RemoteDesktop

=====

=====

Remote Desktop Protocol (RDP) operations directly affect system accessibility, administrative workflows, and security posture. These SOPs ensure every RDP-related action performed through RDM Script Wizard is **controlled, auditable**, and aligned with **enterprise security and operational standards**.

### SOP 1 – Get RDP Status

**Script Name:** Get RDP Status **Category:** RemoteDesktop **Version:** 1.0 **Approved By:** IT Operations / Security

#### 1. Purpose

This script retrieves the current Remote Desktop enablement state and supporting configuration, helping teams validate access, troubleshoot connectivity, and confirm compliance.

#### 2. Scope

- Windows servers and workstations
- Local and remote systems (if supported)

#### 3. Definitions

- **RDP Enabled:** System accepts inbound Remote Desktop connections.
- **NLA:** Network Level Authentication requirement.

#### 4. Preconditions

- Operator must have read access to system configuration.
- System must be reachable.

#### 5. Required Inputs

- None

## 6. Procedure Steps

1. Query RDP Registry Keys
  - Retrieve values controlling RDP enablement and NLA.
2. Query Firewall Rules
  - Check if RDP firewall rules are enabled.
3. Consolidate Status
  - Determine:
    - RDP enabled/disabled
    - NLA enabled/disabled
    - Firewall open/closed
4. Output Formatting
  - Present structured RDP status summary.
5. Logging
  - Log operator and timestamp.

## 7. Expected Output

- RDP enablement state and supporting configuration.

## 8. Post-Execution Validation

- Operator may verify via System Properties or `Get-NetFirewallRule`.

## 9. Error Handling

- Access denied
- Registry keys missing
- Firewall query failure

## 10. Security Considerations

- RDP status reveals system exposure; restrict access.

## 11. Audit Logging Requirements

- Operator ID
- Timestamp

## 12. Organizational Benefit Statement

This script provides a consistent, auditable method for validating RDP configuration, supporting troubleshooting and compliance.

# SOP 2 – Enable RDP

**Script Name:** Enable RDP **Category:** RemoteDesktop

## 1. Purpose

This script enables Remote Desktop access on a system, supporting remote administration, troubleshooting, and operational workflows.

## 2. Scope

- Windows servers and workstations
- Local and remote systems (if supported)

## 3. Definitions

- **Enable RDP:** Allow inbound RDP connections via registry and firewall.

## 4. Preconditions

- Operator must have administrative rights.
- Action must be authorized.
- Firewall rules must be validated.

## 5. Required Inputs

- Optional: Enable/disable NLA

## 6. Procedure Steps

1. Input Collection
  - Wizard prompts for NLA preference.
2. Registry Update
  - Enable RDP listener.
  - Apply NLA setting.
3. Firewall Configuration
  - Enable RDP firewall rules.

#### 4. Post-Change Verification

- Confirm registry values.
- Confirm firewall rules active.

#### 5. Logging

- Log operator, NLA setting, timestamp.

### 7. Expected Output

- Confirmation that RDP is enabled.

### 8. Post-Execution Validation

- Operator may test RDP connectivity.

### 9. Error Handling

- Access denied
- Registry write failure
- Firewall rule failure

### 10. Security Considerations

- Enabling RDP increases attack surface; ensure approvals.
- NLA should remain enabled unless explicitly authorized.

### 11. Audit Logging Requirements

- Operator ID
- NLA setting
- Timestamp

### 12. Organizational Benefit Statement

This script ensures RDP enablement is performed safely and with full accountability, supporting remote administration and troubleshooting.

## SOP 3 – Disable RDP

**Script Name:** Disable RDP **Category:** RemoteDesktop

# 1. Purpose

This script disables Remote Desktop access, supporting security hardening, incident response, and compliance enforcement.

## 2. Scope

- Windows servers and workstations
- Local and remote systems (if supported)

## 3. Definitions

- **Disable RDP:** Prevent inbound RDP connections.

## 4. Preconditions

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

## 5. Required Inputs

- None

## 6. Procedure Steps

1. Registry Update
  - Disable RDP listener.
2. Firewall Configuration
  - Disable RDP firewall rules.
3. Post-Change Verification
  - Confirm registry values.
  - Confirm firewall rules disabled.
4. Logging
  - Log operator and timestamp.

## 7. Expected Output

- Confirmation that RDP is disabled.

## 8. Post-Execution Validation

- Operator may verify via System Properties.

## 9. Error Handling

- Access denied
- Registry write failure
- Firewall rule failure

## 10. Security Considerations

- Disabling RDP may impact remote access workflows; ensure approvals.

## 11. Audit Logging Requirements

- Operator ID
- Timestamp

## 12. Organizational Benefit Statement

This script ensures RDP disablement is performed safely and consistently, supporting security hardening and compliance.

# SOP 4 – Get Active RDP Sessions

**Script Name:** Get Active RDP Sessions **Category:** RemoteDesktop

## 1. Purpose

This script retrieves active Remote Desktop sessions, supporting troubleshooting, access validation, and security monitoring.

## 2. Scope

- Windows servers and workstations
- Local and remote systems (if supported)

## 3. Definitions

- **Session:** A logged-in user context.
- **State:** Active, disconnected, idle.

## 4. Preconditions

- Operator must have permission to query session information.

## 5. Required Inputs

- None

## 6. Procedure Steps

1. Session Enumeration
  - Retrieve all RDP sessions.
2. Attribute Retrieval
  - Extract:
    - Username
    - Session ID
    - State
    - Logon time
    - Idle time
3. Output Formatting
  - Present structured session list.
4. Logging
  - Log operator and timestamp.

## 7. Expected Output

- List of active and disconnected RDP sessions.

## 8. Post-Execution Validation

- Operator may verify using `quser` or Task Manager.

## 9. Error Handling

- Access denied
- Session service unavailable

## 10. Security Considerations

- Session data may reveal sensitive user activity.

## 11. Audit Logging Requirements

- Operator ID

- Timestamp

## 12. Organizational Benefit Statement

This script provides a controlled, auditable method for enumerating RDP sessions, supporting troubleshooting and security monitoring.

# SOP 5 – Disconnect RDP Session

**Script Name:** Disconnect RDP Session **Category:** RemoteDesktop

## 1. Purpose

This script disconnects an active RDP session without logging the user off, supporting troubleshooting, resource management, and incident response.

## 2. Scope

- Windows servers and workstations
- Local and remote systems (if supported)

## 3. Definitions

- **Disconnect:** Session remains active but not interactive.

## 4. Preconditions

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

## 5. Required Inputs

- Session ID or username

## 6. Procedure Steps

### 1. Input Collection

- Wizard prompts for session ID or username.

### 2. Session Resolution

- Identify matching session.

### 3. Safety Check

- Prevent disconnecting critical service accounts unless authorized.

#### 4. Disconnect Operation

- Disconnect session using appropriate API.

#### 5. Post-Disconnect Verification

- Confirm session state is now “Disconnected.”

#### 6. Logging

- Log session ID/username, operator, timestamp.

### 7. Expected Output

- Confirmation of session disconnection.

### 8. Post-Execution Validation

- Operator may verify via `quser`.

### 9. Error Handling

- Session not found
- Access denied
- Operation blocked by system

### 10. Security Considerations

- Disconnecting sessions may interrupt user workflows; ensure approvals.

### 11. Audit Logging Requirements

- Operator ID
- Session ID/username
- Timestamp

### 12. Organizational Benefit Statement

This script ensures RDP session disconnection is performed safely and with full accountability, supporting troubleshooting and resource management.