==

CATEGORY: WindowsRemoteDesktop (RDP)

==

Remote Desktop Protocol (RDP) operations directly affect remote administration, user access, security posture, and compliance. These SOPs ensure every RDP-related action performed through RDAM Script Wizard is **controlled**, **auditable**, and aligned with enterprise security standards.

SOP 1 – Get RDP Status

1. Purpose

Retrieve whether Remote Desktop is enabled and which authentication modes are active.

2. Scope

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

3. Preconditions

- **Operator must have permission to query system configuration**

4. Required Inputs

- **None**

5. Procedure Steps

- **Status Retrieval** – Query RDP enablement state.
- **NLA Check –** Determine if Network Level Authentication is required.
- **Firewall Check** – Confirm RDP firewall rules are enabled.
- **Output Formatting** – Present structured RDP status.
- **Logging** – Operator and timestamp.

6. Expected Output

- **RDP enablement and security configuration**

7. Error Handling

- **Access denied**
- **Registry or service query failure**

8. Security Considerations

- **RDP exposure must be tightly controlled**

9. Audit Logging Requirements

- **Operator ID**
- **Timestamp**

10. Organizational Benefit Statement

This procedure ensures visibility into remote-access readiness and security posture, supporting compliance and operational oversight.

SOP 2 – Enable RDP

1. Purpose

Enable Remote Desktop access on the system.

2. Scope

- **Windows servers and workstations**

3. Preconditions

- **Operator must have administrative rights**
- **Action must be authorized by security policy**

4. Required Inputs

- **Optional: Require Network Level Authentication (NLA)**

5. Procedure Steps

- **Input Collection**
- **Registry Update** – Enable RDP service.

- **NLA Configuration –** Apply NLA requirement if selected.
- **Firewall Configuration –** Enable RDP firewall rules.
- **Post-Enable Verification –** Confirm RDP is active.
- **Logging**

6. Expected Output

- **RDP successfully enabled**

7. Error Handling

- **Access denied**
- **Firewall rule failure**

8. Security Considerations

- **NLA is strongly recommended to prevent unauthorized access**

9. Audit Logging Requirements

- **Operator ID**
- **NLA setting**
- **Timestamp**

10. Organizational Benefit Statement

This procedure ensures RDP is enabled securely and consistently, supporting remote administration while maintaining compliance.

SOP 3 – Disable RDP

1. Purpose

Disable Remote Desktop access to harden security or meet compliance requirements.

2. Scope

- **Windows servers and workstations**

3. Preconditions

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

4. Required Inputs

- **None**

5. Procedure Steps

- **Registry Update –** Disable RDP service.
- **Firewall Configuration –** Disable RDP firewall rules.
- **Post-Disable Verification –** Confirm RDP is disabled.
- **Logging**

6. Expected Output

- **RDP successfully disabled**

7. Error Handling

- **Access denied**
- **Registry update failure**

8. Security Considerations

- **Disabling RDP may impact remote workflows**

9. Audit Logging Requirements

- **Operator ID**
- **Timestamp**

10. Organizational Benefit Statement

This procedure ensures RDP is disabled safely and with full accountability, reducing attack surface and supporting security compliance.

SOP 4 – Get RDP Session List

1. Purpose

Retrieve active RDP sessions for monitoring, troubleshooting, and security review.

2. Scope

- **Windows servers and workstations**
- **Local and remote sessions**

3. Preconditions

- **Operator must have permission to query session data**

4. Required Inputs

- **None**

5. Procedure Steps

- **Session Enumeration –** Retrieve active sessions.
- **Attribute Extraction –** Username, session ID, state, client IP.
- **Output Formatting**
- **Logging**

6. Expected Output

- **List of active RDP sessions**

7. Error Handling

- **Access denied**
- **Session service unavailable**

8. Security Considerations

- **Session data may reveal sensitive user activity**

9. Audit Logging Requirements

- **Operator ID**
- **Timestamp**

10. Organizational Benefit Statement

This procedure provides visibility into remote-access activity, supporting security monitoring and operational diagnostics.

SOP 5 – Disconnect RDP Session

1. Purpose

Disconnect an active RDP session safely.

2. Scope

- **Windows servers and workstations**

3. Preconditions

- **Operator must have administrative rights**
- **Session must exist**

4. Required Inputs

- **Session ID or username**

5. Procedure Steps

- **Input Collection**
- **Session Resolution**
- **Disconnection Operation**
- **Post-Disconnection Verification**
- **Logging**

6. Expected Output

- **Session successfully disconnected**

7. Error Handling

- **Session not found**
- **Access denied**

8. Security Considerations

- **Disconnecting sessions may interrupt user workflows**

9. Audit Logging Requirements

- **Operator ID**
- **Session identifier**
- **Timestamp**

10. Organizational Benefit Statement

This procedure ensures RDP sessions are terminated safely and with full accountability, supporting security and resource management.

SOP 6 – Test RDP Connectivity

1. Purpose

Test whether a remote system is reachable via RDP.

2. Scope

- **Windows servers and workstations**
- **IPv4 and IPv6**

3. Preconditions

- **Operator must have permission to test connectivity**

4. Required Inputs

- **Remote hostname or IP**

5. Procedure Steps

- **Input Collection**
- **Port Test –** Check TCP 3389 availability.
- **Firewall/Reachability Check**
- **Output Formatting**
- **Logging**

6. Expected Output

- **Connectivity status and diagnostic details**

7. Error Handling

- **Host unreachable**
- **Firewall blocking**

8. Security Considerations

- **Connectivity tests may reveal network topology**

9. Audit Logging Requirements

- **Operator ID**
- **Target host**

- **Timestamp**

10. Organizational Benefit Statement

This procedure provides a controlled, auditable method for validating RDP reachability, supporting troubleshooting and remote-access readiness.