CHECKLIST

Windows Server 2022 RDS Security Hardening Checklist

A practical vendor-neutral checklist for hardening Remote Desktop Services on Windows Server 2022, covering exposure, identity, transport, session controls, and validation before production rollout.

Windows Server 2022 Security Hardening for Remote Desktop Services

Purpose

Use this checklist to harden Remote Desktop Services (RDS) on Windows Server 2022 without breaking legitimate administration or remote access workflows. It focuses on reducing attack surface, tightening authentication, limiting session abuse, and verifying controls before production use.

Scope

- Windows Server 2022 hosts running Remote Desktop Services
- Direct RDP access, gateway-based access, or access through jump hosts
- Administrative and controlled end-user remote access scenarios

Pre-rollout decisions

Before changing settings, confirm:

- [ ] Which servers provide RDS access
- [ ] Which networks are allowed to reach RDS
- [ ] Which user groups are permitted to log on through RDS
- [ ] Whether MFA is enforced at a gateway, VPN, or identity layer
- [ ] Which redirection features are required for operations
- [ ] What timeout and lockout behavior is acceptable
- [ ] Who approves exceptions and emergency access

1) Exposure and network reachability

Reduce the number of places from which RDS can be reached.

- [ ] Inventory all RDS entry points
- [ ] Direct public exposure
- [ ] VPN access
- [ ] Bastion or jump host access
- [ ] Remote Desktop Gateway or other access broker
- [ ] Block direct internet exposure unless there is a documented, approved business requirement
- [ ] Restrict inbound RDP to approved source IP ranges or management subnets
- [ ] Place RDS behind a gateway or jump host where possible
- [ ] Verify firewall rules match the intended access path
- [ ] Remove stale rules for old office subnets, contractors, or temporary projects
- [ ] Confirm only required ports are open
- [ ] Document any exception with owner, reason, and expiry date

Validation checks

- [ ] Attempt connection from an unauthorized network and confirm it is blocked
- [ ] Confirm the approved network path is the only working route
- [ ] Review firewall logs for unexpected allowed sources

2) Identity and authorization

Only users who truly need interactive access should be able to log on through RDS.

- [ ] Review membership in the Remote Desktop Users group
- [ ] Remove any account that does not need interactive logon
- [ ] Limit local administrator membership to approved administrative accounts only
- [ ] Avoid using broad groups such as "Domain Users" for RDS logon rights
- [ ] Separate standard user access from privileged administration access
- [ ] Require MFA where supported by your access architecture
- [ ] Use named accounts instead of shared accounts
- [ ] Disable or remove stale, temporary, or emergency accounts after use
- [ ] Ensure service accounts cannot be used for interactive logon unless explicitly required

Validation checks

- [ ] Test logon with an approved standard user account
- [ ] Test logon with an approved admin account from an approved path
- [ ] Confirm unauthorized users are denied access
- [ ] Review denied logon events for unexpected account names

3) Authentication hardening

Strengthen authentication before a session is created.

- [ ] Enforce strong password policy for all interactive accounts
- [ ] Use multifactor authentication where supported
- [ ] Require Network Level Authentication (NLA) if the architecture supports it
- [ ] Avoid legacy authentication paths that create sessions before authentication completes
- [ ] Ensure account lockout policy is enabled and tuned appropriately
- [ ] Confirm privileged accounts use separate credentials from daily-use accounts
- [ ] Review whether smart cards, certificates, or passwordless methods are appropriate for your environment

Validation checks

- [ ] Verify NLA is enabled on the RDS host or collection
- [ ] Confirm clients are prompted for authentication before the full remote session starts
- [ ] Test lockout behavior in a controlled manner
- [ ] Review whether repeated failures are visible in security logs

4) Transport security and certificates

Make sure the connection uses trusted TLS configuration and does not rely on warnings that users may ignore.

- [ ] Use a certificate from a trusted internal or public CA as appropriate
- [ ] Confirm the certificate name matches the server name clients use
- [ ] Ensure clients trust the certificate chain
- [ ] Replace self-signed certificates with trusted certificates where possible
- [ ] Verify the certificate is bound to the correct RDS role or service
- [ ] Confirm TLS settings align with your organization?s security policy
- [ ] Remove or disable weak protocol and cipher options that are not approved
- [ ] Avoid training users to click through certificate warnings

Validation checks

- [ ] Connect from an approved client and confirm there are no certificate warnings
- [ ] Verify the certificate subject or SAN matches the connection name
- [ ] Confirm certificate renewal is tracked before expiration

5) Session redirection and client device features

Disable features that move data between client and server unless they are truly needed.

- [ ] Review whether clipboard redirection is required
- [ ] Review whether drive redirection is required
- [ ] Review whether printer redirection is required
- [ ] Review whether device redirection is required
- [ ] Review whether audio, COM port, or other specialized redirection is needed
- [ ] Disable clipboard redirection unless there is a documented use case
- [ ] Disable drive redirection unless file transfer is operationally required
- [ ] Disable printer redirection unless printing from RDS is necessary
- [ ] Disable device redirection by default and allow only approved exceptions
- [ ] Scope redirection settings to the smallest necessary user groups or host collections

Validation checks

- [ ] Confirm disabled redirection features are not available in the client session
- [ ] Confirm approved redirection still works for documented workflows
- [ ] Test file transfer, copy/paste, and printing behavior against policy expectations

6) Session lifetime and disconnect behavior

Limit how long a session can stay active or idle.

- [ ] Set idle timeout values appropriate to your support model
- [ ] Define disconnected session limits
- [ ] Set a logoff policy for disconnected sessions if required
- [ ] Confirm administrators understand timeout behavior before rollout
- [ ] Review whether long-running maintenance tasks need exceptions
- [ ] Ensure timeout settings align with compliance and operational requirements

Validation checks

- [ ] Leave a session idle and confirm it times out as expected
- [ ] Disconnect a session and verify it behaves according to policy
- [ ] Confirm timeouts do not break critical maintenance procedures

7) Logging and monitoring

Make denial, failure, and unexpected behavior visible.

- [ ] Ensure successful and failed logon events are recorded
- [ ] Enable and review relevant security and RDS logs
- [ ] Monitor repeated failed logons from the same source or account
- [ ] Review denied access attempts for unauthorized source networks
- [ ] Watch for unexpected redirection use or policy changes
- [ ] Forward logs to your central logging or SIEM platform if available
- [ ] Set alerts for unusual login volume, failed authentication spikes, or new source locations

Validation checks

- [ ] Generate a failed logon and verify it appears in logs
- [ ] Generate a denied source connection and verify it appears in logs
- [ ] Confirm log forwarding and alerting are working

8) Privilege and administrative hygiene

Reduce the impact if an RDS session is compromised.

- [ ] Separate daily-use accounts from administrative accounts
- [ ] Use least privilege for RDS administration tasks
- [ ] Limit local administrator rights on session hosts
- [ ] Restrict access to management tools and administrative shares
- [ ] Remove unnecessary software that increases attack surface
- [ ] Keep the server patched and rebooted according to maintenance policy
- [ ] Apply complementary protections such as BitLocker where appropriate for the host role

Validation checks

- [ ] Confirm admin tasks cannot be performed with standard user access
- [ ] Review local group membership on the host
- [ ] Verify patch and reboot cadence is documented and followed

9) Change control and exception handling

Treat every change as a security decision.

- [ ] Document the baseline configuration before hardening
- [ ] Record each setting changed, the reason, and the owner
- [ ] Track exceptions separately from standard policy
- [ ] Assign expiry dates to temporary access or feature exceptions

- [ ] Reassess changes after certificate renewal, firewall updates, gateway changes, or group membership changes
- [ ] Revalidate the configuration after major platform or role updates

Validation checks

- [ ] Confirm the approved baseline can be recreated from documentation
- [ ] Verify exceptions are reviewed on a regular schedule
- [ ] Confirm rollback steps are available if a change causes outages

Production readiness checklist

Use this final list before enabling or expanding production access.

- [ ] RDS is reachable only from approved networks or via approved gateways
- [ ] Only approved users and admin accounts can log on through RDS
- [ ] NLA is enabled where supported
- [ ] TLS certificate trust and naming are validated
- [ ] Clipboard, drive, printer, and device redirection are limited to documented needs
- [ ] Session timeout and disconnect behavior match policy
- [ ] Logging and alerting are active
- [ ] Emergency access is documented and controlled
- [ ] Exceptions have owners and expiry dates
- [ ] A rollback plan exists and has been reviewed

Quick decision guide

Use these questions to decide whether a control belongs in your environment:

- [ ] Does this control reduce exposure or limit compromise impact?

- [ ] Is the feature required for a documented business process?
- [ ] Can the control be validated before rollout?
- [ ] Will the support team know how the behavior should look after the change?
- [ ] Is there a clear owner for exceptions?

If the answer to the first question is yes and the second is no, the control should usually be enabled. If the feature is required, scope it narrowly and monitor it.

Post-change verification summary

After rollout, confirm:

- [ ] Approved users can connect successfully
- [ ] Unauthorized users and networks are blocked
- [ ] Certificate warnings are absent
- [ ] Required redirection works; unneeded redirection does not
- [ ] Session limits behave as expected
- [ ] Logs show both allowed and denied activity
- [ ] Support staff know how to troubleshoot the new baseline

Notes

- Harden RDS in layers rather than relying on a single setting.
- Prioritize exposure reduction, identity controls, NLA, and certificate validation first.
- Revisit the checklist after firewall, gateway, certificate, group membership, or session host changes.
- Keep the deployment boring: only approved clients, only approved users, only approved features.