Allow log on through Remote Desktop Services - Windows 10

By vinaypamnani-msft

Archived: 2026-04-06 01:52:53 UTC

Applies to

- Windows 11
- Windows 10

Describes the best practices, location, values, policy management, and security considerations for the **Allow log on through Remote Desktop Services** security policy setting.

This policy setting determines which users or groups can access the sign-in screen of a remote device through a Remote Desktop Services connection. It's possible for a user to establish a Remote Desktop Services connection to a particular server but not be able to sign in to the console of that same server.

Constant: SeRemoteInteractiveLogonRight

- User-defined list of accounts
- Not Defined

- To control who can open a Remote Desktop Services connection and sign in to the device, add users to or remove users from the Remote Desktop Users group.

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

By default, members of the Administrators group have this right on domain controllers, workstations, and servers. The Remote Desktops Users group also has this right on workstations and servers. The following table lists the actual and effective default policy values. Default values are also listed on the policy's property page.

Server type or GPO	Default value
Default Domain Policy	Not Defined
Default Domain Controller Policy	Not Defined
Domain Controller Local Security Policy	Administrators
Stand-Alone Server Default Settings	Administrators Remote Desktop Users
Domain Controller Effective Default Settings	Administrators
Member Server Effective Default Settings	Administrators Remote Desktop Users

Server type or GPO	Default value
Client Computer Effective Default Settings	Administrators Remote Desktop Users

This section describes different features and tools available to help you manage this policy.

To use Remote Desktop Services to successfully sign in to a remote device, the user or group must be a member of the Remote Desktop Users or Administrators group and be granted the **Allow log on through Remote Desktop Services** right. It's possible for a user to establish a Remote Desktop Services session to a particular server, but not be able to sign in to the console of that same server.

To exclude users or groups, you can assign the **Deny log on through Remote Desktop Services** user right to those users or groups. However, be careful when you use this method because you could create conflicts for legitimate users or groups that have been allowed access through the **Allow log on through Remote Desktop Services** user right.

For more information, see Deny log on through Remote Desktop Services.

A restart of the device isn't required for this policy setting to be effective.

Any change to the user rights assignment for an account becomes effective the next time the owner of the account logs on.

Group Policy settings are applied through GPOs in the following order, which will overwrite settings on the local computer at the next Group Policy update:

1. Local policy settings
2. Site policy settings
3. Domain policy settings
4. OU policy settings

This section describes how an attacker might exploit a feature or its configuration, how to implement the countermeasure, and the possible negative consequences of countermeasure implementation.

Any account with the **Allow log on through Remote Desktop Services** user right can sign in to the remote console of the device. If you don't restrict this user right to legitimate users who must sign in to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

For domain controllers, assign the **Allow log on through Remote Desktop Services** user right only to the Administrators group. For other server roles and devices, add the Remote Desktop Users group. For servers that have the Remote Desktop (RD) Session Host role service enabled and don't run in Application Server mode, ensure that only authorized IT personnel who must manage the computers remotely belong to these groups.

> **Caution:** For RD Session Host servers that run in Application Server mode, ensure that only users who require access to the server have accounts that belong to the Remote Desktop Users group because this built-in group has this logon right by default.

Alternatively, you can assign the **Deny log on through Remote Desktop Services** user right to groups such as Account Operators, Server Operators, and Guests. However, be careful when you use this method because you could block access to legitimate administrators who also belong to a group that has the **Deny log on through Remote Desktop Services** user right.

Removal of the **Allow log on through Remote Desktop Services** user right from other groups (or membership changes in these default groups) could limit the abilities of users who perform specific administrative roles in your environment. You should confirm that delegated activities aren't adversely affected.

- User Rights Assignment
