mstsc

Article • 02/03/2023 • 11 contributors   👍 Feedback

In this article

Syntax

Related links

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Creates connections to Remote Desktop Session Host servers or other remote computers and edits an existing Remote Desktop Connection (.rdp) configuration file.

Syntax

```
mstsc.exe [<connectionfile>] [/v:<server>[:<port>]] [/g:<gat
mstsc.exe /edit <connectionfile>
```

Parameters

⛶ **Expand table**

Parameter	Description
`<connectionfile>`	Specifies the name of an **.rdp** file for the connection.
/v:`<server>[:<port>]`	Specifies the remote computer and, optionally, the port number to which you want to connect.
/g:`<gateway>`	Specifies the RD Gateway server to use for the connection. This parameter is only read if the endpoint PC is specified with **/v**.
/admin	Connects you to a session for administering the server.
/f	Starts Remote Desktop Connection in full-screen mode.
/w:`<width>`	Specifies the width of the Remote Desktop window.
/h:`<height>`	Specifies the height of the Remote Desktop window.
/public	Runs Remote Desktop in public mode. In public mode, passwords and bitmaps aren't cached.
/multimon	Configures the Remote Desktop Services session monitor layout to be identical to the current client-side configuration.
/l	Enumerates the monitor attached to the local PC and the ID associated with each monitor. The monitor ID can be used to populate the selected monitors RDP file setting.
/edit `<connectionfile>`	Opens the specified **.rdp** file for editing.

/restrictedAdmin	This mode won't send your credentials to the remote PC, which can protect you if you connect to a compromised device. Connections made from the remote PC might not be authenticated by other PCs, which impact application functionality and compatibility. The **/admin** parameter is implied.
/remoteGuard	This mode prevents credentials from being sent to the remote PC, which can help protect your credentials if you connect to a compromised device. Unlike Restricted Administrator mode, Remote Guard also supports connections made from the remote PC by redirecting all requests back to your device.
/prompt	Prompts you for your credentials when you connect to the remote PC.
/shadow:`<sessionID>`	Specifies the ID of the session to shadow.
/control	Allows control of the session when shadowing.
/noConsentPrompt	Allows shadowing without user consent.
/?	Displays help at the command prompt.

Remarks

- Default.rdp is stored for each user as a hidden file in the user's **Documents** folder.

- User created **.rdp** files are saved by default in the user's **Documents** folder, but can be saved anywhere.

- To span across monitors, the monitors must use the same resolution and must be aligned horizontally (that is, side-by-side). There's currently no support for spanning multiple monitors vertically on the client system.

Examples

To connect to a session in full-screen mode, type:

```
mstsc /f
```

or

```
mstsc /v:computer1 /f
```

To assign width/height, type:

```
mstsc /v:computer1 /w:1920 /h:1080
```

To open a file called *filename.rdp* for editing, type:

```
mstsc /edit filename.rdp
```

Related links

- Command-Line Syntax Key

Feedback

Was this page helpful?   👍 Yes   👎 No

🌐 English (United States)   ☑☒ Your Privacy Choices   ☼ Theme ⌄

Manage cookies   Previous Versions   Blog ↗   Contribute   Privacy ↗   Terms of Use   Trademarks ↗

© Microsoft 2024