Remote Service Platform

Safety Notice

MIRSP-2026-0001

Advisory ID:	MIRSP-2026-0001
Publish Date:	2026-04-28
Last Updated:	2026-11-14
Revision:	1.1

Summary

Remote Service Platform is using Remote Desktop which lets you connect to high secure Mitel Remote Service Platform via Internet, managing and maintaining customer infrastructure.

Since the Windows security update of April 2026, Microsoft has significantly tightened warnings to prevent phishing attacks.

Every time you open an RDP file, a security dialog appears before any connection is made. It shows the remote computer address and a check box for each local resource the file wants to access.

What the message means

- Verified publisher: If a name is displayed, the RDP file has been digitally signed. This confirms that the file originates from the named organization and has not been modified since it was signed.

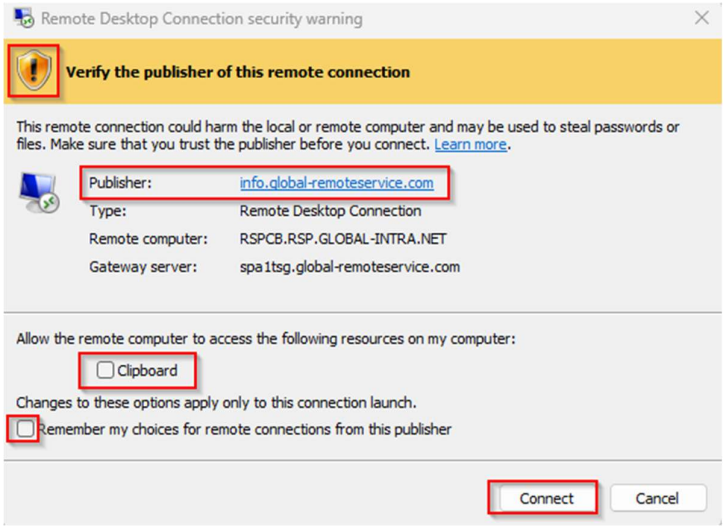
- Unknown publisher: The file is not signed. In this case, Windows cannot verify the origin. This is common with internal or user-created files but poses a security risk if the file comes from an unknown source (e.g., an email attachment).

Mitigations / Workarounds

Mitel Remote Service Platform is always using certified connections only, therefore a “verified publisher” message appears.

To verify the publisher of a remote connection (RDP file), check the digital signature in the warning prompt. A trusted connection displays a valid publisher name; if it says, "Unknown publisher," it is unsigned and potentially insecure. Ensure the signature comes from a trusted entity and hasn't been revoked.

Remote Service Platform is using the presented publisher FQDN (below) which can be trusted.



To avoid recuring message, we recommend selecting the boxes and proceed with “connect”

> **Clipboard: What it does:** Shares the contents of your clipboard (anything you copy and paste) between your device and the remote computer.

Solution/ Recommended Action

To verify the publisher of a remote connection (RDP) file, check the digital signature in the warning dialog or review the **SHA1 thumbprint** of the certificate via Group Policy (gpedit.msc), as well as push the GPO to affected user clients.

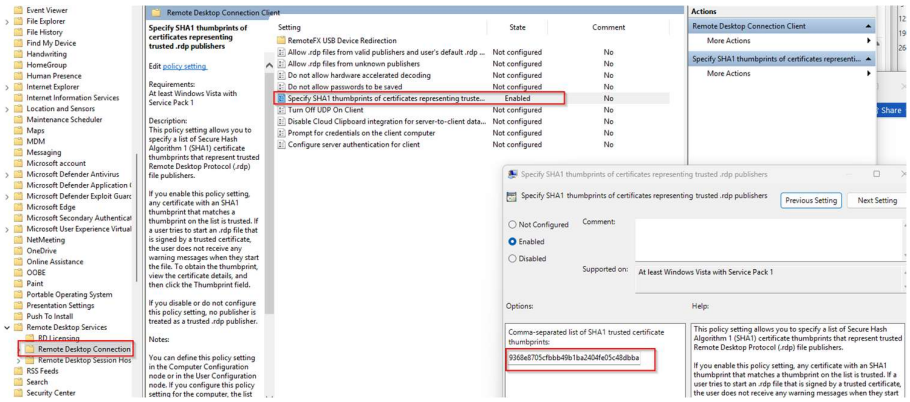
Steps to Verify or Fix Warnings for Remote Service Platform:

- Configure Trusted Publishers: Use Group Policy to import the SHA1 thumbprint of the certificate you trust. Navigate to *Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Connection Client* to add the certificate thumbprint.
- Audit Settings: If an RDP file is not digitally signed or does not match with issued GPO thumbprint, Windows displays a caution dialog listing the destination system again.

Add the following actual Remote Service Platform Certificate thumbprint:

54046a7a848150bf681aec363c6729a2de484f28

Note: the thumbprint must be replaced in case of revoked or updated Certificate as well.



Mitel Copyrights and Trademarks

COPYRIGHTS

All materials appearing anywhere on mitel.com or its subsidiaries' Internet sites are protected by worldwide copyright laws and treaty provisions. The copyright on such materials is held by Mitel Networks Corporation or its subsidiaries (collectively "Mitel"), or by the original creator of the materials. None of the materials may be copied, reproduced, displayed, modified, published, uploaded, posted, transmitted or distributed in any form or by any means other than with Mitel's prior written permission. All rights not expressly granted herein are reserved. Any unauthorized use of the materials appearing on Mitel's Internet sites may violate copyright, trademark and other applicable laws and could result in criminal or civil penalties. The copyrighted materials include all PDF material available for view and download, but this material is not available for reproduction or distribution.

TRADEMARKS

The trademarks, service marks, logos and graphics (the "Trademarks") appearing on Mitel's Internet sites are registered and unregistered trademarks of Mitel Networks Corporation or its subsidiaries (collectively "Mitel") or others. Other product names (not owned by Mitel) used in on this site are used with the permission of the trademark owner or for identification purposes only, and Mitel claims no rights in these trademarks. No license or right is granted by implication or any other means to use any trademark appearing on Mitel's Internet sites. If you have any questions about the use of Mitel's trademarks, or any other trademarks appearing on this site, please contact our legal department at 613-592-2122. Mitel vigilantly enforces its intellectual property rights and will actively seek the recovery of any costs and damages it may incur preventing the misuse or misappropriation of its property. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at iplegal@mitel.com for additional information.