Remote Desktop Services: Enable Restricted Admin mode

Article • 01/17/2024

In this article

Summary

This step-by-step article describes how to enable RestrictedAdmin mode for Remote Desktop. RestrictedAdmin mode prevents the transmission of reusable credentials to the remote system to which you connect using Remote Desktop. This prevents your credentials from being harvested during the initial connection process if the remote server has been compromised.

NOTE:

RestrictedAdmin mode must be explicitly enabled on the destination systems using the Registry setting below, and the account being used to connect must be a member of the local Administrators group on the destination system.

Steps

To enable destination systems to receive incoming Remote Desktop connections using RestrictedAdmin mode:

1. Open Registry Editor: click **Start**, click **Run**, type **regedit**, and then click OK.
2. In Registry Editor, create the following registry key:

   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

   Name: **DisableRestrictedAdmin**

   Type: **REG_DWORD**

   Value: **0** (This will enable RestrictedAdmin mode so that the destination system will accept incoming RestrictedAdmin-enabled connections)
3. This setting takes effect immediately; no reboot is required.

To disable RestrictedAdmin mode, set the value of **DisableRestrictedAdmin** to 1.

Use Remote Desktop in RestrictedAdmin mode

To use Remote Desktop in RestrictedAdmin mode, open a command prompt and enter the following text:`Mstsc.exe /RestrictedAdmin`

NOTE:

In order to use the RestrictedAdmin switch, the initiating system must have the appropriate update installed. For details on the required updates, please refer to the article, "Microsoft Security Advisory 2871997" (https://technet.microsoft.com/en-us/library/security/2871997.aspx). In addition, as mentioned above, the account being used to connect must be a member of the local Administrators group on the destination system.

The /RestrictedAdmin switch can be combined with other switches. For example, the following command would connect to Server01 on TCP port 3390 using the RestrictedAdmin switch:

```
Mstsc.exe /V:Server01:3390 /RestrictedAdmin
```

To require all outbound Remote Desktop requests to use RestrictedAdmin mode:

1. Open Group Policy Management Console: click **Start**, click **Run**, type **gpmc.msc**, and then click OK.
2. Select the group policy which best applies to the systems from which you will initiate Remote Desktop connections.
3. Edit the Group Policy and navigate to the following node:

   Computer Configuration\Policies\Administrative Templates\System\Credentials Delegation

4. Configure the value of “Restrict delegation of credentials to remote servers” to **Enabled**.

5. This setting will take effect when Group Policy refreshes. To immediately refresh group policy, open an elevated command prompt and enter the following text:

```
Gpupdate.exe /target:computer /force
```

To disable RestrictedAdmin mode, configure the above group policy setting to Disabled.

Once group policy has refreshed, you will only be able to issue Remote Desktop connections using RestrictedAdmin mode. No reboot is required.

NOTE:

The Group Policy setting above will force all Remote Desktop connections to use RestrictedAdmin mode. This means that all destination systems must have RestrictedAdmin mode enabled or the Remote Desktop connection request will fail.

Applies to

Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows RT