Prerequisites

07/10/20192 minutes to read

In this article

Check which version of PowerShell is installed

Enable PowerShell Remoting

Enable PowerShell module and script block logging (optional)

Next steps

See also

Just Enough Administration is a feature included in PowerShell 5.0 and higher. This article describes the prerequisites that must be satisfied to start using JEA.

Check which version of PowerShell is installed

To check which version of PowerShell is installed on your system, check the `$PSVersionTable` variable in a Windows PowerShell prompt.

PowerShell

Copy

```
$PSVersionTable.PSVersion
```

Output

Copy

```
Major  Minor  Build  Revision
-----  -----  -----  --------
5      1      14393  1000
```

JEA is available with PowerShell 5.0 and higher. For full functionality, it's recommended that you install the latest version of PowerShell available for your system. The following table describes JEA's availability on Windows Server:

Server Operating System	JEA Availability
Windows Server 2016+	Preinstalled
Windows Server 2012 R2	Full functionality with WMF 5.1
Windows Server 2012	Full functionality with WMF 5.1
Windows Server 2008 R2	Reduced functionality[1] with WMF 5.1

You can also use JEA on your home or work computer:

Client Operating System	JEA Availability
Windows 10 1607+	Preinstalled

Client Operating System	JEA Availability
Windows 10 1603, 1511	Preinstalled, with reduced functionality[2]
Windows 10 1507	Not available
Windows 8, 8.1	Full functionality with WMF 5.1
Windows 7	Reduced functionality[1] with WMF 5.1

- [1] JEA can't be configured to use group-managed service accounts on Windows Server 2008 R2 or Windows 7. Virtual accounts and other JEA features *are* supported.
- [2] The following JEA features aren't supported on Windows 10 versions 1511 and 1603:
  - Running as a group-managed service account
  - Conditional access rules in session configurations
  - The user drive
  - Granting access to local user accounts

  To get support for these features, update Windows to version 1607 (Anniversary Update) or higher.

Install Windows Management Framework

If you're running an older version of PowerShell, you may need to update your system with the latest Windows Management Framework (WMF) update. For more information, see the WMF documentation.

It's recommended that you test your workload's compatibility with WMF before upgrading all of your servers.

Windows 10 users should install the latest feature updates to obtain the current version of Windows PowerShell.

Enable PowerShell Remoting

PowerShell Remoting provides the foundation on which JEA is built. It's necessary to ensure PowerShell Remoting is enabled and properly secured before you can use JEA. For more information, see WinRM Security.

PowerShell Remoting is enabled by default on Windows Server 2012, 2012 R2, and 2016. You can enable PowerShell Remoting by running the following command in an elevated PowerShell window.

PowerShell

Copy

```
Enable-PSRemoting
```

Enable PowerShell module and script block logging (optional)

The following steps enable logging for all PowerShell actions on your system. PowerShell Module Logging isn't required for JEA, however it's recommended you turn on logging to ensure the commands users run are logged in a central location.

You can configure the PowerShell Module Logging policy using Group Policy.

1. Open the Local Group Policy Editor on a workstation or a Group Policy Object in the Group Policy Management Console on an Active Directory Domain Controller
2. Navigate to **Computer Configuration\Administrative Templates\Windows Components\Windows PowerShell**
3. Double-click on **Turn on Module Logging**
4. Click **Enabled**
5. In the Options section, click on **Show** next to Module Names
6. Type `*` in the pop-up window to log commands from all modules.
7. Click **OK** to set the policy
8. Double-click on **Turn on PowerShell Script Block Logging**
9. Click **Enabled**
10. Click **OK** to set the policy
11. (On domain-joined machines only) Run `gpupdate` or wait for Group Policy to process the updated policy and apply the settings

You can also enable system-wide PowerShell transcription through Group Policy.