How to Enable PowerShell Scripting on Managed Devices

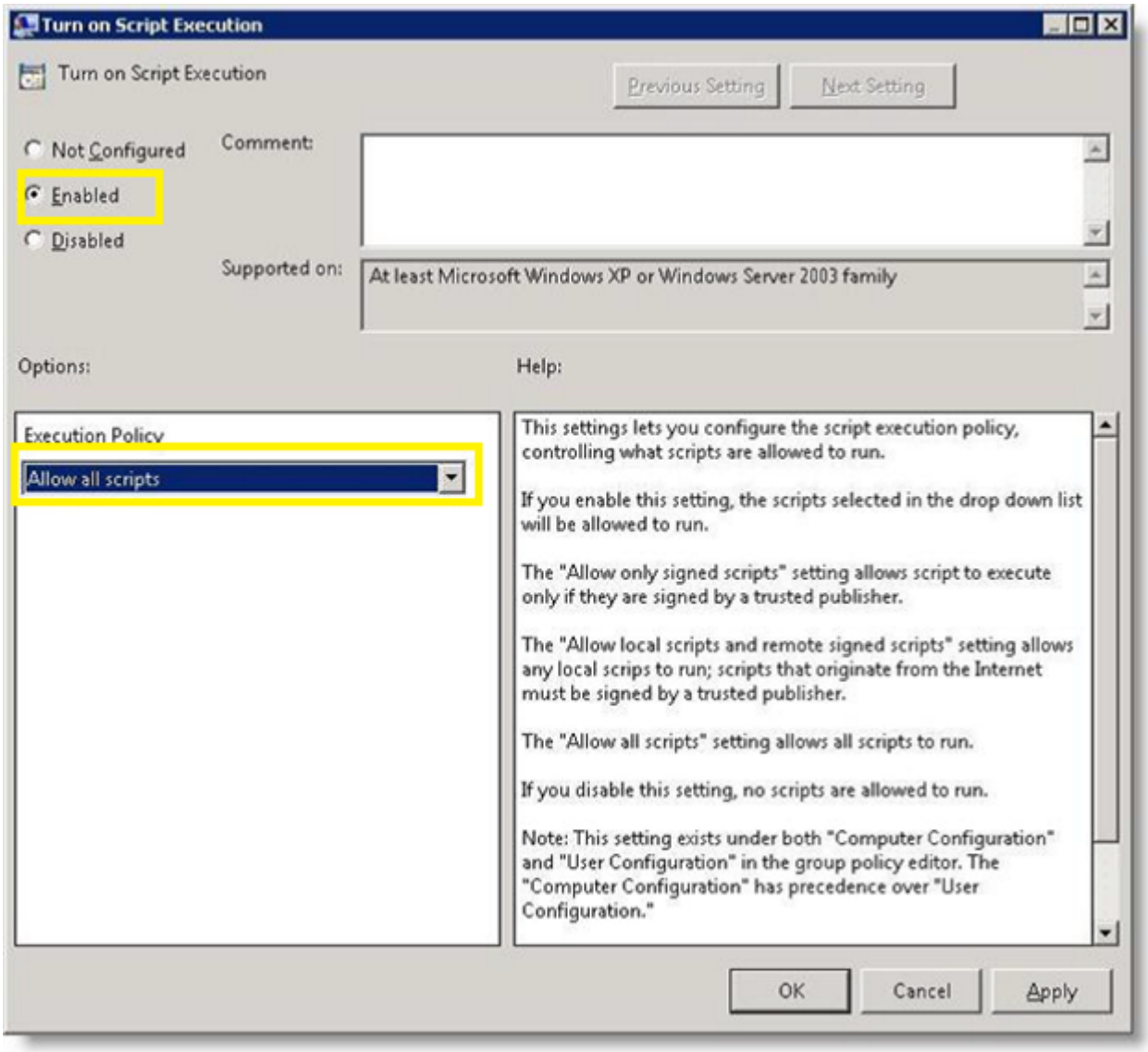
https://campus.barracuda.com/doc/98217178/

If you plan to use PowerShell scripts with Barracuda RMM automation, you must ensure that the managed devices can execute them. This article outlines how to configure this execution through group policy or locally on each device.

Configuration Using Group Policy Edit section

To configure the execution using group policy, follow the steps below:

1. Launch the **Group Policy Management Editor** for the Domain.
2. Browse to **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Windows PowerShell**.
3. Double-click **Turn on Script Execution**.
4. Choose **Enabled**.
5. Under **Options**, choose **Allow all scripts as the Execution Policy**.



6. Select OK.

Local Configuration

To configure locally, please follow the steps below:

1. From a command prompt, enter PowerShell by issuing the command `powershell`
2. Determine the execution policy by issuing the command `get-executionpolicy`
3. The system will respond, advising whether the policy is **Restricted (Default)** or **Unrestricted**.
4. To change **Unrestricted**, issue the command `set-executionpolicy unrestricted`

Figures

1. clipboard_eceb506384cddd7511e098b50330d2a23.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.