



NotifyMDM

Mobile Device Management

PowerShell Configuration Guide

Table of Contents

Windows PowerShell	2
Prerequisites	3
IIS Settings.....	3
ActiveSync Server PowerShell Connection Settings.....	8

Windows PowerShell

Using PowerShell with *NotifyMDM*

When an organization chooses not to proxy email through the *NotifyMDM* server, devices will be able to connect directly to the ActiveSync server to access mail without the requirement of MDM enrollment. As a means of enforcing enrollment, administrators can configure ActiveSync PowerShell settings and employ its capabilities via the *NotifyMDM* dashboard to import device and user information from the ActiveSync server. Once devices are imported they can be managed from the dashboard and administrators can monitor who has enrolled with MDM and who has not. The administrator can set a grace period during which devices must enroll in order to access email. Once the grace period ends, non-compliant devices will be restricted from accessing email.

The PowerShell integration enables *NotifyMDM* to:

- Poll the Exchange ActiveSync server at regular intervals for device and user information and import it to the MDM server. Additions and deletions made on the ActiveSync server are synchronized to MDM.
- Monitor who has not yet enrolled with the *NotifyMDM* server by viewing the Discovered Devices grid.
- Enforce *NotifyMDM* enrollment of auto-discovered devices accessing email by setting a quarantine date on which unenrolled devices will be blocked from accessing email. Once a device is enrolled the quarantine is lifted and the device can again access email.
- Email users when they are nearing the quarantine date. Each device a user has not yet enrolled will receive an email message.

Information on Configuring a PowerShell Server

The following links provide information on PowerShell Server setup and configuration.

Using PowerShell with Exchange 2016

[https://technet.microsoft.com/en-us/library/bb123778\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/bb123778(v=exchg.160).aspx)

Using PowerShell with Exchange 2013

[https://technet.microsoft.com/en-us/library/bb123778\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/bb123778(v=exchg.150).aspx)

Exchange Online PowerShell

[https://technet.microsoft.com/en-us/library/jj200677\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/jj200677(v=exchg.150).aspx)

PowerShell for Office 365

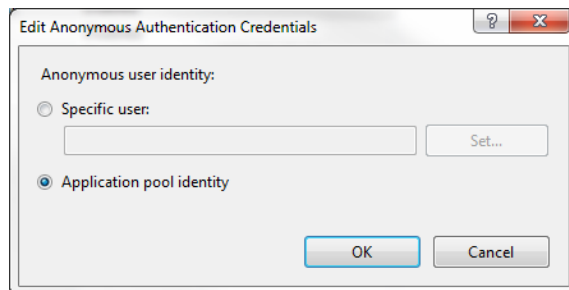
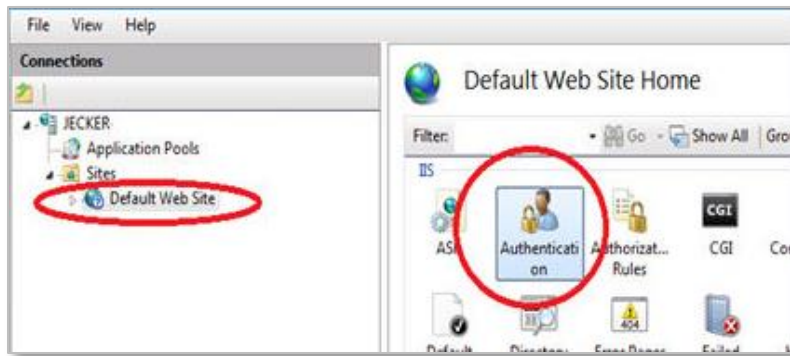
<http://powershell.office.com/>

Prerequisites

- Install Microsoft .NET Framework 4.0 on the server where the *NotifyMDM* Web/HTTP component is installed.
- Use Internet Information Services (IIS) to configure the *NotifyMDM* server to integrate with PowerShell. [here](#)
- Use the *NotifyMDM* dashboard to configure PowerShell connection settings for the ActiveSync server. [here](#)

IIS Settings

1. On the MDM server - Using IIS, configure the server for Anonymous Authentication.
 - Default Web Site > Authentication > Anonymous Authentication.**
 - Select **Edit . . .** from the panel to the right.
 - Select the radio button next to **Application pool identity.**

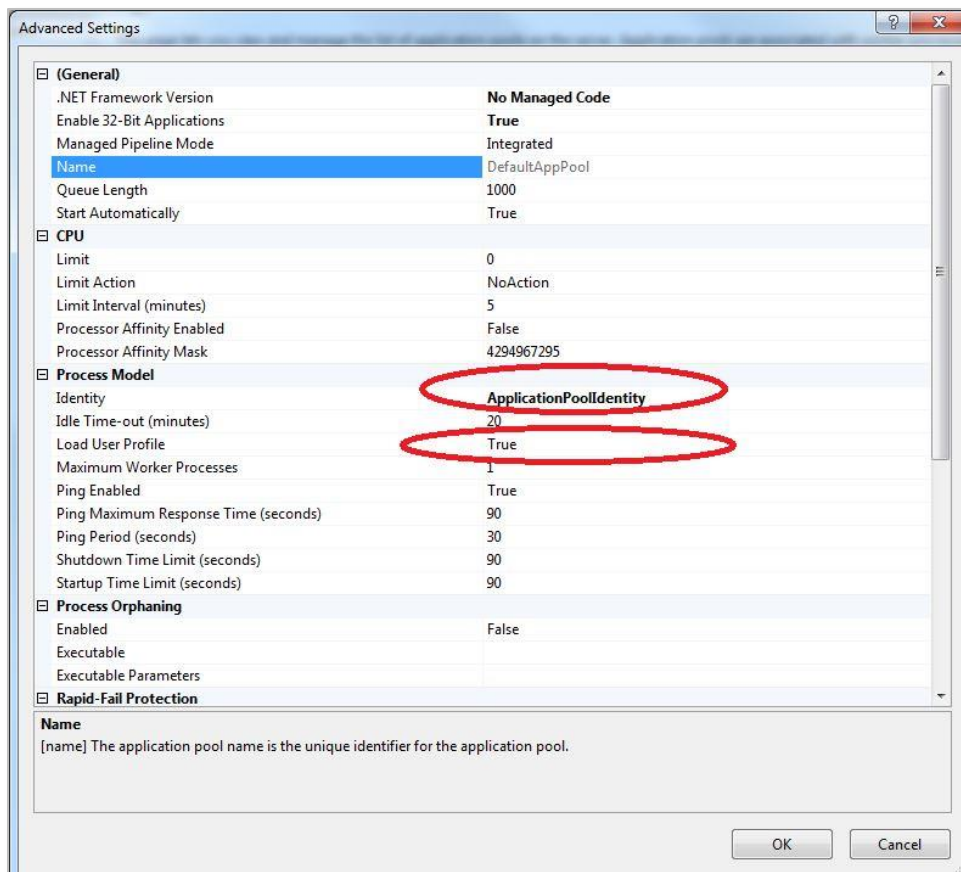
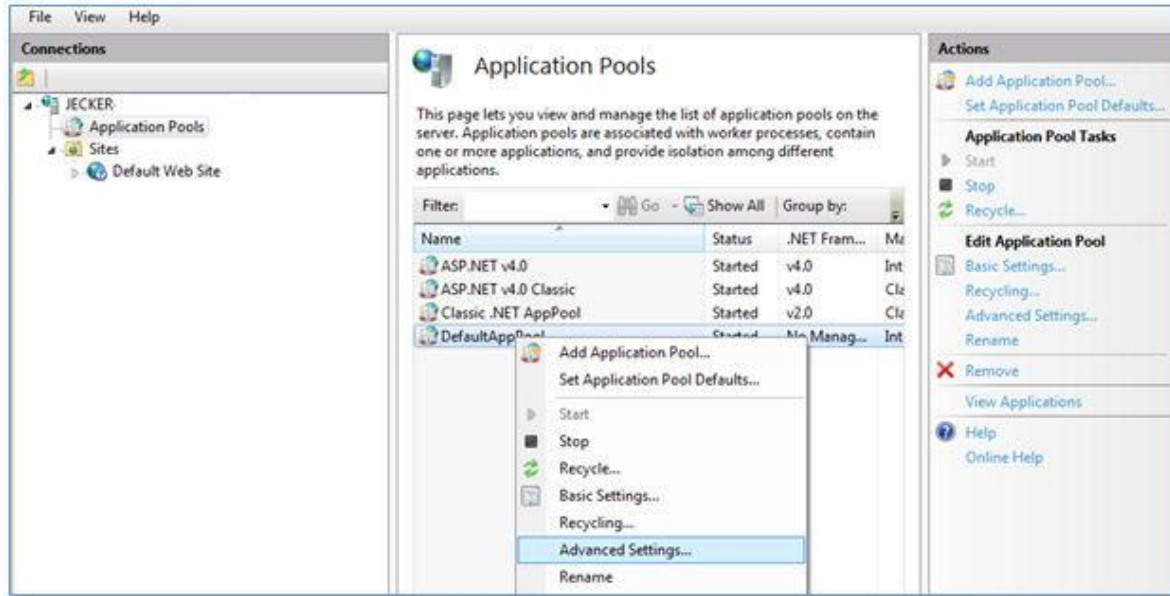


2. On the MDM server - Using IIS, set the application pool user as follows.

-**Application Pools > DefaultAppPool > Advanced Settings . . .**

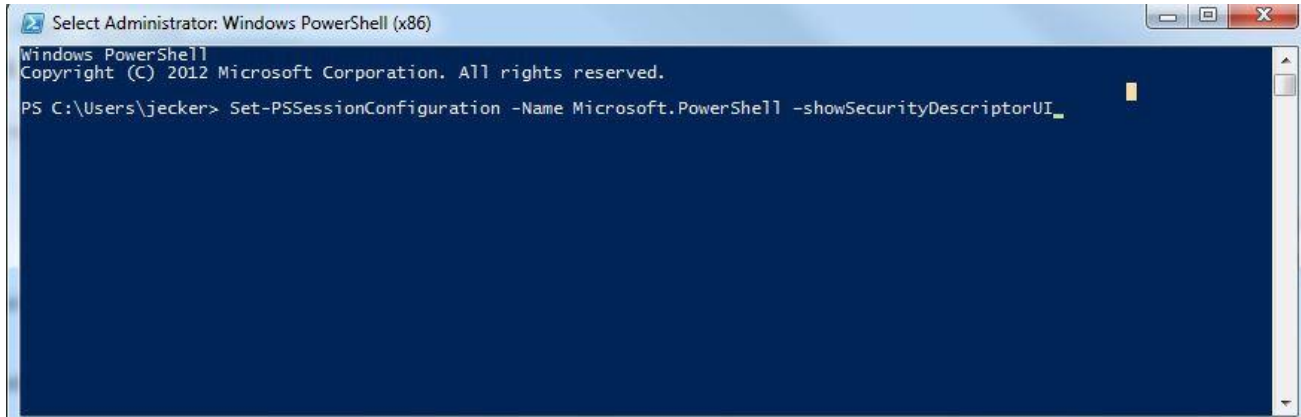
-Click the icon next to **Identity** and select **ApplicationPoolIdentity**.

-Verify that **Load User Profile** is set to **True**.



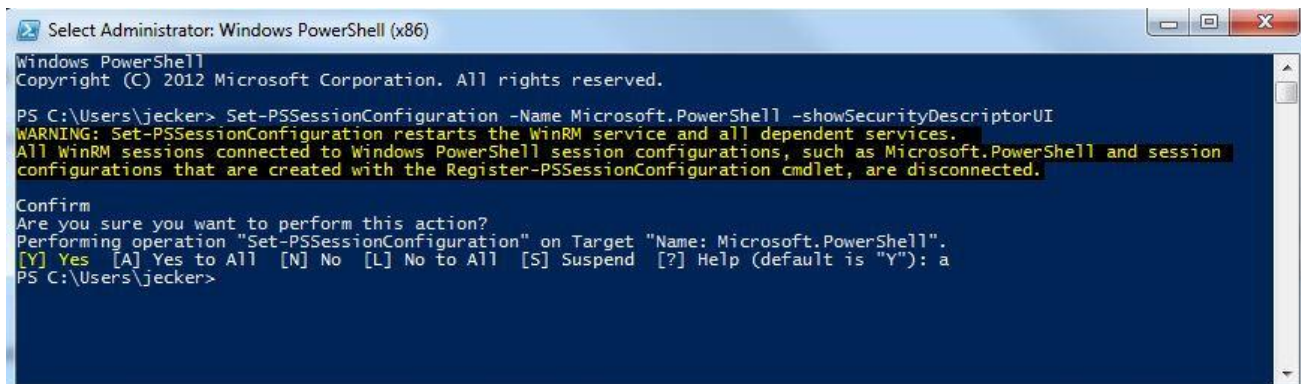
- The application pool identity needs to be granted executive privileges for the PowerShell process. Change permissions by remoting into the web system, opening the PowerShell app on the web server, and running this command:

```
Set-PSSessionConfiguration -Name Microsoft.PowerShell -showSecurityDescriptorUI
```



```
Select Administrator: Windows PowerShell (x86)
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\jecker> Set-PSSessionConfiguration -Name Microsoft.PowerShell -showSecurityDescriptorUI_
```

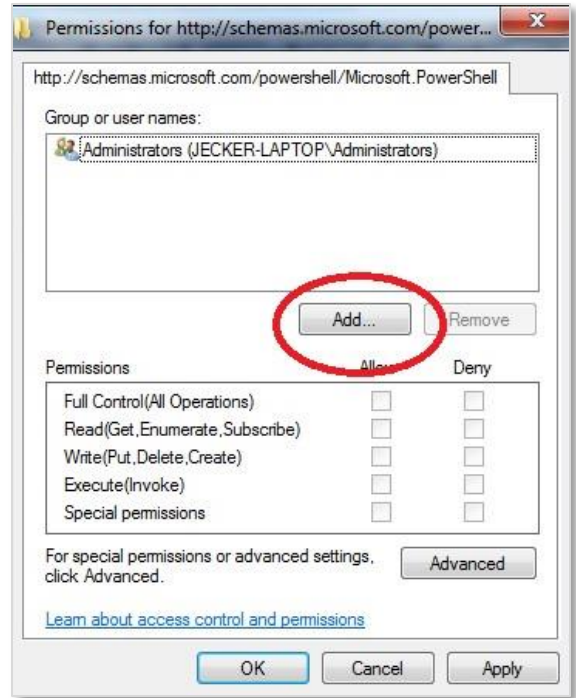


```
Select Administrator: Windows PowerShell (x86)
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

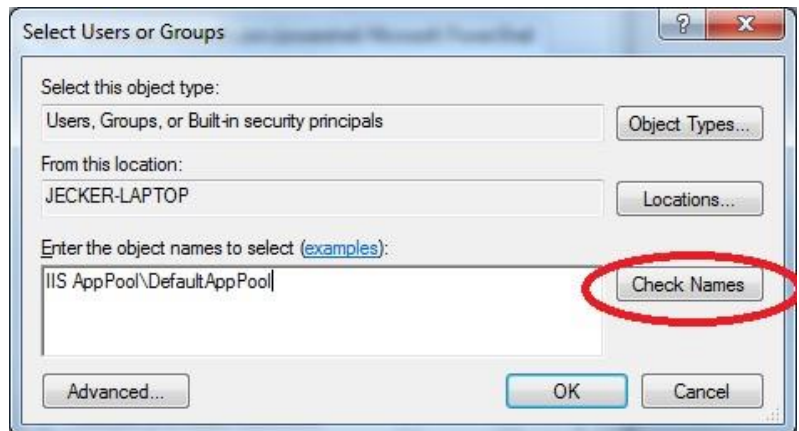
PS C:\Users\jecker> Set-PSSessionConfiguration -Name Microsoft.PowerShell -showSecurityDescriptorUI
WARNING: Set-PSSessionConfiguration restarts the WinRM service and all dependent services.
All WinRM sessions connected to Windows PowerShell session configurations, such as Microsoft.PowerShell and session
configurations that are created with the Register-PSSessionConfiguration cmdlet, are disconnected.

Confirm
Are you sure you want to perform this action?
Performing operation "Set-PSSessionConfiguration" on Target "Name: Microsoft.PowerShell".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): a
PS C:\Users\jecker>
```

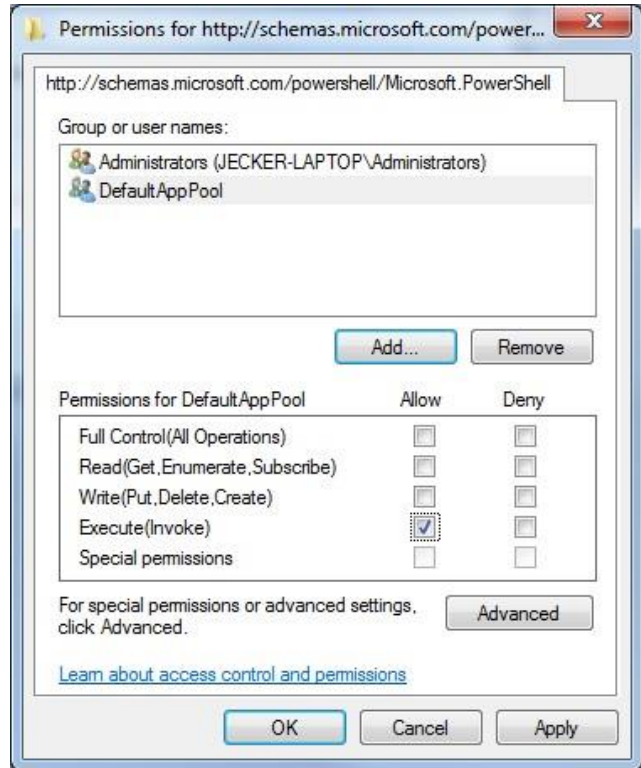
After you accept the confirmation in PowerShell, a permissions dialog opens. Add the user for your app pool here.



The username will be "IIS AppPool\Check name and click **OK** when it finds your user.



Set permissions to allow **Execute**.
Click **OK** to save the change and close the window.



Pay attention to PowerShell. It may ask you to confirm that you want to save the setting changes that you made. Answer **yes** to everything.

4. Restart IIS.

ActiveSync Server PowerShell Connection Settings

Configure PowerShell Settings on the MDM Server:

1. From the *NotifyMDM* administrative dashboard, select **Organization Management > Administrative Servers > ActiveSync Servers**.
2. Select an existing ActiveSync server from the left panel or add one by clicking *Add ActiveSync Server*.
3. Expand the **PowerShell Connections Settings** section and mark the **Enable PowerShell** checkbox.

The screenshot shows the 'ActiveSync Servers' configuration page. Under the 'PowerShell Connection Settings' section, the following options are visible:

- Enable PowerShell:**
- PowerShell Server Address:** 192.168.21.4
- Use SSL:**
- Authentication Type:** Basic (dropdown menu)
- Admin Username:** ex07\administrator
- Admin Password:** Change Password (button)
- Refresh Interval (hours):** 1 (spinner)
- Connect Now:** (button)
- Save any changes to the PowerShell settings before connecting to retrieve data.** (red text)
- Enforce MDM Enrollment:**
- Quarantine Date:** 08/26/2015 (calendar icon)
- Notify Users On:** 08/21/2015 (calendar icon)
- Subject:** Enroll your device '{DEVICE}' with the Device Management
- Message:** (FIRST NAME) (LAST NAME)
You must enroll your mobile device with the Device Management Server by {QUARANTINE DATE} in order to continue accessing email on the device. If the device has not been enrolled by this date, it will cease to retrieve email and you may experience synchronization errors. Once enrolled, email synchronization will resume.
- The following tokens can be used in the email message subject and body: {DEVICE}, {FIRST NAME}, {LAST NAME}, and {QUARANTINE DATE}** (red text)

4. The **PowerShell Server Address** field will automatically populate with the ActiveSync server address if one is defined in MDM. You can provide an internal IP address for PowerShell access to be used instead of the ActiveSync server address.
5. Check the box next to **Use SSL** if the ActiveSync server uses a Secure Sockets Layer.
6. Select the **Authentication Type**. Choose *Basic* or *Kerberos*.
7. Enter the PowerShell administrator credentials in the **Admin Username** and **Admin Password** fields. Username should be entered in the format *<domain>\administrator*.
8. Set the **Refresh Interval** (in hours) to determine the frequency at which the MDM server will connect to the ActiveSync server to update device and user information.
9. Mark the **Enforce MDM Enrollment** checkbox so that discovered devices will be required to enroll against the *NotifyMDM* server.
10. To enforce enrollment, select a **Quarantine Date** on which unenrolled devices will be blocked from accessing email.

11. At **Notify Users On**, select a date on which users will be notified that they are nearing the quarantine date. Each device a user has not yet enrolled will receive an email message.
12. Compose the **Subject** and **Message** of the email to be sent to unenrolled devices or use the default subject and message. Tokens may be used to insert various information from the MDM database into the text: {DEVICE}, {FIRST NAME}, {LAST NAME}, and {QUARANTINE DATE}.
13. Click the **Save Changes** button.
14. Use the **Connect Now** button to manually initiate a connection to the ActiveSync server and retrieve device user and policy information.

Retrieved data will display in the **Discovered Devices** grid. From the dashboard, select the **Smart Devices and Users** view. Click the **Discovered Devices** button located in the right corner above the User/Device Grid. This flips the view to a list of the devices discovered on the ActiveSync server. Devices that have already enrolled the *NotifyMDM* application appear on the standard User/Device Grid as well.

The screenshot shows a button labeled "Discovered Devices" with a refresh icon. Below it is a table with the following data:

Domain	Liability	Ownership	Last NotifyMDM Sync (Server Local)
	Corporate	Personal	04/29/2015 10:45 AM (-04:00 GMT)

The screenshot shows the "Discovered Devices User/Device Grid" with a search and administration panel on the left. The main table contains the following data:

User Name	First Name	Last Name	Access State	MDM Status	Device Type	Device Platform	
bchandler	Bernard	Chandler	Allowed	Discovered	iPhone	iOS	4NVE
bchandler	Bernard	Chandler	Allowed	Discovered	iPhone	iOS	EPL10
cburrows	Craig	Burrows	Allowed	Discovered	SAMSUNGSPHD7	Android	SA
cburrows	Craig	Burrows	Allowed	Discovered	0PJA2	0PJA2	HTC8c
cmclmore	Charlene	McLemore	Allowed	Discovered	iPad	iOS	
cschuster	Carmela	Schuster	Allowed	Enrolled	SAMSUNGSMG92	SAMSUNGSMG92	
cschuster2	Carmela	Schuster2	Allowed	Discovered	SAMSUNGSMG92	SAMSUNGSMG92	
edavidson	Eric	Davidson	Allowed	Discovered	Android	Android	

Discovered Devices User/Device Grid

Note: For more information on the Discovered Devices grid, see the [Managing Users and resources Guide](#): The Discovered Devices Grid.

Disabling PowerShell

Disabling PowerShell connection will sever the connection between MDM and the ActiveSync server. To maintain control over device access to the ActiveSync server, keep the PowerShell settings or set MDM as proxy for the ActiveSync server. (From the dashboard, select *System Management > Organization*. Check the box beside *Proxy ActiveSync Traffic by Default*.)