Enforcing Enrollment of Mobile Devices with Existing ActiveSync Email Accounts

ZENworks® Mobile Management 3.2.x

October 2015

Novell.

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Table of Contents

Windows PowerShell

Using PowerShell with *ZENworks Mobile Management*

When an organization chooses not to proxy email mail through the *ZENworks Mobile Management* server, devices will be able to connect directly to the ActiveSync server to access email without the requirement of MDM enrollment. As a means of enforcing enrollment, administrators can configure ActiveSync PowerShell settings and employ its capabilities via the *ZENworks Mobile Management* 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 *ZENworks Mobile Management* 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 *ZENworks Mobile Management* server by viewing the Discovered Devices grid.

- Enforce *ZENworks Mobile Management* 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

Using PowerShell with Exchange 2013
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

PowerShell for Office 365
http://powershell.office.com/

Prerequisites

- Install Microsoft .NET Framework 4.0 on the server where the *ZENworks Mobile Management* Web/HTTP component is installed.

- Use Internet Information Services (IIS) to configure the *ZENworks Mobile Management* server to integrate with PowerShell

- Use the *ZENworks Mobile Management* dashboard to configure PowerShell connection settings for the ActiveSync server.

IIS Settings

1. On the MDM server - Using IIS, configure the server for Anonymous Authentication.

   - *Default Web Site* > A*uthentication* > *Anonymous Authentication*.

   - Select *Edit . . .* from the panel to the right.

   - Select the radio button next to *Application pool identity*.
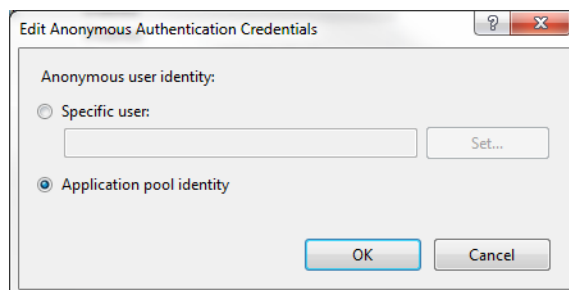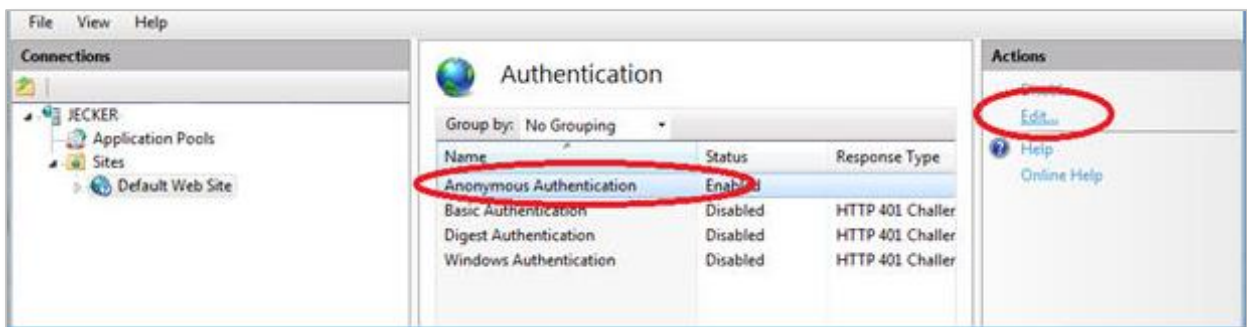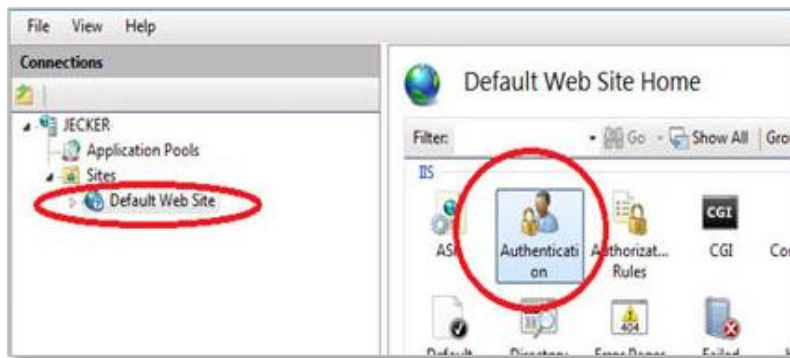
2. On the MDM server - Using IIS, set the application pool user as follows.

> *-Application Pools* > *DefaultAppPool* > *Advanced Settings . . .*
>
> -Click the icon next to *Identity* and select **ApplicationPoolIdentity**.
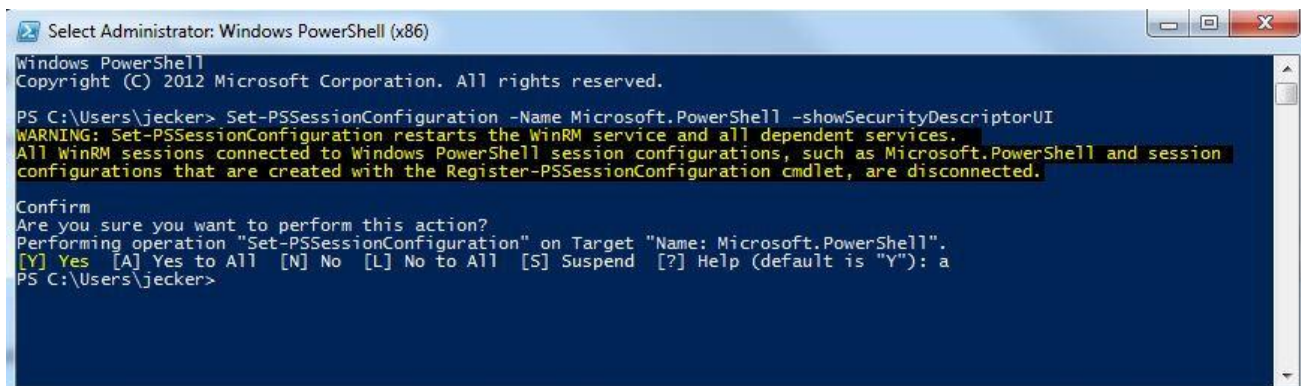>
> -Verify that *Load User Profile* is set to **True**.
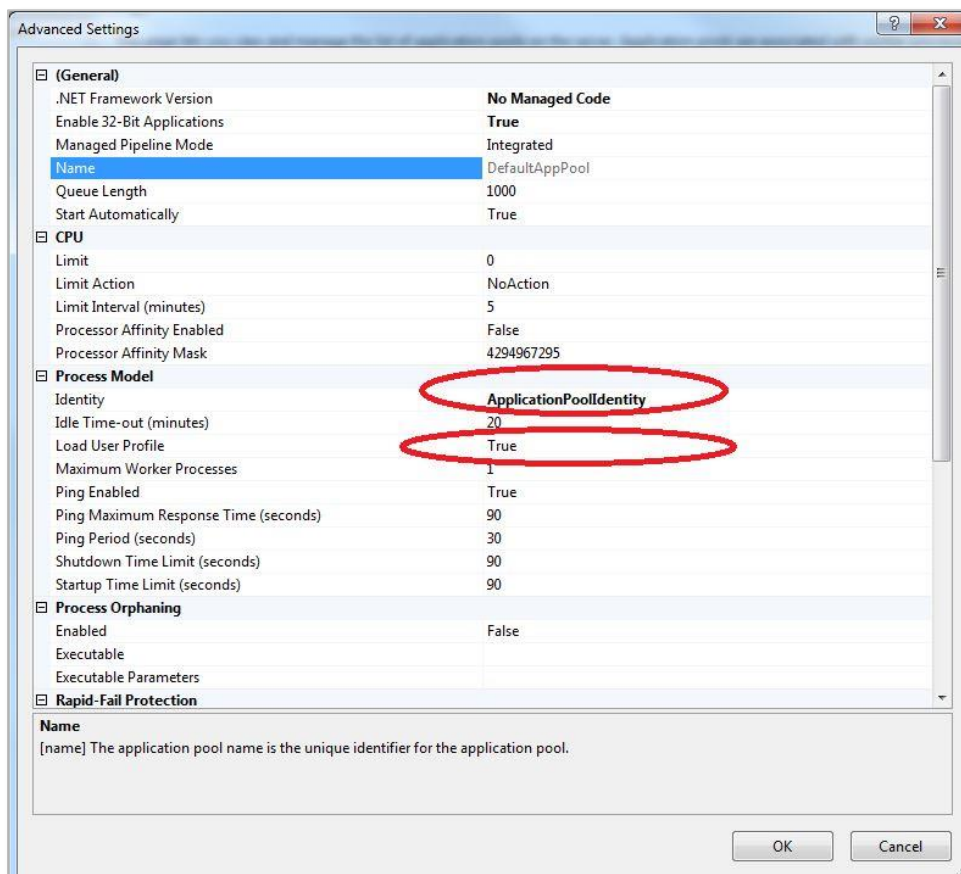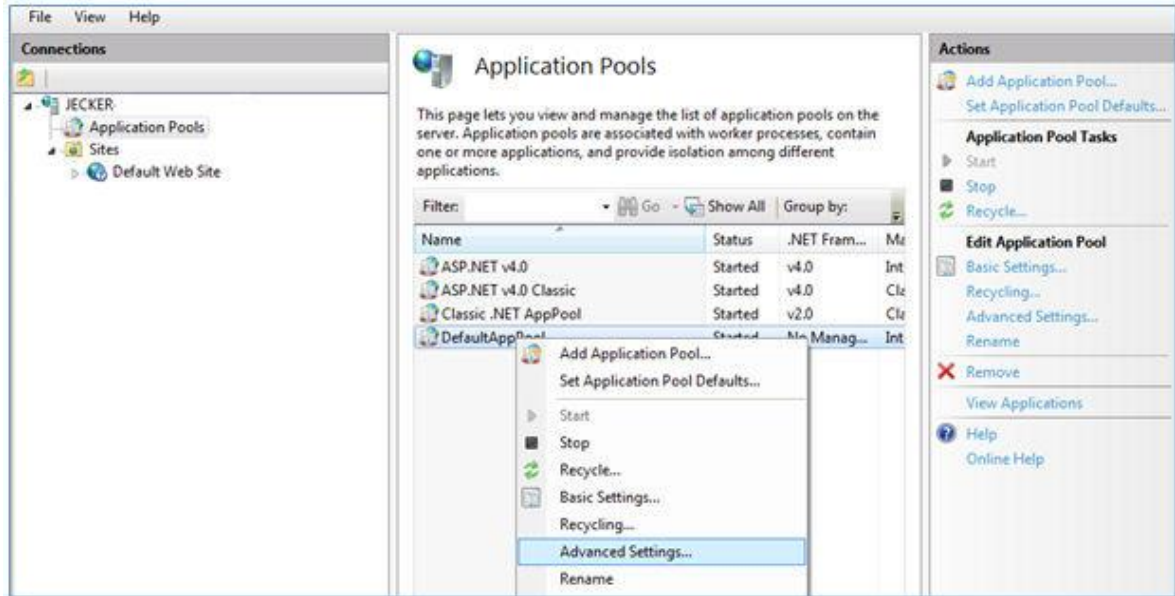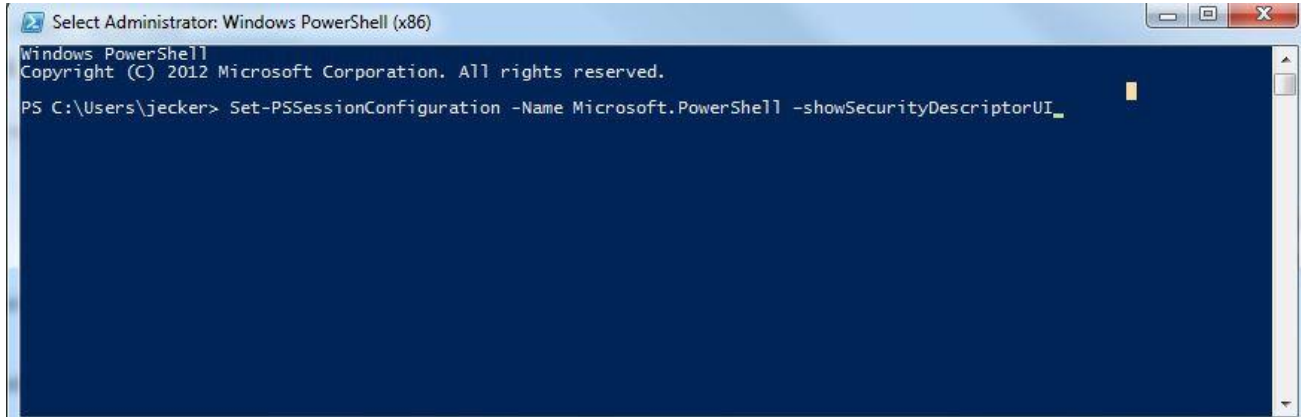
3. The application pool identity needs to be granted executive privileges for the PowerShell process. Change permissions by remoting into the web system, opening the PowerShell app on the web server, and running this command:

Set-PSSessionConfiguration –Name Microsoft.PowerShell –showSecurityDescriptorUI

After you accept the confirmation in PowerShell, a permissions dialog opens. Add the user for your app pool here.
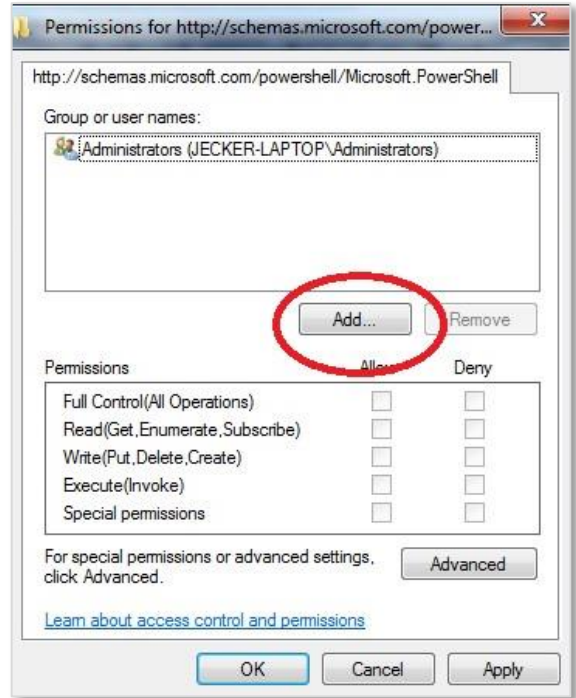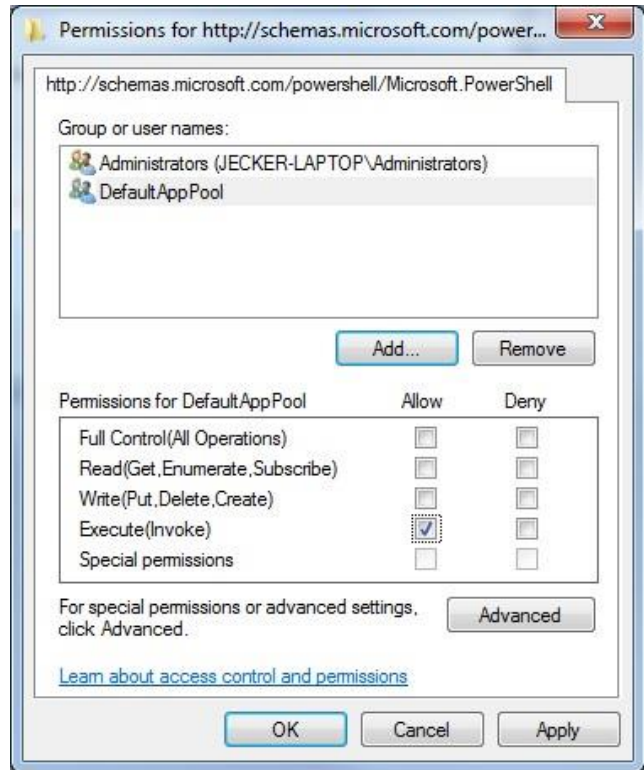
The username will be "IIS AppPool\<The Name of the App Pool MDM is using>";

Check name and click **OK** when it finds your user.
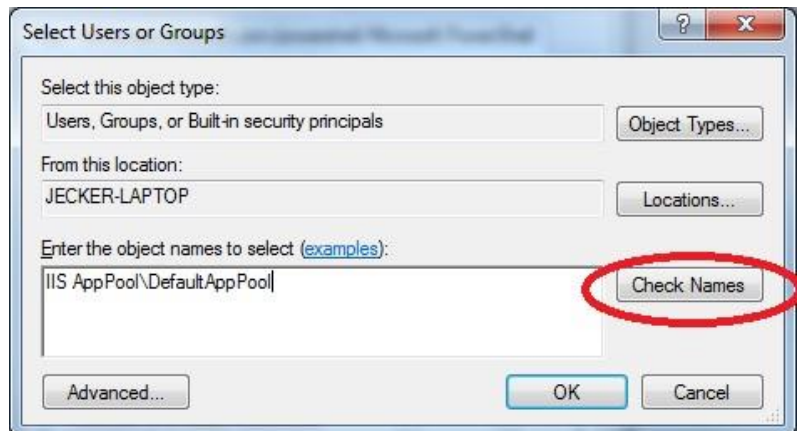
Set permissions to allow *Execute*.

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 *ZENworks Mobile Management* administrative dashboard, select **Organization** > **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.

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 *ZENworks Mobile Management* 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 *ZENworks Mobile Management* application appear on the standard User/Device Grid as well.

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 > Organization*. Check the box beside *Proxy ActiveSync Traffic by Default*.)