

vmware

VMware vCenter™ Protect Update Catalog



# Quick Start Guide

VMware vCenter™ Protect Update Catalog

For use with SCUP 4.5

---

## Copyright

Copyright © 2010 - 2011 VMware Inc. All rights reserved.

No part of this document may be reproduced or retransmitted in any form or by any means electronic, mechanical, or otherwise, including photocopying and recording for any purpose other than the purchaser's personal use without written permission of VMware Inc.

---

## Trademarks

vCenter and the VMware logo are trademarks or registered trademarks of VMware Inc. Microsoft, Windows, System Center Configuration Manager, and System Center Updates Publisher are either trademarks or registered trademarks of Microsoft Corporation.

All other trademarks, tradenames, or images mentioned herein belong to their respective owners.

---

## Document Information and Print History

Document number: N/A

Date	Version	Description
January 2010	Initial release	Initial release of the <b>Shavlik SCUPdates Quick Start Guide</b> .
July 2010	Rev A of this document	Update branding and system requirements, add self-signing certificate information.
January 2011	Rev B of this document	Many new screen shots, add link for list of supported products, make minor corrections to group policy steps, update cover.
March 2011	Rev C of this document	Clarify the certificate creation and group policy setup process for PKI users.
April 2011	Rev D of this document	Update outdated PKI Web link.
November 2011	Rev E of this document	Rebrand the document and change the product name to VMware vCenter Protect Update Catalog.

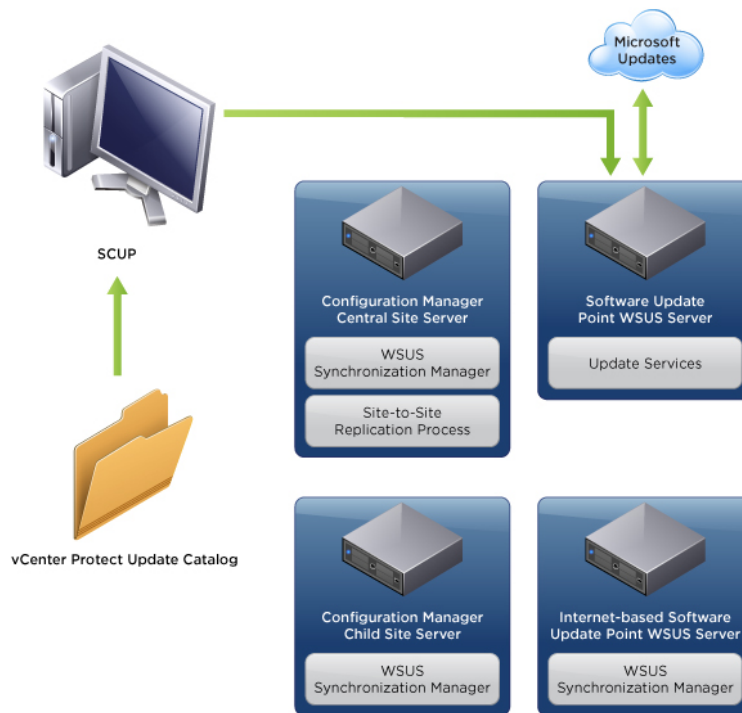
# PREPARING TO USE VMWARE vCENTER™ PROTECT UPDATE CATALOG

## Welcome

This document provides a roadmap of tasks you must perform when preparing to use VMware vCenter™ Protect Update Catalog.

vCenter Protect Update Catalog contains the detection and deployment logic used to patch non-Microsoft products and legacy Microsoft products. The catalog consists of a number of patch update files that can be imported into Microsoft’s System Center Updates Publisher (SCUP). You then use SCUP to publish the update files to Microsoft’s System Center Configuration Manager (SCCM). This allows SCCM to patch your legacy Microsoft products and your non-Microsoft products such as Adobe Reader, Adobe Flash, Apple Quicktime, Firefox, etc.

The following diagram illustrates how vCenter Protect Update Catalog interacts with Microsoft’s SCUP and SCCM components.



For more detailed information see the vCenter Protect Update Catalog section of the VMware IT Management Community (<http://community.shavlik.com>). You will need to become a member of the community in order to gain full access to all available resources.

## System Requirements

In order to use vCenter Protect Update Catalog you must have the following:

- Windows Server platform (2003 Family SP2 or later, or 2008 Family)
- Windows Server Update Services (WSUS) 3.0 SP2 or later
- System Center Configuration Manager (SCCM) 4.0 SP2 or later (in Native or Mixed mode)
- System Center Updates Publisher (SCUP) 4.50.1103.000 or later
- vCenter Protect Update Catalog license

## Add an SCCM Self-signing Certificate

### Creating a Self-signing Certificate

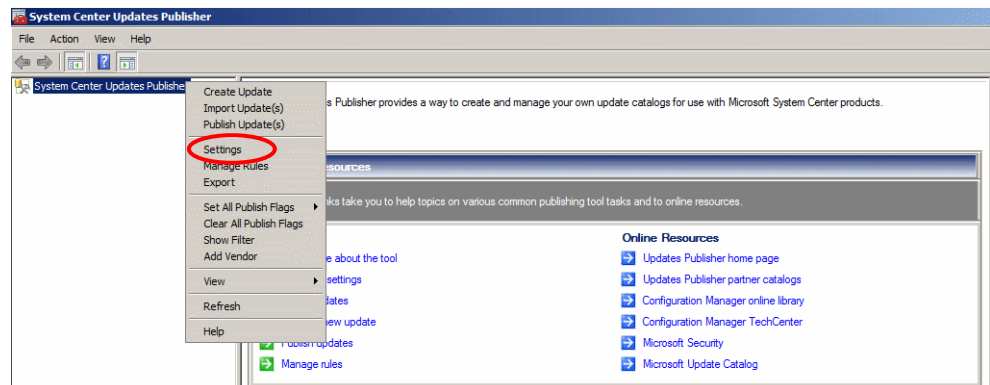
**Important!** If you are using an internal Public Key Infrastructure (PKI) to create and deploy your self-signing certificate (rather than using the default WSUS Publishers Self-signed certificate), skip this section and instead see the following for information on creating the certificate.

<http://mikeshellenberger.wordpress.com/2010/09/02/system-center-updates-publisher-microsoft-pki/>

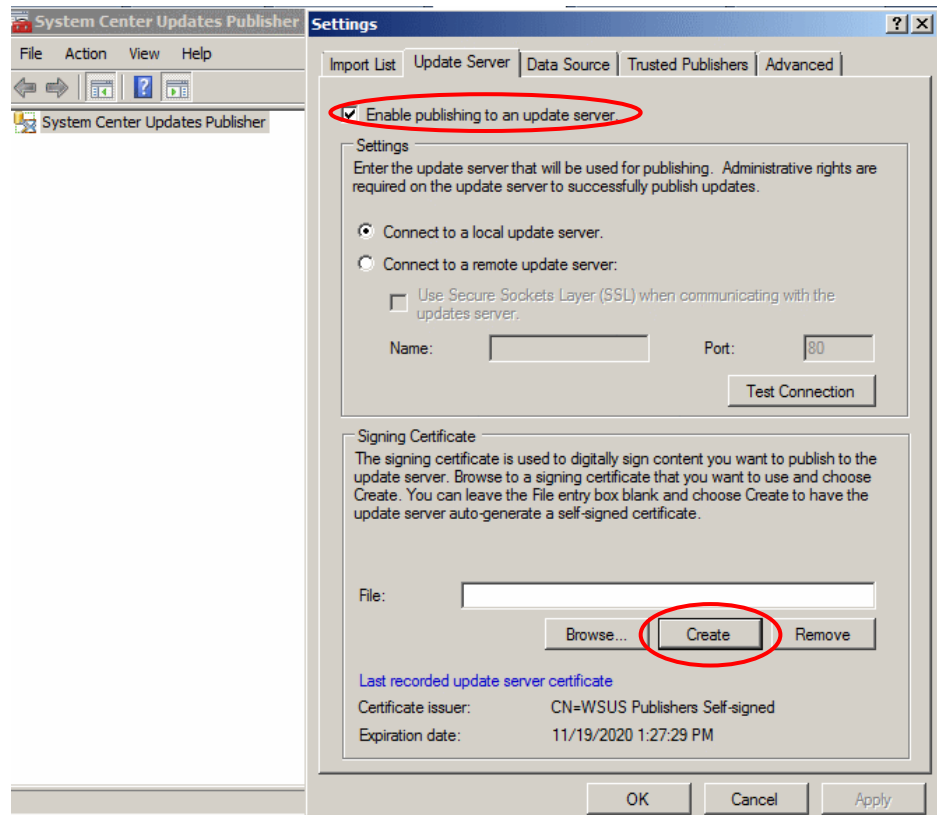
**Note:** If you have already created a self-signing certificate you should review this section to verify all steps have been completed; do not recreate the certificate.

A self-signing certificate is required in order to publish vCenter Protect Update Catalog patch update files to the SCUP and SCCM server components. To create a self-signed certificate for your enterprise:

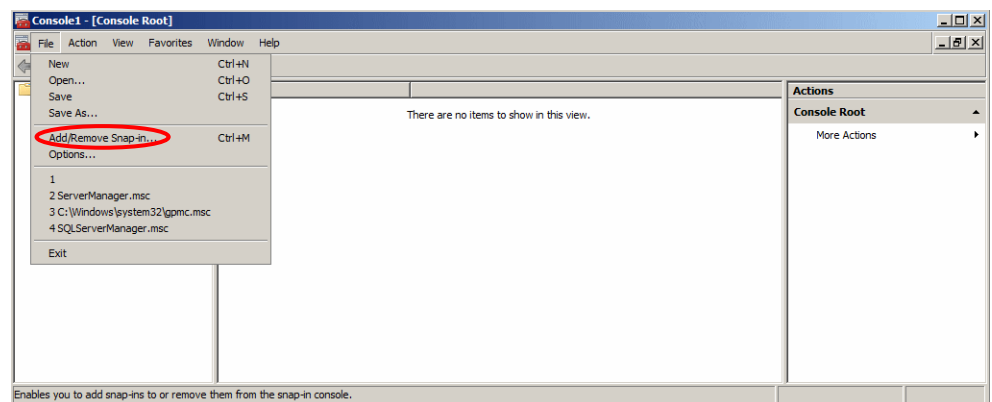
1. Open the SCUP management console.
2. Right-click the root tree **System Center Updates Publisher** and select **Settings**.



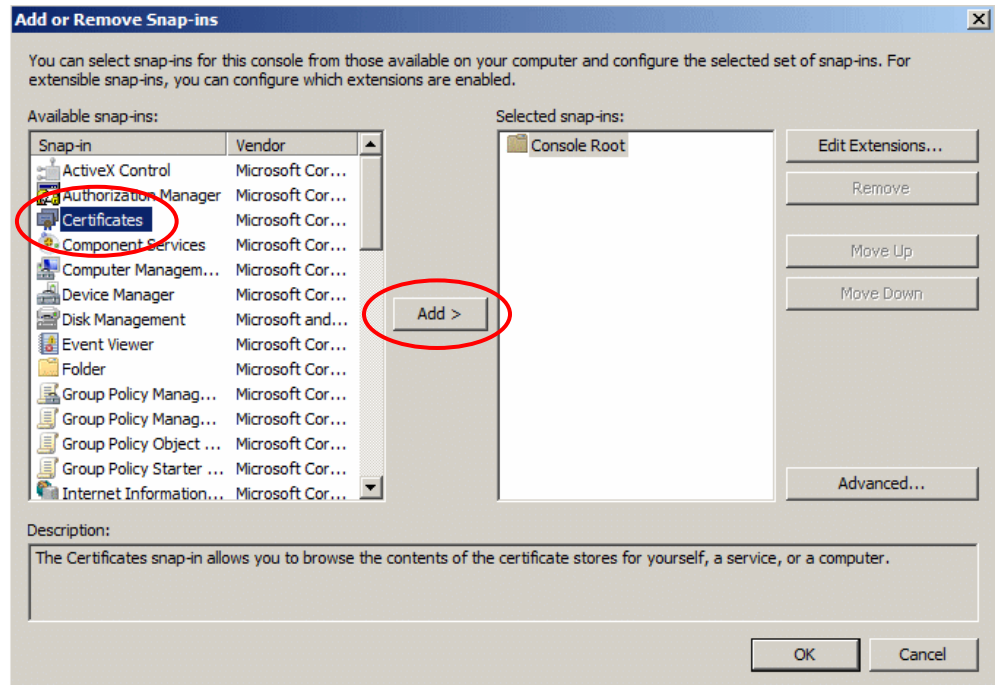
3. Select the **Update Server** tab.



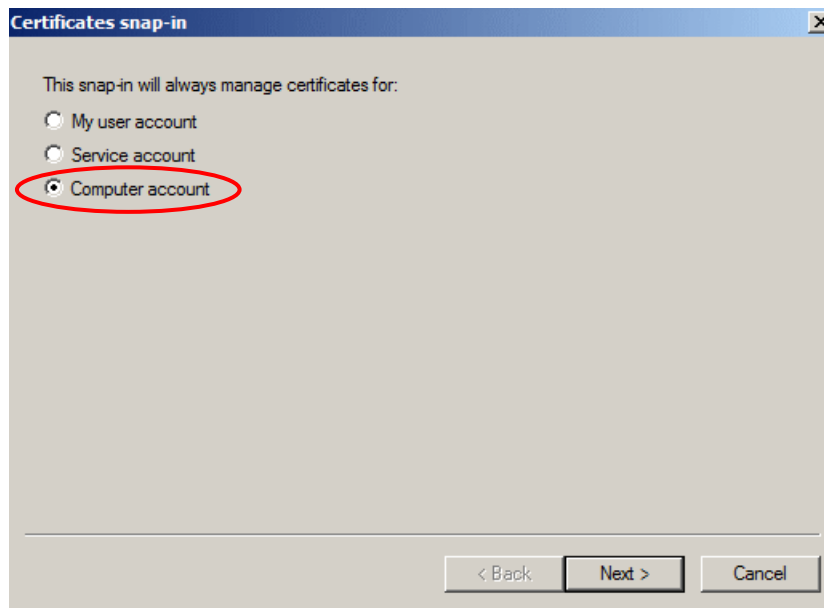
4. Enable the **Enable publishing to an update server** check box.
5. In the **Signing Certificate** area, click **Create**.
6. On the **Certificate Registration** confirmation dialog, click **OK**.
7. Open an MMC console and select **File>Add/Remove Snap-in**.



8. Click **Add**, select **Certificates**, and then click **Add**.



9. Choose **Computer account** and then click **Next**.



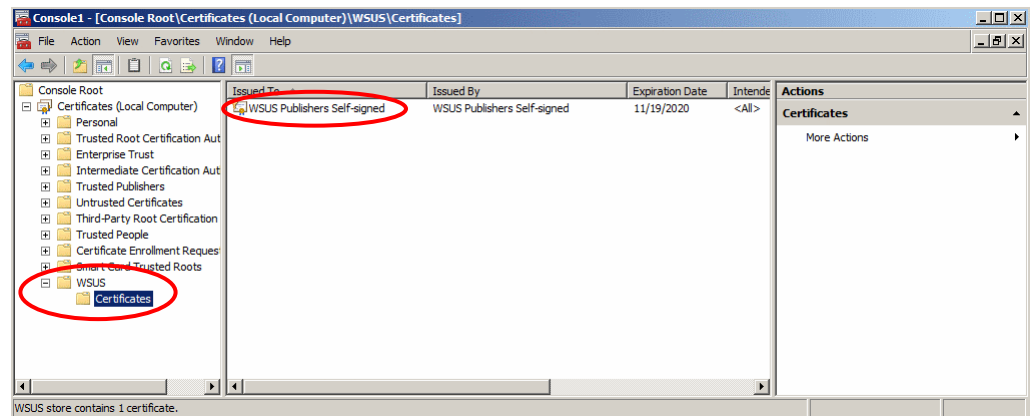
10. On the **Select Computer** dialog, choose **Local computer** and then click **Finish**.
11. Click **OK**.

Save a copy of this MMC for future use as you will be using it often.

## Export Certificate

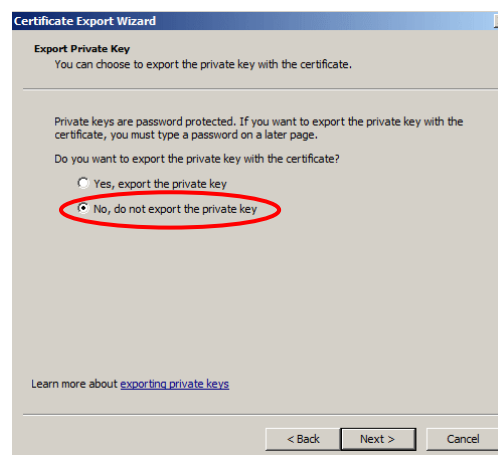
**Important!** Do not export the private key.

You should see a folder called **WSUS > Certificates**.

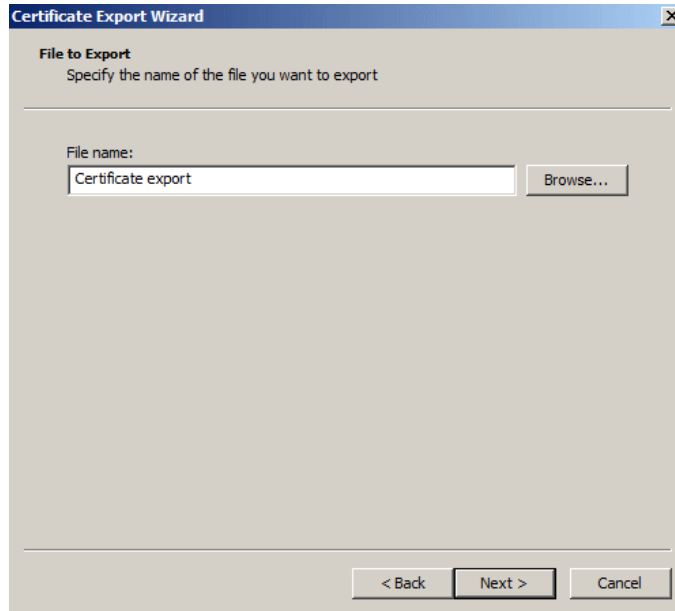


Within this folder you should see a “WSUS Publishers Self-signed” certificate. This certificate should be the only one in your certificate store to have a public and private key.

1. Right-click the **WSUS Publishers Self-signed** key and select **All Tasks > Export**.
2. On the **Welcome to the Certificate Export Wizard** dialog, click **Next**.
3. On the **Export Private Key** dialog, choose **No, do not export the private key** and then click **Next**.



4. On the **Export File Format** dialog, choose **DER encoded binary x.509** and then click **Next**.
5. On the **File to Export** dialog, type a file name and then click **Browse** to specify where you want to save the file.



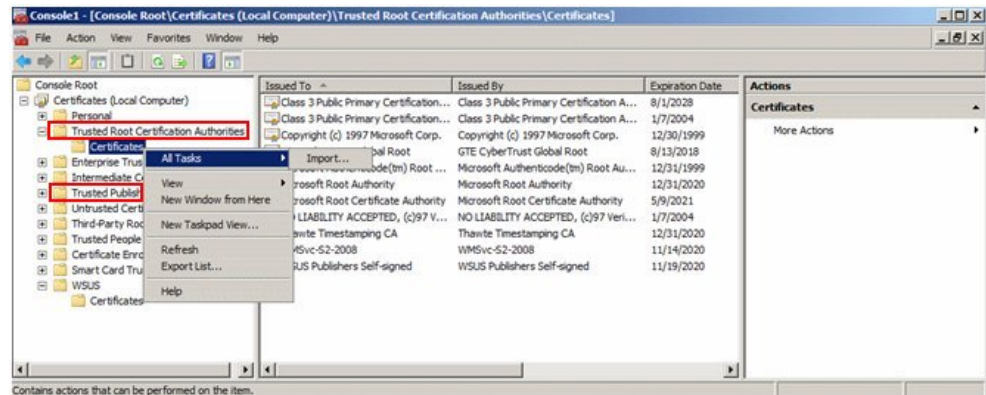
6. Click **Next**.
7. On the **Completing the Certificate Export Wizard** dialog, click **Finish**.
8. On the confirmation dialog, click **OK**.

**Note:** Don't close MMC.

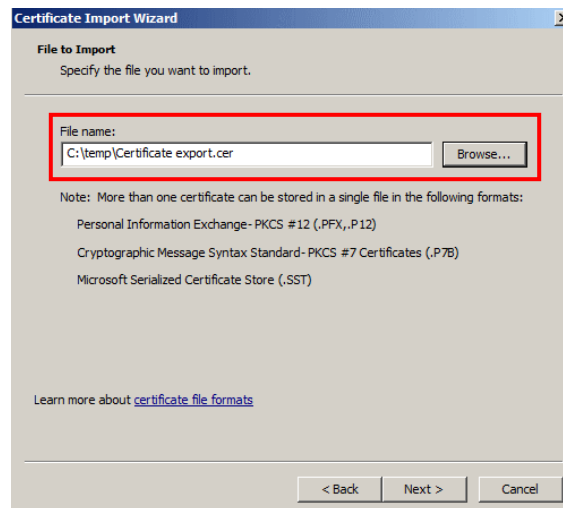
### *Copy the Certificate to the Appropriate Certificate Stores*

You now need to add the new non-private key to the **Trusted Root Certification Authorities** and the **Trusted Publishers** certificate stores on your server. If you use multiple servers that house your SCCM, WSUS and SCUP consoles separately, you must repeat the steps in this section for each server in the chain.

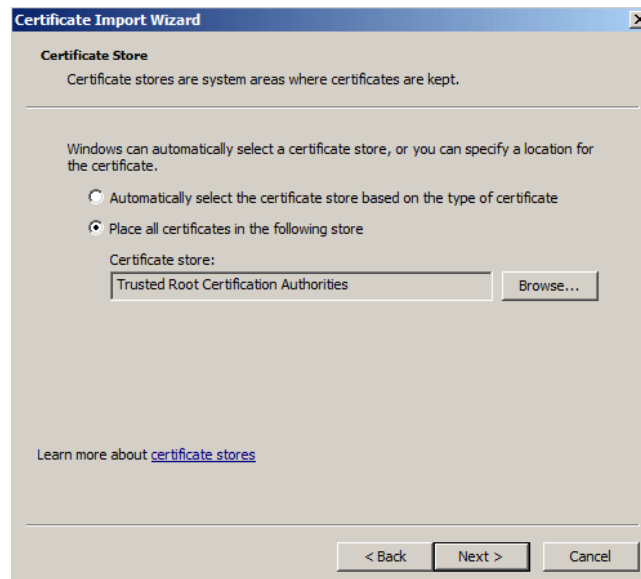
1. In the Certificates Store MMC select **Trusted Root Certification Authorities > Certificates**, right-click **Certificates** and select **All Tasks > Import**.



2. On the **Welcome to the Certificate Import Wizard** dialog, click **Next**.
3. On the **File to Import** dialog, browse for your public key file and then click **Next**.



4. On the **Certificate Store** dialog, choose **Place all certificates in the following store** and then click **Next**.



5. On the **Completing the Certificate Import Wizard** dialog, click **Finish**.
6. On the confirmation dialog click **OK**.
7. Repeat steps 1 – 6, only this time select **Trusted Publishers** in Step 1.

---

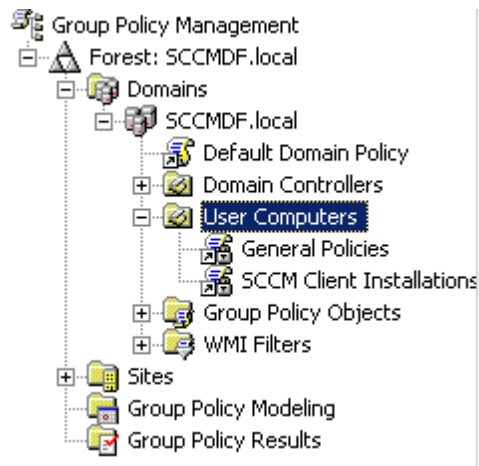
## Windows Server 2008 Group Policy Setup Using WSUS Self-signed Certificates

**Note:** All steps and screen shots used in the remainder of this document are for Windows Server 2008. The steps and screens for Windows Server 2003 may be slightly different.

You must have a few settings in place for proper Native or Mixed mode to work correctly. If you don't have a specific GPO policy for SCCM you should make one for your clients/servers. This makes it easier to manage SCCM issues and policies.

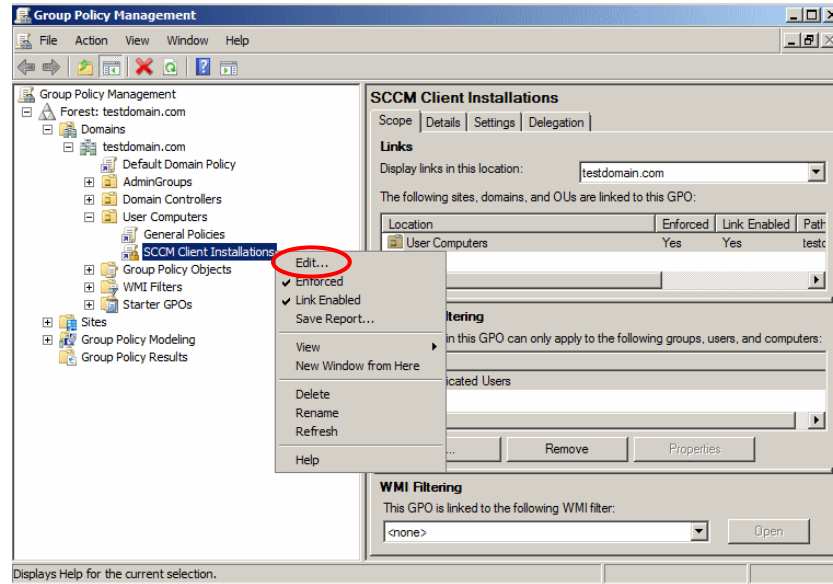
1. Open **Group Policy Management Console** (on Windows Server 2003 this is a download and install from Microsoft).
2. Highlight your domain name and select the organizational unit (OU) you wish to add your policy to.

The following example contains an OU called "User Computers" under the Users and Computers Console. You should add all your users' computers to the OU. This example also contains a policy called "SCCM Client Installations" (SCI) in the Group Policy Management Console. The policy should be enforced (right-click the policy and then select **Enforced**).



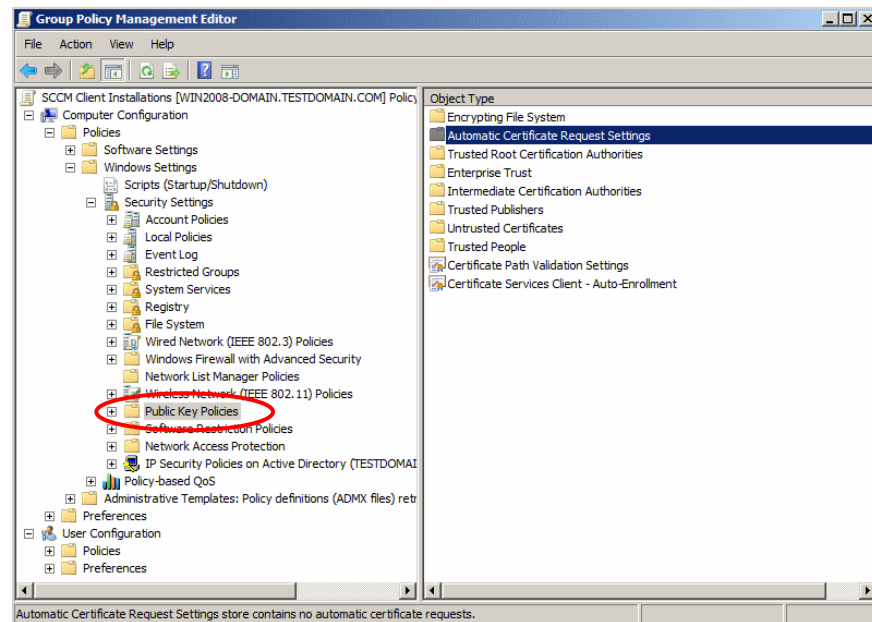
Set all your policies that affect these computers for SCCM in the SCCM Client Installations policy.

1. Right-click the SCCM Client Installations policy and then select **Edit**.



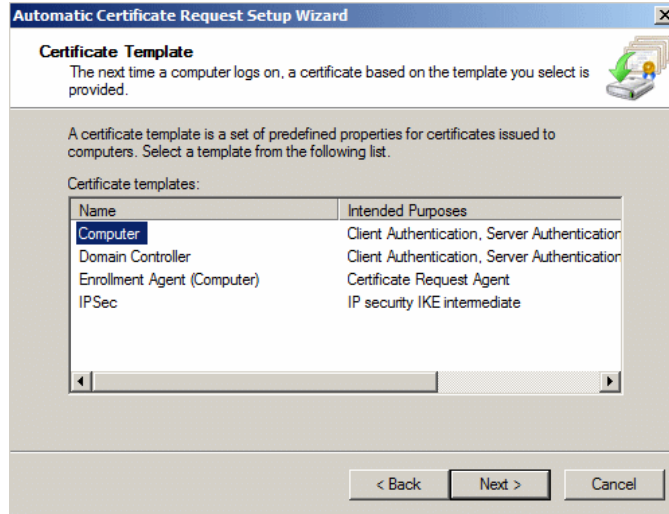
The **Group Policy Object Editor** dialog is displayed. It is used to manage your policies to be applied.

2. Select **Computer Configuration > Windows Settings > Security Settings > Public Key Policies**.



3. In the right-hand pane, right-click **Automatic Certificate Request Settings** and select **New > Automatic Certificate Request**.

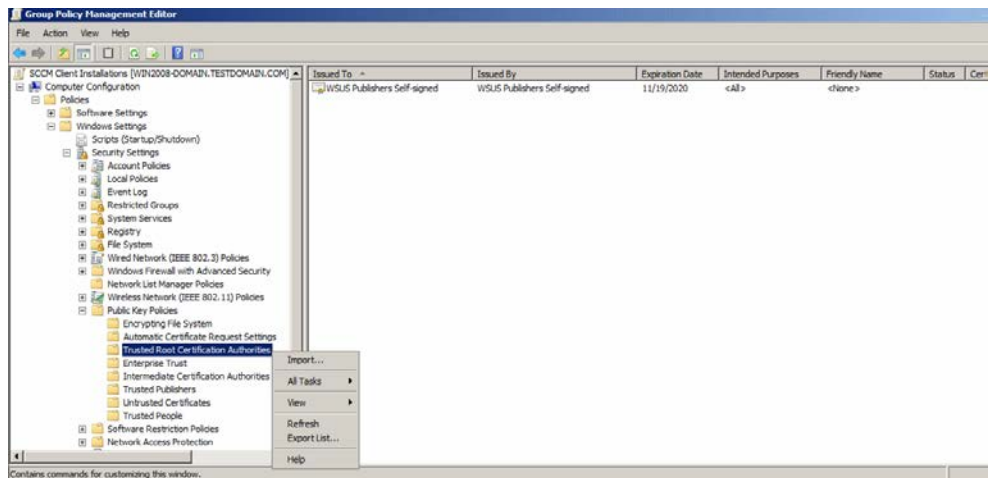
4. On the **Welcome to the Automatic Certificate Request Setup Wizard** dialog, click **Next**.
5. On the **Certificate Template** dialog, select **Computer** and then click **Next**.



6. On the **Completing Automatic Certificate Request Setup Wizard** dialog, click **Finish**.

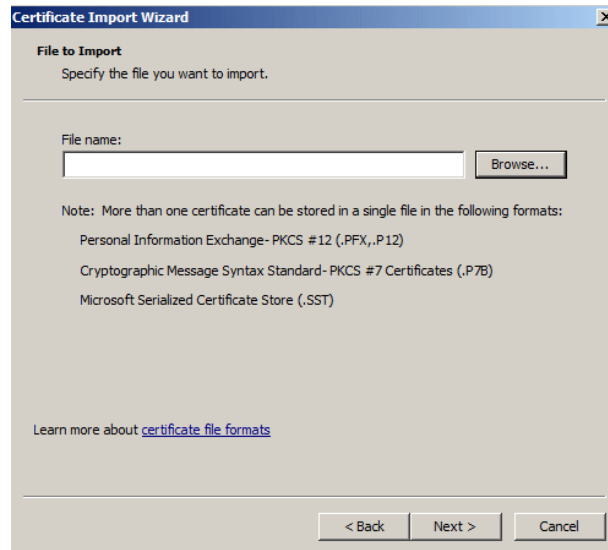
**Note:** If you are using an internal Public Key Infrastructure (PKI) to create and deploy your self-signing certificate (rather than using the default WSUS Publishers Self-signed certificate), use your PKI certificate in place of the WSUS certificate in Steps 7 – 15.

7. Select **Computer Configuration > Windows Settings > Security Settings > Public Key Policies > Trusted Root Certification Authorities**.

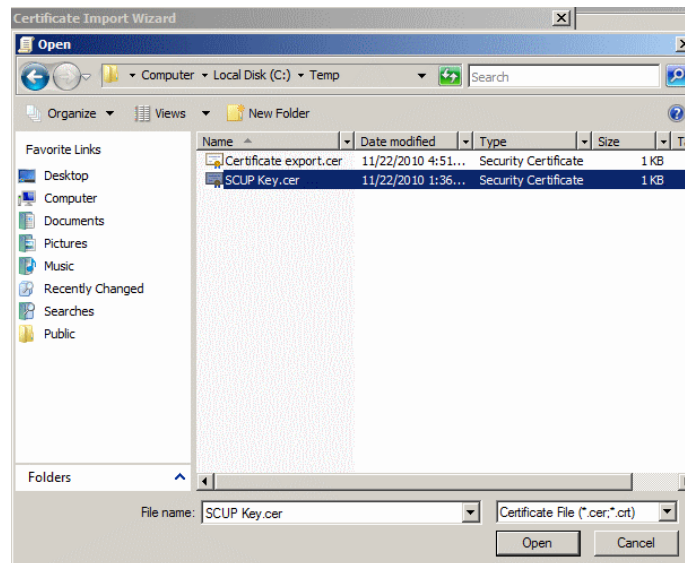


8. Right-click on **Trusted Root Certification Authorities** and then select **Import**.
9. On the **Welcome to the Certificate Import Wizard** dialog, click **Next**.

- On the **File to Import** dialog, click **Browse** and locate your public key file.

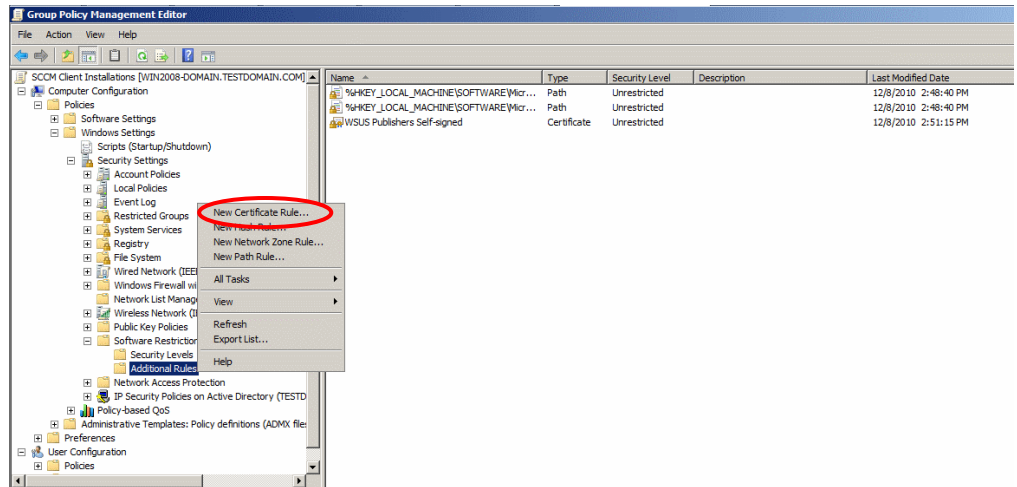


- Select the public key file and then click **Open**.



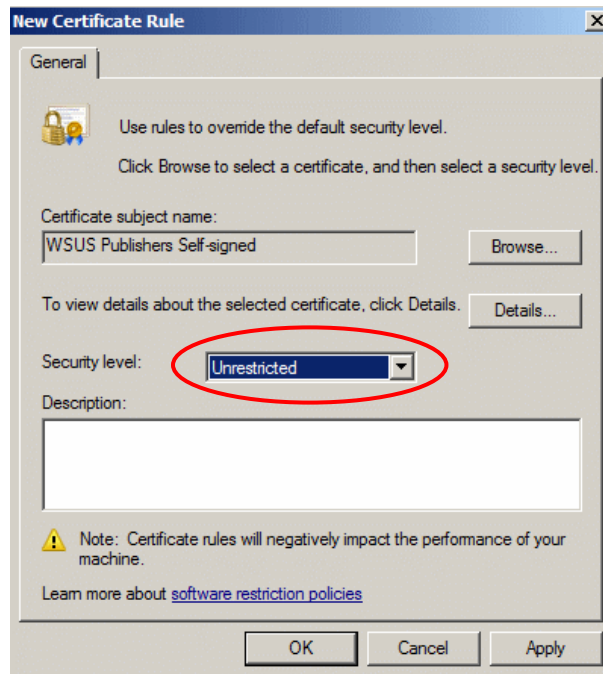
- On the **File to Import** dialog, click **Next**.
- On the **Certificate Store** dialog, choose **Place all certificate in the following store** and then click **Next**.
- On the **Completing the Certificate Import Wizard** dialog, click **Finish**.
- On the confirmation dialog, click **OK**.
- Select **Computer Configuration > Windows Settings > Security Settings > Software Restriction Policies**.

17. Right-click **Additional Rules** and select **New Certificate Rule**.



18. Click **Browse**, locate the public key file, and then click **Open**.

19. Change the security level to **Unrestricted** and then click **OK**.

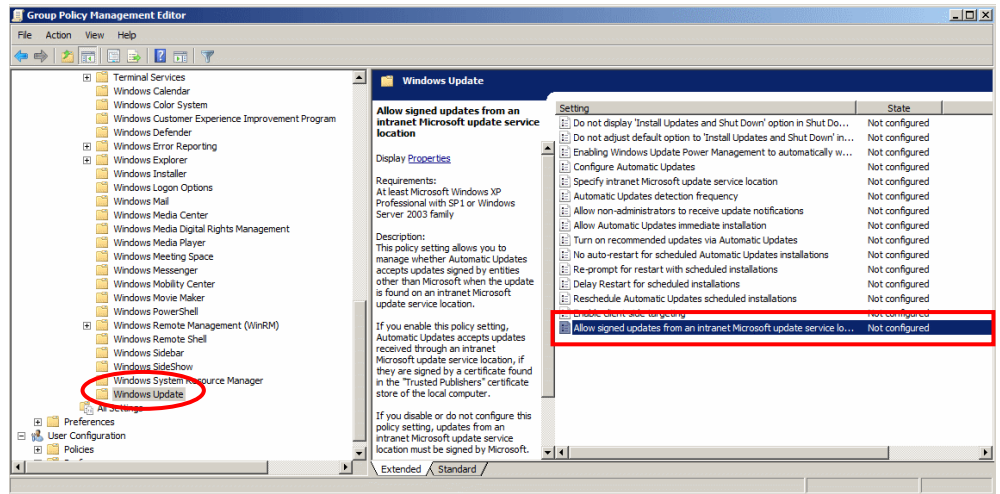


20. On the subsequent confirmation dialogs, click **Yes** and then **OK**.

Now the clients will get the certificates from GPO.

21. Select **Computer Configuration > Administrative Templates > Windows Components > Windows Update**.

22. Double-click **Allow signed updates from an intranet Microsoft update service location**.



23. On the **Setting** tab, choose **Enabled** and then click **OK**.

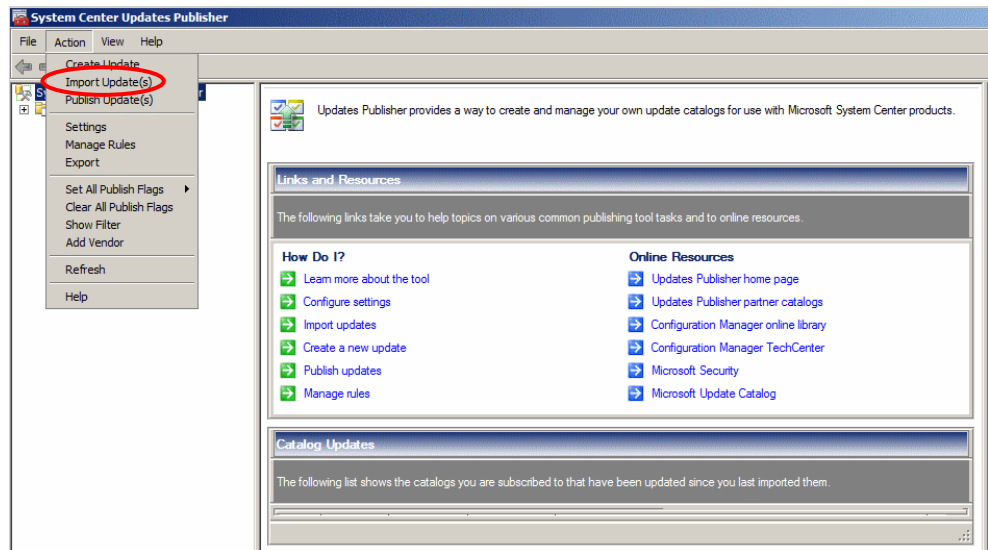
## Download the Latest Catalog File

Before beginning the import process you should always download the most current vCenter Protect Update Catalog file. You will receive an e-mail message whenever a newer file is available. The e-mail message will specify the location of the catalog file as well as the credentials needed to log on to the site. Simply download and save the file to your computer or to a location on your computer network.

## Import the Catalog File into SCUP

Importing the catalog file into SCUP is a very easy process.

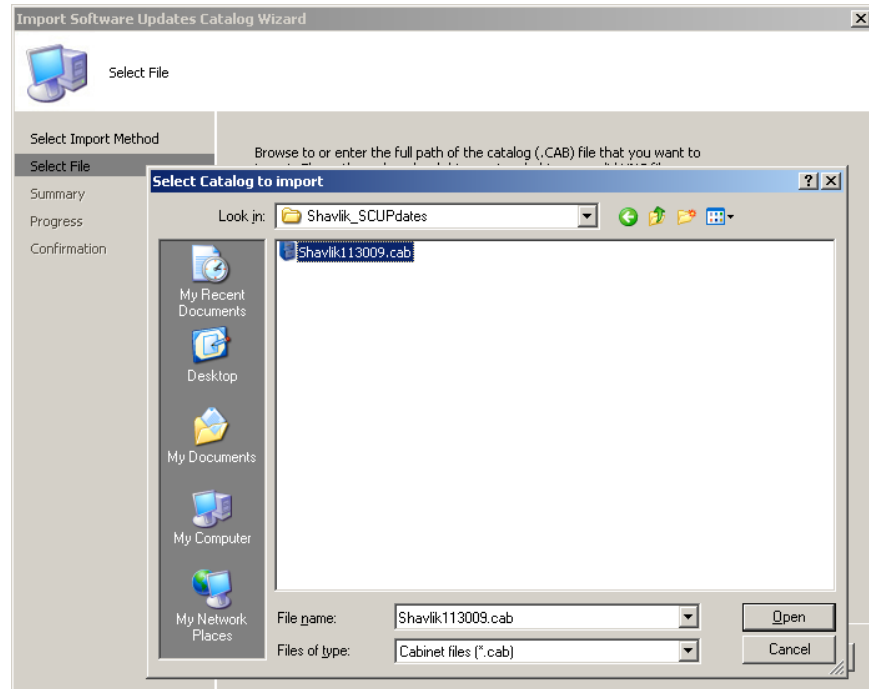
1. Start System Center Updates Publisher (SCUP).
2. Select **Actions > Import Update(s)**.



The **Import Software Updates Catalog Wizard** is displayed.

3. Choose **Single Catalog Import** and then click **Next**.
4. On the **Select File** dialog, click **Browse** and then specify the location of the vCenter Protect Update Catalog file.

For example:

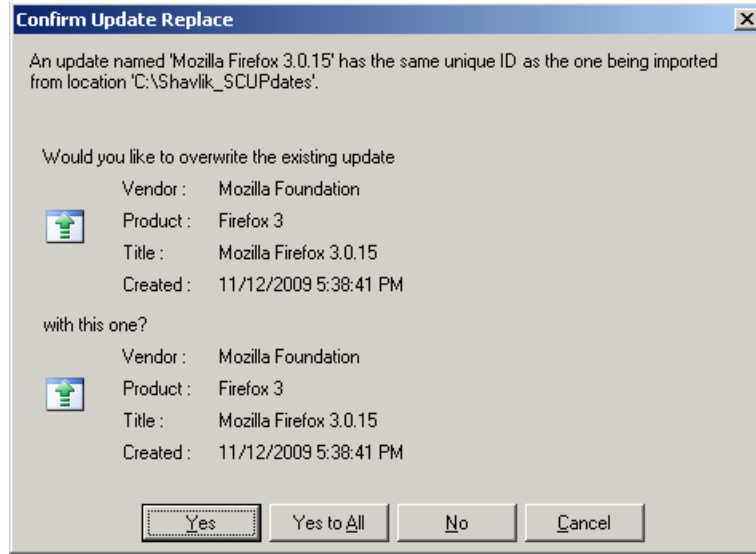


5. Select the file and then click **Open**.
6. On the **Select File** dialog click **Next**.
7. On the **Summary** dialog, verify that you have specified the correct file and then click **Next**.
8. (Optional) If you are asked to validate the catalog, click **Accept**.



All vCenter Protect Update Catalog files are signed with a valid certificate. You may wish to choose **Always accept catalog from "Shavlik Technologies"** to bypass this validation dialog in the future.

During the import process some previous updates may already exist. In this case you are presented with a **Confirm Update Replace** dialog. For example:



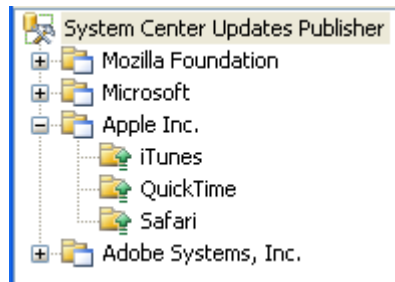
Always click **Yes** to overwrite the existing update. VMware may provide bug fixes in the vCenter Protect Update Catalog data that require an update.

9. On the **Confirmation** dialog, click **Close**.

The System Center Updates Publisher home page is redisplayed.

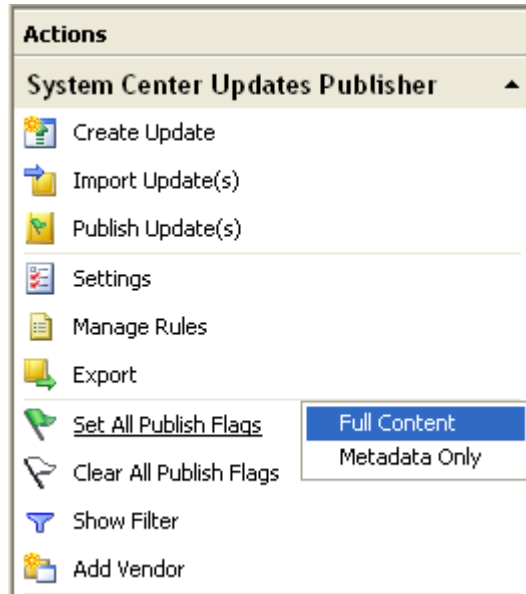
10. In the console tree in the left-hand pane, select the product(s) you want to publish.

You can specify all products by selecting the top level item (System Center Updates Publisher). Or, you can drill down as far as you want by specifying individual product vendors, individual products, or even individual article IDs within a product.



11. In the **Actions** area in the right-hand pane, click **Set All Publish Flags > Full Content**.

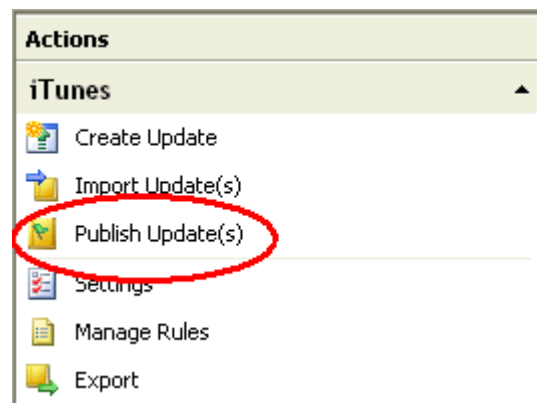
**Note:** Be sure to select **Full Content**. vCenter Protect Update Catalog does not support the **Metadata Only** option.



The associated Publish flags will turn green. For example:

Article ID	Name	Severity	Type	Creation Date	Language	Publish	Publish Type	Expire
QAI0901	iTunes 9.0.1	Critical	Security ...	11/12/2009	English		Full Content	False
QAI0901	iTunes 9.0.1 x64	Critical	Security ...	11/12/2009	English		Full Content	False
QAI0902	iTunes 9.0.2 x64	Low	Security ...	11/12/2009	English		Full Content	False
QAI0902	iTunes 9.0.2	Critical	Security ...	11/12/2009	English		Full Content	False

- In the **Actions** area in the right-hand pane, click **Publish Updates**.



This pushes the update files to SCCM.

- Click **Next** on all subsequent dialogs to complete the process.

You may need to answer questions from the software publishers about the updates.

You can now use SCCM to deploy the non-Microsoft product patches.

## Supported Products

---

For a complete list of the products supported by vCenter Protect Update Catalog, see:

<http://community.shavlik.com/answers/viewQuestion.apexp?id=906C0000000TSjuIAG>

## Support Information

---

For technical assistance with vCenter Protect Update Catalog, please refer to one of the following support options:

- Browse the vCenter Protect Update Catalog section of the VMware IT Management Community at <http://community.shavlik.com>
- E-mail us at [shavlik-scupdates@vmware.com](mailto:shavlik-scupdates@vmware.com)
- Phone Technical Support at (866) 407-5279