

Upgrade Guide

VMware vCenter™ Protect 8.0

vmware®

Copyright

Copyright © 2009 – 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

VMware vCenter Protect and the VMware logo are trademarks or registered trademarks of VMware Inc.

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
June 2009	NetChk Protect 7.0	Initial release of the Shavlik NetChk Protect 7.x Upgrade Guide .
August 2009	NetChk Protect 7.1 Document Rev A	Add SQL Server 2000 and C++ prereq info for 7.1 users, and info about the asset management feature. Add data rollup functional difference.
November 2009	NetChk Protect 7.2 Document Rev B	Add Windows 7 info to system requirements section.
April 2010	NetChk Protect 7.5	Add info about Scan View, the new power management feature, improvements to software asset scan and virtual machine capabilities.
May 2010	NetChk Protect 7.5, Document Rev A	Clarify licensing information, some additional feature descriptions.
September 2010	NetChk Protect 7.6	Update product branding, add information about new 7.6 features and improvements.
March 2011	NetChk Protect 7.8	Add information about new 7.8 features and improvements.
October 2011	VMware vCenter Protect 8.0	Update product branding, add info about 8.0 upgrade tasks. Remove all info about versions prior to 7.5.
December 2011	VMware vCenter Protect 8.0, Document Rev A	Add step explaining how to compress the database before beginning the upgrade process.

WELCOME

Acquisition Note

Shavlik Technologies is now part of VMware. To reflect this acquisition, beginning with version 8.0 the product name has changed from Shavlik NetChk Protect to VMware vCenter Protect.

Purpose of this Guide

Welcome to VMware vCenter Protect 8.0. This document describes how to upgrade from NetChk Protect 7.5, 7.6, or 7.8 to VMware vCenter Protect 8.0. If you are currently using a version that is older than NetChk Protect 7.5, you must first upgrade to 7.8 before upgrading to 8.0.

In addition to describing the upgrade procedure, this document lists a number of functional differences you should be aware of when upgrading to VMware vCenter Protect 8.0. It also highlights the areas in the user interface that have changed significantly.

New System Requirements and Prerequisites

Please note the following new console requirements and prerequisites for VMware vCenter Protect 8.0.

- SQL Server 2008 R2 Express Edition SP1 is installed if you do not have SQL Server.
- Microsoft .NET Framework 2.0 SP2 (required in order to use the ITScripts feature)
- Windows PowerShell 2.0 or later (required in order to use the ITScripts feature)
- Windows Imaging Component
- Remote Desktop connections must be allowed in order to use the RDP feature

All missing software prerequisites will be automatically installed during the upgrade process.

See the *VMware vCenter Protect Installation Guide* for the complete list of system requirements.

UPGRADE PROCEDURE

Overview

This section describes how to upgrade from Shavlik NetChk Protect version 7.5, 7.6, or 7.8 to VMware vCenter Protect 8.0. If you are taking this opportunity to move the console to a new machine, you should perform the upgrade before moving to the new machine.

Before performing the upgrade, be sure to read the *Significant Changes and Enhancements* section on page 15 so you are aware of how the upgrade will affect your system.

Note: If you are currently using a version that is older than 7.5 you must upgrade to version 7.8 before upgrading to version 8.0. Use the following link to download version 7.8:

<http://www.shavlik.com/downloads.aspx>

Performing the Upgrade

1. Compress the database used to store scan results, patch deployment results, and threat remediation results.

You can do this in SQL Server Management Studio by right-clicking the ShavlikScans database and selecting **Tasks > Shrink > Database**. For additional database maintenance information see:

<http://supportteamblog.shavlik.com/2010/01/13/sql-database-maintenance/>

2. Create a backup of your current database using SQL Server Management Studio.
3. (Optional) If you use listening agents, you should change their configuration to temporarily increase the frequency with which they perform a check-in.

Here's why: Once the upgrade is complete, the listening agents will not be able to respond to the console's "check in now" command until after they have checked in and downloaded the updated engines and XML data files. By shortening the check-in period you will shorten the amount of time that the agents are not functioning as listening agents.

- To modify the check-in frequency: On the **General Settings** tab of your agent policy, change the **Check-In interval** to be 10 minutes and then click **Save and Update Agents**. If you have many agents and are concerned about performance issues you can use a slightly higher value of 20 or 30 minutes.
- To verify that your agents have the configuration change: In Agent Manager, use the **Last Agent Check In** column to verify that your agents have checked in after the check in frequency was changed.

4. Close all programs running on the console machine, including Shavlik NetChk Protect.
5. Download the VMware vCenter Protect 8.0 executable file to your console machine using the following link:

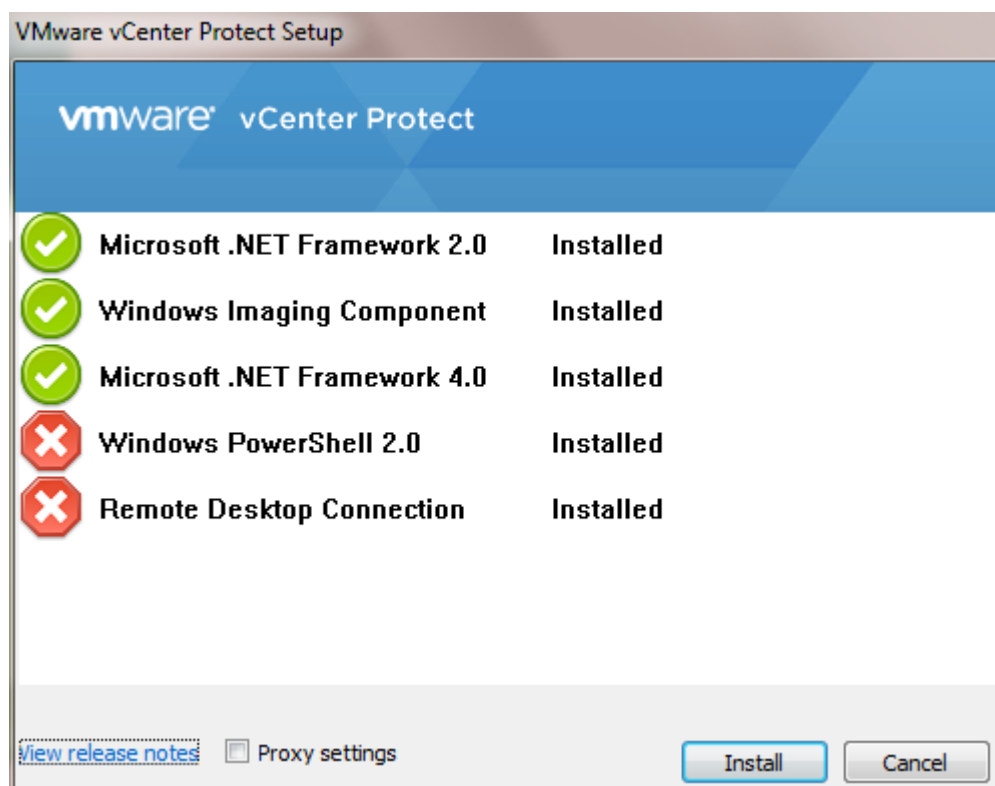
<http://www.shavlik.com/downloads.aspx>

6. Begin the installation process using one of the following methods:
 - Double-click the file named **VMwareProtect.exe**.
 - Type the file name at a command prompt. Doing so enables you to use one or more command-line options. You should consider this method if you are upgrading a very large database. The `DBCMMANDTIMEOUT` option is used to specify the SQL command timeout value during installation. The default value is 1800 seconds (30 minutes). The recommended value is 15 minutes per GB, so if you have a 4 GB database you should increase the timeout value to 3600 seconds (60 minutes). For example:

```
VMwareProtect /wi:"DBCMMANDTIMEOUT =3600"
```

7. On the **A previous Protect version x.x has been detected on your system. Would you like to upgrade?** dialog, click **Yes**.

A dialog similar to the following is displayed.



8. Click **Install** to install any missing prerequisites.

The Setup Wizard may need to perform a reboot during this portion of the installation process if the Microsoft .NET Framework 4.0 requirement is missing. If a reboot is required, when the machine is restarted the Setup dialog will reappear. Simply click **Install** again to proceed with the upgrade.

The **Welcome** dialog is displayed.

9. Read the information on the **Welcome** dialog and then click **Next**.

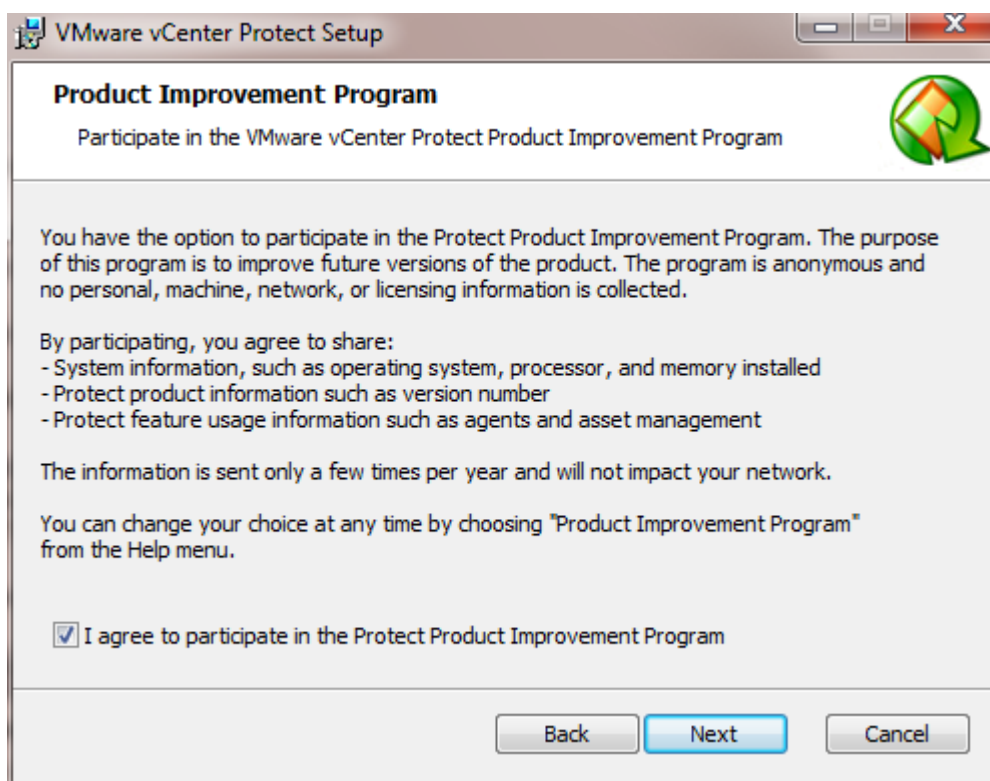
The license agreement is displayed. You must accept the terms of the license agreement in order to install the program.

10. To continue with the installation click **Next**.

The **Destination Folder** dialog is displayed.

11. If you want to change the default location of the program, click the browse button and choose a new location. You also have the option here to install a shortcut icon on your desktop. When you are done, click **Next**.

The **Product Improvement Program** dialog is displayed.



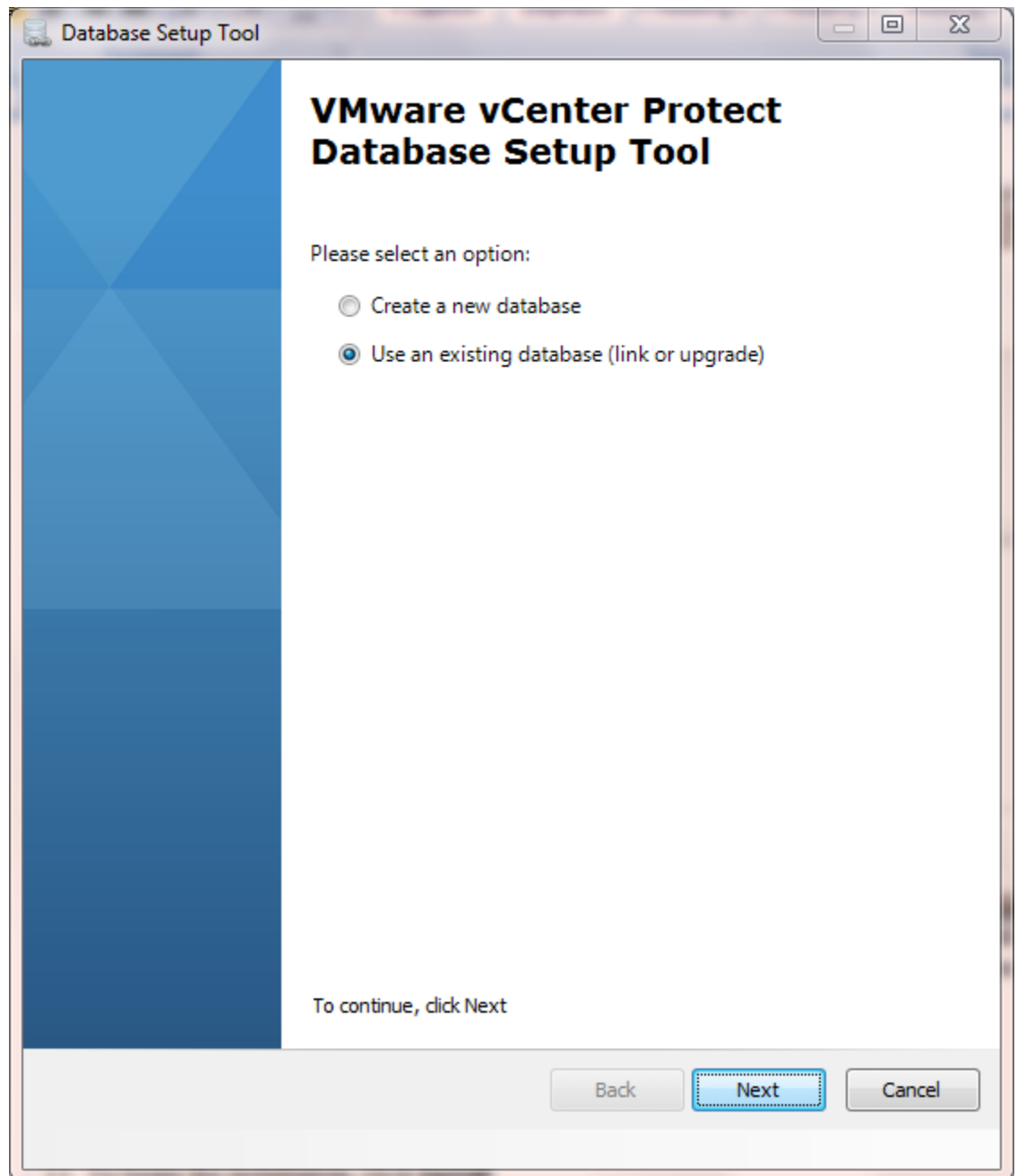
Read the description and decide if you agree to participate in the program. The program enables VMware Inc to collect product usage information that will help improve future versions of the product.

12. Click **Next**.

The **Ready to Install** dialog is displayed.

13. To begin the installation, click **Install**.

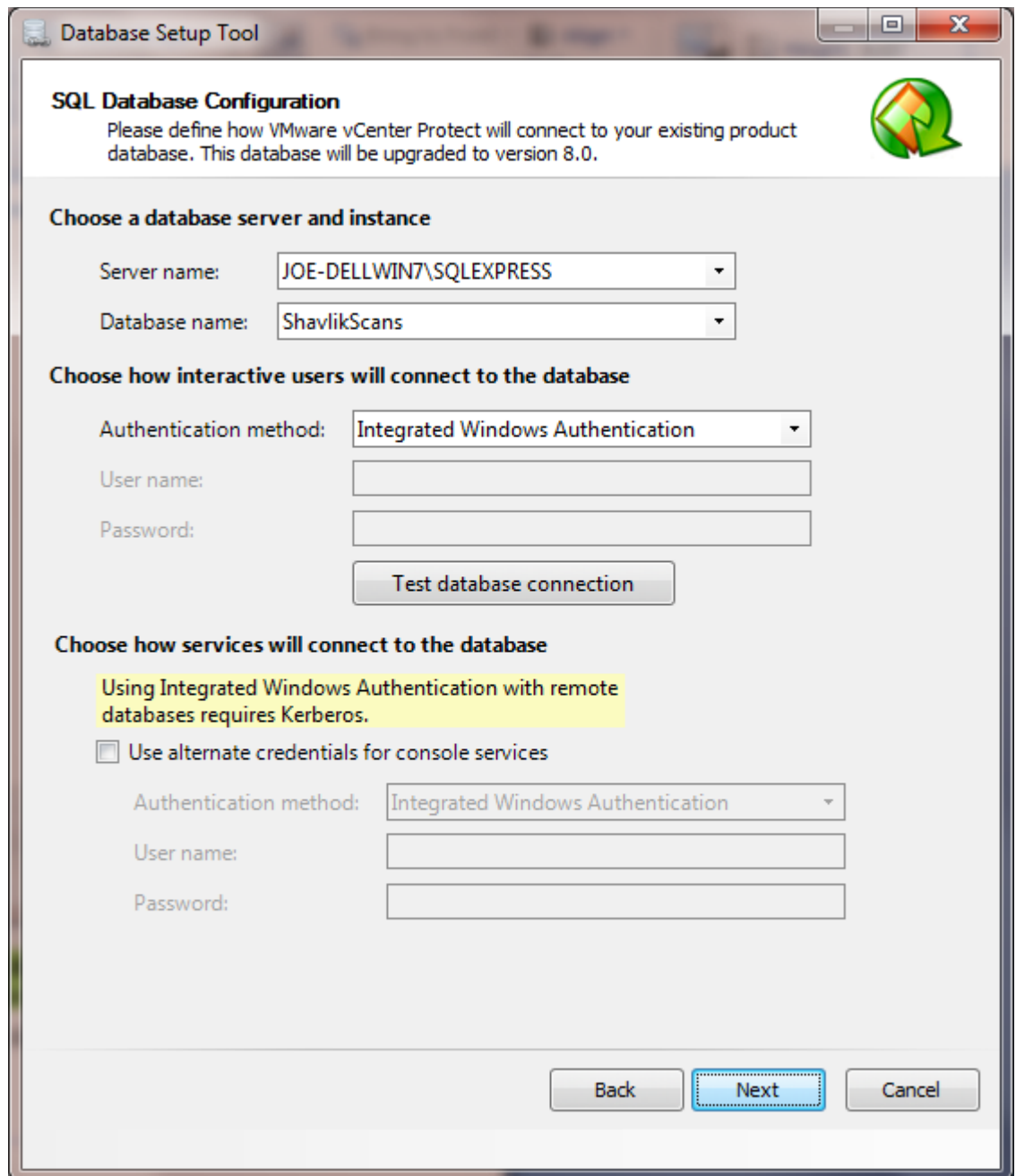
Near the end of the installation process the **Database Setup Tool** dialog is displayed.



Important! In the next step DO NOT select **Create a new database**. If you do a new database will be created and your existing data will not be used.

14. Make sure **Use an existing database** is selected and then click **Next**.

A dialog similar to the following is displayed:



The screenshot shows the 'Database Setup Tool' window with the following configuration:

- SQL Database Configuration**
Please define how VMware vCenter Protect will connect to your existing product database. This database will be upgraded to version 8.0.
- Choose a database server and instance**
 - Server name: JOE-DELLWIN7\SQLEXPRESS
 - Database name: ShavlikScans
- Choose how interactive users will connect to the database**
 - Authentication method: Integrated Windows Authentication
 - User name: [Empty]
 - Password: [Empty]
 - Test database connection button
- Choose how services will connect to the database**
 - Using Integrated Windows Authentication with remote databases requires Kerberos.
 - Use alternate credentials for console services
 - Authentication method: Integrated Windows Authentication
 - User name: [Empty]
 - Password: [Empty]
- Navigation buttons: Back, Next (highlighted), Cancel

15. Use the boxes provided to define how users and services will access the SQL Server database.

Choose a database server and instance

- **Server name:** You can specify a machine or you can specify a machine and the SQL Server instance running on that machine.
- **Database name:** Specify the database name you want to use. The default database name in versions prior to 8.0 is **ShavlikScans**.

Choose how interactive users will connect to the database

Specify the credentials you want the program to use when a user performs an action that requires access to the database.

- **Integrated Windows Authentication:** This is the recommended and default option. VMware vCenter Protect will use the credentials of the currently logged on user to connect to the SQL Server database. The **User name** and **Password** boxes will be unavailable.
- **Specific Windows User:** Select this option only if the SQL Server database is on a remote machine. This option will have no effect if the database is on the local (console) machine. (See *Supplying Credentials* in the **VMware vCenter Protect Administration Guide** for more information about local machine credentials.) All VMware vCenter Protect users will use the supplied credentials when performing actions that require interaction with the remote SQL Server database.
- **SQL Authentication:** Select this option to enter a specific user name and password combination when logging on to the specified SQL Server.

Caution! If you supply SQL authentication credentials and have not implemented SSL encryption for SQL connections, the credentials will be passed over the network in clear text.

- **Test database connection:** To verify that the program can use the supplied interactive user credentials to connect to the database, click this button.

Choose how services will connect to the database

Specify the credentials you want the background services to use when making the connection to the database. These are the credentials that the results importer, various agent operations, and other services will use to log on to SQL Server and provide status.

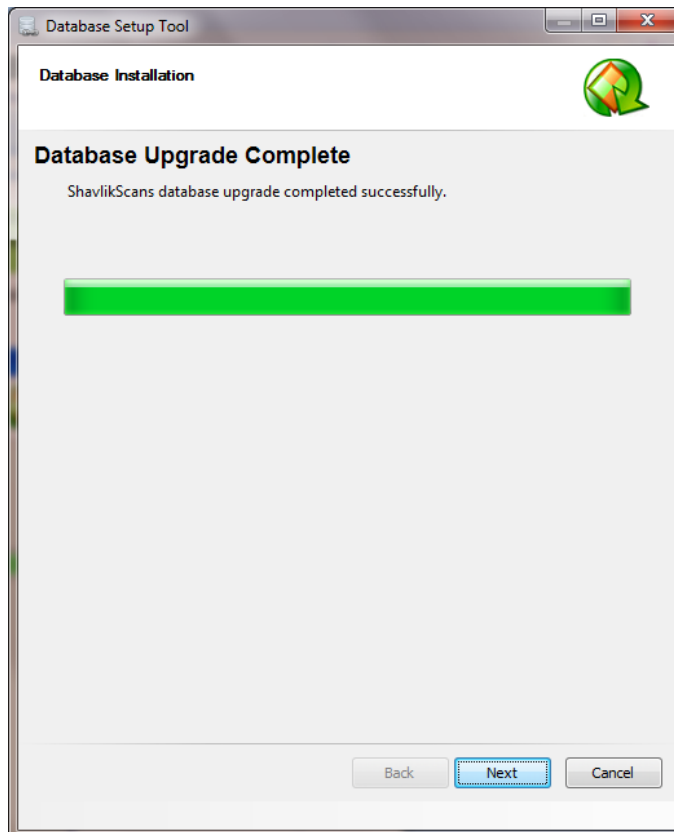
- **Use alternate credentials for console services:**
 - If the SQL Server database is installed on the local machine you will typically ignore this option by **not** enabling this check box. In this case the same credentials and mode of authentication that you specified above for interactive users will be used.
 - You will typically only enable this check box if the SQL Server database is on a remote machine. When the database is on a remote machine you need an account that can authenticate to the database on the remote database server.
- **Authentication method:** Available only if **Use alternate credentials for console services** is enabled.
 - **Integrated Windows Authentication:** Selecting this option means that the machine account will be used to connect to the remote SQL Server. The Kerberos network authentication protocol must be available in order to securely transmit the credentials. The **User name** and **Password** boxes will be unavailable.

Note: If you choose **Integrated Windows Authentication** the installation program will attempt to create a SQL Server login for the machine account. If the account creation process fails, see *SQL Server Post-Installation Notes* in the *VMware vCenter Protect 8.0 Installation Guide* for instructions on manually configuring a remote SQL Server to accept machine account credentials. Do this after you complete the VMware vCenter Protect upgrade process but before you start the program.

- **Specific Windows User:** Select this option to enter a specific user name and password combination. VMware vCenter Protect's background services will use these credentials to connect to the SQL Server database. This is a good fallback option if for some reason you have difficulties implementing integrated Windows authentication.
 - **SQL Authentication:** Select this option to provide a specific user name and password combination for the services to use when logging on to SQL Server.
16. After providing all the required information, click **Next**.

Note: If the installation program detects a problem with any of the specified credentials, an error message will be displayed. This typically indicates that a user account you specified does not exist. Make a correction and try again.

Your database is upgraded to the 8.0 format. When the database upgrade is complete the following dialog is displayed:



17. Click **Next**.
18. On the **Installation Complete** dialog click **Finish**.
19. On the **Completed the VMware vCenter Protect Setup Wizard** dialog, enable the **Launch VMware vCenter Protect** check box and then click **Finish**.

UPGRADE TASKS PERFORMED ON THE CONSOLE

In order to complete the upgrade, the following tasks must be performed on the VMware vCenter Protect console.

Reset Your Agent Proxy and Email Credentials

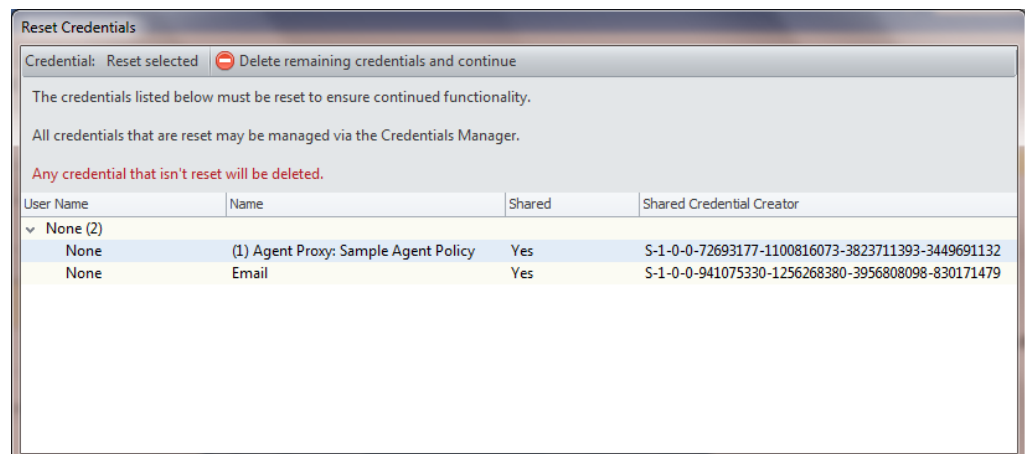
This task is necessary if you had agent proxy credentials and/or email credentials defined in your previous version of the program.

1. If needed, start VMware vCenter Protect.

The program should have started automatically if you enabled the **Launch VMware vCenter Protect** check box in the final dialog of the upgrade process. If you forgot to enable this check box, simply start the program yourself using the Windows Start menu.

The **Reset Credentials** dialog is displayed. For example:

Note: If the **Reset Credentials** dialog is NOT displayed it means you have no credentials that require immediate action and you can simply skip this section.



Due to changes in the way the program now handles credentials, the agent proxy credential and the email credential you had defined in the previous version of the program must be reset. If you don't reset a credential it will no longer be available in the upgraded program and the services that require the credential will no longer work.

Note: If you choose not to reset a credential and then later realize that it is needed, you will be able to add it back later using the VMware vCenter Protect interface.

2. Select a credential and then click **Reset selected**.

The **Define Credential** dialog is displayed. For example:

Define Credential

Name this credential so it can be used elsewhere:

(1) Agent Proxy: Sample Agent Policy

Reset the credential:

User name: Joe-DellWin7\Joe

Password:

Verify password:

Share this with background tasks, Agents, and other features

[What are the security implications?](#)

Creating a new credential here requires sharing it with the service.

Save Cancel

3. Provide the following information:

- **Name this credential so it can be used elsewhere:** This friendly name is something that will help you recognize the purpose of the credential when you see it in other areas of the program. You can choose to use the default friendly name or you can specify your own.
- **User name:** By default the name of the currently logged on user will be used. Change this if necessary.
- **Password:** You must respecify the password used with this credential. The program has no way of decrypting the original credential to extract the password so it is mandatory for you to supply it here.

Note: If you don't remember the password do not guess. It is better to cancel this operation and delete the credential than it is to provide bad information. You can add the credential back later when you learn the correct credential information.

- **Verify password:** Retype the password.

4. Click **Save**.

The credential is reset and then removed from the **Reset Credentials** dialog.

5. Repeat Steps 2 – 5 until you have reset all desired credentials.

6. (Conditional) If there are credentials remaining in the list that you do not want to reset, click **Delete remaining credentials and continue**.

The VMware vCenter Protect home page is displayed.

Assign Aliases to the Console

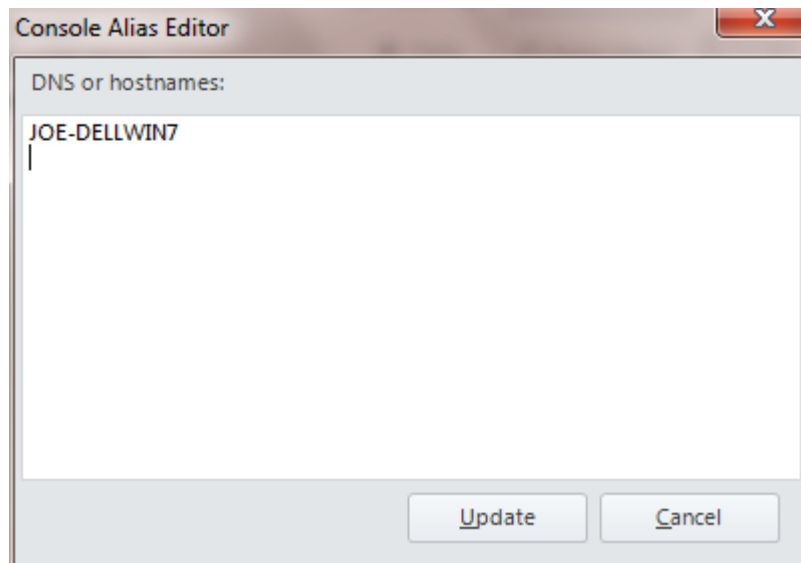
This task is necessary only if you use agents and if one of the following conditions exists:

- You have assigned the console machine to a new domain
- You have given the console a new common name or IP address
- You manually installed your agents and they use an IP address to communicate with the console

Under these conditions you must use the **Console Alias Editor** tool to identify the old console names or addresses as trusted aliases. If you don't, when an agent checks in with the VMware vCenter Protect console it will not be able to verify that the machine it contacted is a trusted machine.

1. Select **Tools > Console Alias Editor**.

The **Console Alias Editor** dialog is displayed. It will contain the names and IP addresses currently used to identify the console machine. For example:

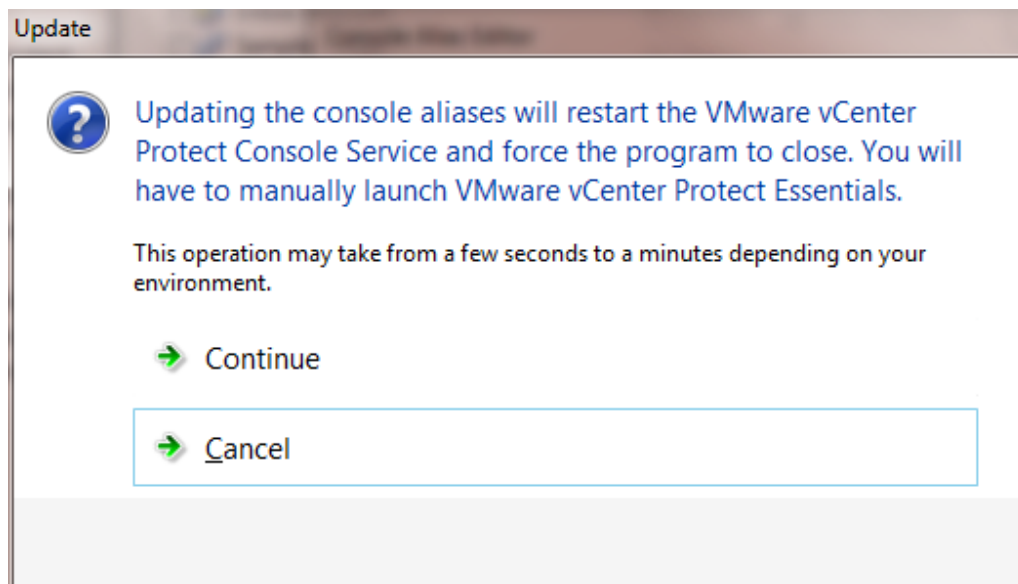


2. Type the names and/or IP addresses that you want to use as an alias for the console machine.

You can specify IP addresses using either an IPv4 or IPv6 format.

3. Click **Update**.

The following dialog is displayed:



In order to update the console aliases the console service must be restarted and VMware vCenter Protect must be closed and then manually restarted.

IMPORTANT! The agents will not recognize a new alias until after they check-in with the restarted console. The check-in must be initiated by an agent either manually using the agent client program or via a scheduled check-in; a check-in command issued from the console to an agent will not update the console certificate.

Synchronize Your Distribution Servers

You must update your distribution servers with the latest patches and/or scan engines and XML definition files contained on the console. This is particularly important if your agents use distribution servers to download these files. The distribution servers must be synchronized with the updated console files **prior** to the agents performing their check-in.

To synchronize your distribution servers:

1. Select **Help > Refresh Files** to make sure the console contains all the latest files.
2. Select **Manage > Distribution Servers** and then select the **Synchronize** tab.
3. In the bottom half of the dialog, select all the distribution servers in the list and then click **Synchronize engines and definitions**.

Don't worry if the agents happen to check in before you have finished synchronizing the distribution servers. The agents will be updated the next time they perform their check-in.

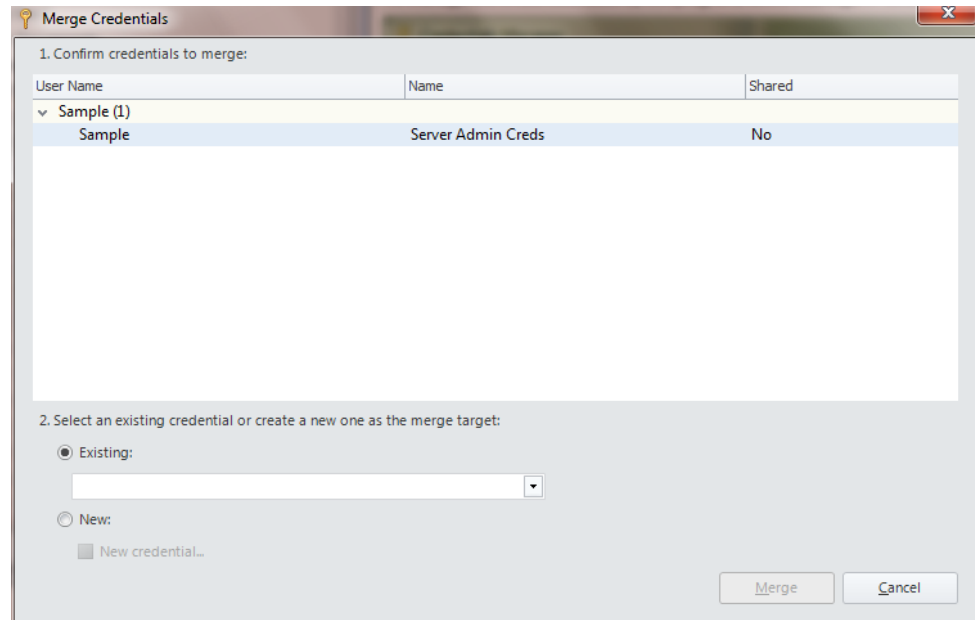
Consolidate Duplicate Credentials

It is strongly recommended that you use the Credentials Manager to review your current list of credentials and consolidate any duplicate credentials. Why might there be duplicate credentials? The most likely reason is that in the previous version of the product you may have used the same user name/password pair for several different purposes, and that same credential may now be identified by several different friendly names. By consolidating duplicate credentials you will reduce confusion when performing any console management tasks that involve the selection of a credential. And if your organization's security policy requires all credentials to change on a periodic basis, consolidating credentials will also greatly reduce maintenance time because you will have far fewer credentials to update.

To consolidate credentials:

1. Access the Credentials Manager by selecting **Manage > Credentials**.
2. Select the credential you want to merge with another credential and then click **Merge**.

The **Merge Credentials** dialog is displayed. For example:



3. At the bottom of the dialog do one of the following:
 - Select an existing credential: The credential(s) specified in the **Confirm credentials to merge** list will be merged with the credential you select here.
 - Create a new credential: The credential(s) specified in the **Confirm credentials to merge** list will be merged with the new credential you create here.

Note: A shared credential can only be merged with another shared credential. Therefore, if any of the credentials in the **Confirm credentials to merge** list are shared, then (1) only shared credentials will be offered for selection in the **Existing** box, and (2) any new credential you create will automatically be defined as a shared credential.

4. Click **Merge**.
5. Read the message on the confirmation dialog and if you agree with the merger, click **Merge**.
6. Repeat Steps 2 – 5 until you have consolidated all duplicate credentials.

Reset Your Agent Check-In Frequency

If at the very beginning of the upgrade procedure you temporarily changed the check-in frequency in your agent policy, you should change it back to its original setting.

1. Verify that all agents have checked in since the upgrade was performed.

In Agent Manager, use the **Last Agent Check In** column to verify that your agents have recently checked in.

2. On the **General Settings** tab of your agent policy, change the **Check-In interval** back to its original value.

SIGNIFICANT CHANGES & ENHANCEMENTS IN VMWARE vCENTER PROTECT 8.0

New Product Name

Shavlik Technologies is now part of VMware. To reflect this acquisition, beginning with version 8.0 the product name has changed from Shavlik NetChk Protect to VMware vCenter Protect.

Support for the Use of PowerShell Scripts

Windows PowerShell is a task automation framework. It is built on Microsoft .NET Framework and provides administrators the ability to quickly and easily perform management tasks on Windows machines and applications. The ITScripts function of VMware vCenter Protect supports the use of PowerShell 2.0 and WinRM 2.0, enabling you to execute a variety of scripts on the console and on remote target machines.

Credentials Manager

The Credentials Manager is now used to manage all credentials used within the program. It is also used to set the default credential for the program.

Although you can supply new credentials from several different areas of the program, all of the credentials can be edited and deleted from this single location. This greatly simplifies the credentials management process. For example, if a password that is used to authenticate a specific group of machines changes, you simply use the Credentials Manager to update the associated credential. All items assigned to that credential are automatically updated with the new password.

Remote Desktop Protocol Integration

The Microsoft Remote Desktop Protocol (RDP) provides the ability to remotely manage Windows-based machines over a network connection. RDP capabilities are supported in VMware vCenter Protect, enabling you to use stored machine credentials to quickly connect the VMware vCenter Protect console to a target machine. With Remote Desktop you can access the target machine's programs, files, and resources as if you were physically sitting in front of the machine. For a complete list of the features of Remote Desktop, please visit any number of sites on the Web.

Power Status Scan

You can easily determine the current power status of one or more machines in your organization. From either Machine View or Scan View you simply right-click the desired machines and select **Power > Status Scan**. The results are available from the Results pane or by generating a Power Status report.

Multiple Administrator Support

VMware vCenter Protect now contains a number of built-in protections that allow two or more administrators to safely access the program at the same time. There are two basic scenarios in which multiple administrators might typically be used.

- Two or more administrators on the same console machine
- Two or more consoles sharing one database

Details are provided in the Help system.

Home Page Changes

The home page has been redesigned. It is now a completely functional area, enabling you to perform patch, asset, power, and ITScripts operations quickly and easily. In addition, the charts have been moved to their own dedicated page, providing a larger area in which to view the information.

Machine Group Changes

The top section of the machine group interface has been reworked. The option to select a template has been removed and you now initiate all actions using the new **Run operation** button. All decisions for performing the desired operation are now selected on the new **Run Operation** dialog, which closely mirrors the redesigned home page.

Managed Machine Changes

You can now define several additional properties for each machine contained in VMware vCenter Protect's database of managed machines. The new properties include:

- Credential
 - RDP port
 - ITScripts port
-

Console Alias Editor

This is a new tool that enables you to identify trusted aliases for the console. The aliases are referenced by agents checking in with the console. The most common time to use this tool will be during an upgrade from an earlier version of VMware vCenter Protect.

Background info: When an agent checks in with the VMware vCenter Protect console it must verify that the machine it contacted is a trusted machine. It does this using the trusted names and IP addresses contained in the certificate that is exchanged between the agent and the console. If you assign the console machine to a new domain or give it a new common name or IP address, any existing agents that recognize the console by its old name or address will no longer trust the console machine. To get around this issue you simply identify the old console names or addresses as trusted aliases. This is done using the **Console Alias Editor** tool.

Threat Integration with Windows Action Center

When you install an agent that contains a threat task, Windows Action Center will now acknowledge that the machine is using VMware vCenter Protect Agent as its security program. You can use Windows Action Center to:

- Update data
- Enable Active Protection when it is disabled
- View the state of virus protection and spyware protection