NetWitness® Platform XDR

Version 12.2.0.0

Windows Legacy Collection

NETWITNESS
Platform XDR

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

March, 2023

Contents

NetWitness Legacy Windows Collection Update & Installation Instructions

NetWitness Legacy Windows collection collects event data from multiple Windows Event Source domains.

It supports collection from:

- Windows 2003 and earlier event sources
- NetApp ONTAP host evt files

This document contains the following sections:

Setup Requirements

This section provides the NetWitness Legacy Windows Collector Setup requirements.

Caution: If you are installing or updating to version 11.x, in order to use the Security Analytics Legacy Windows Collector with NetWitness, you need to first install the following windows updates:

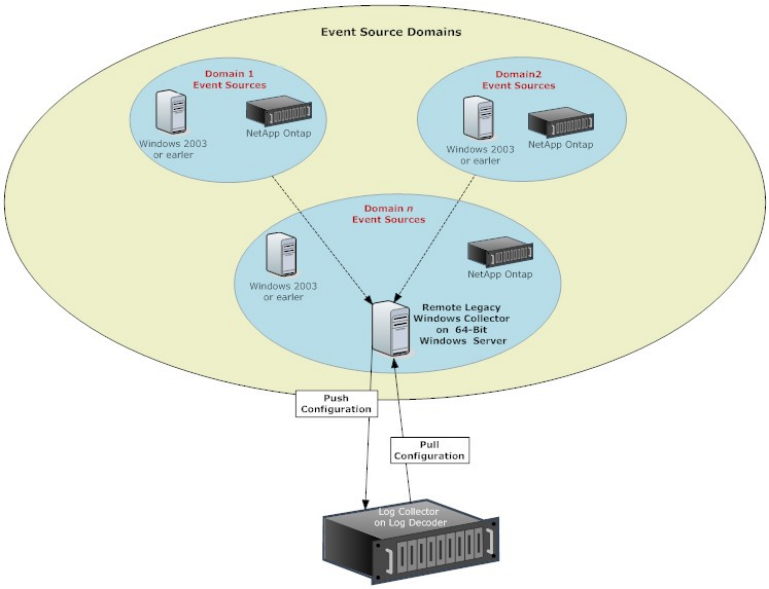
• KB2919355
• KB2919442
• KB2999226
• KB3173424

If these updates are not installed, you will get an error message, and the Legacy Windows Collector will not be installed.

To set up the NetWitness ® Platform Legacy Windows Collector, you need:

- Any of the following physical or virtual systems that can reach the Windows 2003 event source domains:
  - Windows 2008 R2 SP1 64-Bit Server,
  - Windows 2012 Server, or
  - Windows 2016 Server, or
  - Windows 2019 Server
- A minimum of 20% free disk space. For example, you need at least 20 GB of free space if your system drive is 100 GB in size.

IMPORTANT: Do not install the Legacy Windows Collector on a domain controller.



- For NetWitness Platform 11.6 and Later (Upgrade and Fresh Install), you must download and install Visual studio 2019 x64 runtime before running the Windows Legacy Collector installer. You can download the Visual Studio 2019 x64 at https://support.microsoft.com/en-us/help/2977003/the-latest-supported-visual-c-downloads.

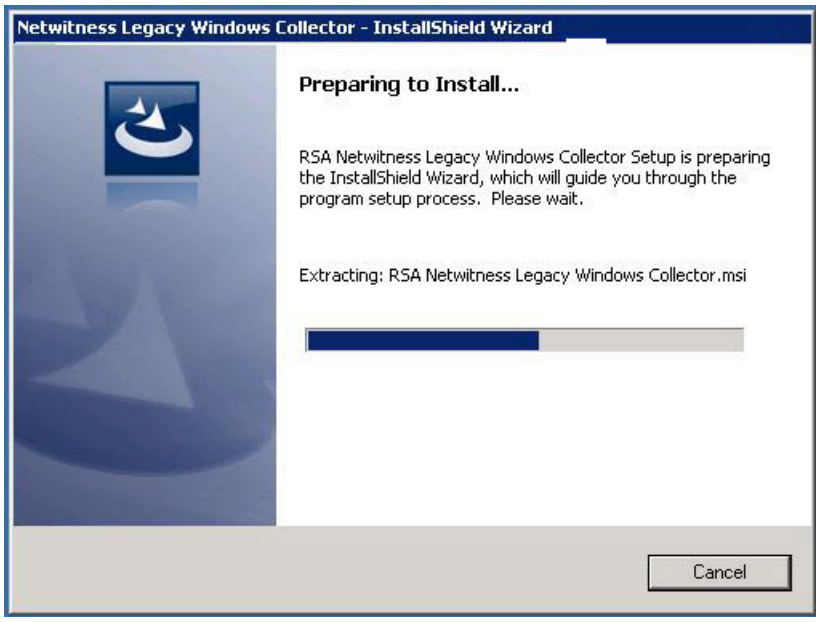
Update the NetWitness Legacy Windows Collector from 10.6.x to 12.0

This section tells you how to update the NetWitness 10.6.x Legacy Windows Collector to 12.0

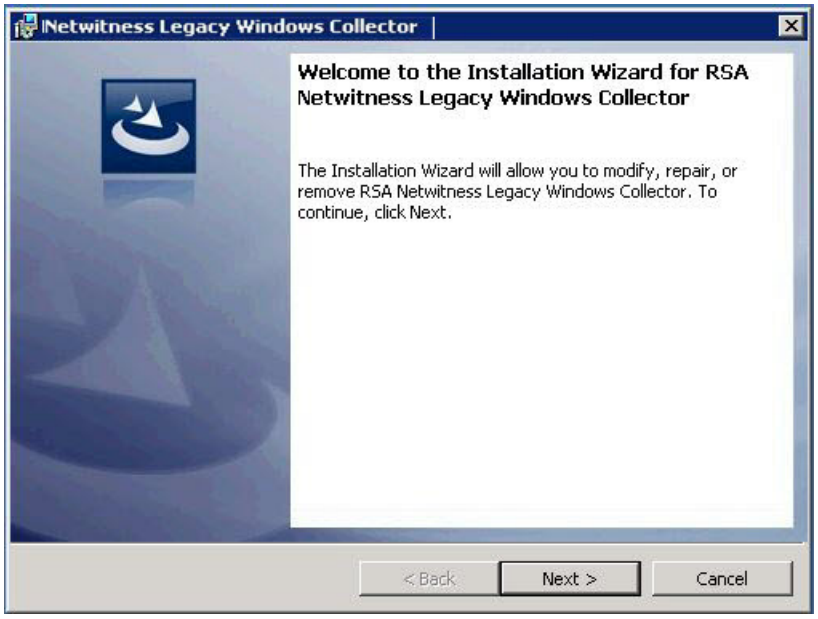
To update the NetWitness 10.6.x Legacy Windows Collector to 12.0 on a Windows 64-Bit server:

1. Depending on your version of NetWitness, navigate to one of the following URLs on NetWitness Community:
   - For NetWitness 11.6.1.1, go to https://community.netwitness.com//t5/netwitness-platform-downloads/rsa-netwitness-platform-11-6-1-1-patch-download/ta-p/643401 and click **NetWitness Platform 11.6.1.1 Upgrade Pack to download the ZIP archive**.
   - For NetWitness 11.6, go to https://community.netwitness.com/t5/netwitness-platform-downloads/rsa-netwitness-11-6-legacy-windows-collector-download/ta-p/606860 and click **NetWitness Logs & Network 11.6 Legacy Windows Collector** to download the ZIP archive.
   - For NetWitness 11.5, go to https://community.netwitness.com/t5/netwitness-platform-downloads/rsa-netwitness-11-5-legacy-windows-collector-download/ta-p/572571 and click **NetWitness Logs & Network 11.5 Legacy Windows Collector** to download the ZIP archive.
   - For NetWitness 11.4, go to https://community.netwitness.com/t5/netwitness-platform-downloads/rsa-netwitness-11-4-legacy-windows-collector-download/ta-p/565269 and click **NetWitness Logs & Packets 11.4 Legacy Windows Collector** to download the ZIP archive.
   - For NetWitness 11.3, go to https://community.netwitness.com/t5/netwitness-platform-downloads/rsa-netwitness-11-3-legacy-windows-collector-download/ta-p/556065 and click **NetWitness Logs & Packets 11.3 Legacy Windows Collector** to download the ZIP archive.
   - For NetWitness 11.2, go to https://community.netwitness.com/t5/netwitness-platform-downloads/rsa-netwitness-11-2-legacy-windows-collector-download/ta-p/526984 and click **NetWitness Logs & Packets 11.2 Legacy Windows Collector** to download the ZIP archive.
   - For NetWitness 11.1, go to https://community.netwitness.com/t5/netwitness-platform-downloads/rsa-netwitness-11-1-legacy-windows-collector-download/ta-p/551450 and click **NetWitness Logs & Packets 11.1 Legacy Windows Collector** to download the ZIP archive.
2. Unzip the downloaded file.
3. Log on to a Windows 2008, 201, 2016, or 2019 Server.
4. Copy **NWLegacyWindowsCollector-*version-number*.exe** to the Windows Server.
5. Right click on **NWLegacyWindowsCollector-*version-number*.exe** and select **Run As Administrator**.

   The Preparing to Install…. page of update installation wizard is displayed.

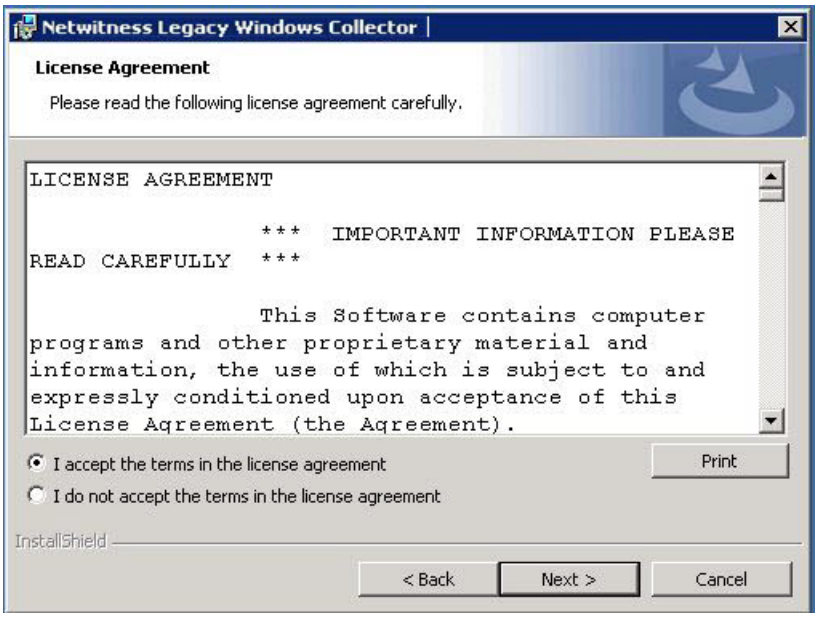


After the update installation program extracts NetWitness Legacy Windows Collector installation files, the **Welcome** page is displayed.



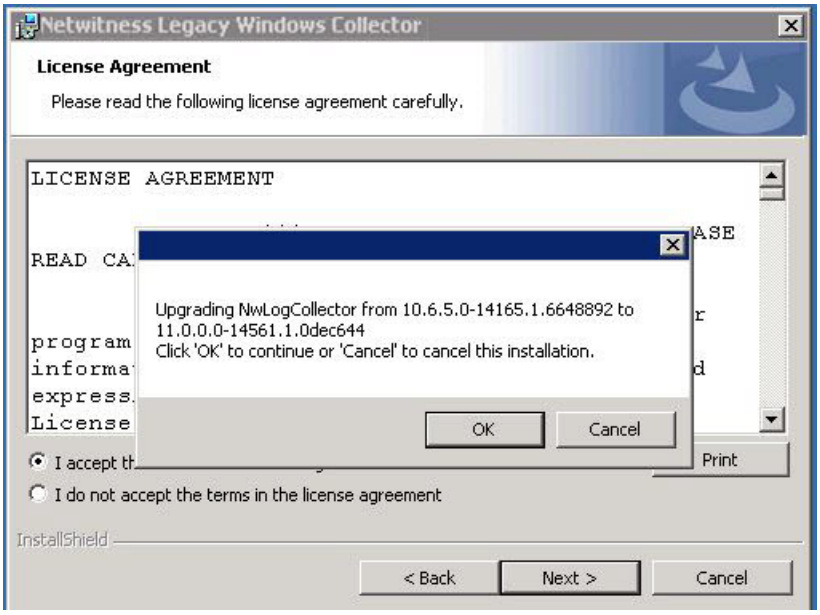
6. Click **Next**.

   The License Agreement page is displayed.



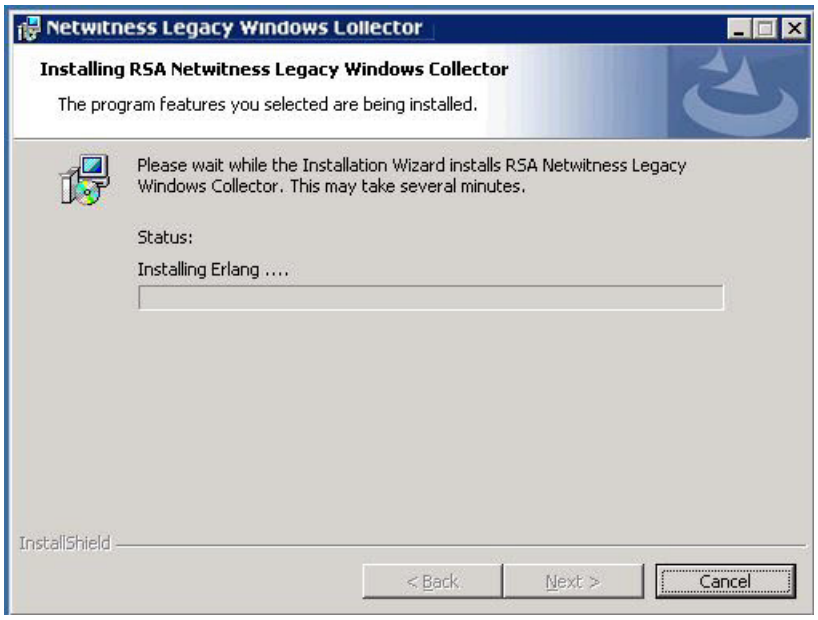
7. Read the License agreement carefully, select the **I accept the terms in the license agreement** radio button, and click **Next**.

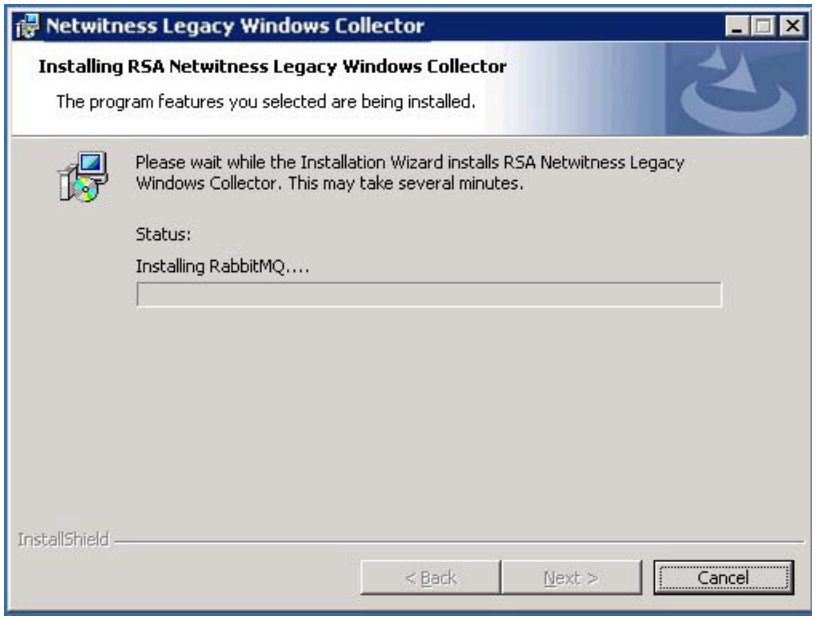
   Before it starts the update, the wizard asks if you want to continue or cancel the installation of the update.



8. Click **OK** to continue installing the update.
9. Click Install.

   The Installation screens for the Legacy Windows Collector page is displayed.

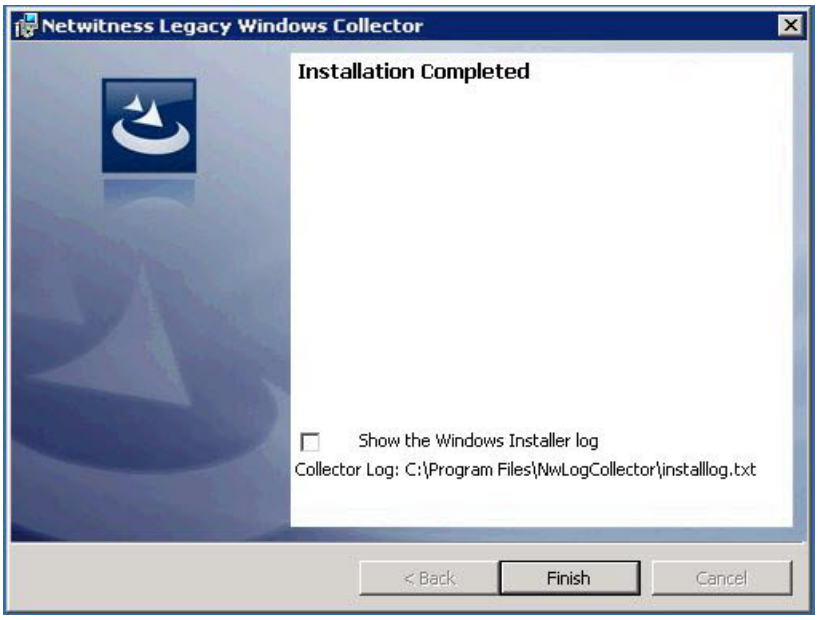




After the update installation completes, the **Next** button becomes active.

10. Click **Next**.

    The Installation Completed page is displayed.



11. (Optional) If you want to review a log of the update installation, select the **Show the Windows Installer** log checkbox.
12. Click **Finish**.
13. Reboot the machine.

This completes the update of the Legacy Windows Collector to NetWitness 12.0.

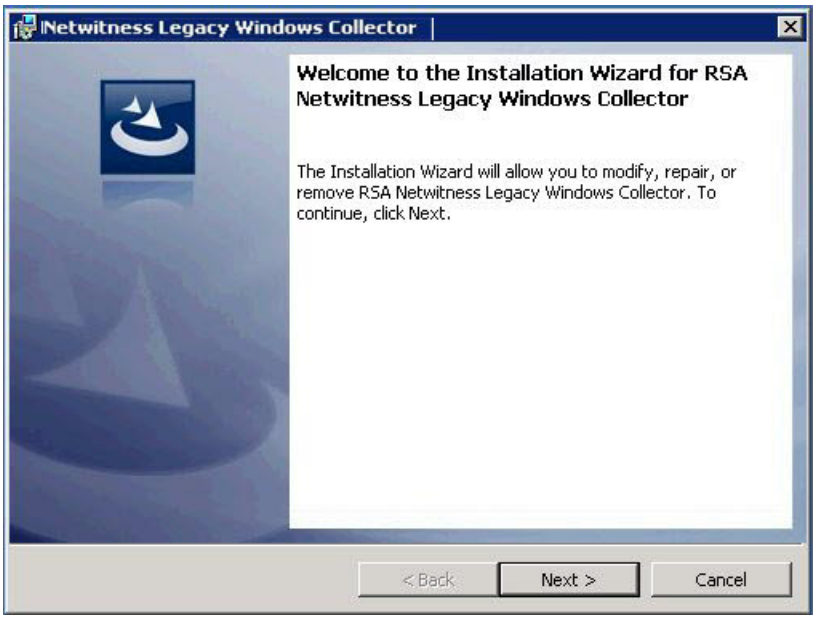
Fresh Install 12.0 Legacy Windows Collector

This section describes how to install the 12.0 Legacy Windows Collector on a Windows 2008, 2012, 2016, or 2019 64-Bit server

To install the NetWitness Legacy Windows Collector on a Windows 2008, 2012, 2016, or 2019 64-Bit server:

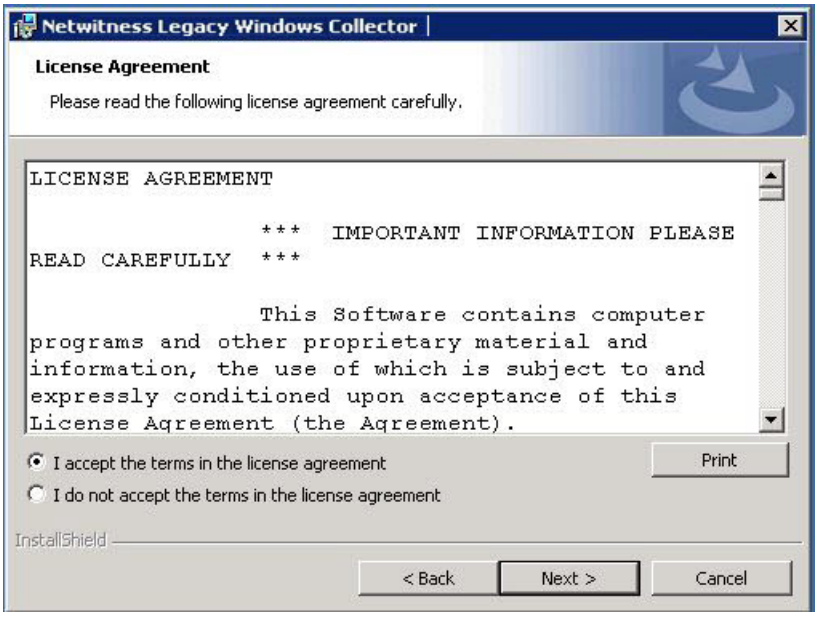
1. Depending on your version of NetWitness Platform, navigate to one of the following URLs on NetWitness Community:
   - For NetWitness 11.6.1.1 only, navigate to https://community.netwitness.com//t5/netwitness-platform-downloads/rsa-netwitness-platform-11-6-1-1-patch-download/ta-p/643401 on NetWitness Community. Click NetWitness Logs & Network 11.6.1.1 Legacy Windows Collector to download the ZIP archive.
   - For NetWitness 11.6, navigate to https://community.netwitness.com/t5/netwitness-platform-downloads/rsa-netwitness-11-6-legacy-windows-collector-download/ta-p/606860 on NetWitness Community. Click NetWitness Logs & Packets 11.6 - Legacy Windows Collector to download the ZIP archive.
   - For NetWitness 11.7, navigate to https://community.netwitness.com/t5/netwitness-platform-downloads/rsa-netwitness-11-7-legacy-windows-collector-download/ta-p/644208 on NetWitness link. Click NetWitness Platform 11.7 Legacy Windows Collector to download the ZIP archive.
   - For NetWitness 12.0, navigate to https://community.netwitness.com/t5/rsa-netwitness-platform-staged/netwitness-12-0-legacy-windows-collector-download/ta-p/684864 on NetWitness link. Click NetWitness Platform 12.0 Legacy Windows Collector to download the ZIP archive.
2. Unzip the downloaded file.
3. Copy the **NWLegacyWindowsCollector-*version-number*.exe** to the Windows Server.
4. Right click on the **NWLegacyWindowsCollector-*version-number*.exe** and select **Run As Administrator**.

   The **Welcome** page of installation wizard is displayed.



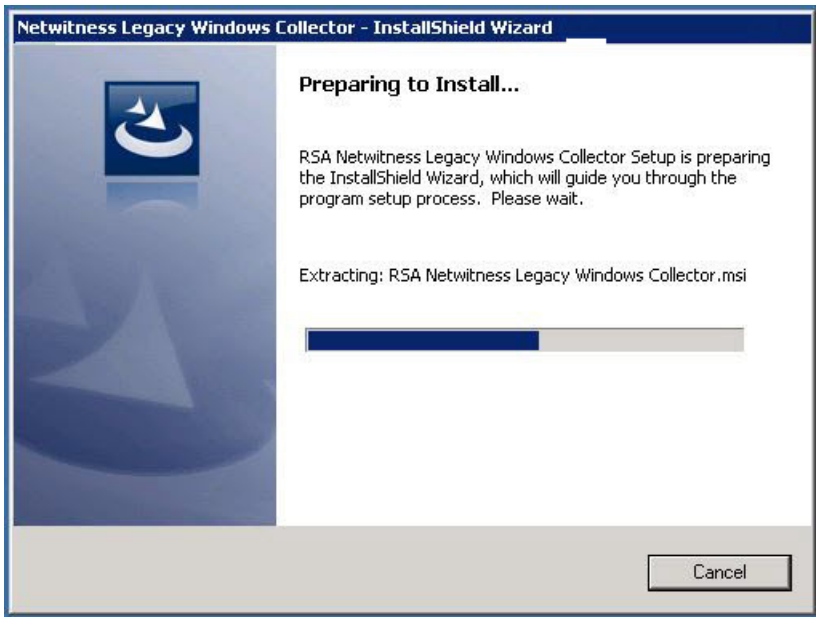
5. Click **Next**.

   The License Agreement page is displayed.



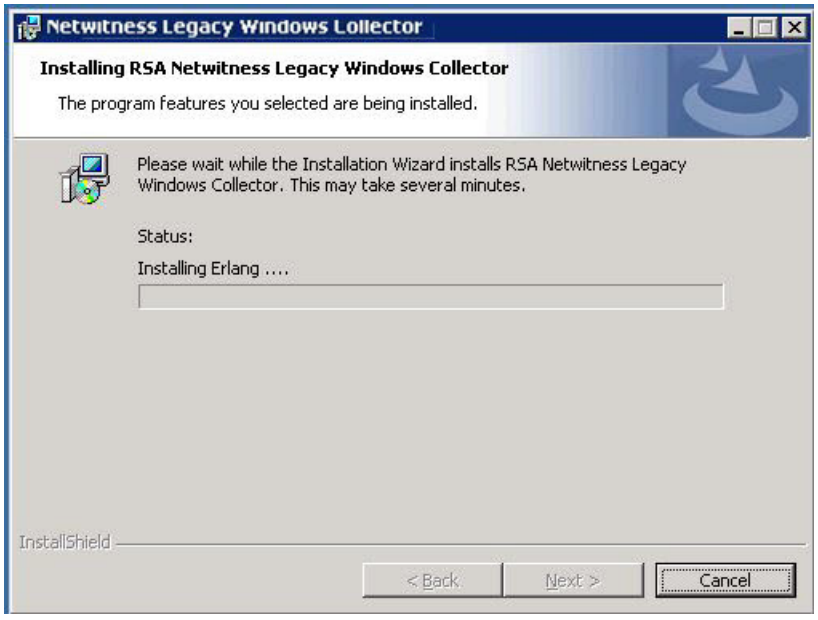
6. Read the License agreement carefully, select the **I accept the terms in the license agreement** radio button, and click **Next**.

   The Ready to Install the Program page is displayed.

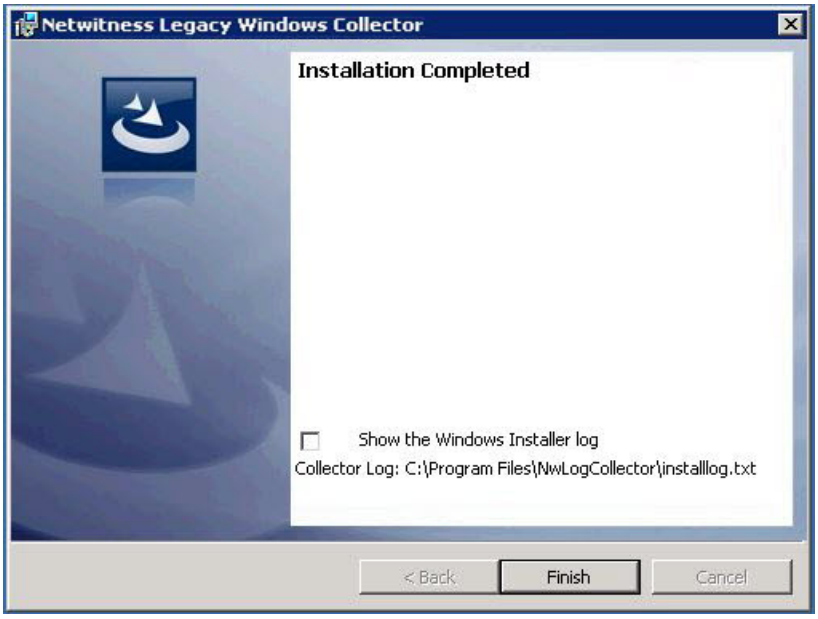


7. Click **Install**.

   The Installation screens for the Legacy Windows Collector page are displayed.



The Installation Completed page is displayed.



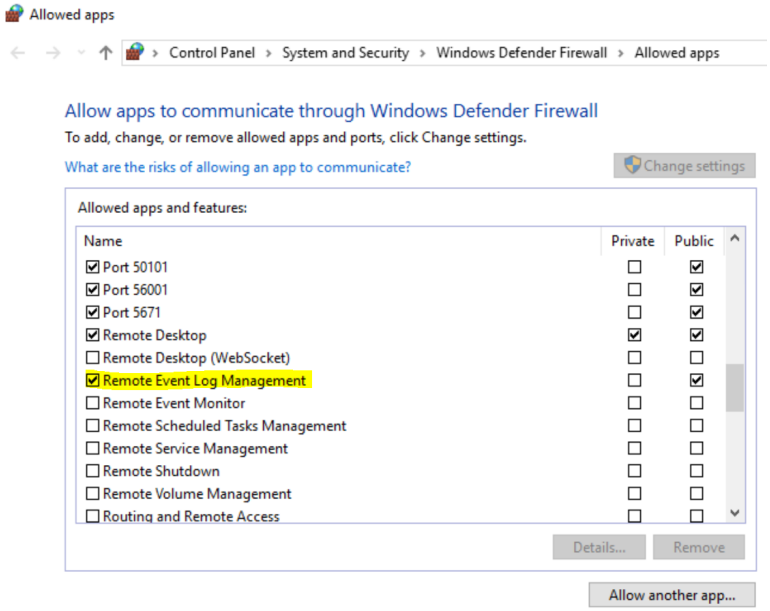
8. (Optional) If you want to review a log of the installation, select the **Show the Windows Installer** log checkbox.
9. Click **Finish**.
10. Reboot the machine.

This completes the installation of the 12.0 Legacy Windows Collector. Please refer to the **Windows Legacy and NetApp Collection Configuration Guide** on NetWitness Community for instructions on how to configure Legacy Windows collection in NetWitness.

Configure the Windows Server

For the NetWitness to communicate with the Windows Server, you need to allow Remote Event Log Management on the Windows Server.

1. On the Windows Server, in Services, start the Remote Registry Service.
2. In Firewall, enable Remote Event Log Management for your network, as shown below.



Change the Windows Legacy Collector IP Address

Note: The procedures in this section apply to NetWitness 11.5 and later only.

On occasion, you may need to change the IP address of your Windows Legacy Collector. You may also need to edit any Destination Groups that you have configured.

Change WLC IP Address

The following procedure describes how to change the IP address for your system.

1. Log onto the Windows Legacy Collector system and manually change the IP address on the system.
2. In the UI, confirm that the Log Collector service corresponding to the WLC system shows up in error (Red). It might take some time for it to reflect the changed status.
3. On the NetWitness Server, use the **nw-manage** utility to view the host information for the WLC using the following command:

   ```
   nw-manage --list-hosts
   ```

   Sample output from running the command is shown here:

   ```
   {
   "id" : "fdb8150c-e040-459e-8cc5-3c60ec2c65ae",
   "displayName" : "WLC-HOST-104",
   "hostname" : "10.101.216.102",
   "ipv4" : "10.101.216.102",
   "ipv4Public" : null
   } ]
   ```

   You use the value of **"id"** from your output in the following step.
4. Use the **nw-manage** utility to change the IP address of the WLC. For the **host-id** argument, use the value for the **"id"** that you noted from step 3. For the **ipv4** value, use the new IP Address to which you are changing.

   ```
   nw-manage --update-host --host-id "fdb8150c-e040-459e-8cc5-3c60ec2c65ae" --
   ipv4 10.101.216.105
   ```
5. After you see the message that the previous command ran successfully, go to the NetWitness Server UI and verify that the WLC service is running without any errors.

Edit Destination Groups For Log Collectors and VLCs

The Windows Legacy Collector is often configured with Destination Groups to forward events to Log Collectors or Virtual Log Collectors. If the IP address of any such Destination LC or VLC is changed, the Windows Legacy Collector can no longer forward events. To remediate this, you must edit the Destination groups for the WLC, making sure to select the new LC or VLC IP Address.

Troubleshoot a Fresh or Upgrade Install

Logs to Examine for Information

Refer to the following log files if you need to troubleshoot problems:

- `%systemDrive%\Netwitness\ng\logcollector\MessageBroker.log`
- `%systemDrive%\Program Files\NwLogCollector\installlog.txt`

Run `C:\Program Files\NwLogCollector\ziplogfiles.vbs` to generate the ***`hostname`***`_WLCversion_timestamp.zip` that contains all the log files and other information needed for troubleshooting.

Issues with the Lockbox

When you create a lockbox password on a new Windows Legacy Collector, you might see the following error:

```
failed to set secure storage password: failed to create lockbox: The Lockbox or cryptography library could not be found.
```

This can occur if you are running Windows Legacy Collector version 11.x.

If you encounter this issue, download and install both of the following redistributable packages:

- Visual C++ 2010: https://www.microsoft.com/en-us/download/details.aspx?id=14632
- Visual C++ 2012: https://www.microsoft.com/en-us/download/details.aspx?id=30679

(Optional) Backup and Restore Legacy Windows Collector

This section tells you how to upgrade from 10.6.4 to NetWitness 12.0 for the Legacy Windows Collector.

Note: You only need to do this if you are changing the Windows VM where you run the Windows Legacy Collector.

During upgrade to NetWitness 12.0, the backup script for the Windows Legacy Collector is invoked automatically, and creates the 10.6.4 configuration and run-time backups. After the 12.0 installation is completed, run the Restore script to restore the configuration and run-time files for the updated Windows Legacy Collection.

Restore the Windows Legacy Collection Backup after Upgrade

To restore the Windows Legacy Collection setup on a newly upgraded NetWitness 11 platform:

1. On the Windows Legacy Collector, open a command prompt window.
2. Navigate to **C:\Program Files\NwLogCollector**, where the scripts are stored.
3. Run the following commands for restoring a backup:
   - Backup configuration files: `WLC-Restore.bat "Config-bkup_`***`timestamp`***`.zip"`
   - Backup run-time files: `WLC-Restore.bat "Runtime-bkup_`***`timestamp`***`.zip"`
4. Once the restore is completed, set the lockbox SSV to use the password that you created during 10.6.4 setup.
   a. In the **Security Analytics** menu, select **Services**, then select your Windows Legacy Collector and choose **Explore**.
   b. From the left navigation pane, expand **logcollection > properties > crypto**.
   c. Run the following command: `op=setssv pw=`***`password_for_10.6.x_lockbox`***, and hit **Send**.

Revert Windows Legacy Collection from 12.0 Back to 10.6.4

To revert the Windows Legacy Collection setup from 12.0 back to 10.6.4:

1. Uninstall the 12.0 Setup. Note the location of the backup folder created by the system during the uninstall procedure.

2. Install the 10.6.4 version of the Windows Legacy Collector.
3. Navigate to **C:\Program Files\NwLogCollector**, where the scripts are stored.
4. Run the Restore script from backup folder present in **C:\Program Files\NwLogCollector** to restore the configuration and run-time setup on the 10.6.4 Windows Legacy Collector.
   - Backup configuration files: `WLC-Restore.bat "Config-bkup_`***`timestamp`***`.zip"`
   - Backup run-time files: `WLC-Restore.bat "Runtime-bkup_`***`timestamp`***`.zip"`
5. Once the restore is completed, set the lockbox SSV to use the password that you created during 10.6.4 setup.
   a. In the **Security Analytics** menu, select **Services**, then select your Windows Legacy Collector and choose **Explore**.
   b. From the left navigation pane, expand **logcollection > properties > crypto**.
   c. Run the following command: `op=setssv pw=`***`password_for_10.6.x_lockbox`***, and hit **Send**.

Add a Windows Legacy Collector Host and Service in NetWitness Platform

For this version of the Windows Legacy Collector, NetWitness has provided a script that replaces the manual steps of adding a Windows Legacy Collector host and service in the NetWitness UI.

To create a Windows Legacy Collector Host and Service in NetWitness:

1. SSH to your NetWitness server.
2. Run the following command:

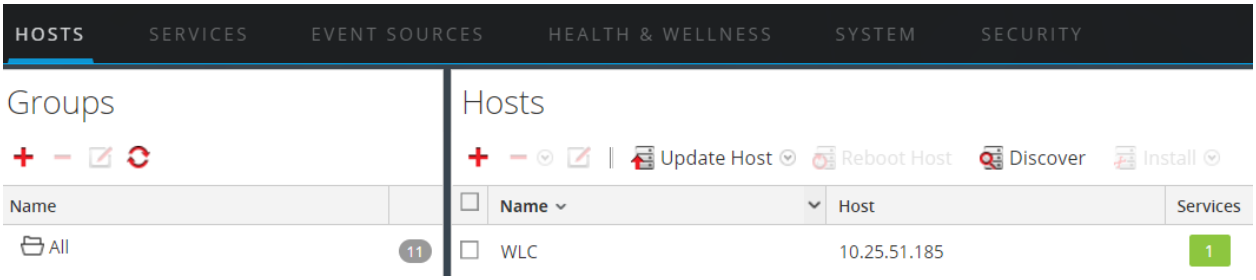
   ```
   wlc-cli-client --host-display-name hostDisplayName --service-display-name
   serviceDisplayName --host WLChostIPAddress --port 50101 --use-ssl false
   ```

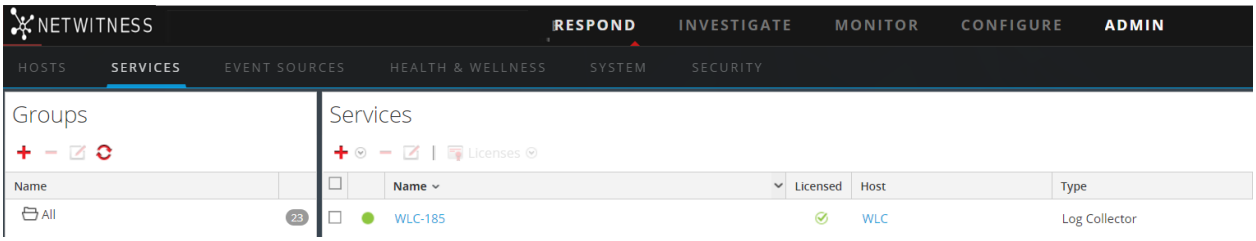
   The parameters are explained below:

   - **--host-display-name**: the name for the host as it is displayed in the NetWitness Hosts page
   - ***--service-display-name***: the name for the host as it is displayed in the NetWitness Services page
   - **--host**: the IP address for the Windows Legacy Collector
   - **--port**: the port NetWitness uses to communicate with the Windows Legacy Collector. The recommended value is 50101.
3. You will be prompted to supply the following information:
   - **Windows Log Collector REST Username** and **Windows Log Collector REST Password**: you must supply admin credentials for the Windows Legacy Collector.
   - **Security Server Username** and **Security Server Password**: you must supply admin credentials for NetWitness.

Note: If the **Security Server Password** contains any special character, you must use backslash (\) before the special character. For example, if the password is **netwitness@123**, enter the password as **netwitness\@123**.

After you complete this procedure, you should see the Windows Legacy Collector Host and Service as shown in the following screenshots.




NETWITNESS
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Groups
Name
All
23
Services
Licenses
Name
Licensed
Host
Type
WLC-185
WLC
Log Collector