



Windows Legacy Collection Configuration Guide

for RSA NetWitness® Platform 11.x



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at <https://community.rsa.com> contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

April 2019

NetWitness Legacy Windows Collection Update & Installation Instructions

RSA NetWitness® Platform 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](#)
- [Update the RSA NetWitness® Suite Legacy Windows Collector from 10.6.x to 11.x](#)
- [Fresh Install 11.x Legacy Windows Collector](#)
- [Troubleshooting for Fresh or Upgrade Install](#)
- [\(Optional\) Backup and Restore Legacy Windows Collector](#)
- [Add a Windows Legacy Collector Host and Service in RSA NetWitness® Platform](#)

Setup Requirements

This section provides the RSA NetWitness® Suite 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:

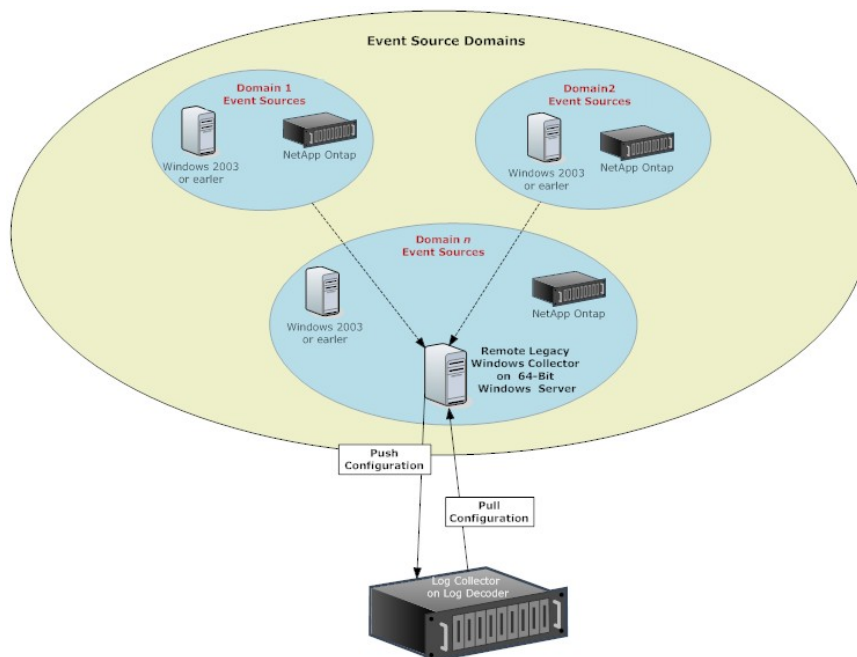
- KB2919355
- KB2919442
- KB2999226
- KB3173424

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 RSA NetWitness ® Suite Legacy Windows Collector, you need:

- Any physical or virtual Windows 2008 R2 SP1 64-Bit Server that can reach the Windows 2003 event source domains.
- 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.



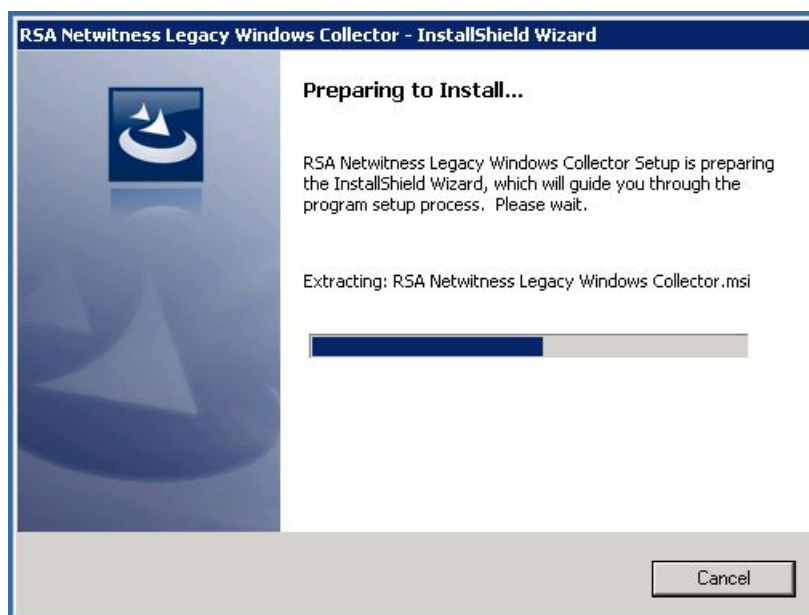
Update the RSA NetWitness® Suite Legacy Windows Collector from 10.6.x to 11.x

This section tells you how to update the RSA NetWitness® Platform 10.6.x Legacy Windows Collector to 11.

To update the RSA NetWitness® Suite 10.6.x Legacy Windows Collector to 11 on a Windows 2008 R2 SP1 64-Bit server:

1. Navigate to <https://community.rsa.com/docs/DOC-83034> on RSA link. Click **RSA NetWitness Logs & Packets 11.x - Legacy Windows Collector** to download the ZIP archive.
2. Unzip the downloaded file.
3. Log on to a Windows 2008 machine.
4. Copy **NWLegacyWindowsCollector-version-number.exe** to the Windows 2008 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.

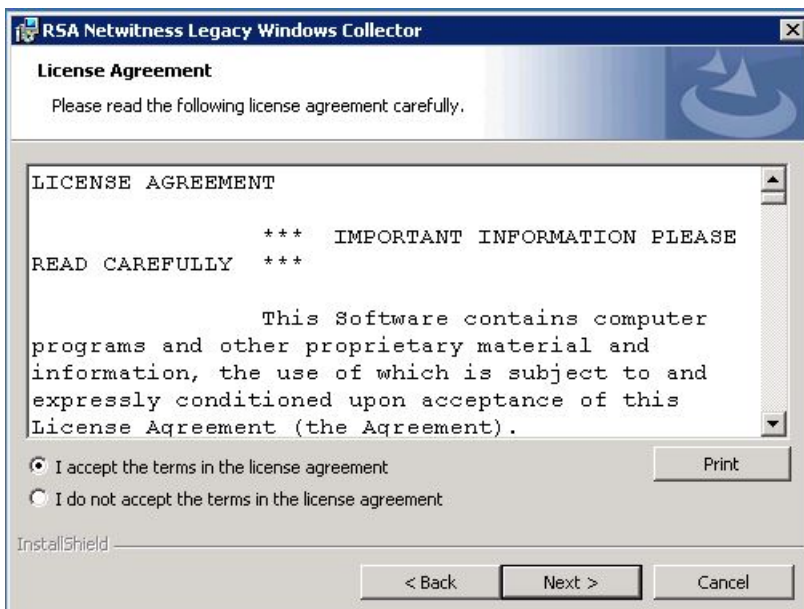


After the update installation program extracts RSA NetWitness® Suite Legacy Windows Collector installation files, the **Welcome** page is displayed.



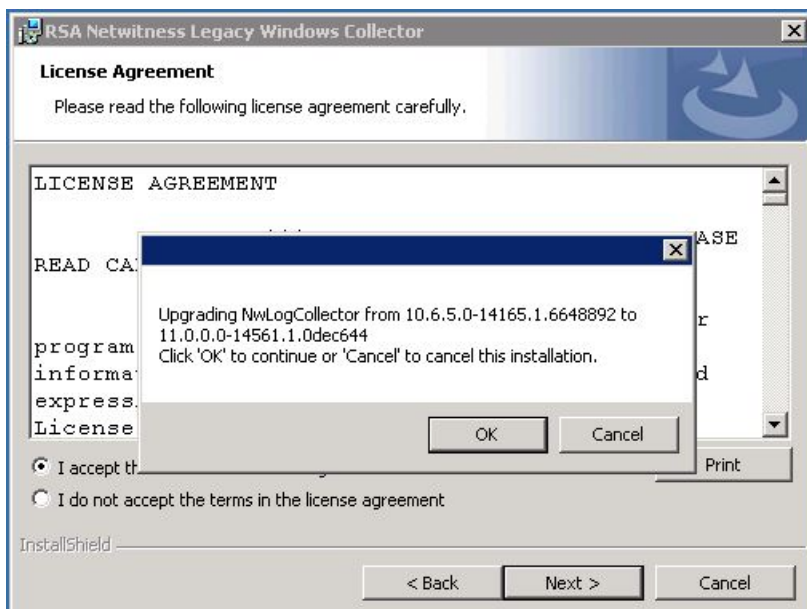
6. Click **Next**.

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.

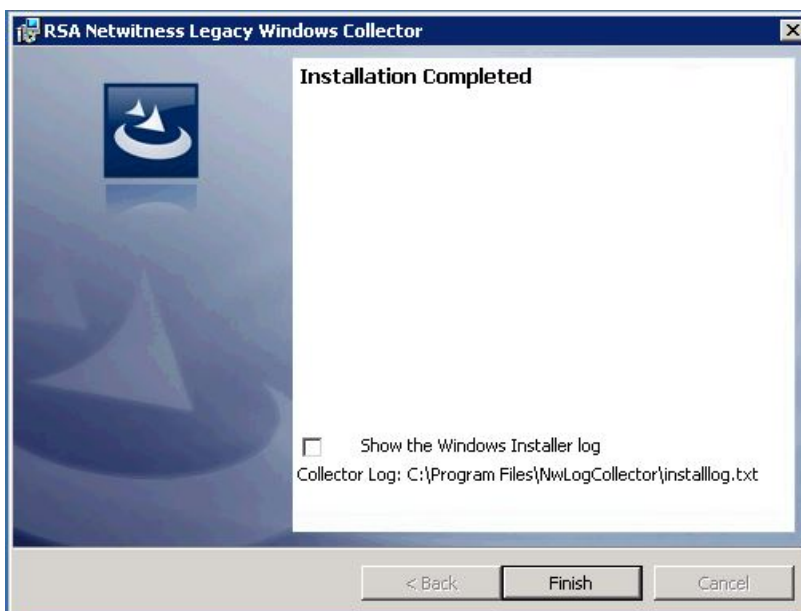




After the update installation completes, the **Next** button becomes active.

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 RSA NetWitness® Platform 11.x.

Fresh Install 11.x Legacy Windows Collector

This section describes how to install the 11.x Legacy Windows Collector on a Windows 2008 R2 SP1 64-Bit server

To install the RSA NetWitness® Platform Legacy Windows Collector on a Windows 2008 R2 SP1 64-Bit server:

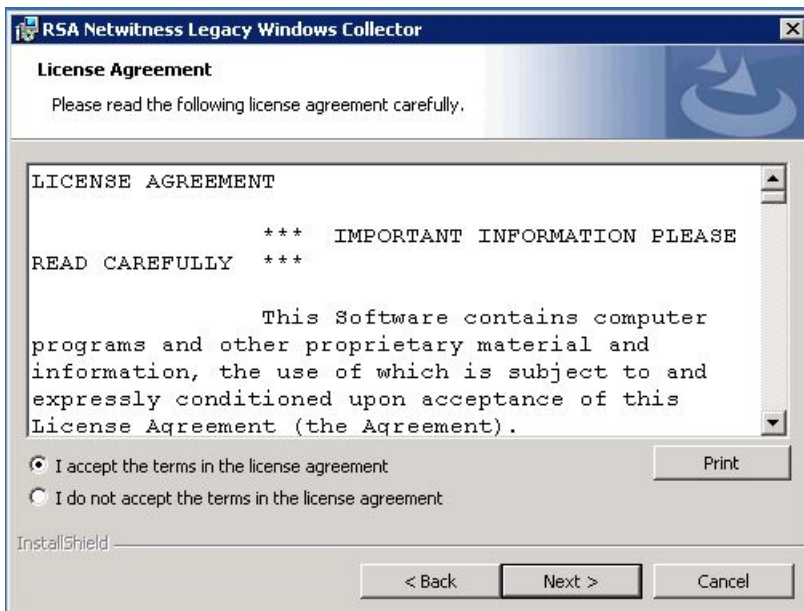
1. Navigate to <https://community.rsa.com/docs/DOC-83034> on RSA link. Click **RSA NetWitness Logs & Packets 11.x - Legacy Windows Collector** to download the ZIP archive.
2. Unzip the downloaded file.
3. Copy the **NWLegacyWindowsCollector-version-number.exe** to the Windows 2008 server.
4. Right click on the **NWLegacyWindowsCollector-version-number.exe** and select **Run As Administrator**.

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



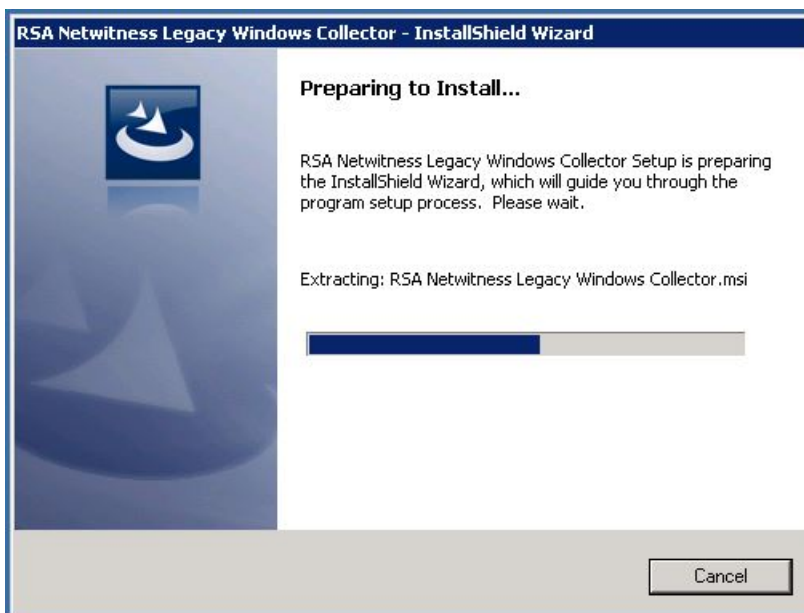
5. Click **Next**.

The License Agreement page is displayed.



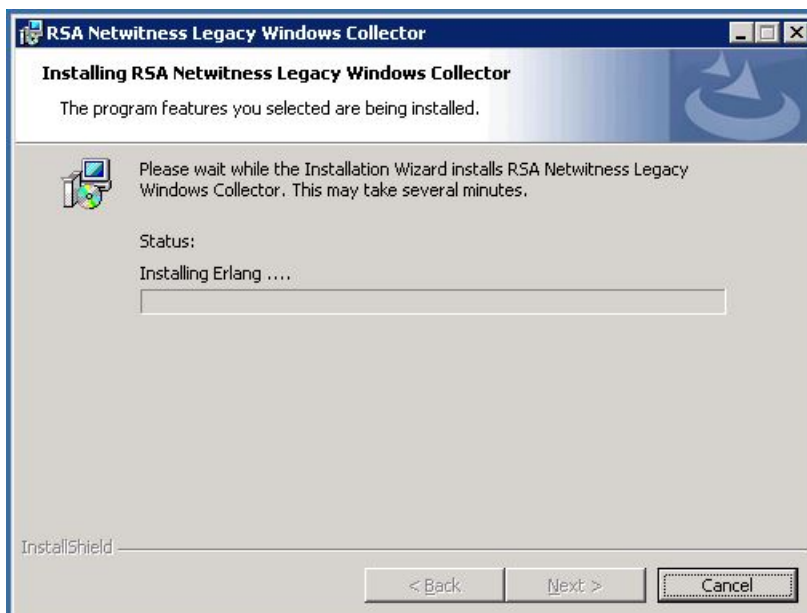
6. Read the License agreement carefully, select the **I accept the terms in the license agreement** radio button, and click **Next**.

The Ready to Install the Program page is displayed.

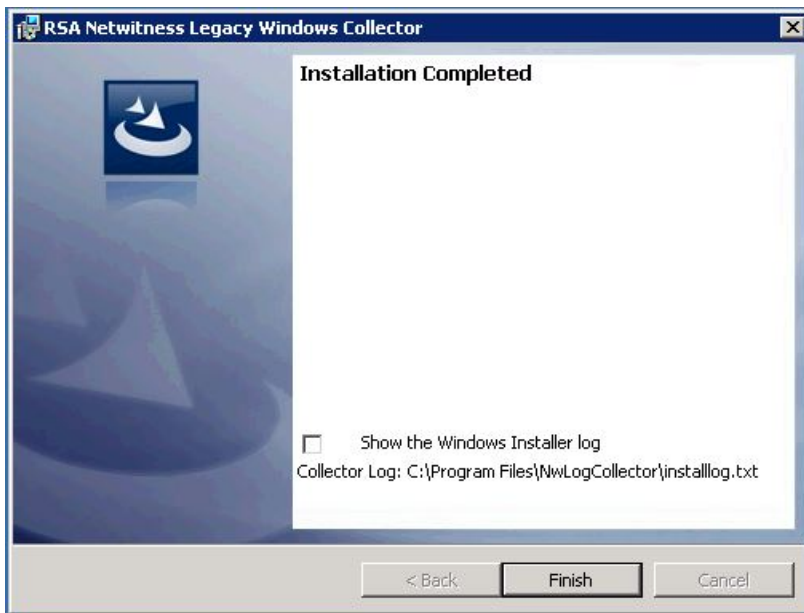


7. Click **Install**.

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 11.x Legacy Windows Collector. Please refer to the **Windows Legacy and NetApp Collection Configuration Guide** on RSA Link for instructions on how to configure Legacy Windows collection in RSA NetWitness® Platform.

Troubleshooting for 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 11.x 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 RSA NetWitness® Platform 11.x, the backup script for the Windows Legacy Collector is invoked automatically, and creates the 10.6.4 configuration and run-time backups. After the 11.x 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 RSA NetWitness® Platform 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 11.x Back to 10.6.4

To revert the Windows Legacy Collection setup from 11.x back to 10.6.4:

1. Uninstall the 11.x 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 RSA NetWitness® Platform

For this version of the Windows Legacy Collector, RSA 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 RSA NetWitness Suite.

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

The first screenshot shows the 'HOSTS' tab in the NetWitness UI. The 'Groups' panel on the left has a count of 11. The 'Hosts' table on the right contains one entry:

Name	Host	Services
WLC	10.25.51.185	1

The second screenshot shows the 'SERVICES' tab. The 'Groups' panel on the left has a count of 23. The 'Services' table on the right contains one entry:

Name	Licensed	Host	Type
WLC-185	✓	WLC	Log Collector