RSA NETWITNESS® SUITE

NetWitness® Endpoint Installation Guide

for Version 4.4

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

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.

July 2020

Contents

RSA NETWITNESS ENDPOINT 4.4 INSTALLATION GUIDE

This guide provides information about installing and configuring RSA NetWitness Endpoint 4.4.

The following topics are covered in this guide:

For information about NetWitness Endpoint, its components, product features, related technologies, and using the product, see the **RSA NetWitness Endpoint 4.4 User Guide**, available on RSA Link.

Technical Support

Support Option	Online Address
RSA Link	https://community.rsa.com
Contact RSA Support	https://community.rsa.com/docs/DOC-1294
Community	https://community.rsa.com/community/products/netwitness
Support Plans and Options	https://community.rsa.com/docs/DOC-40401
Email	support@rsa.com

SYSTEM REQUIREMENTS

This topic provides information about the system requirements for installing and configuring NetWitness Endpoint.

Supported Operating Systems for NetWitness Endpoint Servers

NetWitness Endpoint Servers (including the Roaming Agents Relay) run under Microsoft Windows only. Recommended are:

- Microsoft Windows 2008 SP2
- Microsoft Windows 2008 R2
- Microsoft Windows 2012
- Microsoft Windows 2012 R2
- Microsoft Windows 2016 R2
- Microsoft Windows 2019

For testing purposes, servers can also run on:

- Microsoft Windows Vista (32 or 64 bit)
- Microsoft Windows 7 (32 or 64 bit)
- Microsoft Windows 8 (32 or 64 bit)
- Microsoft Windows 8.1 (32 or 64 bit)

Supported Operating Systems for NetWitness Endpoint Agents

NetWitness Endpoint agents can run under Microsoft Windows, Macintosh OS-X systems, or select Linux distributions.

Windows OS Support

- Microsoft Windows XP 32-bit SP3
- Microsoft Windows XP 64-bit SP2
- Microsoft Windows Vista SP1 (32 & 64-bit)
- Microsoft Windows 7 (32 & 64-bit)

- Microsoft Windows 8 (32 & 64-bit)
- Microsoft Windows 8.1 (32 & 64-bit)
- Microsoft Windows 10 (32 & 64-bit)
- Microsoft Windows 2003 Server SP2 (32 & 64-bit)
- Microsoft Windows 2008 Server (32 & 64-bit)
- Microsoft Windows 2008 R2 (32 & 64-bit)
- Microsoft Windows 2012 Server
- Microsoft Windows 2012 Server R2
- Microsoft Windows 2016 Server
- Microsoft Windows 2019 Server

Mac OS Support

- OS-X 10.8 (Mountain Lion)
- OS-X 10.9 (Mavericks)
- OS-X 10.10 (Yosemite)
- OS-X 10.11 (El Capitan)
- OS-X 10.12 (Sierra)
- OS-X 10.13 (High Sierra)
- OS X 10.14 (Mojave)

Linux OS Support

- CentOS 6.x and 7.x
- Red Hat Linux 6.x and 7.x

Prerequisites

Database Prerequisite

The NetWitness Endpoint Server requires Microsoft SQL Server, which must be pre-installed. For step-by-step instructions to install Microsoft SQL Server, see Step 1: Install Microsoft SQL Server.

The RSA NetWitness Endpoint database will be attached to your Microsoft SQL Server instance. The supported versions are:

- Microsoft SQL Server 2012 Standard Edition
- Microsoft SQL Server 2012 Enterprise Edition
- Microsoft SQL Server 2014 Standard Edition
- Microsoft SQL Server 2014 Enterprise Edition
- Microsoft SQL Server 2016 Standard Edition
- Microsoft SQL Server 2016 Enterprise Edition
- Microsoft SQL Server 2019 Standard Edition
- Microsoft SQL Server 2019 Enterprise Edition

Note: RSA recommends Microsoft SQL Server 2012, 2014, 2016, or 2019 Enterprise Edition. The Standard Edition has core and memory usage limitations, so larger deployments may require Enterprise Edition to meet the specifications outlined in the following sections. Also, note that the Management tools installation is separate from the Microsoft SQL Server installation for SQL Server 2016 and 2019 editions. Please refer to their respective Microsoft SQL Server Enterprise installation guides for detailed steps.

Microsoft SQL Server can be installed and run on a separate physical or virtual machine from the NetWitness Endpoint Server. The NetWitness Endpoint UI can still be run locally on the operator's machine, even if the Microsoft SQL Server instance is running remotely. The NetWitness Endpoint ConsoleServer service account must have sysadmin rights on the SQL database.

Java Prerequisite

To support the NetWitness Endpoint Meta Service integration with NetWitness Suite 11.0, you must install Java JRE version 8 update 131 or later on the NetWitness Endpoint server. For more information on Java JRE, go to http://www.oracle.com/technetwork/java/index.html. For more information about the Meta Service integration, see "NetWitness Suite Endpoint Meta Integration" in the *RSA NetWitness Endpoint 4.4 User Guide*.

Note: Only Java JRE version 8 and its updates are supported. Java JRE versions 9 or later are not supported.

Additional Components Included During Installation

NetWitness Endpoint uses Microsoft .NET 4.6.1 and Microsoft Visual C++ 2010, 2012, and 2015. There is no need to manually pre-install these components, however, as the NetWitness Endpoint Installer will automatically download and install them for you.

NetWitness Endpoint uses Secure Sockets Layer (SSL); however, the SSL version included in the supported operating systems will work with NetWitness Endpoint.

Distributed Installation

NetWitness Endpoint has a scalable architecture. Depending on your needs, you can use different installation configurations:

- Single-Server Mode has only one instance of the NetWitness Endpoint server and all endpoints connect to that server. Each NetWitness Endpoint server instance includes ConsoleServer, database server, and API server. Single-server mode can be deployed using one of the following two options:
  - Install the NetWitness Endpoint server, database server, and API server on one machine and the NetWitness Endpoint UI on a different machine (recommended configuration).
  - Install all components (NetWitness Endpoint server, database server, API server, and NetWitness Endpoint UI) on the same machine.
- Multi-Server Mode has more than one instance of the NetWitness Endpoint server, with one instance being the Primary server and the rest (up to three) being Secondary servers. Multi-server mode can be deployed according to the following guidelines:
  - RSA recommends that each instance of a NetWitness Endpoint server (Primary or Secondary) be installed on a separate machine.
  - Install the NetWitness Endpoint UI on a separate machine (for example, the analyst workstation); there can be multiple instances of the UI installed on different machines.

Note: When installing, RSA requires that all the servers connect through at least a gigabit network.

The components are listed below, some of which are installed using the NetWitness Endpoint Installer, and some of which must be installed separately.

Components to install using the NetWitness Endpoint Installer:

- NetWitness Endpoint ConsoleServer (for Primary server and Secondary servers)
- NetWitness Endpoint UI
- NetWitness Endpoint Agent (separate packagers for each agent type: Windows, Mac, and Linux)
- NetWitness Endpoint API Server

Components that require separate installation:

- Microsoft SQL Server (must be installed before using the NetWitness Endpoint Installer)
- (Optional) OPSWAT Metascan REST Server
- (Optional) YARA
- (Optional) NetWitness Endpoint Roaming Agents Relay (RAR)

Note: The Microsoft SQL database requires a high-performance environment. See below for minimum requirements for the NetWitness Endpoint database server.

Sizing Recommendations for NetWitness Endpoint Components

NetWitness Endpoint Database Server

The following table details the minimum hardware configuration and required database storage for the NetWitness Endpoint database server according to the size of the environment by number of endpoints. These requirements also allow for installing the NetWitness Endpoint ConsoleServer on the same machine. For environments of 10K endpoints or more, the database disk storage should be on SSDs. The following requirements apply for Microsoft SQL 2012 and 2014, Standard or Enterprise editions.

Deployment Size	Cores	Memory (GB)	Disk (GB)	Disk Speed (64K block random IOPS)
Trial - 10	4	16	100	-
PoC - 1K	8	32	500	-
Small - 5K	12	64	1000	3000
Medium - 10K	16	128	2000	3000
Standard - 25K	20	192	2000	6000
Large - 50K (see Notes below)	20	256	4000	6000

If using Microsoft SQL Server 2016 Standard Edition, the following requirements apply:

Deployment Size	Core	Memory (GB)	Disk (GB)
Standard -- 20K	16	200	2000

Note: The maximum number of modules supported with Microsoft SQL 2016 Standard Edition is 2.5 million.

Note: For more information on database and OS partitions sized for 50K deployments, refer to the following sections: Recommendations for Configuring the Microsoft SQL Database Disk and Partitions and Installation and Configuration Guidelines for RSA-Provided NetWitness Endpoint Hardware.

Note: Per day maximum of 10k scheduled scans should be configured.

NetWitness Endpoint ConsoleServer and NetWitness Endpoint API Server

1. There is no advantage to hosting the NetWitness Endpoint ConsoleServer on a separate computer, but it is a supported configuration if it is not possible to host the ConsoleServer on the database server. If co-hosted on the NetWitness Endpoint database server hardware, no additional requirements are necessary.
2. The following table shows the recommended hardware for hosting the NetWitness Endpoint ConsoleServer on a dedicated computer, which can be a virtual machine.
3. Disk space is only used to host the operating system and installed software. The NetWitness Endpoint ConsoleServer does not store data locally.
4. Additional hardware is not required for the API server, which integrates with Security Analytics, except for the small (Trial / POC) installation. In a small deployment, additional processing power and memory are required (as indicated in the table below).
5. The NetWitness Endpoint API server always co-exists with the ConsoleServer. There is no option to install it separately. The following specifications are for ConsoleServer and API server only (UI is not included).

Deployment Size	Cores (Standalone / with SA Integration)	Memory (GB)	Disk (GB)
PoC - 1K	4 / 8	8 / 12	100
Medium - 10K	8	16	100
Standard - 25K	16	32	100

NetWitness Endpoint UI

The analyst's usual workstation should be sufficient to host the NetWitness Endpoint UI, with a minimum of 2 cores and 8 GB of RAM

NetWitness Endpoint Roaming Agents Relay (RAR) Server

1. The link speed between the NetWitness Endpoint ConsoleServer and the RAR server should not be less than 300 Mbps (or 40 MBps).
2. Agent Relays are measured based on the maximum number of concurrent roaming agents, rather than number of endpoints overall. When sizing the RAR, make sure you understand the percentage of the workforce traveling at any one time. As an example, EMC sized its NetWitness Endpoint RAR at 10% of the workforce, which seems to provide sufficient headroom for its employees' collective traveling habits, even during peak travel, such as large conferences.
3. A worker on VPN does not use the Roaming Agents Relay. So the remote workforce already connected to the network does not enter the RAR calculation above.
4. In the event that a RAR connection is unavailable, the endpoint will buffer the data and continue trying to find the server / fallback on the Relay.
5. Each RAR can connect to multiple ConsoleServers, but each ConsoleServer can connect to only one RAR.
6. The RAR lives outside the corporate network, such as in a DMZ or the Cloud. The RAR requires a publicly accessible DNS alias that agents will leverage when outside the corporate network.

Concurrent Active Roaming Agents* Irrespective of Deployment Size	Cores	Memory (GB)	Disk (GB)
Small - (Trial or PoC)	4	8	100
Medium - <5K	12	16	100
Large - 5-20K	12	32	100

*Concurrent active roaming agents = maximum number of endpoints roaming at the same time (disconnected from the corporate network and outside a VPN connection).

Recommendations for Configuring the Microsoft SQL Database Disk and Partitions

If you are using your own hardware, this section provides some basic guidelines to ensure optimum system performance.

RSA strongly recommends the following configuration when using a single RAID 10 volume for the NetWitness Endpoint SQL database: You must use a 64K block size in Windows with a 1024 offset and NTFS file system when formatting the partition. If you do not use the recommended configuration, you may experience a serious impact in your system's performance.

There are four key files managed by the Microsoft SQL Server, all of which have specific requirements to ensure optimal system performance, as outlined below:

1. **NetWitness Endpoint database**
   The NetWitness Endpoint database file contains all the data about NetWitness Endpoint and is very performance-sensitive. It should be stored on a device that has excellent random access for both reads and writes. An SSD-based array is generally required to meet the requirements for this partition (see Disk Speed in requirements table).
2. **NetWitness Endpoint database transaction log**
   The transaction log is only accessed sequentially, unlike the database, but performance is still very important. It is suggested that it be stored on a separate 10K RPM or higher based HDD array, or included on the SSD-based array for the database (and available storage increased accordingly).
3. **SQL Server temporary database**
   This database is used by the server for intermediate calculations and temporary storage. It is very performance-sensitive and should be stored on a device that has excellent random access for both reads and writes. An SSD-based array is generally required to meet the requirements for this partition (see Disk Speed in requirements table), and this can be the same array as the NetWitness Endpoint database, given sufficient storage for both.
4. **SQL Server temporary database transaction log**
   This transaction log should be co-located with the temporary database as the first option or co-located with the NetWitness Endpoint database transaction log as a second option.

Note: When configuring SAN on your hardware, particularly logical unit numbers (LUNs), RSA strongly recommends that you refer to the following White Paper: https://www.emc.com/collateral/technical-documentation/h14621-microsoft-sql-server-best-practice.pdf

Installation and Configuration Guidelines for RSA-Provided NetWitness Endpoint Hardware

The following information provides guidelines for installing and configuring NetWitness Endpoint on dedicated Dell hardware that is purchased from RSA.

For hardware purchased from RSA, the recommended RAID configurations are as follows:

- RAID 1: 2 x 1.2TB 10K – OS (OS , SQL, and NetWitness Endpoint)
- RAID 6: 6 x 1TB 7.2K – Files (Downloaded files, SQL Database Backup)
- RAID 10: 10 x 800GB SSDs (~4 Usable) – DB (Queued Data, NetWitness Endpoint database, NetWitness Endpoint database transaction log, SQL Server temp database transaction log, SQL Server temp database)

Configure RAID volumes in the BIOS

The first step is to configure the RAID volumes in the BIOS. This can be done by pressing F2 to access System Setup. The following volumes must be created:

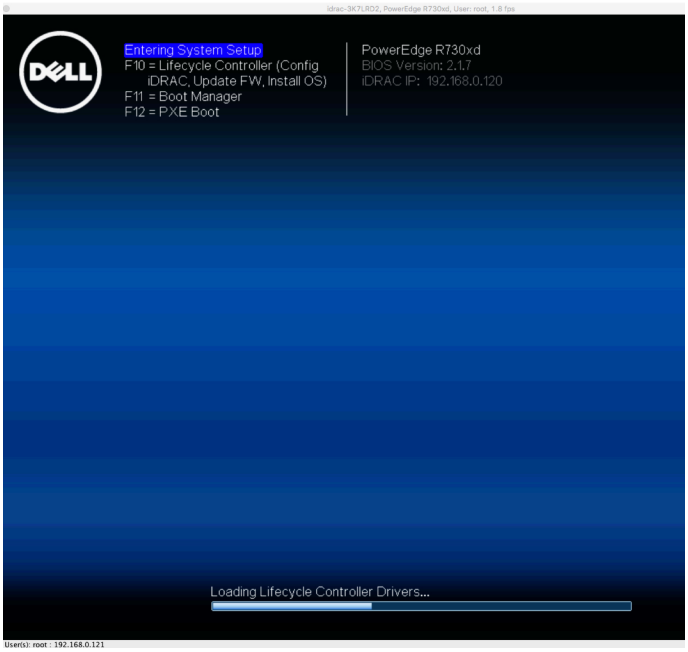
- OS volume (2x 1.2 TB 10K hard drives): RAID 1
- Files volume (6x 1 TB 7.2K RPM HDs): RAID 6
- Data volume (10x 800 GB SSDs): RAID 10

The following procedure details the steps for configuring the RAID volumes.

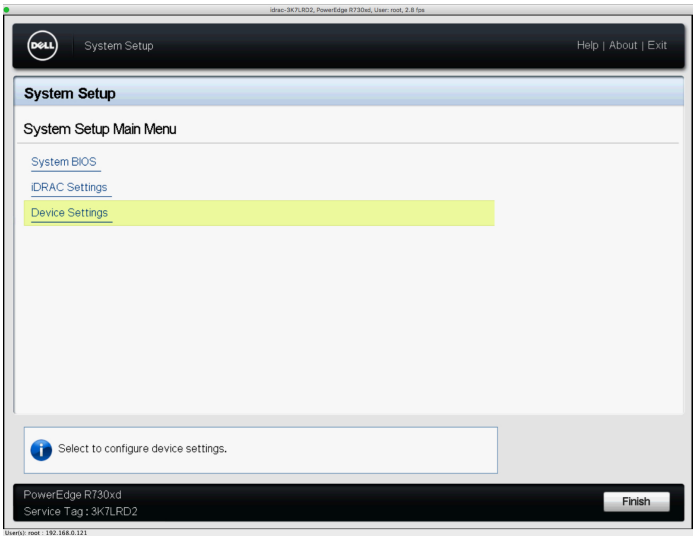
The following information may be pertinent for setting up the machine:

- IDRAC IP Address = 192.168.0.120
  IDRAC credentials = root/calvin
- Sda=volgroup0=c drive
  Sdb=volgroup1=f drive
  Sdc=volgroup2=d drive

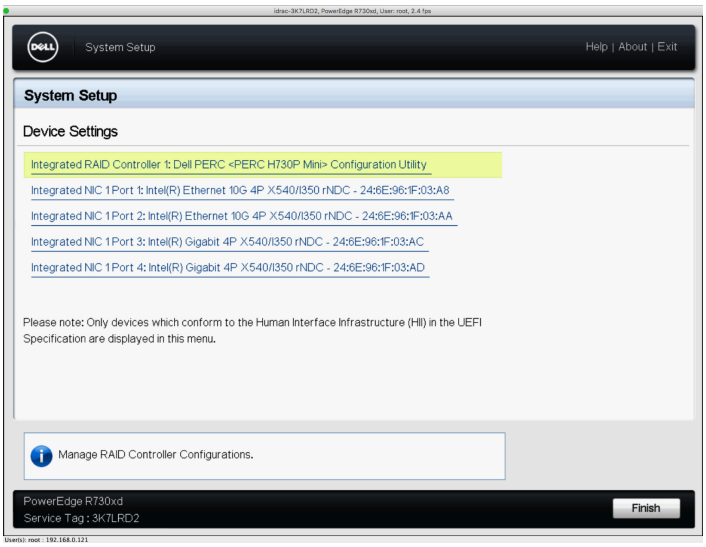
1. Press **F2** on bootup to navigate to System Setup.



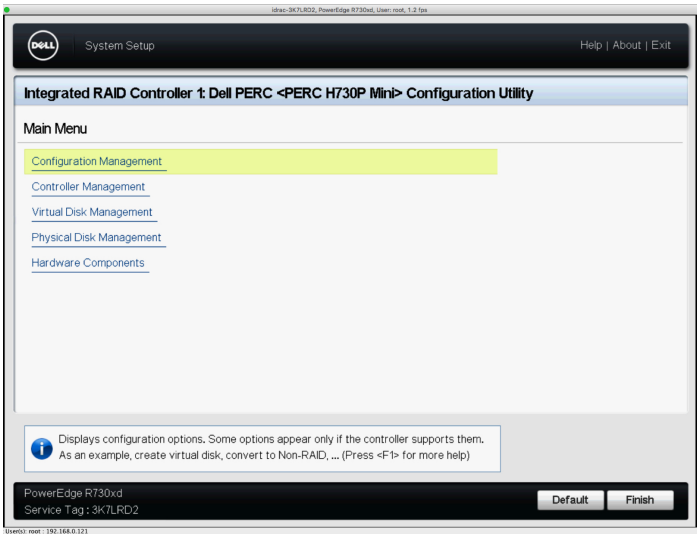
2. Select **Device Settings**.



3. Select **Integrated RAID Controller 1:Dell PERC <PERC H730P Mini> Configuration Utility**.

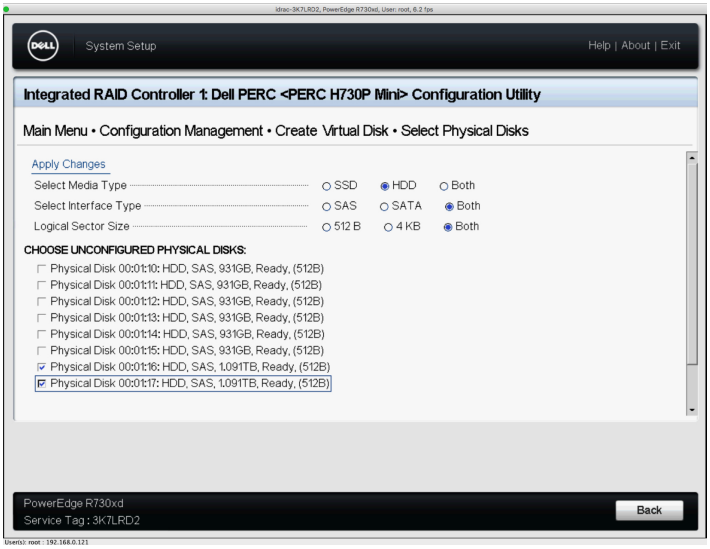


4. Select **Configuration Management**.



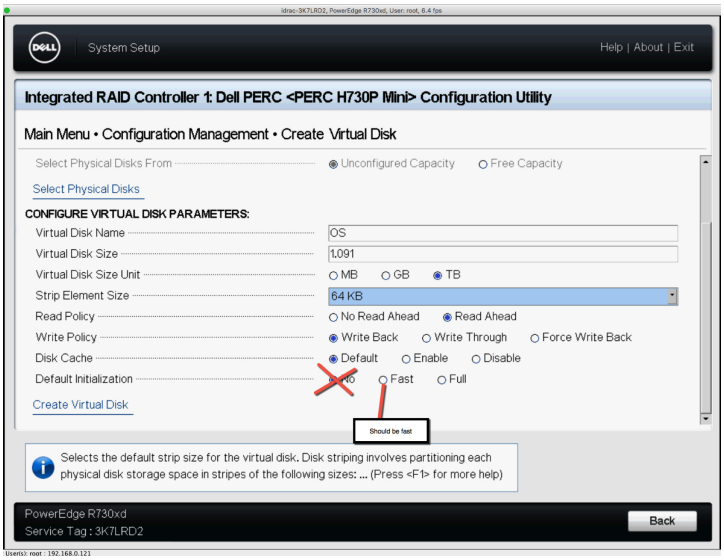
5. Select **Create Virtual Disk**.

6. Select **RAID 1** from the drop-down list.
7. Select **Physical Disk**.
8. Check the two drives that are 1.091TB.

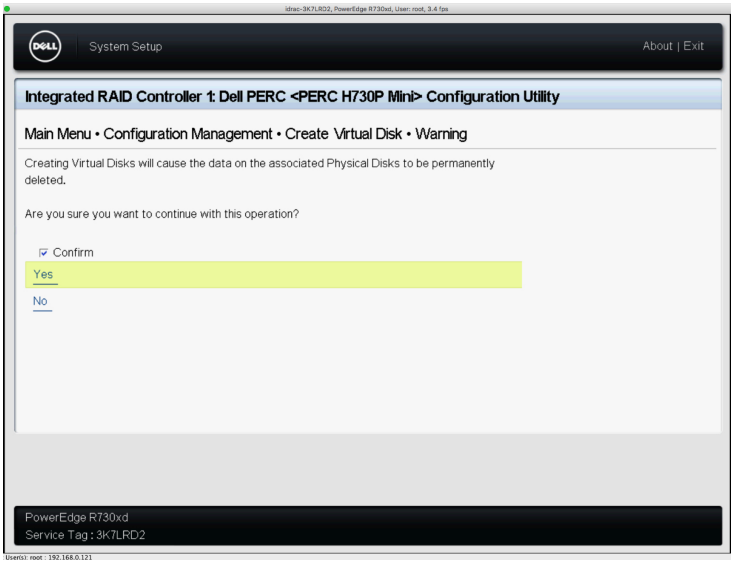


9. Click **Apply Changes**.
10. Name the volume **OS**.

11. Select **Fast** for initialization.

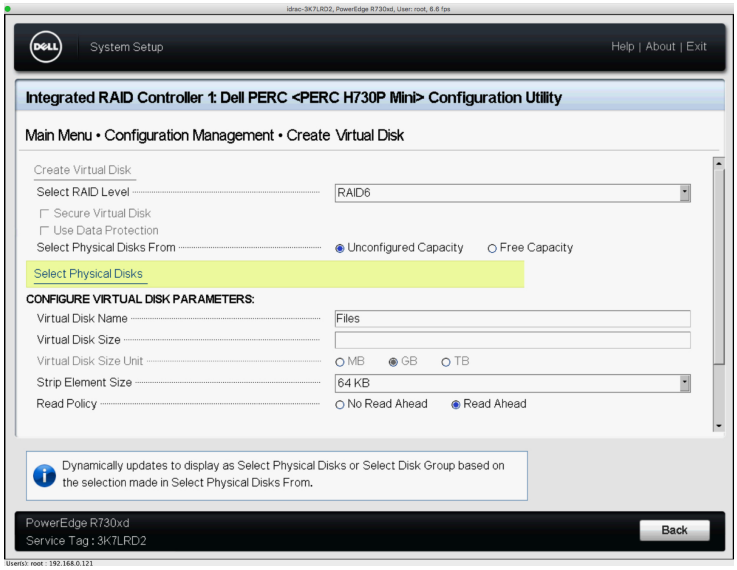


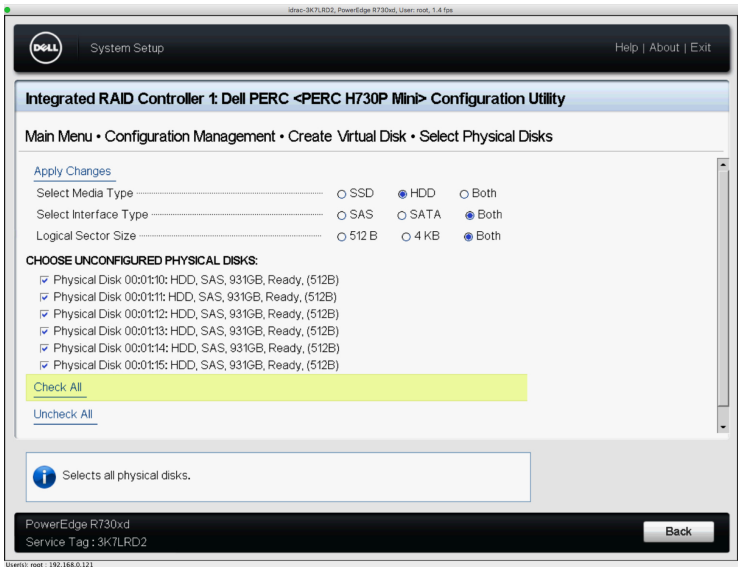
12. Click **Create Virtual Disk** and then confirm the action.



13. Repeat steps 5-12 for the next volume, using the following settings:
    - Select RAID 6
    - Select all the 931GB drives or click **Check All**
    - Apply the changes
    - Name the volume **Files**
    - Select **Fast** initialization

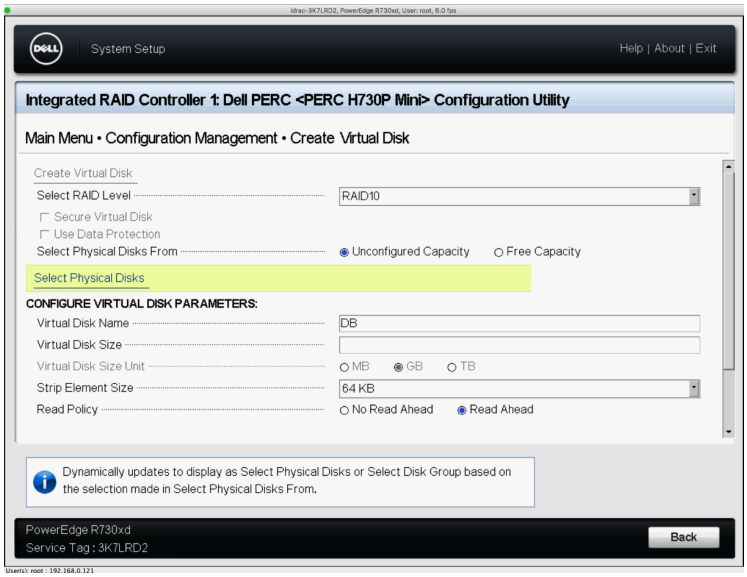
- Click **Create Virtual Disk**

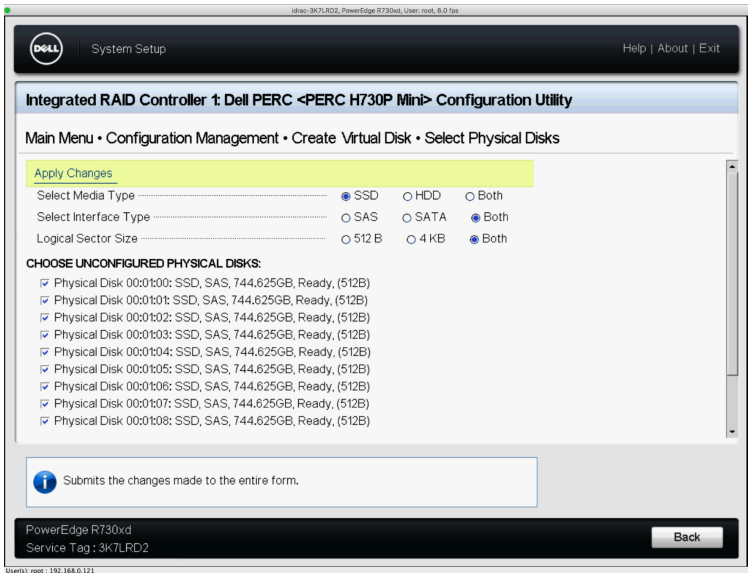




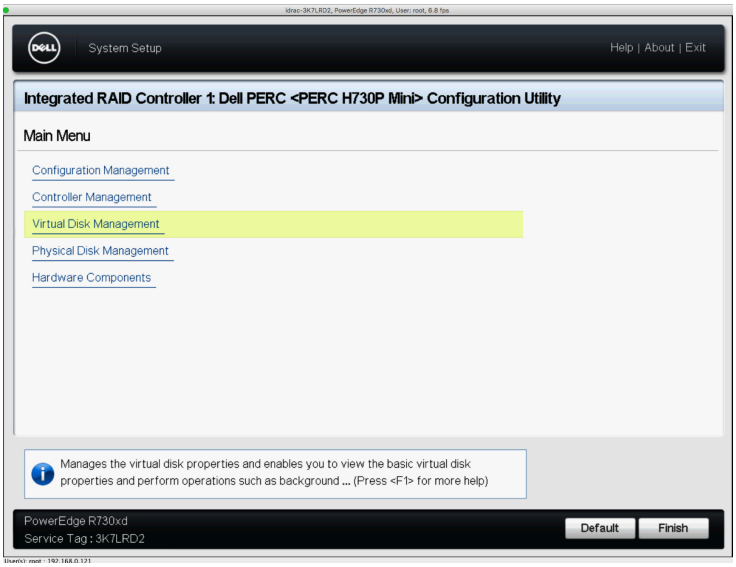
14. Repeat steps 5-12 for the next volume, using the following settings:
    - Select RAID 10
    - Switch from HDD to SSD in physical disk and select all the drives
    - Apply the changes
    - Name the volume **DB**
    - Select **Fast** initialization
    - Should be 64K stripe by default but if not then change it

- Click **Create Virtual Disk**



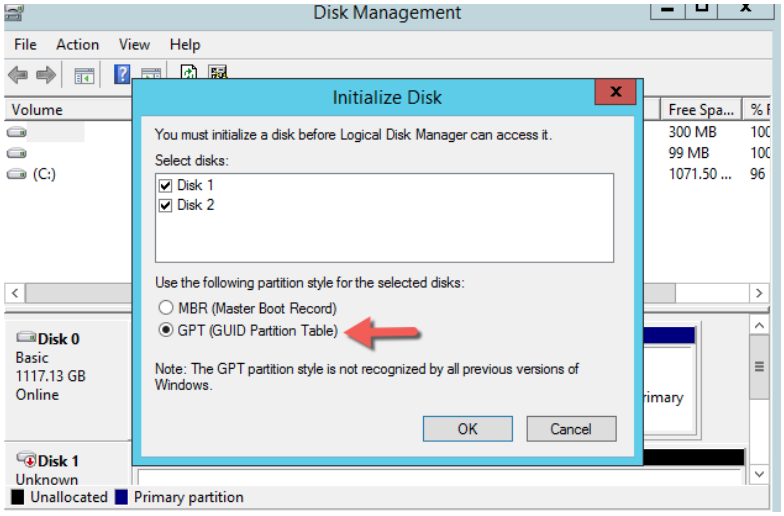


15. Go back one menu, click **Virtual Disk Management**, and double-check that all drives are listed.

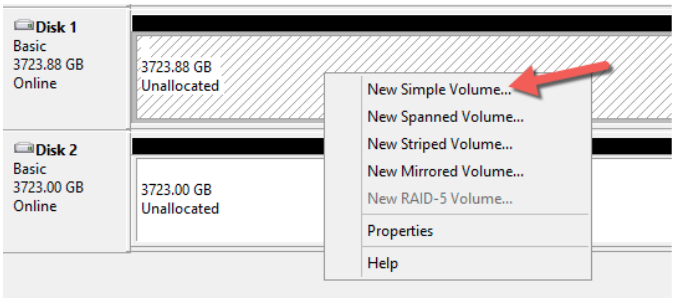


16. Reboot the machine.
17. Install Windows Server to **C:** (OS or sda).

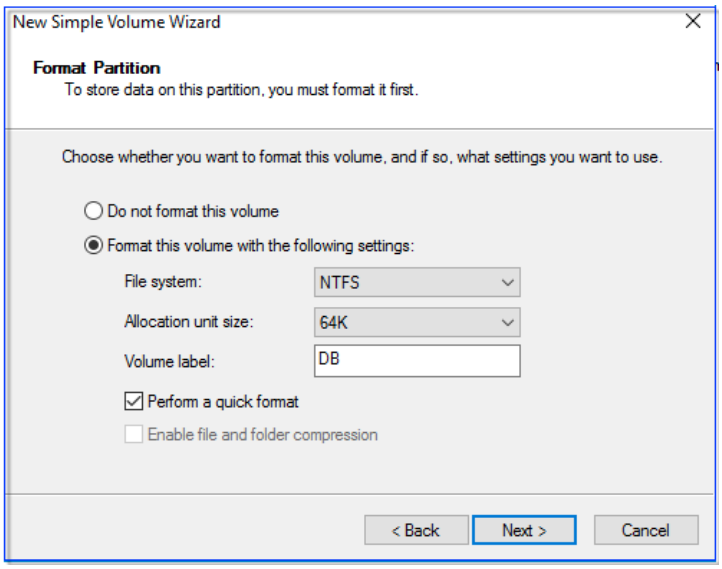
18. Select **GPT** as the Partition Style during Initialize Disk step in Disk Management, as shown below:



19. After initializing the disk, create the volume as **New Simple Volume**:



20. On the New Simple Volume Wizard, select the options as shown below:



Install Microsoft Windows Server on the OS Volume

Install Microsoft Windows Server 2012 on the OS volume. Format the OS volume as **C:**. Format the data volume as **D:** and the files volume as **F:**, both in NTFS.

Caution: For the RAID 10 Data volume, it is very important that you configure it as follows when you format it via Disk Management: 64K stripe on volume and 64K block size in Windows with a 1024 offset and NTFS file system. If it is configured any other way it will have very serious impacts on system performance.

Install Microsoft SQL Server Enterprise

Install Microsoft SQL Server 2014 Enterprise on **C:\Program Files\Microsoft SQL Server**, but set the data root directory as **D:\NWE**. For detailed instructions, see Step 1: Install Microsoft SQL Server.

Caution: Making any modifications to the Microsoft SQL database other than what is specified in the NetWitness Endpoint documentation is not supported and may result in errors when installing the NetWitness Endpoint product.

Split the Microsoft SQL Temp DB into Eight Files

Split the Temp database into eight files with the following script:

```
ALTER DATABASE tempdb MODIFY FILE (NAME='tempdev' ,
FILENAME='D:\NWE\DATA\tempdb.mdf' , SIZE=25600MB, FILEGROWTH = 0)

ALTER DATABASE tempdb  ADD FILE (NAME='tempdev2',
FILENAME='D:\NWE\DATA\tempDB2.ndf', SIZE=25600MB, FILEGROWTH = 0)

ALTER DATABASE tempdb  ADD FILE (NAME='tempdev3',
FILENAME='D:\NWE\DATA\tempDB3.ndf', SIZE=25600MB, FILEGROWTH = 0)

ALTER DATABASE tempdb  ADD FILE (NAME='tempdev4',
FILENAME='D:\NWE\DATA\tempDB4.ndf', SIZE=25600MB, FILEGROWTH = 0)

ALTER DATABASE tempdb  ADD FILE (NAME='tempdev5',
FILENAME='D:\NWE\DATA\tempDB5.ndf', SIZE=25600MB, FILEGROWTH = 0)

ALTER DATABASE tempdb  ADD FILE (NAME='tempdev6',
FILENAME='D:\NWE\DATA\tempDB6.ndf', SIZE=25600MB, FILEGROWTH = 0)

ALTER DATABASE tempdb  ADD FILE (NAME='tempdev7',
FILENAME='D:\NWE\DATA\tempDB7.ndf', SIZE=25600MB, FILEGROWTH = 0)

ALTER DATABASE tempdb  ADD FILE (NAME='tempdev8',
FILENAME='D:\NWE\DATA\tempDB8.ndf', SIZE=25600MB, FILEGROWTH = 0)
```

Configure SQL DB Parallelism

Configure the maximum degree of parallelism and the cost threshold for parallelism, using the following script:

```
USE ECAT$PRIMARY;
GO
EXEC sp_configure 'show advanced options', 1;
GO
RECONFIGURE WITH OVERRIDE;
GO
EXEC sp_configure 'max degree of parallelism', 8;
GO
RECONFIGURE WITH OVERRIDE;
GO
EXEC sp_configure 'show advanced options', 1 ;
GO
RECONFIGURE WITH OVERRIDE;
GO
EXEC sp_configure 'cost threshold for parallelism', 50 ;
GO
RECONFIGURE WITH OVERRIDE;
GO
```

Dell NetWitness Endpoint Hardware Specification

The following table provides the exact specifications for the Dell NetWitness Endpoint hardware.

Description	Quantity
PowerEdge R730xd XL (210-ADES)	1
PE R730 XL R730/xd XL Motherboard MLK (329-BCZK)	1
Dell Hardware Limited Warranty Plus On Site Service (976-9007)	1
Basic Hardware Services: Business Hours (5X10) Next Business Day On Site Hardware Warranty Repair 3 Year (976-9079)	1

Description	Quantity
Dell ProSupport Service Offering Declined (991-2878)	1
Declined recommended ProSupport service - Call your Dell Sales Rep if Upgrade Needed (996-8029)	1
US Order (332-1286)	1
On-Site Installation Declined (900-9997)	1
PowerEdge R730xd Shipping (340-AKPM)	1
R730/xd PCIe Riser 2, Center (330-BBCO)	1
R730xd PCIe Riser 1 Filler Blank, Right (374-BBHT)	1
Intel Ethernet X540 DP 10Gb BT + I350 1Gb BT DP Network Daughter Card (540-BBCC)	1
iDRAC8 Enterprise, integrated Dell Remote Access Controller, Enterprise (385-BBHO)	1
Chassis with up to 24, 2.5" Hard Drives (350-BBFD)	1
Bezel (325-BBEJ)	1
Performance BIOS Settings (384-BBBL)	1
UEFI BIOS (800-BBDM)	1
Unconfigured RAID for H330/H730/H730P (1-28 HDDs or SSDs) (780-BBLP)	1
PERC H730P Integrated RAID Controller, 2GB Cache (405-AAEH)	1
Intel Xeon E5-2680 v4 2.4GHz,35M Cache,9.60GT/s QPI,Turbo,HT,14C/28T (120W) Max Mem 2400MHz (338-BJDO)	1
Intel Xeon E5-2680 v4 2.4GHz,35M Cache,9.60GT/s QPI,Turbo,HT,14C/28T (120W) Max Mem 2400MHz (338-BJEE)	1
32GB RDIMM, 2400 MT/s, Dual Rank, x4 Data Width (370-ACNS)	8
2400MT/s RDIMMs (370-ACPH)	1
Performance Optimized (370-AAIP)	1

Description	Quantity
800GB Solid State Drive SAS Mix Use MLC 12Gbps 2.5in Hot-plug Drive, PX04SM (400-ALXS)	10
1TB 7.2K RPM Near-Line SAS 12Gbps 2.5in Hot-plug Hard Drive (400-ALUN)	6
1.2TB 10K RPM SAS 12Gbps 2.5in Hot-plug Hard Drive (400-AJON)	2
No Trusted Platform Module (461-AADZ)	1
No Systems Documentation, No OpenManage DVD Kit (631-AACK)	1
ReadyRails Static Rails for 2/4-post Racks (770-BBBE)	1
Dual, Hot-plug, Redundant Power Supply (1+1), 1100W (450-ADWM)	1
NEMA 5-15P to C13 Wall Plug, 125 Volt, 15 AMP, 10 Feet (3m), Power Cord, North America (450-AALV)	2
No Operating System (619-ABVR)	1
No Media Required (421-5736)	1
DIMM Blanks for System with 2 Processors (370-ABWE)	1
Standard Heatsink for PowerEdge R730/R730xd (374-BBHM)	1
Standard Heatsink for PowerEdge R730/R730xd (374-BBHM)	1
Solutions Program Support (927-3179)	1

INSTALLATION

This topic provides detailed installation instructions for installing NetWitness Endpoint. The installation instructions in this topic assume you are deploying a brand new NetWitness Endpoint 4.4 installation.

If you are updating an existing NetWitness Endpoint 4.x to 4.4, refer to the section Update Installation.

If you are currently on RSA ECAT 3.5, you should first uninstall ECAT 3.5 and then install NetWitness Endpoint 4.4; however, agents currently on 3.5 can be upgraded using the 4.4 agent packager.

Installation consists of the following steps, some of which are optional:

- Step 1: Install Microsoft SQL Server
- Step 2: Configure SQL Server
- Step 3: Install Primary ConsoleServer
- Step 4: (Optional) Export Primary Server Certificates
- Step 5: (Optional) Import Primary Server Certificates
- Step 6: (Optional) Install Secondary Server
- Step 7: Configure Multi-Server Through NetWitness Endpoint UI
- Step 8: Run NetWitness Endpoint ConsoleServerOutput
- Step 9: (Optional) Install Metascan
- Step 10: (Optional) Install YARA
- Step 11: Deploy Agents (Windows)
- Step 12: Deploy Agents (Mac)
- Step 13: Deploy Agents (Linux)
- Step 14: (Optional) Deploy Roaming Agents Relay
- Step 15: Launch NetWitness Endpoint UI

Step 1: Install Microsoft SQL Server

This topic provides general guidance for installing Microsoft SQL Server 2012, focusing on necessary configuration for NetWitness Endpoint. This is a three-part process, as described in the following sections:

- Part 1: Install Microsoft SQL Server
- Part 2: Split the Microsoft SQL Temp DB into Eight Files
- Part 3: Configure SQL DB Parallelism

Caution: Making any modifications to the Microsoft SQL database other than what is specified in the NetWitness Endpoint documentation is not supported and may result in errors when installing the NetWitness Endpoint product.

Part 1: Install Microsoft SQL Server

The instructions below are for SQL Server 2012, but the process is similar for SQL Server 2014 or 2016, and these instructions should serve for any of these versions.

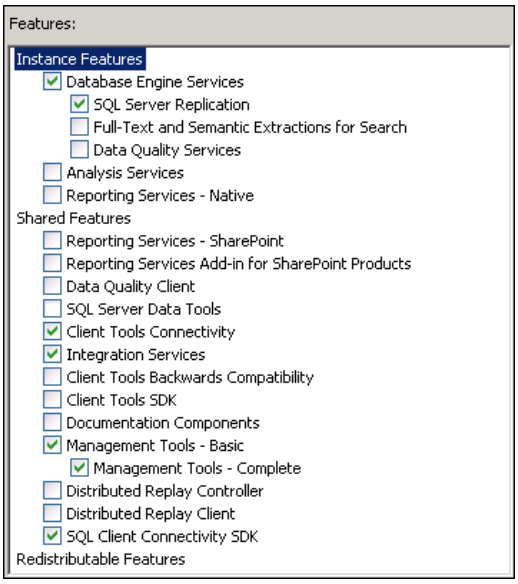
For detailed instructions and screenshots, refer to the documentation that came with your version of Microsoft SQL Server.

To install Microsoft SQL Server:

1. Run the SQL Server installation program by double-clicking the file **SETUP.EXE** (or, it may auto-run on its own, or may ask you to select the file to run).
   The "SQL Server Installation Center" is displayed. The **Planning** panel consists of the links to the documentation relevant to installation.
2. Select **Installation** in the menu on the left.
3. Click the option **New SQL Server stand-alone installation or add features to an existing installation**.
   The SQL Server 2012 Setup wizard is displayed.
4. The wizard will automatically perform the **Setup Support Rules**, an analysis of your computer to identify potential installation problems. Click **Show Details**.
   The results of the system analysis are displayed.
5. Make sure any issues it identifies (that do not have Status “Passed”) are dealt with before moving on. When finished, click **OK**.
6. Wait for the Product Key dialog to open and do one of the following:

- Select **Evaluation** (which is the default). This will install the free trial edition, with a 180-day expiration (a license may be purchased later).
- Select **Enter the product key**, and enter your product key, if you have already purchased a license.

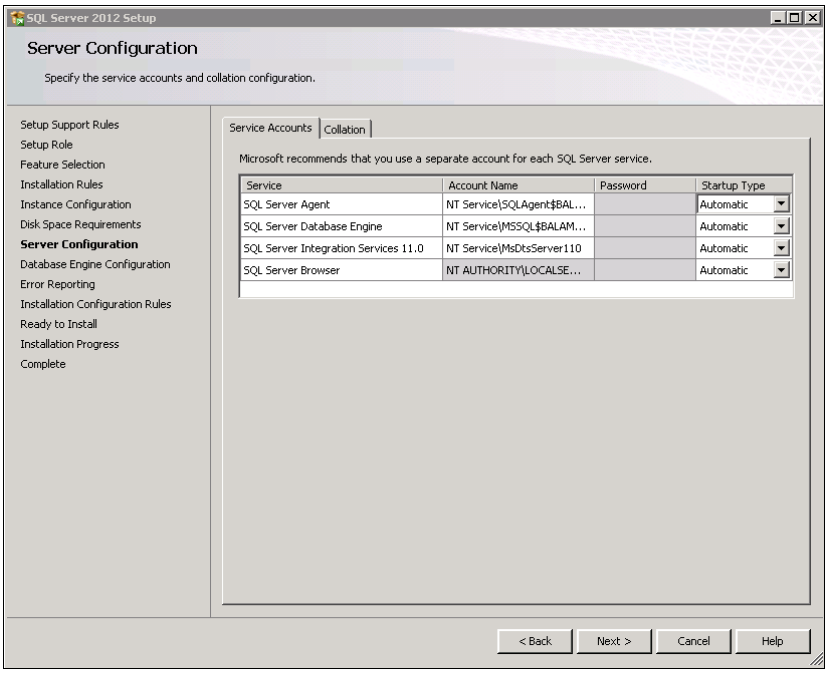
8. Click **Next**.
   The License Terms dialog is displayed.
9. Check **I accept the license** terms after reading the license terms fully.
10. Click **Next**.
    The Product Updates dialog is displayed.
11. If there are any product updates to install, it is recommended that you choose to perform any such updates by checking **Include SQL Server product updates** (it should be checked by default).
12. Click **Next**.
    The Install Setup Files dialog is displayed.
13. Click **Install** and wait for the **Setup Support Rules** panel to open (this will take some time). The results of another system check are displayed.
14. Again, make sure that all rules have **Status** "Passed" before proceeding. (To re-check the same rules, click **Re-run**.)
15. Click **Next**.
    The Setup Role dialog is displayed.
16. Select **SQL Server Feature Installation**, which allows you to customize exactly which features you want installed.
17. Click **Next**.
    The Feature Selection dialog is displayed.
18. Check at least the features shown below.



Note: These selections are for SQL Server 2012. Other versions may have slightly different choices.

19. Click **Next** and wait for the Installation Rules dialog to display.
20. The installer will perform yet another check of the system for potential problems. As before, make sure you have dealt with any issues it reports.
21. Click **Next**.
    The Instance Configuration dialog is displayed.
22. The **Instance ID** and locations of various directories for your SQL Server instance (as well as its name, if you choose to make it a named instance) are set at this step. Choose the settings for the instance you are creating. You may simply choose the defaults if you like.

    Note: If you choose to create a named instance (which is not required) record the name for future use.
23. Click **Next** and wait for the Disk Space Requirements dialog to display.
24. Make sure you have adequate disk space to install.
25. Click **Next** and wait for the Server Configuration dialog to display.
26. In the Service Accounts tab, enter settings as shown below.



Note: You may ignore the Collation tab.

27. Click **Next** and wait for the Database Engine Configuration dialog to display.
28. In the **Server Configuration** tab, under **Authentication Model**, check **Mixed Mode (SQL Server authentication and Windows authentication).**
29. Under **Specify the password for the SQL Server system administrator (sa) account**, enter and confirm a secure password of your choosing.
30. Under **Specify SQL Server administrators**, add all user accounts that will have access to the SQL Server database:
    a. Click **Add Current User** to add yourself.
    b. Click **Add**… to give access to other users, including the NetWitness Endpoint ConsoleServer Service account.

Note: When using a workgroup, you may create the same username and password on all machines that will access the SQL server. They must be identical to ensure a remote connection. Under a domain configuration, just add the desired users from the domain.

Note: You may ignore the Data Directories and FILESTREAM tabs.

31. Click **Next**.
    The Analysis Services Configuration dialog is displayed. This step is optional and not recommended as it consumes a high level of resources. This can also be configured at any

time following installation.

32. Click **Next**.
    The Reporting Services Configuration dialog is displayed. This step is optional and not recommended as it consumes a high level of resources. This can also be configured at any time following installation.
33. Click **Next**.
    The Error Reporting dialog is displayed.
34. Make sure any options to report data are left unchecked (which should be the default).
35. Click **Next**.
    The Installation Configuration Rules dialog is displayed, and runs a final system check.
36. As before, ensure there are no problems (all rules have **Status** "Passed").
37. Click **Next**.
    The Ready to Install dialog is displayed, which displays a summary of installation features and other information.
38. You may review this information, as a final check that you are ready to install.
39. Click **Install**.
    The Installation Progress dialog is displayed, with a progress bar for the main install sequence. This will take some time. When the install completes, the Complete dialog is displayed, reporting on the success of installation.
40. Ensure all components have a **Status** of "Succeeded".
41. Click **Close** and then exit the installer.

Part 2: Split the Microsoft SQL Temp DB into Eight Files

Split the Temp database into eight files with the following script:

```
ALTER DATABASE tempdb MODIFY FILE (NAME='tempdev' ,
FILENAME='D:\NWE\DATA\tempdb.mdf' , SIZE=25600MB, FILEGROWTH = 0)

ALTER DATABASE tempdb  ADD FILE (NAME='tempdev2',
FILENAME='D:\NWE\DATA\tempDB2.ndf', SIZE=25600MB, FILEGROWTH = 0)

ALTER DATABASE tempdb  ADD FILE (NAME='tempdev3',
FILENAME='D:\NWE\DATA\tempDB3.ndf', SIZE=25600MB, FILEGROWTH = 0)

ALTER DATABASE tempdb  ADD FILE (NAME='tempdev4',
FILENAME='D:\NWE\DATA\tempDB4.ndf', SIZE=25600MB, FILEGROWTH = 0)

ALTER DATABASE tempdb  ADD FILE (NAME='tempdev5',
FILENAME='D:\NWE\DATA\tempDB5.ndf', SIZE=25600MB, FILEGROWTH = 0)
```

```
ALTER DATABASE tempdb ADD FILE (NAME='tempdev6',
FILENAME='D:\NWE\DATA\tempDB6.ndf', SIZE=25600MB, FILEGROWTH = 0)
ALTER DATABASE tempdb ADD FILE (NAME='tempdev7',
FILENAME='D:\NWE\DATA\tempDB7.ndf', SIZE=25600MB, FILEGROWTH = 0)
ALTER DATABASE tempdb ADD FILE (NAME='tempdev8',
FILENAME='D:\NWE\DATA\tempDB8.ndf', SIZE=25600MB, FILEGROWTH = 0)
```

Part 3: Configure SQL DB Parallelism

Configure the maximum degree of parallelism and the cost threshold for parallelism, using the following script:

```
USE ECAT$PRIMARY;
GO
EXECsp_configure'show advanced options', 1;
GO
RECONFIGURE WITH OVERRIDE;
GO
EXECsp_configure'max degree of parallelism', 8;
GO
RECONFIGURE WITH OVERRIDE;
GO
EXECsp_configure'show advanced options', 1 ;
GO
RECONFIGURE WITH OVERRIDE;
GO
EXECsp_configure'cost threshold for parallelism', 50 ;
GO
RECONFIGURE WITH OVERRIDE;
GO
```

Step 2: Configure SQL Server

This topic provides information about configuring SQL server. The SQL Server configuration includes two procedures:

- Enable TCP/IP with Encryption
- Configure SQL Server Option CLR ENABLED

Caution: Making any modifications to the Microsoft SQL database other than what is specified in the NetWitness Endpoint documentation is not supported and may result in errors when installing the NetWitness Endpoint product.

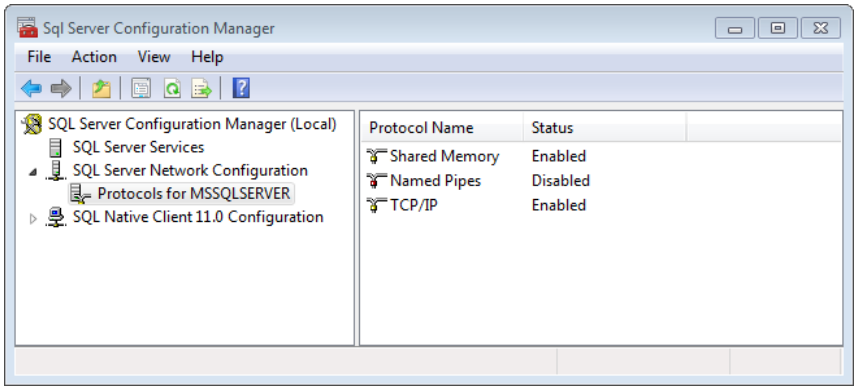
Enable TCP/IP with Encryption

Enabling TCP/IP Encryption is essential to protect your data across the network. This is the only way to protect the sensitive information sent from the database to the ConsoleServer or to the UI.

Note: TCP/IP encryption is mandatory for a multi-server installation. This also must be enabled on all secondary servers.

To enable TCP/IP with encryption:

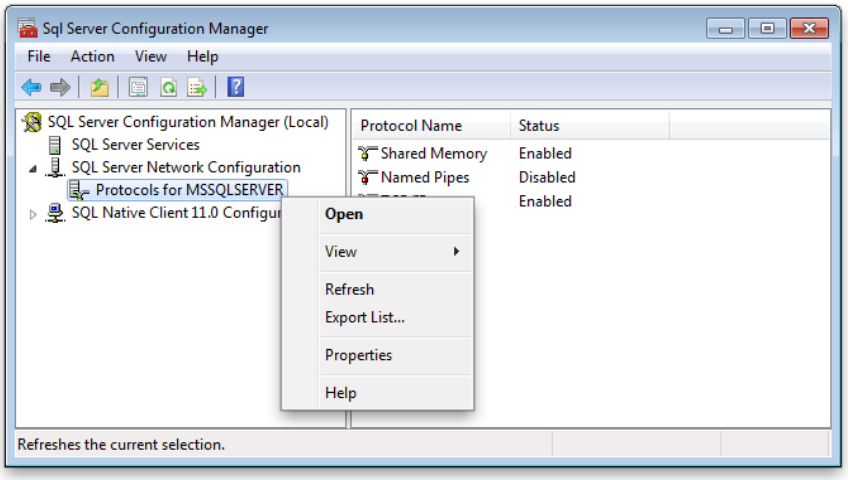
1. Go to **Start > All Programs > Microsoft SQL Server 2012 > Configuration Tools > SQL Server Configuration Manager**.
2. In the navigation panel on the left, expand **SQL Server Network Configuration** to reveal the nodes under it.
3. Select the node of the instance you want to configure (there will be a node for each instance of SQL Server installed on the current machine).



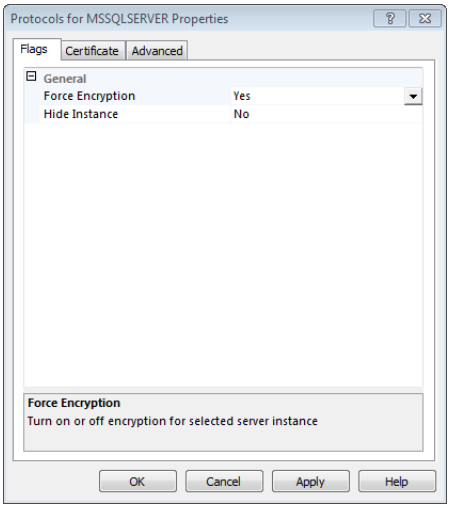
4. Make sure that next to **TCP/IP**, the status is set to **Enabled** (it may already be enabled). This can be changed using the contextual menu (right-click).

Note: The ports used by the SQL Server instance can also be changed from this window. Consult the SQL Server documentation.

5. Right-click the instance node in the navigation panel and select **Properties**.



6. On the **Force Encryption** property, select **Yes** to enable encryption.



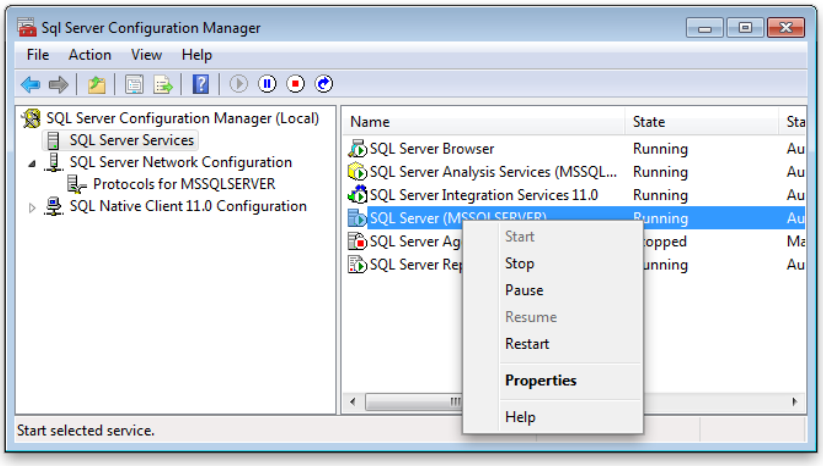
7. Click **OK** to save changes.

8. Select **SQL Server Services** in the navigation panel. Your SQL Server instance is displayed in the list on the right, as "SQL Server (NAME-OF-YOUR-SQLSERVER-INSTANCE)".

   Note: An unnamed instance will appear as "SQL Server (MSSQLSERVER)".

9. Right-click your instance, and select **Restart**. This must be done for your changes to take effect.

   Note: Only instances that have been changed need to be restarted.



10. When the instance has finished restarting, select **File > Exit** to quit the Configuration Manager.

Configure SQL Server Option CLR ENABLED

The **CLR ENABLED** option must be set to 1 to use the NetWitness Endpoint UI. Failure to enable this option will prevent the NetWitness Endpoint UI from connecting to the SQL Server.

Note: This may be configured automatically for you.

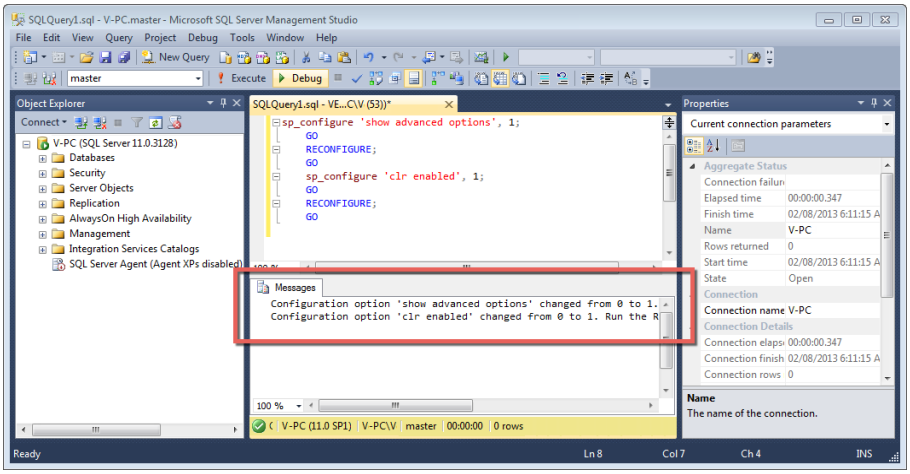
To enable the CLR ENABLED option:

1. Go to **Start > All Programs > Microsoft SQL Server 2012 > SQL Server Management Studio**.
2. If presented with a login window, log on with Windows authentication by clicking **Connect**.
3. Click **New Query** and paste the following SQL script:

```
sp_configure 'show advanced options', 1;
    GO
    RECONFIGURE;
    GO
    sp_configure 'clr enabled', 1;
    GO
    RECONFIGURE;
    GO
```

4. Click **Execute**.
   As shown below, the Messages tab should say:
   `Configuration option 'show advanced options' changed from 0 to 1.`

```
Configuration option 'clr enabled' changed from 0 to 1
```



5. Click **File > Exit** to quit Management Studio.

> **Note:** You may be asked if you want to save the query to a file, which you may do, although it is not necessary. For more information, go to: http://msdn.microsoft.com/en-us/library/ms131048.aspx

Step 3: Install Primary ConsoleServer

Now that you have Microsoft SQL Server installed and configured for NetWitness Endpoint (NWE), you can install the NetWitness Endpoint Primary ConsoleServer (also referred to as NetWitness Endpoint Primary Server or just NetWitness Endpoint Server). You can install the Primary ConsoleServer with or without a NetWitness Endpoint UI (the following steps, however, assume you are installing both a NetWitness Endpoint Server and a NetWitness Endpoint UI).

> **Note:** The NetWitness Endpoint Primary Server depends on the Microsoft Visual Studio 2015, 2012, and 2010 runtimes. However, the installer will automatically install these if they are not found on the target machine.

Before You Begin

If you are setting up a multi-server environment, you must first set up a network shared downloads folder, into which agents will upload files. This must be accessible to the secondary servers. Record the path name of this folder, which you will need later in the installation process.

ConsoleServer Arguments

While installing the NetWitness Endpoint Primary ConsoleServer, you may have to run various commands from the command line. By running the help command, you get the supported arguments for the ConsoleServer.

From the command line, execute the command `ConsoleServer -help`
For example:
`C:\ECAT\Server>consoleserver -help`

The supported arguments are:

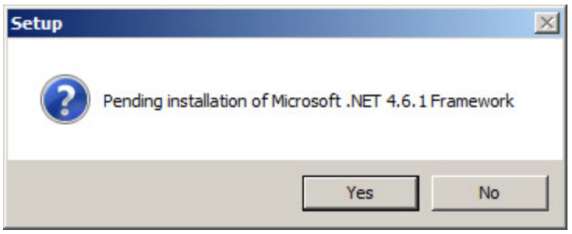
```
/help
Shows this help message
/logerr[:Output file path]
Use this argument to optionally redirect the error output to a
different file. Specify 'none' as path to disable logging.
/cid
Displays the license agreement and license computer ID. (CID)
/install
Installs ECAT Server as a service. Cannot be used with other
arguments.
/uninstall
Removes RSAECATServer service.
```

Procedure

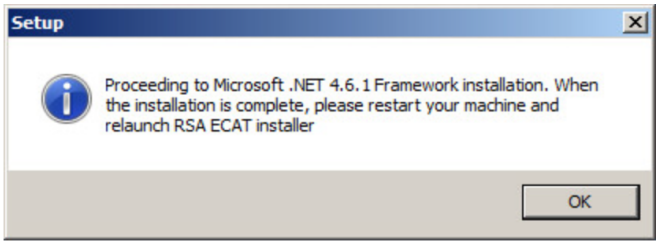
To install a Primary ConsoleServer:

Note: If you attempt to do a new install of a version of NetWitness Endpoint that only supports update installations, a message will display and you will not be able to continue. Refer to the associated NetWitness Endpoint Release Notes for supported installation and upgrade paths.

1. If not already done, unzip the archive file:
   rsa_nwe_*<4.4.x.x>*_sw.zip
2. Find and double-click the installer **executable** file:
   rsa_nwe_*<4.4.x.x>*_sw.exe
3. A prerequisite for NetWitness Endpoint includes the Microsoft .NET Framework 4.6.1. If this is not already installed, the following screen will display (if Microsoft .NET Framework 4.6.1 is already installed, the RSA NetWitness Endpoint Welcome dialog is displayed, as shown in Step 8):

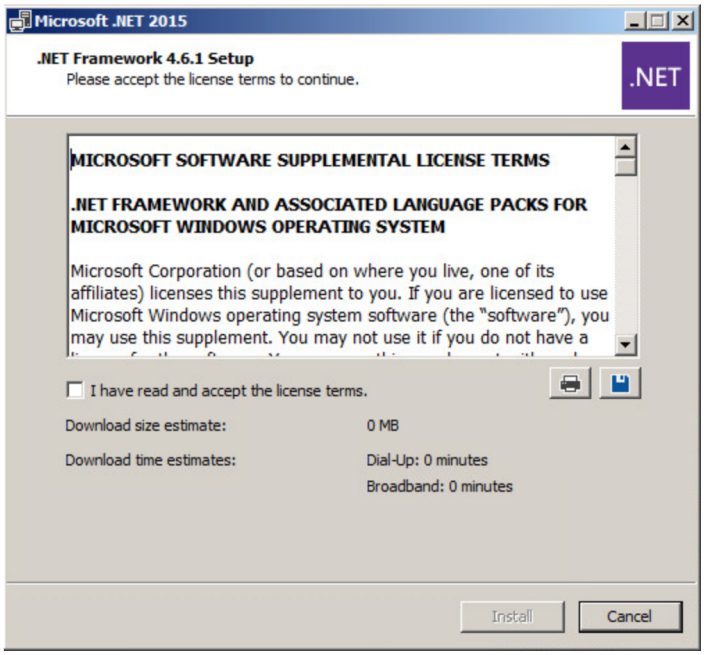


4. Click **Yes** to continue (if you click **No**, the installer quits and you will not be able to complete any further installation).
   The following dialog is displayed:

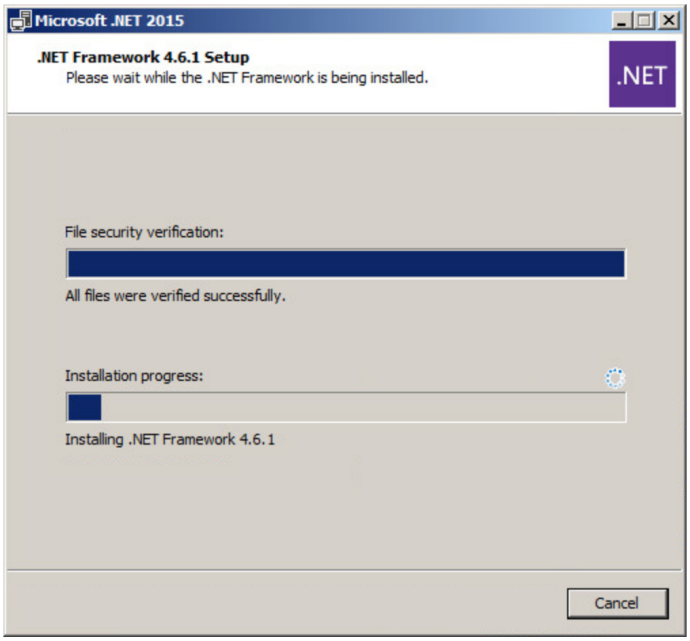


Note: If the machine on which you are installing NetWitness Endpoint has not been kept current with Windows updates, a message may display indicating that the installation of Microsoft .NET 4.6.1 is blocked pending the prerequisite installation of the Windows update corresponding to KB2919355. You must update the machine before you can proceed with the Microsoft .NET 4.6.1 installation. For more information, see:
https://support.microsoft.com/en-us/kb/2919355
https://msdn.microsoft.com/en-us/library/hh925569%28v=vs.110%29.aspx

5. Click **OK** to continue.
   The Microsoft .NET Framework 4.6.1 Setup dialog is displayed:

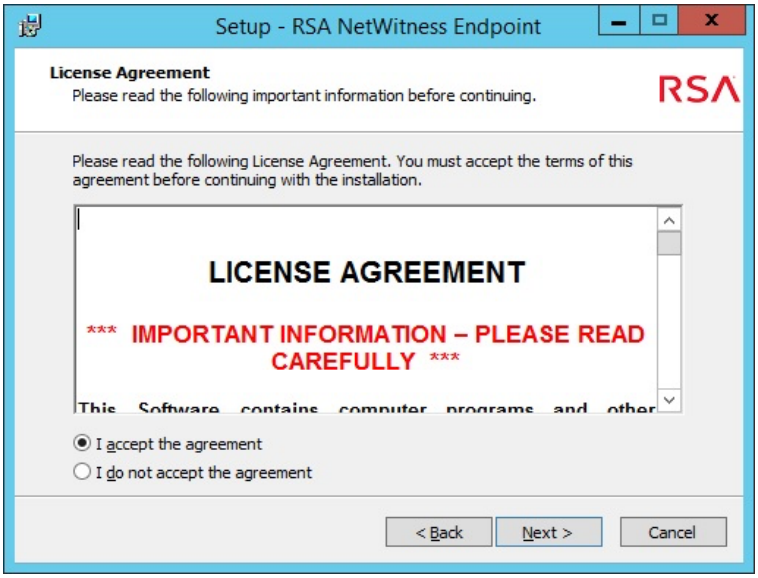


6. Select the checkbox to indicate you accept the license terms and then click **Install**. The following dialog is displayed to indicate the installation progress:

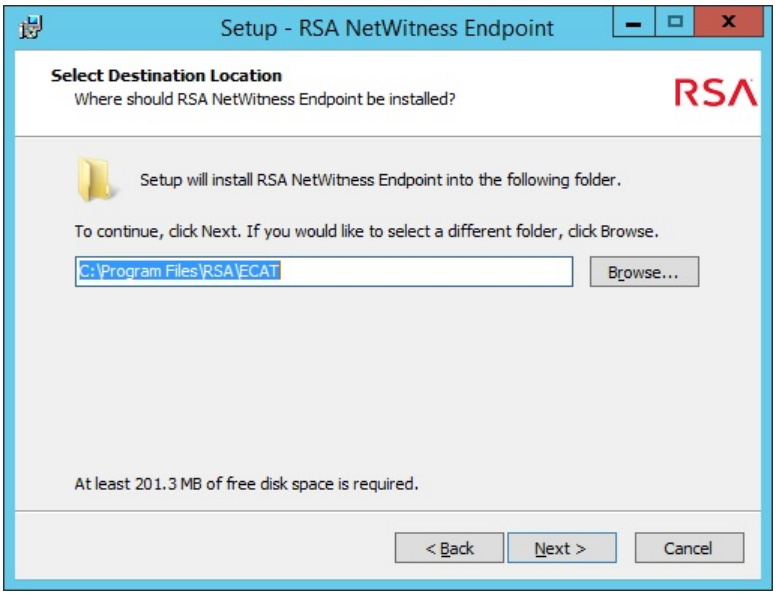


7. Once the installation is complete the installer dialog will close and you will have to reboot the machine.
8. Re-launch the NetWitness Endpoint installer executable file as instructed above in Step 2. The RSA NetWitness Endpoint installer Welcome dialog is displayed.

9. Click **Next** to continue.
   The License Agreement dialog is displayed.



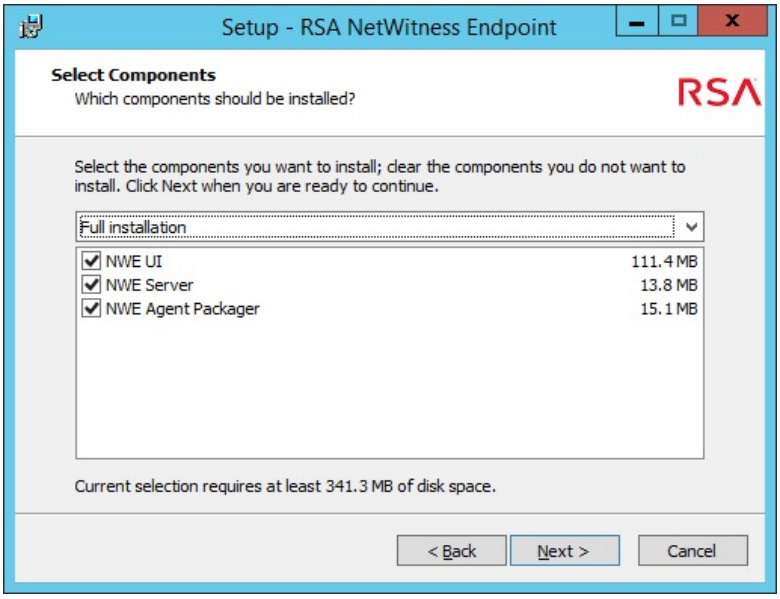
10. You must accept the terms of the license agreement to proceed. Click **Next**.
    The Select Destination Location dialog is displayed, as shown below:



11. Select the destination location for the installation files. A default location is provided, or you can click **Browse...** to select a different location. All components will be installed in the selected location, with subfolders for UI, Server, and Agent.

Note: If you have installed previous versions of NetWitness Endpoint you may notice that the default location has changed from **C:\ECAT** to **C:\Program Files\RSA\ECAT**. Although it is still possible to install NetWitness Endpoint in **C:\ECAT**, it is now recommended to install in **C:\Program Files\RSA\ECAT**.

12. Once you have selected the desired destination location for the installation files, click **Next**. The Select Components dialog is displayed, as shown below:



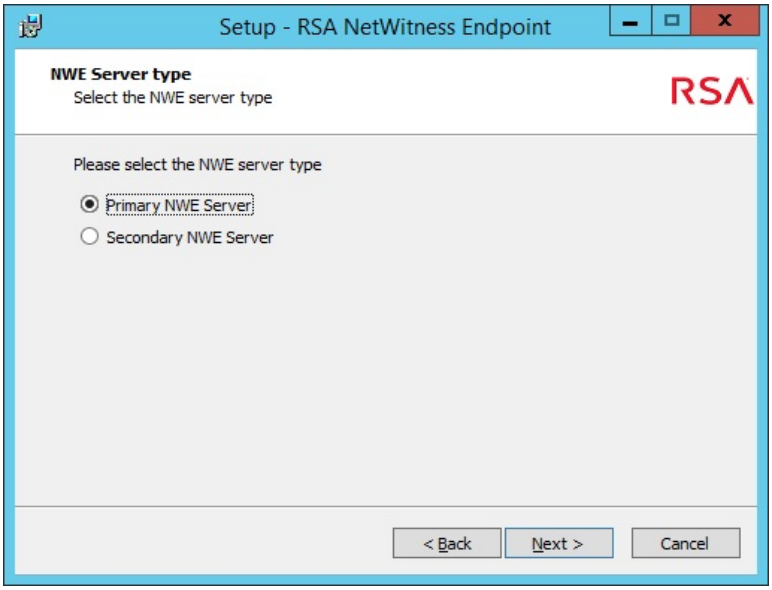
13. Select the installation type and components you wish to install from the following options in the drop-down list:

    - **Compact installation**: installs the NetWitness Endpoint UI only
    - **Full installation**: installs the NetWitness Endpoint UI, NetWitness Endpoint Server, and NetWitness Endpoint Agent Packager
    - **Custom installation**: installs the components selected by clicking the checkboxes next to the desired item below the drop-down (For example, to install just the NetWitness Endpoint Primary Server, select **Custom installation** and check the box next to **NWE Server**.)

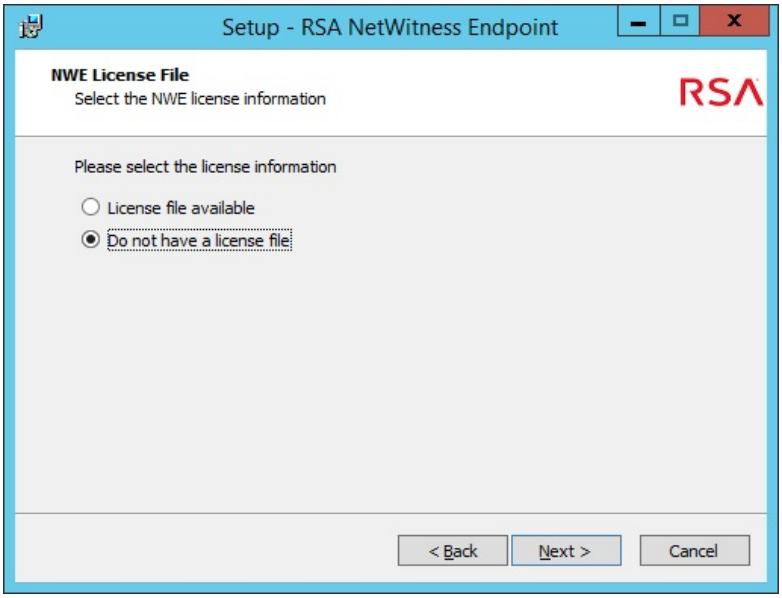
    Note: At this stage, the installation of the NetWitness Endpoint UI is optional. Its absence will not prevent the Primary ConsoleServer from working properly.

    Note: Each of the components selected to install will create a separate folder under the installation destination folder previously selected in Step 11. For example, if using the default installation destination folder, the NetWitness Endpoint UI will be installed to: **C:\Program Files\RSA\ECAT\UI**.

14. Click **Next**.
    The NWE Server Type dialog is displayed, as shown below:



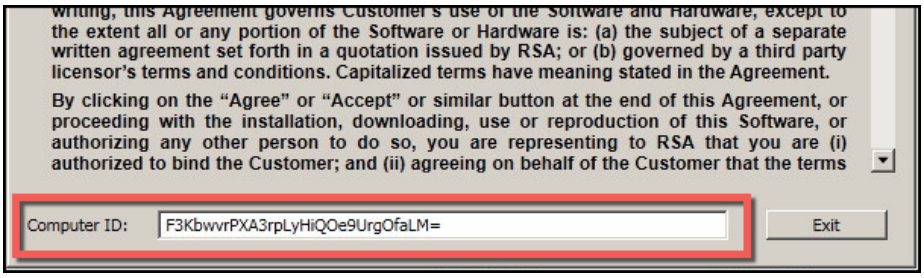
15. Select **Primary ECAT Server** and click **Next**.
    The NWE License File dialog is displayed, as shown below:



16. Do one of the following:

    - If you have a license file, select **License file available** and click **Next**.
    - If you do not have a license file, select **Do not have a license file**. You will then need to agree to a License Agreement to continue. Click **I Agree** on the License Agreement dialog shown below:

This will generate a **Computer ID**, which you should write down.

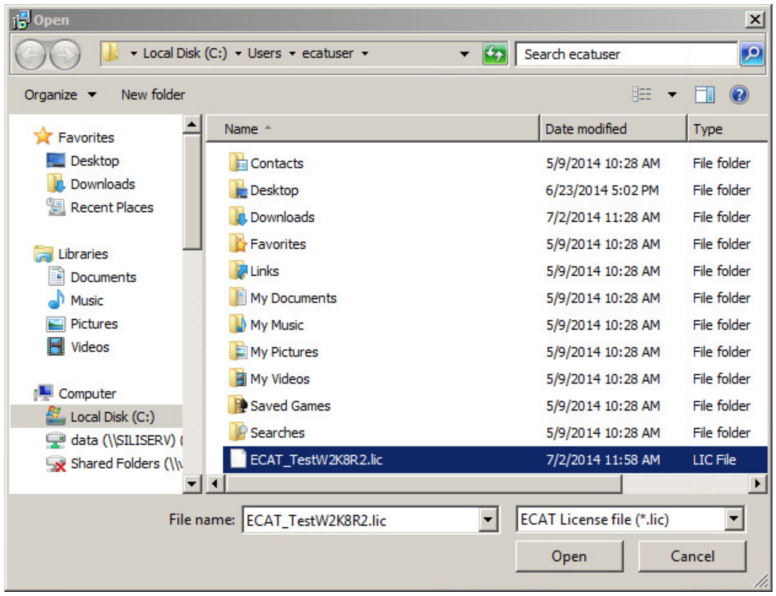


Click **Exit** to quit installation. You must now generate a license file. Instructions for downloading your license should have been sent via email to the contact listed on the order (if you did not receive the email, contact RSA Customer Support). For further step-by-step instructions on generating your license file, go to RSA Download Central. Once you have your license file you will have to re-launch the NetWitness Endpoint installation.

Note: If you lose your Computer ID (CID), you can retrieve it by running the following ConsoleServer command from the command line. This command displays the license agreement and CID:

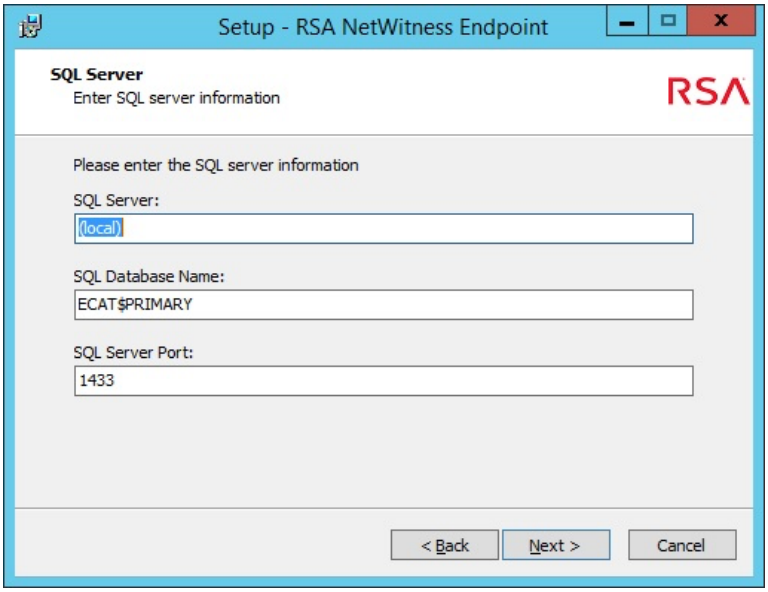
```
ConsoleServer /cid
```

17. Browse to the location of your license file, as shown below:



18. Click **Open**.

    The SQL Server dialog is displayed, as shown below:

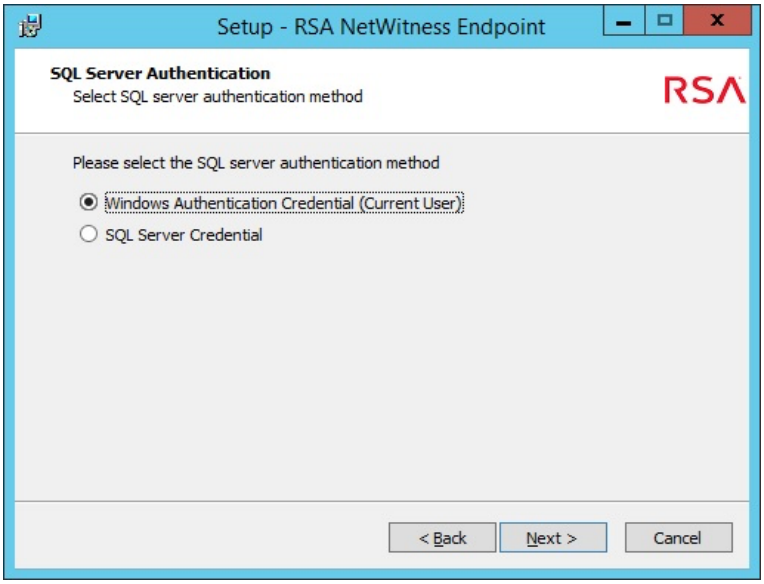


19. Enter the SQL Server you are using for NetWitness Endpoint. You can use the default entry for SQL Database Name or enter a new name of your choosing. You can leave the default value for SQL Server Port, enter 0, or leave it blank.

    (If a port number other than the default value is detected, a message is displayed to indicate that SQL Server is running on port 1443, and you must click **OK** to continue.)

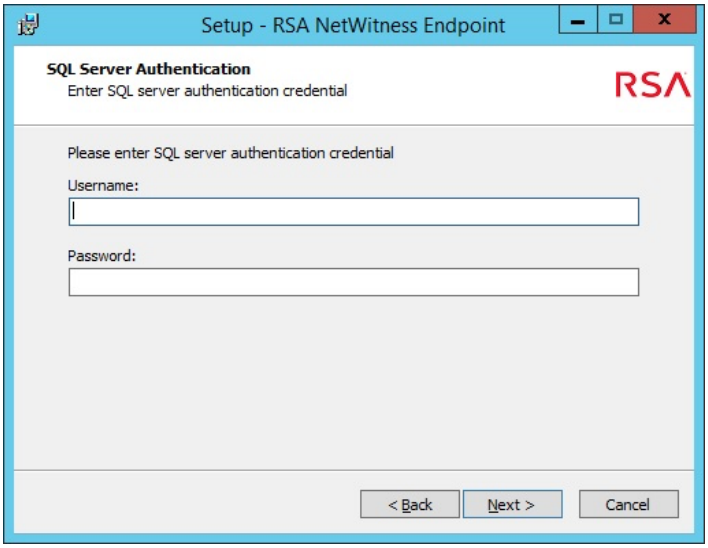
20. Click **Next**.

    The SQL Server Authentication dialog is displayed, as shown below:

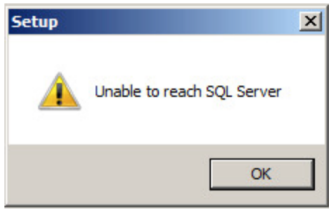


21. Do one of the following:

    - Select **Windows Authentication Credential** and click **Next**.
    - Select **SQL Server Credential** and click **Next**. The following dialog is displayed:



      Enter the necessary SQL Server authentication username and password and click **Next**. The NetWitness Endpoint installer will now test the database access for the SQL Server, SQL Database Name, and SQL Server Port. If access is successful, you will proceed to the next step. If the installer cannot reach the SQL Server the following message is displayed:



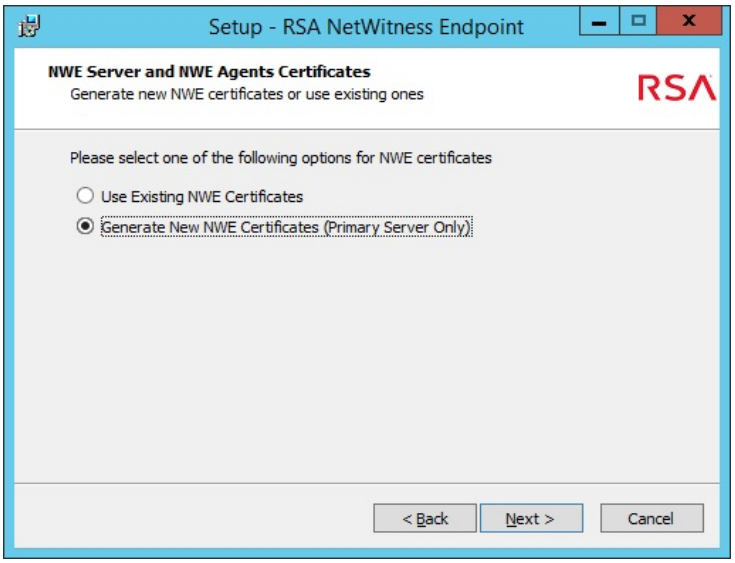
Click **OK**. The SQL Server Authentication dialog displays and you can re-enter the SQL Server credentials or click **Back** to return to the SQL Server Authentication dialog if you wish to change your authentication method. You must resolve the authentication before proceeding to the next step.

Note: It is considered a best practice to select the default: **Windows authentication credentials (current user)**. It is not recommended to use SQL Server credentials to configure a production database. To change the authentication type after completing the installation, see Manage Authentication After Installation.

Note: If SQL Server is installed on a remote machine and cannot be reached, you may need to manually create a firewall rule on the remote SQL Server to allow communication on TCP port 1433.

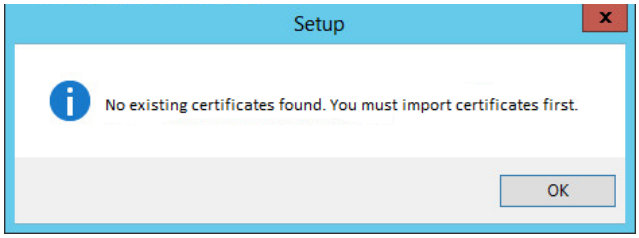
Note: If in attempting to connect to the SQL Server it is determined that there is already an existing database, a message is displayed with options to either reuse or delete the existing database. For more information, see Manage Existing Database During Installation.

22. The NWE Server and NWE Agents Certificates dialog is displayed, as shown below:

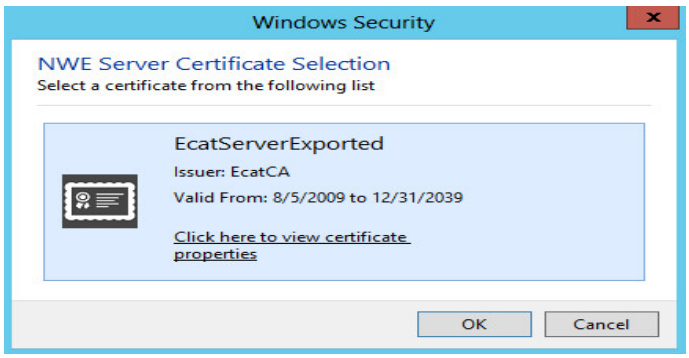


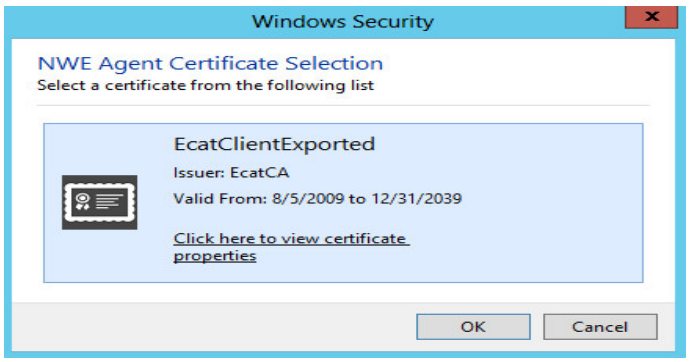
23. Do one of the following:

- If you already have NetWitness Endpoint certificates, you can select **Use Existing NWE Certificates** and click **Next**.
  If no NetWitness Endpoint certificates are found, the following message is displayed:



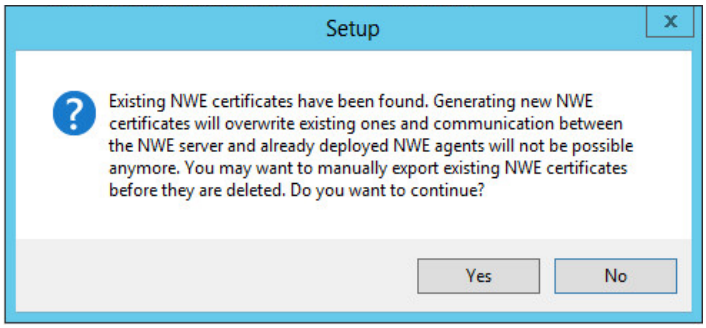
  Click **OK** to return to the previous dialog.
  If NetWitness Endpoint certificates are found, the certificates are displayed as shown below:



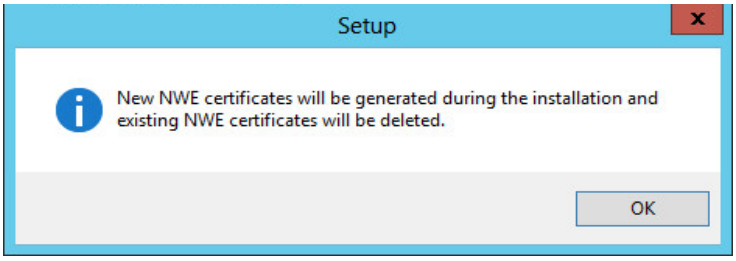


  Click **OK** to accept each certificate. The ECAT Server Directories dialog will be displayed, as shown below in Step 20.

- If you do not have certificates, you can select **Generate New NWE Certificates** and click **Next**.
  If existing certificates are found, the following message is displayed:



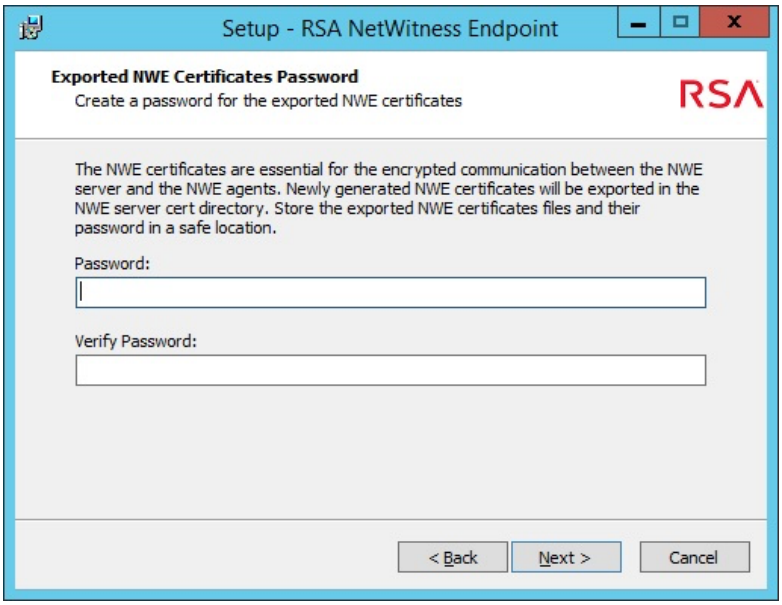
Click **No** to return to the previous dialog. If you click **Yes**, the following message is displayed:



Click **OK** to continue deleting existing certificates.

Caution: Deleting existing NetWitness Endpoint certificates cannot be undone and may negatively impact your communication between the NetWitness Endpoint Server and already deployed NetWitness Endpoint agents. It is strongly advised that you first manually export existing NetWitness Endpoint certificates before they are deleted. After clicking **OK**, the certificates are not deleted immediately but rather at the time of actual installation.

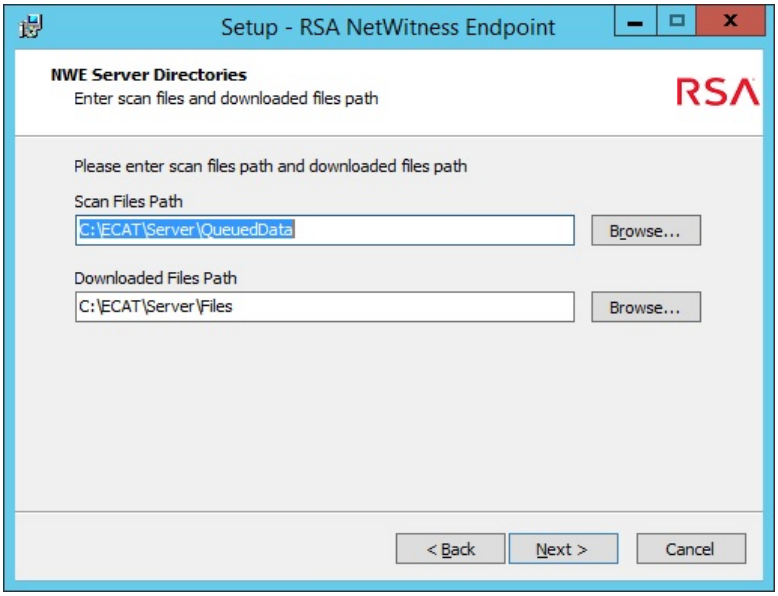
24. If you previously selected to generate new certificates, the Exported NWE Certificates Password dialog is displayed, as shown below:



You must create a password for the new certificates, which will be exported into the NetWitness Endpoint Server cert directory (default location = **C:\Program Files\RSA\ECAT\Server\Cert**). You should record this password in a secure location for future reference.

Click **Next**.

25. On the NWE Server Directories dialog, shown below, you must enter the desired directories for scan files and downloaded files.



26. A default location is provided for the **Scan Files Path**, but you can click **Browse…** to select a different location for storing agent scan files.

Note: If the NetWitness Endpoint Server is on a different machine than the SQL database, you must create a shared folder on the SQL database server. There are different methods of providing access to the database. For more information, see Scan Data Folder.

Note: The default location is the same as previous NetWitness Endpoint installations to maintain backward compatibility. Also, it is not advisable to store files in **C:\Program Files\RSA\ECAT\Server**.

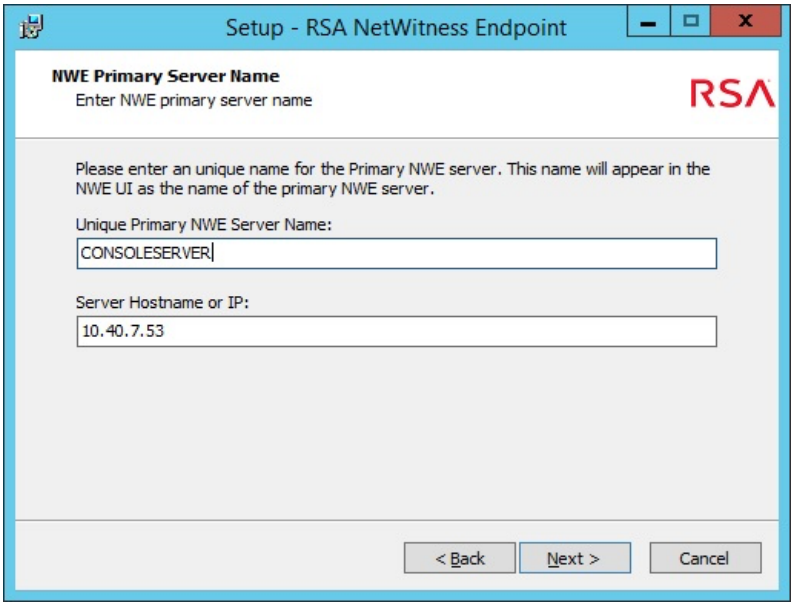
27. A default location is provided for the **Downloaded Files Path**, but you can click **Browse…** to select a different location for storing downloaded files.

Note: In a multi-server installation, this path *must* be a shared network folder.

Note: The default location is the same as previous NetWitness Endpoint installations to maintain backward compatibility. Also, it is not advisable to store files in **C:\Program Files\RSA\ECAT\Server**.

28. Click **Next**.

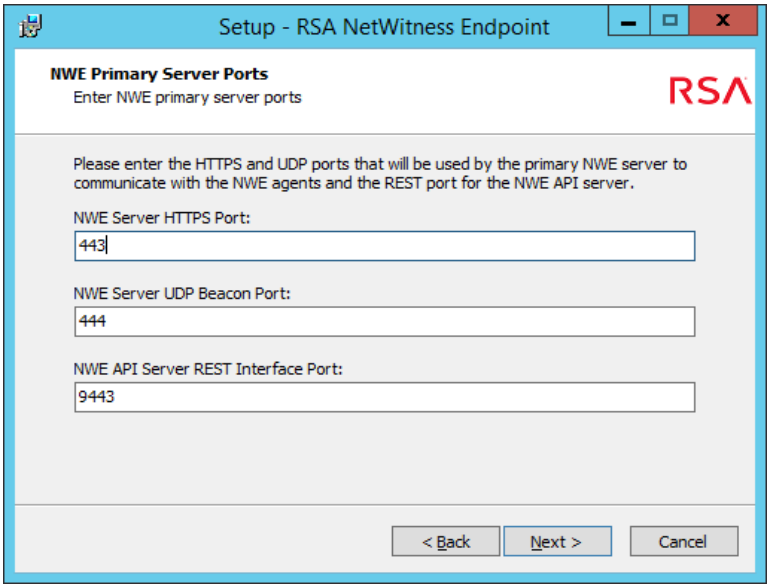
The NWE Primary Server Name dialog is displayed, as shown below:



29. Provide a unique name for the Primary ConsoleServer. (The Installer will provide a default suggestion, but you may change it.)

Note: Your IP address will be provided automatically for **Server Hostname or IP**. If you enter a Server Hostname instead, it must be a fully qualified DNS name for the Machine Containment function to work properly. If you enter a partial DNS name, agent machines will go offline and a manual agent uninstall and reinstall will be required.

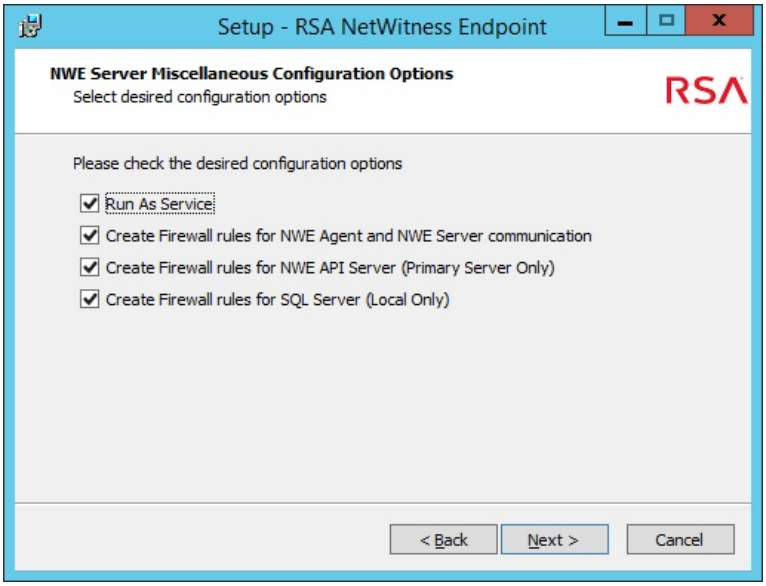
30. Click **Next**.
    The NWE Primary Server Ports dialog is displayed, as shown below:



31. The following default port numbers, which are used internally by NetWitness Endpoint for communication between its various components, are provided, but can be changed:
    NWE Server HTTPS Port: 443
    NWE Server UDP Beacon Port: 444
    NWE API Server REST Interface Port: 9443

32. Click **Next**.
    Port availability is checked and if any ports are found to be invalid or already in use an error message is displayed. You will need to change the necessary port numbers before continuing.

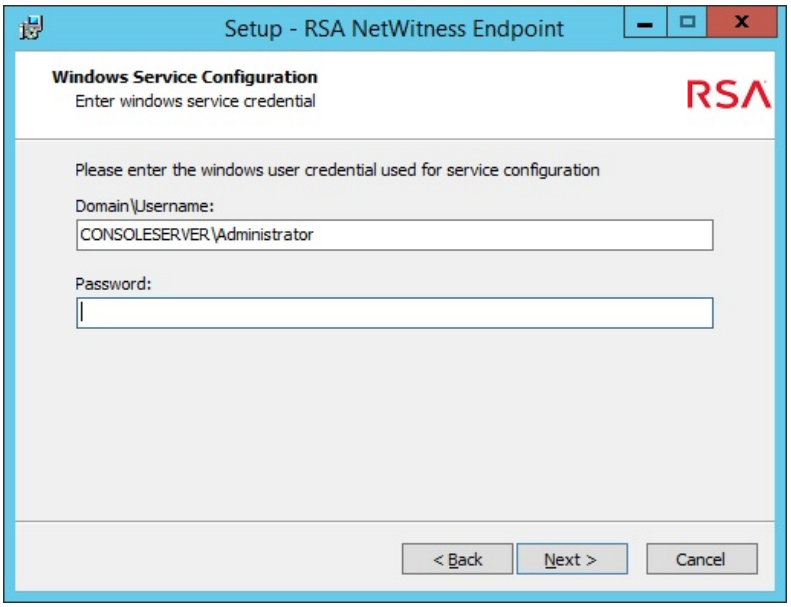
33. On the NWE Server Miscellaneous Configuration Options dialog, shown below, you can select additional configuration options.



34. Select the checkboxes to enable the desired options:

- **Run As Service**: Enable this option if you want the NetWitness Endpoint Server to run as a service. Selecting this option also installs the Endpoint Meta Integrator as a service (for more information, see "NetWitness Suite Endpoint Meta Integration" in the *NetWitness Endpoint User Guide*).
- **Create Firewall rules for NWE Agent and NWE Server communication**: This option is necessary if you have an active firewall as you will need to create firewall rules to allow communication between the NetWitness Endpoint Server and the NetWitness Endpoint Agent through the firewall.
- **Create Firewall rules for NWE API Server (Primary Server Only)**: This option will be grayed out if installing an NetWitness Endpoint Secondary Server.
- **Create Firewall rules for SQL Server (Local Only)**: This option may be necessary if you have an active firewall as you may also need to create a firewall rule to allow communication between the NetWitness Endpoint Server and SQL Server. This option will be grayed out if SQL Server runs on a remote machine.

35. Click **Next**.
    If you selected the **Run As Service** option on the previous dialog, the Windows Service Configuration dialog is displayed, as shown below:

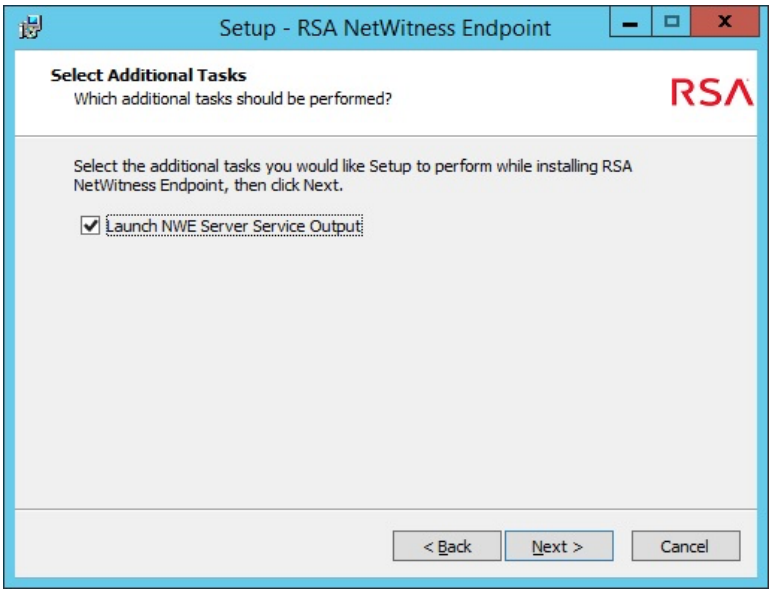


36. Enter a username and password to allow the NetWitness Endpoint Server, which will be running as a service, to log on to the machine on which the NetWitness Endpoint Server is installed. The current Domain and Username are automatically entered by default.

> **Note:** Enter a username in the form DOMAIN\username, and its password. You may use either SQL Server credentials or your Windows authentication. If you use Windows authentication, you must choose an account that has administration privileges on the local machine. The entered credentials and database rights will be validated when you click **Next**.

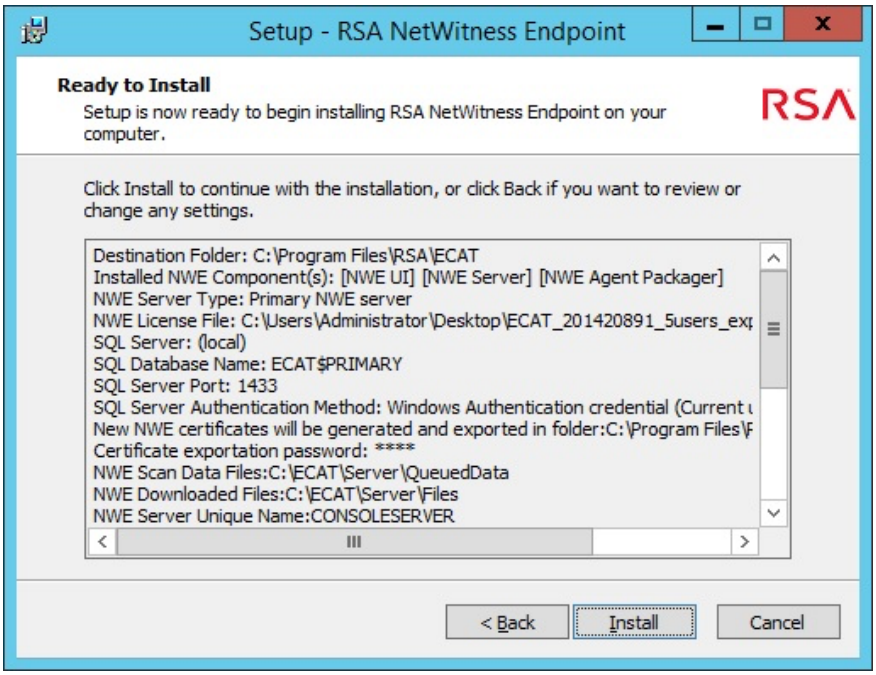
37. Click **Next**.

    If you previously selected the **Run As Service** option, the Select Additional Tasks dialog is displayed, as shown below:



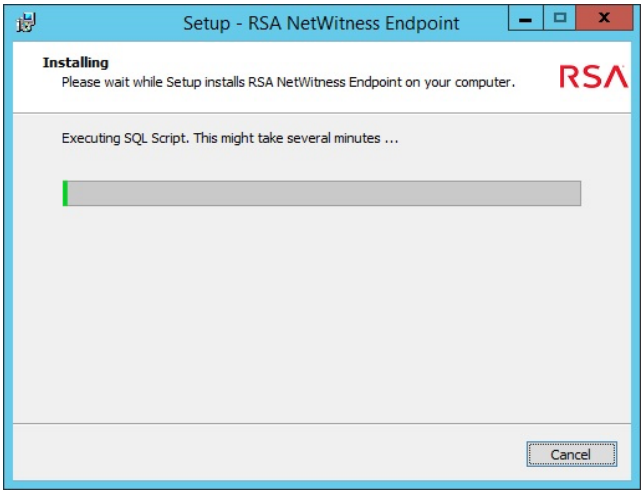
38. Select to enable the **Launch NWE Server Service Output** option if you want this action performed during Setup.

39. Click **Next**.
    The Ready to Install dialog is displayed, as shown below:



40. You should review all of the options you selected in the previous steps, which are displayed in this dialog. If you wish to change any options you may do so by clicking **<Back** to go back through the previous dialogs.

41. Click **Install** to proceed with installing the NetWitness Endpoint Server.
    The Installing dialog is displayed, as shown below:



42. At this point the installer performs the following functions according to selected options:
    - Creates the SQL database, configuration files for NetWitness Endpoint Server and API server, services, and firewall rules
    - Generates NetWitness Endpoint certificates (and deletes existing NetWitness Endpoint certificates)
    - Copies files

Note: The installation will take some time. Please wait while the process is completed, or click **Cancel** to cancel the installation.

43. When the installation process is complete, the following dialog is displayed:

44. Click **Finish** to exit the NetWitness Endpoint Setup Wizard.

Note: If you selected to run the NetWitness Endpoint Primary Server as a service, you should set the service to restart automatically following a failure, using the server properties dialog.

Note: If you are also using RSA NetWitness Suite 11.0 or later and wish to use the NetWitness Endpoint Meta Service to integrate data from NetWitness Endpoint agents with the NetWitness Suite Log Decoder, you must also install Java JRE version 8 update 131 or later (only Java JRE version 8 and its updates are supported, Java JRE versions 9 or later are not supported). For more information on Java JRE, go to http://www.oracle.com/technetwork/java/index.html. For more information about the Meta Service integration, see "NetWitness Suite Endpoint Meta Integration" in the *NetWitness Endpoint User Guide*.

Step 4: (Optional) Export Primary Server Certificates

This process is done automatically during the installation process and all generated certificates are exported to C:\Program Files\RSA\ECAT\Server\cert.

For reference purposes, this topic provides information about making a backup of the Primary Server certificates by exporting the certificates from the ConsoleServer machine.

Note: Losing the Private Keys for the certificates would break the secure connection between the Agents and the ConsoleServer. Hence, you must make sure to back up the Private Keys in a secure place from which they can be restored during a fresh Windows install in the event of a material failure of the server.

Once a primary server is installed, it is highly recommended to export its encryption certificates to a file, for use on other machines, or on the same machine if they were deleted by mistake from the certificate location. You will also need to perform this step if (1) the NetWitness Endpoint ConsoleServer is to be run from a different location, or (2) you wish to generate packages on a different machine than the one they were created on, or (3) you are planning a multi-server deployment.

Certificate Public Key

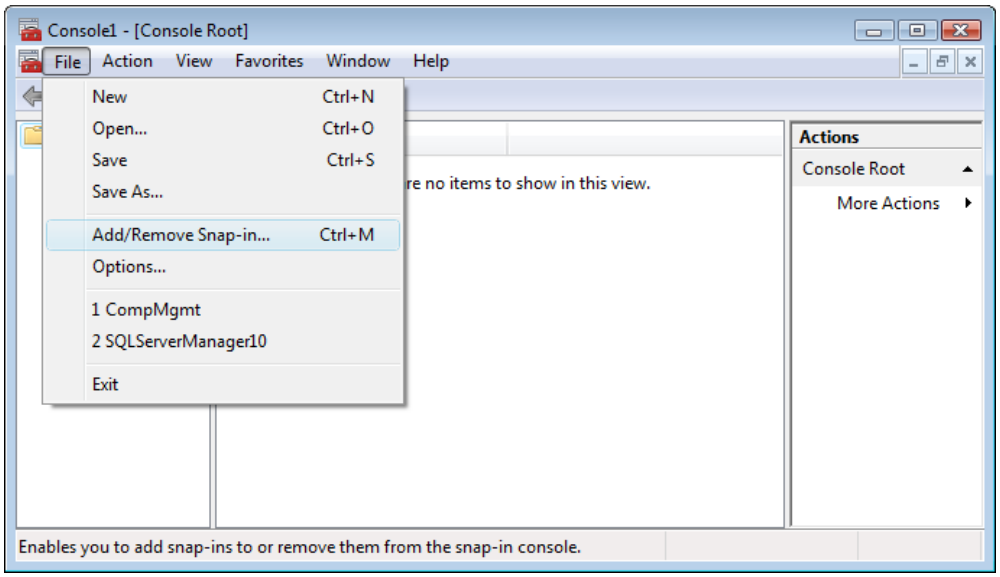
The Public Key for the generated certificates can be found in the folder:
SERVER_INSTALLATION_FOLDER\Server\cert

Exporting Certificates from the ConsoleServer Machine

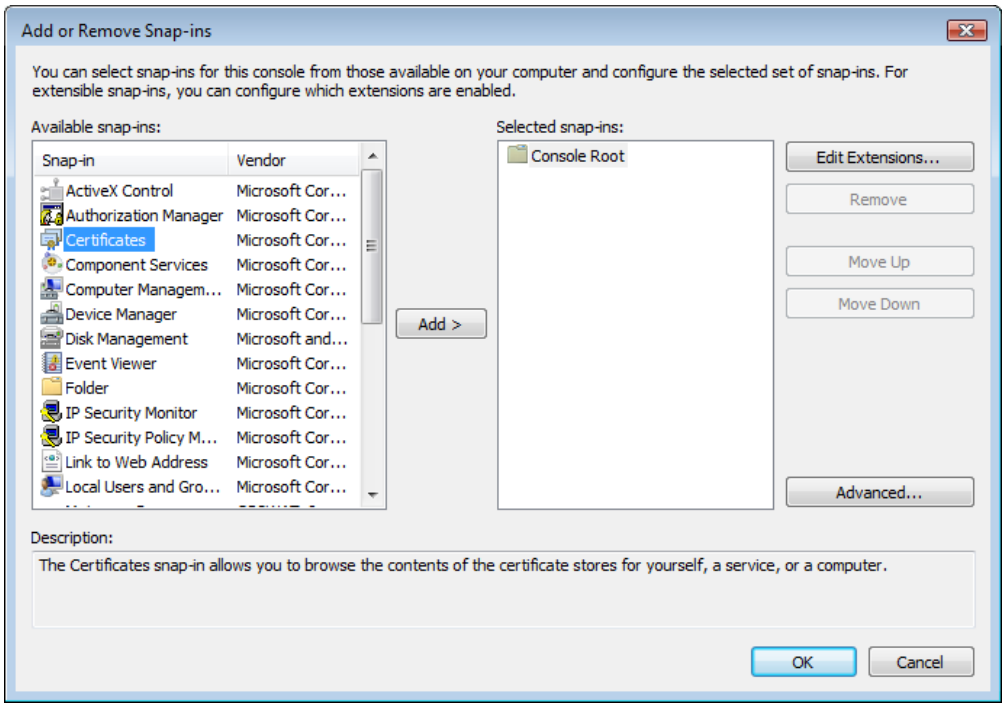
If for any reason the certificates files are not accessible from the above folder, it is also possible to export them from the server.

To export the certificates from the NetWitness Endpoint ConsoleServer machine:

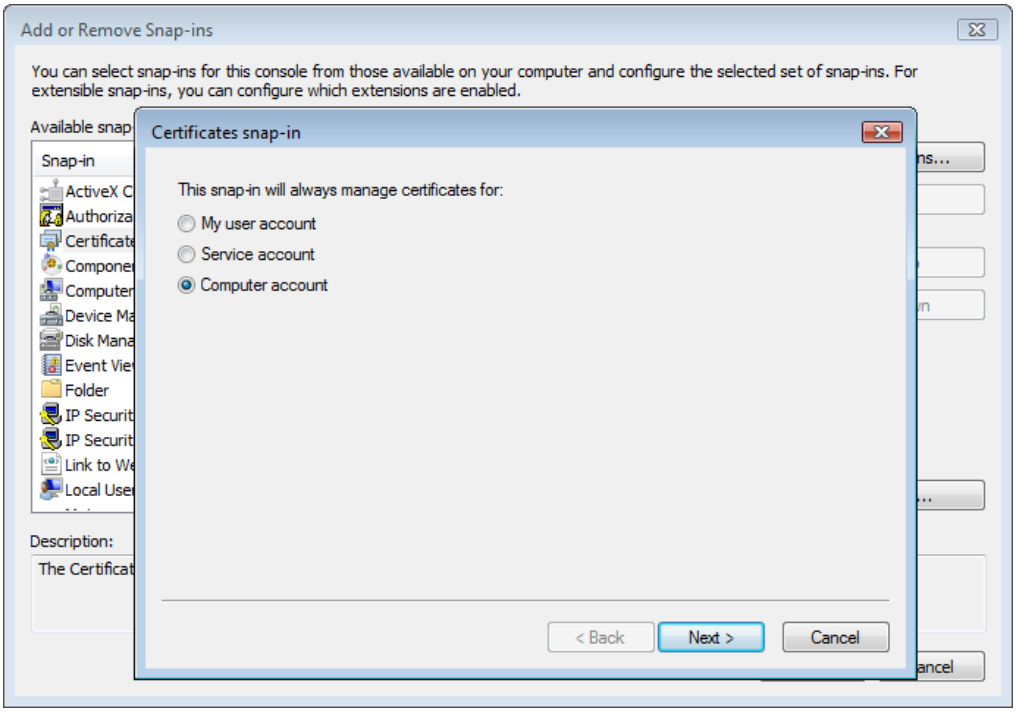
1. Run **mmc** from a command line. This opens the Microsoft Windows management console.
2. Select **File > Add/Remove Snap-in**.



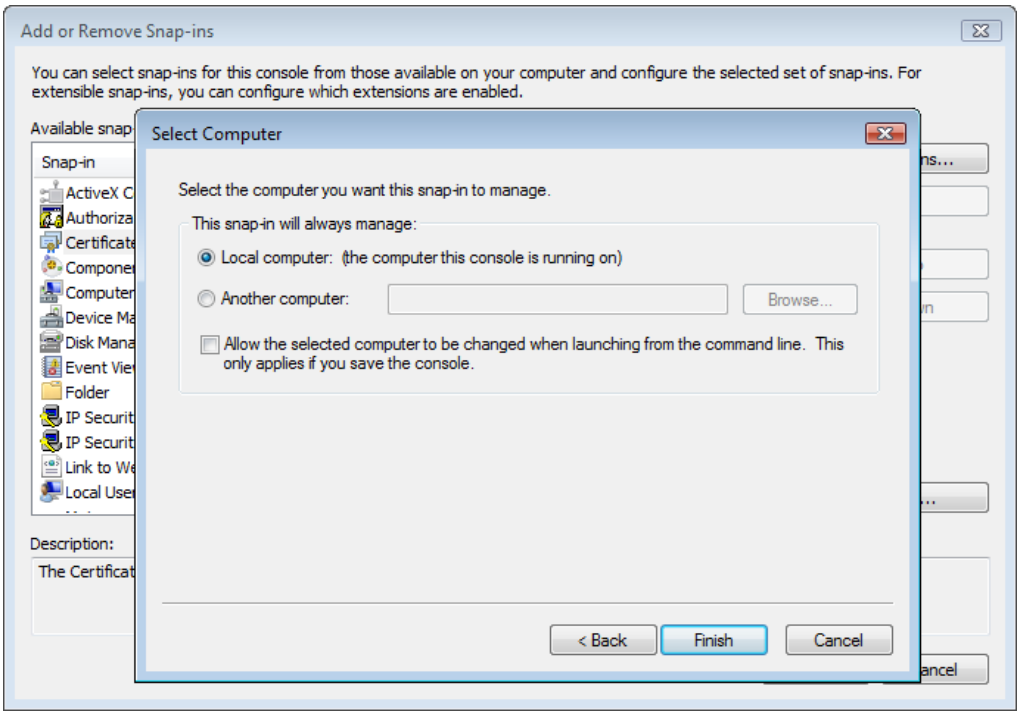
3. From the list of available snap-ins, select **Certificates** and click **Add**.



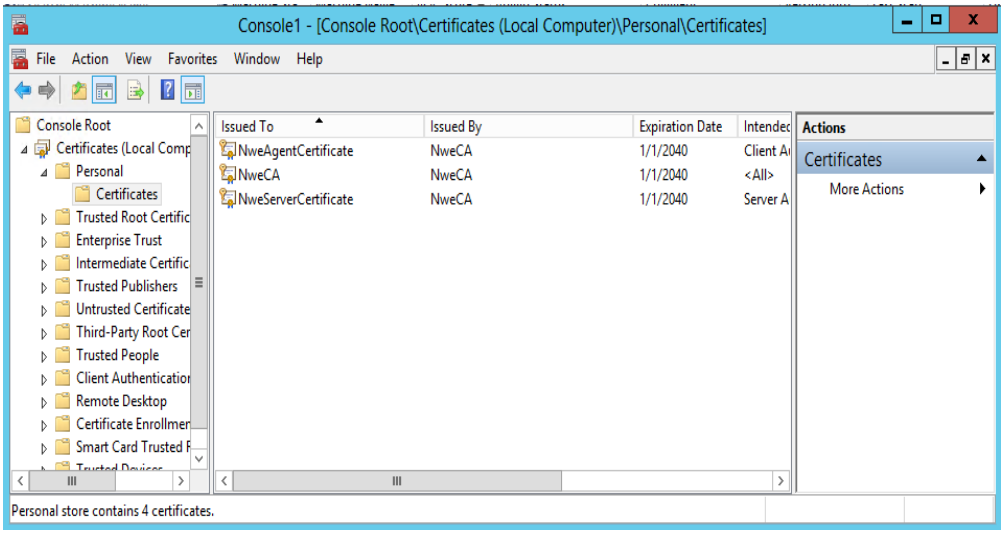
4. Select **Computer Account** and click **Next**.



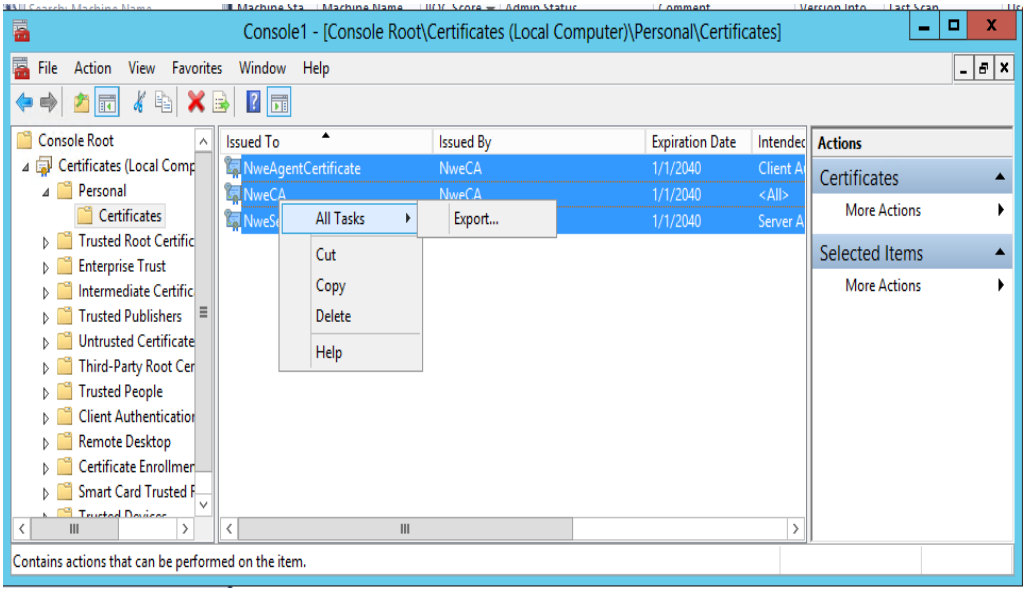
5. Select **Local computer** and click **Finish**.



6. Click **OK** in **Add or Remove Snap-ins**.
7. You should now be able to see the generated certificates under **Certificates (Local Computer) > Personal > Certificates**.



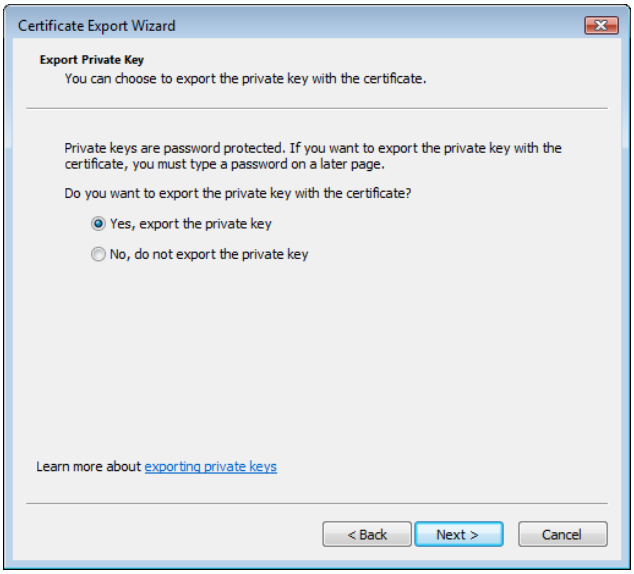
8. Select all the NetWitness Endpoint certificates, right-click, and select **All Tasks > Export**.



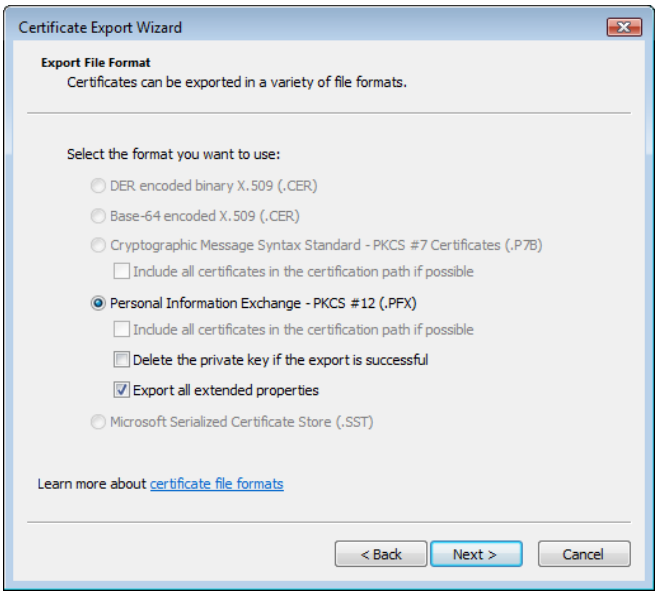
The Certificate Export Wizard will start.

9. Click **Next.**

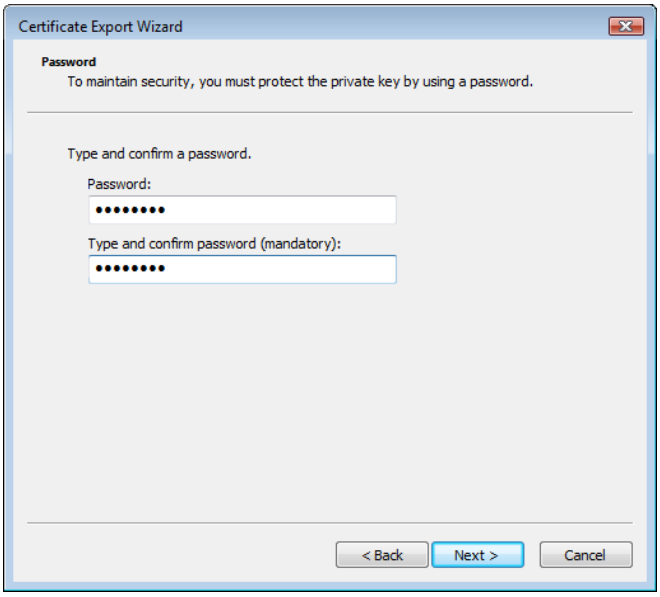
10. Select **Yes, export the private key** and click **Next**.



11. Select **Personal Information Exchange** and **Export all extended properties** and click **Next**.

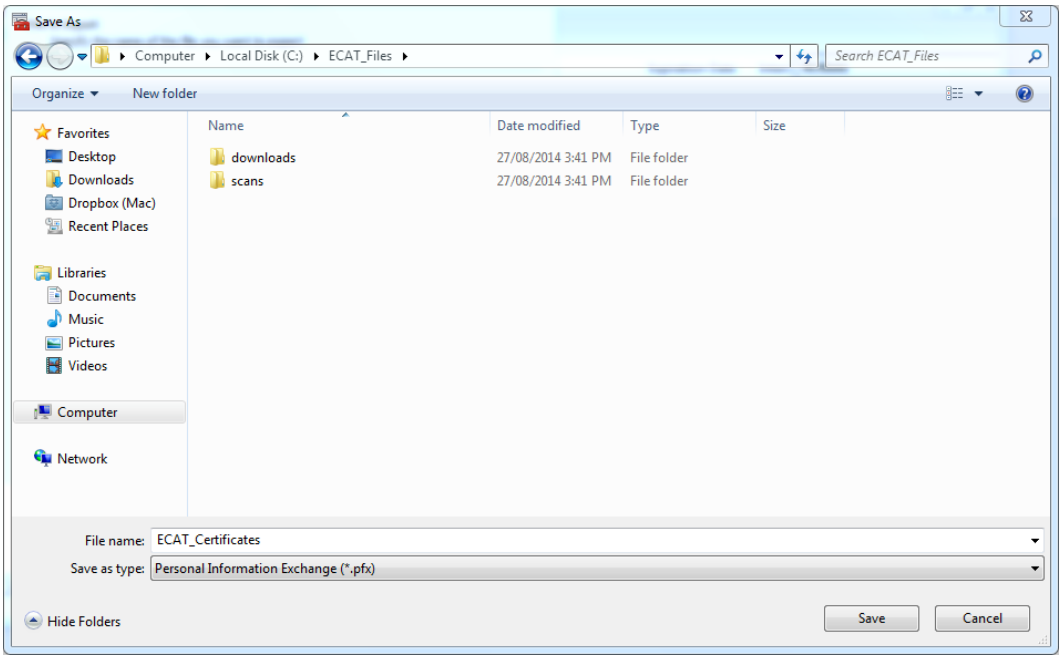


12. Enter a Password for the certificate encryption and click **Next**.

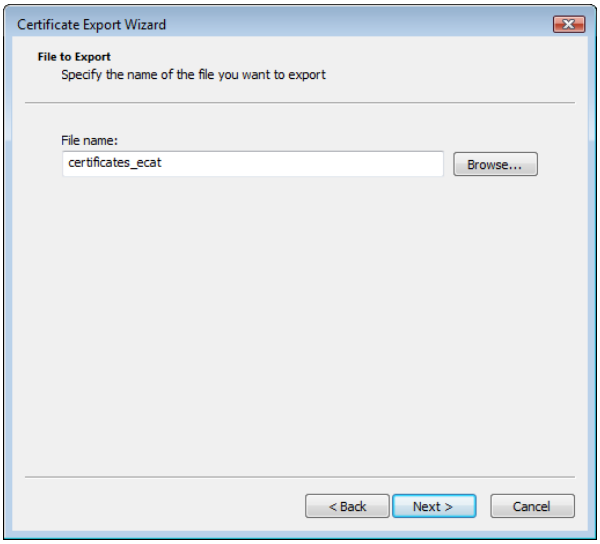


> **Note:** This password will be required later to import the certificates on the other machine.

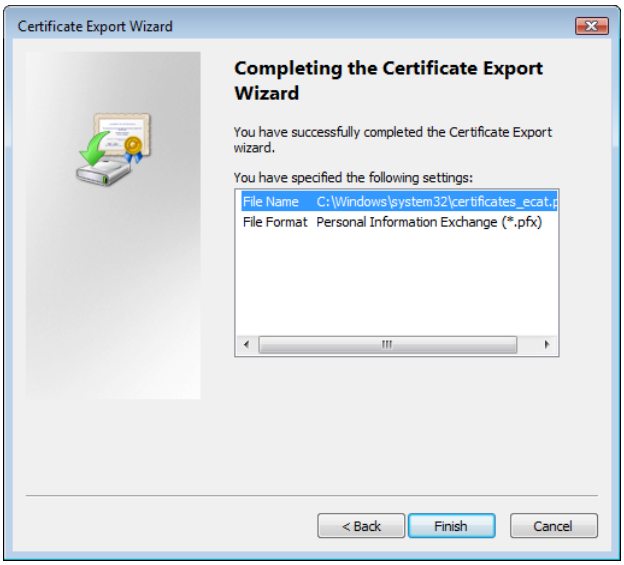
13. After **File name**, enter the path name for the exported certificates file. You may click **Browse**… to browse to an appropriate location. Click **Save** when done.



14. Click **Next**.



15. Verify that the export was successful.
16. Click **Finish**.



17. Select **File > Exit** to exit **mmc**.

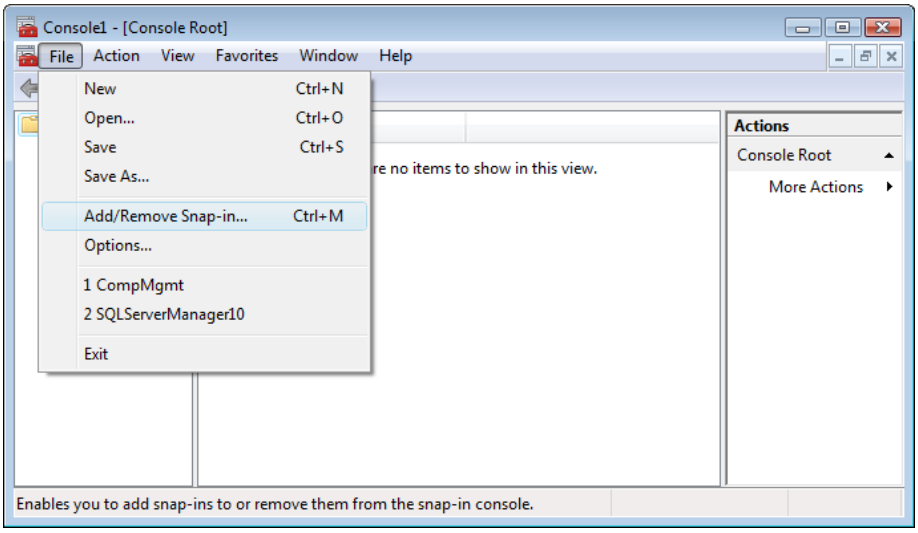
Step 5: (Optional) Import Primary Server Certificates

Perform this step to import the (.pfx) encryption certificates (exported in the previous step) into the relevant machine(s). If (1) the NetWitness Endpoint ConsoleServer is to be run from a different location, then import the certificates into that machine, or (2) if you wish to generate packages on a different machine than the one they were created on, then import the certificates into that machine, or (3) if you are planning a multi-server deployment, then import the certificates into any machine on which you plan to install a secondary server.

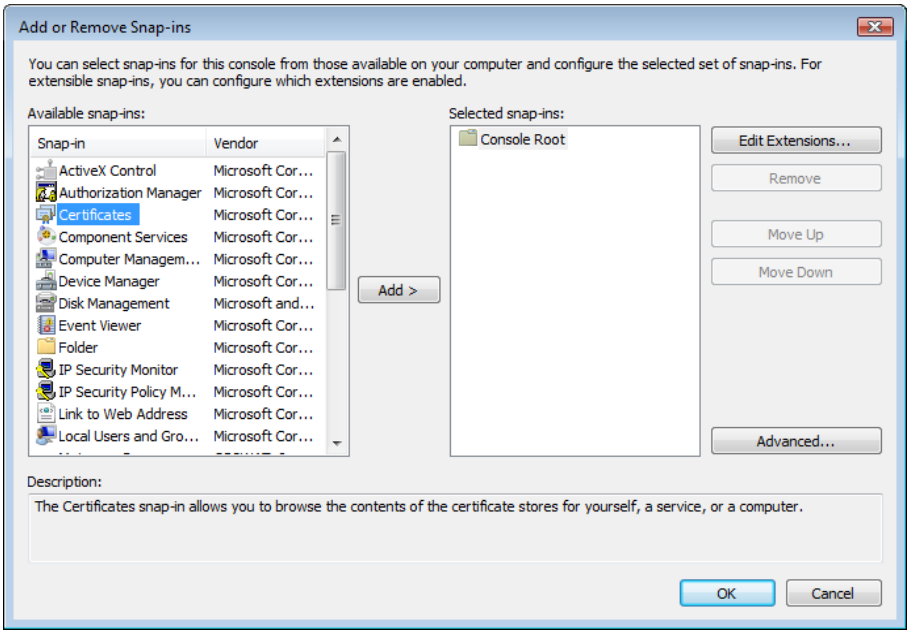
To import the certificates:

1. Copy the certificate file to the new machine.
2. Run **mmc** from a command line. This opens the Microsoft Windows management console.

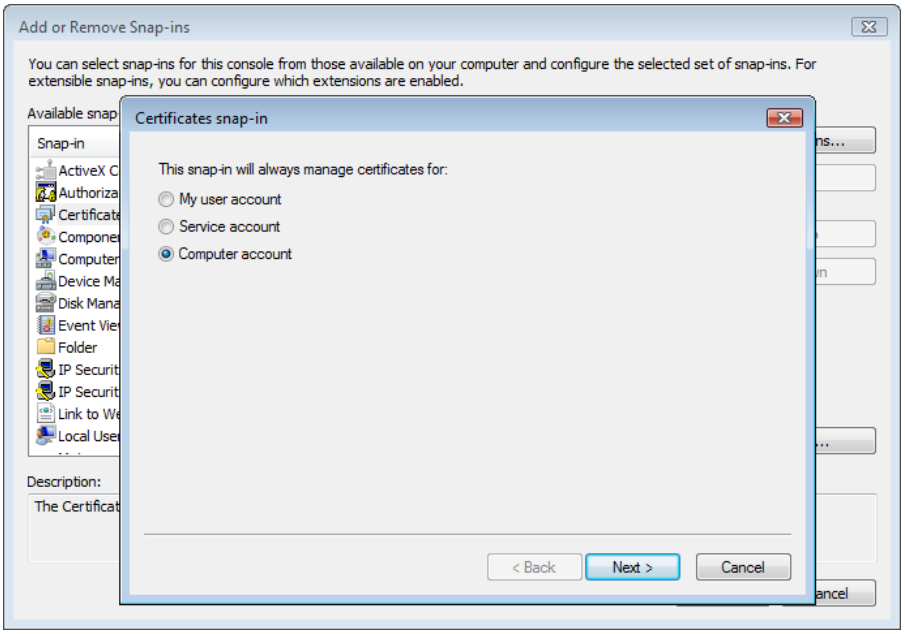
3. Select **File > Add/Remove Snap-in**.



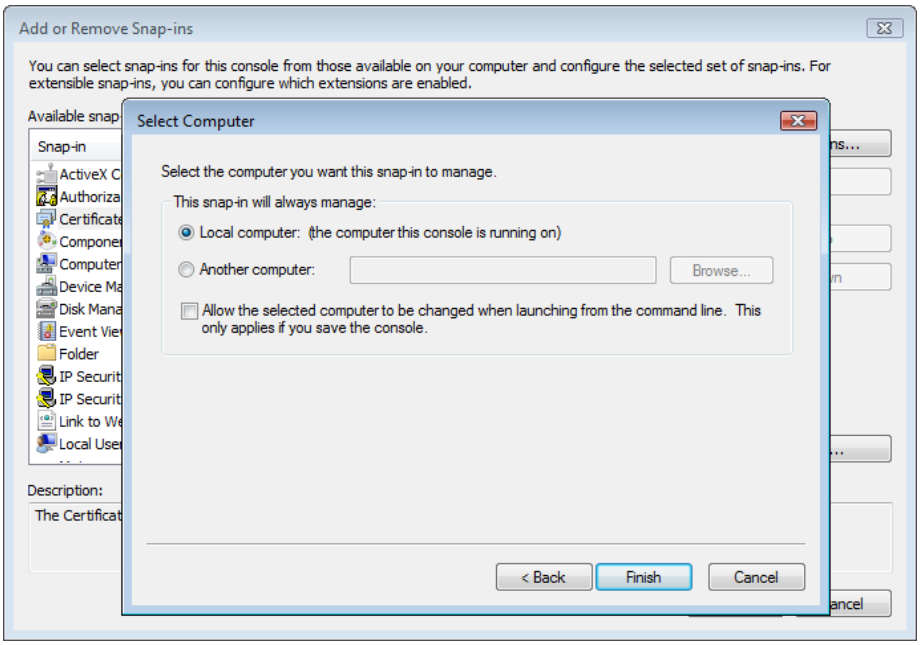
4. From the list of available snap-ins, select **Certificates** and click **Add**.



5. Select **Computer Account** and click **Next**.

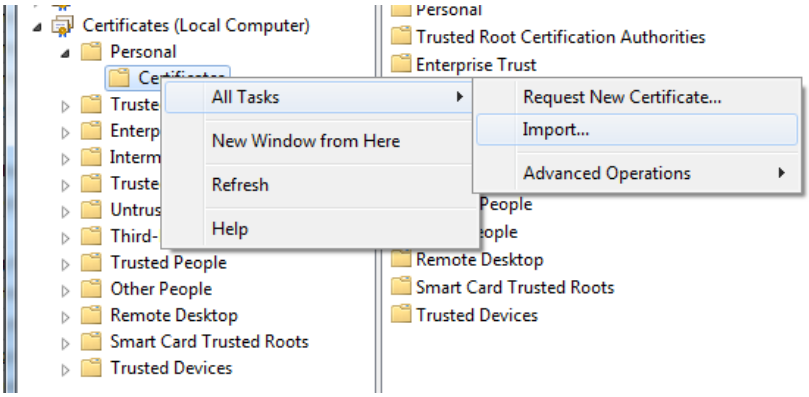


6. Select **Local computer** and click **Finish**.



7. Click **OK** in Add or Remove Snap-ins.

8. Right-click on **Certificates (Local Computer) > Personal > Certificates** and select **All Tasks > Import**.

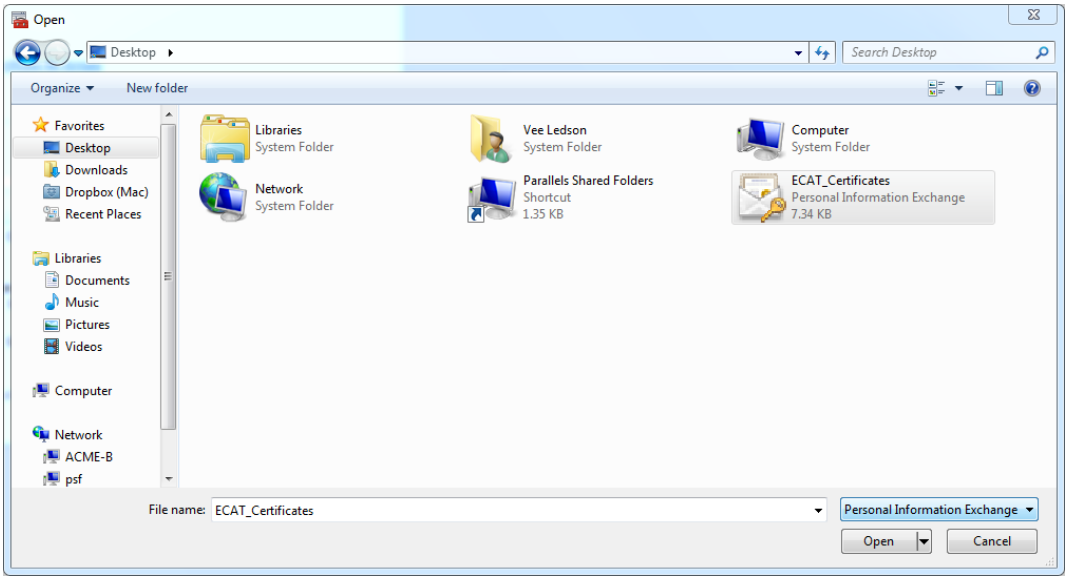


The Certificate Import Wizard is displayed.

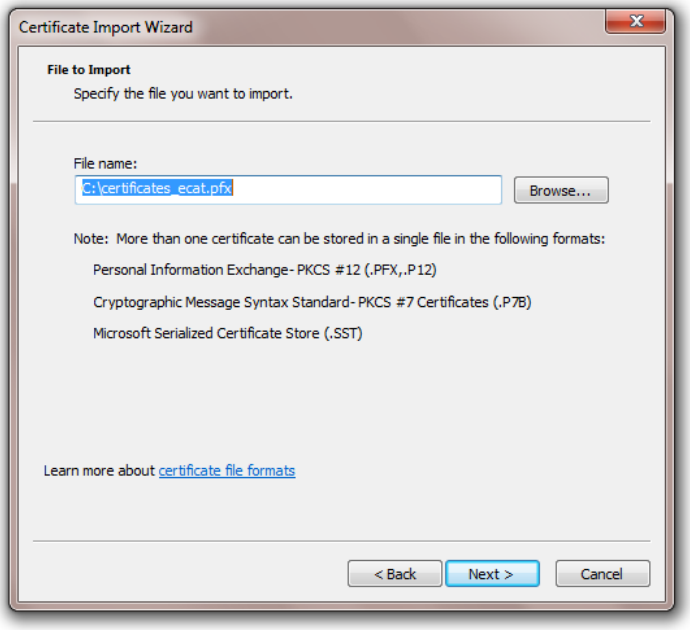
9. Click **Next**.

10. Click **Browse**… to navigate to the location of the certificate file.

11. When importing the .pfx file, select **Personal Information Exchange (.PFX,.P12)** as the file format, select the file, and click **Open**.

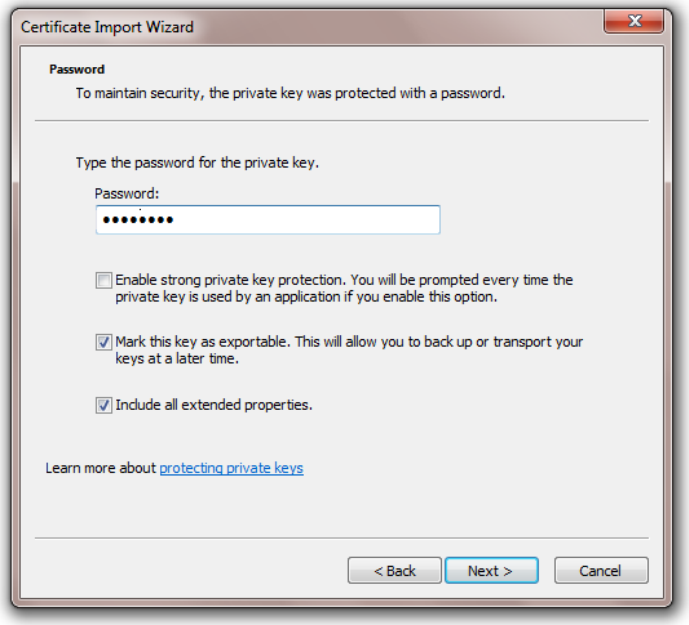


12. Click **Next**.

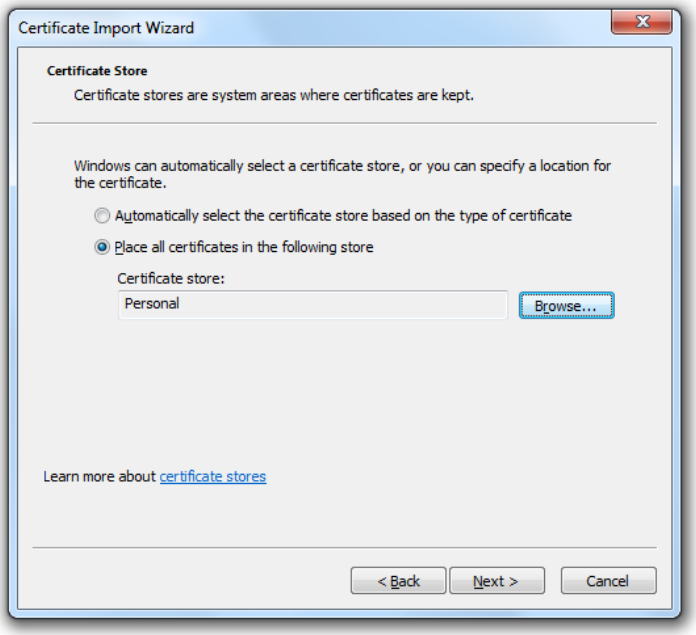


13. Enter the password, if any, that you used when exporting the certificates. The option **Mark this key as exportable** must be selected.

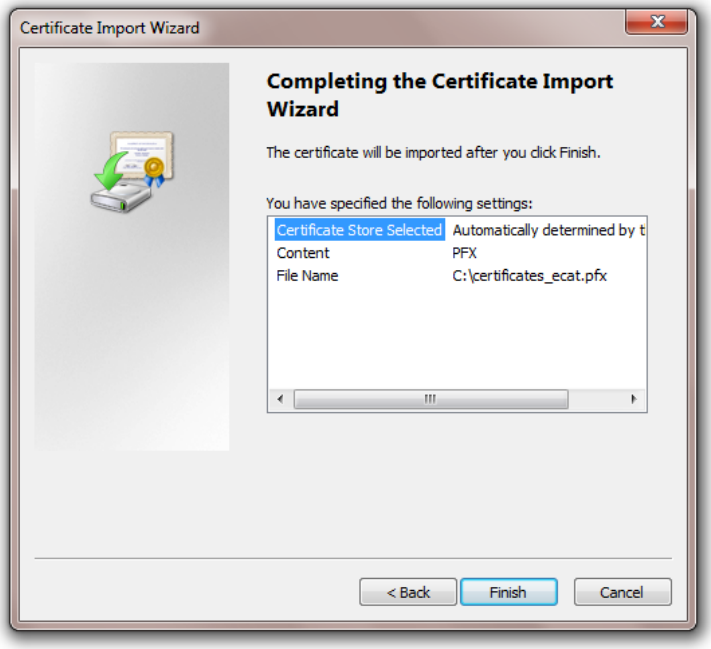
14. Click **Next**.



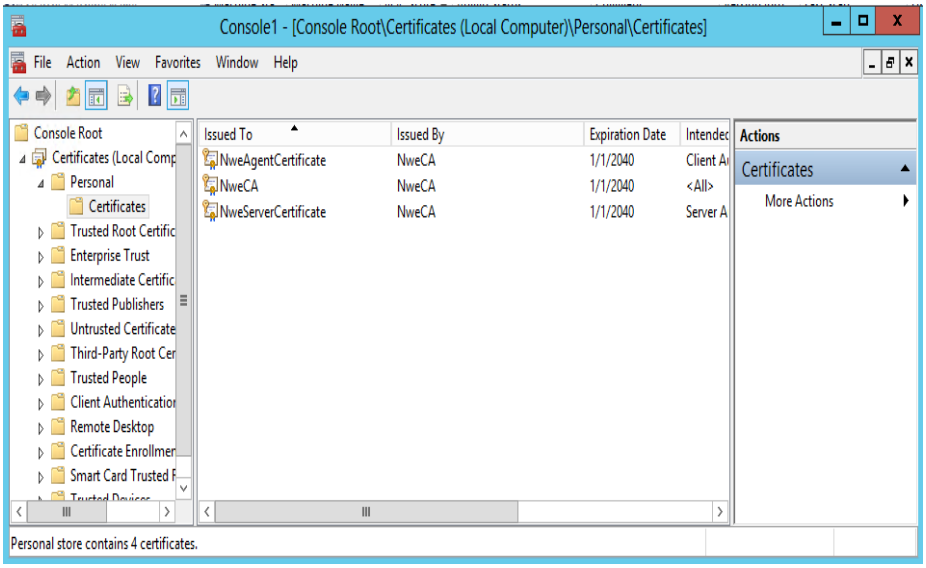
15. Leave the certificate store selection to the default settings, and click **Next**.



16. Click **Finish** to import the certificates.



17. Verify successful import into the personal certificate store by returning to **mmc** and selecting **Certificates (Local Computer) > Personal > Certificates**. You should see the NetWitness Endpoint certificates in the center pane.



18. Select **File > Exit** to exit **mmc**.

Step 6: (Optional) Install Secondary Server

Once there is a Primary Server installed, you can optionally install up to a maximum of three Secondary servers. If using Secondary servers, all agent traffic should be pointed to Secondary servers and not to the Primary Server. Please note that Secondary servers should be used only for scale, not for geographic distribution. The workload will be divided automatically between the Primary Server and all the Secondary servers.

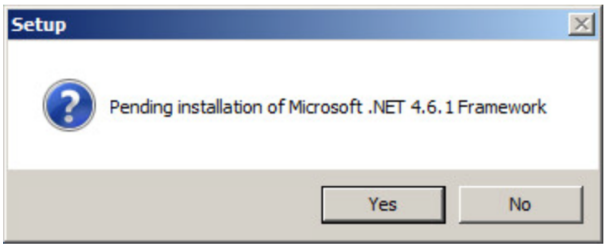
Note: Please consult your local RSA Account Team if considering an installation that includes Secondary servers.

The purpose of having a Secondary server is to offload the SQL Database from some of its work. Each instance of ConsoleServer needs to have access to a separate instance of SQL Server, which must also be on a separate machine. At the moment, Secondary servers cannot be used for the sole purpose of segmenting the NetWitness Endpoint network, as all agents will need the capability to report to the Primary Server.

Note: For a multi-server environment, there must be a shared network downloads folder for files uploaded by agents.

The process for installing a Secondary server is very similar to installing the NetWitness Endpoint Primary server. To install a Secondary server:

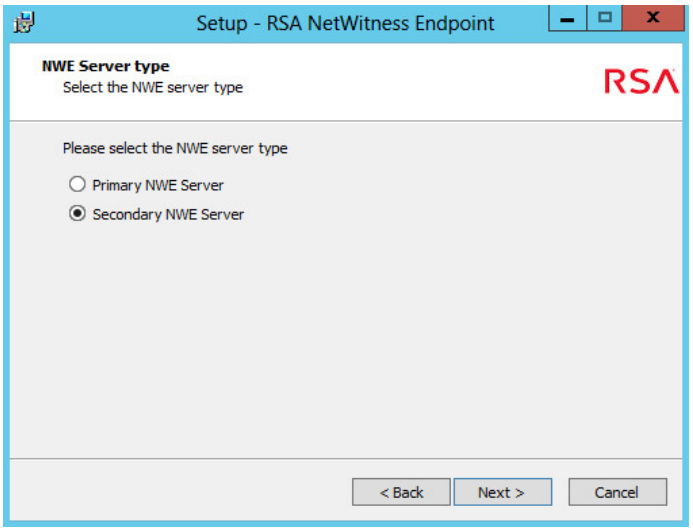
1. If not already done, unzip the archive file:
   rsa_nwe_<*4.4.x.x*>_sw.zip
2. Find and double-click the installer executable file:
   rsa_nwe_<*4.4.x.x*>_sw.exe
3. A prerequisite for NetWitness Endpoint includes the Microsoft .NET Framework 4.6.1. If this is not already installed, the following screen will display (if Microsoft .NET Framework 4.6.1 is already installed, the Installation Wizard is displayed):



4. Refer to steps 4-8 in the topic Step 3: Install Primary ConsoleServer to complete installation of Microsolft .NET Framework.
5. On the Installation Wizard dialog, click **Next**.
   The Select Destination Location dialog is displayed.

6. Select the destination location for the installation files. A default location is provided, or you can click **Browse...** to select a different location.
7. Click **Next**.
   The Select Components dialog is displayed.
8. Select **Custom installation** from the drop-down list and then click the checkbox next to **NWE Server**.

   Note: Because this is a Secondary server, do not select the NetWitness Endpoint UI. It is recommended that the NetWitness Endpoint UI connect only to the Primary Server.
9. Click **Next**.
   The NWE Server Type dialog is displayed, as shown below:



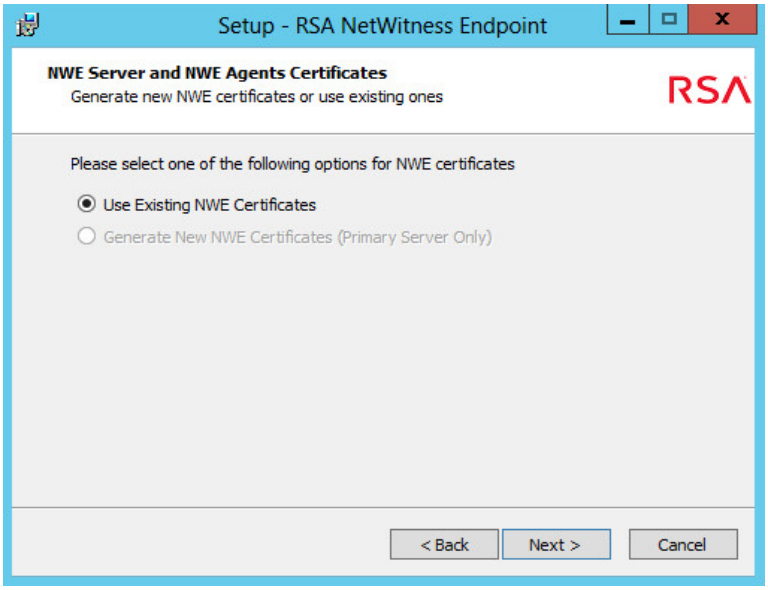
10. Select **Secondary NWE Server** for server type and click **Next**.
    The SQL Server dialog is displayed.
11. Enter the SQL Server you are using for NetWitness Endpoint. The settings are the same as for the NetWitness Endpoint Primary Server, except the Database Name. You can use the default name or enter a different Database Name of your choosing.
12. Click **Next**.
    The SQL Server Authentication dialog is displayed (which is the same as for the NetWitness Endpoint Primary server).
13. Select the desired authentication method and click **Next**.
    If you select the SQL Server Credential option, you must also enter a valid SQL server username and password and click **Next**. The system then verifies database access and, if it cannot reach the SQL Server, displays an error message.

Note: It is considered a best practice to select the default: Windows authentication credentials (current user). It is not recommended to use SQL Server credentials to configure a production database. To change the authentication type after completing the installation, see Manage Authentication After Installation.

Note: If SQL Server is installed on a remote machine and cannot be reached, you may need to manually create a firewall rule on the remote SQL Server to allow communication on TCP port 1433.

Note: If in attempting to connect to the SQL Server it is determined that there is already an existing database, a message is displayed with options to either reuse or delete the existing database. For more information, see Manage Existing Database During Installation.

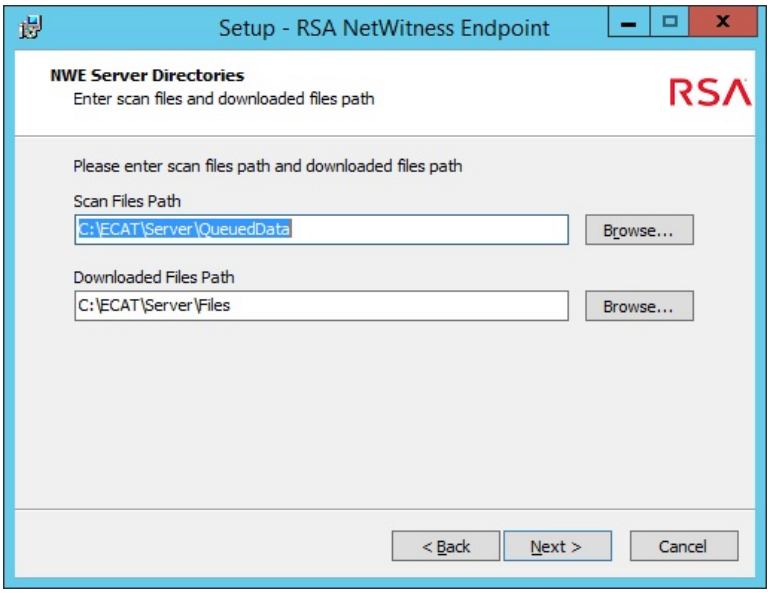
13. On the NWE Server and NWE Agents Certificates dialog, select the option **Use Existing NWE Certificates**,as shown below:



Note: You must have previously imported the NetWitness Endpoint Primary ConsoleServer certificate to the Secondary server.

13. Click **Next**.

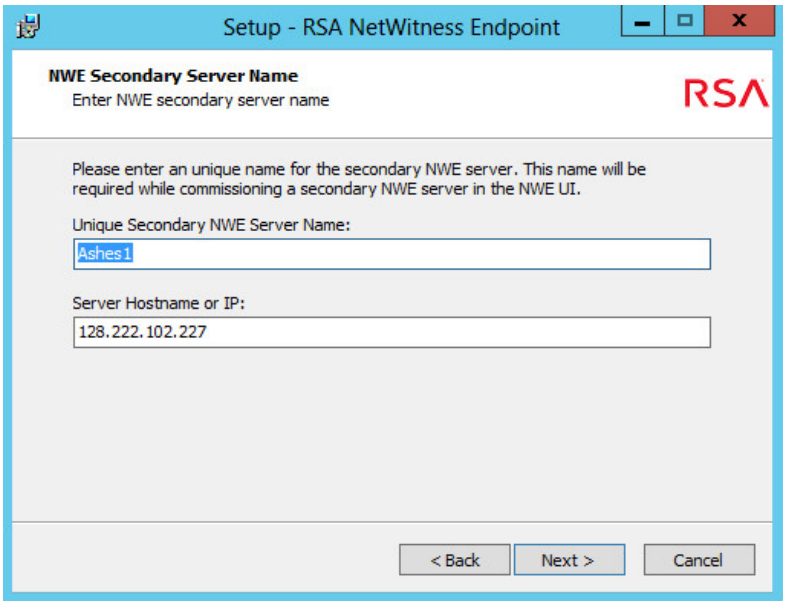
    The NWE Server Directories dialog is displayed, as shown below:



Enter the Scan Files Path and Download Files Path.

Note: The Downloaded Files Path must match the directory selected for the NetWitness Endpoint Primary Server. Also, the Scan Files Path should be local to the secondary database.

15. Click **Next**.The NWE Secondary Server Name dialog is displayed, as shown below:

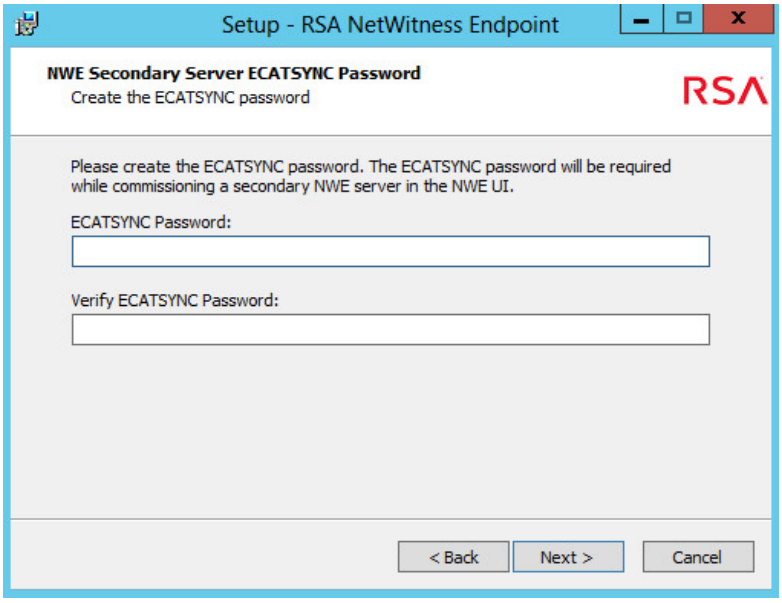


Enter a unique name for the Secondary server.

Note: Your IP address will be provided automatically for **Server Hostname or IP**. If you enter a Server Hostname instead, it must be a fully qualified DNS name for the Machine Containment function to work properly. If you enter a partial DNS name, agent machines will go offline and a manual agent uninstall and reinstall will be required.

16. Click **Next**.

    The NWE Secondary Server ECATSYNC Password dialog is displayed, as shown below:



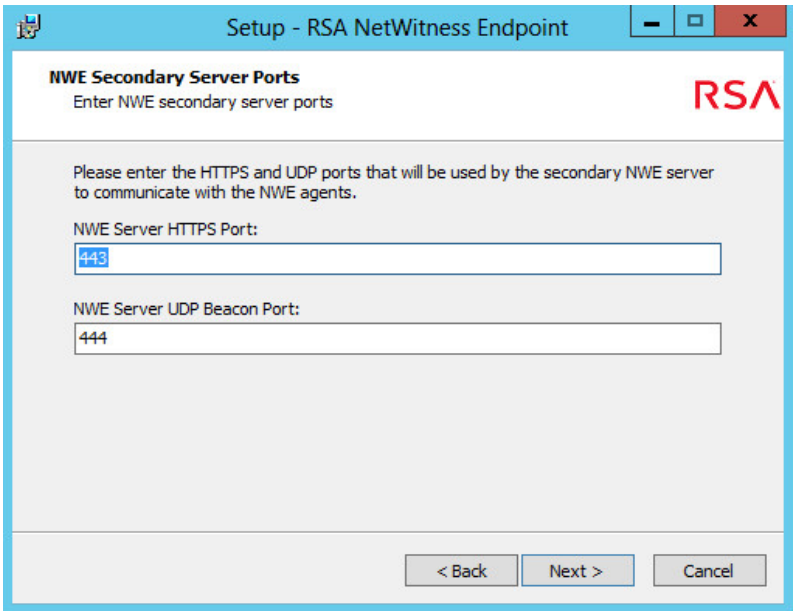
17. Create a password that will be used to synchronize databases between different servers.

Note: An ECATSYNC password is mandatory to configure and commission the NetWitness Endpoint Secondary server in the NetWitness Endpoint UI. A warning message will display if fields are left blank or do not match.

Note: You need to remember the ECATSYNC password for Secondary server commissioning from the NetWitness Endpoint UI, as detailed in the topic Step 7: Configure Multi-Server Through NetWitness Endpoint UI.

18. Click **Next**.

    The NWE Secondary Server Ports dialog is displayed, as shown below:



19. Enter the following port numbers, which are used internally by NetWitness Endpoint for communication between its various components:
    - NWE Server HTTPS port: 443
    - NWE Server UDP Beacon port: 444

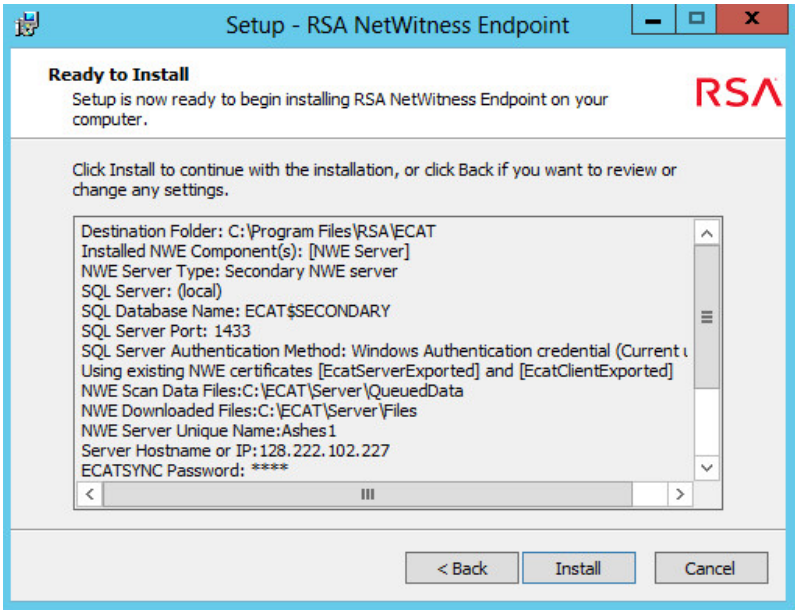
    Note: Port availability will be verified and an error message will display if the specified ports are invalid or already used.
20. Click **Next**.
    The NWE Server Miscellaneous Configuration Options dialog is displayed (which is the same as for the NetWitness Endpoint Primary server).
21. Click the checkboxes to enable the desired options:
    - **Run As Service**: Enable this option if you want the NetWitness Endpoint server to run as a service. Selecting this option also installs the Endpoint Meta Integrator as a service (for more information, see "NetWitness Suite Endpoint Meta Integration" in the *NetWitness Endpoint User Guide*).
    - **Create Firewall rules for NWE agent and NWE server communication**: This option is necessary if you have an active firewall as you will need to create firewall rules to allow communication between the NetWitness Endpoint server and the NetWitness Endpoint agent through the firewall.
    - **Create Firewall rules for SQL Server**: This option may be necessary if you have an active firewall as you may also need to create a firewall rule to allow communication

between the NetWitness Endpoint server and SQL Server. However, it is of no use to create this firewall rule if the SQL Server runs on a remote machine.

22. Click **Next**.

- If you selected the **Run As Service** option on the previous dialog, the Windows Service Configuration dialog is displayed.
  Enter a domain\username and password to allow the NetWitness Endpoint server, which will be running as a service, to log on to the machine on which NetWitness Endpoint server is installed. (You may use either SQL Server credentials or your Windows authentication. If you use Windows authentication, it is recommended you choose an account that has administration privileges on the local machine, to ensure smooth operation of the server.)
  Click **Next**.
- If you previously selected the **Run As Service** option, the Select Additional Tasks dialog is displayed.
  Click to enable the **Launch NWE Server Service Output** option if you want this action performed during Setup.
  Click **Next**.

23. The Ready to Install dialog is displayed, as shown below:



24. You should review all of the options you selected in the previous steps, which are displayed in this dialog. If you wish to change any options you may do so by clicking **<Back** to go back through the previous dialogs.

25. Click **Install** to proceed with the installation.

    If installation has been successful, the Setup Successful dialog box is displayed.

> **Note:** The installation will take some time. Please wait while the process is completed, or click **Cancel** to cancel the installation.

> **Note:** If you selected to run the NetWitness Endpoint Secondary Server as a service, you should set the service to restart automatically following a failure, using the server properties dialog.

Step 7: Configure Multi-Server Through NetWitness Endpoint UI

After installing all of the ConsoleServers in a multi-server deployment (including the Primary Server), you need to configure the overall deployment using the NetWitness Endpoint UI. This configuration can be accessed through **Server Configuration** in the NetWitness Endpoint UI **Main Menu**.

Configure ConsoleServer Through NetWitness Endpoint UI

After installing the Primary ConsoleServer, the Primary Server gets added into the database automatically. Secondary servers, on the other hand, must be manually added through the NetWitness Endpoint UI.

> **Note:** The Roaming Agents Relay (RAR) is a separate component that provides visibility to endpoints that are disconnected from a corporate network. RAR can be deployed as a cloud service. For information about installing and configuring RAR, see the topic Step 14: (Optional) Deploy Roaming Agents Relay.

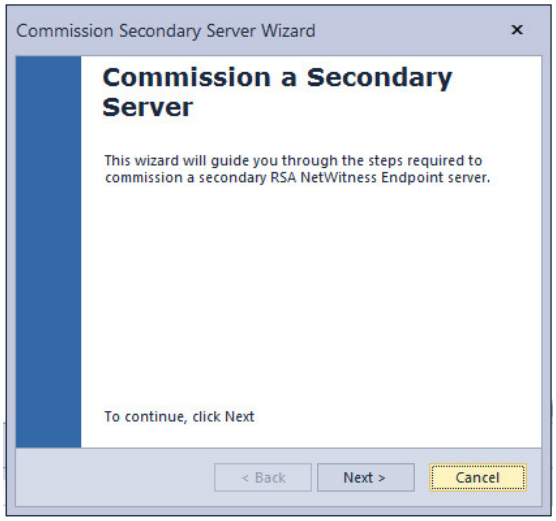
To add a secondary ConsoleServer:

> **Note:** This does not install the server, which has presumably already been installed.

1. Open the NetWitness Endpoint UI.
2. Select **Server Configuration** in the **Main Menu**.

3. Click **Commission New Server** in the **Server Configuration** tab.

4. The Commission Secondary Server Wizard is displayed. Click **Next**.



5. In **Connect to Secondary Database**, enter the following information:

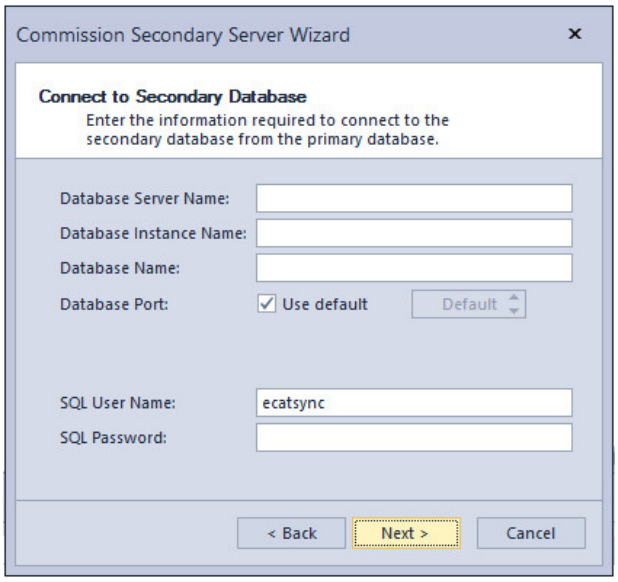
   a. Database server name (the name of the machine hosting the database for the secondary server).

   b. Database instance name (if any).

   c. The name of the secondary database.

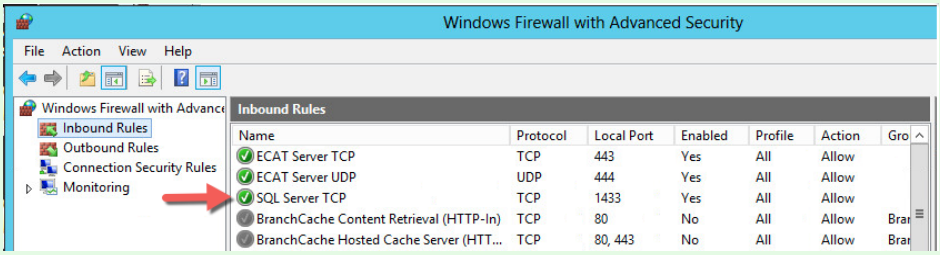
   d. The database port: The option to use the default port (TCP 1433) is automatically selected. To use a different port, uncheck **Use default** and enter the custom port that the SQL Server is running on.

e. Enter the password for the NetWitness Endpoint synchronization account that you set earlier.

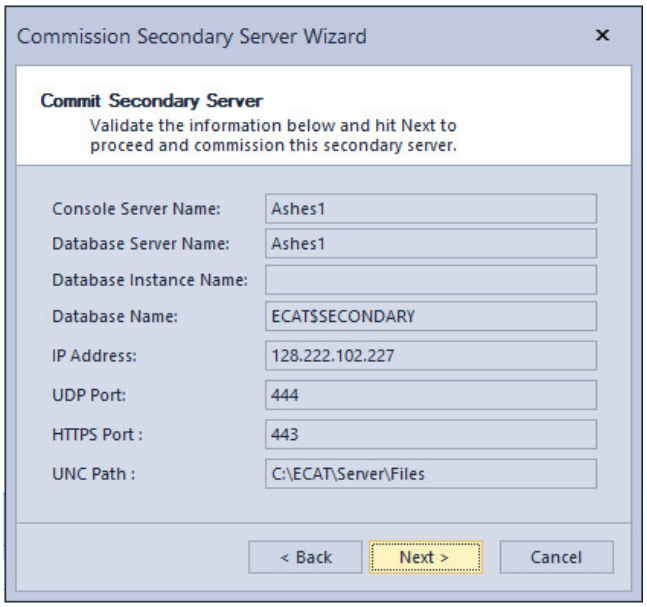


6. Click **Next**. You will be prompted to commit to the secondary server information.

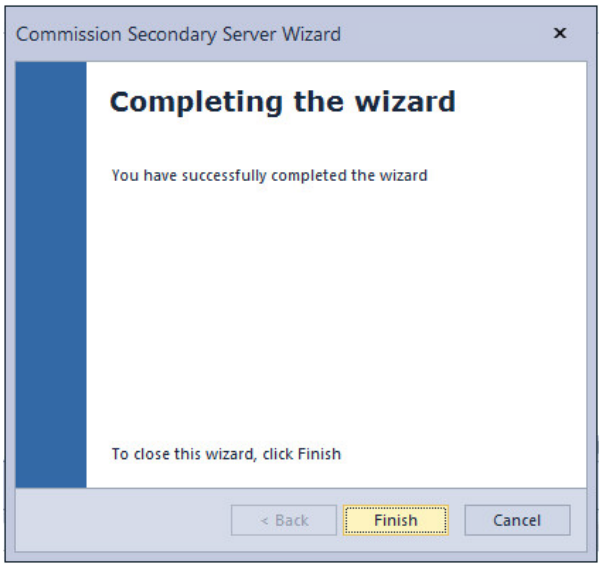
Note: If the message "Named Pipes Provider: Could not open a connection to SQL Server [1326]" is displayed while commissioning a secondary server, there may be a connectivity problem between the Primary and secondary SQL Server. In the case of remote SQL Server installation, firewall rules may have to be created manually on both Primary and secondary SQL Servers to allow communication on TCP port 1433, as shown below. (For local SQL Server, the rules should have been created if you checked the "Create firewall rules ..." option during Primary and secondary server installation, as described in the topics Step 3: Install Primary ConsoleServer, procedure step 22, and Step 6: (Optional) Install Secondary Server, procedure step 17.)



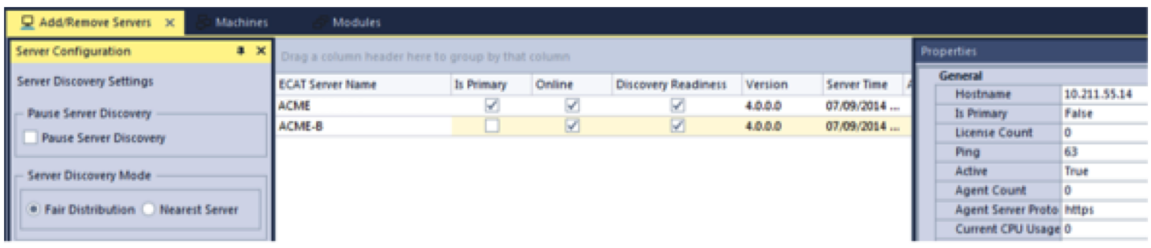
7. Verify the information displayed, and click **Next**.



8. The Wizard displays a successful completion message. Click **Finish**.



9. Your secondary server should now appear in the list of servers in the NetWitness Endpoint UI as shown below:



Caution: After completing the installation process for a secondary server, you must first start the Primary Server before starting the new secondary server, for the first time only. Otherwise, an error message is displayed when you try to start the new secondary server.

Pause Server Discovery

Checking **Pause Server Discover** under **Add/Remove Servers** allows you to pause/resume the server assignments to NetWitness Endpoint agents. This feature can be useful when NetWitness Endpoint agents are being installed across the deployment and the NetWitness Endpoint admin does not want the agents to discover their ConsoleServer immediately. For example, this may be done if Console Servers are still being installed.

When this field is checked, none of the newer agents will be able to discover their server. However, this field has no impact on those agents in the deployment that have already discovered their server.

Server Discovery Mode

You can choose between two different methods for agents to be distributed amongst the servers. Under **Add/Remove Servers**, checking **Fair Distribution** will ensure that each server gets a roughly equal share of agents assigned to it. With this selection, agents will be distributed to the servers in a round-robin fashion.

Another option is to have agents connect to the closest server. Check the **Nearest Server** option, and the agents will be assigned to the closest server (this is determined as the server with the fastest ping response time).

Step 8: Run NetWitness Endpoint ConsoleServerOutput

If you have installed ConsoleServer as a service and selected the option "Launch Server Console" during the last stage of installation, ConsoleServer itself is now installed and running as a service.

If **ConsoleServerServiceOutput.exe** is not already running, and you wish to view the output messages from ConsoleServer, do the following:

Select **Start > All Programs > RSA NWE> NWE ServerOutput**.

Messages will appear in different colors depending on the type of message:

- White messages display normal messages or logs.
- Yellow messages indicate warnings.
- Red messages indicate errors, although some of them may not be critical.

Step 9: (Optional) Install Metascan

OPSWAT Metascan (now called Metadefender Core) is an advanced multi-scanning software engine that may (optionally) be used with NetWitness Endpoint. It combines unique technologies and multiple anti-malware engines from market leaders (such as CA, ESET, AVG, and others) and improves the likelihood of catching malware on downloaded modules.

If you are not installing Metascan, skip ahead to Step 10: (Optional) Install YARA.

Note: Metascan can be installed on the same machine where the NetWitness Endpoint ConsoleServer is running, or on another server on the LAN. For performance reasons, however, it is highly recommended to install Metascan on a different machine as it requires at least 10 GB of free space (but you should verify current requirements with OPSWAT Metascan).

Note: While installing Metascan, Windows might ask for several authorizations, especially when installing the antivirus engines. Make sure to allow all of them (some drivers cannot be verified by Windows).

To install and configure Metascan:

1. Obtain the Metascan installation executable from:
   https://portal.opswat.com/user/register
   When downloading the installation executable, select Metadefender Core version 4.8.0. This is the version currently verified to work with NetWitness Endpoint.
2. Double-click the .exe file to run the installation wizard.
3. Accept the End-User License Agreement.
4. On the Custom Setup dialog, you can either keep the default settings or make changes.
5. Click **Install** on the Ready to install Metascan dialog and wait until the Completed the Metascan... dialog is displayed. This may take some time.
6. Click **Finish** and wait until the Metascan Install/Uninstall Complete dialog is displayed.
7. Click **Close**.
   Metascan is now installed.
8. Set the service to autostart.
9. Start the service.

   Note: Do not forget to start the service. ConsoleServer will not start if it is configured to work with Metascan locally, but Metascan itself is not started.

10. To complete the set up process for Metascan, you will need to enter configuration information through the NetWitness Endpoint UI. For more information, see "Monitoring and External Components" in the *RSA NetWitness Endpoint User Guide*.

Step 10: (Optional) Install YARA

YARA is an open source static analysis tool that may (optionally) be used with NetWitness Endpoint. It uses a set of custom rules to help identify and classify known threats on downloaded modules.

Note: YARA should be installed on the same machine where the NetWitness Endpoint ConsoleServer is running.

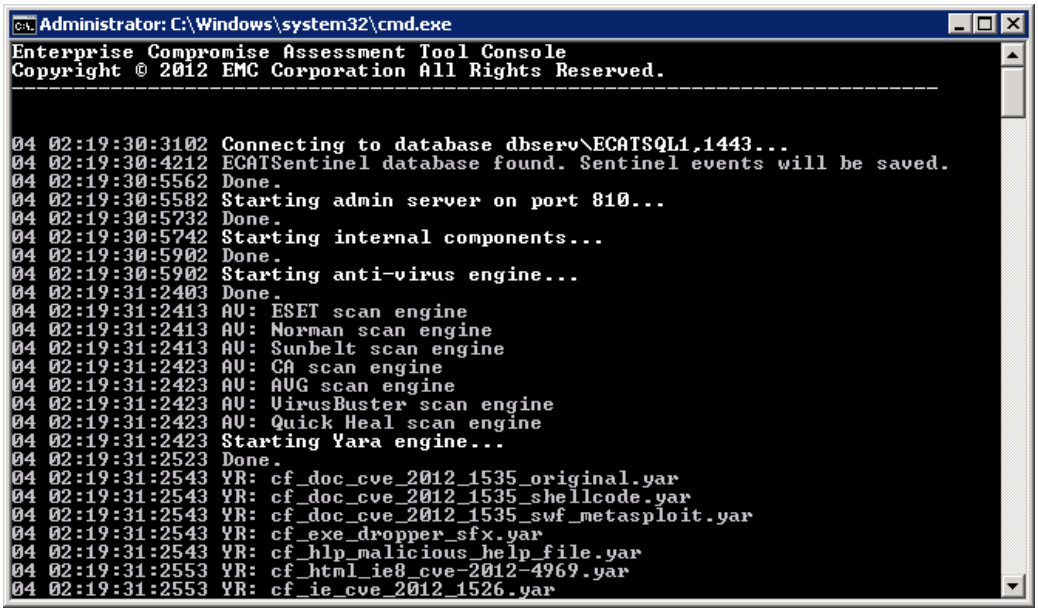
To install YARA:

1. Save the main executable and your rules file into a folder relative to **ConsoleServer.exe**.
2. Enter configuration information in the Monitoring and External Components dialog in the NetWitness Endpoint UI. For more information, see *Monitoring and External Components* in the RSA NetWitness Endpoint User Guide.

The YARA user's manual and executable file can be downloaded from:
http://code.google.com/p/yara-project/downloads/list

Note: The Python version is not supported by NetWitness Endpoint.

Note: When YARA is enabled, the NetWitness Endpoint ConsoleServer will show the rules file(s) ("YR") being used.



Limitation with Certain YARA Versions

With YARA versions 3.3 and 3.4, only one rule file (*.yar) is supported.

If you have created multiple rules, you must consolidate them into one rule file using YARA include statements. However, in order for YARA rule re-scan to work the main rule file must be updated (re-saved) any time individual rule files are updated. Using a newer version of YARA that supports specifying a rule file folder is preferred. Note that the RSA ECAT Server service must be restarted in order for YARA rescan to work.

For more information on YARA Rules, see http://yara.readthedocs.org/en/latest/writingrules.html#including-files.

Step 11: Deploy Agents (Windows)

The agent software runs under the following Windows operating systems.

- Windows XP 32-bit SP3
- Windows XP 64-bit SP2
- Windows Vista (32 & 64-bit)
- Windows 7 (32 & 64-bit)
- Windows 8 (32 & 64-bit)
- Windows 8.1 (32 & 64-bit)
- Windows 10 (32 & 64-bit)
- Windows 2003 Server SP2 (32 & 64-bit)
- Windows 2008 Server (32 & 64-bit)
- Windows 2008 R2 (32 & 64-bit)
- Windows 2012 Server
- Windows 2012 Server R2
- Windows 2016 Server

Task 1: Generate the Agent Executable

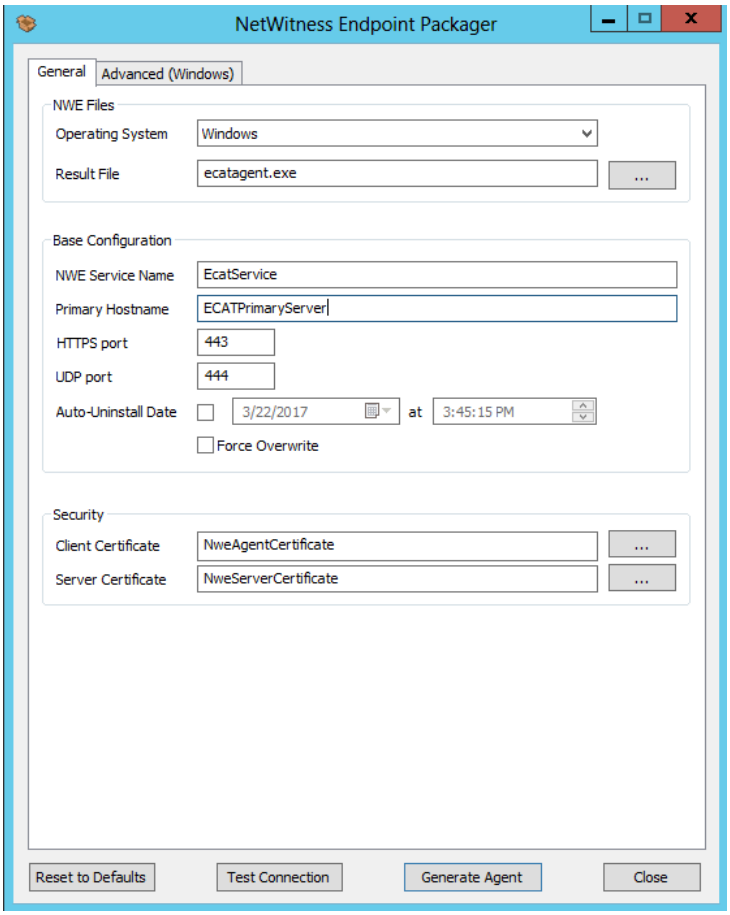
The NetWitness Endpoint Packager is an independent application used to generate an installer program that can be run on client machines to install the NetWitness Endpoint agent. The same Packager application can generate installer programs for each type of agent (Windows, Mac, or Linux).

Note: Make sure that you generate the installer on a machine where the proper certificates are installed (ones that match the certificates from ConsoleServer).

To generate the agent executable:

1. Select **Start > All Programs > RSA NWE > NWE Packager**.

   The NetWitness Endpoint Packager dialog is displayed, as shown below:



Caution: Never, under any circumstances, change the NetWitness Endpoint Service Name after any agents have been deployed. The default Service Name can only be changed before deploying agents.

2. In the **General** tab, enter required information as follows:

Field	Description
ECAT Files	
Operating System	Select Windows.
Result File	The name of the agent installer file. This can be copied to a new client machine and executed to install the agent. For Windows, this will normally be a **.exe** file.
Base Configuration	
ECAT Service Name	The name of the agent in the services list. For Windows agents only. The default name, EcatService, can be changed to something specific for your environment. **Caution:** Never, under any circumstances, change the NetWitness Endpoint Service Name after any agents have been deployed.
Primary Hostname	The static IP or the domain name of the NetWitness Endpoint Primary Server.
HTTPS port	The secure HTTP port number used by ConsoleServer.
UDP port	The UDP port number used by ConsoleServer.
Auto-Uninstall Date	The date and time the NetWitness Endpoint agent automatically uninstalls. It can be left blank if not required.
Force Overwrite	An option to overwrite the installed agent, regardless of the version. For Windows agents only. If this option is not selected, the same NetWitness Endpoint installer can be run multiple times on a system, but will install the agent only once. **Note:** Do not select this option if the NetWitness Endpoint agent is deployed through login scripts.
Security	

Field	Description
Client Certificate	Select the client certificate generated when the NetWitness Endpoint Server was configured. The default name is **NweAgentCertificate**. The client public certificate is bundled in the generated package and is the same for each installed client.
Server Certificate	Select the server certificate generated when the NetWitness Endpoint Server was configured. The default name is **NweServerCertificate**.

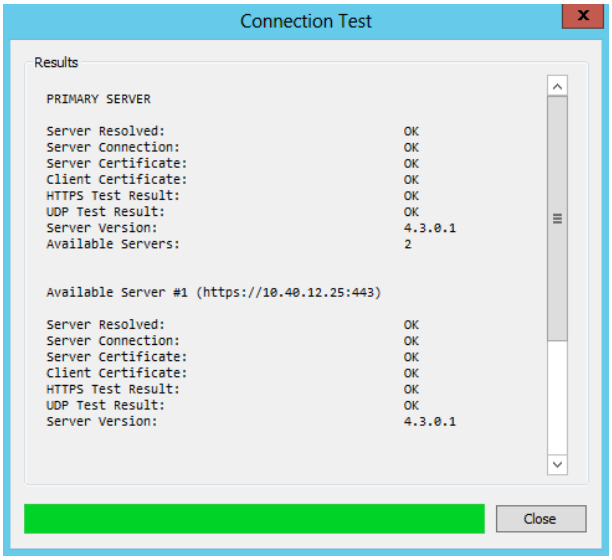
3. In the **Advanced** tab, enter information as follows.

Field	Description
NWE Service	
Display name	The display name of the client service.
Description	The description of the client service.
NWE Driver	
Service Name	The name of the driver in the services list. The default name, EcatServiceDriver, should be changed to something specific from your environment. Use caution if you change the name after deployment, as it might affect upgrades of the remote system.
Display Name	The display name of the driver service.
Description	The description of the driver service.
Proxy	
Server(s)	The proxy server list contains one or more of the following strings separated by semicolons: [<protocol>=]<server>[":"<port>] This field can be left empty if not required.

Field	Description
Exception(s)	The proxy exception list contains one or more of the following strings separated by semicolons: <server> This field can be left empty if not required.
Certificate Validation	Choose one of the options from the drop-down to determine how the agent will validate the NetWitness Endpoint Server certificate: - Thumbprint (default selection) - Full chain - None **Note:** By default, this setting will match the Agent Certificate Validation option selected in the Server Configuration panel of the NetWitness Endpoint UI, but it may be changed if desired. For more information, see the topic *Server Configuration Window* in the **RSA NetWitness Endpoint User Guide**.
Settings	
Monitoring Mode	An option to control the activation of the behavior tracking component. For Windows agents only. - No Monitoring - Network Monitoring Only - Full Monitoring - This is the default option and must be selected for behavior tracking and to use the Blocking System or Containment feature. - Full Monitoring, Except Network For more information on Monitoring Mode options, see the topic "Tracking Systems" in the *RSA NetWitness Endpoint User Guide*. Force disable WFP switch: Agents running on Windows Vista or newer Windows operating systems automatically switch to the more advanced WFP mode of network monitoring. You can disable this auto-switch behavior by clicking the checkbox for this option before creating the agent package, which will make agents on all Windows operating systems work in the legacy TDI mode of network monitoring.
Beacon interval(s)	The rate at which the client notifies the server of its status (in seconds).

4. To verify that the configuration parameters are valid, and to test the network connection to all enabled servers before deployment, click **Test Connection**, and ensure it reports **OK** for

all of its tests.



5. To generate the agent install file, click **Generate Agent**, depending on the target agent platform.
   The Agent executable is now ready to be deployed on a computer with the deployment method of your choice.

   Note: To update the agent of the same version, select the **Force Overwrite** option in the NetWitness Endpoint Packager (see step 2 above).

Task 2: Deploy the Agent (Windows)

Note: If the installation process fails for any reason and the connection to the server is available, the installer will send an error log to the server.

For all agent status icons, see the topic "Agent Status Icons" in the *NetWitness Endpoint User Guide*.

The agent can be deployed by any of the following methods:

- **Option 1 (Preferred):** Manually running the agent installer (administrator rights are required) on the client machine (this will be a .exe for Windows).

  Note: A Windows .exe installer simply starts the agent up invisibly, running in the background. There is no interaction or feedback.

- **Option 2:** Manually running the client MSI file:
  - ECAT000032.msi (32-bit operating system)
  - ECAT000064.msi (64-bit operating system)

    Note: The MSI files should not be renamed.
- **Option 3:** Active Directory scripts.

Task 3: Update an Agent

You may update one agent, a set of agents, or all agents to the latest version of the NetWitness Endpoint agent.

Updating an agent can be done using any one of the following three methods:

- Using NetWitness Endpoint UI
- Using Agent Installer
  - Command Line
  - Double-click
- Any other Deployment Tools

Note: Updating an agent can also be done with deployment software.

Updating an Agent Using the NetWitness Endpoint UI

Updating an agent is a three-step process:

1. Generate the installer on the server machine.
2. Queue the update on the NetWitness Endpoint UI.
3. Wait for the agent to confirm the update.

Note: Make sure that you generate the installer on a machine where the proper certificates are installed (ones that match the certificates from ConsoleServer).

Upon successful completion of an update, the installation date on the computer list will be updated, though a refresh might be needed to see it. In addition, the events panel will show the result of the update. This is true for the client events panel and the global events panel.

To update an agent:

1. Generate a new agent installer.

   Note: The new agent should have the same service name as the original.

2. Open the **Machines** list from the Main Menu.
3. Right click on the machine and select **Agent Maintenance** > **Update Agent**. (Alternatively, several agents can be selected by holding CTRL or SHIFT to be updated simultaneously.)
4. Navigate to the location of the generated file, select the desired file and click **Proceed**. The Update Agent window will then display the package file information.
5. Click **Update**.

> **Note:** The installation date on the computer list will be updated when an update was successfully applied, though a refresh might be needed to see it.

To update all agents:

1. Generate a new agent installer.

> **Note:** The new agent should have the same service name as the original.

2. Select **Tools** > **Agent Maintenance** > **Update All Agents**.
3. Under **Update package**, navigate to the location of the generated file, select the desired file and click **Proceed**.
   The Update Agent window will then display the package file information.
4. Click **Update**.

Updating an Agent Using Agent Installer

To update an agent using Agent Installer, simply double-click the agent installer (.exe file) (preferred method). When generating the installer package for updating agents, be sure to verify the Force Overwrite option.

To update an agent through command-line, run the following command:

```
msiexec /fvam <filename.msi>
```

Step 12: Deploy Agents (Mac)

The agent software runs under the following Mac operating systems:

- OS-X 10.8 (Mountain Lion)
- OS-X 10.9 (Mavericks)
- OS-X 10.10 (Yosemite)
- OS-X 10.11 (El Capitan)
- OS-X 10.12 (Sierra)

- OS-X 10.13 (High Sierra)
- OS-X 10.14 (Mojave)

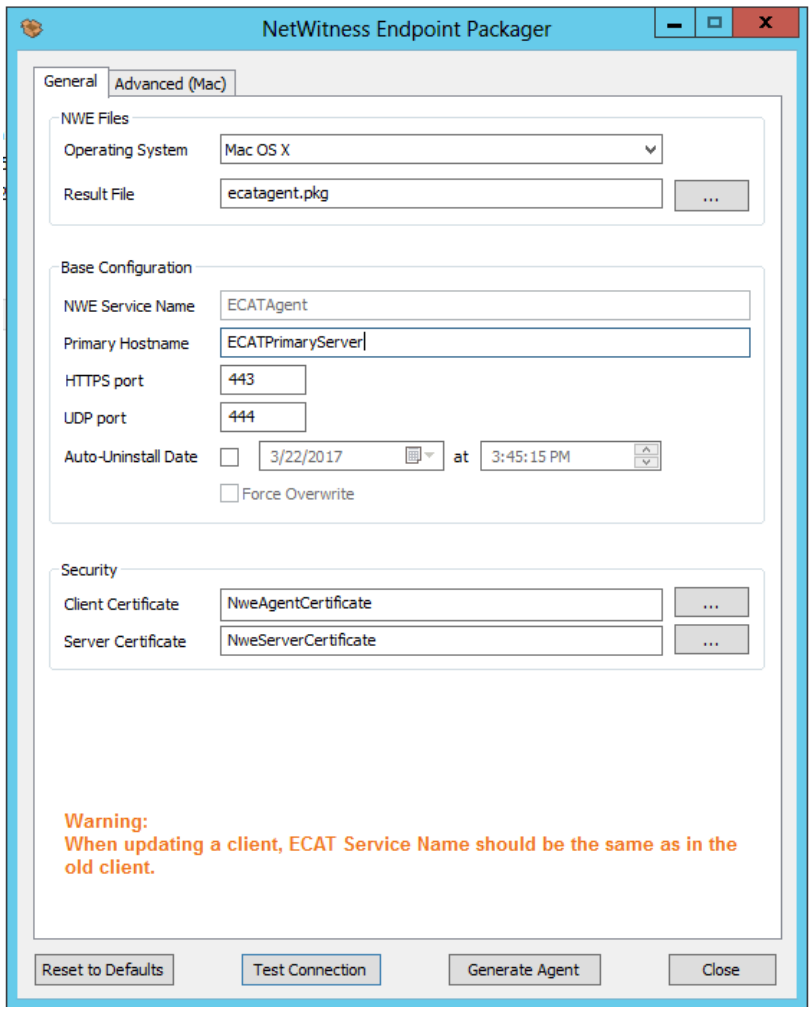
Task 1: Generate the Agent Executable (Mac)

The NetWitness Endpoint Packager is an independent application used to generate an installer program that can be run on client machines to install the NetWitness Endpoint agent. The same Packager application can generate installer programs for each type of agent (Windows, Mac, or Linux).

Note: Make sure that you generate the installer on a machine where the proper certificates are installed (ones that match the certificates from ConsoleServer).

To generate the agent executable:

1. Select **Start > All Programs > RSA NWE > NWE Packager**.
   The NetWitness Endpoint Packager dialog is displayed, as shown below:



2. In the **General** tab, enter all required information as follows:

Field	Description
ECAT Files	
Operating System	Select Mac OS X.
Result File	The name of the agent installer file. This can be copied to a new client machine and executed to install the agent. For Mac agent, this must have a .pkg extension.
Base Configuration	

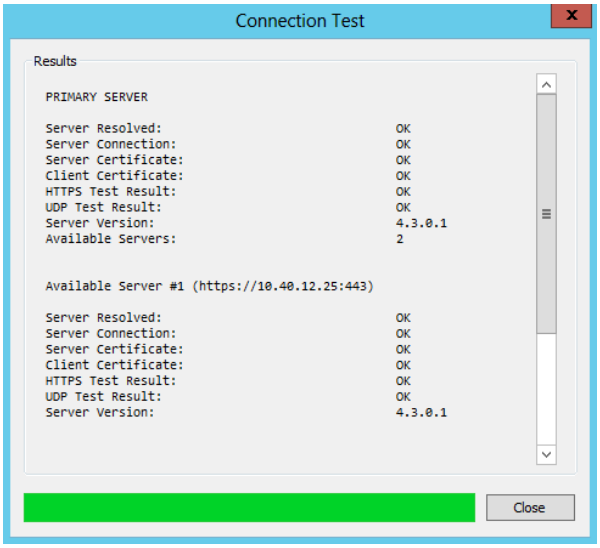
Field	Description
ECAT Service Name	This setting is not honored by Mac agents. On Mac machines, the agent runs as a daemon with the label ECATAgent.
Primary Hostname	The URL of the master console server to which the agent starts talking as soon as it is installed.
Auto-Uninstall Date	The date and time the NetWitness Endpoint agent automatically uninstalls. It can be left empty if not required.
Force Overwrite	This option is ignored for Mac agents, as the Mac installer will always overwrite the existing installation.
Security	
Client Certificate	Selects the client certificate generated, which the Mac agent will use to communicate with the NetWitness Endpoint Server. The default name is **NweAgentCertificate**. The client public certificate is bundled in the generated package and is the same for each installed client.
Server Certificate	Selects the server certificate generated when the NetWitness Endpoint Server was configured. The default name is **NweServerCertificate**.

3. Click **Advanced** tab. Only the following fields are supported for Mac agent:

Field	Description
Certificate Validation	Choose one of the options from the drop-down to determine how the agent will validate the NetWitness Endpoint Server certificate: - Thumbprint (default selection) - Full chain - None **Note:** By default, this setting will match the Agent Certificate Validation option selected in the Server Configuration panel of the NetWitness Endpoint UI, but it may be changed if desired. For more information, see the topic *Server Configuration Window* in the RSA NetWitness Endpoint **User Guide**.

Field	Description
Monitoring Mode	Choose an option to control the activation of the behavior tracking component: - No Monitoring - Full Monitoring (includes behavior tracking) For more information on Monitoring Mode options, see the topic *Tracking Systems* in the **NetWitness Endpoint User Guide**.
Beacon interval(s)	The rate at which the client notifies the server of its status (in seconds).

4. To verify that the configuration parameters are valid, and to test the network connection to all enabled servers before deployment, click **Test Connection**, and ensure it reports **OK** for all of its tests.



5. To generate the agent install file, click **Generate Agent.**
   The Agent executable is now ready to be deployed on a computer with the deployment method of your choice.

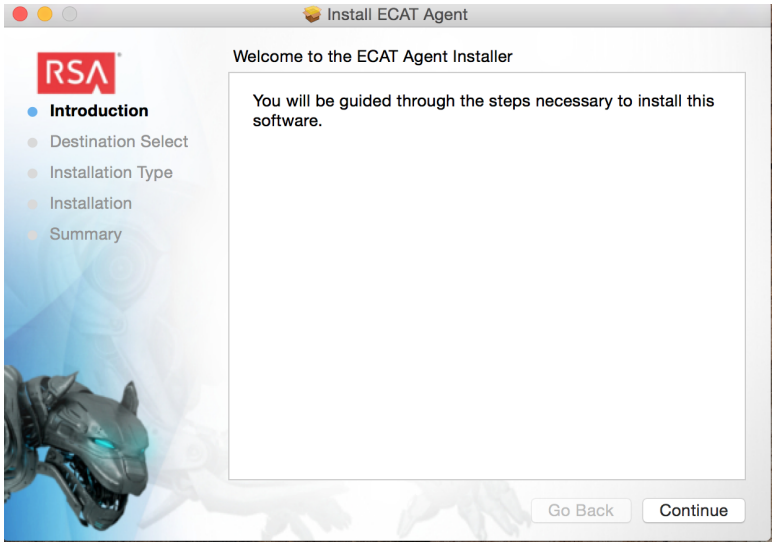
Task 2: Deploy the Agent (Mac)

Note: If the installation process fails for any reason and the connection to the server is available, the installer will send an error log to the server. To view the error log message, go to the location `/var/log/install.log`.

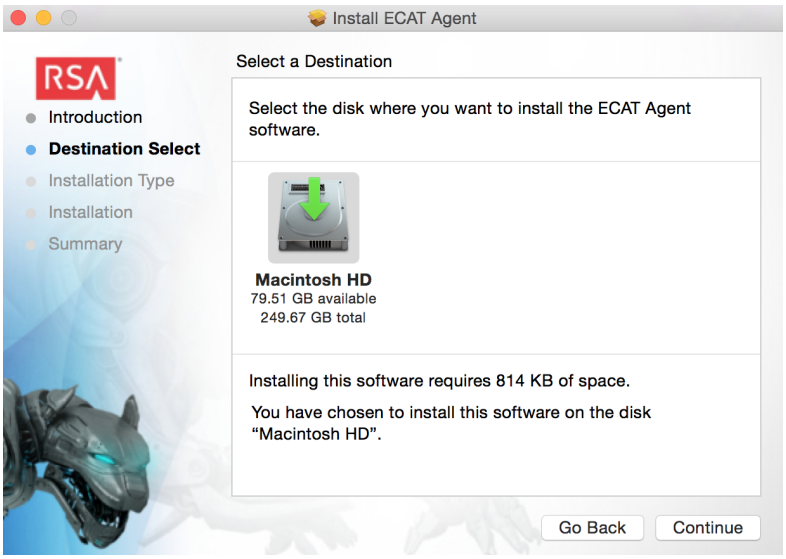
The agent can be deployed by any of the following methods:

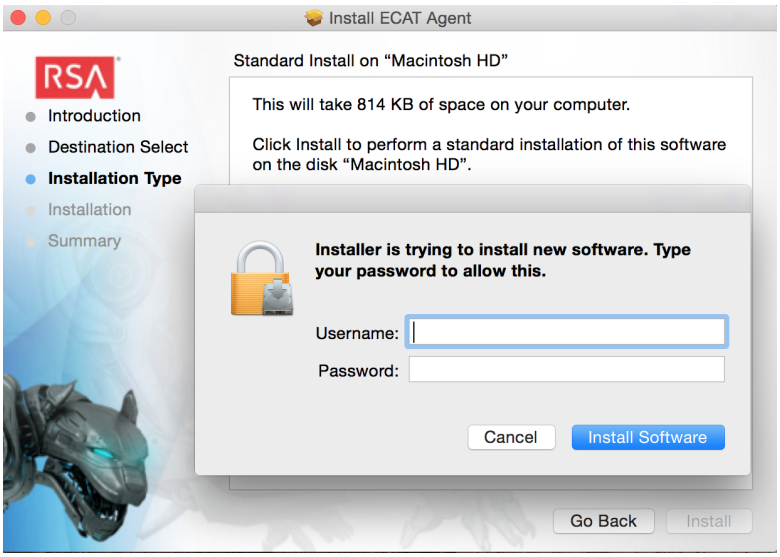
- **Option 1:** Manually running the agent installer (administrator rights are required) on the client machine (this will be a .pkg for Mac). The Mac .pkg installer takes you through a series of interactive installation steps.

  1. Copy the generated .pkg file to the target Mac machine. (Administrator rights are required for installation.)
  2. Double-click the .pkg file and click **Continue**.



  2. Follow the instructions on the screen and enter the administrator username/password when prompted.





- **Option 2:** Command line installation.

  To run the command, Open Terminal on the Mac and run the command:

  ```
  sudo installer -pkg $PATH_TO_ECAT_PKG -target /
  ```

  (Enter the administrator password when prompted)

  Note: Command line installation opens up possibilities for automation and remote installation. Admins can use an SSH session to remotely copy and install the package on the Mac machines. For this, make sure the in-built SSH server on Mac OS-X is enabled.

  To verify a Mac agent is running, open **Activity Monitor** and look for NetWitness Endpoint agent.

- **Option 3:** Any other automatic deployment system of your choosing.

Task 3: Managing Agent Daemon

A NetWitness Endpoint agent on a Mac machine registers itself as a daemon and runs continuously in the background. As part of installation, the following are installed:

- Main Executable:
  `/usr/local/ecat/ECATAgent`
- Driver:
  `/usr/local/ecat/ECATKext.kext`

To temporarily disable the Mac daemon:

In Terminal, run the command:

```
sudo launchctl unload /Library/LaunchDaemons/
com.rsa.ecat.agent.daemon.plist
```

To restart the Mac daemon:

In Terminal, run the command:

```
sudo launchctl load /Library/LaunchDaemons/
com.rsa.ecat.agent.daemon.plist
```

Task 4: Verifying Mac Agents

After deploying the Mac agents, you can verify if a Mac agent is running by using any one of the following methods:

- **Option 1**: Using the NetWitness Endpoint UI
  The **Machines** window contains the list of all computers with a NetWitness Endpoint agent. Mac machines are shown alongside the Windows machines.

  Note: Click **Tools > Refresh** or press F5 to refresh the Machines list when you need the latest data.

  From the **Machines** window, see the Machine Status column to check the status of the machine. For more information, see the topic *Agents Status Icons* in the RSA NetWitness Endpoint User Guide.

- **Option 2:** Using Activity Monitor
  Open Activity Monitor (/Applications/Utilities/Activity Monitor.app) and look for NetWitness Endpoint Agent.

- **Option 3:** Using Command Line
  Run the below command to get the PID:
  `pgrep ECATAgent`

- **Option 4:** To check the NetWitness Endpoint version, run the command:

```
grep a /var/log/system.log | grep ECATAgent | grep Version:
```

If you want to update an agent to the latest version of the NetWitness Endpoint agent, see the topic *Updating an Agent* in the **Managing Agents** section of the RSA NetWitness Endpoint User Guide.

Step 13: Deploy Agents (Linux)

The agent software runs under either i386 or x84_64 architecture and under the following Linux operating systems:

- CentOS 6.x and 7.x
- Red Hat Linux 6.x and 7.x

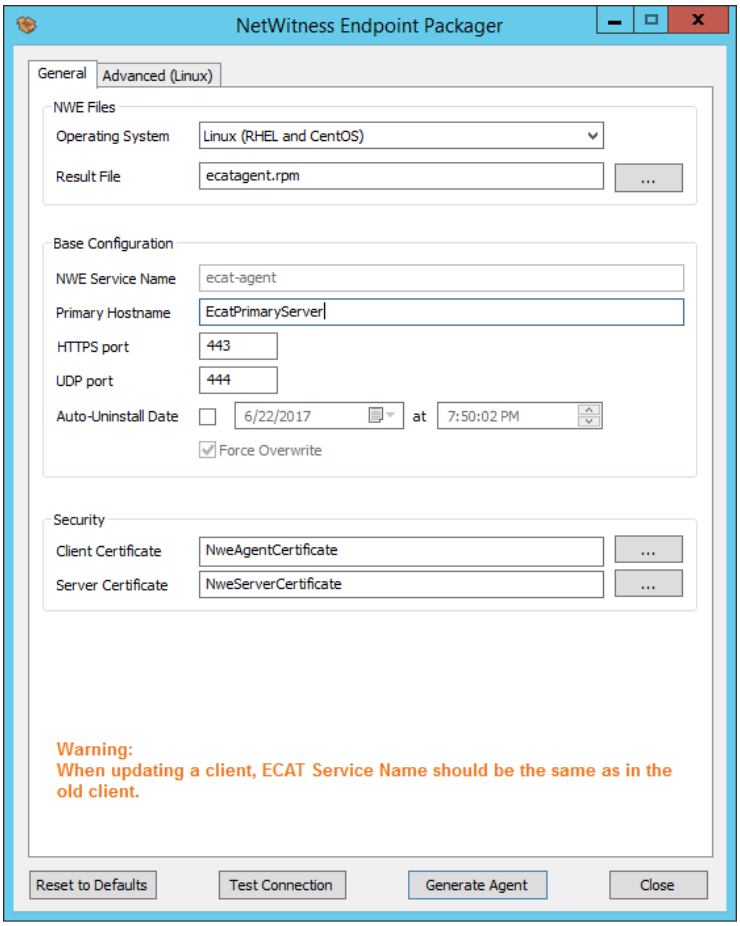
Task 1: Generate the Agent Installer (Linux)

The NetWitness Endpoint Packager is an independent application used to generate an installer application that, when installed on a client machine, can be used to run a program to install the NetWitness Endpoint agent. The same Packager application can generate installer programs for each type of agent (Windows, Mac, or Linux).

Note: Make sure that you generate the installer on a machine where the proper certificates are installed (ones that match the certificates from ConsoleServer).

To generate the agent installer:

1. Select **Start > All Programs > RSA NWE > NWE Packager**.
   The NetWitness Endpoint Packager dialog is displayed, as shown below.


NetWitness Endpoint Packager
General
Advanced (Linux)
NWE Files
Operating System
Linux (RHEL and CentOS)
Result File
ecatagent.rpm
...
Base Configuration
NWE Service Name
ecat-agent
Primary Hostname
EcatPrimaryServer
HTTPS port
443
UDP port
444
Auto-Uninstall Date
6/22/2017
at
7:50:02 PM
Force Overwrite
Security
Client Certificate
NweAgentCertificate
Server Certificate
NweServerCertificate
Warning:
When updating a client, ECAT Service Name should be the same as in the old client.
Reset to Defaults
Test Connection
Generate Agent
Close

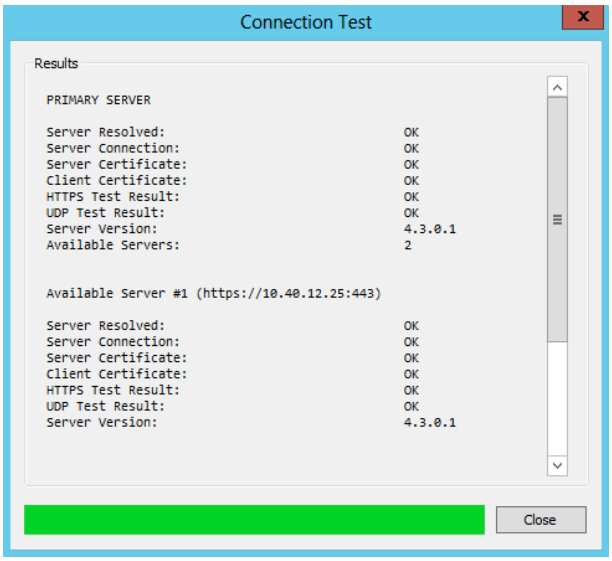
2. In the **General** tab, enter the following information:

Field	Description
NWE Files	
Operating System	Select either Linux or Linux 64-bit (RHEL and CentOS).
Result File	The name of the agent installer file. This can be copied to a new client machine and executed to install the agent. For Linux agent, this must have a .rpm extension.
Base Configuration	
NWE Service Name	This is set automatically to "ecat-agent" and is not configurable.
Primary Hostname	The IP address/hostname of the Primary ConsoleServer to which the agent starts talking as soon as it is installed.
HTTPS Port	The secure HTTP port number used by the ConsoleServer. The default value is 443.
UDP Port	The UDP port number used by the ConsoleServer. The default value is 444.
Auto-Uninstall Date	The date and time the NetWitness Endpoint agent automatically uninstalls. It can be left empty if not required
Force Overwrite	This option is ignored as it is not applicable for Linux agents.
Security	
Client Certificate	Select the client certificate generated, which the Linux agent will use to communicate with the NetWitness Endpoint Server. The default name is **NweAgentCertificate**. The client public certificate is bundled in the generated package and is the same for each installed client.
Server Certificate	Select the server certificate generated when the NetWitness Endpoint Server was configured. The default name is **NweServerCertificate**.

3. Click **Advanced** tab. Only the following two fields are supported for Linux agent.

Field	Description
Certificate Validation	Choose one of the options from the drop-down to determine the way the agent will validate the NetWitness Endpoint Server certificate: - Thumbprint (default selection) - Full chain - None
Beacon interval(s)	The rate at which the client notifies the server of its status (in seconds).

4. To verify that the configuration parameters are valid, and to test the network connection to all enabled servers before deployment, click **Test Connection**, and ensure it reports **OK** for all of its tests.



5. To generate the agent install file, click **Generate Agent.**
   The Agent installer is now ready to be deployed on a computer with the deployment method of your choice.

Task 2: Deploy the Agent (Linux)

The agent can be deployed by any of the following methods:

- **Option 1:** Manually running the agent installer (administrator rights are required) on the client machine (this will be a .rpm for Linux). The Linux rpm installer takes you through a series of interactive installation steps.

1. The NetWitness Endpoint ConsoleServer must be reachable from the NetWitness Endpoint client machine.
2. Copy the generated .rpm file to the target Linux machine. (Administrator rights are required for installation.)
3. Double-click the .rpm file and click **Continue**.
4. Follow the instructions on the screen and enter the administrator username/password when prompted.

- **Option 2:** Command line installation.
  To run the command, open Terminal on the Linux machine and run the following command as root (installer file name should match the agent installer file name generated in Task 1 above):
  `rpm -iv <installer file name>.rpm`
  For example, using the default installer file names, you could enter one of the following commands:
  `rpm -iv ecatagent.rpm` (for i386 architecture)
  `rpm -iv ecatagent(64-bit).rpm` (for x84_64 architecture)
  (Enter the administrator password when prompted.)

Task 3: Verifying Linux Agents

After deploying the Linux agents, you can verify if a Linux agent is running by using any one of the following methods:

- **Option 1:** Using the NetWitness Endpoint UI
  The **Machines** window contains the list of all computers with a NetWitness Endpoint agent. Linux machines are shown alongside the Windows and Mac machines.

  Note: Click **Tools > Refresh** or press F5 to refresh the Machines list when you need the latest data.

  From the **Machines** window, see the Machine Status column to check the status of the machine. For more information, see the topic *Agents Status Icons* in the NetWitness Endpoint User Guide.
- **Option 2:** Using Command Line
  Run the below command to get the PID:
  If agent version is 4.3.0.3 or earlier: `pgrep ecat-agent`
  If agent version is 4.3.0.4 (or later): `pgrep nwe-agent`

- **Option 3:** To check the NetWitness Endpoint version, run the command:
  If agent version is 4.3.0.3 or earlier: `cat /usr/local/ecat/ecat.cfg | grep ecat_version`
  If agent version is 4.3.0.4 (or later): `cat /opt/rsa/nwe-agent/config/nwe-agent.cfg | grep ecat_version`
- **Option 4:** To get the package version information, run the command:
  `rpm -qa | grep "agent Service name"`
- **Option 5:** To stop the Linux agent, run the command:
  `Service "agent Service name" stop`
- **Option 6:** To uninstall the Linux agent, run the command:
  `rpm -e "agent Service name"`

The following are the default locations (as of release 4.3.0.4) for the Linux agent installation:

- The Linux agent is installed to the `/opt/rsa/nwe-agent` directory
- The Linux agent binary is intalled to `/opt/rsa/nwe-agent/bin`
- The certificate and configuration are installed to `/opt/rsa/nwe-agent/config`

If you want to update an agent to the latest version of the NetWitness Endpoint agent, see the topic *Update an Agent* in the RSA NetWitness Endpoint User Guide.

Step 14: (Optional) Deploy Roaming Agents Relay

The NetWitness Endpoint Roaming Agent Relay (RAR) extends NetWitness Endpoint's visibility into endpoints disconnected from a corporate network. The RAR can be deployed as a cloud service or in a private DMZ, and it is packaged for flexible deployment, as a modular component.

This section provides an introduction to the NetWitness Endpoint Roaming Agents Relay (RAR) and instructions to deploy the RAR Server.

Information on the NetWitness Endpoint RAR, including complete installation instructions, is provided in the following topics:

- Roaming Agents Relay Overview
- Deploy Roaming Agents Relay Server
- Install and Configure RAR
- Configure the ConsoleServer for RAR
- Configure the NetWitness Endpoint UI

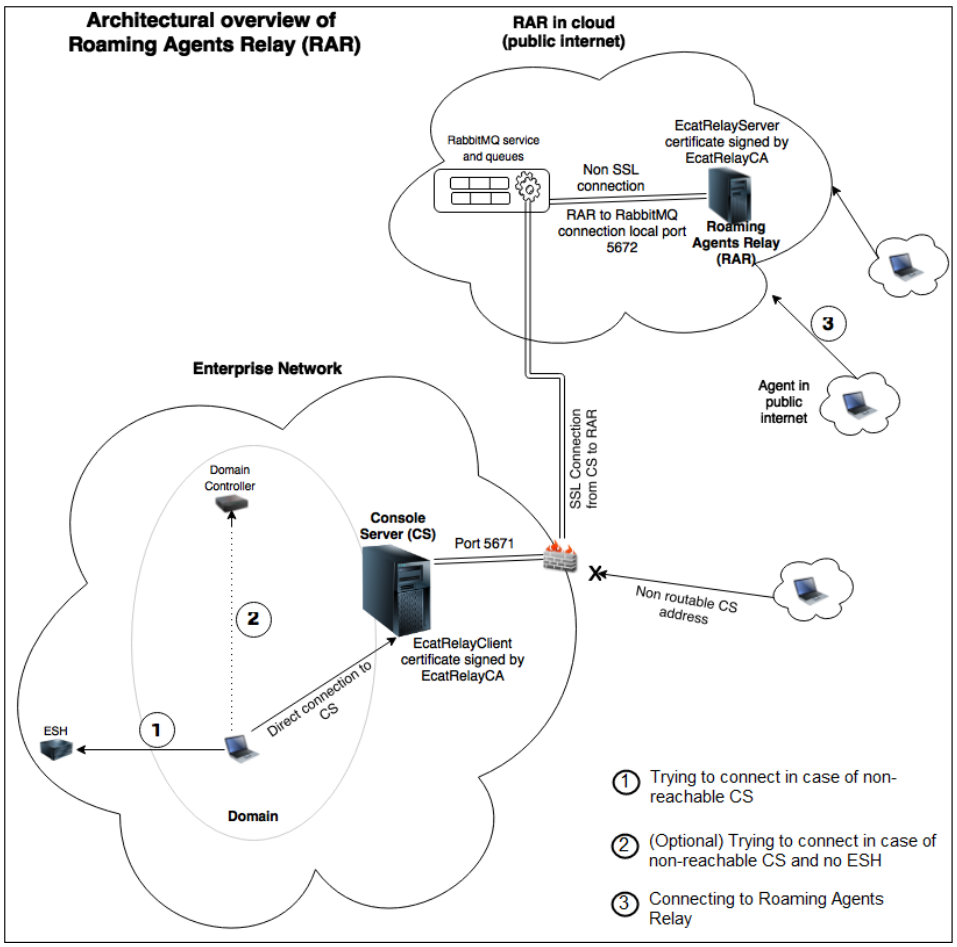
- Edit or Delete RAR Servers
- Decommission Relay Server

Roaming Agents Relay Overview

For endpoints located within the corporate network, NetWitness Endpoint has great behavioral tracking and analysis capabilities where every action on the endpoint is monitored to the finest detail and reported to the NetWitness Endpoint server that analyzes the data and detects the malware in the system. If the endpoints are outside the corporate network, the agent can no longer communicate with the NetWitness Endpoint server, and the endpoint behavior will not be evaluated. Modifying the firewall settings to accommodate NetWitness Endpoint will increase the attack surface and is not an acceptable workaround. The Roaming Agents Relay is designed to address this problem. A RAR server can be set up in the public environment that is accessible to both an endpoint outside the network and the NetWitness Endpoint server within the enterprise network. The endpoint outside the enterprise network sends the data to the RAR Server and the NetWitness Endpoint server pulls data from the RAR server. Thus the communication between the endpoint and the NetWitness Endpoint server happens through the secure infrastructure provided by the RAR server.

Roaming Agents Relay Architecture

The following figure describes the architecture for the Roaming Agents Relay.



Within the enterprise network, the NetWitness Endpoint agents that are deployed on client machines (laptops, desktops, servers) communicate with the NetWitness Endpoint ConsoleServer normally. When the NetWitness Endpoint agent is unable to connect to the ConsoleServer for any reason, the following sequence of actions takes place:

1. The agent tries to resolve Enterprise Specific Hostname (ESH).
2. (Optional) The agent tries to resolve Machine Domain Controller.
3. If RAR server is configured, the agent connects to the RAR server.

On configuring the RAR Server, a unique 256-bit AES key is generated for all NetWitness Endpoint agents. The agents within the enterprise network will receive the unique key and relay related information. Once the NetWitness Endpoint agents are outside the network, the agents will go through the following sequence before automatically switching to the Relay Server:

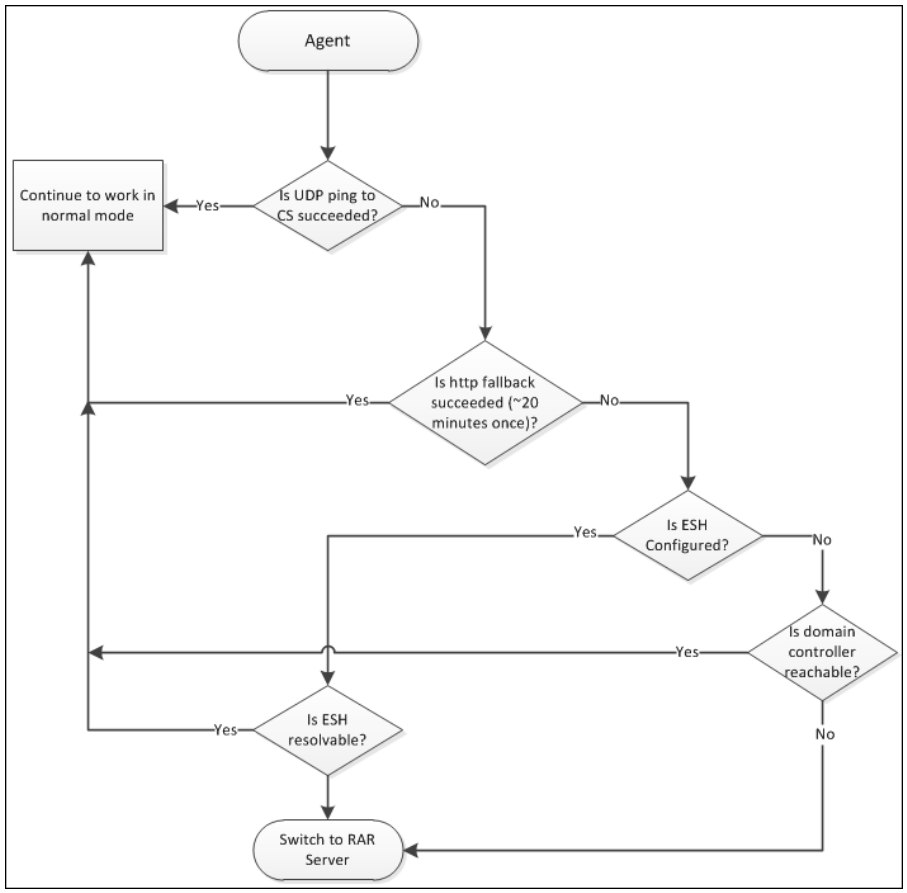
1. Unable to reach the ConsoleServer after a period of time (~ 20 minutes).
2. Unable to resolve Enterprise Specific Hostname (ESH).
   The **ESH Identifier** stands for **Enterprise Specific Hostname Identifier** and is particularly used for machines which are not in the domain.

Or

3. Unable to resolve the machine domain controller.

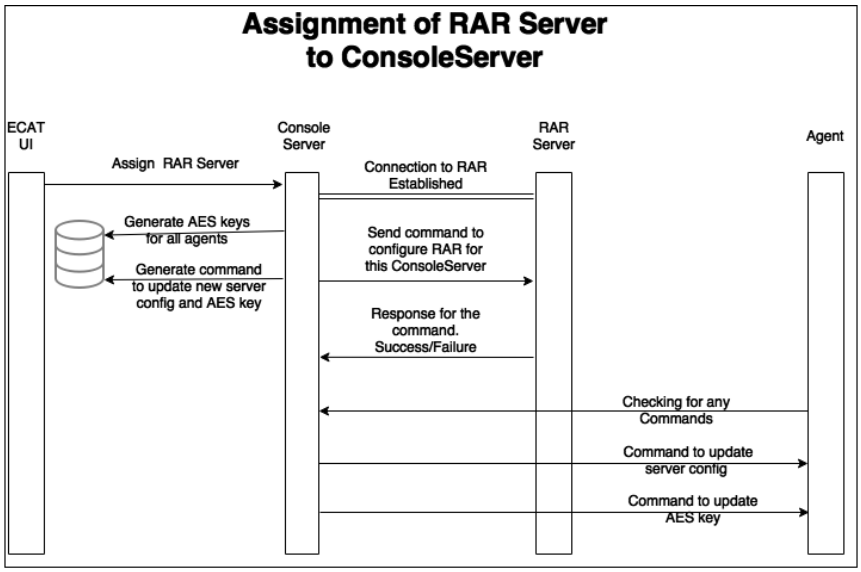
Note: During a temporary downtime of the ConsoleServer, you should prevent switching to RAR.

The above flow is also explained using a flow chart as shown in the following figure:



Assignment of RAR Server to ConsoleServer

When the NetWitness Endpoint agent tries to connect to the RAR server, there is a sequence of actions that takes place within the NetWitness Endpoint environment. The following figures describes the flow.



Advantages of Roaming Agents Relay

The NetWitness Endpoint Roaming Agents Relay offers the following advantages:

- It monitors and protects endpoints outside the enterprise network.
- It does not require any firewall to be set up.
- Agents can automatically determine if the endpoint is roaming and connect to either the NetWitness Endpoint ConsoleServer or the RAR server.

Deploy Roaming Agents Relay Server

This topic provides information about deploying the Roaming Agents Relay in the NetWitness Endpoint environment.

To deploy the RAR, you must do the following:

1. Install and Configure RAR
2. Configure the ConsoleServer for RAR
3. Configure the NetWitness Endpoint UI
   - Create Cloud Relay Configuration
   - Assign Relay Server to ConsoleServer
   - Enable RAR

Before installing RAR, you must ensure you meet the following hardware and software requirements:

Hardware

This following hardware requirements should be sufficient to handle up to 5,000 agents. More detailed hardware requirements are provided in the topic System Requirements.

- 100 GB disk space
- 12 cores
- 16 GB RAM

Software

The following additional software should be installed before installing RAR:

1. Erlang (tested with version 22.0); you will also need to copy the Erlang cookie (filename `.erlang.cookie`) from the system folder (`C:\Windows`) to the user folder (`C:\Users\<user_name>`).
2. RabbitMQ (tested with version 3.7.17); you should also enable the RabbitMQ management UI by running the following command: `rabbitmq-plugins enable rabbitmq_management`.
3. OpenSSL (latest)
4. Microsoft .NET Framework 4.6.1

Install and Configure RAR

This section provides detailed information on installing and configuring RAR.

To install and configure RAR, do the following:

1. Install Erlang.
2. Install RabbitMQ.
3. Create a base directory such as **C:\ECAT.**

   Note: RSA recommends using **C:\ECAT** as the base directory, though it is not mandatory. The instructions in this guide assume you have used the recommended path.
4. Create the directory **C:\ECAT\Relay** and extract all the files from the **rsa_nwe_4.4.x.x_roaming_agents_relay.zip** file into this directory.
5. **(Optional)** Configure the RabbitMQ ports by editing the **rabbitmq.config** file.
   a. Restart the RabbitMQ service to apply the configuration changes.
   b. Change the port numbers appropriately in the configuration files of RoamingAgentsRelay and ConsoleServer and restart them for proper communication.

Note: The port "`tcp_listeners`" is used by RoamingAgentsRelay and the port "`ssl_listeners`" is used by ConsoleServer to communicate with the RabbitMQ service.

6. Set the location of the RabbitMQ configuration file. From an elevated (Run as Administrator) command prompt, execute the following commands:

```
rabbitmq-service.bat remove
set RABBITMQ_BASE=C:\ECAT\Relay
setx -m RABBITMQ_BASE C:\ECAT\Relay
rabbitmq-service.bat install
rabbitmq-service.bat start
```

The usage of each command is given below:

`rabbitmq-service.bat remove` -> remove RabbitMQ Service
`set RABBITMQ_BASE=C:\ECAT\Relay` -> Set path in this command prompt context
`setx -m RABBITMQ_BASE C:\ECAT\Relay` - > Set path in global context
`rabbitmq-service.bat install` -> Install RabbitMQ Service
`rabbitmq-service.bat start` -> Start RabbitMQ Service

For more information, see https://www.rabbitmq.com/configure.html#customise-windows-environment.

Note: If you ever need to change the location of the RabbitMQ configuration file, you must re-install RabbitMQ. For more information, see https://www.rabbitmq.com/configure.html.

7. Extract the **RoamingAgentsRelay.zip** file into **C:\ECAT\Relay**.
   a. Copy **OpenSSL.exe**, **ssleay32.dll**, and **libeay32.dll** from OpenSSL binary zip to the same directory as the tool.
   b. **(Optional)** Provide a different name to "vhost" in the configuration file of the tool **RoamingAgentsRelayConfigTool.exe.config** against "CLSERVVhost". The default is **ecat**. If you change the default, you must update the changes in the **RoamingAgentsRelay.exe.config** and ConsoleServer configuration file. "VHost" is a virtual segregation within RabbitMQ machine. All the queues and exchanges are created within the "VHost".

   Note: VHost must not be changed unless required.

8. In an elevated (Run as Administrator) command prompt, execute "**RoamingAgentsRelayConfigTool.exe**" from its current location.

9. Set the RabbitMQ install directory. Click **Browse** and select the directory.
   For example, **C:\Program Files\RabbitMQ Server**.
10. Enter a password from the User Interface of the tool (A password is required to export the certificates with their private key).
11. Click **Configure**.
12. Verify the configuration as follows:
    - Check the log file of the tool for any errors.
    - Once the configuration is completed, the following files will be created:
      - EcatRelayServer.pem
      - EcatRelayServer.key
      - EcatRelayCA.pem
      - EcatRelayCA.cer
      - EcatRelayServer.pfx
      - EcatRelayClient.pfx
13. Create the directory "**C:\ECAT\Relay\Certs** and copy the files **EcatRelayServer.pem**, **EcatRelayServer.key**, and **EcatRelayCA.pem** to the new directory.

    Note: Retain the files **EcatRelayClient.pfx** and **EcatRelayCA.cer** to be used to configure ConsoleServer for RAR as explained in the following sections.
14. Click **Restart RabbitMQ Service**.
15. Open http://localhost:15672 in the browser and log in with username "`ecat`" and password "`ecat`" for managing RabbitMQ.

    Note: Use the appropriate port if it was previously changed in the configuration file.
16. Navigate to the folder **C:\ECAT\Relay** and validate the correctness of vhost, port, and credentials in the file **RoamingAgentsRelay.exe.config**.
17. Execute Roaming Agents Relay using one of the following options:
    - Run **RoamingAgentsRelay.exe** (requires local admin rights).
    - In an elevated command prompt, install Roaming Agents Relay as a service using the below command:
      `RoamingAgentsRelay.exe /install`.
      Open Windows services and start the service **RSA ECAT Relay Server**.

18. If **RoamingAgentsRelay** is installed as a service, open **RelayServerOutput.exe** to view the messages.

Configure the ConsoleServer for RAR

After you install and configuring RAR, you must configure the NetWitness Endpoint ConsoleServer for RAR.

To configure the ConsoleServer for RAR:

1. Copy **EcatRelayClient.pfx** and **EcatRelayCA.cer** from the RoamingAgentsRelay machine.
2. Import these certificates to the **Personal** folder of the **Local Computer** in certificate store. For more information, see http://sanganakauthority.blogspot.com/2012/02/install-certificate-in-local-computer.html.
3. Move **EcatRelayCA** to **Trusted Root Certification Authorities**.
4. Navigate to **C:\Program Files\RSA\ECAT\Server** or the location where ConsoleServer is installed and do the following:
   a. Open **ConsoleServer.exe.config**.
   b. Make sure that the "CLSERVVhost" entry has value configured previously.
5. Restart the RSAECATServer service or restart ConsoleServer application if it is not running as service.

Configure the NetWitness Endpoint UI

To configure the NetWitness Endpoint UI, you must first ensure the RAR is installed and configured and the ConsoleServer is configured for RAR.

The configuration of the NetWitness Endpoint UI consists of the following steps:

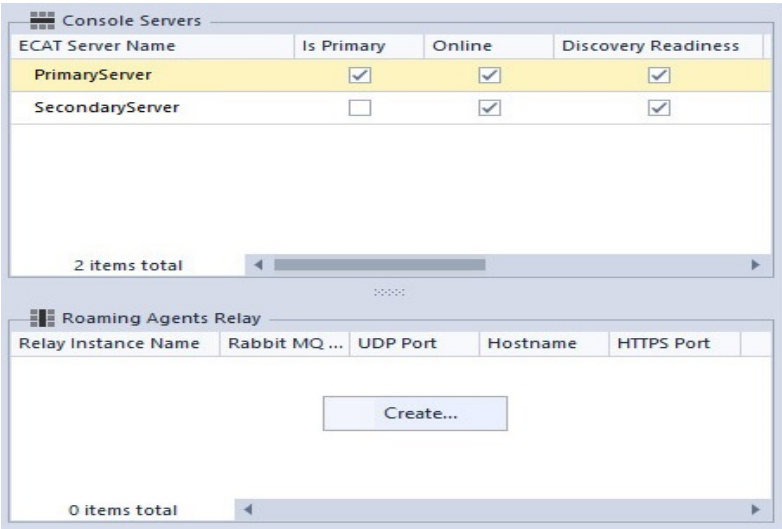
- Step 1: Create Cloud Relay Configuration
- Step 2: Assign Relay Server to ConsoleServer
- Step 3: Enable Roaming Agents Relay

Step 1: Create Cloud Relay Configuration

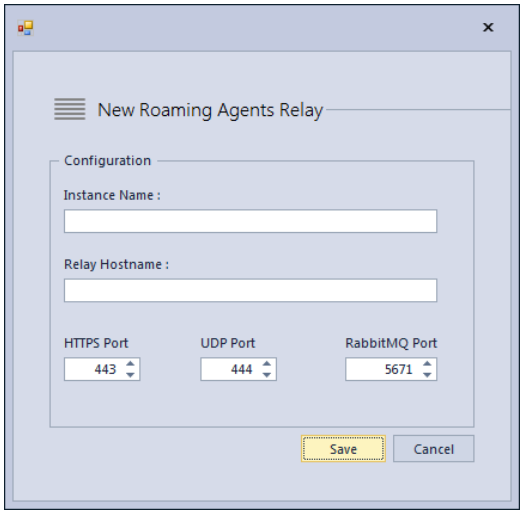
To configure the Cloud Relay:

1. Open the NetWitness Endpoint UI and log in using the user credentials with appropriate privileges to configure Relay Server. For more information on Users, Roles, and Permissions, see the section *Role-Based Access Control* in the RSA NetWitness Endpoint User Guide.

2. From the **Main Menu**, click **Server Configuration**.
3. Right-click within the Roaming Agents Relay window and click **Create**.



The New Roaming Agents Relay window is displayed.



4. Enter the following fields:

Name	Description
Instance Name	Enter a unique name to identify the RAR
Relay Hostname	Provide the hostname or IP address where the RAR server can be reached.
HTTPS Port and UDP Port	Enter the values of HTTPS port and UDP port that were previously configured in **RoamingAgentsRelay.exe.config**.

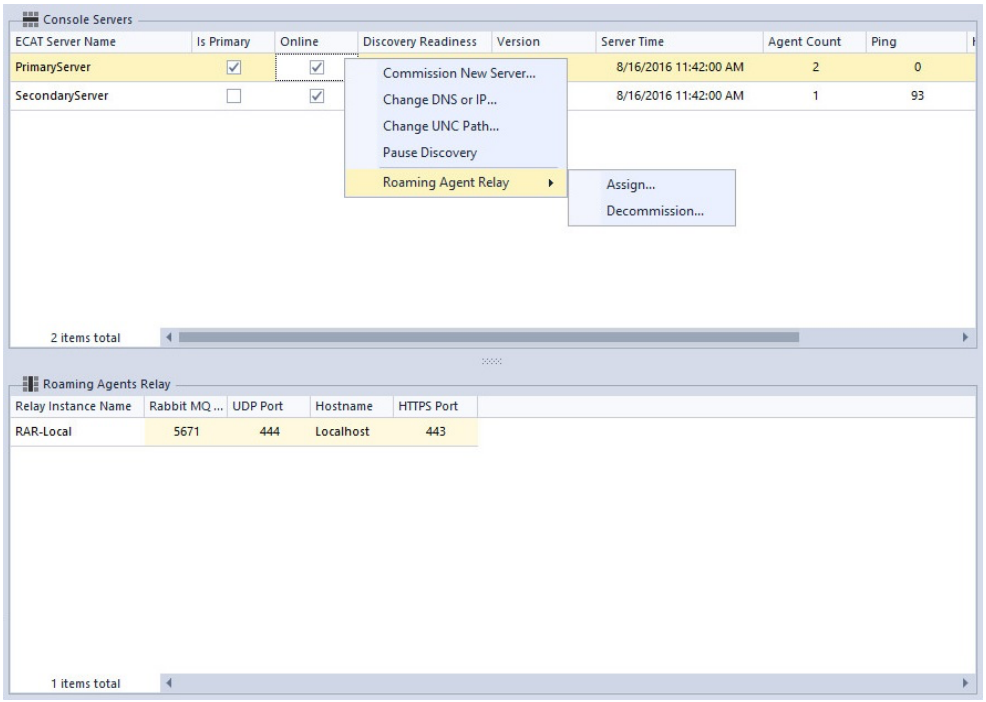
Name	Description
RabbitMQ Port	Enter the value of port "`ssl_listeners`" configured in **rabbitmq.config**.

5. Click **Save**.

Step 2: Assign Relay Server to ConsoleServer

To assign Relay server to ConsoleServer:

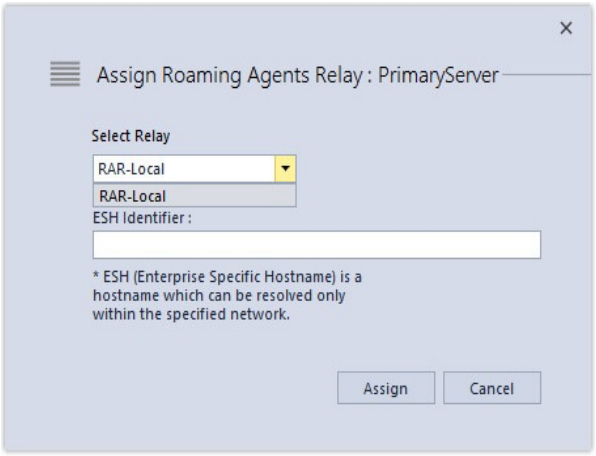
1. From the **Main Menu**, click **Server Configuration**.
2. Right-click on the ConsoleServer for which the relay server must be assigned and select **Roaming Agent Relay** > **Assign** as shown in the following figure.



The Assign Roaming Agent Relay window is displayed.

Note: For each ConsoleServer, you can assign only one single RAR server. But a single RAR server can be assigned to multiple ConsoleServers.

3. From the **Select Relay** drop-down, select the relay server to be assigned to the ConsoleServer.



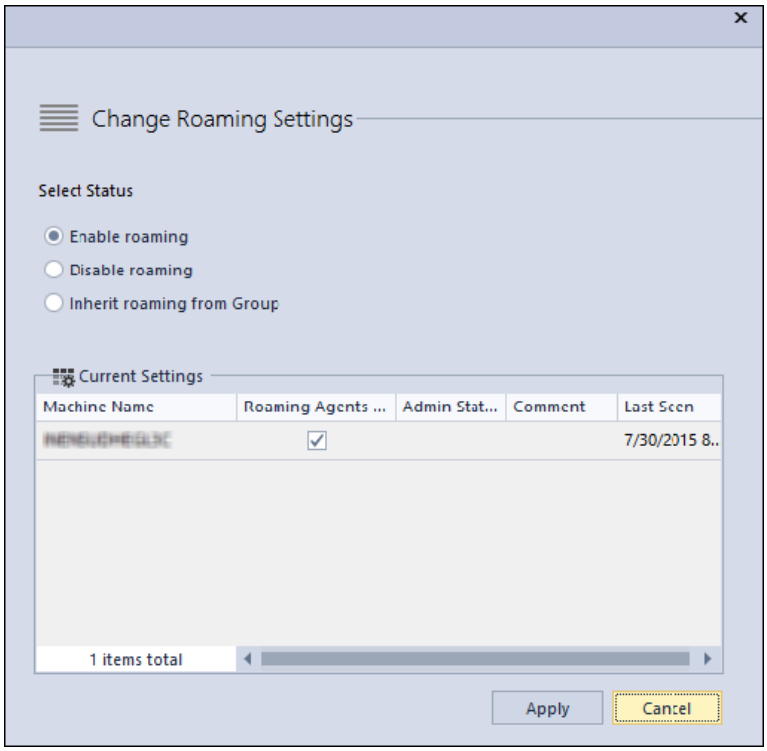
4. (Optional) Enter a hostname resolvable only within the enterprise network to help the agent identify if it is inside or outside the network.
5. Click **Assign**.
   The Relay server is assigned to the ConsoleServer. This also generates a unique 256-bit AES key for all NetWitness Endpoint agents. Also, the agents will receive the relay-related information automatically.

   Note: The unique key and relay information will be sent to the agents only if the agents are within the corporate network.
6. Make sure that Cloud Relay is enabled.
   The Cloud Relay feature is enabled by default. To verify or change the status, see **Step 3: Enable/Disable RAR** below.

Step 3: Enable Roaming Agents Relay

The Roaming Agents Relay is enabled by default. To change the status, use any one of the following options:

- Using the Machine View:
  a. Right-click the machine and select **Roaming** > **Roaming Settings**.
     The Change Roaming Settings dialog is displayed.



b. To enable RAR feature, select the "Enable Roaming" radio button.

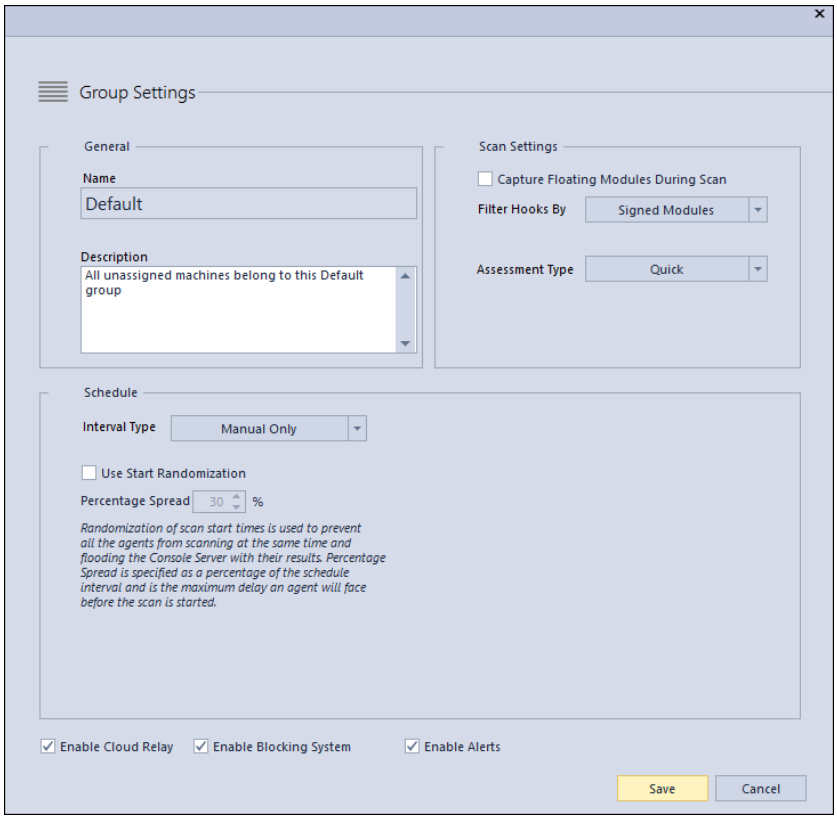
c. To disable RAR feature, select the "Disable Roaming" radio button.

d. Click **Apply**.

- Using Machine Groups:

  a. Click **Configure** > **Machine Groups**.

  b. Right-click the machine group and select **Edit Group**.
  The Group Settings dialog is displayed.



c. To enable RAR feature, select the "Enable Cloud Relay" checkbox.

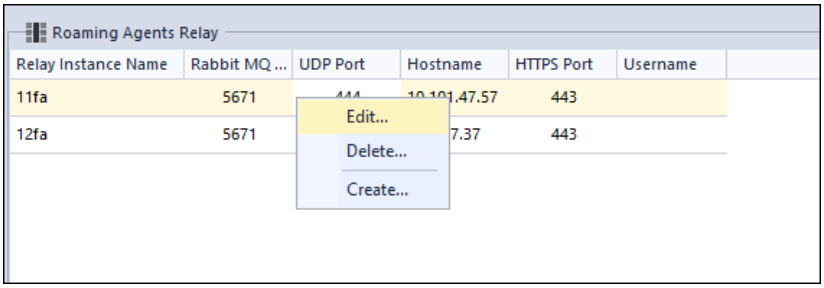
d. To disable RAR feature, uncheck the "Enable Cloud Relay" checkbox.

e. Click **Save**.

Edit or Delete RAR Servers

To edit a RAR server:

1. From the **Main Menu**, click **Server Configuration**.
2. Right-click on the RAR server to be edited and select **Edit**.



3. Make the required changes and click **Save**.

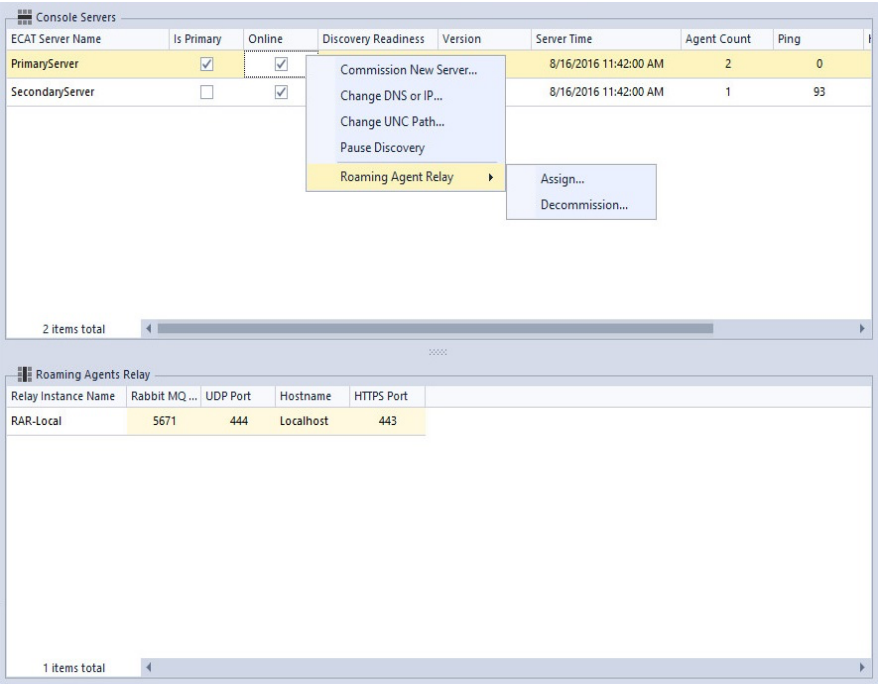
To delete a RAR server:

1. From the **Main Menu**, click **Server Configuration**.
2. Right-click on the RAR server to be deleted and select **Delete.**

Decommission Relay Server

To remove the configuration of the Relay server from the NetWitness Endpoint ConsoleServer, do the following:

1. From the **Main Menu**, click **Server Configuration**.
2. Right-click on the ConsoleServer for which the Relay server will be unassigned and select **Roaming Agent Relay** > **Decommission** as shown in the following figure.



3. Click **Yes** on the confirmation screen.

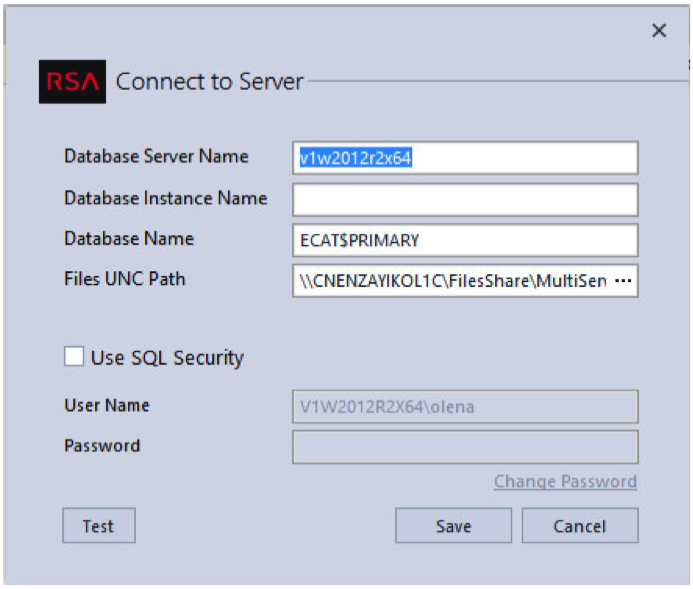
Step 15: Launch NetWitness Endpoint UI

After installing the servers and required components of NetWitness Endpoint and deploying the agent machine, the next step is to launch the NetWitness Endpoint UI. This topic provides information about launching the NetWitness Endpoint UI for the first time after installation.

Launch NetWitness Endpoint UI

To launch the NetWitness Endpoint UI:

1. Select **Start > All Programs > RSA NWE > NWE UI** to run the NetWitness Endpoint UI (user interface).
2. If you are opening the NetWitness Endpoint UI for the first time after installation, the Configuration dialog is displayed. If you have previously connected to the NetWitness Endpoint database with this installation, the NetWitness Endpoint UI will automatically reconnect every time you open the NetWitness Endpoint UI.



3. Complete the dialog as follows.

Field Name	Description
Database Server Name	Name of the machine running the SQL Server.
Database Instance Name	Name of the SQL Server instance (if it was named, otherwise leave this blank).
Database Name	Name of the database used by NetWitness Endpoint. This was entered during installation, and is the database automatically generated on the SQL Server. If you need to look up the name, select **Start > All Programs > Microsoft SQL Server 2012 > SQL Server Management Studio**, and look under **Databases**.
Files UNC Path	The path name for the folder where agents will upload files. (It must be a shared network folder for a multi-server environment.)

Field Name	Description
Use SQL Security	Check this if you want to use SQL Security, instead of Windows authentication, and enter your User Name and Password.

Note: OPSWAT does not support UNC File path. Hence, it is recommended to use a non-UNC file path for OPSWAT scan.

Note: To use UNC file path for OPSWAT scan, you must mount the share on the file system as a symbolic link. For more information, see https://my.opswat.com/hc/en-us/articles/202371520-How-do-I-scan-mapped-drives-with-Metascan-.

Reconfigure the NetWitness Endpoint UI

If you are not opening the NetWitness Endpoint UI for the first time, you get connected to the database automatically. But, you can still reconfigure the connection settings manually, at any time.

To reconfigure the NetWitness Endpoint UI:

1. Select **Configure** > **Connection** from the **Top Menu**.
2. Update the Configuration dialog box and click **Save**.

To exit the NetWitness Endpoint UI:

Click the close box in the upper right-hand corner of the NetWitness Endpoint UI window.

UPDATE INSTALLATION

This topic provides information for existing NetWitness Endpoint users to update to the latest NetWitness Endpoint release, as described in the following topics:

1. Prerequisites: Always check for necessary prerequisites before applying an update.
2. Update Scenarios: Information and directions for applying the latest NetWitness Endpoint software update.
3. Troubleshooting Update Issues: If you have trouble updating your NetWitness Endpoint installation, this section provides troubleshooting information.

Prerequisites

Before installing any update, it is strongly recommended to do the following:

1. Backup all Microsoft SQL Server NetWitness Endpoint databases, primary and secondary. To do so, use the standard Microsoft SQL Server tools such as SQL Server Management Studio, as explained below.
2. Create a backup copy of the server and client certificates, as explained below.
3. Follow the recommended guidelines for using the Microsoft Windows Update service to avoid interference with the NetWitness EndpointConsoleServer and the NetWitness Endpoint update process, as detailed below.

How to Create a Full SQL Database Backup

In case the update installation fails, the NetWitness Endpoint SQL database should be backed up according to the instructions provided here: https://msdn.microsoft.com/en-us/library/ms187510(v=sql.110).aspx.

Instructions to restore a database backup are provided here: https://msdn.microsoft.com/en-us/library/ms177429(v=sql.110).aspx

How to Create a Backup Copy of the Server and Client Certificates

These certificates are used to safely encrypt the communication between the NetWitness Endpoint Server and the NetWitness Endpoint agents. If they are lost or overwritten, they cannot be recovered and the previously deployed agent will not be able to communicate with the NetWitness Endpoint Server anymore.

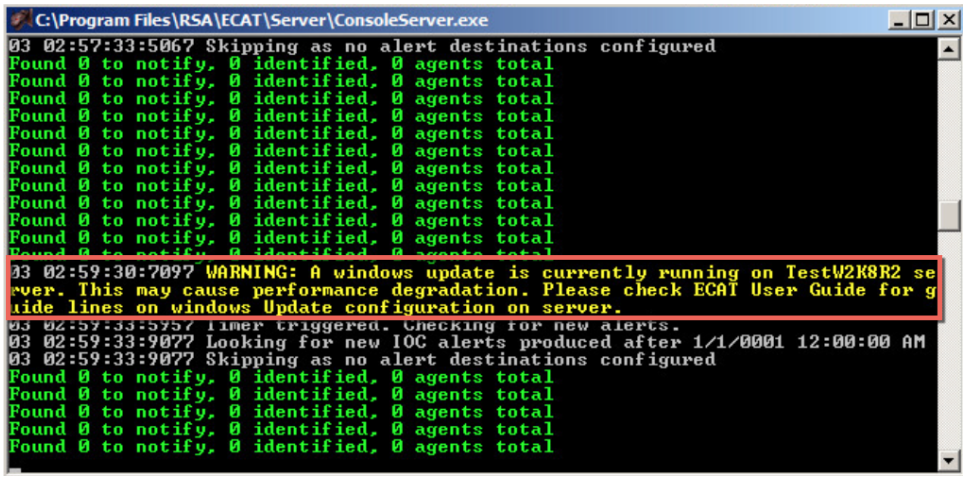
To create a backup copy of the server and client certificates, follow the instructions given in Step 4: (Optional) Export Primary Server Certificates in the Installation section.

Microsoft Windows Update Service Guidelines

To avoid a potential error message during the NetWitness Endpoint update procedure, caused by the Microsoft Windows Update service affecting the connection to the SQL Server, it is strongly recommended that you stop the Windows Update service before initiating the NetWitness Endpoint update installation. Furthermore, to avoid interference with the NetWitness Endpoint system, RSA recommends that you keep the Windows Update service turned off and use the following process for applying Windows Updates:

1. Stop the RSA ECAT Server and RSA ECAT API Server services.
2. Stop the SQLServerAgent service.
3. Turn on the Windows Update service and proceed with the Windows Update and all necessary steps such as download, installation, and reboot.
4. When the Windows Update is complete, turn off the Windows Update service.
5. Restart the SQLServerAgent service.
6. Restart the ECAT Server and ECAT API Server services.

Additionally, if the NetWitness Endpoint ConsoleServer is running and detects that a Windows Update is in process, the following message is displayed in the ConsoleServer:



Update Scenarios

This topic describes the procedures for updating to NetWitness Endpoint 4.4.x.x and NetWitness Endpoint Roaming Agents Relay (RAR) 4.4.x.x from supported upgrade paths. Supported upgrade paths are specified in the *RSA NetWitness Endpoint <4.4.x.x> Release Notes*.

NetWitness Endpoint 4.4.x.x Update Procedure

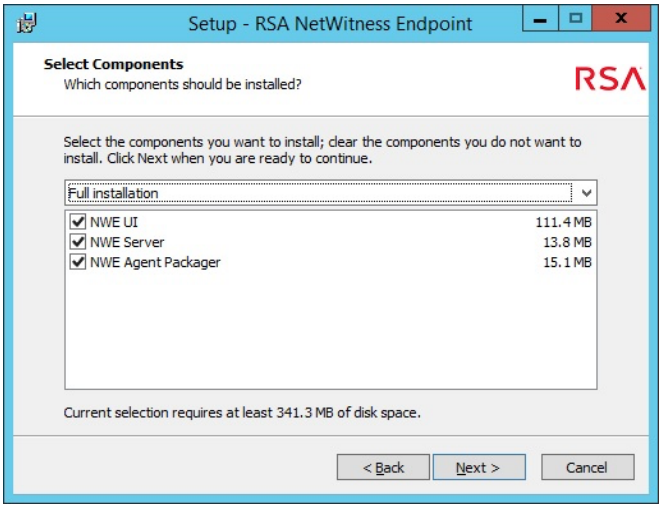
The update procedure is similar to installing the NetWitness Endpoint Primary Server, with noted deviations. For additional details refer to Step 3: Install Primary ConsoleServer. If you are using any NetWitness Endpoint secondary servers, you will need to repeat this process for each secondary server.

Note: If you have modified the `metakeysconfiguration.xml` file (default location: `C:\Program Files\RSA\ECAT\Server`), you must make a backup copy of this file before updating to a later version of NetWitness Endpoint 4.4. After the update is complete, you will need to manually restore the mappings from the backup configuration file.

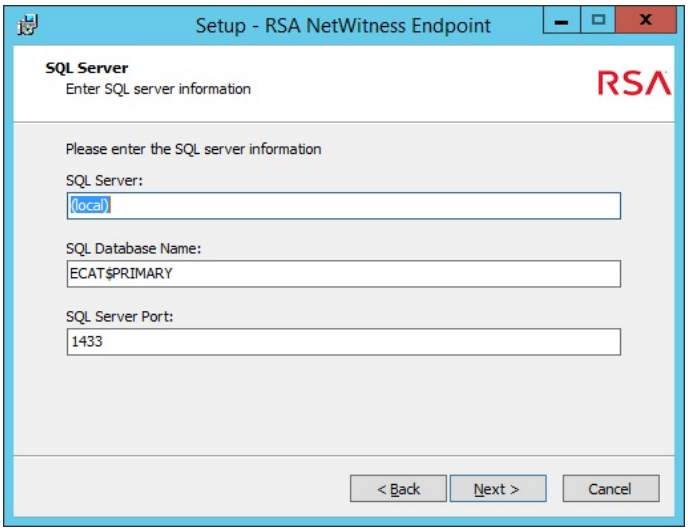
Note: If you attempt to update NetWitness Endpoint from an unsupported path, a message will display and you will not be able to continue with the update. Refer to the release notes for information on supported update paths.

To update to NetWitness Endpoint 4.4.x.x:

1. Close all existing NetWitness Endpoint applications.
2. Stop the SQLServerAgent service.
3. If not already done, unzip the archive file:
   rsa_nwe_*<4.4.x.x>*_sw.zip
4. Find and double-click the installer executable file:
   rsa_nwe_*<4.4.x.x>*_sw.exe
   The RSA NetWitness Endpoint Welcome screen for upgrade installations is displayed.
5. Click **Next**. The installer will attempt to detect and pre-fill existing installation configurations. Installed components, if detected, are pre-checked on the Select Components dialog, shown below.

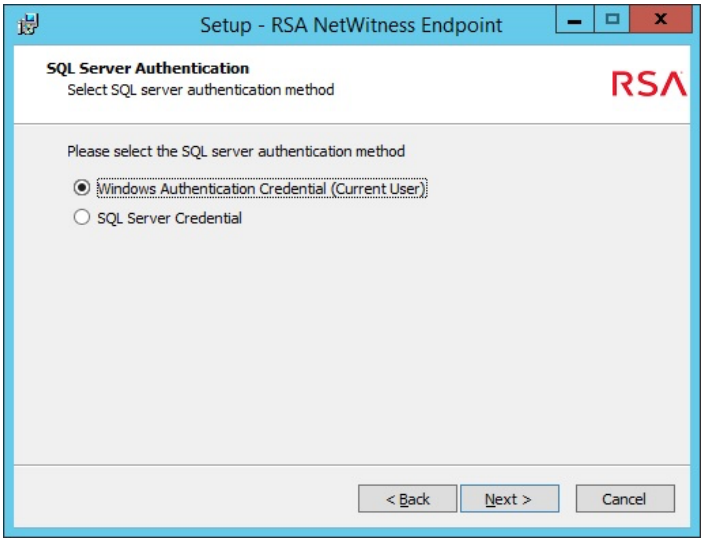


6. If you wish to change the pre-selected options, select the installation type and components you wish to install from the following options in the drop-down list:
   - **Compact installation**: installs the NetWitness Endpoint UI only
   - **Full installation**: installs the NetWitness Endpoint UI, NetWitness Endpoint Server, and NetWitness Endpoint Agent Packager
   - **Custom installation**: installs the components selected by clicking the checkboxes next to the desired item below the drop-down (For example, to install just the NetWitness Endpoint Primary server, select **Custom installation** and check the box next to **NWE Server**.)
7. While selecting the programs to install, make sure to select **NWE Agent Packager** as you will also need to update all agents.
8. By default, the update installs the selected components to the **C:\Program Files\RSA\ECAT** directory.
9. If you are updating from 4.1.2.0, and if YARA was previously enabled, a message is displayed asking if you want to copy the existing YARA executable and rules to the new location and update the configuration in the new installation. If you click **Yes**, the files are copied to the new location. If you click **No**, the YARA files will not be moved. Following the update, YARA and OPSWAT can be configured from the Monitoring and External Components option in the NetWitness Endpoint UI. (If you are updating from 4.2.0.x (or later), you will not see this message as this was done during the 4.2 update.)
10. Click **Next**.
11. On the SQL Server dialog, shown below, enter the SQL Server you are using for NetWitness Endpoint It is not recommended to change the default entry for SQL Database Name. Set the SQL Server Port only if necessary.

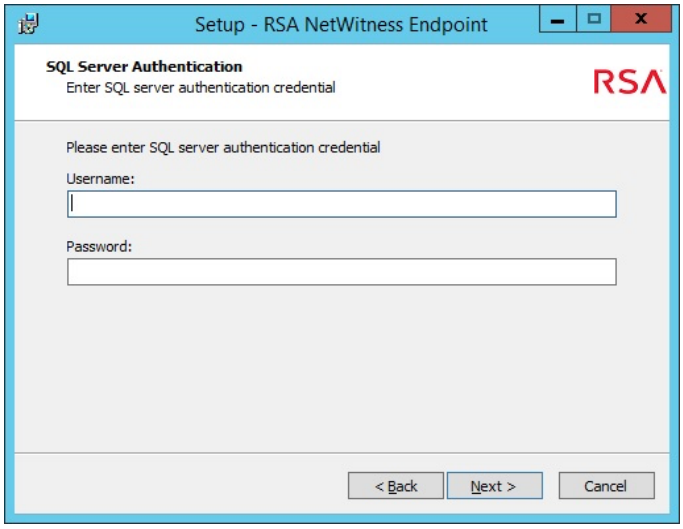


12. Click **Next**.

    The SQL Server Authentication dialog is displayed, as shown below:



13. Do one of the following:
    - Select **Windows Authentication Credential** and click **Next**.
    - Select **SQL Server Credential** and click **Next**. The following dialog is displayed:



Enter the necessary SQL Server authentication username and password and click **Next**.

Note: If in attempting to connect to the SQL Server it is determined that there is already an existing database, a message is displayed with options to either reuse or delete the existing database. For more information, see Manage Existing Database During Installation.

14. The installer checks for Firewall rules and, if found, re-creates them.
15. On the Ready to Install dialog, review the installation configuration information. If you want to make changes, click **Back** to return to previous configuration dialogs.
16. Click **Install** to complete the upgrade installation.
17. Restart the SQLServerAgent service on both Primary and Secondary servers.
18. Start the NetWitness Endpoint Primary and Secondary servers.
19. Once the update is applied on all the servers, generate a new package and update all agents using the option **Tools > Agent Maintenance > Update All Agents** in the NetWitness Endpoint UI.
20. Initiate scans on updated agents.

Note: For all agents communicating through RAR, you should wait until agents are communicating directly to the ConsoleServer before updating to ensure a successful update.

Note: After updating all agents, some data in the NetWitness Endpoint UI may be out of date. Clearing the cache or checking again after the initial scan should load the latest information.

Additional Components

The following additional components are optional and may be installed separately after updating to NetWitness Endpoint 4.4.x.x.

- REST API Server
  To install the REST API Server, run the **ApiServer.exe** file located in the folder **C:\Program Files\RSA\ECAT\Server**.
  For more information about the REST API Server, see the topic *REST API Server* in RSA NetWitness Endpoint User Guide.
- Roaming Agents Relay (RAR)
  For information about installing and configuring the Roaming Agents Relay Server, see Step 14: (Optional) Deploy Roaming Agents Relay.

NetWitness Endpoint Roaming Agents Relay (RAR) 4.4.x.x Update Procedure

If you are currently using RAR, you must also update the RAR installation by following these instructions:

1. If not already completed, update the NetWitness Endpoint ConsoleServer to NetWitness Endpoint 4.4.x.x using the method described above.

Caution: It is very important that you update the NetWitness Endpoint ConsoleServer to NetWitness Endpoint 4.4.x.x before updating RAR.

2. Download the NetWitness Endpoint Roaming Agents Relay zip package (**rsa_nwe_*<4.4.x.x>*_roaming_agents_relay.zip**)
3. Do one of the following:
   - If running RAR as a service, stop the **RoamingAgentsRelay** service
   - Close the **RoamingAgentsRelay.exe** application
4. Extract the following files from the zip package to the existing Roaming Agents Relay folder (default location: **C:\ECAT\Relay**\), replacing older matching files if required:
   a. Newtonsoft.Json.dll
   b. RabbitMQ.Client.dll
   c. RabbitMQ.config
   d. RelayCustomActionLib.dll
   e. RelayServerOutput.exe

f. RoamingAgentsRelay.exe

g. RoamingAgentsRelayConfigTool.exe
Note: Do not replace config files unless required.

5. Open **RoamingAgentsRelayConfigTool.exe** and click **Upgrade to Current version**.
6. Do one of the following:
   - If running RAR as a service, start the **RoamingAgentsRelay** service
   - Run **RoamingAgentsRelay.exe** as an application

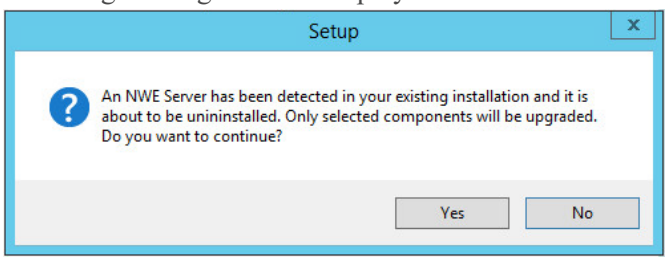
Troubleshooting Update Issues

Possible Update Issues

In some special cases, error messages could display during the update process, as described in the following sections.

NetWitness Endpoint Server Detected But Not Selected for Update

If the Update Installer program detects a NetWitness Endpoint Server in the environment, but the NetWitness Endpoint Server option is unchecked on the Select Components dialog, the following message will be displayed:

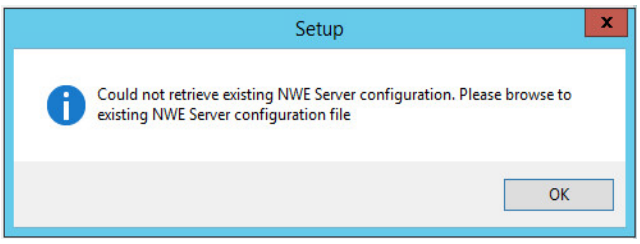


If you click **Yes**, the existing NetWitness Endpoint Server will be uninstalled.
If you click **No**, you will return to the Select Components dialog.

Installer Unable to Retrieve NetWitness Endpoint Server Configuration

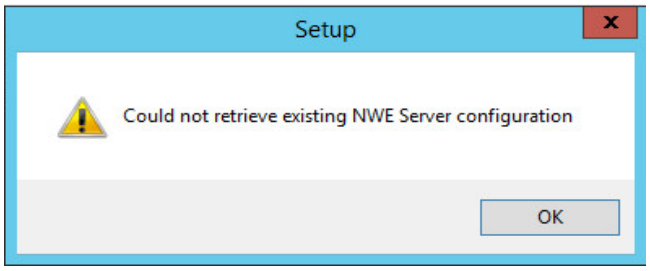
The installer gathers NetWitness Endpoint Server configuration information from the **ConsoleServer.exe.config** file, as well as information from the SQL database and from Windows for firewall and Windows Service settings.

- If the installer cannot find the **ConsoleServer.exe.config** file, the following message is displayed:



Click **OK**.
A dialog is displayed where you can browse to locate and select the **ConsoleServer.exe.config** file.

- If the installer cannot retrieve the **ConsoleServer.exe.config** file or the file is invalid, the following message is displayed:



Click **OK**. At this point your only option is to browse to another installation path to try to locate the configuration file. If the installer cannot retrieve the previous installation's configuration you cannot proceed with the update installation.

Once the installer has valid NetWitness Endpoint Server configuration information, it will proceed with the update installation.

Review Log File

If you have any issues with completing the update, the NetWitness Endpoint installer generates a log file that gets saved to the following location:
C:\Users\Administrator\AppData\Local\Temp.
The default filename is:
Setup Log YYYY-MM-DD #SSS.txt

The log file records the following activities:

- All actions taken
- All information collected from the user
- All information collected by other means
- Return codes of all actions
- All error messages

If Update Fails

If the update fails, the database will automatically rollback to its original state. You can reinstall with the existing database just by relaunching the NetWitness Endpoint installer. The NetWitness Endpoint system will be reinstalled and the database will be upgraded if needed.

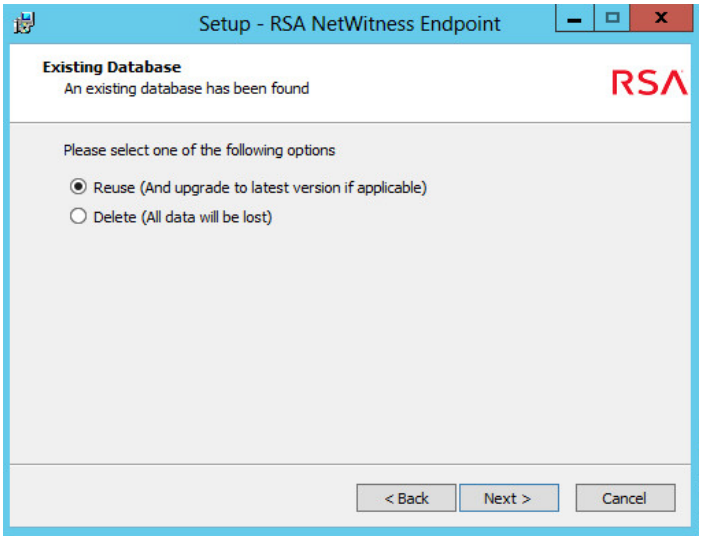
ADDITIONAL PROCEDURES

This topic provides additional information related to installing and configuring NetWitness Endpoint 4.4, as follows:

Manage Existing Database During Installation

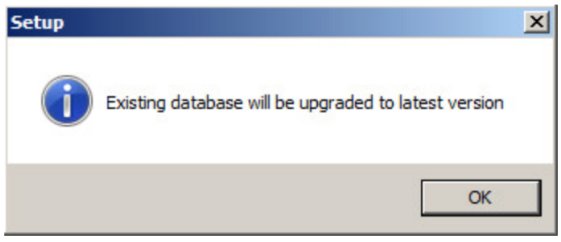
When installing or re-installing either a Primary or secondary ConsoleServer, if the installer encounters an existing SQL database, a special dialog displays. The user must then select how to manage the existing database, as explained in the following steps.

1. During the installation (or re-installation) of a Primary or secondary ConsoleServer, after selecting the SQL server authentication method, the installer attempts to access the SQL Server. If the installer determines that there is an existing database, the following dialog is displayed:

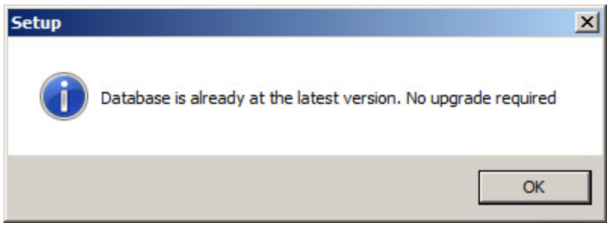


2. Do one of the following:

- Select **Reuse** and click **Next**. The existing database will be reused and upgraded to the latest version (if applicable).
  - If the database upgrade is supported for the existing database version, the following message is displayed:

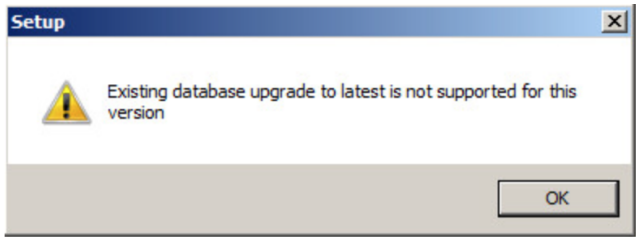


    Or, if the database is already at the latest version, the following message is displayed:



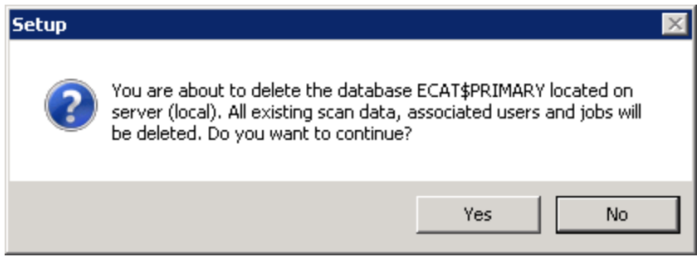
    Click **OK** to continue. Configuration settings from the existing database will be reflected going forward rather than the default options, but can be changed.

  - If the database upgrade is not supported for this upgrade path, the following message is displayed:

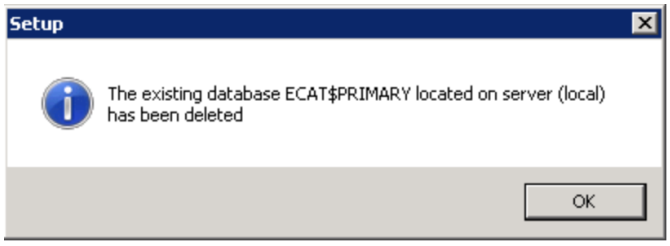


    Click **OK** to return to the Existing Database dialog. Your options in this case are to cancel the installation, delete the existing database, or create a new database with another name.

- Select **Delete** and click **Next**. The existing database, and all its data, will be deleted. The following warning message is displayed:

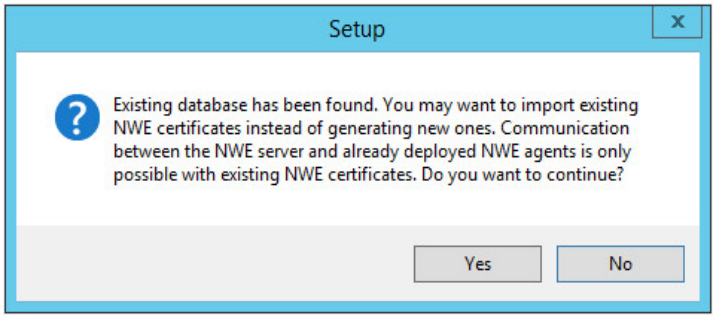


- If you click **No**, you will be returned to the Existing Database dialog.
- If you click **Yes**, the following confirmation message is displayed:



Click **OK** to continue.

3. The NetWitness Endpoint Server and NetWitness Endpoint Agents Certificates dialog is displayed, and you can continue the normal installation process for either the Primary or secondary ConsoleServer. However, if you select to generate new NetWitness Endpoint certificates and the installer does not find any existing certificates, the following message will display:



4. If you have an existing database, it is strongly recommended that you import your existing certificates instead of generating new ones to ensure the NetWitness Endpoint server can continue to communicate with already deployed NetWitness Endpoint agents.
   Click **No** to return to the previous dialog or **Yes** to continue generating new certificates.
5. Continue the normal installation process.

Manage Authentication After Installation

This topic provides information about choosing the type of authentication after the installation has completed.

To use SQL Authentication

1. Open the *ConsoleServer.exe.config* XML file and add the following line:
   ```
   <add key="DbSaUser" value="[Username]"></add>
   ```
2. Using the command prompt, do the following:
   start:
   ```
   > ConsoleServer.exe /setdbpswd
   ```

To use Windows Authentication

1. Open the *ConsoleServer.exe.config* XML file.
2. Remove the following line (or set value to ""):
   ```
   <add key="DbSaUser" value=""></add>
   ```

Configure External Tools

There are different external components that can be configured in NetWitness Endpoint. You can also monitor these external components using the NetWitness Endpoint UI.

Some of the external components that are supported are:

- RSA NetWitness Suite
- RSA Live
- RSA Netwitness v9.7
- SMTP
- Syslog
- Incident Management
- OPSWAT Scan Engine
- YARA Scan Engine

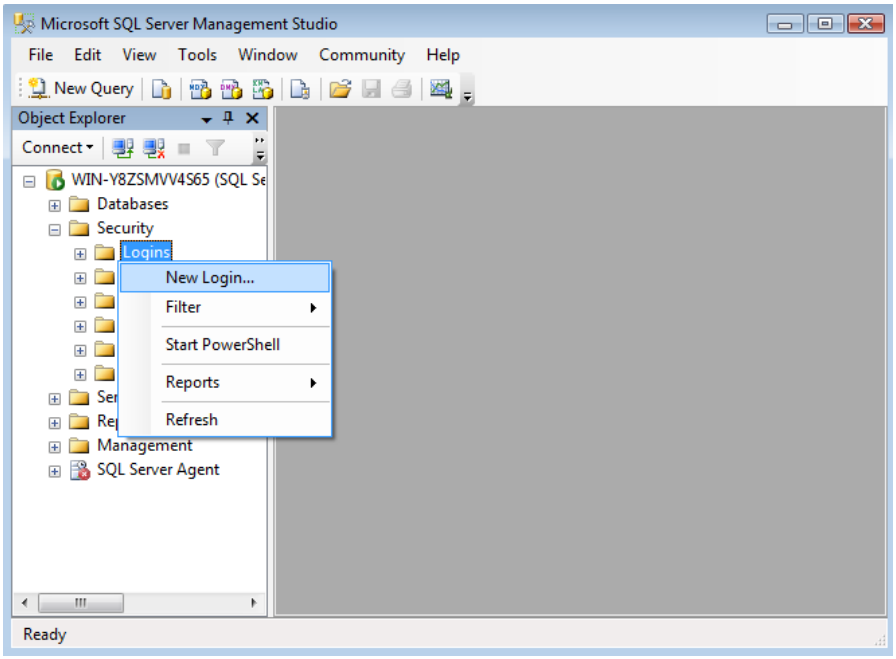
For more information about configuring these external components, see, *Monitoring and External Components* in the RSA NetWitness Endpoint User Guide.

Add a User to the Microsoft SQL Server

This topic provides information about adding a user to Microsoft SQL Server.

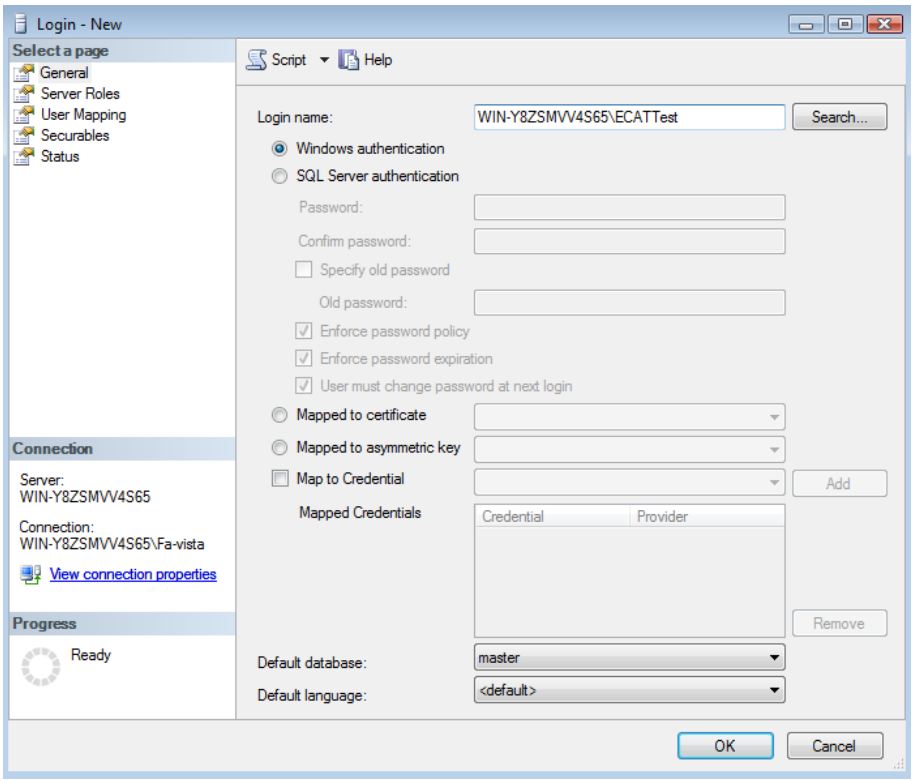
To add a user to the Microsoft SQL Server:

1. Open the **Microsoft SQL Management Studio**.
2. Expand the **Security** folder.
3. Right-click on **Logins**.
4. Select **New Login**.

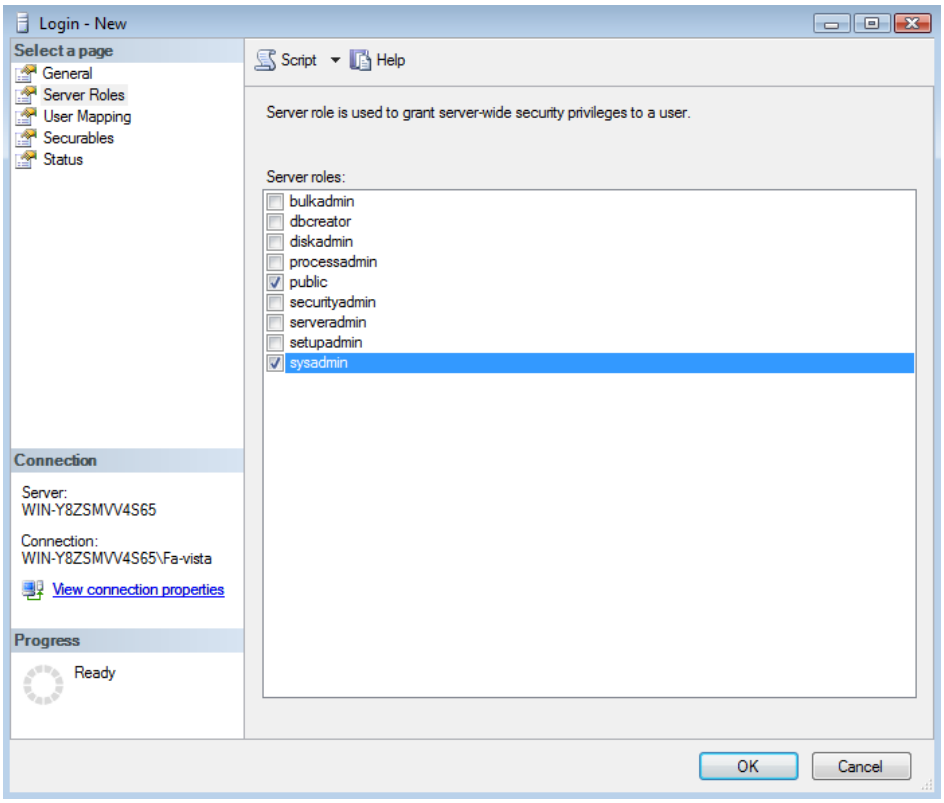


5. Make sure **Windows Authentication** is selected.

6. Enter the **Login name** or do a search for it.



7. Select **Server Roles**.
8. Check the **sysadmin** server role.



9. Click **OK** to finish

Note: NetWitness Endpoint requires the sysadmin server role to function properly. To avoid possible interactions with other databases, it is recommended to create a separate instance of SQL Server.

Configure Proxy Settings of ConsoleServer

This topic describes how to configure proxy settings for the NetWitness Endpoint ConsoleServer.

It is possible to add proxy configuration settings directly in the ConsoleServer.exe.config file (using standard .NET). An example of such a configuration would look like this:

```
<configuration>
    […appSettings… system.serviceModel…]
    <system.net>
        <defaultProxy>
            <proxy
                usesystemdefault="False"
                proxyaddress="http://theproxydomain:8888"
                bypassonlocal="True"
            />
        </defaultProxy>
    </system.net>
</configuration>
```

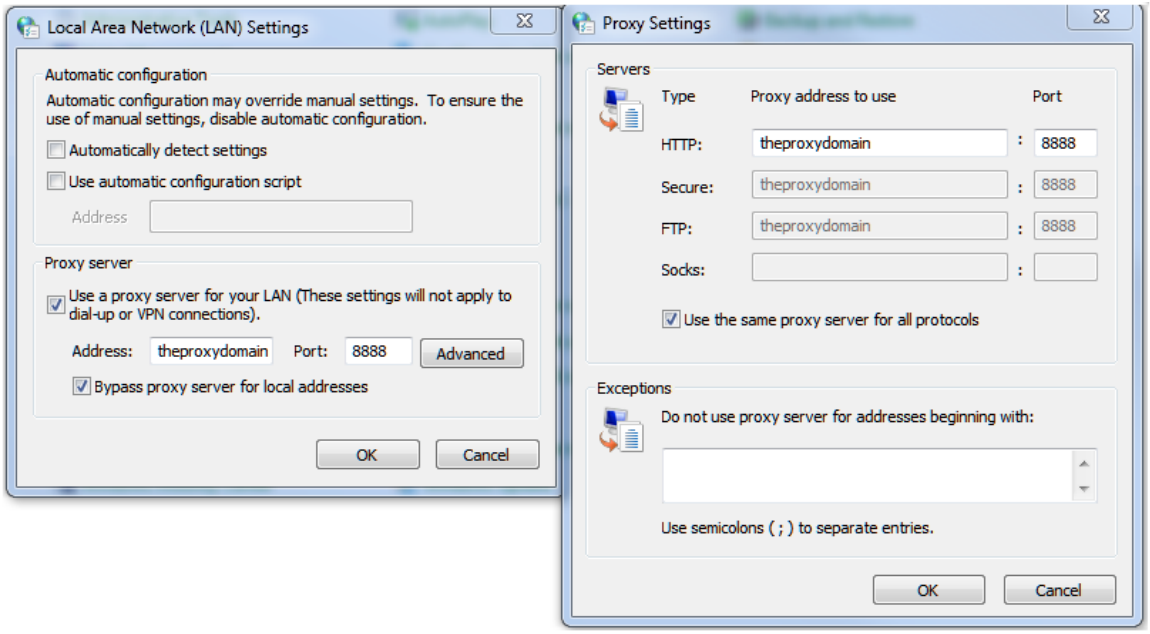
Adding configuration settings in this way allows for re-copying all the settings normally found in Internet Options (under the Connections tab, in LAN Settings).

Note: In order for Meta Integrator to successfully connect to Log Decoder, a web proxy exception may need to be configured. This can be done either in Internet Options or in ConsoleServer.exe.config using the bypasslist XML node. Depending on the network configuration, the bypass proxy server for local addresses (bypassonlocal in XML) may produce the same result.

For complete instructions for this procedure, refer to:

- <defaultProxy> reference: https://docs.microsoft.com/en-us/dotnet/framework/configure-apps/file-schema/network/defaultproxy-element-network-settings
- <proxy> reference: https://docs.microsoft.com/en-us/dotnet/framework/configure-apps/file-schema/network/proxy-element-network-settings
- <bypasslist>: https://docs.microsoft.com/en-us/dotnet/framework/configure-apps/file-schema/network/bypasslist-element-network-settings

The following figure shows the equivalent of the configuration example provided above as it would look in Internet Options:



Enabling Proxy Authentication and Using Credential Manager

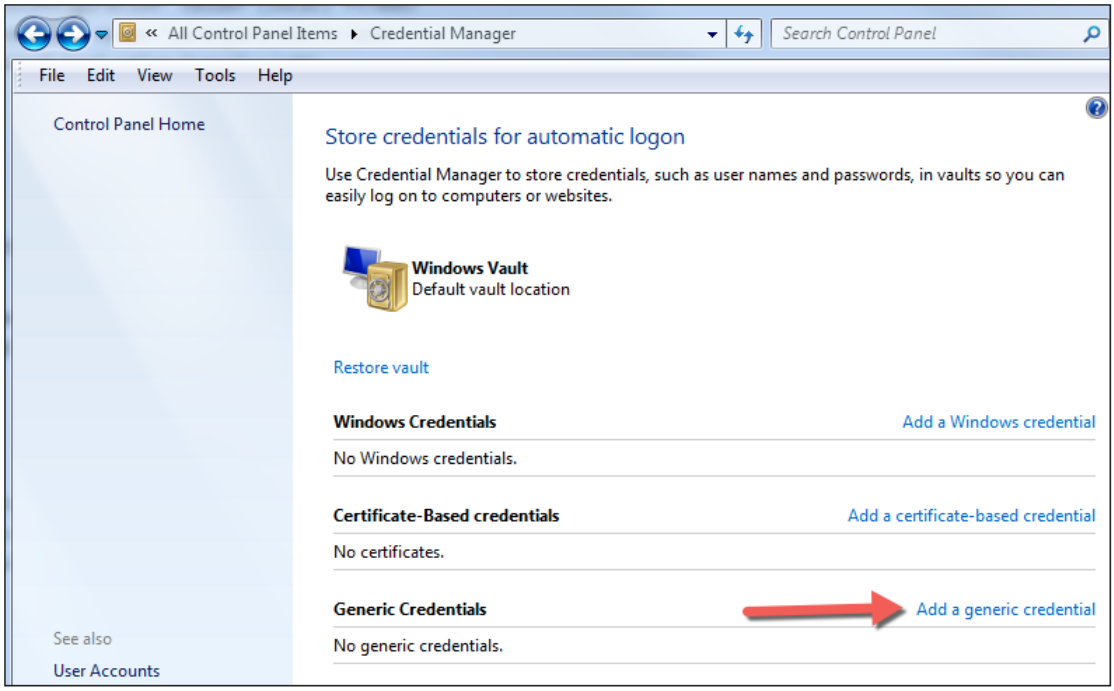
You can enable Proxy Authentication using service account credentials by adding a new property to the `<defaultProxy>` node called: `useDefaultCredentials=true`.

The config file in this case would look like this:

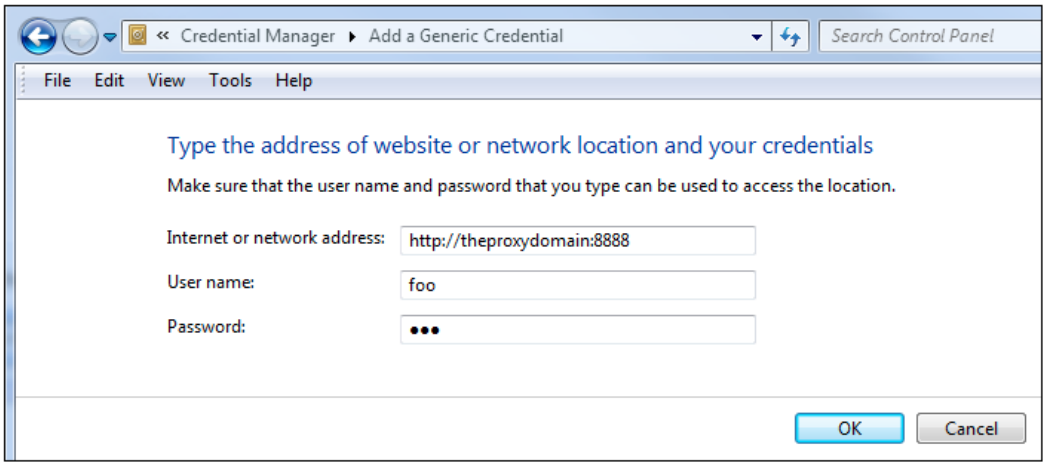
```
<system.net>

    <defaultProxy useDefaultCredentials="true">
        <proxy
            usesystemdefault="False"
            proxyaddress="http://theproxydomain:8888"
            bypassonlocal="True"
        />
    </defaultProxy>
</system.net>
```

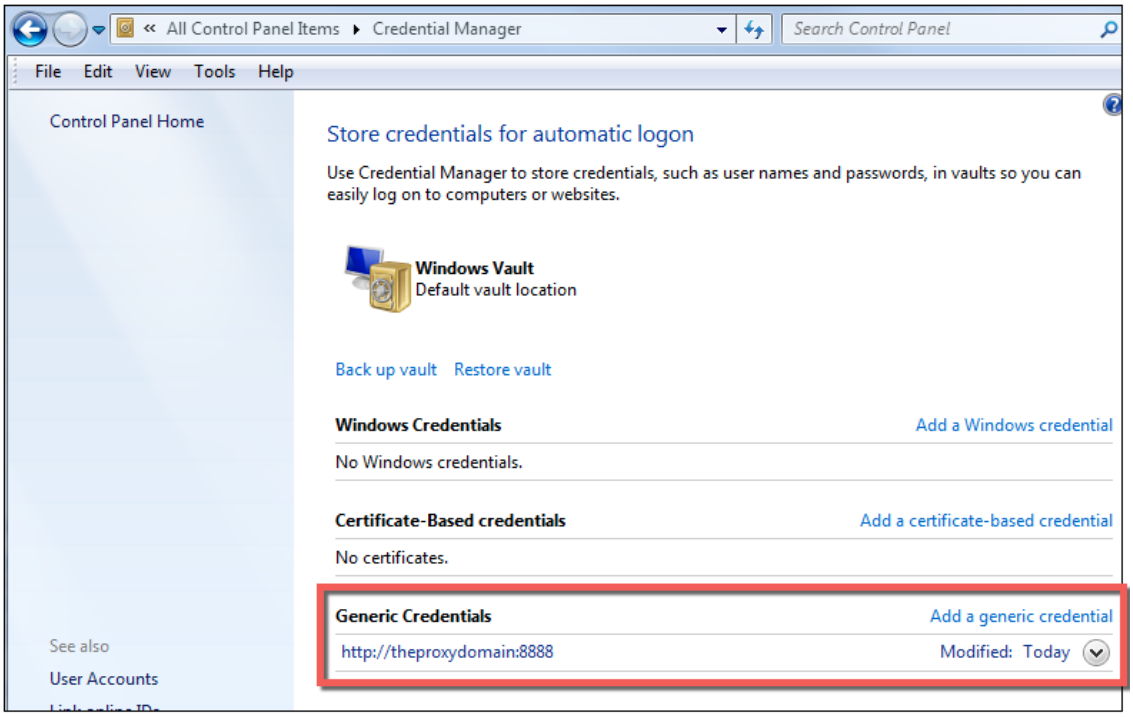
If the service account is not authorized to use the proxy server, then you can optionally create a new generic credential in the Credential Manager (found in the Windows Control Panel), by selecting **Add a generic credential**, as shown below:



On the next screen, you need to enter the URL of your proxy server and the user name and password required for the proxy, as shown below:



When you click **OK**, the following window is displayed, showing the new generic credential.



Note: Authenticated proxy servers are supported by using NTLM authentication. Basic authentication is not supported with proxy servers.

Configuring RSA Live Behind a Proxy

RSA Live feeds are pulled by the ConsoleServer, which you will need to configure like the example shown above. However, the activity of configuring the Live credentials and other fields occurs in the ApiServer. This means that any configuration changes you made to the ConsoleServer.exe.config file will also have to be made in the ApiServer.exe.config file.

Using the ConsoleServerSync Tool Behind a Proxy

If Phase 2 of the ConsoleServerSync process occurs in an environment that is behind a proxy, the associated ConsoleServerSync.exe.config file will have to contain the same modifications made to the ConsoleServer.exe.config file.

Modify Current Installation

If you wish to modify your current NetWitness Endpoint installation, you can run the NetWitness Endpoint installer in maintenance mode. The maintenance mode is only active when NetWitness Endpoint is already installed and the installer for the same version is launched. The maintenance mode only accommodates adding or removing components.

To modify your current NetWitness Endpoint installation, do the following:

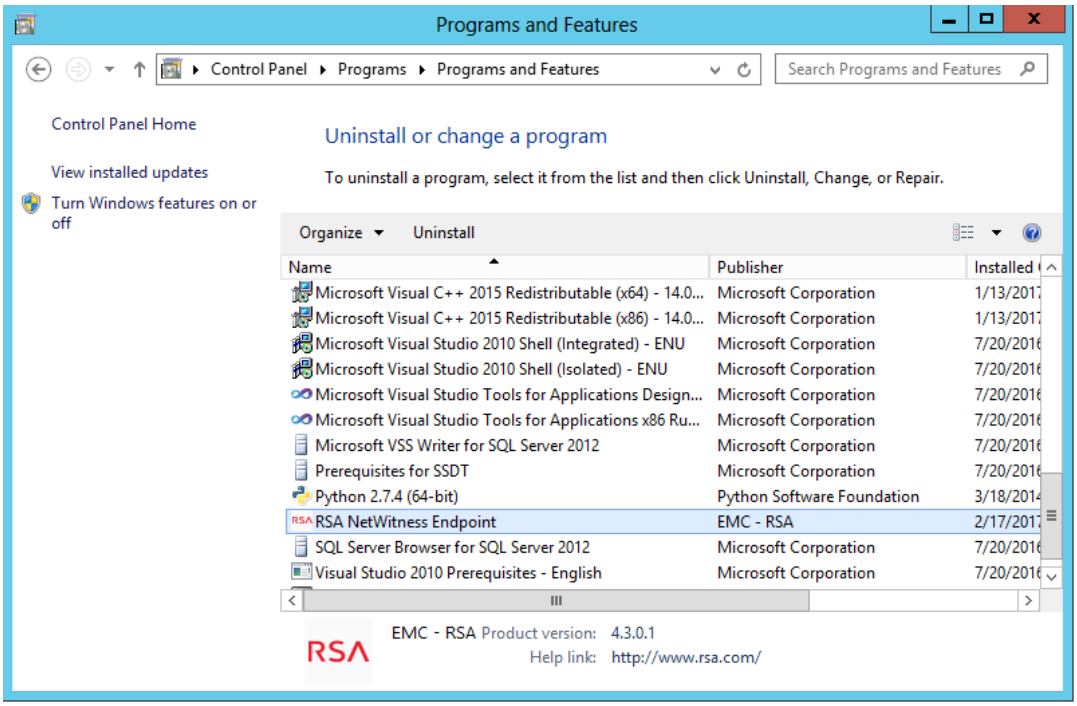
1. Stop all NetWitness Endpoint applications.
2. Find and double-click the installer executable file for your current NetWitness Endpoint installation (this is the same file you used to install the Primary ConsoleServer). The RSA ECAT installer Welcome dialog for maintenance mode is displayed.
3. Click **Next**.
4. The installer gathers information about the previous installation and displays previously specified configuration options rather than the default options as it follows the same procedure as a full installation.
5. When the Select Components dialog is displayed, the component options will reflect the previous installation.
6. You can change your installation configuration as follows:
   - To remove a currently installed component, uncheck the checkbox next to it in the Select Components dialog.
   - To install a component not previously installed, check the checkbox next to it in the Select Components dialog.
7. Click **Next** and continue through the remaining installer dialogs (same as for a full installation).
8. Click **Install** on the Ready to Install dialog to complete the installation modification process.

Uninstall NetWitness Endpoint

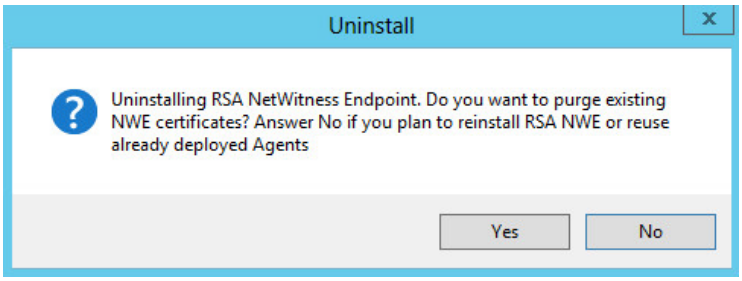
To uninstall the NetWitness Endpoint Primary ConsoleServer:

Note: NetWitness Endpoint agents are uninstalled through the NetWitness Endpoint UI. For information, see the topic *Uninstall Agents and Remove Agents from the Database* in the RSA NetWitness Endpoint User Guide.

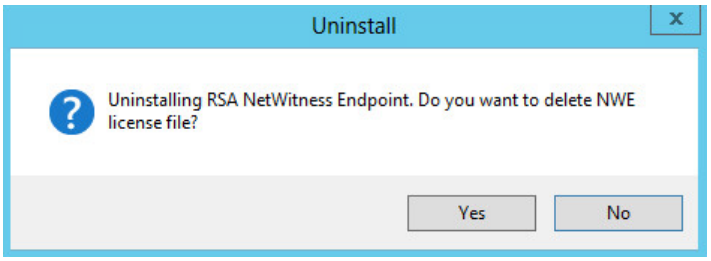
1. On the machine hosting the NetWitness Endpoint Primary ConsoleServer, open the **Control Panel** and go to **Programs and Features**, as shown below:



2. In the list of programs, right-click **RSA ECAT** and select **Uninstall**.
   The following message is displayed:

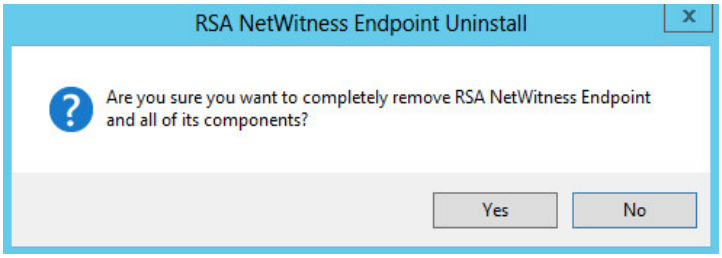


3. If you plan to reinstall NetWitness Endpoint or reuse already deployed agents, you should click **No**. If you click **Yes**, the existing NetWitness Endpoint certificates will be purged. In either case, the following message is displayed:

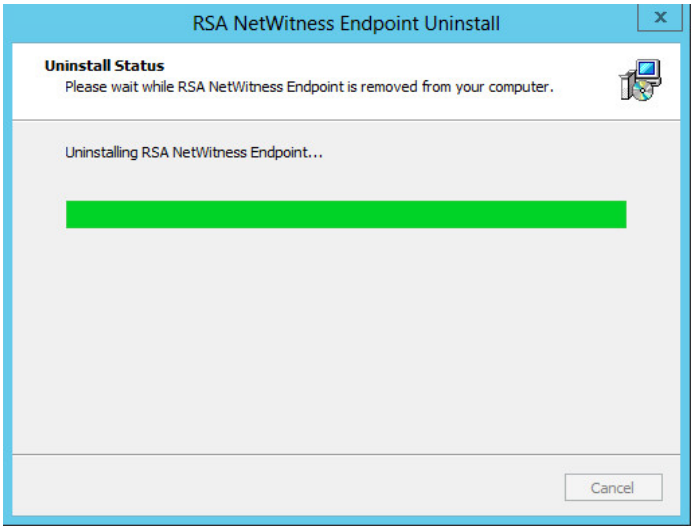


4. If you plan to reinstall NetWitness Endpoint, you should click **No**. If you click **Yes**, the NetWitness Endpoint license file will be deleted. In either case, the following message is

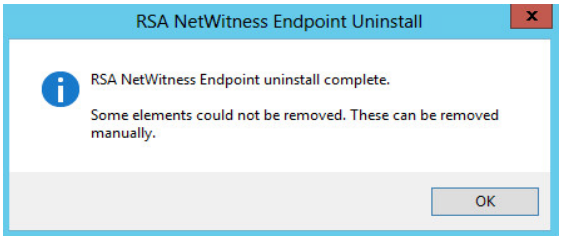
displayed:



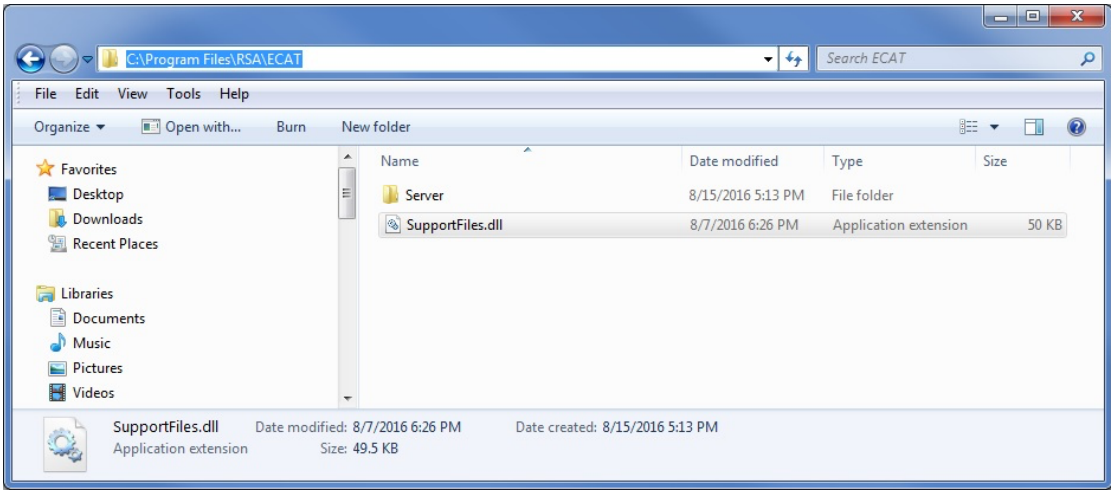
5. If you click **No**, the uninstall process stops and nothing will have been deleted, purged, or uninstalled. If you want to go ahead and uninstall NetWitness Endpoint, click **Yes**. The Uninstall Status dialog is displayed, as shown below:



6. Once NetWitness Endpoint is completely uninstalled, the following message is displayed:



7. There is a **SupportFiles.dll** file that is not deleted, but which can be deleted manually, as shown below:



Note: In all cases, the existing NetWitness Endpoint SQL database remains.

REFERENCES

The following topics provide reference information that pertains to installing and configuring NetWitness Endpoint.

Network Distributed Installation Considerations

There are a number of different possible configurations for the setup of the system over a set of server machines.

Each of these components could be independently deployed on a different machine:

- Microsoft SQL Server
- NetWitness Endpoint ConsoleServer
- NetWitness Endpoint UI
- OPSWAT Metascan

Ideally, the SQL Server and NetWitness Endpoint ConsoleServer should reside on the same machine to speed up the data insertion once the scans are received from the clients. If they are installed on different machines, a good gigabit LAN connection is recommended.

User Login Considerations

The NetWitness Endpoint ConsoleServer uses the Microsoft SQL Windows Authentication system to verify that the right users are granted access to the information.

Any NetWitness Endpoint UI user must have a valid login on the machine where the NetWitness Endpoint ConsoleServer is installed.

Therefore, administrators who need permission to operate NetWitness Endpoint should be allowed to manage the SQL Server database, and must have the required SQL Server access rights on the database.

It is preferable that all users of the NetWitness Endpoint UI, NetWitness Endpoint ConsoleServer, and the SQL Server belong to the same Active Directory domain. This will facilitate the login setup. For security reasons, it is recommended to use a different SQL instance for NetWitness Endpoint databases.

Note: If the network administrators do not belong to a domain, all the accounts in the different computers of the NetWitness Endpoint UI, NetWitness Endpoint ConsoleServer, and the SQL server must have exactly the same username and password.

Note: Permission issues are particularly important when the SQL database and the NetWitness Endpoint ConsoleServer are on separate servers and the QueuedData directory is hosted on the ConsoleServer. If this is the case, you must enable delegation on the SQL Server service account. If you fail to enable delegation under these conditions, the following error is logged to the **ConsoleServer-Error.log** file: "System.ComponentModel.WarningException: LIVE Kernel Download failed." When this occurs, any updated kernel definitions present in the **KernelData.csv** file are not added to the database. For more information, refer to Knowledge Base article 000034586, available on RSA Link.

To add a user to the Microsoft SQL Server, see Add a User to the Microsoft SQL Server.

Firewall Considerations

All NetWitness Endpoint executables must be allowed through the firewall to work.

When the option is checked, the Installshield should create firewall exceptions automatically.

Most firewalls will display a prompt when the NetWitness Endpoint ConsoleServer or the NetWitness Endpoint UI is started for the first time requesting authorization to receive a remote connection. This permission must always be granted. Under some circumstances, the Microsoft SQL Server might not be granted this permission and the firewall rules should then be added manually.

Required Firewall Permissions

- Microsoft SQL Server:
  - The program **sqlservr.exe**, usually located in:
    C:\Program Files\Microsoft SQL Server
    MSSQL10.MSSQLSERVER\MSSQL\Bin\sqlservr.exe
  - The program **sqlbrowser.exe**, usually located in:
    C:\Program Files\Microsoft SQL Server\90\Shared\sqlbrowser.exe
  - The default SQL Server connection port: 1433.

- NetWitness Endpoint UI
  - The program **ConsoleUI.exe**, usually located in:
    UI_INSTALLATION_FOLDER**ECATUI.exe**
- NetWitness Endpoint ConsoleServer:
  - The program **ConsoleServer.exe**, usually located in:
    MAIN_ECAT_FOLDER**Server\ConsoleServer.exe**
  - The default SSL connection port: 443.
  - The default UI connection port: 808.
    (Both ports can be set to a different value on NetWitness Endpoint Configuration.)
- OPSWAT MetascanServer:

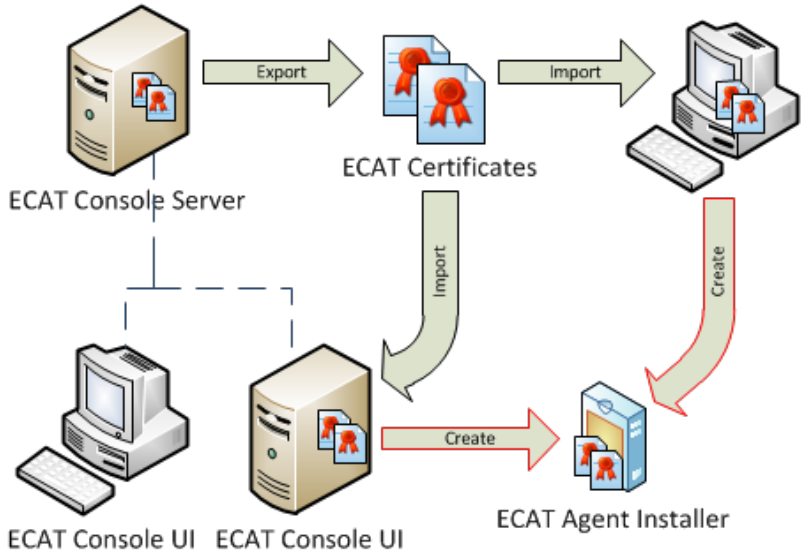
  Note: If installed on a different server, OPSWAT Metascan needs its connection port to be opened.

  The default OPSWAT Metascan Server connection port: 8008.

Agent Installers from Machines Other than the NetWitness Endpoint Server

When working with multiple server machines, the NetWitness Endpoint UI can be run from a different machine than the one on which the NetWitness Endpoint ConsoleServer was installed.

To be able to generate agent installers with the NetWitness Endpoint packager on a different machine, the certificates must be exported and then imported. The certificates must first be exported from the machine where they were originally created, most likely the NetWitness Endpoint ConsoleServer machine. They should then be imported into the machine where the agents are going to be generated with the NetWitness Endpoint packager.



Note: Although it is possible to export certificates to different machines to generate agent installers, caution must be taken to ensure the security of those certificates. They are used to encrypt the communication to and from the agents.

The certificates are only needed for the NetWitness Endpoint ConsoleServer and the NetWitness Endpoint Packager. To run the NetWitness Endpoint UI, no certificates are required.

Scan Data Folder

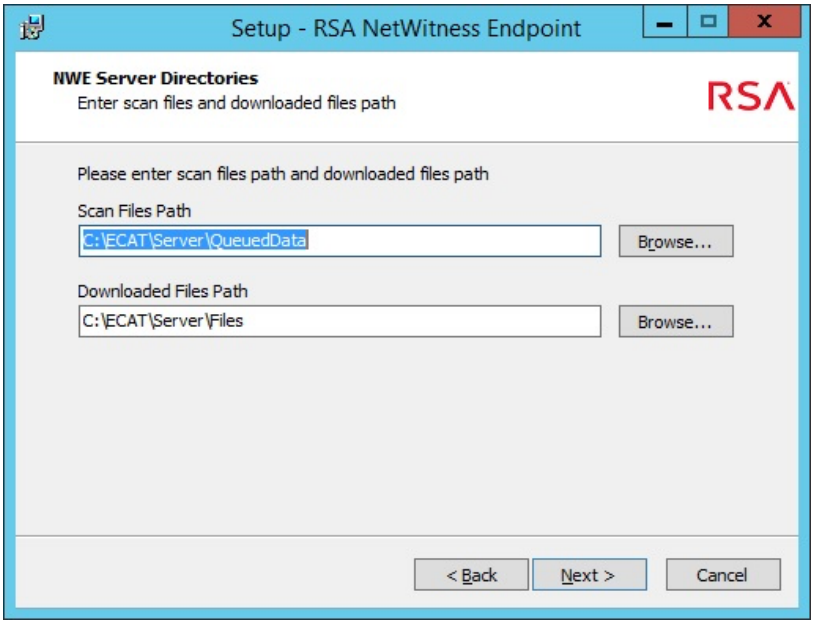
The scan files received by the NetWitness Endpoint ConsoleServer must finally be consumed by the SQL database. For some reason, if the connection between the server and the database is not established, the scan files accumulate in the **QueuedData** folder of the ConsoleServer machine. Hence it is recommended to host the Scan Data folder on the database machine.

There are two scenarios that are explained below:

- Scenario 1: ConsoleServer and database on same machine
- Scenario 2: ConsoleServer and database on different machines

Scenario 1: ConsoleServer and Database on Same Machine

While installing the NetWitness Endpoint ConsoleServer, the default value for the Scan Data folder is:
`C:\ECAT\server\QueuedData`



The files are placed in the **QueuedData** folder of the ConsoleServer, to be consumed by the database later. If required, the scan files can also be placed on a different drive on the ConsoleServer machine.

Conclusion: This set up works fine without any issues.

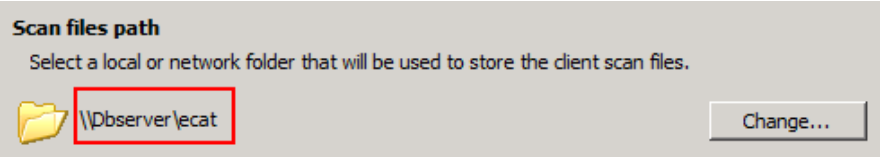
Scenario 2: ConsoleServer and Database on Different Machines

This scenario can work in two different methods as explained below.

Note: Regardless of which method you choose, the SQL Instance User and SQL Agent User need read/write/modify permissions and Active Directory delegation to the QueuedData folder.

Method 1: The Scan Data files are written on the database server (DbServer)

For this setup, you must specify the Scan Data folder in the installer as:
`\\DbServer\QueuedData`



This requires a shared folder on the Dbserver.

Conclusion: This method is recommended when the database is on a remote machine.

Method 2: The Scan Data files are written to the ConsoleServer (EcatServer) and retrieved by the database server (DbServer)

For this setup, you must specify the Scan Data folder in the installer as:
`\\EcatServer\QueuedData`

This set up requires the SQL Server user to have enough permissions to access the ConsoleServer and allow delegation in Active Directory.

Note: The database user has limited permissions, and reading on a remote machine is blocked by default.

Conclusion: This method does not work just by sharing a folder on EcatServer as it also requires sufficient user permissions.

Command Line Arguments for Installation Tasks

Export Certificates

You can export newly created certificates using the following commands:

```
c:\windows\System32\certutil.exe -privatekey -exportpfx -p "
{certificatePassword}" "NweCA" "' +
{InstallationPath}\Server\cert\NweCA.pfx

c:\windows\System32\certutil.exe -privatekey -exportpfx -p "
{certificatePassword}" "NweCA" "' +
{InstallationPath}\Server\cert\\NweAgentCertificate.pfx

c:\windows\System32\certutil.exe -privatekey -exportpfx -p "
{certificatePassword}" "NweCA" "' +
{InstallationPath}\Server\cert\\NweServerCertificate.pfx
```

Set SQL Authentication Password

You can set the password for SQL authentication for the NetWitness Endpoint server and the NetWitness Endpoint API server with already encrypted password using the following commands:

```
{InstallationPath}\server\ConsoleServer.exe /decryptandsetdbpswd
{sqlEncryptedPassword}

{InstallationPath}\server\APIServer.exe /decryptandsetdbpswd
{sqlEncryptedPassword}
```

The password is set encrypted for security reasons, but it can also be set with unencrypted password using the following commands:

```
{InstallationPath}\server\ConsoleServer.exe /setdbpswd
{sqlPassword}

{InstallationPath}\server\APIServer.exe /setdbpswd {sqlPassword}
```

Create or Delete Firewall Rules

You can create firewall rules for NetWitness Endpoint agents and NetWitness Endpoint server communication using the following commands:

```
C:\windows\System32\netsh.exe advfirewall firewall add rule
name="RSA ECAT Server TCP" dir=in localport={TCPPort} action=allow
protocol=TCP

C:\windows\System32\netsh.exe advfirewall firewall add rule
name="RSA ECAT Server UDP" dir=in localport={UDPPort} action=allow
protocol=UDP
```

And delete firewall rules using these commands:

```
C:\windows\System32\netsh.exe advfirewall firewall delete rule
name="RSA ECAT Server TCP" dir=in protocol=TCP

C:\windows\System32\netsh.exe advfirewall firewall delete rule
name="RSA ECAT Server UDP" dir=in protocol=UDP
```

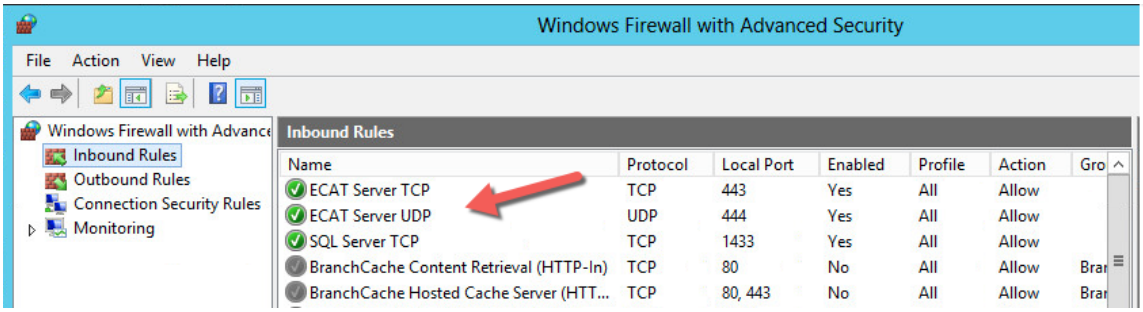
You can create the firewall rule for SQL Server using the following command:

```
C:\windows\System32\netsh.exe advfirewall firewall add rule
name="SQL Server TCP" dir=in localport={SQLPort} action=allow
protocol=TCP
```

And delete the firewall rule using this command:

```
C:\windows\System32\netsh.exe advfirewall firewall delete rule
name="SQL Server TCP" dir=in protocol=TCP
```

Once created, firewall rules should look like this:



Create, Start, Stop, and Delete Services

You can create services for NetWitness Endpoint server and NetWitness Endpoint API server using the following commands:

```
{InstallationPath}\server\ConsoleServer.exe /install /user
{WinServiceUsername} /password {winServicePassword}
```

```
{InstallationPath}\server\APIServer.exe /install /user
{WinServiceUsername} /password {winServicePassword}
```

And start the services using these commands:

```
c:\windows\System32\net.exe  Start RSAECATServer
```

```
c:\windows\System32\net.exe  Start RSAECATAPIServer
```

And stop the services using these commands:

```
c:\windows\System32\net.exe  Stop RSAECATServer
```

```
c:\windows\System32\net.exe  Stop RSAECATAPIServer
```

And delete the services using these commands:

```
c:\windows\System32\sc.exe delete RSAECATServer
```

```
c:\windows\System32\sc.exe delete RSAECATServer
```

or

```
{InstallationPath}\Server\ConsoleServer.exe /uninstall
```

```
{InstallationPath}\Server\APIServer.exe /uninstall
```

Installation Log File

If you have any issues with completing the NetWitness Endpoint installation process, the NetWitness Endpoint installer generates a log file that gets saved to the following location: **C:\Users\Administrator\AppData\Local\Temp**.
The default filename is:
Setup Log YYYY-MM-DD #SSS.txt

The log file records the following activities:

- All actions taken
- All information collected from the user
- All information collected by other means
- Return codes of all actions
- All error messages

List of Host and Service Ports

The supported host and service ports for NetWitness Endpoint are as follows:

From Host	To Host	To Ports (Protocol)	Comments
NetWitness Endpoint Server	NetWitness Endpoint SQL Server	1433 (TCP)	Standard SQL communication port (default value)
NetWitness Endpoint Agent	NetWitness Endpoint Server	443 (TCP), 444 (UDP)	Communication from the Agent to the NetWitness Endpoint Server (default values)
NetWitness Endpoint UI	NetWitness Endpoint SQL Server	1433 (TCP)	To view the data in the UI
NetWitness Endpoint UI	NetWitness Endpoint Server	9443 (TCP), 808 (TCP)	For configuring external components and other REST communications

From Host	To Host	To Ports (Protocol)	Comments
NetWitness Endpoint Server	RSA NetWitness Suite	5671 (TCP), 443 (TCP)	IM integration
RSA NetWitness Suite	NetWitness Endpoint Server	9443 (TCP)	Recurring feed integration
NetWitness Endpoint Server	Log Decoder	514 (TCP/UDP)	For syslog traffic to NetWitness Suite (If using a different syslog vendor, you need to check with the vendor as the TCP port may change.)
NetWitness Endpoint Server	Liveecat.rsa.com; cms.netwitness.com	443 (TCP)	Live integration
NetWitness Endpoint Server	www.microsoft.com	443, 80 (TCP)	Microsoft .NET 4.5 and SQLXML download during the application install
NetWitness Endpoint Server	File share	445, 137, 139	With read/write access rights
NetWitness Endpoint SQL Server	File share	445, 137, 139	With read/write access rights
NetWitness Endpoint UI	File share	445, 137, 139	With read/write access rights; (optional) without this analyst will not be able to inspect a module when running UI from their machine
NetWitness Endpoint Server	Queued Data folder	445, 137, 139	With read/write access rights

From Host	To Host	To Ports (Protocol)	Comments
NetWitness Endpoint SQL Server	Queued Data folder	445, 137, 139	With read/write access rights
NetWitness Endpoint Server	RAR (Remote Agents Relay)	5671 (RabbitMQ)	Bi-directional communication between NetWitness Endpoint Server and RAR Server
NetWitness Endpoint Agent	RAR (Remote Agents Relay)	443 (TCP), 444 (UDP)	Communication from the Agent to the RAR Server (default values)
NetWitness Endpoint UI, custom client app, or browser	NetWitness Endpoint Server	9443 (HTTPS)	REST API Interface port (default)

Note: Use port 9443 for the REST API interface (this is the default).