NetWitness Investigator 10.6
Release Notes

Introduction

This document lists what's new and changed in RSA® NetWitness Investigator 10.6. Read this document before deploying or upgrading RSA NetWitness Investigator.

Product Documentation

The following documentation is provided with this release.

NOTE: This user guide is based on RSA NetWitness Investigator version 9.8. Much of the content still applies for RSA NetWitness Investigator version 10.6. The sections of the guide that are affected by changes in this release are described in What's New.

Document	Location
Investigator User Guide	https://community.rsa.com/community/products/netwitness/investigator

NOTE: The online help in the NetWitness Investigator user interface is version 9.8.

What's New

The following features are new, or have changed, from version 10.5 to version 10.6:

- The product name is changed from RSA Security Analytics Investigator in version 10.5 to NetWitness Investigator. The product name has been changed in all major windows and dialogs.
- There are two ways to activate RSA NetWitness Investigator:
  - As an Enterprise customer, you only need to connect to your existing NetWitness (formerly Security Analytics) infrastructure. Once connected (to a Broker or Concentrator, for example), you are automatically activated and can create hundreds of collections of up to 1 TB of packets-per-collection.
  - As a Freeware customer, you have access to 25 local collections that you can use to import or capture up to 2 GBs of packets each.
- NetWitness Investigator 10.6 has support for all the new Lua parser capabilities in Security Analytics 10.6.
  - A few functional Lua parsers are included in the product as reference examples.
- A few fixed issues.

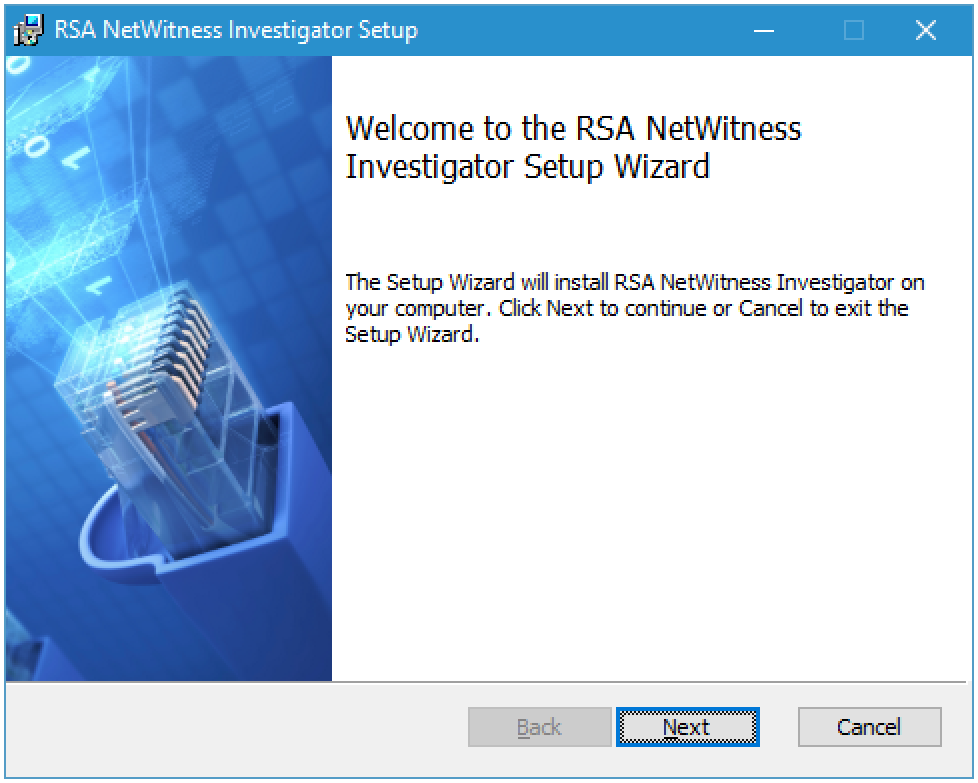
The following table describes the content in the Investigator User Guide that is affected by changes in NetWitness Investigator version 10.6.

Section	Description of Update
About This Guide	Information for contacting RSA Customer Support has changed. See the Contacting RSA Customer Support section of this document for the correct information.
Chapter 1: Overview	The Administrator thick client is no longer available.
	The Informer application is no longer available.
	System requirements have changed. There are no specific hardware requirements. The only supported software platform is Windows 64-bit.
	The installation procedure has changed. Installation steps are included in this document in Installation.
Chapter 2: Investigator Basics	Licensing keys and registration have been removed. Instead, all you are required to do is to activate Investigator (after installation) by connecting to a Security Analytics Core Service such as Decoder, Concentrator, Broker or Archiver. Once activated, all local collection capabilities are enabled.
	Some of the sections on menus, views, and other user interface elements have minor changes.
Chapter 3: Getting Started	Information in the following sections has changed: • Assembler Properties table in the Configure Investigator > Process section • Audio Codecs information in the Configure Investigator section • Advanced information in the Configure Investigator section
Chapter 6: Data Analysis	Information in the following sections has changed: • Navigation View > Navigation Toolbar > Index Calculation • Context Menus > Navigation Context Menu

Installation

The installation of NetWitness Investigator Enterprise must be performed on the Windows 64-bit platform. The necessary files are included in the installer package, which is available from https://community.rsa.com/community/products/netwitness/investigator.

1. Double-click on the installation file.
   The Investigator Setup Wizard opens.

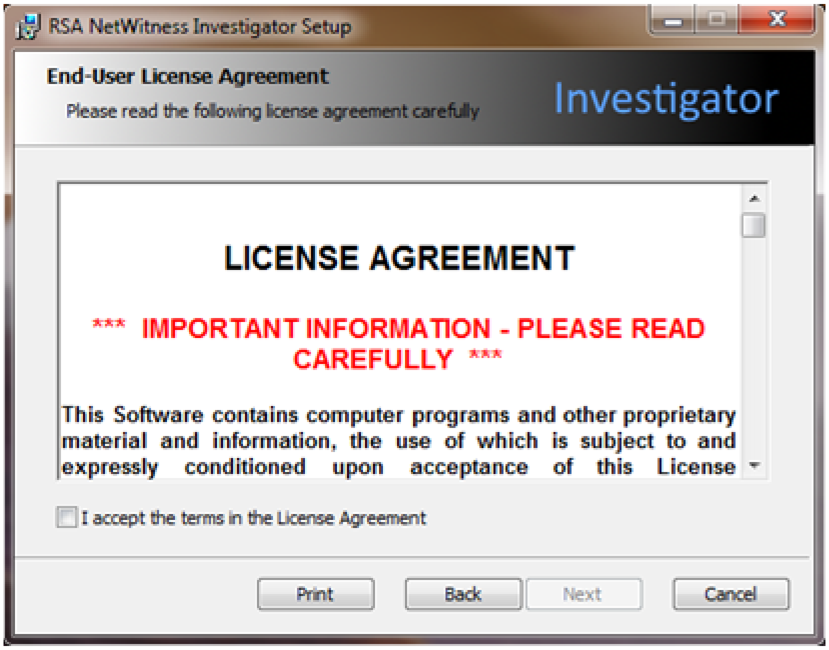


RSA NetWitness Investigator Setup

Welcome to the RSA NetWitness Investigator Setup Wizard

The Setup Wizard will install RSA NetWitness Investigator on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

2. Click **Next**.
   The **License Agreement** window opens.



End-User License Agreement

Please read the following license agreement carefully

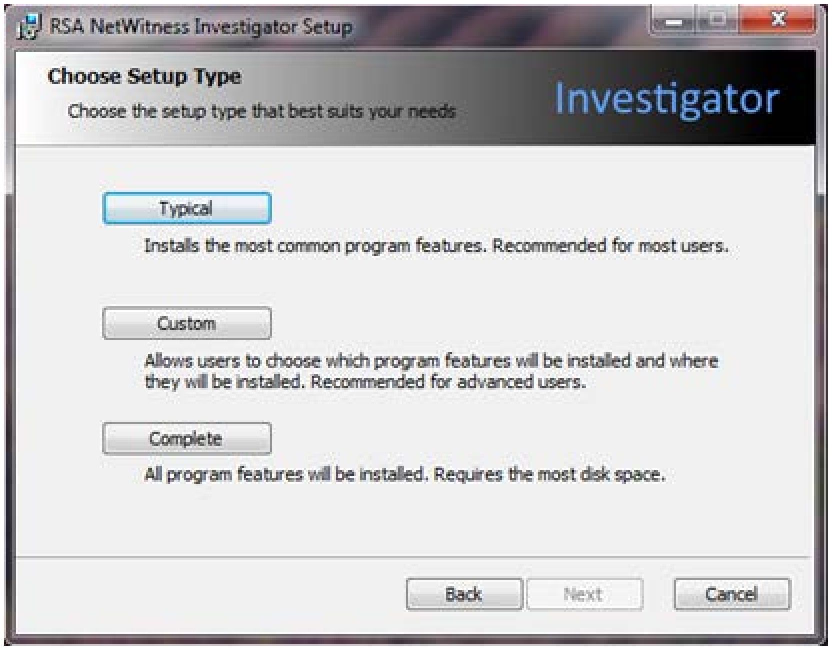
LICENSE AGREEMENT

*** IMPORTANT INFORMATION - PLEASE READ CAREFULLY ***

This Software contains computer programs and other proprietary material and information, the use of which is subject to and expressly conditioned upon acceptance of this License

□ I accept the terms in the License Agreement

3. Select the **I accept the terms in the License Agreement** check box, and then click **Next**.
   The Choose Setup Type window opens with the options **Typical**, **Custom**, and **Complete**.



Choose Setup Type

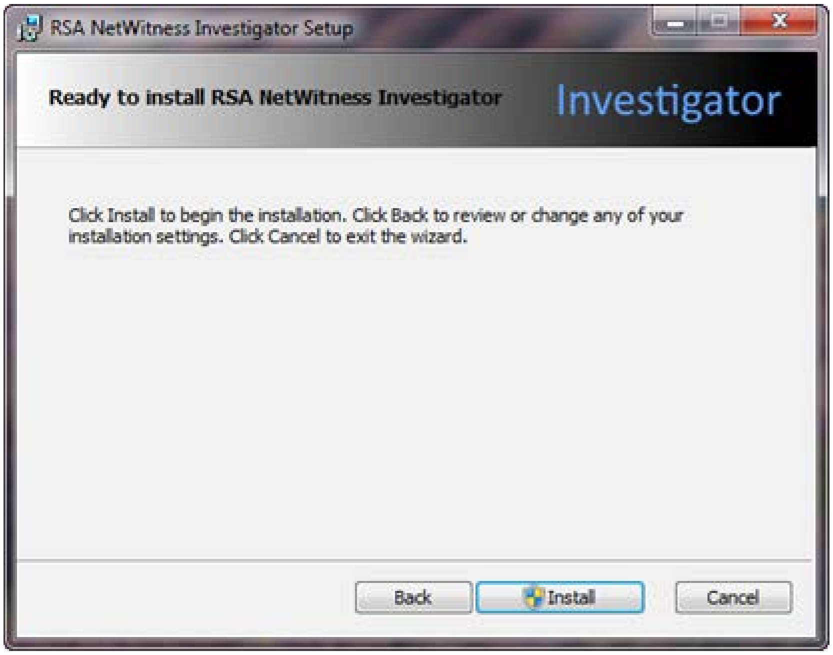
Choose the setup type that best suits your needs

Typical: Installs the most common program features. Recommended for most users.

Custom: Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.

Complete: All program features will be installed. Requires the most disk space.

4. Click the option that is most appropriate (in this document, **Typical** is used), and then click **Next**.
   The Ready to install RSA NetWitness Investigator window opens.

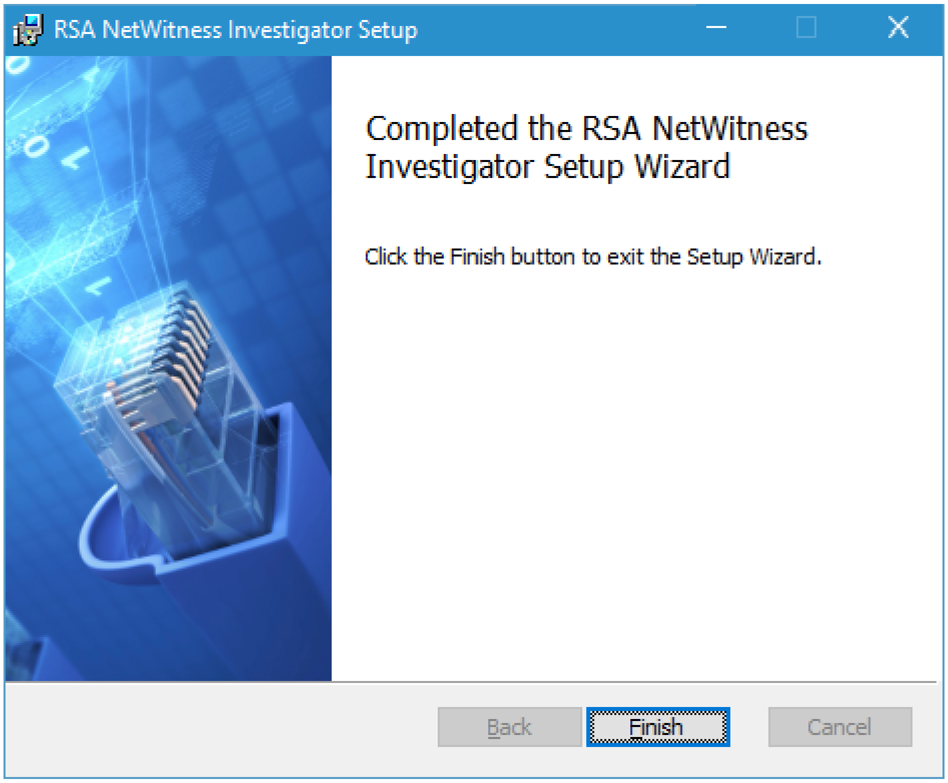


RSA NetWitness Investigator Setup
Ready to install RSA NetWitness Investigator
Investigator

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

5. Click Install.
   A window opens that shows the progress of the installation.

6. When the installation process completes, the Completed the RSA NetWitness Investigator Setup Wizard window opens.



Completed the RSA NetWitness Investigator Setup Wizard

Click the Finish button to exit the Setup Wizard.

Click **Finish** to complete the installation.

Uninstall Investigator

1. Close all programs.
2. From the Start menu, click Control Panel.
3. Double-click the Programs and Features icon.
4. Highlight NetWitness Investigator 10.6 from the list of installed applications, and then click Remove.
5. Follow the instructions.

Activate Investigator

There are two ways to activate NetWitness Investigator:

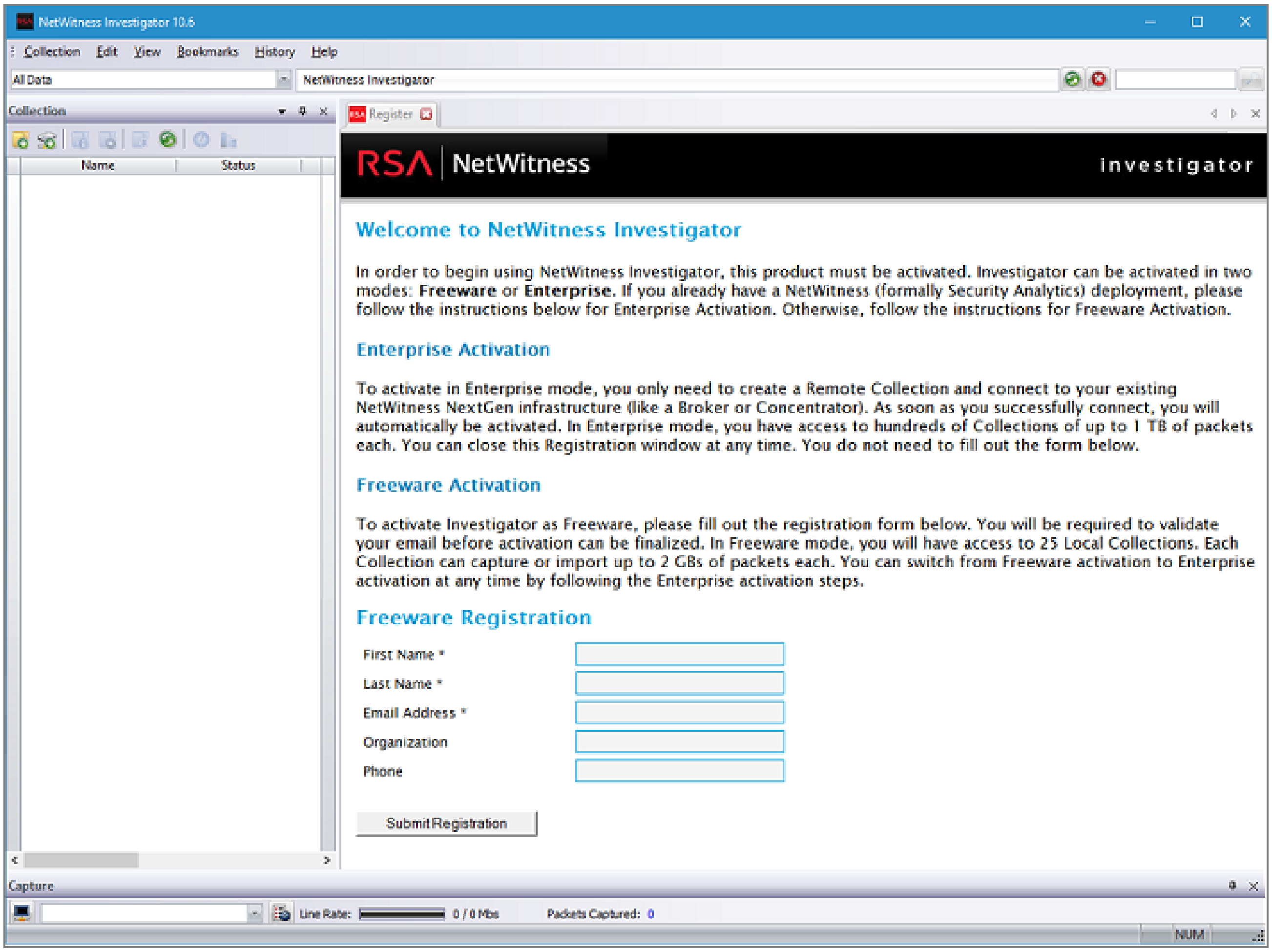
- If you already have RSA Security Analytics or NetWitness installed, you can use the Enterprise mode by connecting to your NetWitness (formerly Security Analytics) deployment.
- In Freeware mode, you have access to 25 local collections. Each local collection can be used to capture or import up to 2 GBs of packets.

Note: If you want to capture packets to and from your local desktop, you must download and install the WinPcap library. A link to this download page is provided on the Welcome page after you activate NetWitness Investigator.

Activate NetWitness Investigator Using Enterprise

1. From the Start menu, open NetWitness Investigator.

   The Welcome to NetWitness Investigator registration page is displayed.



Welcome to NetWitness Investigator

In order to begin using NetWitness Investigator, this product must be activated. Investigator can be activated in two modes: **Freeware** or **Enterprise.** If you already have a NetWitness (formally Security Analytics) deployment, please follow the instructions below for Enterprise Activation. Otherwise, follow the instructions for Freeware Activation.

Enterprise Activation

To activate in Enterprise mode, you only need to create a Remote Collection and connect to your existing NetWitness NextGen infrastructure (like a Broker or Concentrator). As soon as you successfully connect, you will automatically be activated. In Enterprise mode, you have access to hundreds of Collections of up to 1 TB of packets each. You can close this Registration window at any time. You do not need to fill out the form below.

Freeware Activation

To activate Investigator as Freeware, please fill out the registration form below. You will be required to validate your email before activation can be finalized. In Freeware mode, you will have access to 25 Local Collections. Each Collection can capture or import up to 2 GBs of packets each. You can switch from Freeware activation to Enterprise activation at any time by following the Enterprise activation steps.

Freeware Registration

First Name *

Last Name *

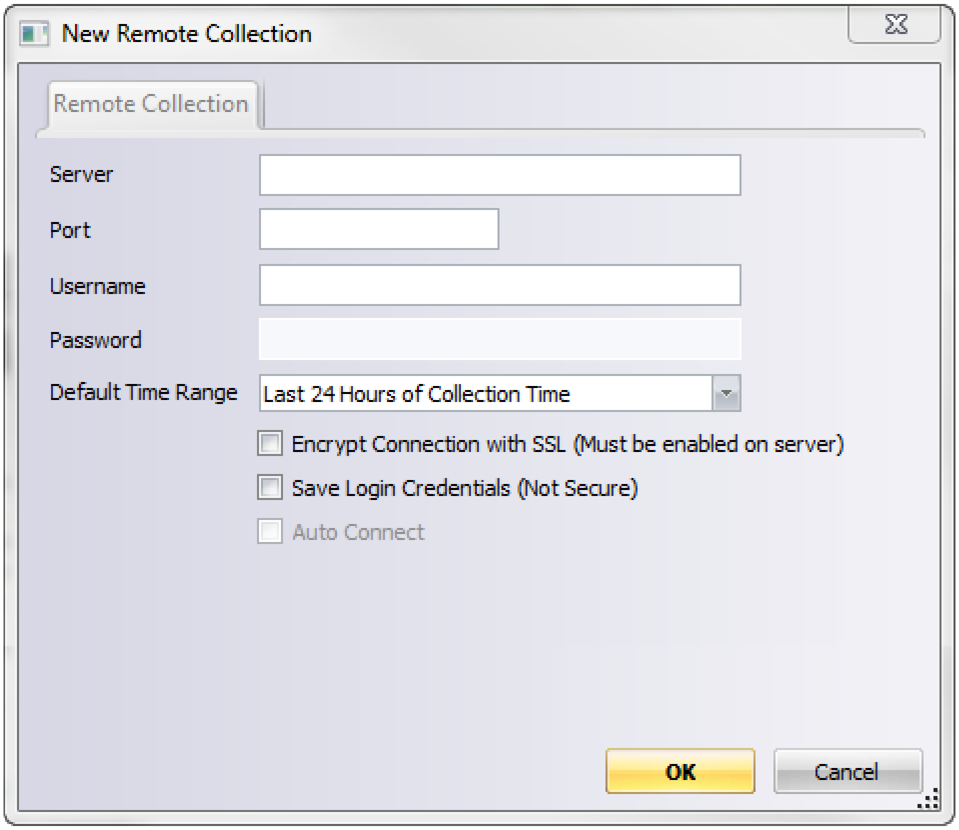
Email Address *

Organization

Phone

Submit Registration

2. In the menu bar, click **Connection** > **New Remote Collection**.
   The New Remote Collection dialog is displayed.



Server

Port

Username

Password

Default Time Range: Last 24 Hours of Collection Time

□ Encrypt Connection with SSL (Must be enabled on server)

□ Save Login Credentials (Not Secure)

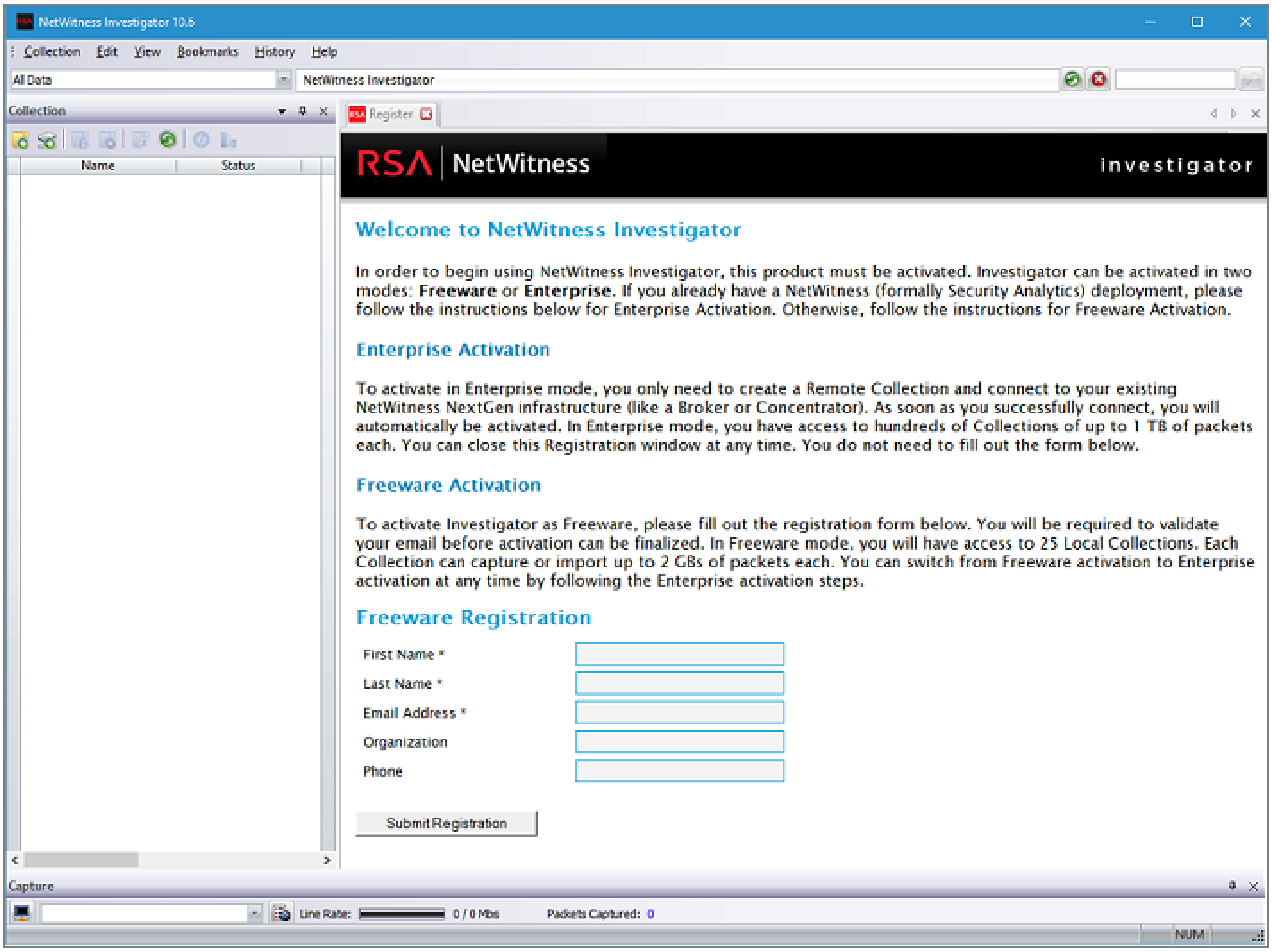
□ Auto Connect

3. Enter the server information for the Remote Collector system and click **OK**.
   The following message is displayed:
   ```
   Congratulations, you have successfully activated the product for
   Enterprise use. You have a full license for all local and remote
   collections.
   ```
   Click **OK**.
4. A message is displayed that asks if you would like to install a Demo Collection, which contains sample data that you can use to explore the features of Investigator. To install the Demo Collection, click **Yes**.

The NetWitness Investigator user interface is now activated and ready for use. You can use the sample data in the Demo Collection to learn more about NetWitness Investigator. For information that describes the user interface, see “Chapter 2: Investigator Basics” in the *Investigator User Guide*.

Activate NetWitness Investigator Freeware Version

1. From the Start menu, open NetWitness Investigator.
   The Welcome to NetWitness Investigator registration page is displayed.



Welcome to NetWitness Investigator

In order to begin using NetWitness Investigator, this product must be activated. Investigator can be activated in two modes: **Freeware** or **Enterprise.** If you already have a NetWitness (formally Security Analytics) deployment, please follow the instructions below for Enterprise Activation. Otherwise, follow the instructions for Freeware Activation.

Enterprise Activation

To activate in Enterprise mode, you only need to create a Remote Collection and connect to your existing NetWitness NextGen infrastructure (like a Broker or Concentrator). As soon as you successfully connect, you will automatically be activated. In Enterprise mode, you have access to hundreds of Collections of up to 1 TB of packets each. You can close this Registration window at any time. You do not need to fill out the form below.

Freeware Activation

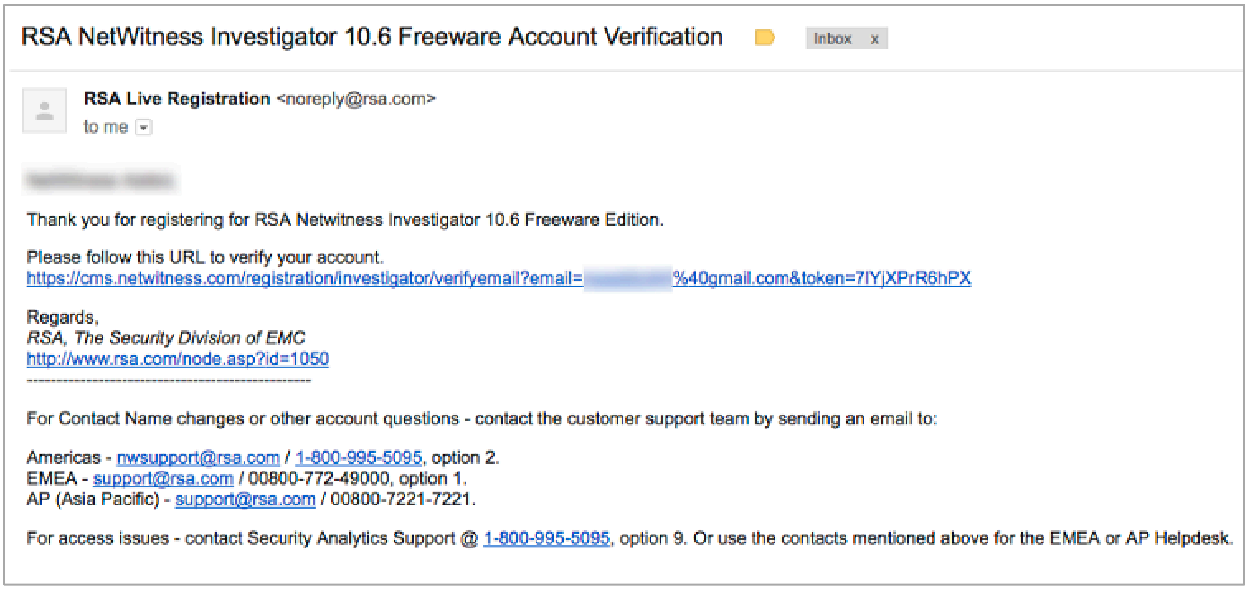
To activate Investigator as Freeware, please fill out the registration form below. You will be required to validate your email before activation can be finalized. In Freeware mode, you will have access to 25 Local Collections. Each Collection can capture or import up to 2 GBs of packets each. You can switch from Freeware activation to Enterprise activation at any time by following the Enterprise activation steps.

Freeware Registration

First Name *
Last Name *
Email Address *
Organization
Phone

2. In the **Freeware Registration** section, complete the information. The fields with the stars (*) are required. Click **Submit Registration**.

3. You receive an email from RSA Live Registration asking you to click on a URL to verify your account. Click on the URL.



RSA NetWitness Investigator 10.6 Freeware Account Verification

RSA Live Registration <noreply@rsa.com>
to me

[redacted]

Thank you for registering for RSA Netwitness Investigator 10.6 Freeware Edition.

Please follow this URL to verify your account.
https://cms.netwitness.com/registration/investigator/verifyemail?email=[redacted]%40gmail.com&token=7lYjXPrR6hPX

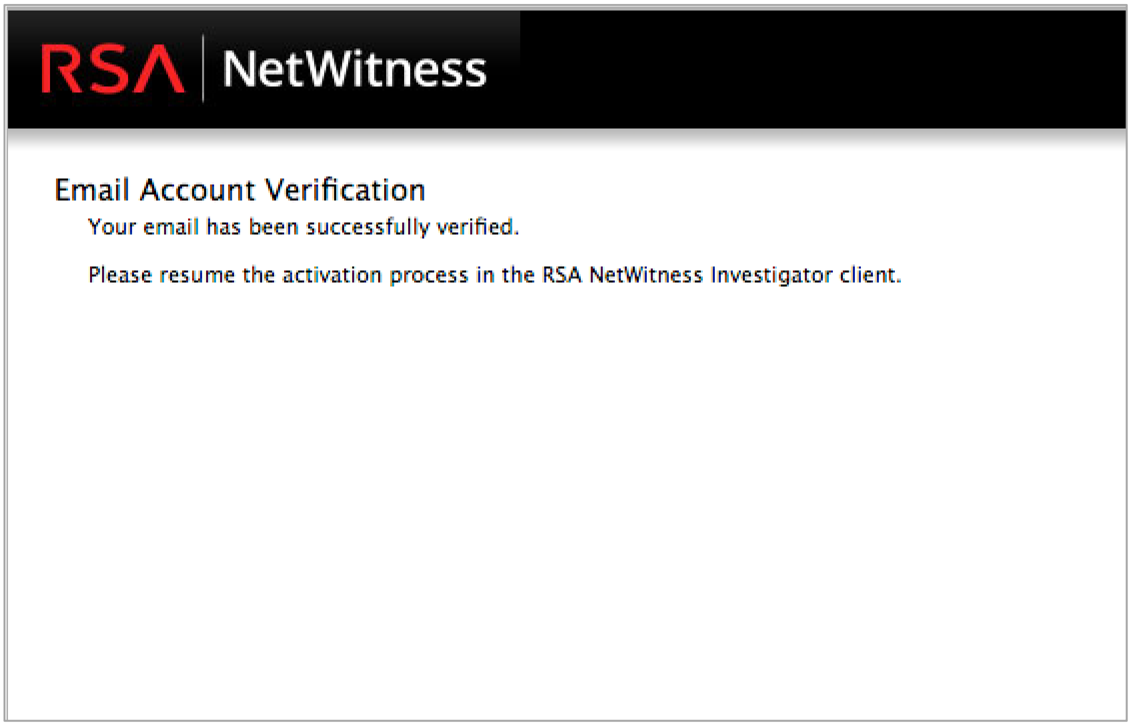
Regards,
RSA, The Security Division of EMC
http://www.rsa.com/node.asp?id=1050

For Contact Name changes or other account questions - contact the customer support team by sending an email to:

Americas - nwsupport@rsa.com / 1-800-995-5095, option 2.
EMEA - support@rsa.com / 00800-772-49000, option 1.
AP (Asia Pacific) - support@rsa.com / 00800-7221-7221.

For access issues - contact Security Analytics Support @ 1-800-995-5095, option 9. Or use the contacts mentioned above for the EMEA or AP Helpdesk.

4. After your email address is validated, you receive confirmation similar to the following:

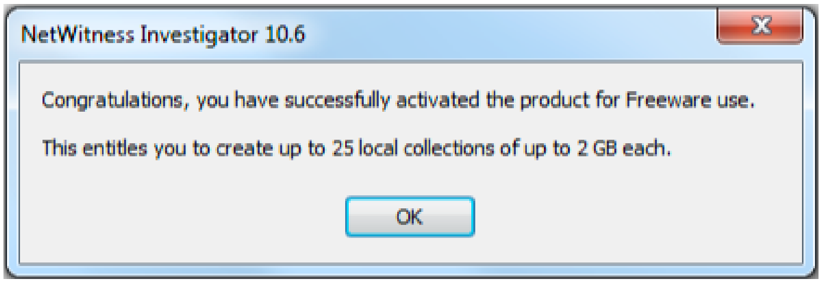


Email Account Verification

Your email has been successfully verified.

Please resume the activation process in the RSA NetWitness Investigator client.

5. In NetWitness Investigator, the Email Validation Required dialog is displayed. Click **Activate Freeware**. The following message is displayed:

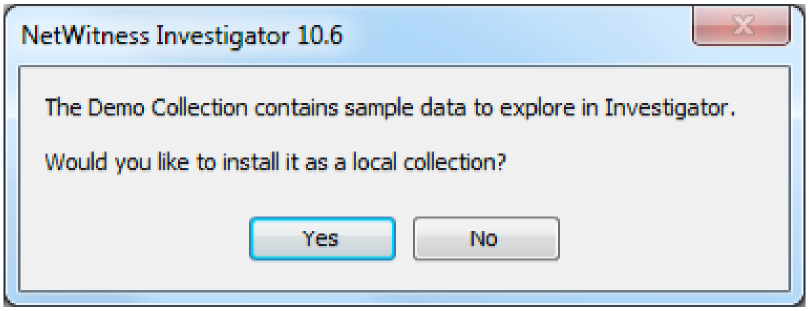


Congratulations, you have successfully activated the product for Freeware use.

This entitles you to create up to 25 local collections of up to 2 GB each.

Click **OK**.

6. A message is displayed that asks if you would like to install a Demo Collection, which contains sample data that you can use to explore the features of Investigator.



The Demo Collection contains sample data to explore in Investigator.

Would you like to install it as a local collection?

To install the Demo Collection, click **Yes**.

The NetWitness Investigator user interface is now activated and ready for use. You can use the sample data in the Demo Collection to learn more about NetWitness Investigator. For information that describes the user interface, see “Chapter 2: Investigator Basics” in the *Investigator User Guide*.

Contacting RSA Customer Support

Use the following contact information if you have any questions or need assistance.

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

Preparing to Contact RSA Customer Support

When you contact RSA Customer Support, you should be at your computer. Be prepared to give the following information:

- The version number of the RSA NetWitness or Security Analytics product or application you are using.
- The type of hardware you are using.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm.

License Agreement

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

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by EMC.

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 in the thirdpartylicenses.pdf file.

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

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license. EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.