RSA enVision
NIC SFTP Agent Configuration

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers: **www.rsa.com**

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.rsa.com/legal/trademarks_list.pdf**.

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.

Contents

RSA enVision NIC SFTP Agent Configuration **4**

NIC SFTP Agent Overview **5**

Run the Microsoft Visual C++ 2005 Redistributable Package **6**

Install the NIC SFTP Agent **7**

Set Up the NIC SFTP Agent **9**

Create the Public/Private Key Pair **11**

Import the Public Key to enVision **12**

Create a User Account or Use an Existing Account **13**

Cache the Key for Connection **14**

Appendix **15**

Troubleshooting the NIC SFTP Agent 16

Upgrading from NIC FTP Agent 18

NIC SFTP Agent Parameters 19

RSA enVision NIC SFTP Sample Files 23

RSA enVision NIC SFTP Agent Configuration

The NIC SFTP Agent is supported on Microsoft Windows 7, 2000, 2003, 2008, and XP operating systems.

Some event sources that use FTP have internal FTP agents and do not require the NIC SFTP Agent. See the individual event source configuration section to see whether the event source requires the NIC SFTP Agent.

The NIC SFTP Agent works with the NIC File Reader Service. After you have configured the event source and set up the NIC SFTP Agent, you must also set up the NIC File Reader Service and the FTP Server. For information on setting up the NIC File Reader Service and the FTP Server, see the enVision Help.

The NIC SFTP Agent sends the log file data to the system via Secure FTP. You can configure the NIC SFTP Agent to check a particular file as often as once every minute and as seldom as once every day. At each check, any new data written to the file since the last check is sent to the configured host using Secure FTP. Error and informational logs generated by the agent are sent to the configured logging host using UDP.

All configuration information is stored in the SFTP Agent Configuration file, **sftpagent.conf** on the individual event source.

NIC SFTP Agent Overview

The SFTP agent is a client server architecture, the RSA enVision platform being the server and the SFTP Agent—which is installed on the event source that sends logs to enVision—being the client. To configure the agent, you install the agent on the event source, configure the agent on the event source, generate keys on the client, and import the keys onto the RSA enVision platform.

To configure the NIC SFTP Agent:

1. Run the Microsoft Visual C++ 2005 Redistributable Package. See **Run the Visual C++ Package**.
2. Install the agent on the event source. See **Install the NIC SFTP Agent**.
3. Modify the sftpagent.conf file for the correct environment. See **Set Up the NIC SFTP Agent**.
4. Generate the key pair on the event source. See **Create and Configure the Public Key**.
5. Import Public.txt onto the enVision appliance. See **Import the Public Key**.
6. Create a user account (or use an existing account) under which to run the SFTP Agent Service. See **Create a User Account**.
7. Cache keys for the connection. See **Cache the Keys**.
8. Start the NIC SFTP Agent Service from the Windows Services Control panel.

If you have any problems, see the **Troubleshooting** section.

Run the Microsoft Visual C++ 2005 Redistributable Package

The Microsoft Visual C++ 2005 Redistributable Package (**vcredist_x86.exe**) installs runtime components of Visual C++ Libraries required to run applications developed with Visual C++. You must install these runtime components before you install the NIC SFTP Agent.

To run the Microsoft Visual C++ 2005 Redistributable Package:

1. Download either of the following packages:
   - Microsoft Visual C++ 2005 Redistributable Package (x86): **http://www.microsoft.com/downloads/details.aspx?familyid=32bc1bee-a3f9-4c13-9c99-220b62a191ee&displaylang=en**
   - Microsoft Visual C++ 2005 SP1 Redistributable Package (x86): **http://www.microsoft.com/downloads/details.aspx?familyid=200B2FD9-AE1A-4A14-984D-389C36F85647&displaylang=en**
2. Click **Download**, and run **vcredist_x86.exe**.

   The following table lists available packages and versions of Windows Server (acceptable combinations are specified with **Yes** in the corresponding cell).

Visual C++ Redis-tributable Package	Windows Server 2008 x86	Windows Server 2008 64-bit
2008 x86	No	No
2008 x64	N/A	No
2008 sp1 x86	No	No
2008 sp1 x64	N/A	No
2005 x86	Yes	Yes
2005 x64	N/A	No
2005 sp1 x86	Yes	Yes
2005 sp1 x64	N/A	No

Install the NIC SFTP Agent

Important: Install the NIC SFTP Agent on the machine that is sending logs to RSA enVision.

To install the NIC SFTP Agent:

1. Log on to RSA SecurCare Online.
2. Under **Browse by Product Family**, click **RSA enVision**.
3. In the **See Also** section, click **enVision Secure FTP Agent**.
4. In the **Latest RSA enVision Downloads** section, click **RSA enVision *<latest version>* Secure FTP Agent Updates**.
5. Click **Secure FTP Agent**, and follow the on-screen instructions to install the NIC SFTP Agent onto your event source with the following choices:

   Note: Users can install NIC SFTP Agent silently using command line parameters, see **Silent Installation Mode** below for instructions.

   Configuration File Selection Prompt:

   a. Select **No** when asked if you would like to create a configuration file for the NIC SFTP Agent.

   b. Select the **template.ini** file to read and display configuration data in the **Configuration Section Selection**.

   c. Select the section from **Section(s) Available** column and press **Add Section** button to add in configuration file. Click **Next** when finished.

   Generate Keys:

   a. If you would like the installer to create public and private keys, select **Yes**. A public key file will be generated and private keys will be created in the cache. Select **No** if you would like to manually generate keys for the NIC SFTP Agent.

   b. Follow prompts to begin installation.

   View / Edit Configuration File:

   a. If you like to view the configuration file and make changes, select **Yes** to open the sftpagent.conf file.

   Install Complete:

   a. At the end of the installation you will see the option to view the public key file. This is selected by default.

   b. Press the **Finish** button to display the public key file . Close this file to end the installation.

Silent Installation Mode:

The NIC SFTP Agent can be installed silently using command line parameters. This option may be useful for customers installing the NIC SFTP Agent on multiple machines using their own method to deploy the installation file and execute it.

Silent installation supports following command line parameters:

a. **Silent** – Run installer in silent mode.

b. **Template="ini file"** – SFTP Agent configurations template ini file with path name.

c. **generateKey** – To generate the public and private key.

d. **createConfigFile sections="section names"** – To create sftpagent.conf file using mentioned section names from template file. Section names are comma separated.

Set Up the NIC SFTP Agent

Important: : If you are upgrading from the NIC FTP Agent to the NIC SFTP Agent, you may skip this task.

RSA provides a sample configuration file for each of the event sources that requires the NIC SFTP Agent. You must rename that file to **sftpagent.conf** and edit the settings for the event source. For more information, see **RSA enVision NIC SFTP Sample Files**.

To set up the NIC SFTP Agent:

1. Remove the name of your event source from the name of the NIC SFTP Agent configuration file that you downloaded. For example, if you downloaded **sftpagent.conf.apachetomcat**, rename the file as **sftpagent.conf**.
2. Use a text editor to open the **sftpagent.conf** file.
3. You must change the following parameters from their default settings:

Note: Configure either the file, or the directory specifications. You cannot configure both.

Setting	Description
agent.logginghost	agent.logginghost=*enVision_IP* Change *enVision_IP* to the IP address of the RSA enVision server to where the event source is sending log file information.
file0	**file0=C:*path_to_first_log_file***
file0.ftp	Modify the parameter to match the complete path name of a log file. You can set file1, file2, and so on, so that each log file is identified. Alternatively, if the log files are located in the same directory, you can set the dir0 parameter. **file0.ftp=*enVision_IP*,nic_sshd,publickey,*event_source_IPaddress*** The values are as follows: • *enVision_IP* is the IP address of the RSA enVision server • *event_source* is the folder name for the event source • *IPaddress* is the IP address for the event source See the details for **dir.ftp** for an example.
dir0	dir0.ftp=*enVision_IP*,nic_sshd,publickey,*event_source_IPaddress*
dir0.ftp	The values are as follows:

Setting	Description

	• *enVision_IP* is the IP address of the RSA enVision server
	• *event_source* is the folder name for the event source
	• *IPaddress* is the IP address for the event source
	For example, assume the following:
	• the event source we are configuring is a GlobalSCAPE EFT Server, and its IP Address is 1.1.1.1.
	• the logs for the GlobalSCAPE EFT Server are stored in C:\ProgramData\GlobalSCAPE\EFT Server\logs
	• the IP address of the RSA enVision appliance is 172.16.0.51
	The values for dir0 and dir0.ftp are as follows:
	`dir0=C:\ProgramData\GlobalSCAPE\EFT Server\Logs`
	`dir0.ftp=172.16.0.51,nic_ sshd,publickey,GLOBALSCAPE_EFT_SERVER_1.1.1.1`

4. Configure any of the other parameters based on your environment and the specific event source that is sending its logs to the enVision platform. For details of all the parameters, see **NIC SFTP Agent Parameters**.
5. Save the **sftpagent.conf** file.

Create the Public/Private Key Pair

You must create a key pair on the machine on which the NIC SFTP Agent is installed and configure the enVision SSH server to accept the key.

Note: You create the key pair on the event source that is sending information to the RSA enVision platform.

To generate the public/private key:

1. Double-click **puttygen.exe** in the **C:\nicsftpagent** directory. The PuTTY Key Generator starts.
2. Select **SSH2 RSA** as the type of key to generate.
3. Click **Generate**. Move the mouse in the PuTTY Key Generator window until the key is generated.
4. Click **Save private key** and follow these steps.
   a. Select **Yes** to not use a passphrase.
   b. Save the file as private.ppk in the C:\nicsftpagent directory.
5. To create the **public.txt** file, follow these steps:
   a. Select and copy the text in the **Public key for pasting into SSH** field.
   b. Use a file editor, such as Notepad, to create a new file.
   c. Paste the copied text into the new file.
   d. Save the file as **public.txt** in the **C:\nicsftpagent** directory.
   e. Close the editor.

Import the Public Key to enVision

After you generate the public/private key pair on your event source, you must import the public key onto the RSA enVision platform.

To import the new key to the enVision platform:

1. Copy the **public.txt** file that you created to the **\bin** directory.
2. From a command prompt, change to the ***installdir*\bin** directory, and type:

```
add_winsshd_key.bat public.txt
```

You should receive system feedback saying that the import was successful. If not, run the command again.

Next, you either use an existing account or create a new user account for the SFTP Agent Service.

Create a User Account or Use an Existing Account

After you import the public key to the RSA enVision platform, you must either use an existing user account or create a new user account on the event source to run the SFTP Agent Service.

To create a user account on the event source:

1. On the Windows **Start** menu, click **Programs** > **Administrator Tools** > **Active Directory users and computers**.
2. Click **Action** > **New** > **User** and create a new user under whom the service will run.

   Note: The user account should be a member of the local admin group. The account must also have access to the files that are sent to the enVision platform.

3. Modify the NIC SFTP Agent Service to use this user account.
   a. Right-click NIC SFTP Agent, and select Properties.
   b. Click the **Log On** tab.
   c. Select **This account**.
   d. Type the user name and password for the account that you are using to run the SFTP Agent Service.
   e. Click **OK**.
4. Log off from the event source, then log back on using this new user account.
5. The user account that runs these steps must be the same user that will run the service. To see your username, type the following command at a command prompt:

   ```
   echo %USERDOMAIN%/%USERNAME%
   ```

   The system displays your current user name. (Make note of your user name.)

Next, you must cache the keys for the connection.

Cache the Key for Connection

After you create the user account that runs the NIC SFTP Agent service, you must cache the keys to connect the event source to the RSA enVision platform.

To cache the keys on the event source:

1. Log on to the machine with the account to be used for the NIC SFTP Agent Service. (You must log on as the same user who installed the NIC SFTP Agent Service.)
2. Run the following command from the **C:\nicsftpagent** directory:

   ```
   psftp -i private.ppk -l nic_sshd -v enVision-IP-address
   ```

   - *private.ppk* is the file containing the private key
   - *enVision-IP-address* is the IP address of the enVision appliance

   The system displays a message that the server host key is not in the registry.
3. Type **Y**, and press ENTER to trust the host.
4. At the **psftp** prompt, type **quit**, and press ENTER.

The key is now cached in the registry of the event source.

Appendix

The appendix for the NIC SFTP Agent documentation contains the following sections:

Troubleshooting the NIC SFTP Agent

Upgrade to the NIC SFTP Agent

NIC SFTP Agent Parameters

NIC SFTP Sample Files

Troubleshooting the NIC SFTP Agent

To troubleshoot, you must first stop the service, and then run a command to view debugging messages.

To troubleshoot the NIC SFTP Agent:

1. Stop the NIC SFTP Agent Service from the Windows Services window.
2. Open a new command shell, and change directories to the **NIC SFTP Agent** installation directory.
3. Type:

```
nicsftpagent -v
```

4. Review the debug messages that are displayed.

The following sections describe some possible messages and how to fix the corresponding issues.

Error opening SFTP Agent Configuration file

If the file is not present, you get the following error:

```
Error opening file: sftpagent.conf
```

To resolve the issue, find or recreate the file and move it to the NIC SFTP Agent installation directory.

Private Key Issues

If there is a problem with the generation of the key files, you may receive a message similar to the following:

```
Reading private key file "private.ppk"
Unable to use this key file (unable to open file)
Unable to use key file "private.ppk" (unable to open file)
```

Or, you may receive a message like the following if there is a key issue:

```
Offered public key
Server refused our key
Server refused public key
nic_sshd@enVision_IP's password:
```

To resolve the issue, regenerate the key pairs and re-import the private key onto the RSA enVision platform.

To view, add, or remove public keys:

1. Log onto the RSA enVision Appliance.
2. Run **e:\nic*version-number**server-name*WinSSHD\sshdctrl.exe**.
3. Click **Settings** > **Edit Settings**.

4. Under **Access Control**, click **Windows accounts**.
5. Select the **nic_sshd** entry and click **Edit**.
6. Click **Public Keys**.

This displays all the keys that have been added to RSA enVision. If you need to delete a key, remove it from the list, restart the NIC SFTP Agent Service, and re-import the key.

Password Issue

If you need to reset your password, you receive a Usage Warning message, and the system requests a password such as the following:

```
nic_sshd@enVision_IP's password:
```

To reset your NIC_sshd password:

1. Log onto the RSA enVision Appliance.
2. Run **e:\nic*version-number**server-name*WinSSHD\sshdctrl.exe**.
3. Clear the password cache, and reset the nic_sshd account entry for the correct domain.
4. Edit the Domain order and change the Domain to the correct value.

Upgrading from NIC FTP Agent

If you are already using the NIC FTP Agent, you must upgrade to the Secure FTP agent (NIC SFTP Agent). Install the NIC SFTP Agent and follow the rest of the instructions for configuring the agent.

The NIC SFTP Agent installation overwrites the existing installation. The existing files are backed up and the **fptagent.conf** file is renamed **sftpagent.conf**. RSA enVision removes the NIC FTP Agent Service, and installs the NIC SFTP Agent Service as an automatic service.

After the upgrade, some of the ports that enVision uses are changed. The following table lists the updated port numbers.

Note: If you have a multiple appliance site with Enhanced Availability, all Cluster Appliances (CAs) must be able to support all LC roles. This means you must specify the same configuration information on each CA in the Enhanced Availability system.

Event Source	Port Details
Apache HTTP Server	• Microsoft Windows: TCP 22 • UNIX: TCP 21
Cisco Access Control Server	TCP 22
Microsoft Internet Information Services	TCP 22
Oracle	• Microsoft Windows: TCP 22 • UNIX: TCP 21
RSA Authentication Manager	TCP 22

NIC SFTP Agent Parameters

The following tables describe the SFTP Agent parameters that are available for configuration. The parameters are separated into agent, file, and directory categories.

Note: Configure either the file, or the directory specifications. You cannot configure both.

Agent Parameters

The following agent parameters are available.

Setting	Description
agent.logginghost	Hostname or IP address of the enVision appliance to which the logs will be sent. This is the address or hostname of your enVision appliance. For multiple appliance sites, this is the address or hostname of your D-SRV. **Important:** : You must change this value before running the SFTP Agent.
agent.logginglevel	Highest level of logging collected. The values are **0** (least verbose) to **7** (most verbose). The default value is **6**, which is the sftpagent logging level for internal debug messages.
agent.poscleaninterval	Time interval for deletion of the POS directory. The POS folder contains temporary files created by the SFTP Agent. If not configured, the agent does not purge the POS folder. The default value is 0, which means that you must manually clean up the POS folder. The syntax of the parameter is *n-u*, where n represents the number and u represents the unit. Use any of the following units: • **s**: seconds • **min**: minutes • **h**: hours • **d**: days • **w**: weeks • **y**: years. One year (1-y) is the maximum value. Setting the parameter higher than 1-y sets the cleanup interval to the maximum interval of one year. For example, to set the cleanup interval to every two minutes, use the following: agent.poscleaninterval=2-min
agent.retrysendfile	Number of times the agent attempts to resend the log file. For systems with a high data transfer rate and a large volume of messages, you may send the files multiple times. This helps ensure that enVision receives the data, even in cases where some file transmissions fail due to network congestion.

Setting	Description
	The default value is **3**. Acceptable values are **1** to **10**. To turn off the feature and to send files only once, set the value to **0**.

File Parameters

The following file parameters are available.

Setting	Description
file*N*	Name of the file to monitor. **Note:** : You do not need to enclose the path in double quotes. There is an issue that occurs on Windows 64-bit Operating System, such as Windows Server 2008, Windows 7, and Windows Vista. A 32-bit application cannot access any files in the **%windir%\System32** path because the OS redirects them to the **%windir%\SysWOW64** path. The workaround is to configure the NIC SFTP Agent to use the following file specification: `file0=c:\windows\sysnative\target.txt`
file*N*.interval	The amount of time (in seconds) to wait between file checks.
file*N*.compression	Data is compressed before sending when the value is **true**, and not when **false**.
file*N*.enabled	File is monitored when the value is **true**, and ignored when **false**.
file*N*.ftp	Defines FTP settings, including the host and directory where files in the monitored directory are to be sent and the credentials to be used. The syntax is as follows: ***server_IP*,*port*,nic_sshd,publickey,*directory*** where: • ***server_IP*** is the name or IP address of the enVision appliance. You must replace the text ***server_IP*** with the IP address of the enVision appliance (in a multiple appliance site use the IP address of the LC where the event source is configured). **Important:** You must change this value prior to running the SFTP Agent. • ***port*** sets the port to listen on. You do not need to set this parameter if you are using the default port. • **nic_sshd,publickey** sets the authentication to use the **nic_sshd** user (which is required) and to use public key authentication. For multiple appliance sites, place the public keys on the LC where the event source is being collected (the same as ***server_ip*** address). • ***directory*** is the directory on the remote appliance relative to the **enVision/ftp_files**

Setting	Description
	directory for this event source configuration. For example, if this IIS event source IP address is 11.22.33.444, the remote directory would be IIS_11.22.33.444. **Important:** You must change this value prior to running the SFTP Agent. **Note:** The directory settings for the file*N*.ftp key should match the settings from the NIC File Reader Service configuration.
file*N*.suffix (optional, depending on the event source type)	Suffix attached to the file names of some event sources, only if the event source type has a suffix. For example, Cisco Secure ACS files have a suffix.
file*N*.delete_after_read	Deletes the file after the data in the file has been successfully sent to RSA enVision via FTP when the value is **true**.
file*N*.has_header	Set to **false** if the log file does not have a header line at the top. Set to **true** for all other cases. If the value is **true**, the header is sent with every file. **Note:** This field is only available for RSA enVision 3.3.5 and later.

Directory Parameters

The following directory parameters are available.

Setting	Description
dir*N*	Parent directory of the directory to monitor. **Note:** You do not need to enclose the directory in double quotes.
dir*N*.dirspec	Directory to monitor. This value can contain wildcards, for example, **Logfiles** matches the Logfiles directory; **LogFiles*** matches directories such as LogFiles1, LogFiles2 and so on. **Note:** Wildcard and regular expression strings are case sensitive.
dir*N*.filespec	Defines what is monitored. Use * to monitor everything. **Note:** Wildcard and regular expression strings are case sensitive.
dir*N*.interval	The amount of time (in seconds) to wait between directory checks.
dir*N*	Data is compressed before sending when the value is **true**, and not when **false**.

Setting	Description
.compression	
dir*N*.enabled	Directory is monitored when the value is **true**, and ignored when **false**.
dir*N*.ftp	Defines FTP settings, including the host and directory where files in the monitored directory are to be sent and the credentials to be used. The syntax is as follows: ***server_IP*,*port*,nic_sshd,publickey,*directory*** • ***server_IP*** is the name or IP address of the enVision appliance. You must replace the text ***server_IP*** with the IP address of the enVision appliance (in a multiple appliance site use the IP address of the LC where the event source is configured). **Important:** You must change this value prior to running the SFTP Agent. • ***port*** sets the port to listen on. You do not need to set this parameter if you are using the default port. • **nic_sshd,publickey** sets the authentication to use the **nic_sshd** user (which is required) and to use public key authentication. For multiple appliance sites, place the public keys on the LC where the event source is being collected (the same as ***server_ip*** address). • ***directory*** is the directory on the remote appliance relative to the **enVision/ftp_files** directory for this event source configuration. For example, if this IIS event source IP address is 11.22.33.444, the remote directory would be IIS_11.22.33.444. **Important:** You must change this value prior to running the SFTP Agent. **Note:** The directory settings for the dir*N*.ftp key should match the settings from the NIC File Reader Service configuration. For example, in a multiple appliance site, if the LC is 11.22.33.444, and the IIS is 11.22.33.5, the line is: `dir0.ftp=11.22.33.444,nic_sshd,publickey,IIS_11.22.33.5`
dir*N*.has_ header	Set to **false** if the log file does not have a header line at the top of the file. Set to **true** in all other cases. If **true**, the header is sent with every file transfer. (this field is available for enVision release 3.3.5 and later).

RSA enVision NIC SFTP Sample Files

RSA provides sample NIC SFTP Agent configuration files. All configuration information is stored in the configuration files, **sftpagent.conf.*eventsourcename***, where *eventsourcename* is the name of your event source. The files are available in the following places:

- On the Device Configurations page of RSA SecurCare Online. The sample files are listed as additional downloads for the corresponding event source.
- On the enVision appliance. The sample files are located in the ***installdir*\etc*device-name*\sftp** folder.

  Where:

  - *installdir* is the installation directory. The RSA enVision installation directory is **E:\nic*version-number**server-name***.
  - *device-name* is the name of the event source.

  For example, the NIC SFTP sample file for Apache Tomcat could be located at the following folder:

  E:\nic\4000\SRV\etc\devices\apachetomcat\sftp\sftpagent.conf.apachetomcat.