



# DefendX Software Vision™

## Reports Pack

### Installation Guide

### Version 9.1

*This guide details the use of DefendX Software Vision™. Upon completion of the steps within this document, DefendX Software Vision will successfully report on your enterprise community.*



## Table of Contents

Executive Summary .....	3
Installation .....	4
In This Guide .....	4
DefendX Software Data Collection Agent Administration .....	5
DefendX Software Data Collection Agent Configuration .....	5
Configuring New Active Directory Server .....	6
Configuring DefendX Software Data Collection Agent for Windows .....	8
Configuring DefendX Software Data Collection Agent for NAS, NetApp .....	17
Configuring DefendX Software Data Collection Agent for NAS EMC .....	27
DefendX Software Data Collection Agent Database Configuration .....	36
Configuring DefendX Software Data Collection Agent for HNAS .....	37
Configuring DefendX Software Data Collection Agent for NAS, EMC Isilon .....	44
DefendX Software Data Collection Agent Schedule Configuration .....	50
Viewing DefendX Software Vision Agent Status Utility .....	52
Purging the DefendX Software Vision Database .....	54
Notification Settings .....	57
Mail Settings .....	59
About DefendX Software .....	60
DefendX Software Professional Services .....	60
Legal & Contact Information .....	61

## Executive Summary

Thank you for your interest in DefendX Software Vision™. DefendX Software Vision is a critical component of an overall file data management (FDM) architecture and is part of the DefendX Software integrated suite of products. Together, these products are designed to help organizations control and report on their current and ever-growing Windows® storage infrastructure.

DefendX Software Vision provides a complete view of storage consumption within enterprise organizations. Providing reports on users, files, directories, volumes, sites, mailbox folders, and servers across your entire organization, DefendX Software Vision is the premiere enterprise reporting application. By using the DefendX Software Vision drill-down filtering technology, administrators can focus on the most important and growing concerns within their enterprise environments.

DefendX Software Vision reports on enterprise storage resources; for example, some of the built-in reports display data related to the following:

- End-user storage consumption
- File type utilization
- Prediction and trend analysis

DefendX Software Vision is different from all other storage-reporting applications in several important ways. In particular, it has the lowest labor cost, which industry analysts agree represents 75% or more of total cost of ownership (TCO). To assist with lowering costs, DefendX Software provides and supports multiple installation methods for DefendX Software Vision, including Microsoft® SMS installations, MSI installations, and Active Directory group policy object installations. DefendX Software Vision supports virtually any installation method your organization customarily uses.

## Installation

For installation instructions, please refer to the following:

- *Installation Guide – DefendX Software Vision Analysis Server* for details about installing DefendX Software Vision™ Analysis Server.
- *Installation Guide – DefendX Software Data Collection Agent for Active Directory* for details about installing DefendX Software Data Collection Agent for Active Directory.
- *Installation Guide – DefendX Software Data Collection Agent for Windows* for details about installing DefendX Software Data Collection Agent Windows Version.
- *Installation Guide - DefendX Software Data Collection Agent for NAS, NetApp®* for details about installing DefendX Software Data Collection Agent for NAS, NetApp Edition.
- *Installation Guide - DefendX Software Data Collection Agent for NAS, EMC®* for details about installing DefendX Software Data Collection Agent for NAS, EMC Edition.
- *Installation Guide – DefendX Software Data Collection Agent for NAS, EMC® Isilon* for details about installing DefendX Software Data Collection Agent for NAS, EMC Isilon Edition.

This guide covers two main topics: configuring DefendX Software Data Collection Agent™ and configuring and managing DefendX Software Vision.

## In This Guide

The screenshots within the user manual do not necessarily reflect your environment. The screenshots here are meant to reflect all Data Collection Agents supported with DefendX Software Vision.

## DefendX Software Data Collection Agent Administration

DefendX Software Data Collection Agent™ is a critical component of an overall file data management (FDM) architecture and is part of the DefendX Software integrated suite of products. Together, these products are designed to help organizations control and report on their current and ever-growing storage infrastructure.

The DefendX Software Vision supports the following Data Collection Agents:

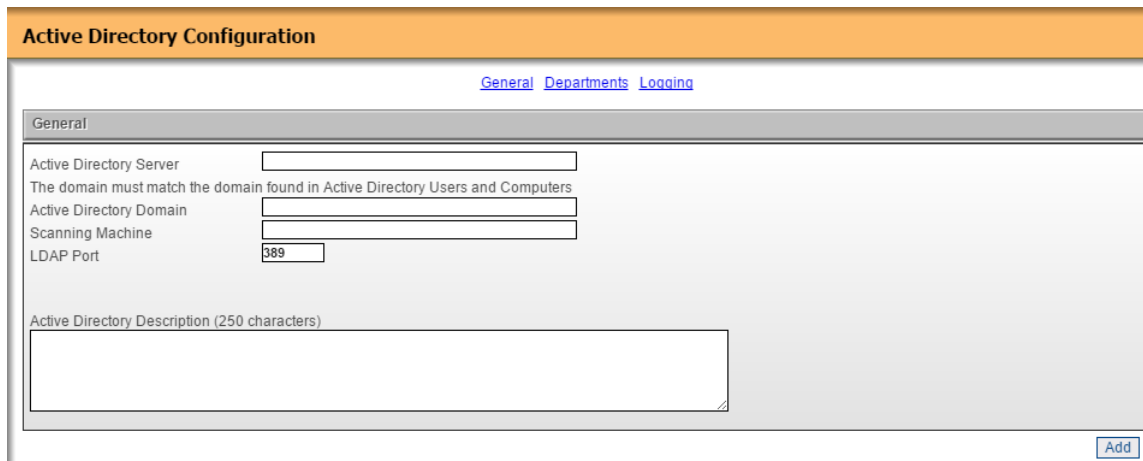
- DefendX Software Data Collection Agent for NAS, NetApp Edition
- DefendX Software Data Collection Agent for NAS, EMC Edition
- DefendX Software Data Collection Agent Windows Version
- DefendX Software Data Collection Agent for Active Directory Edition
- DefendX Software Data Collection Agent for NAS, EMC Isilon Edition

## DefendX Software Data Collection Agent Configuration

Depending on the platform adapted in your environment, you will have to configure one type of DefendX Software Data Collection Agent from the list above. Before using DefendX Software Data Collection Agent, the new configuration settings must be created for each storage unit (Filer®, VNX/Unity, etc.) that the agent will scan. Follow these steps to create a new configuration:

## Configuring New Active Directory Server

1. From the DefendX Software Vision™ Analysis Server machine, open the DefendX Software Data Collection Agent™ Administration by clicking **Start > All Programs > DefendX Storage Software Vision > DefendX Software Vision Data Agent Administration**.
2. In the left-hand main menu, click **New AD Configuration** to open the **Active Directory Configuration** window.

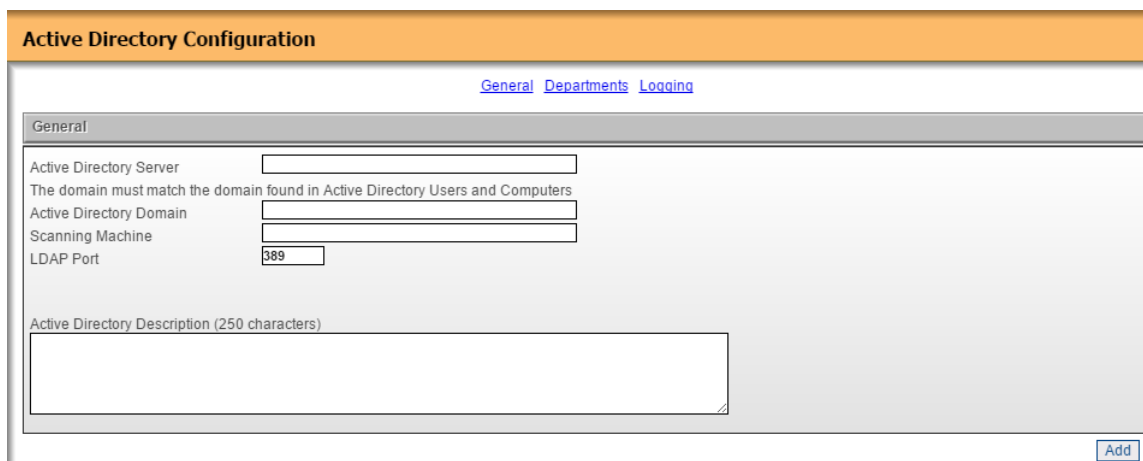


The screenshot shows the 'Active Directory Configuration' window with the 'General' tab selected. The window has a title bar with the text 'Active Directory Configuration'. Below the title bar are three tabs: 'General', 'Departments', and 'Logging'. The 'General' tab is active and contains the following fields:

- Active Directory Server**: A text input field.
- The domain must match the domain found in Active Directory Users and Computers**: A text input field.
- Active Directory Domain**: A text input field.
- Scanning Machine**: A text input field.
- LDAP Port**: A text input field with the value '389' entered.
- Active Directory Description (250 characters)**: A large text area.

An 'Add' button is located at the bottom right of the window.

3. In the **General** dialog box, enter the AD server, AD domain, scanning machine, LDAP port, and description (if desired) and then click the **Add** button.



This screenshot is identical to the one above, showing the 'Active Directory Configuration' window with the 'General' tab selected. It displays the same set of input fields for configuring an Active Directory server, including the 'Add' button at the bottom right.

4. From the **Home** page, under the **Active Directory Configurations** section, click the **AD server** name you want to update/configure.

5. In the **Departments** dialog box, enter the **Active Directory Department** attribute name and then click the **Update** button.

The screenshot shows the 'Active Directory Configuration (ADQA)' dialog box with the 'Departments' tab selected. The tab is highlighted in a grey bar. Below the tab, there is a text area with the following text: 'File Reporter Department reports require the name of the Active Directory attribute that contains the department name assigned to each user. Please supply the name of the Active Directory Department attribute.' Below this text, there is a label 'Active Directory Department Attribute Name' and a text input field containing the word 'Department'. To the right of the input field is a small blue downward arrow. At the bottom right of the dialog box, there are three buttons: 'Update', 'Reset', and 'Delete'.

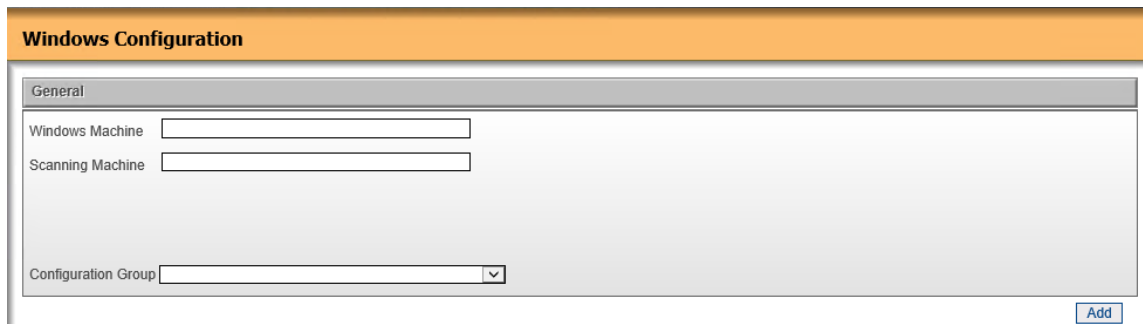
6. In the **Logging** dialog box, specify how you want the system to log events as they occur. Select any of the logging options and then click the **Update** button.
- No Logging: Prevents logging events to the log file.
  - Minimal Detail: Logs a few event details to the log file.
  - Full Detail: Logs all the details to the log file.

**NOTE:** The agent writes to a log file located in the install directory.

The screenshot shows the 'Active Directory Configuration (ADQA)' dialog box with the 'Logging' tab selected. The tab is highlighted in a grey bar. Below the tab, there is a text area with the following text: 'This section controls how verbose the system logs events as they occur. The agent writes to a log file located in the install directory.' Below this text, there are three radio button options: 'No Logging', 'Minimal Detail' (which is selected), and 'Full Detail'. At the bottom right of the dialog box, there are three buttons: 'Update', 'Reset', and 'Delete'.

## Configuring DefendX Software Data Collection Agent for Windows

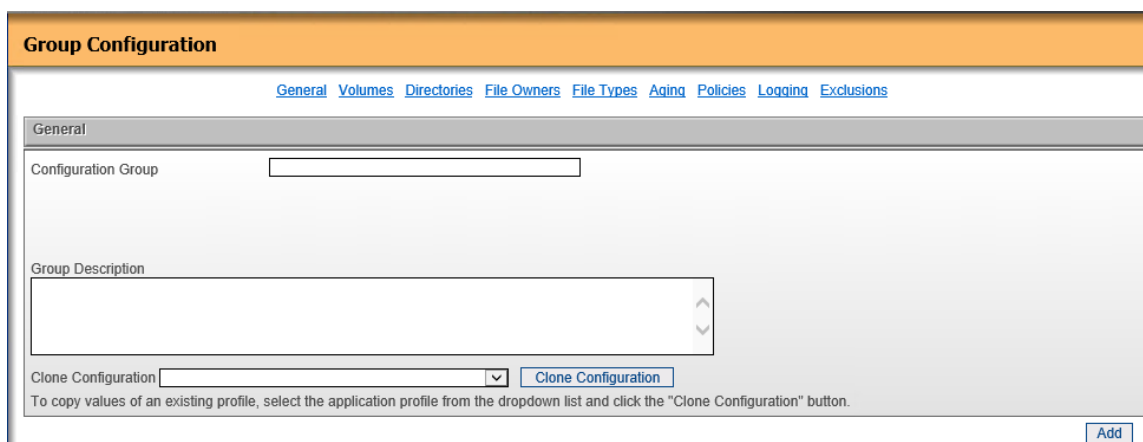
1. From the DefendX Software Vision™ Analysis Server machine, open the DefendX Software Data Collection Agent™ Administration by clicking **Start > All Programs > DefendX Storage Software Vision > DefendX Software Vision Data Agent Administration**.
2. In the left-hand main menu, click **New Windows Configuration** to open the Agent Configuration window.



The screenshot shows the 'Windows Configuration' dialog box. It has an orange header bar with the title 'Windows Configuration'. Below the header is a tabbed interface with the 'General' tab selected. The 'General' tab contains three input fields: 'Windows Machine', 'Scanning Machine', and 'Configuration Group'. The 'Configuration Group' field is a dropdown menu. An 'Add' button is located at the bottom right of the dialog box.

3. In the **General** dialog box, enter the Windows Server Name which will be scanned, and the name of the Scanning machine (a Windows server with DefendX Software Data Collection Agent, Windows Edition installed) and a description (if desired) and then click the **Add** button.

**NOTE:** To copy values of an existing profile, select the application profile from the **Clone Configuration** dropdown list and then click the **Clone Configuration** button.



The screenshot shows the 'Group Configuration' dialog box. It has an orange header bar with the title 'Group Configuration'. Below the header is a tabbed interface with the 'General' tab selected. The 'General' tab contains a 'Configuration Group' input field, a 'Group Description' text area, and a 'Clone Configuration' dropdown menu. A 'Clone Configuration' button is located next to the dropdown menu. Below the dropdown menu, there is a note: 'To copy values of an existing profile, select the application profile from the dropdown list and click the "Clone Configuration" button.' An 'Add' button is located at the bottom right of the dialog box.

4. From the **Home** page, under the **Windows Configurations** section, click the group name of the **Windows Configuration** you want to update/configure.
5. In the **Volumes** dialog box, select the resources you want to include in the data scan and then click the **Add** button.

**NOTE:** To include all the volumes in the scanning operation, click the **Include all Volumes** checkbox.

**Group Configuration (Default)**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

**Volumes**

☐ Scan All Volumes  
If this box is checked all Volumes will be scanned.

**Volumes Currently Configured -**

C:\  
D:\  
E:\  
F:\  
G:\  
H:\  
I:\  
J:\

Select the volumes you wish to scan from the list above. Hold down the CTRL key to select multiple volumes.

Update

Reset

Delete

6. In the **Directories** dialog box, click the **Include All Directories** check box if you want the agent to report all directories scanned. Click the **Update** button.

**NOTE:** You still can limit the directory depth; in this case, you need to specify a depth value at which directories will be included to minimize your Database size. The agent will still scan all the directories on the specified volumes.

**Group Configuration (Default)**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

**Directories**

The Data Collection Agent will scan all directories gathering information for reporting. The agent can report all directories scanned or can limit the directory depth for reporting. Please specify whether to include all directories or specify the depth of directories to include.

☐ Include All Directories

☒ Specify Max Directory Depth

Additional Directories To Include. Example: C:\Program Files\Application1

7. In the **File Owners** dialog box, click the **Include All Owners** checkbox to let the agent track consumed space for all file owners during the scan. Click the **Update** button.

**NOTE:** You still can choose to include only specific owners; click the **Include Specified Owners** checkbox to minimize your Database size (use the **Add** and **Remove** buttons to add/remove owners to/from the list). The agent will still scan all files owned by all file owners for the specified volumes.

The screenshot shows the 'Group Configuration (Default)' dialog box with the 'File Owners' tab selected. The tab is highlighted in orange. Below the tab, there are several navigation links: [General](#), [Volumes](#), [Directories](#), [File Owners](#), [File Types](#), [Aging](#), [Policies](#), [Logging](#), and [Exclusions](#). The 'File Owners' section has a title bar 'File Owners' and a description: 'The Data Collection Agent can track consumed space for file owners. Please select whether to include all owners or choose to only include specific owners.' There are two radio buttons: 'Include All Owners' (selected) and 'Include Specified Owners'. Below the radio buttons, there is a text input field labeled 'Owners To Include. Enter Active Directory User Logon Names, example: Administrator'. To the right of the input field are 'Add' and 'Remove' buttons. Below the input field is a large empty list box. At the bottom right of the dialog are 'Update', 'Reset', and 'Delete' buttons.

8. In the **File Types** dialog box, enter the file extensions you want to include in the business file types, temporary file types, and other file types during the scan. Click the **Update** button.

**NOTE:** You can select to include/exclude other file types entered or select to include/exclude duplicate files.

**File Types**

File Reporter will generate the core business file type reports based on the following file extensions. Use a comma-separated list to specify multiple file extensions. Example: doc, xls, ppt

Business File Types

File Reporter will generate the temporary file type reports based on the following file extensions. Use a comma-separated list to specify multiple file extensions. Example: tmp, temp, zar

Temporary File Types

File Reporter will generate the other tracked file type reports based on the following file extensions. Use a comma-separated list to specify multiple file extensions. Example: mp3, wav

Other File Types

☒ Include the Other File Types entered above  
☐ Exclude the Other File Types entered above

Duplicate Files  
☒ Include Duplicate Files

9. In the **Aging** dialog box, set the number of files to collect per age category and per volume. Enter a date (or select it in the calendar), or enter a number and select a value from the drop-down list to determine how old a modified file needs to be for reporting purposes. Enter a date (or select it in the calendar), or enter a number and select a value from the drop-down list to determine how old an accessed/not accessed file needs to be for reporting purposes. Click the **Update** button.

**Aging**

Enter the number of files to collect that meet the aging criteria below. The number of files collected is per age category and per volume.

Files to Collect

Enter a date, (or select it in the calendar below), or enter a number and select a value from the drop down list to determine how old a file needs to be for reporting purposes. Use the format MM/DD/YYYY for the Date or 999 for the Days, Months and Years.

☒ Not Modified in the Last

☐ Not Modified Since

Enter a date, (or select it in the calendar below), or enter a number and select a value from the drop down list to determine how old a file needs to be for reporting purposes. Use the format MM/DD/YYYY for the Date or 999 for the Days, Months and Years.

☒ Not Accessed in Last

☐ Not Accessed Since

10. In the **Policies** dialog box, specify whether you want to include/exclude your DefendX Software QFS® policy information in the DefendX Software Vision™ Reports.

**NOTE:** DefendX Software QFS must be installed on a DefendX Software Data Collection Agent server to report policy information for that server.

Policies
<p>The Data Collection Agent can gather policy information from QFS. Please select whether the agent should gather policy information from QFS.</p> <p><input checked="" type="checkbox"/> Include QFS Policies</p> <p><a href="#">Update</a> <a href="#">Reset</a> <a href="#">Delete</a></p>

11. In the **Logging** dialog box, specify how you want the system to log events as they occur. Select any of the logging options and then click the **Update** button.

- No Logging: Prevents logging events to the log file.
- Minimal Detail: Logs a few event details to the log file.
- Full Detail: Logs all the details to the log file.

**NOTE:** Enabling logging will enter events into the DataAgent\_<machine name>\_YYYY\_MM\_DD.log file found in the install directory. This feature is very useful for troubleshooting purposes.

**Group Configuration (Default)**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

**Logging**

This section controls how verbose the system logs events as they occur. The agent writes to a log file located in the install directory.

☐ No Logging

☒ Minimal Detail

☐ Full Detail

[Update](#) [Reset](#) [Delete](#)

12. In the **Exclusions** dialog box, you can see the directories that will be excluded from the Duplicate Files and Aging Files reports. These default directories are areas in which the server and administrator create files. Click **Update** to save your changes when the configuration is complete.

**Group Configuration (Default)**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

Exclusions

The following directories will be excluded from the duplicate files and aging files reports.

Excluded Directories
c:\temp
c:\windows
d:\temp
d:\windows
e:\temp
e:\windows

Update

Reset

Delete

## Configuring DefendX Software Data Collection Agent for NAS, NetApp

1. From the DefendX Software Vision Analysis Server machine, open the DefendX Software Data Collection Agent Administration by clicking **Start > All Programs > DefendX Storage Software Vision™ > DefendX Software Vision Data Agent Administration**.
2. In the left-hand main menu, click **New Filer Configuration** to open the **Filer Configuration** window.
3. Specify the Filer type: (Cluster-Mode or 7-Mode)
4. Fill the information required.
5. In the **General** dialog box, enter the Filer name and other information required along with the Filer description (if desired) and then click the **Add** button.

**NOTE:** To copy values of an existing profile, select the application profile from the **Clone Configuration** dropdown list and then click the **Clone Configuration** button.

### 7-Mode Configuration

The screenshot shows the 'Filer Configuration' window with the '7-Mode Configuration' tab selected. The window has a title bar 'Filer Configuration' and a navigation bar with links: General, Volumes, Directories, File Owners, File Types, Aging, Policies, Logging, Exclusions. The 'General' tab is active, showing fields for 'Filer ONTAP Version', 'Filer Name', 'This is a vfiler hosted by filer Scanning Machine', and 'Filer Description (250 characters)'. There are radio buttons for '7 Mode' (selected) and 'Cluster Mode'. At the bottom, there is a 'Clone Configuration' dropdown menu, a 'Clone Configuration' button, and an 'Add' button. A note at the bottom states: 'To copy values of an existing profile, select the application profile from the dropdown list and click the "Clone Configuration" button.'

**Filer Configuration**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

**General**

Filer ONTAP Version ☐ 7 Mode ☐ Cluster Mode

Filer Name

This is a vfiler hosted by filer

Scanning Machine

Filer Description (250 characters)

Clone Configuration

To copy values of an existing profile, select the application profile from the dropdown list and click the "Clone Configuration" button.

## Cluster-Mode Filer Configuration

**Filer Configuration**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

General

Filer ONTAP Version

☐ 7 Mode ☒ Cluster Mode

CIFS Server Name

Cluster IP Address

Scanning Machine

Please enter the credentials to access the Cluster to retrieve configuration information.

User Name

Set/Change Password ☒

Password

Confirm Password

Filer Description (250 characters)

Clone Configuration

Clone Configuration

To copy values of an existing profile, select the application profile from the dropdown list and click the "Clone Configuration" button.

Add

For cluster-mode filers, enter the name of your CIFS server, preferred connector IP address, cluster IP address, user name and password for account on the cluster.

The account entered must be a local account on the cluster and has admin role for the ontapi application. Use the following command to create this user:

```
$ security login create -username DefendX_user -application ontapi -authmethod password -role admin
```

- From the **Home** page, under the **Filer Configurations** section, click the Filer® name that you want to update/configure.

7-Mode Filer Configurations			
Listed below are the current Filer Configurations. To view an existing Filer Configuration click on the "Filer Name". To create a new Filer Configuration, click the "New Filer Configuration" button.			
NetApp Filer Name	Host Filer	Scanning Machine	Description
<a href="#">ntp-filer</a>		DCAMain	

Cluster-Mode Filer Configurations			
Listed below are the current Filer Configurations. To view an existing Filer Configuration click on the "Filer Name". To create a new Filer Configuration, click the "New Filer Configuration" button.			
CIFS Server	IP Address	Scanning Machine	Description
<a href="#">vs1qacifs</a>	10.30.3.253	DCAMain	C mode scan

7. In the **Volumes** dialog box, select the resources you want to include in the data scan and then click the **Update** button.

**NOTE:** To include all the volumes in the scanning operation, click the **Scan all Volumes** checkbox.

**Filer Configuration (sup-tap90-svm1)**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

NetApp Filer Volumes

Select which Filer Volumes will be scanned.

☒ Scan all Volumes

☐ Scan Specified Volumes

Volumes To Include (Note: Enter just the volume name. For instance: vol0 or public)

8. In the **Directories** dialog box, click the **Include All Directories** check box if you want the agent to report all directories scanned. Click the **Update** button.

**NOTE:** You still can limit the directory depth; in this case, you need to specify a depth value at which directories will be included to minimize your Database size. The agent will still scan all directories.

**Filer Configuration (sup-tap90-svm1)**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

**Directories**

The Data Collection Agent will scan all directories gathering information for reporting. The agent can report all directories scanned or can limit the directory depth for reporting. Please specify whether to include all directories or specify the depth of directories to include.

☐ Include All Directories

☒ Specify Max Directory Depth

Additional Directories To Include. (Full mount path from the vServer root) Example: \ or \Users\Mike

9. In the **File Owners** dialog box, click the **Include All Owners** checkbox to let the agent track consumed space for all file owners during the scan. Click the **Update** button.

**NOTE:** You still can choose to only include specific owners; click the **Include Specified Owners** checkbox to minimize your Database size (use the Add and Remove buttons to add/remove owners to/from the list). The agent will still scan all files owned by all file owners for the specified volumes.

**Filer Configuration (sup-tap90-svm1)**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

**File Owners**

The Data Collection Agent can track consumed space for file owners. Please select whether to include all owners or choose to only include specific owners.

☒ Include All Owners  
☐ Include Specified Owners

Owners To Include. Enter Active Directory User Logon Names, example: Administrator

10. In the **File Types** dialog box, enter the file extensions you want to include in the business file types, temporary file types, and other file types during the scan. Click the **Update** button.

**NOTE:** You can select to include/exclude other file types entered or select to include/exclude duplicate files.

The screenshot shows the 'File Types' dialog box. It has a title bar 'File Types'. Inside, there are three sections for specifying file extensions. Each section has a text box and a label. The first section is for 'Business File Types' with the text 'File Reporter will generate the core business file type reports based on the following file extensions. Use a comma-separated list to specify multiple file extensions. Example: doc, xls, ppt'. The text box contains 'doc', xls', xlt', vsd', pst', mdb', one'. The second section is for 'Temporary File Types' with the text 'File Reporter will generate the temporary file type reports based on the following file extensions. Use a comma-separated list to specify multiple file extensions. Example: tmp, temp, zar'. The text box contains 'tmp,temp'. The third section is for 'Other File Types' with the text 'File Reporter will generate the other tracked file type reports based on the following file extensions. Use a comma-separated list to specify multiple file extensions. Example: mp3, wav'. The text box contains 'mp3, avi, wma, wav, mov, aiff, aac'. Below these sections are two radio buttons: 'Include the Other File Types entered above' (selected) and 'Exclude the Other File Types entered above'. At the bottom left is a section for 'Duplicate Files' with a checked checkbox 'Include Duplicate Files'. At the bottom right are three buttons: 'Update', 'Reset', and 'Delete'.

File Types

File Reporter will generate the core business file type reports based on the following file extensions. Use a comma-separated list to specify multiple file extensions. Example: doc, xls, ppt

Business File Types

File Reporter will generate the temporary file type reports based on the following file extensions. Use a comma-separated list to specify multiple file extensions. Example: tmp, temp, zar

Temporary File Types

File Reporter will generate the other tracked file type reports based on the following file extensions. Use a comma-separated list to specify multiple file extensions. Example: mp3, wav

Other File Types

☒ Include the Other File Types entered above  
☐ Exclude the Other File Types entered above

Duplicate Files  
☒ Include Duplicate Files

11. In the **Aging** dialog box, set the number of files to collect per age category and per volume. Enter a date (or select it in the calendar), or enter a number and select a value from the drop-down list to determine how old a modified file needs to be for reporting purposes. Enter a date (or select it in the calendar), or enter a number and select a value from the drop-down list to determine how old an accessed/not accessed file needs to be for reporting purposes. Click the **Update** button.

**Aging**

Enter the number of files to collect that meet the aging criteria below. The number of files collected is per age category and per volume.

Files to Collect

Enter a date, (or select it in the calendar below), or enter a number and select a value from the drop down list to determine how old a file needs to be for reporting purposes. Use the format MM/DD/YYYY for the Date or 999 for the Days, Months and Years.

☒ Not Modified in the Last

☐ Not Modified Since

Enter a date, (or select it in the calendar below), or enter a number and select a value from the drop down list to determine how old a file needs to be for reporting purposes. Use the format MM/DD/YYYY for the Date or 999 for the Days, Months and Years.

☒ Not Accessed in Last

☐ Not Accessed Since

12. In the **Policies** dialog box, specify whether you want to include/exclude your DefendX Software QFS® policy information in the DefendX Software Vision reports.

**NOTE:** DefendX Software QFS® must be installed on a DefendX Software Data Collection Agent™ Filer to report policy information for that Filer.

Policies

The Data Collection Agent can gather policy information from QFS. Please select whether the agent should gather policy information from QFS.

☒ Include QFS Policies

Update

Reset

Delete

13. In the **Logging** dialog box, specify how you want the system to log events as they occur. Select any of the logging options and then click the **Update** button.

- No Logging: Prevents logging events to the log file.
- Minimal Detail: Logs a few event details to the log file.
- Full Detail: Logs all the details to the log file.

**NOTE:** Enabling logging will enter events into the DataAgent\_<Filer® name>\_YYYY\_MM\_DD.log file found in the install directory. This feature is very useful for troubleshooting purposes.

**Filer Configuration (sup-tap90-svm1)**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

**Logging**

This section controls how verbose the system logs events as they occur. The agent writes to a log file located in the install directory.

☐ No Logging  
☒ Minimal Detail  
☐ Full Detail

[Update](#) [Reset](#) [Delete](#)

14. In the **Exclusions** dialog box, you can see the directories that will be excluded from the Duplicate Files and Aging Files reports. These defaults are areas in which the Filer® and administrator create files. Click **Update** to save your changes when the configuration is complete.

**Filer Configuration (sup-tap90-svm1)**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

**Exclusions**

The following directories will be excluded from the duplicate files and aging files reports.

Excluded Directories
c:\temp
c:\windows
d:\temp
d:\windows
e:\temp
e:\windows

## Configuring DefendX Software Data Collection Agent for NAS EMC

1. From the DefendX Software Vision™ Analysis Server machine, open the DefendX Software Data Collection Agent™ Administration by clicking **Start > All Programs > DefendX Storage Software Vision > DefendX Software Vision Data Agent Administration**.
2. In the left-hand main menu, click **New VNX/Unity Configuration** to open the **VNX/Unity Configuration** window.

### VNX Configuration

**VNX Configuration**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

General

Server Type

☒ VNX ☐ Unity

CIFS Server Name

Control Station Host Name

Scanning Machine

Please enter the credentials to access the control station to retrieve configuration information.

User Name

Set/Change Password ☒

Password

Confirm Password

CIFS Server Description

Clone Configuration

Clone Configuration

To copy values of an existing profile, select the application profile from the dropdown list and click the "Clone Configuration" button.

Add

### Unity Configuration

**Unity Configuration**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

General

Server Type

☐ VNX ☒ Unity

CIFS Server Name

Unisphere Host Name

Scanning Machine

Please enter the credentials to access the Unisphere to retrieve configuration information.

User Name

Set/Change Password ☒

Password

Confirm Password

CIFS Server Description

Clone Configuration

Clone Configuration

To copy values of an existing profile, select the application profile from the dropdown list and click the "Clone Configuration" button.

Add

3. In the **General** dialog box, enter the VNX/Unity CIFS server name and other required information along with the VNX/Unity server description, and then click the **Add** button.

**NOTE:** To copy values of an existing profile, select the application profile from the **Clone Configuration** dropdown list and then click the **Clone Configuration** button.

4. From the **Home** page, under the **EMC VNX and EMC Unity Configuration** sections, click the CIFS server name you want to update/configure.

EMC VNX Configurations			
Listed below are the current EMC VNX Configurations. To view an existing EMC VNX Configuration click on the "CIFS Server Name". To create a new EMC VNX Configuration, click the "New VNX/Unity Configuration" button.			
CIFS Server	Control Station Host Name	Scanning Machine	Description
<a href="#">testvnx</a>	10.40.4.255	fr-qa	

EMC Unity Configurations			
Listed below are the current EMC Unity Configurations. To view an existing EMC Unity Configuration click on the "CIFS Server Name". To create a new EMC Unity Configuration, click the "New VNX/Unity Configuration" button.			
CIFS Server	Unisphere Host Name	Scanning Machine	Description
<a href="#">sup-unity-cifs1</a>	10.40.4.65	fr-qa	

5. In the **Volumes** dialog box, select the resources you want to include in the data scan and then click the **Update** button.

**NOTE:** To include all the volumes in the scanning operation, click the **Scan all Volumes** checkbox.

**Unity Configuration (sup-unity-cifs1)**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

**Volumes**

Select which Volumes will be scanned.

☒ Scan all Volumes  
☐ Scan Specified Volumes

Volumes To Include (Note: Enter just the volume name. For instance: vol0 or public)

6. In the **Directories** dialog box, click the **Include All Directories** check box if you want the agent to report all directories scanned. Click the **Update** button.

**NOTE:** You still can limit the directory depth for storing in the database; in this case, you need to specify a depth value for directories to minimize your Database size. The agent will still scan all directories.

**Unity Configuration (sup-unity-cifs1)**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

**Directories**

The Data Collection Agent will scan all directories gathering information for reporting. The agent can report all directories scanned or can limit the directory depth for reporting. Please specify whether to include all directories or specify the depth of directories to include.

☐ Include All Directories

☒ Specify Max Directory Depth

Additional Directories To Include. Example: 'public\Application1'

7. In the **File Owners** dialog box, click the **Include All Owners** checkbox to let the agent track consumed space for all file owners during the scan. Click the **Update** button.

**NOTE:** You still can choose only to include specific owners; select the **Include Specified Owners** checkbox to minimize your Database size (use the **Add** and **Remove** buttons to add/remove owners to/from the list). The agent will still scan all files owned by all file owners for the specified volumes.

**Unity Configuration (sup-unity-cifs1)**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

**File Owners**

The Data Collection Agent can track consumed space for file owners. Please select whether to include all owners or choose to only include specific owners.

☒ Include All Owners  
☐ Include Specified Owners

Owners To Include. Enter Active Directory User Logon Names, example: Administrator

8. In the **File Types** dialog box, enter the file extensions you want to include in the business file types, temporary file types, and other file types during the scan. Click the **Update** button.

**NOTE:** You can select to include/exclude other file types entered or select to include/exclude duplicate files.

**File Types**

File Reporter will generate the core business file type reports based on the following file extensions. Use a comma-separated list to specify multiple file extensions. Example: doc, xls, ppt

Business File Types

File Reporter will generate the temporary file type reports based on the following file extensions. Use a comma-separated list to specify multiple file extensions. Example: tmp, temp, zar

Temporary File Types

File Reporter will generate the other tracked file type reports based on the following file extensions. Use a comma-separated list to specify multiple file extensions. Example: mp', wav

Other File Types

☒ Include the Other File Types entered above  
☐ Exclude the Other File Types entered above

Duplicate Files  
☒ Include Duplicate Files

9. In the **Aging** dialog box, set the number of files to collect per age category and per volume. Enter a date (or select it in the calendar), or enter a number and select a value from the drop-down list to determine how old a modified file needs to be for reporting purposes. Enter a date (or select it in the calendar), or enter a number and select a value from the drop-down list to determine how old an accessed/not accessed file needs to be for reporting purposes. Click the **Update** button.

**Aging**

Enter the number of files to collect that meet the aging criteria below. The number of files collected is per age category and per volume.

Files to Collect

Enter a date, (or select it in the calendar below), or enter a number and select a value from the drop down list to determine how old a file needs to be for reporting purposes. Use the format MM/DD/YYYY for the Date or 999 for the Days, Months and Years.

☒ Not Modified in the Last

☐ Not Modified Since

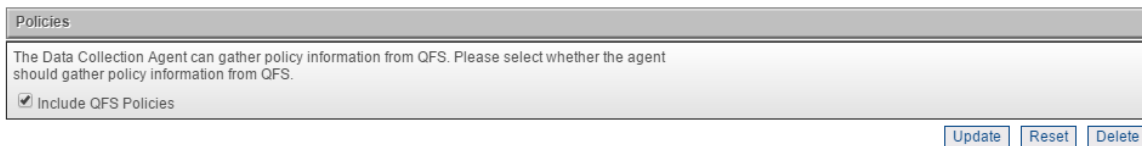
Enter a date, (or select it in the calendar below), or enter a number and select a value from the drop down list to determine how old a file needs to be for reporting purposes. Use the format MM/DD/YYYY for the Date or 999 for the Days, Months and Years.

☒ Not Accessed in Last

☐ Not Accessed Since

10. In the **Policies** dialog box, specify whether you want to include/exclude your DefendX Software QFS® policy information in the DefendX Software Vision™ Reports.

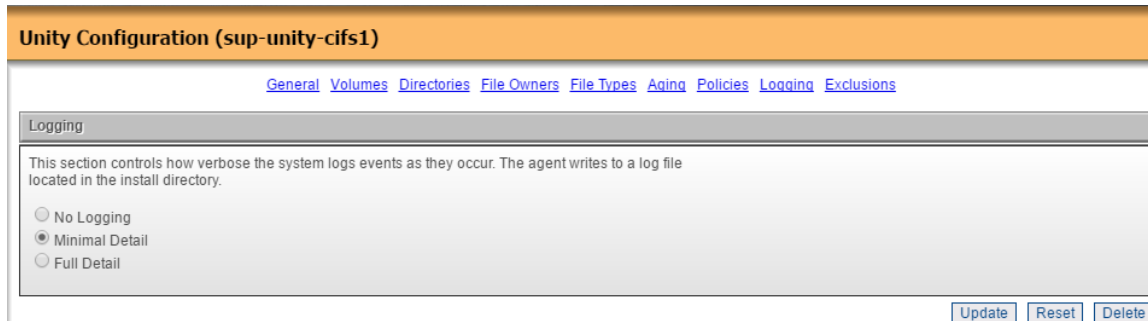
**NOTE:** DefendX Software QFS must be installed on a DefendX Software Data Collection Agent server to report policy information for that server.



11. In the **Logging** dialog box, specify how you want the system to log events as they occur. Select any of the logging options and then click the **Update** button.

- No Logging: Prevents logging events to the log file.
- Minimal Detail: Logs a few event details to the log file.
- Full Detail: Logs all the details to the log file.

**NOTE:** Enabling logging will enter events into the DataAgent\_<VNX name>\_YYYY\_MM\_DD.log file found in the install directory. This feature is very useful for troubleshooting purposes.



12. In the **Exclusions** dialog box, you can see the directories that will be excluded from the Duplicate Files and Aging Files reports. These defaults are areas in which the VNX/Unity and administrator create files. Click **Update** to save your changes when the configuration is complete.

**Unity Configuration (sup-unity-cifs1)**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

**Exclusions**

The following directories will be excluded from the duplicate files and aging files reports.

Excluded Directories
c:\temp
c:\windows
d:\temp
d:\windows
e:\temp
e:\windows

Update

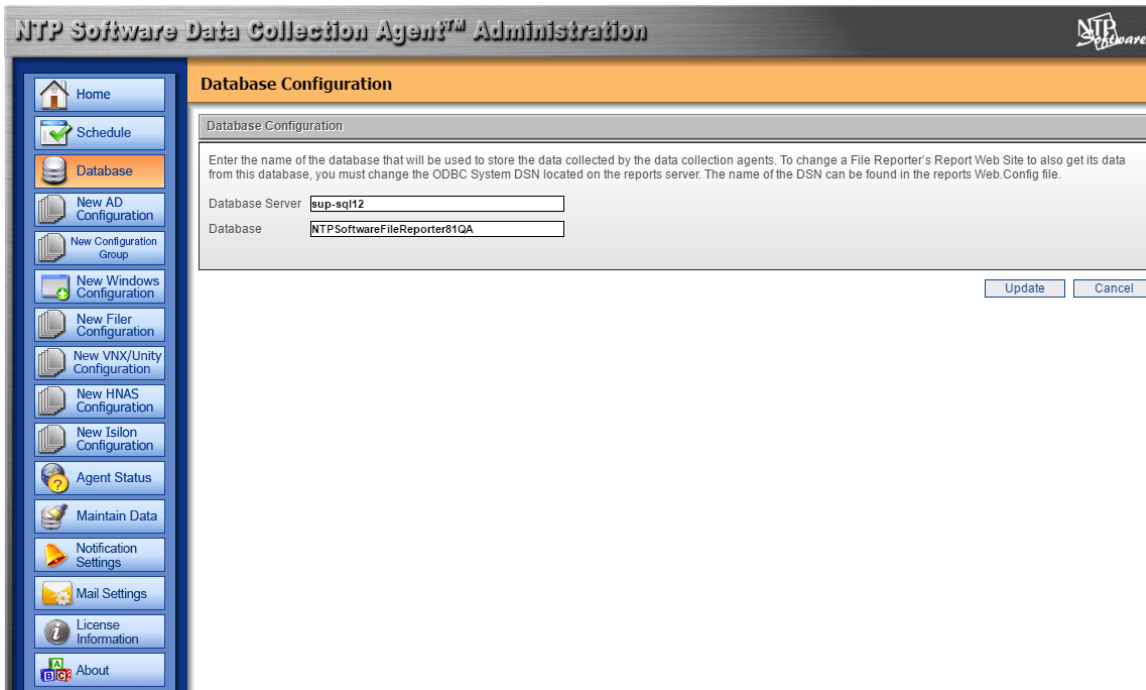
Reset

Delete

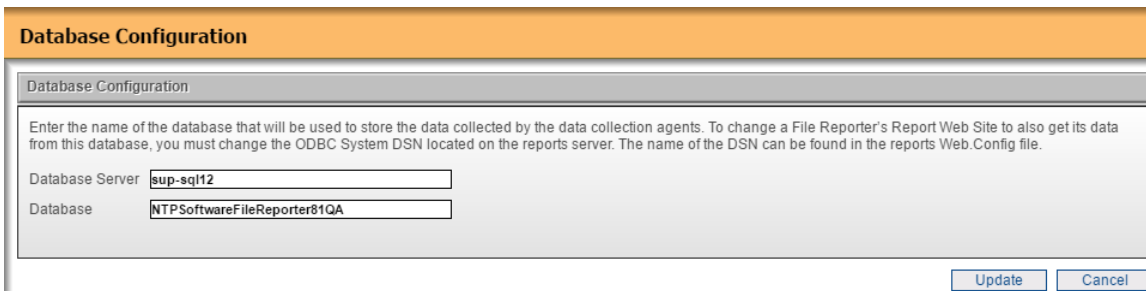
## DefendX Software Data Collection Agent Database Configuration

To configure the database of DefendX Software Data Collection Agent™, do the following:

1. In the left-hand main menu, click **Database** to open the **Database Configuration** window.



2. In the **Database Configuration** dialog box, update the database server and the database.



3. Click the **Update** button to save your changes.

**NOTE:** To change a Vision's Report Web Site to get data from the specified database, please make sure to change the ODBC System DSN located on the reports server. The name of the DSN can be found in the reports Web.Config file.

## Configuring DefendX Software Data Collection Agent for HNAS

1. From the DefendX Software Vision™ Analysis Server machine, open the DefendX Software Data Collection Agent™ Administration by clicking **Start > All Programs > DefendX Storage Software Vision > DefendX Software Vision Data Agent Administration**.
2. In the left-hand main menu, click **New HNAS Configuration** to open the **HNAS Configuration** window.

The screenshot shows the 'EVS Configuration' window with the 'General' tab selected. The window has a title bar 'EVS Configuration' and a menu bar with links: General, Volumes, Directories, File Owners, File Types, Aging, Policies, Logging, Exclusions. The 'General' tab is active, showing fields for 'Hitachi NAS EVS Name', 'Scanning Machine', and 'EVS Description (250 characters)'. There is a 'Clone Configuration' dropdown menu and a 'Clone Configuration' button. A note at the bottom states: 'To copy values of an existing profile, select the application profile from the dropdown list and click the "Clone Configuration" button.' An 'Add' button is located at the bottom right.

**EVS Configuration**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

**General**

Hitachi NAS EVS Name

Scanning Machine

EVS Description (250 characters)

Clone Configuration

To copy values of an existing profile, select the application profile from the dropdown list and click the "Clone Configuration" button.

3. In the **General** dialog box, enter the Hitachi NAS EVS machine name, the scanning machine along with the description, and then click the **Add** button.

**NOTE:** To copy values of an existing profile, select the application profile from the **Clone Configuration** dropdown list and then click the **Clone Configuration** button.

4. From the **Home** page, under the **Hitachi NAS Configurations** section, click the Isilon name you want to update/configure.

Hitachi NAS Configurations		
Listed below are the current Hitachi NAS EVS Configurations. To view an existing Hitachi NAS EVS Configuration click on the "EVS Name". To create a new Hitachi NAS EVS Configuration, click the "New HNAS Configuration" button.		
EVS Name	Scanning Machine	Description
<a href="#">evs09cifs</a>	fr-qa	

5. In the **Volumes** dialog box, enter the root share and then click the **Update** button.

**EVS Configuration (evs09cifs)**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

**EVS Volumes**

Select which EVS Volumes will be scanned.

☒ Scan all Volumes

☐ Scan Specified Volumes

Volumes To Include (Note: Enter just the volume name. For instance: vol0 or public)

6. In the **Directories** dialog box, click the **Include All Directories** check box if you want the agent to report all directories scanned. Click the **Update** button.

**NOTE:** You still can limit the directory depth for storing in the database; in this case, you need to specify a depth value for directories to minimize your Database size. The agent will still scan all directories.

The screenshot shows the 'EVS Configuration (evs09cifs)' window with the 'Directories' tab selected. The tab is highlighted in orange. Below the title bar, there are several tabs: General, Volumes, Directories, File Owners, File Types, Aging, Policies, Logging, and Exclusions. The 'Directories' tab is active, showing a text area with the following text: 'The Data Collection Agent will scan all directories gathering information for reporting. The agent can report all directories scanned or can limit the directory depth for reporting. Please specify whether to include all directories or specify the depth of directories to include.' Below this text, there are two radio buttons: 'Include All Directories' and 'Specify Max Directory Depth'. The 'Specify Max Directory Depth' radio button is selected, and a text box next to it contains the value '4'. Below this, there is a text box labeled 'Additional Directories To Include. Example: \FS01\Application1' with an 'Add' button and a 'Remove' button. At the bottom right of the dialog, there are three buttons: 'Update', 'Reset', and 'Delete'.

7. In the **File Owners** dialog box, click the **Include All Owners** checkbox to let the agent track consumed space for all file owners during the scan. Click the **Update** button.

**NOTE:** You still can choose only to include specific owners; select the **Include Specified Owners** checkbox to minimize your Database size (use the **Add** and **Remove** buttons to add/remove owners to/from the list). The agent will still scan all files owned by all file owners for the specified volumes.

The screenshot shows the 'EVS Configuration (evs09cifs)' window with the 'File Owners' tab selected. The tab is highlighted in orange. Below the title bar, there are several tabs: General, Volumes, Directories, File Owners, File Types, Aging, Policies, Logging, and Exclusions. The 'File Owners' tab is active, showing a text area with the following text: 'The Data Collection Agent can track consumed space for file owners. Please select whether to include all owners or choose to only include specific owners.' Below this text, there are two radio buttons: 'Include All Owners' and 'Include Specified Owners'. The 'Include All Owners' radio button is selected. Below this, there is a text box labeled 'Owners To Include. Enter Active Directory User Logon Names, example: Administrator' with an 'Add' button and a 'Remove' button. At the bottom right of the dialog, there are three buttons: 'Update', 'Reset', and 'Delete'.

8. In the **File Types** dialog box, enter the file extensions you want to include in the business file types, temporary file types, and other file types during the scan. Click the **Update** button.

**NOTE:** You can select to include/exclude other file types entered or select to include/exclude duplicate files.

The screenshot shows the 'File Types' dialog box. It has a title bar 'File Types'. Inside, there are three sections for specifying file extensions: 'Business File Types', 'Temporary File Types', and 'Other File Types'. Each section has a text input field and a descriptive paragraph. Below these sections are two radio buttons for 'Include the Other File Types entered above' and 'Exclude the Other File Types entered above'. At the bottom, there is a 'Duplicate Files' section with a checked checkbox for 'Include Duplicate Files'. At the very bottom right, there are three buttons: 'Update', 'Reset', and 'Delete'.

File Types

File Reporter will generate the core business file type reports based on the following file extensions. Use a comma-separated list to specify multiple file extensions. Example: doc, xls, ppt

Business File Types

File Reporter will generate the temporary file type reports based on the following file extensions. Use a comma-separated list to specify multiple file extensions. Example: tmp, temp, zar

Temporary File Types

File Reporter will generate the other tracked file type reports based on the following file extensions. Use a comma-separated list to specify multiple file extensions. Example: mp3, wav

Other File Types

☒ Include the Other File Types entered above  
☐ Exclude the Other File Types entered above

Duplicate Files  
☒ Include Duplicate Files

Update Reset Delete

9. In the **Aging** dialog box, set the number of files to collect per age category and per volume. Enter a date (or select it in the calendar), or enter a number and select a value from the drop-down list to determine how old a modified file needs to be for reporting purposes. Enter a date (or select it in the calendar), or enter a number and select a value from the drop-down list to determine how old an accessed/not accessed file needs to be for reporting purposes. Click the **Update** button.

**Aging**

Enter the number of files to collect that meet the aging criteria below. The number of files collected is per age category and per volume.

Files to Collect

Enter a date, (or select it in the calendar below), or enter a number and select a value from the drop down list to determine how old a file needs to be for reporting purposes. Use the format MM/DD/YYYY for the Date or 999 for the Days, Months and Years.

☒ Not Modified in the Last

☐ Not Modified Since

Enter a date, (or select it in the calendar below), or enter a number and select a value from the drop down list to determine how old a file needs to be for reporting purposes. Use the format MM/DD/YYYY for the Date or 999 for the Days, Months and Years.

☒ Not Accessed in Last

☐ Not Accessed Since

10. In the **Policies** dialog box, specify whether you want to include/exclude your DefendX Software QFS® policy information in the DefendX Software Vision™ Reports.

**NOTE:** DefendX Software QFS must be installed on an DefendX Software Data Collection Agent server to report policy information for that server.

Policies

The Data Collection Agent can gather policy information from QFS. Please select whether the agent should gather policy information from QFS.

☒ Include QFS Policies

Update

Reset

Delete

11. In the **Logging** dialog box, specify how you want the system to log events as they occur. Select any of the logging options and then click the **Update** button.

- No Logging: Prevents logging events to the log file.
- Minimal Detail: Logs a few event details to the log file.
- Full Detail: Logs all the details to the log file.

**NOTE:** Enabling logging will enter events into the DataAgent\_<HNAS name>\_YYYY\_MM\_DD.log file found in the install directory. This feature is very useful for troubleshooting purposes.

EVS Configuration (evs09cifs)

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

Logging

This section controls how verbose the system logs events as they occur. The agent writes to a log file located in the install directory.

☐ No Logging  
☒ Minimal Detail  
☐ Full Detail

Update

Reset

Delete

12. In the **Exclusions** dialog box, you can see the directories that will be excluded from the Duplicate Files and Aging Files reports. These defaults are areas in which the Isilon and administrator create files. Click **Update** to save your changes when the configuration is complete.

**EVS Configuration (evs09cifs)**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

**Exclusions**

The following directories will be excluded from the duplicate files and aging files reports.

Excluded Directories
c:\temp
c:\windows
d:\temp
d:\windows
e:\temp
e:\windows

## Configuring DefendX Software Data Collection Agent for NAS, EMC Isilon

13. From the DefendX Software Vision™ Analysis Server machine, open the DefendX Software Data Collection Agent™ Administration by clicking **Start > All Programs > DefendX Storage Software Vision > DefendX Software Vision Data Agent Administration**.
14. In the left-hand main menu, click **New Isilon Configuration** to open the **Isilon Configuration** window.

The screenshot shows the 'Isilon Configuration' window. At the top is an orange header bar with the title 'Isilon Configuration'. Below the header is a navigation bar with tabs: 'General', 'Volumes', 'Directories', 'File Owners', 'File Types', 'Aging', 'Policies', 'Logging', and 'Exclusions'. The 'General' tab is selected. The main area contains the following fields:

- 'EMC Isilon NAS Name' with a text input field.
- 'Scanning Machine' with a text input field.
- 'Isilon Description (250 characters)' with a large text area.
- 'Clone Configuration' with a dropdown menu and a 'Clone Configuration' button.

Below these fields is a note: 'To copy values of an existing profile, select the application profile from the dropdown list and click the "Clone Configuration" button.' At the bottom right is an 'Add' button.

In the **General** dialog box, enter the EMC Isilon NAS machine name, the scanning machine along with the description, and then click the **Add** button.

**NOTE:** To copy values of an existing profile, select the application profile from the **Clone Configuration** dropdown list and then click the **Clone Configuration** button.

15. From the **Home** page, under the **EMC Isilon NAS Configurations** section, click the Isilon name you want to update/configure.

EMC Isilon NAS Configurations		
Listed below are the current EMC Isilon NAS Configurations. To view an existing EMC Isilon NAS Configuration click on the "Isilon Name". To create a new EMC Isilon NAS Configuration, click the "New Isilon Configuration" button.		
Isilon Name	Scanning Machine	Description
<a href="#">isilontest</a>	fr-qa	

16. In the **Volumes** dialog box, enter the root share and then click the **Update** button.

**Isilon Configuration (isilontest)**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

Isilon Root Share

Root Share (Note: Enter just the share name. For instance: ifs)

ifs

Update

Reset

Delete

17. In the **Directories** dialog box, click the **Include All Directories** check box if you want the agent to report all directories scanned. Click the **Update** button.

**NOTE:** You still can limit the directory depth for storing in the database; in this case, you need to specify a depth value for directories to minimize your Database size. The agent will still scan all directories.

**Isilon Configuration (isilontest)**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

Directories

The Data Collection Agent will scan all directories gathering information for reporting. The agent can report all directories scanned or can limit the directory depth for reporting. Please specify whether to include all directories or specify the depth of directories to include.

☐ Include All Directories

☒ Specify Max Directory Depth

Additional Directories To Include. Example: \\fs\\Application1

Add

Remove

Update

Reset

Delete

18. In the **File Owners** dialog box, click the **Include All Owners** checkbox to let the agent track consumed space for all file owners during the scan. Click the **Update** button.

**NOTE:** You still can choose only to include specific owners; select the **Include Specified Owners** checkbox to minimize your Database size (use the **Add** and **Remove** buttons to add/remove owners to/from the list). The agent will still scan all files owned by all file owners for the specified volumes.

**Isilon Configuration (isilontest)**

[General](#) [Volumes](#) [Directories](#) [File Owners](#) [File Types](#) [Aging](#) [Policies](#) [Logging](#) [Exclusions](#)

**File Owners**

The Data Collection Agent can track consumed space for file owners. Please select whether to include all owners or choose to only include specific owners.

☒ Include All Owners  
☐ Include Specified Owners

Owners To Include. Enter Active Directory User Logon Names, example: Administrator

19. In the **File Types** dialog box, enter the file extensions you want to include in the business file types, temporary file types, and other file types during the scan. Click the **Update** button.

**NOTE:** You can select to include/exclude other file types entered or select to include/exclude duplicate files.

**File Types**

File Reporter will generate the core business file type reports based on the following file extensions. Use a comma-separated list to specify multiple file extensions. Example: doc, xls, ppt

Business File Types

File Reporter will generate the temporary file type reports based on the following file extensions. Use a comma-separated list to specify multiple file extensions. Example: tmp, temp, zar

Temporary File Types

File Reporter will generate the other tracked file type reports based on the following file extensions. Use a comma-separated list to specify multiple file extensions. Example: mp\*, wav

Other File Types

☒ Include the Other File Types entered above  
☐ Exclude the Other File Types entered above

Duplicate Files  
☒ Include Duplicate Files

20. In the **Aging** dialog box, set the number of files to collect per age category and per volume. Enter a date (or select it in the calendar), or enter a number and select a value from the drop-down list to determine how old a modified file needs to be for reporting purposes. Enter a date (or select it in the calendar), or enter a number and select a value from the drop-down list to determine how old an accessed/not accessed file needs to be for reporting purposes. Click the **Update** button.

**Aging**

Enter the number of files to collect that meet the aging criteria below. The number of files collected is per age category and per volume.

Files to Collect

Enter a date, (or select it in the calendar below), or enter a number and select a value from the drop down list to determine how old a file needs to be for reporting purposes. Use the format MM/DD/YYYY for the Date or 999 for the Days, Months and Years.

☒ Not Modified in the Last

☐ Not Modified Since

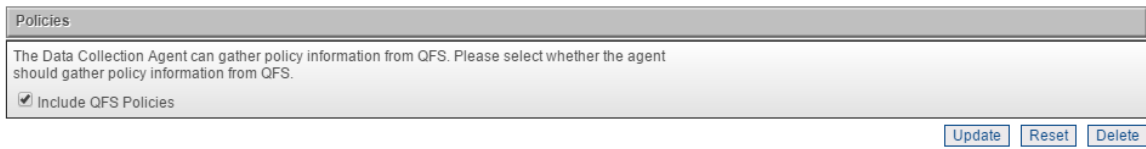
Enter a date, (or select it in the calendar below), or enter a number and select a value from the drop down list to determine how old a file needs to be for reporting purposes. Use the format MM/DD/YYYY for the Date or 999 for the Days, Months and Years.

☒ Not Accessed in Last

☐ Not Accessed Since

21. In the **Policies** dialog box, specify whether you want to include/exclude your DefendX Software QFS® policy information in the DefendX Software Vision™ Reports.

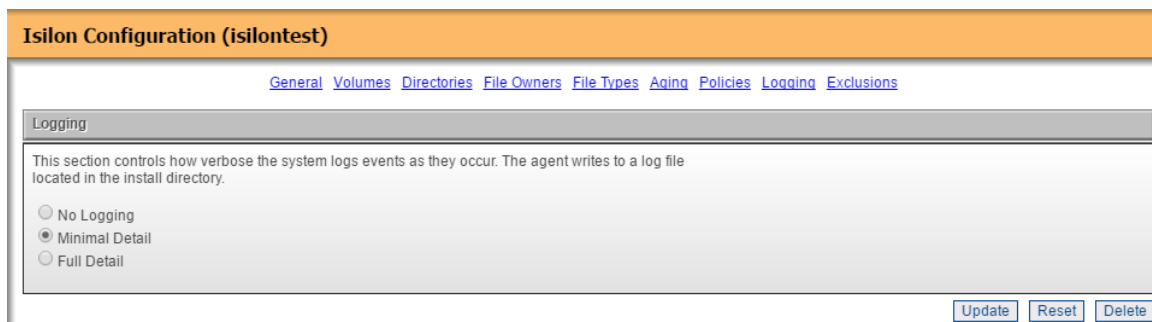
**NOTE:** DefendX Software QFS must be installed on a DefendX Software Data Collection Agent server to report policy information for that server.



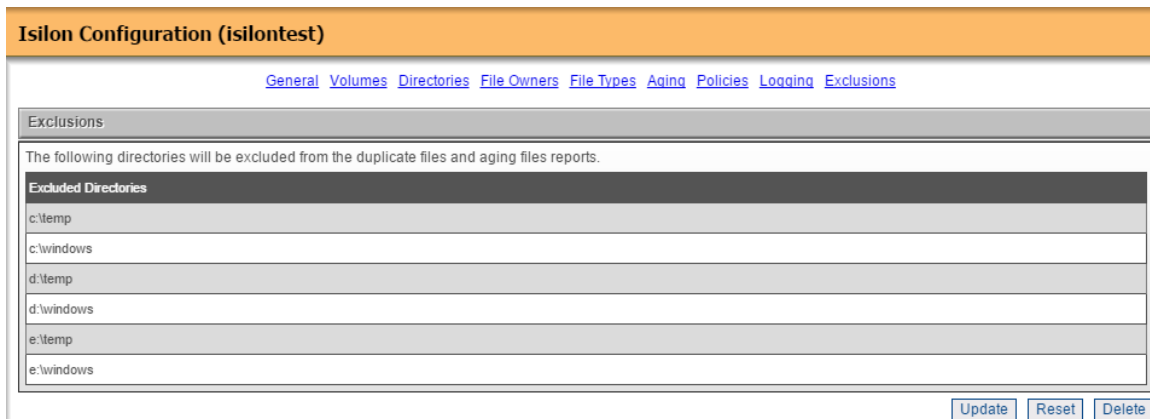
22. In the **Logging** dialog box, specify how you want the system to log events as they occur. Select any of the logging options and then click the **Update** button.

- No Logging: Prevents logging events to the log file.
- Minimal Detail: Logs a few event details to the log file.
- Full Detail: Logs all the details to the log file.

**NOTE:** Enabling logging will enter events into the DataAgent\_<Isilon name>\_YYYY\_MM\_DD.log file found in the install directory. This feature is very useful for troubleshooting purposes.



23. In the **Exclusions** dialog box, you can see the directories that will be excluded from the Duplicate Files and Aging Files reports. These defaults are areas in which the Isilon and administrator create files. Click **Update** to save your changes when the configuration is complete.



The screenshot shows the 'Isilon Configuration (isilontest)' window with the 'Exclusions' tab selected. The tab is highlighted in orange. Below the tab, there is a text box stating 'The following directories will be excluded from the duplicate files and aging files reports.' Below this text box is a table with the heading 'Excluded Directories'. The table contains six rows, each with a directory path: 'c:\temp', 'c:\windows', 'd:\temp', 'd:\windows', 'e:\temp', and 'e:\windows'. At the bottom right of the window, there are three buttons: 'Update', 'Reset', and 'Delete'.

Excluded Directories
c:\temp
c:\windows
d:\temp
d:\windows
e:\temp
e:\windows

## DefendX Software Data Collection Agent Schedule Configuration

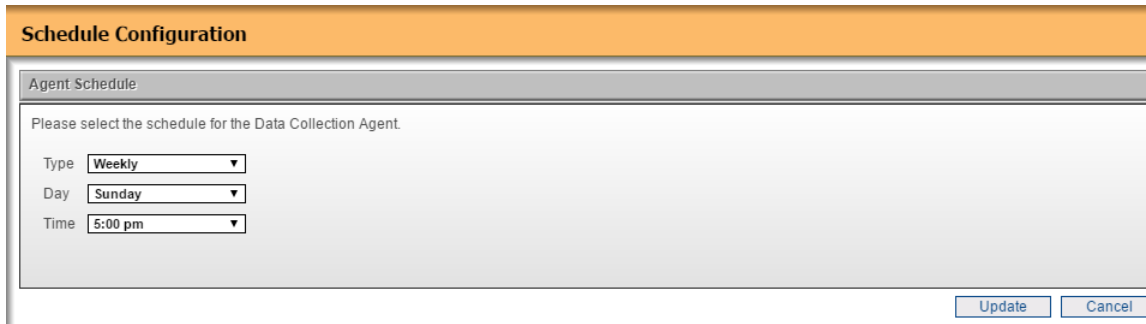
To configure the schedules of DefendX Software Data Collection Agent, do the following:

1. In the left-hand main menu, click **Schedule** to open the **Schedule Configuration** window.



The screenshot shows the 'NTP Software Data Collection Agent™ Administration' window. The 'Schedule Configuration' tab is selected and highlighted in orange. On the left side, there is a vertical menu with various options: Home, Schedule, Database, New AD Configuration, New Configuration Group, New Windows Configuration, New Filer Configuration, New VNX/Unity Configuration, New HNAS Configuration, New Isilon Configuration, Agent Status, Maintain Data, Notification Settings, Mail Settings, License Information, and About. The 'Schedule' option is highlighted. The main area of the window is titled 'Agent Schedule' and contains the text 'Please select the schedule for the Data Collection Agent.' Below this text are three dropdown menus: 'Type' (set to 'Weekly'), 'Day' (set to 'Sunday'), and 'Time' (set to '5:00 pm'). At the bottom right of the window, there are two buttons: 'Update' and 'Cancel'.

2. In the **Agent Configuration** dialog box, select daily/weekly/monthly scan schedule and set the time to run the scan.



**Schedule Configuration**

Agent Schedule

Please select the schedule for the Data Collection Agent.

Type: **Weekly** ▼

Day: **Sunday** ▼

Time: **5:00 pm** ▼

Update Cancel

**NOTE:** As scans use a lot of network resources during the scanning operation, it is strongly recommended to run weekly or monthly scans instead of daily scans.

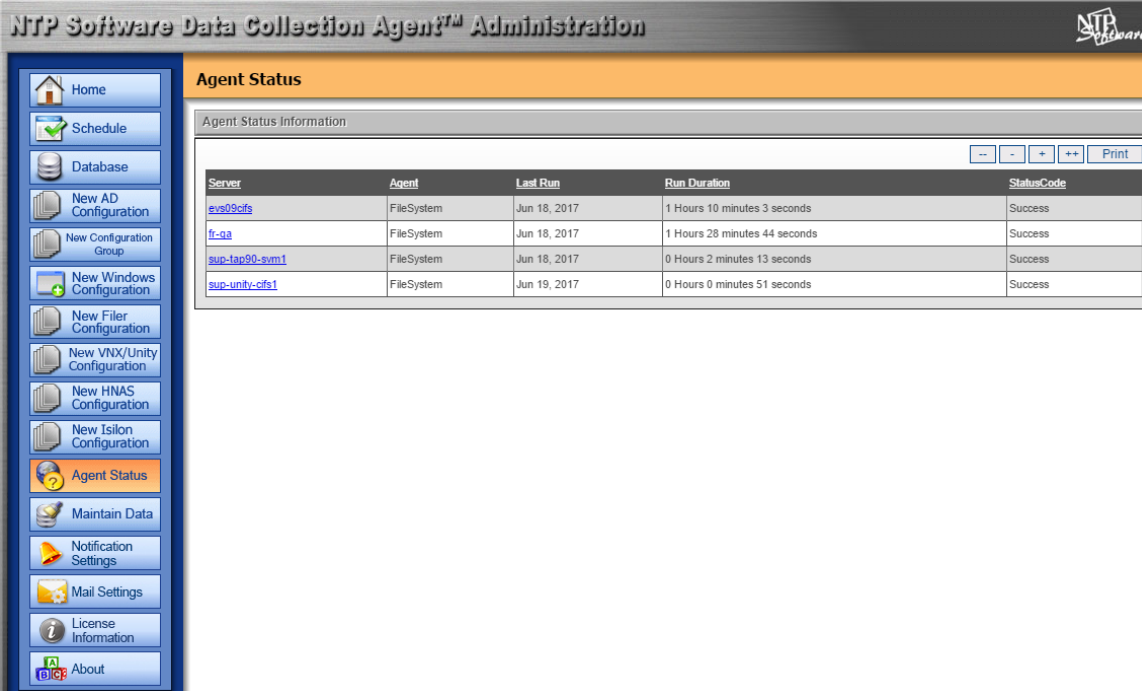
3. To run forced scan, navigate to the installation folder and run the *DataAgent.exe*  
For example: To run Hitachi scan, in the command prompt navigate to installation folder,  
C:\Program Files\DefendXSoftware\Data Collection Agent\HNAS>  
Then execute the command *DataAgentHNAS.exe*

## Viewing DefendX Software Vision Agent Status Utility

DefendX Software Vision™ is an agent-based application. Each server in your environment has its own DefendX Software Data Collection Agent, which is responsible for scanning, processing, and reporting the individual server's data to the database. Network communication problems can cause an agent to fail to report its complete dataset to the database. DefendX Software provides a status utility to help determine whether a communication problem might have occurred, and if so, where it happened.

To view the agent status utility, do the following:

1. In the left-hand main menu, click **Agent Status**. The Agent Status Information screen shows the date and duration of the last successful scan of each server on the network.

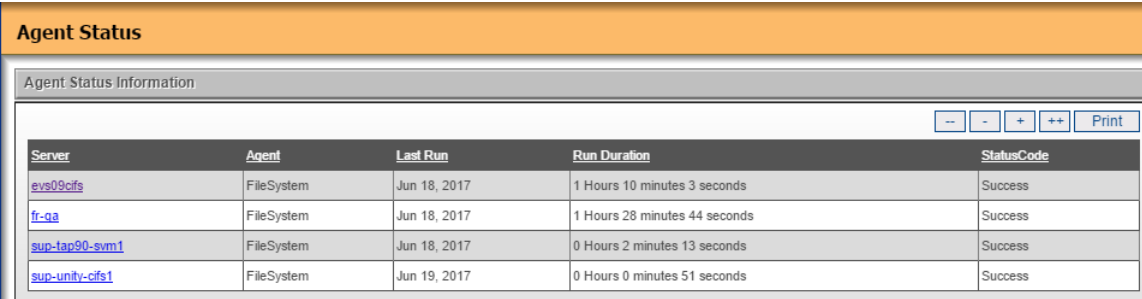


The screenshot shows the 'NTP Software Data Collection Agent™ Administration' window. The left-hand menu is expanded to 'Agent Status'. The main content area is titled 'Agent Status' and contains a sub-section 'Agent Status Information'. Below this is a table with the following data:

Server	Agent	Last Run	Run Duration	StatusCode
<a href="#">evs09cifs</a>	FileSystem	Jun 18, 2017	1 Hours 10 minutes 3 seconds	Success
<a href="#">fr-ga</a>	FileSystem	Jun 18, 2017	1 Hours 28 minutes 44 seconds	Success
<a href="#">sup-tap90-svm1</a>	FileSystem	Jun 18, 2017	0 Hours 2 minutes 13 seconds	Success
<a href="#">sup-unity-cifs1</a>	FileSystem	Jun 19, 2017	0 Hours 0 minutes 51 seconds	Success

**NOTE:** Click the headers of the view displayed in the figure to sort the data in ascending or descending order.

2. In the **Agent Status Information** dialog box, click a server name to open its details page.



The screenshot shows the 'Agent Status' dialog box. The 'Agent Status Information' section contains a table with the following data:

Server	Agent	Last Run	Run Duration	StatusCode
<a href="#">evs09cifs</a>	FileSystem	Jun 18, 2017	1 Hours 10 minutes 3 seconds	Success
<a href="#">fr-ga</a>	FileSystem	Jun 18, 2017	1 Hours 28 minutes 44 seconds	Success
<a href="#">sup-tap90-svm1</a>	FileSystem	Jun 18, 2017	0 Hours 2 minutes 13 seconds	Success
<a href="#">sup-unity-cifs1</a>	FileSystem	Jun 19, 2017	0 Hours 0 minutes 51 seconds	Success

3. In the **Agent Status Details** window, you can view all the scans that have run on that server.

Agent Status				
Agent Status Details				
Server: evs09cifs Run Date: 6/18/2017 5:00:01 PM <div> <input type="button" value="--"/> <input type="button" value="-"/> <input type="button" value="+"/> <input type="button" value="++"/> <input type="button" value="Print"/> </div>				
Step Description	Run Duration	Status Code	Records Inserted/Scanned	Failed Records
Volume EVS09_FS: Scan Phase	1 Hours 9 minutes 44 seconds	Success	6743	0
Volume EVS09_FS: Data Transfer Phase (DIR)	0 Hours 0 minutes 1 seconds	Success	41	0
Volume EVS09_FS: Data Transfer Phase (EXT)	0 Hours 0 minutes 3 seconds	Success	115	0
Volume EVS09_FS: Data Transfer Phase (tblExtFiles)	0 Hours 0 minutes 1 seconds	Success	40	0
Volume EVS09_FS: Data Transfer Phase (Files)	0 Hours 0 minutes 0 seconds	Success	1	0
Volume EVS09_FS: Data Transfer Phase (UserDir)	0 Hours 0 minutes 1 seconds	Success	65	0
Volume EVS09_FS: Data Transfer Phase (tblLargestUserFiles)	0 Hours 0 minutes 1 seconds	Success	10	0
Volume EVS09_FS: Data Transfer Phase (DupFiles)	0 Hours 0 minutes 1 seconds	Success	51	0
Volume EVS09_FS: Data Transfer Phase (UDirAge)	0 Hours 0 minutes 2 seconds	Success	46	0
Volume EVS09_FS: Data Transfer Phase (DirAge)	0 Hours 0 minutes 1 seconds	Success	41	0
< 2				

**IMPORTANT:** If a scan did not complete successfully, the status utility shows a breakdown for each agent's status to help determine where the problem occurred.

#### NOTES:

- Clicking a server's name displays a full report about the scans that have run on that server.
- This report includes a description of the phase (whether scanning, data analysis, or data transfer), the time duration of the phase, and the phase status (whether Success or Failed).
- It also shows the number of records for a data transfer operation or scanned records for a scanning operation.
- Use the   or   buttons to increase or decrease the number of records displayed per page.
- Use the  button to obtain a hard copy of the results.

## Purging the DefendX Software Vision Database

By default, DefendX Software Vision™ performs weekly scans on all of your enterprise servers with DefendX Software Data Collection Agents installed. Because DefendX Software does not impose size limits on the DefendX Software Vision database, the database could grow extremely large over time. We recommend using the database purging utility routinely to clean your DefendX Software Vision database.

**NOTE:** Purging data from the database also removes the data from report displays.

**IMPORTANT:** Database maintenance functionality requires the **SQL Server Agent service to be running on the SQL Server**. If this service is not running, no database maintenance will be performed.

To purge DefendX Software Vision database, do the following:

1. In the left-hand main menu, click **Maintain Data**.

The screenshot displays the 'NTP Software Data Collection Agent™ Administration' window. The left-hand menu is visible, with 'Maintain Data' highlighted. The main content area is titled 'Database Maintenance' and contains two sections: 'Execute Maintenance Task Immediately' and 'Scheduled Maintenance Tasks'.

**Execute Maintenance Task Immediately**

Purge data collected on and/or before selected date...  ☐ Purge data collected before the selected date and (optionally) the server

You can optionally specify the maximum number of hours for which you allow your operation to run

**Scheduled Maintenance Tasks**

☐ Enable automatic purging (delete data older than...)  Week(s) old

☐ Purge data previously summarized

☐ Enable automatic summarization (summarize data older than...)  Week(s) old

Schedule time:

[Scheduled Requests Status](#)

**Note:** Database Maintenance functionality requires the SQL Server Agent service to be running on the SQL Server.

DefendX Software Vision Database Maintenance offers a variety of options for purging data including:

- Purging data collected on a selected date with the option to purge all data before the selected date
- Purging of data from a specific server
- Enabling Automatic Purging (purge data older than a specific time period)
- Enabling Automatic Summarization (summarize data older than a specific time period)

**NOTE:** The Automatic Purging and Automatic Summarization will execute on a daily basis at the time specified.

2. In the **Maintain Data Settings** window, select the purging criteria you want to apply based on the criteria sets specified previously. Click the **Save Schedule** button.

Database Maintenance

Execute Maintenance Task

Immediately

Purge data collected on and/or before selected date...

10/1/2017

☐ Purge data collected before the selected date

and (optionally) the server

All servers

You can optionally specify the maximum number of hours for which you allow your operation to run

1

Start Purging

Scheduled Maintenance Tasks

☐ Enable automatic purging (delete data older than...)

Week(s)

old

☐ Purge data previously summarized

☐ Enable automatic summarization (summarize data older than...)

Week(s)

old

Schedule time: 12:00 am

Save Schedule

[Scheduled Requests Status](#)

Note: Database Maintenance functionality requires the SQL Server Agent service to be running on the SQL Server.

3. Press the **Start Purging** button to begin an on-demand purge function based on the criteria sets selected.

**NOTE:** Because of the permanent nature of the data deletion, an administrator is required to enable the function before performing a purge. We also recommend performing a backup before any purge takes place.

Database Maintenance

Execute Maintenance Task  
Immediately

Purge data collected on and/or before selected date...

10/1/2017

☐ Purge data collected before the selected date

and (optionally) the server

All servers

You can optionally specify the maximum number of hours for which you allow your operation to run

1

Start Purging

Scheduled Maintenance Tasks

☐ Enable automatic purging (delete data older than...)

Week(s)

old

☐ Purge data previously summarized

☐ Enable automatic summarization (summarize data older than...)

Week(s)

old

Schedule time:

12:00 am

Save Schedule

[Scheduled Requests Status](#)

Note: Database Maintenance functionality requires the SQL Server Agent service to be running on the SQL Server.

4. Once **Start Purging** is selected you will be asked if you are sure you want to continue. After selecting **OK** a **Request Status** option will appear. To see the status of your selected purge, simply click **Request Status** and a new window will pop up which will include the status of your job.

Database Maintenance

Execute Maintenance Task  
Immediately

Purge data collected on and/or before selected date...

10/1/2017

☐ Purge data collected before the selected date

and (optionally) the server

qa-fr

You can optionally specify the maximum number of hours for which you allow your operation to run

1

Start Purging

Your request for data purging was submitted successfully. Its Request ID is 18. You can check the status of your request by following the link below.

[Request Status](#)

Maintenance Requests Status								
ID	Type	Description	Status	Owner	Created	Picked for Execution	Completed	Notes/Errors
18	Purge by date/server	Purge data that was obtained on 2017-10-01 from the qa-fr server.	Submitted	NT AUTHORITY\USER	2017-10-05 16:33:45.1800000			

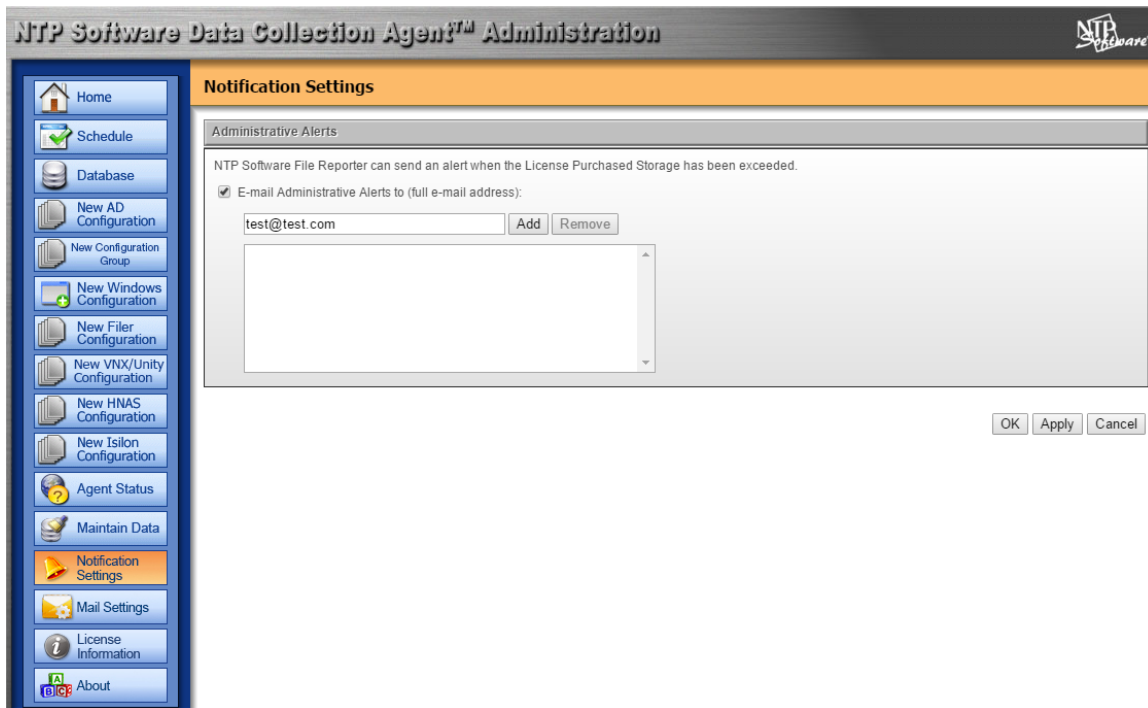
[Refresh](#)

**NOTE:** Once a job is submitted, SQL Server Agent can take up to 15 minutes to start processing the request. The status page does not auto-refresh but can be refreshed to update the current status.

## Notification Settings

DefendX Software Vision can notify an administrator once the license for purchased storage has been exceeded. To setup this notification, do the following:

1. In the left-hand main menu, click **Notification Settings**.



2. To add an E-mail address type it into the menu next to the Add/Remove buttons and press **Add**. Once you have added all E-mail addresses that you want to have notified, press **Apply**.

**Notification Settings**

Administrative Alerts

NTP Software File Reporter can send an alert when the License Purchased Storage has been exceeded.

☒ E-mail Administrative Alerts to (full e-mail address):

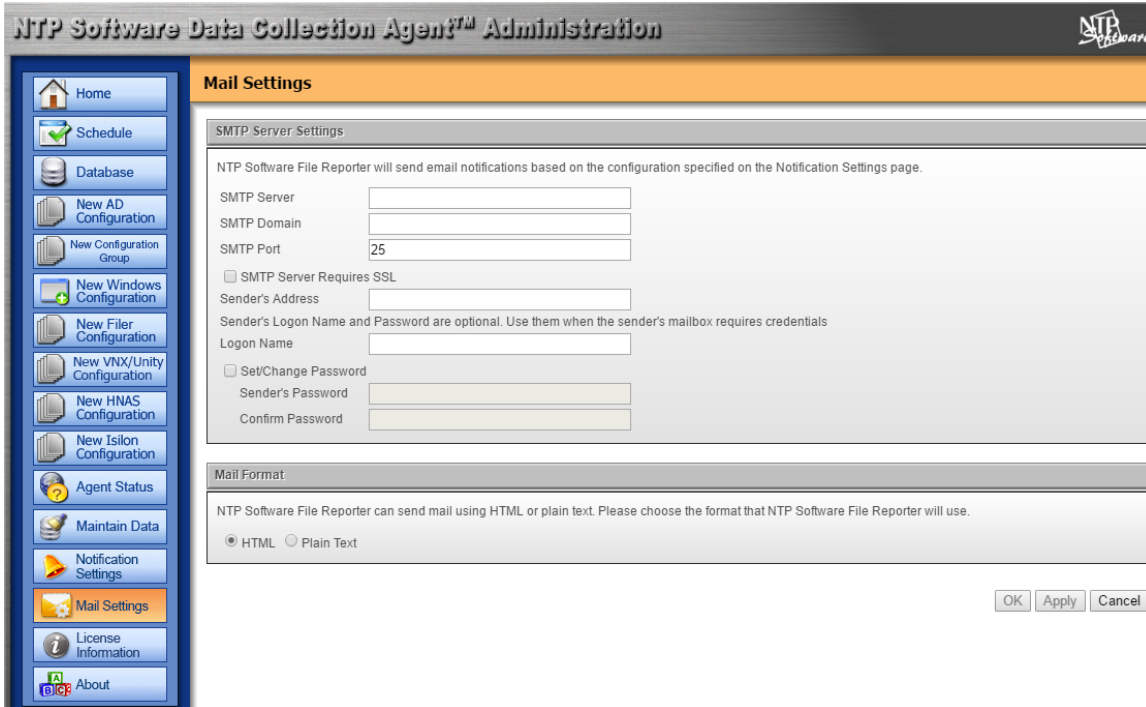
test@test.com    Add    Remove

OK    Apply    Cancel

## Mail Settings

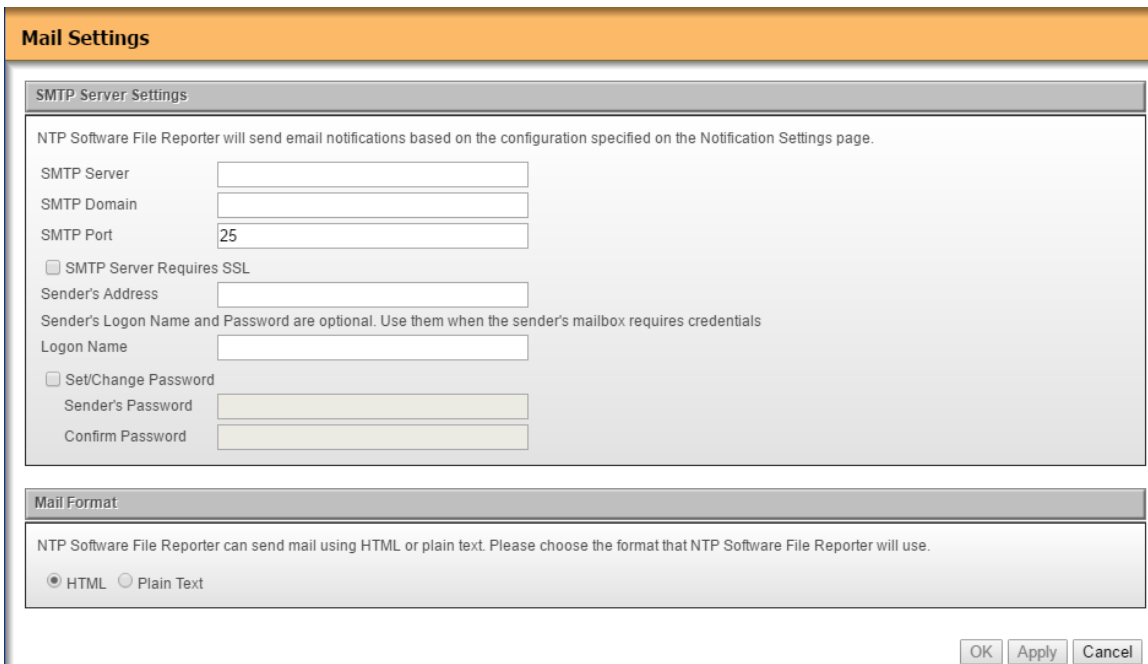
E-mail server settings are entered here for DefendX Software Vision notifications in this area. In order for E-mail notifications to work E-mail server settings must be input accurately. To setup your Mail Settings, do the following:

1. In the left-hand main menu, click **Mail Settings**.



The screenshot shows the 'NTP Software Data Collection Agent™ Administration' window. On the left is a vertical menu with options: Home, Schedule, Database, New AD Configuration, New Configuration Group, New Windows Configuration, New File Configuration, New VNX/Unity Configuration, New HNAS Configuration, New Isilon Configuration, Agent Status, Maintain Data, Notification Settings, Mail Settings (highlighted), License Information, and About. The main area is titled 'Mail Settings' and contains two sections: 'SMTP Server Settings' and 'Mail Format'. The 'SMTP Server Settings' section includes fields for SMTP Server, SMTP Domain, SMTP Port (set to 25), a checkbox for 'SMTP Server Requires SSL', a field for 'Sender's Address', a note about optional Logon Name and Password, a field for 'Logon Name', a checkbox for 'Set/Change Password', and fields for 'Sender's Password' and 'Confirm Password'. The 'Mail Format' section includes a note about choosing the format and radio buttons for 'HTML' (selected) and 'Plain Text'. At the bottom right are 'OK', 'Apply', and 'Cancel' buttons.

2. Fill out the appropriate settings for your E-mail server then hit **Apply**.



This is a detailed view of the 'Mail Settings' form. It features an orange header bar with the title 'Mail Settings'. Below the header is a section titled 'SMTP Server Settings' with a grey background. Inside this section, a note states: 'NTP Software File Reporter will send email notifications based on the configuration specified on the Notification Settings page.' The form includes input fields for 'SMTP Server', 'SMTP Domain', and 'SMTP Port' (containing the value '25'). There is a checkbox labeled 'SMTP Server Requires SSL'. Below this is a field for 'Sender's Address' and a note: 'Sender's Logon Name and Password are optional. Use them when the sender's mailbox requires credentials'. This is followed by a field for 'Logon Name', a checkbox labeled 'Set/Change Password', and fields for 'Sender's Password' and 'Confirm Password'. Below the 'SMTP Server Settings' section is another section titled 'Mail Format' with a grey background. It contains a note: 'NTP Software File Reporter can send mail using HTML or plain text. Please choose the format that NTP Software File Reporter will use.' and two radio buttons: 'HTML' (selected) and 'Plain Text'. At the bottom right of the form are 'OK', 'Apply', and 'Cancel' buttons.

## About DefendX Software

DefendX Software helps organizations secure their critical business files and maximize the value of their enterprise file storage resources. From comprehensive intelligence, modeling, costing and chargeback to seamless file movement, protection and archiving, DefendX provides industry-leading capabilities to eliminate waste and align the value of files with the storage resources they consume. With DefendX, important file locations and the users who access them can be monitored to provide governance, protect against theft and enforce compliance policies. For more than 20 years, DefendX Software has been helping public and private sector customers around the world save money and eliminate risk every day.

## DefendX Software Professional Services

DefendX Software's Professional Services offers consulting, training, and design services to help customers with their storage management challenges. We have helped hundreds of customers to implement cost-effective solutions for managing their storage environments. Our services range from a simple assessment to in-depth financial analyses.

For further assistance in creating the most cost-effective Storage Management Infrastructure, please contact your DefendX Software Representative at 800-390-6937.

## Legal & Contact Information

The information contained in this document is believed to be accurate as of the date of publication. Because DefendX Software must constantly respond to changing market conditions, what is here should not be interpreted as a commitment on the part of DefendX Software, and DefendX Software cannot guarantee the accuracy of any information presented after the date of publication.

This user manual is for informational purposes only. DEFENDX SOFTWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

DefendX Software and other marks are either registered trademarks or trademarks of DefendX Software in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

DefendX Software products and technologies described in this document may be protected by United States and/or international patents.

DefendX Software  
119 Drum Hill Road, #383  
Chelmsford MA 01824  
Phone: 1-800-390-6937  
E-mail: [info@DefendX.com](mailto:info@DefendX.com)  
Web Site: <http://www.DefendX.com>

Copyright © 2020 DefendX Software. All rights reserved. All trademarks and registered trademarks are the property of their respective owners.

Doc#DFX1277EF