



Assureon<sup>®</sup>  
Administration Guide

---

Version 8.3

Copyright © 2000-2020 Nexsan Technologies, Inc.. All Rights Reserved Worldwide. [www.nexsan.com](http://www.nexsan.com)

### **Trademarks**

Assureon® is a registered trademark of Nexsan Technologies, Inc.. SATABlade, SATABoy, SATABeast, Nexsan E60™, Nexsan E60X™, Nexsan E18™, and the Nexsan logo are trademarks or registered trademarks of Nexsan.

Microsoft, Microsoft Windows, Microsoft Internet Explorer, Microsoft SQL Server, and Microsoft Visual Studio .NET are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

### **Patents**

This product is protected by one or more of the following patents, and other pending patent applications worldwide:

United States patents US7,801,871, US8,086,578

United Kingdom patents GB2296798B, GB2297636B

### **About This Document**

Unauthorized use, duplication, or modification of this document in whole or in part without the written consent of Nexsan Technologies, Inc. is strictly prohibited.

Nexsan reserves the right to make changes to this manual, as well as the equipment and software described in this manual, at any time without notice. This manual may contain links to Web sites that were current at the time of publication, but have since been moved or become inactive. It may also contain links to sites owned and operated by third parties. Nexsan is not responsible for the content of any such third-party site.

# Contents

---

- Contents** ..... **iii**
  
- Chapter 1: Getting started** ..... **11**
  - Launching the System Administration Web interface ..... 12
  
- Chapter 2: Assureon system administration** ..... **15**
  - Overview of Assureon system administration ..... 16
    - File Systems, Organizations, and Watches ..... 16
  - Main menu ..... 18
  - Configuring the System ..... 19
  - System Administrator Web access ..... 20
  - Security options ..... 22
  - High-speed Assureon with RoCE ..... 23
  - Setting thresholds ..... 24
    - Setting thresholds for statistics gathering ..... 25
    - Setting disk capacity thresholds ..... 26
    - Setting thresholds for message queues ..... 27
    - Monitoring network connectivity ..... 28
    - Setting Assureon client thresholds ..... 29
    - Setting SQL jobs thresholds ..... 29
    - Setting CPU and memory thresholds ..... 31
    - Monitoring the folders for Organizations ..... 32
    - Setting the update interval for service monitoring ..... 33
    - Setting the Ingestion update interval ..... 33
    - Setting hardware monitoring thresholds ..... 33
  - Viewing the Assureon Server status ..... 35
    - Statistics panel ..... 36
    - Disks panel ..... 36
    - Queues panel ..... 36
    - Connectivity panel ..... 37
    - SQL Jobs panel ..... 37
    - CPU & Memory panel ..... 37
    - Folders panel ..... 37
    - Services panel ..... 37
    - Ingestion panel ..... 37

Hardware panel .....	37
Viewing overall system health .....	38
Clients .....	38
External storage .....	39
Monitoring the System State .....	40
About thresholds .....	41
Monitoring tasks .....	42
Monitoring Assureon Queues .....	42
Searching for and restoring files .....	44
Generating reports .....	47
Viewing space consumption, disposition details, and predictive analytics .....	48
Viewing client trends .....	49
Viewing summary and date-specific reports .....	49
Using the Access Control pages .....	52
Classifying archived files - Access Classification page .....	52
Configuring read access .....	53
Reviewing file access logs .....	56
Working with retention rules .....	58
Adding a retention rule .....	59
Using archive folders .....	61
Setting archive folder rules .....	61
Using archive folder templates .....	62
Using the Clients page .....	64
Running a client synchronization .....	66
Displaying client Information .....	66
Using the Assureon Services page .....	68
Managing services .....	68
Using the Archive Folders Editor .....	70
Tasks .....	71
Archive Folders .....	71
Archive Folders for .....	75
The Search Engine .....	76
The Indexing wizard .....	77
Using Watch variables .....	77
Unity Active Archive .....	81
Using the Events page .....	82
Working with event logs .....	82
Managing email alerts .....	83
Using the System Audit Trail .....	85
Managing disposition of files .....	87
Setting disposition overrides .....	87
Selecting files for disposition .....	89
Working with scheduled disposition jobs .....	91
Viewing disposition logs .....	92
Changing the disposition schedule .....	93
Scheduling disposition of excess file versions .....	94
Disposing of excess file versions manually .....	95
Using the Auditing page .....	96
Managing integrity audits .....	96
Using the Scheduled Audit Configuration wizard .....	98
Using the Manual Audit Configuration wizard .....	99
Viewing integrity audit logs .....	101

---

Viewing incomplete transaction logs .....	102
Configuring File Systems and Organizations .....	104
About Organizations and File Systems .....	107
Active-Active Plus configurations .....	107
Non-ASP model .....	107
ASP fully-hosted model .....	107
ASP DR model .....	108
Using the File System wizard .....	108
Applying Rollover settings .....	111
Advanced system administration tasks .....	114
Using the IIS Administration page .....	114
Certificate mapping .....	115
Virtual directory configuration .....	115
IIS administration .....	115
DNS records update .....	115
Using the Job Management page .....	115
Using the Storage Devices page .....	117
Using the Authorization Management page .....	117
Using the Organization Security page .....	118
Using the Options page .....	119
Using the Support page .....	121
Using Remote Desktop .....	121
Using CallHome .....	121
Logs .....	122
Upgrades .....	122
Contact Us .....	122
<b>Chapter 3: The Client Service .....</b>	<b>123</b>
Installing the Client Service .....	124
Client Service taskbar icon .....	126
Assureon client options .....	126
Secure File Transfers .....	128
Client Service For Laptops .....	128
Assureon property sheet .....	128
Low disk space warning .....	129
Archive folder icons .....	129
Safe Shortcuts .....	129
About Sparse Files .....	129
About Virtual Shortcuts .....	130
About the Filter Driver .....	130
About empty files .....	131
<b>Chapter 4: Assureon Explorer .....</b>	<b>133</b>
About Assureon Explorer .....	134
Restore options .....	135
Assureon Explorer command line .....	136
<b>Chapter 5: The File Synchronization utility .....</b>	<b>137</b>
File Synchronization dialog box .....	138
Starting a new file sync .....	139

Archiving Sync .....	140
Shortcutting - Safe Shortcuts .....	142
Reporting - View Sync Reports .....	143
Directory Security - Sync .....	145
Disposition - Delete disposed shortcuts .....	146
File Synchronization command line .....	148
Scheduling a synchronization process using the Windows Task Scheduler .....	148
Change Journal .....	149
File Sync Request Watcher .....	150
<b>Appendix A: Environment-specific configurations .....</b>	<b>153</b>
Using certificates for authentication .....	154
Installing a certificate .....	154
Exporting and mapping a new certificate .....	158
Configuring the client to use a certificate .....	161
Integration with Symantec EV .....	162
Creating an Assureon Archive partition .....	162
Installing Assureon Client Services .....	163
Creating an Archive folder .....	163
Scheduling a Sync .....	164
Security Certificate .....	164
ADAM security model .....	164
Mac OS character support .....	166
Opened firewall ports .....	166
Windows updates .....	167
Read files from site 2 .....	167
NFS access .....	168
Creating a UNIX mount point .....	170
<b>Appendix B: Advanced options .....</b>	<b>173</b>
Backing up with a replicated configuration .....	174
Assureon server outage .....	174
Shutting down or restarting Assureon .....	174
Store data protection .....	174
Time synchronization .....	175
Clustered NAS .....	175
Virtual Shortcuts with Clustered NAS .....	175
Database Transaction Log Shipping .....	175
NTFS security integration .....	176
Data Migration wizard .....	176
<b>Appendix C: System messages .....</b>	<b>177</b>
Disposition messages .....	178
Key Manager messages .....	179
Key Server proxy messages .....	180
Manifest Server messages .....	181
Object Request Broker messages .....	181
Storage Server messages .....	185
Storage Web Services messages .....	186
Restore Server messages .....	186

**Glossary** .....187

**Index** .....191





# About this document

This guide contains detailed information about the Assureon System Administration console, a Web-based portal used to manage and monitor the system and files stored within the system.

This guide assumes that Assureon is installed and that you have a user name and password to access the system administration console. Access to the system administration pages is controlled by security groups. The AssureonAdmin user has access to all the pages. Depending on your user, you may not have access to all the pages described in this guide. For more information, see [System Administrator Web access on page 20](#).

## Audience

This guide has been prepared for the following audience:

- IT system administrators
- Engineers
- Technicians

## Conventions

Here is a list of text conventions used in this document:

Convention	Description
<u>underlined blue</u>	Cross-references, hyperlinks, URLs, and email addresses.
<b>boldface</b>	Text that refers to labels on the physical unit or interactive items in the graphical user interface (GUI).
monospace	Text that is displayed in the command-line interface (CLI) or text that refers to file or directory names.
<b>monospace bold</b>	Text strings that must be entered by the user in the command-line interface or in text fields in the graphical user interface (GUI).
<i>italics</i>	System messages and non-interactive items in the graphical user interface (GUI) References to Software User Guides

## Notes, Tips, Cautions, and Warnings

**Note** Notes contain important information, present alternative procedures, or call attention to certain items.

**Tip** Tips contain handy information for end-users, such as other ways to perform an action.



**CAUTION:** In hardware manuals, cautions alert the user to items or situations which may cause damage to the unit or result in mild injury to the user, or both. In software manuals, cautions alert the user to situations which may cause data corruption or data loss.



**WARNING:** Warnings alert the user to items or situations which may result in severe injury or death to the user.

## Contacting Nexsan

For questions about Nexsan products, please visit the [Nexsan support](#) Web page, and the Nexsan Assureon [Documents and Downloads](#) page. If you are unable to find the answer to your question there, please see our contact information below.

## Service and support

Nexsan's Technical Services Group provides worldwide assistance with installation, configuration, software support, warranty, and repair for all Nexsan products. A variety of service and support programs are available to provide you with the level of coverage and availability your operation requires.

Nexsan Assureon Documents & Downloads page:

[https://helper.nexsansupport.com/asu\\_downloads.html](https://helper.nexsansupport.com/asu_downloads.html)

Contact Nexsan Assureon support:

[https://helper.nexsansupport.com/asu\\_support](https://helper.nexsansupport.com/asu_support)

Worldwide Web site:

[www.nexsan.com](http://www.nexsan.com)

# Chapter 1

## Getting started

---

The section provides information about these topics:

[Launching the System Administration Web interface](#) .....12

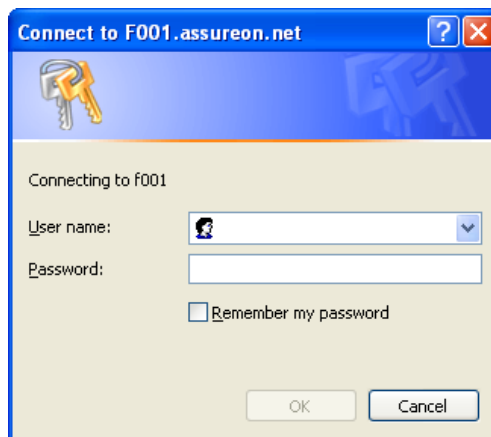
## Launching the System Administration Web interface

After Assureon has been installed, you can access the Assureon System Administration main menu using Internet Explorer.

► **To access the main menu:**

1. Launch Internet Explorer from any server on the local network or from the server.

Figure 1-1: Connect to Assureon dialog box



2. Type the Web address where the system has been installed:

`http://<IP of F001 Assureon server>` or

`http://<fully qualified Assureon server name>`

- Specify the user name and password provided to you by your Assureon technician. For the user name, be sure to prefix it with the domain name (for example: ASU123456\AssureonAdmin).

Figure 1-2: System State page and the main menu

The screenshot displays the Nexsan Assureon interface. At the top, the 'System State' tab is active, with 'Thresholds' and 'Tasks' also visible. The main menu on the left includes sections for Files, Configuration, and Administration, with sub-items like Search and Restore, Reports, Access Control, Retention, Archive Folders, Clients, Services, Events, Disposition, Auditing, File Systems, Advanced, and Support. The central dashboard features a status bar with 'Assureon' (red X), 'Clients' (green check), and 'External Storage' (red X). Below this is a table with columns for State, Domain, CPU & Memory, Disks, Folders, Queues, Services, Connectivity, Ingestion, SQL Jobs, and Hardware. The table lists two states: F001-117117 and F002-117117, both with a red X in the State column. To the right of the table are several monitoring panels: Statistics (showing file processing and transactions for Assureon, Org01, and Org02), CPU & Memory (showing usage for F001 and F002), Folders, Services (showing Assureon Events Manager as Stopped), Ingestion (showing F001 and F002 as Enabled), and Hardware (showing DIMM, Disk, and Fan status as Ok).

State	Domain	CPU & Memory	Disks	Folders	Queues	Services	Connectivity	Ingestion	SQL Jobs	Hardware
✖ F001-117117	ASU117117	✔	✔	✔	✔	✖	✖	✔	✔	✔
✖ F002-117117	ASU117117	✔	✔	✔	✔	✔	✖	✔	✔	✔



# Chapter 2

## Assureon system administration

---

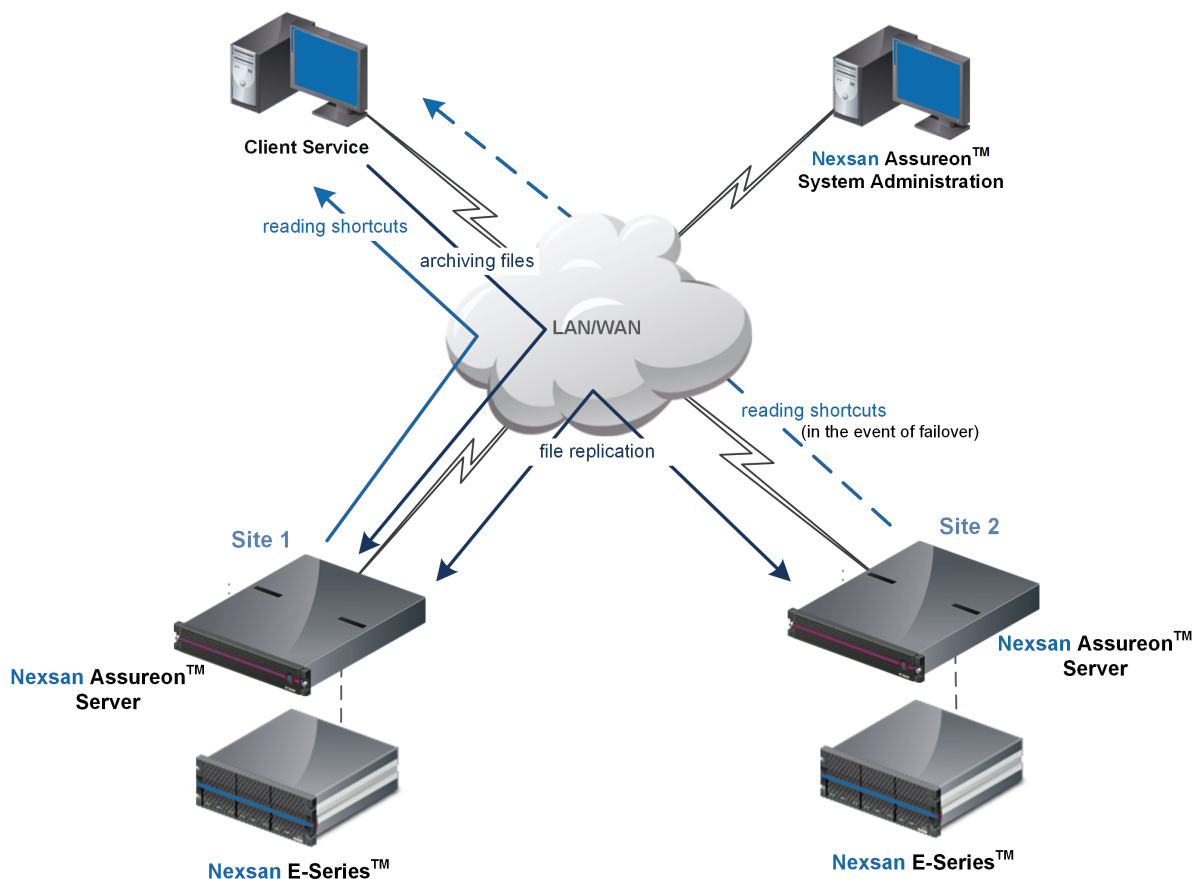
This section provides information about these topics:

Overview of Assureon system administration .....	16
Main menu .....	18
Configuring the System .....	19
System Administrator Web access .....	20
Security options .....	22
High-speed Assureon with RoCE .....	23
Setting thresholds .....	24
Viewing the Assureon Server status .....	35
Monitoring the System State .....	40
Searching for and restoring files .....	44
Generating reports .....	47
Using the Access Control pages .....	52
Working with retention rules .....	58
Using archive folders .....	61
Using the Clients page .....	64
Using the Assureon Services page .....	68
Using the Archive Folders Editor .....	70
Using the Events page .....	82
Managing disposition of files .....	87
Using the Auditing page .....	96
Configuring File Systems and Organizations .....	104
Advanced system administration tasks .....	114
Using the Support page .....	121

## Overview of Assureon system administration

Nexsan Assureon is a secure storage software system for the storage and retrieval of files. Assureon protects important data for extended periods of time, ensuring that files are secured, never get corrupted, and are not deleted prematurely. Assureon has two major components, both of which are managed using the Assureon System Administration user interface:

- **Assureon Client Services:** A set of services responsible for policy-based archiving of data to Assureon, as well as reading and restoring files and shortcuts from Assureon. The Client Services are installed on a dedicated server and configured to monitor a directory, or group of directories, called an archive folder. Any changes made to a file in an archive folder will trigger selection and processing rules. Selected files are sent to the Assureon Server.
- **Assureon Server:** This component contains the servers with the life cycle management services that handle the encryption, storage, access control and disposition of files. The Assureon Server is delivered pre-installed with a pre-selected storage device.



## File Systems, Organizations, and Watches

Assureon supports multiple archives, referred to as File Systems, and multiple Organizations (collections of file systems).

An organization is a group of one or more file systems which share retention rules, access classifications and reports. Searching, restoring, auditing and disposition of files is also organization-based. An Assureon cluster may have more than one organization, but each is strictly independent. This independence allows Assureon Plus (multiple site) configurations to be used in ASP configurations, which are described below.



A file system consists of a database, storage location (the stores), manifest and audit files as well as replication options. Think of it as a self-contained archive that shares properties with the other file systems within an organization.

You create watches to serve as rules that monitor changes to files based on folders, organization, and retention rules, updating the file system (archive) as required.

## Main menu

The main menu, displayed to the left of all System Administration console pages, contains the following sub-menus:

### Files

- **Search and Restore** – Searches and retrieves files based on selection criteria
- **Reports** – Displays management and technical reports
- **Access Control**

### Configuration

- **Access Control** – Creates classifications for access and management purposes
- **Retention** – Creates retention rules for the archived files
- **Archive Folders** – Specifies file archiving rules for the archive folders

### Administration

- **Clients** – Displays the status of installed Client Services and monitors file transfers
- **Services** – Starts and Stops services across the servers
- **Events** – Displays events sent to the Assureon and SQL Server event logs in a centralized location
- **Disposition** – Sets disposition selection, schedule, override, version control and displays the access log
- **Auditing** – Displays audit integrity and incomplete transaction log information
- **File Systems** – Manages organizations and file systems
- **Advanced** – Displays Monthly Roll, Job Management, Firewall, Storage Devices, IIS Administration, Authentication Management and Organization Security pages
- **Support** – Displays remote desktop configurations, logs upload configurations, software updates, and Nexsan contact information.

**Note** Other users can be configured to access all or part of the Assureon System Administration menus and be restricted to specific organizations; see [Console Access](#) for details.

## Configuring the System

► **Before you start configuring your system, verify that it is up-and-running:**

1. Use the [System State](#) page to check on the overall health of the system.
2. Use the [Events](#) page to make sure that the system is not reporting any problems. You can also configure the system to email you events.

► **To configure the system for archiving:**

Before you can use the system to store files, there must be an organization and a file system configured. Typically, your system will come pre-configured and ready to use, but you may make changes to the configuration, create retention rules, access classifications and archive folders. You will also need to install the Client Service on the computers from which files will be taken.

- Use the [File System wizard](#) to create a new [organization](#) and file system.
- Use the [Retention Rules](#) page to create retention rules based on policy. Retention rules define how long a file is kept and whether it is stored in encrypted or compressed form.
- Use the [Access Classification](#) page to specify how stored files will be classified. Classifications are used to access and manage archived files.
- Use the [Archive Folders Configuration](#) and the [Archive Folders Editor](#) pages to create archive folders for computers. Files copied or created in archive folders are selected and processed according to retention rules and classifications.
- [Install the Client Service](#) on the computers.

► **To configure email alerts:**

During the initial set-up process, configure email alerts to receive messages related to the system. Use the [Email Alerts](#) page to set and manage your alerts. It is strongly recommended to:

- Enable the Daily Summary email.
- Enable the System State Alert email for errors. Set it to send email alerts for errors that persist for roughly more than 60 minutes.

► **To configure the system for file disposition:**

After an archived file has passed its expiration date (as specified by the retention rule), it becomes a candidate for disposition. Disposition refers to the act of deleting a file from storage. Expired files are not automatically deleted from storage, they must first be selected using the [Disposition Selection](#) page. Disposition occurs according to the disposition schedule and because it is a CPU and IO intensive process, it should be scheduled for off-peak periods. To configure the disposition time:

- Use the [Disposition Schedule](#) page to verify or modify the disposition schedule.

► **To configure the system for file retrieval:**

Stored files can be retrieved using a variety of methods, depending on company policy. Users using computers with archive folders may be able to retrieve files using shortcuts or [Assureon Explorer](#). Administrators and authorized users can retrieve individual files or groups of files, using the [Restore Files](#).

For more information about file retrieval, see [Classifying archived files - Access Classification page on page 52](#).

## System Administrator Web access

Access to the Assureon System Administration pages (and to the [Assureon Property Sheet](#)) is controlled through security groups in Active Directory or ADAM. At installation, the following **Users** security groups are created in the Active Directory of the Assureon Server. Access to System Administration pages is controlled by membership to these groups. For example, users added to the ILM Enterprise Administrators group have access to all pages, while users in ILM Users can restore files but not run dispositions. For details, see the table included below.

**Note** Users added to these groups have access to **all** organizations.

In order of hierarchy (access to all system administration pages to only a few), the groups are:

- ILM Enterprise Administrators
- ILM Domain Administrators
- ILM Enterprise Operators
- ILM Domain Operators
- ILM Domain Users
- ILM Users

In addition, when an **organization** is created, organization-specific **FSOrganizations** security groups are created in the Active Directory of the Assureon Server. Like the Users security groups, access to System Administration pages is controlled by membership to a group. At this level, not all System Administration pages are available. For example, the Services page is not available, even to ILM Enterprise Administrators.

Users added to these groups **only have access to their** organizations. For example, in FSOrganizations:

- org1.ILM Enterprise Administrators
- org1.ILM Domain Administrators
- org1.ILM Enterprise Operators
- org1.ILM Domain Operators
- org1.ILM Domain Users
- org1.ILM Users

To add users to security groups, use the Windows Active Directory Users and Computers dialog box (accessed by clicking Start, Control Panel, then Administrative Tools)

**Note** When a user is added to a security group (at the Users or FSOrganizations levels), the Assureon System Administration user interface, [Authorization Management](#) page, the **Reset** option must be used to refresh the Assureon Authorization Manager with the new information.

AssureonManager and AssureonAdmin are automatically added to the **Users** ILM Enterprise Administrator and ILM Domain Administrator groups.

**Note** In order for ILM Domain Administrator and the ILM Domain Operator users to be able to add subclassifications, they must also be added as members of the classification-based security group. See [Access Classification](#) for more information.

► **Example:**

If you want user sam.carter to be able to restore files (and not be able to do anything else via the System Administration UI) from organization org1\_Fiscal2009 (and not from any other available organizations), then add the user to the Active Directory, FSOrganizations, Org1\_Fiscal2009, Org1\_Fiscal2009. ILM Users group

and then click the Reset option on the [Authorization Management](#) page. When the user accesses the user interface using their credentials, only the Restore Files and Search menu options will be available for org1\_Fiscal2009.

The following table describes the system administration pages that can be accessed per security group. Pages marked in red are NOT available to users in the FSOrganizations security group.

Administration Interface Page	ILM Enterprise Administrators	ILM Domain Administrators	ILM Enterprise Operators	ILM Domain Operators	ILM Domain Users	ILM Users
System State	x		x	x		
Restore Files	x				x	x
Search	x	x			x	x
Reports	x	x	x	x		
Access Control: Add Classifications	x	x	x	x		
Access Control: Read Access, Access Log	x		x	x		
Retention	x	x	x	x		
Archive folders	x		x	x		
Clients	x		x	x		
Services	x	x				
Events	x	x				
Disposition: Override, Selection, Scheduled Jobs	x	x				
Disposition: <b>Schedule</b> , Log, Version Control	x					
Auditing	x					
<b>File Systems</b>	x	x				
<b>Advanced</b>	x					
<b>Advanced: Authorization Management</b>	x	x				

## Security options

Assureon may be configured to use the following security models:

- [Anonymous](#)
- [Trust \(with Assureon Access Classifications\)](#)
- [Trust \(with NTFS security integration\)](#)
- [Digital certificate](#)
- [ADAM](#)

The security options are typically configured during the installation process or by an on-site installer. To change the security options, please contact Nexsan Support.

### ***Anonymous***

The anonymous access security model has the following features:

- ADAM, a trust relationship to the corporate domain or digital certificates are not required.
- Access to files is controlled using NTFS permissions.
- Full access to the system administration UI is limited to the Assureon Admin user; access to the system administration restore and search options is open to everyone.

This option is not recommended because access to archived files is open to everyone.

For more information about configuring Assureon for use with this security model, please contact [Nexsan Support](#).

### ***Trust (with Assureon Access Classifications)***

For the trust model using access classifications, a one-way outgoing Windows trust relationship is established between the Assureon and the corporate domain. The trust is also used to define the FSWManager user, used to run the Assureon Client Service installed on user servers.

This is the recommended security option, as it has the following advantages:

- Enhanced security and the existing security infrastructure can be used.
- Access to files is controlled using organization and classification-based AD security groups (and optionally NTFS).
- Access to the system administration UI is controlled using Assureon domain AD security.

For more information about configuring Assureon for use with this security model, please contact [Nexsan Support](#).

### ***Trust (with NTFS security integration)***

For the trust model using NTFS security integration, a two-way Windows trust relationship is established between the Assureon and the corporate domain. This security model may be used instead of, or in conjunction with, Assureon Access Classifications.

This is another recommended security option, as it has the following advantages:

- Enhanced security and the existing security infrastructure can be used.
- Access to files is controlled using established NTFS folder permissions.

- Access to the system administration UI, Restore Files and Search pages is automatically granted; Users can only view and restore their own files. Full access to the system administration UI is controlled using Assureon domain AD security.
- Security is set per client computer and enabled using the Assureon System Administration [Client Information dialog box](#).
- Once enabled for a computer, the archive folders for that computer must be configured (with the [Archive Folder Editor page](#)) to use the model with the [Real-time](#) or [Sync Folder Security](#) options.

For more information about configuring Assureon for use with this security model, please contact [Nexsan Support](#).

### **Digital certificate**

The digital certificate security model relies on certificates to ensure authentication. Certificates are issued from the Certification Authority installed on the Assureon server to Assureon clients. Only clients with the right certificate are allowed access to files. This option is intended for customers who want greater security and who do not have a corporate Active Directory domain server or ADAM installed.

Access to files and to the System Administration UI is controlled using certificates mapped to Assureon active directory security groups.

For more information about configuring Assureon for use with this security model, please see [Using certificates for authentication](#).

### **ADAM**

The ADAM (Active Directory Application Mode) security model allows customers who do not have a trust relationship between their corporate and Assureon servers to manage user security.

Access to files and to the System Administration UI is controlled by ADAM and Assureon AD security.

For more information about this model, please see [ADAM Security Model](#).

## **High-speed Assureon with RoCE**

Assureon 8.3 introduces support for an optional high-speed, end-to-end RoCE (RDMA over Converged Ethernet) implementation that delivers blazing-fast 40GbE read functionality for virtual shortcuts.

Using high-speed Assureon with RoCE, you can now configure an Assureon Edge to replace files archived to Assureon with virtual shortcuts—instead of physical shortcuts or stubs. Virtual shortcuts over RoCE consume no disk space on the Assureon Edge server and reside purely in memory as reference points to the files in Assureon. When a user or application reads a virtual shortcut on the Assureon Edge/client, the corresponding file is instantaneously retrieved from the Assureon archive and presented to the user or application as if it was the actual file. This retrieval is achieved using RDMA (Remote Directory Memory Access) over a 40Gb/s Converged Ethernet (RoCE) connection between the Assureon server and Assureon Edge/client.

When you purchase high-speed Assureon with RoCE, you get a complete end-to-end solution for your data protection and archival needs, including RDMA-enabled Network Interface Cards (NICs) on the Assureon server and all Edge/client servers, as well as an optionally available 100Gb/s Ethernet Switch System for larger deployments.

For more information about High-speed Assureon with RoCE, please contact your Nexsan Account Representative.

## Setting thresholds

Use this topic for instructions about setting thresholds. In addition to specific configuration settings, for each threshold, you can configure whether to send email alerts when a threshold is reached or exceeded, and specify whether to ignore error and warning messages.

Setting thresholds for statistics gathering .....	25
Setting disk capacity thresholds .....	26
Setting thresholds for message queues .....	27
Monitoring network connectivity .....	28
Setting Assureon client thresholds .....	29
Setting SQL jobs thresholds .....	29
Setting CPU and memory thresholds .....	31
Monitoring the folders for Organizations .....	32
Setting the update interval for service monitoring .....	33
Setting the Ingestion update interval .....	33
Setting hardware monitoring thresholds .....	33

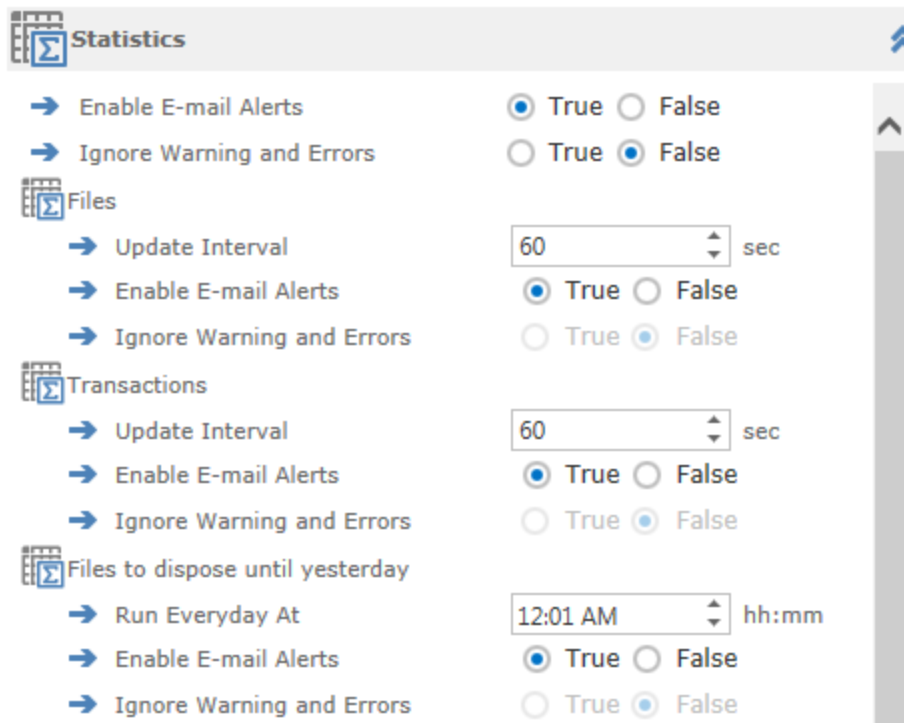


## Setting thresholds for statistics gathering

Use the Statistics panel to configure the following thresholds:

- **Files** – The total number of unique files archived on Assureon.
- **Transactions** – The total number of files sent to Assureon for processing.
- **Files to dispose until yesterday** – The number of expired files as of midnight.
- **Files processed yesterday** – The number of files processed the previous day.
- **Files processed in the last hour** – The number of files processed on Assureon in the last hour (give or take 10 minutes).
- **Files read since** – The number of files read or restored since the specified day and hour.
- **Safe shortcuts to create** – The number of safe shortcuts to create.

Figure 2-1: Thresholds tab—Statistics panel



### ► To configure threshold parameters on the Statistics panel:

1. For each applicable threshold, specify the **Update Interval**, in seconds, when you want the system to monitor the corresponding threshold. For example, to monitor the number of transactions sent to Assureon for processing every 60 seconds, specify 60 for the Transactions Update Interval.
2. For each applicable threshold, specify the time, in the **Run Everyday At** field, at which you want the system to process the threshold each day.
3. For each threshold, set the **Enable E-mail Alerts** and/or **Ignore Warning and Errors** options to **True** or **False**. For these options to be enabled, you must first set the global **Enable E-mail Alerts** and **Ignore Warning and Errors** options to **True**, at the top of the Statistics panel.
4. Click **Save**.

► **To enable the Enable E-mail Alerts or Ignore Warning and Errors options for all thresholds in the Statistics panel:**

1. Set the **Enable E-mail Alerts** option at the top of the Statistics panel to **True**.
2. Set the **Ignore Warning and Errors** option at the top of the Statistics panel to **True**.
3. Click **Save**.

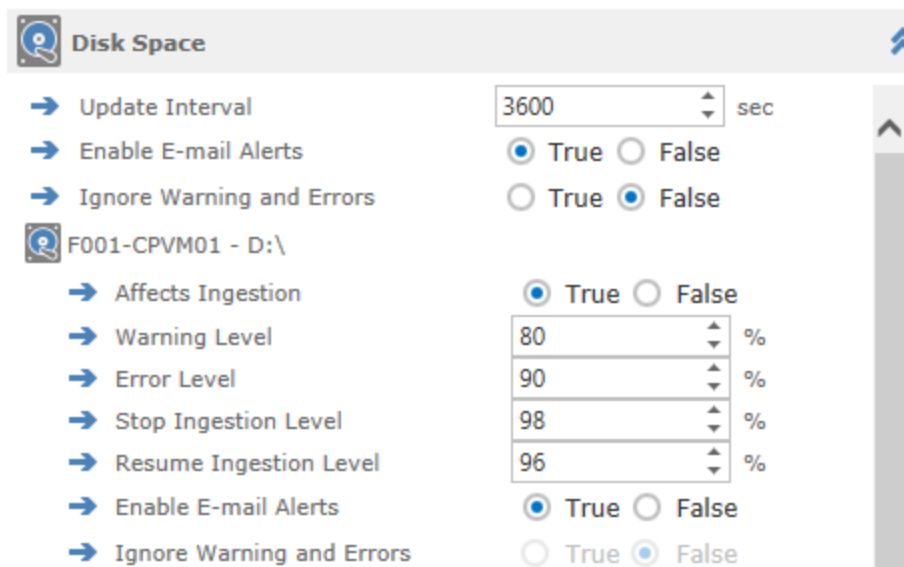
► **To disable the E-mail Alerts or Ignore Warning and Errors options for all thresholds in the Statistics panel:**

1. Set the **Enable E-mail Alerts** option at the top of the Statistics panel to **False**. The corresponding option for each threshold is disabled.
2. Set the **Ignore Warning and Errors** option at the top of the Statistics panel to **False**. The corresponding option for each threshold is disabled.
3. Click **Save**.

## Setting disk capacity thresholds

Use the Disk Space panel to set various disk capacity thresholds for each disk or volume associated with the system.

Figure 2-2: Thresholds tab—Disk Space panel



► **To configure disk capacity threshold parameters on the Disk Space panel:**

1. For each volume or disk, specify whether or not the thresholds for that volume affect File Ingestion on it, by setting the relevant **Affects Ingestion** option to **True** or **False**.
2. For each volume's threshold, specify the desired threshold level in percentage of disk capacity. For example, if you want the system to stop file ingestion on volume `F : \` when its disk capacity reaches 95%, set the **Stop Ingestion Level** threshold for volume `F : \` to 95%, as applicable.
3. For each volume, set the **Enable E-mail Alerts** and/or **Ignore Warning and Errors** options to **True** or **False**. For these options to be enabled, you must first set the global **Enable E-mail Alerts** and **Ignore Warning and Errors** options to **True**, at the top of the Disk Space panel, as described below.
4. Click **Save**.

- ▶ **To enable the Enable E-mail Alerts or Ignore Warning and Errors options for all thresholds in the Disk Space panel:**
  1. Set the **Enable E-mail Alerts** option at the top of the Disk Space panel to **True**.
  2. Set the **Ignore Warning and Errors** option at the top of the Disk Space panel to **True**.
  3. Click **Save**.
- ▶ **To disable the E-mail Alerts or Ignore Warning and Errors options for all thresholds in the Disk Space panel:**
  1. Set the **Enable E-mail Alerts** option at the top of the Disk Space panel to **False**. The corresponding option for each threshold is disabled.
  2. Set the **Ignore Warning and Errors** option at the top of the Disk Space panel to **False**. The corresponding option for each threshold is disabled.

## Setting thresholds for message queues

Use the Queue panel to configure thresholds for Assureon message queues. For more information about queues, see [Monitoring Assureon Queues on page 42](#).

All message queue thresholds have a global Update Interval, at the top of the Queues panel. Specify the interval, in seconds, when you want the system to monitor all thresholds.

Figure 2-3: Thresholds tab—Queues panel

The screenshot shows the 'Queues' configuration panel. It is organized into sections with expandable/collapsible arrows on the left. The top section is for global settings: 'Update Interval' is a numeric input field with '3600' and 'sec' units; 'Enable E-mail Alerts' has a radio button selected for 'True'; 'Ignore Warning and Errors' has a radio button selected for 'False'. Below are three queue-specific sections: 'auditQueue', 'cachenotification', and another unnamed section. Each of these sections has 'Warning Level' and 'Error Level' as numeric input fields (both set to 10000 and 50000 respectively, with 'msgs' units), and 'Enable E-mail Alerts' and 'Ignore Warning and Errors' as radio button options. In the 'auditQueue' and 'cachenotification' sections, 'Enable E-mail Alerts' is set to 'True' and 'Ignore Warning and Errors' is set to 'False'.

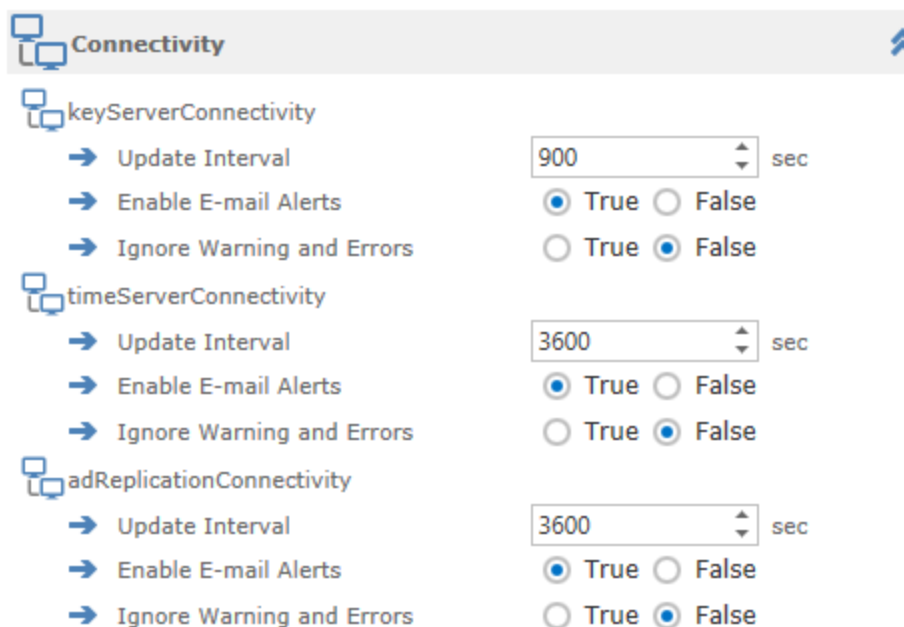
- ▶ **To configure message queues thresholds on the Queues panel:**
  1. For each message queue, specify the desired threshold levels, in the number of messages, when the system generates warnings and errors. For example, if you want the system to generate warning messages when the dispositionqueue reaches a threshold of 10000 messages, set the Warning Level threshold for the dispositionqueue threshold to 10000.

2. For each message queue, set the Enable E-mail Alerts and/or Ignore Warning and Errors options to True or False. For these options to be enabled, you must first set the global Enable E-mail Alerts and Ignore Warning and Errors options to True, at the top of the Queues panel.
  3. Click Save.
- **To enable the Enable E-mail Alerts or Ignore Warning and Errors options for all thresholds in the Queues panel:**
1. Set the Enable E-mail Alerts option at the top of the Queues panel to True.
  2. Set the Ignore Warning and Errors option at the top of the Queues panel to True.
  3. Click Save.
- **To disable the E-mail Alerts or Ignore Warning and Errors options for all thresholds in the Queues panel:**
1. Set the Enable E-mail Alerts option at the top of the Queues panel to False. The corresponding option for each threshold is disabled.
  2. Set the Ignore Warning and Errors option at the top of the Queues panel to False. The corresponding option for each threshold is disabled.
  3. Click Save.

## Monitoring network connectivity

Use the Connectivity panel to configure thresholds that monitor network connectivity status from the server to other Assureon components, including the Key Server, Time Server, Windows Update Server, and so on.

Figure 2-4: Thresholds tab—Connectivity panel



- **To configure threshold parameters on the Connectivity panel:**
1. For each threshold, specify the **Update Interval**, in seconds, when you want the system to monitor the corresponding threshold. For example, to monitor connectivity to the Assureon Key Server every hour, specify 3600 for the `keyServerConnectivity` threshold.

- For each threshold, set the **Enable E-mail Alerts** and/or **Ignore Warning and Errors** options to **True** or **False**.
- Click **Save**.

## Setting Assureon client thresholds

Use the Clients panel to configure threshold parameters for each Assureon Client associated with the Assureon server.

Figure 2-5: Thresholds tab—Clients panel

The screenshot shows the 'Clients' panel in the Assureon interface. It lists two clients with their respective configuration options:

- ASUCPVM01\F001-CPVM01**
  - Enable E-mail Alerts:  True  False
  - Ignore Warning and Errors:  True  False
  - Minimum Files: 0 (Files)
  - Minimum Bytes: 0 (Bytes)
  - Days of Week: Su,M,T,W,Th,F,S
  - Enable E-mail Alerts:  True  False
  - Ignore Warning and Errors:  True  False
- CIMAT\EDGE**
  - Minimum Files: 0 (Files)
  - Minimum Bytes: 0 (Bytes)
  - Days of Week: Su,M,T,W,Th,F,S
  - Enable E-mail Alerts:  True  False
  - Ignore Warning and Errors:  True  False

### ► To configure threshold parameters on the Clients panel:

- For each threshold, specify the threshold values for Minimum Files and Minimum Bytes at which threshold-level messages are generated by the system.
- For each threshold, specify days of week when you want the system to process the threshold; enter values in this format, using commas: Su,M,T,W,Th,F,S.
- For each threshold, set the Enable E-mail Alerts and/or Ignore Warning and Errors options to True or False.
- Click Save.

## Setting SQL jobs thresholds

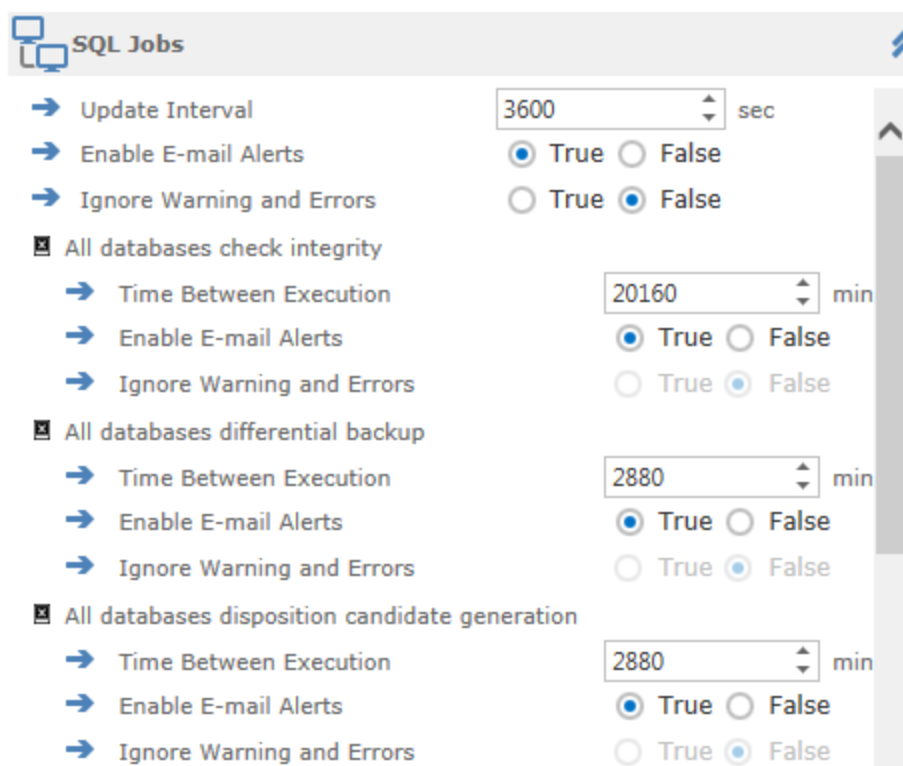
The SQL Jobs panel to configure thresholds that monitor the SQL jobs that are run against the Assureon database. You can verify if the SQL jobs that should be running have executed successfully in the [System State—Assureon](#) page.

The SQL Jobs panel enables you to configure the following thresholds:

- All databases check integrity** – Verifies there is no data corruption on the databases.
- All databases differential backup** – Performs a backup of the data that changed since the last backup.

- **All databases disposition candidate generation** – Generates a list of expired files that can be expired from the SysAdmin.
- **All databases file shrink** – Reduces the size of database files.
- **All databases full backup** – Performs an entire backup of all databases.
- **All databases log backup** – Performs a backup of all event logs for all databases.
- **Report New - CAS Base Generation** – Creates a report that describes data stored in Assureon. This is the baseline report from which the incremental reports will be generated.
- **Report New - CAS Incremental and Decremental** – Updates the baseline with the changes that have occurred since the last incremental report.
- **Report New - CAS Report Data Generation** – Generates the final aggregated reports for customers.

Figure 2-6: Thresholds tab—SQL Jobs panel



- ▶ **To set the update interval for all thresholds in the SQL Jobs panel:**
  - Specify the **Update Interval**, in seconds.
- ▶ **To enable the Enable E-mail Alerts or Ignore Warning and Errors options for all thresholds in the SQL Jobs panel:**
  1. Set the **Enable E-mail Alerts** option at the top of the Disk Space panel to **True**.
  2. Set the **Ignore Warning and Errors** option at the top of the Disk Space panel to **True**.
  3. Click **Save**.

► **To disable the E-mail Alerts or Ignore Warning and Errors options for all thresholds in the SQL Jobs panel:**

1. Set the **Enable E-mail Alerts** option at the top of the Disk Space panel to **False**. The corresponding option for each threshold is disabled.
2. Set the **Ignore Warning and Errors** option at the top of the Disk Space panel to **False**. The corresponding option for each threshold is disabled.
3. Click **Save**.

► **To configure threshold parameters for each threshold:**

1. Specify the **Time Between Execution**, in minutes, when you want the system to wait until the SQL job has completed before starting another one.
2. For each threshold, set the **Enable E-mail Alerts** and/or **Ignore Warning and Errors** options to **True** or **False**.
3. Click **Save**.

## Setting CPU and memory thresholds

Use the CPU and Memory panels to set thresholds for the percentage of CPU and memory consumed by the Assureon server.

Figure 2-7: CPU and Memory panels

The image shows two configuration panels: CPU and Memory. Each panel has a title bar with an icon and an upward arrow. Below the title bar are five settings, each with a right-pointing arrow icon to its left. The settings are: Update Interval (60 sec), Warning Level (98%), Error Level (99%), Enable E-mail Alerts (True), and Ignore Warning and Errors (False). The radio buttons for 'True' and 'False' are visible for the last two settings.

Setting	Value	Unit
Update Interval	60	sec
Warning Level	98	%
Error Level	99	%
Enable E-mail Alerts	<input checked="" type="radio"/> True <input type="radio"/> False	
Ignore Warning and Errors	<input type="radio"/> True <input checked="" type="radio"/> False	

► **To configure threshold parameters on the CPU and Memory panels:**

1. For each threshold, specify the **Update Interval**, in seconds, when you want the system to monitor the corresponding threshold.

For example, to monitor CPU usage every 60 seconds, specify 60 for the Update Interval on the CPU panel.

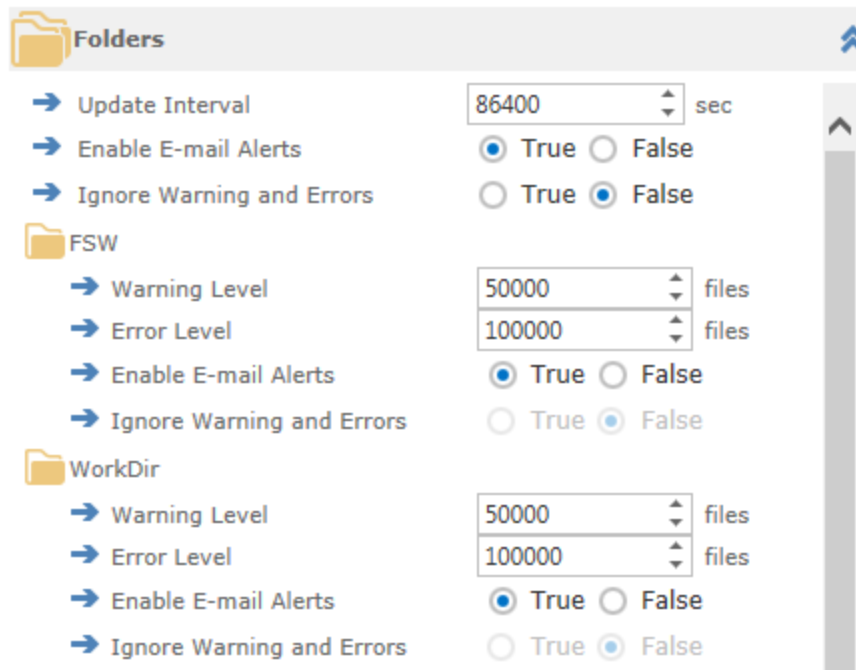
- For each threshold, specify the desired **Warning** and **Error**-level thresholds in percentage of CPU or memory capacity, as applicable.  
For example, if you want the system to generate warnings when CPU usage reaches 60%, set the CPU Warning Level threshold 60%.
- For each threshold, set the **Enable E-mail Alerts** and/or **Ignore Warning and Errors** options to **True** or **False**.
- Click **Save**.

## Monitoring the folders for Organizations

Use the Folders panel to configure thresholds to monitor the total number of files in Assureon folders for each Organization.

All folder thresholds have a global Update Interval, at the top of the Folders panel. Specify the interval, in seconds, when you want the system to monitor all thresholds.

Figure 2-8: Thresholds tab—Folders panel



### ► To configure folder thresholds:

- For each folder, specify the desired threshold levels, in the number of files, when the system generates warnings and errors. For example, if you want the system to generate warning messages when the FSW folder reaches a threshold of 10000 files, set the Warning Level threshold for the folder to 10000.
- For each folder, set the **Enable E-mail Alerts** and/or **Ignore Warning and Errors** options to **True** or **False**. For these options to be enabled, you must first set the global **Enable E-mail Alerts** and **Ignore Warning and Errors** options to **True**, at the top of the Folders panel.
- Click **Save**.

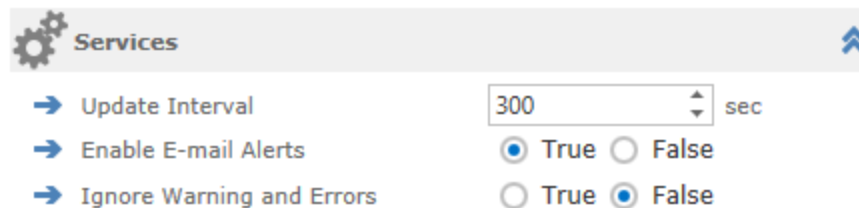


- ▶ **To enable the Enable E-mail Alerts or Ignore Warning and Errors options for all folders in the Folders panel:**
  1. Set the **Enable E-mail Alerts** option at the top of the Folders panel to **True**.
  2. Set the **Ignore Warning and Errors** option at the top of the Folders panel to **True**.
  3. Click **Save**.
- ▶ **To disable the E-mail Alerts or Ignore Warning and Errors options for all folders in the Folders panel:**
  1. Set the **Enable E-mail Alerts** option at the top of the Folders panel to **False**. The corresponding option for each threshold is disabled.
  2. Set the **Ignore Warning and Errors** option at the top of the Folders panel to **False**. The corresponding option for each threshold is disabled.

## Setting the update interval for service monitoring

Use the Services panel to configure the update interval when you want the system to monitor services. You can also enable the Enable E-mail Alerts and Ignore Warning and Errors options for services-related messages.

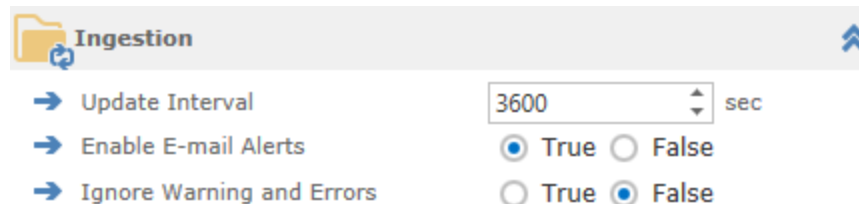
Figure 2-9: Thresholds tab—Services panel



## Setting the Ingestion update interval

Use the Ingestion panel to configure the Update Interval when you want the system to monitor Ingestion tasks. You can also specify the Enable E-mail Alerts and Ignore Warning and Errors options for Ingestion-related messages.

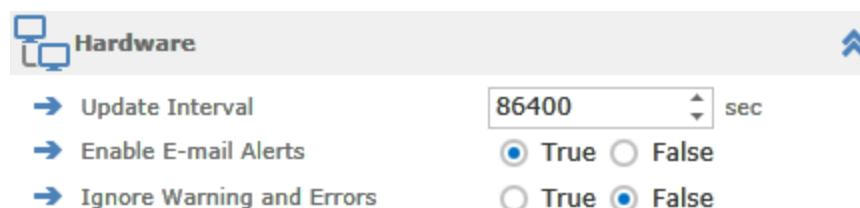
Figure 2-10: Thresholds tab—Ingestion panel



## Setting hardware monitoring thresholds

Use the Hardware panel to configure thresholds to monitor the hardware components for each Assureon server.

Figure 2-11: Thresholds tab—Hardware panel



- ▶ **To set the update interval for all hardware components in the SQL Jobs panel:**
  - Specify the **Update Interval**, in seconds.
- ▶ **To enable the Enable E-mail Alerts or Ignore Warning and Errors options for all hardware components:**
  1. Set the **Enable E-mail Alerts** option at the top of the Folders panel to **True**.
  2. Set the **Ignore Warning and Errors** option at the top of the Folders panel to **True**.
  3. Click **Save**.
- ▶ **To disable the E-mail Alerts or Ignore Warning and Errors options for all hardware components:**
  1. Set the **Enable E-mail Alerts** option at the top of the Folders panel to **False**. The corresponding option for each threshold is disabled.
  2. Set the **Ignore Warning and Errors** option at the top of the Folders panel to **False**. The corresponding option for each threshold is disabled.

## Viewing the Assureon Server status

The **Assureon** link displays the system state of the Assureon servers. The first section under this link displays a summary of component state per server, while the bottom displays details per component. The top section table contains information about system components per Assureon server. A green check mark indicates that everything is good. A yellow icon (warning) indicates a potential problem that needs to be investigated. A red icon (error) indicates a problem that needs to be addressed. To view additional details, click on an icon in the table.

Email alerts may be configured for warnings and errors. See the [Email Alerts](#) page for details.

The **System State** page will automatically refresh every 10 seconds. To refresh the page manually, click the refresh icon, located in the upper-right corner of the page.

**Note** The automatic and manual page refresh timers do not update the **Statistics** panel, which has its own refresh option (see below). Also, some counters are set on individual timers and are not affected by the refresh.

If required, the page refresh rate may be customized. To do so, contact Assureon [customer support](#) for details.

Figure 2-12: System State page – Assureon servers

The screenshot shows the 'System State' page in the Assureon interface. At the top, there are tabs for 'Files', 'System State', 'Thresholds', and 'Tasks'. Below the tabs, there are navigation links for 'Search and Restore', 'Reports', 'Configuration', and 'Administration'. The main content area is divided into several sections:

- System State Summary Table:**

State	Domain	CPU & Memory	Disks	Folders	Queues	Services	Connectivity	Ingestion	SQL Jobs	Hardware
✖ F001-117117	ASU117117	✓	✓	✓	✓	✖	✖	✓	✓	✓
✖ F002-117117	ASU117117	✓	✓	✓	✓	✓	✖	✓	✓	✓
- Statistics:** A tree view showing statistics for 'Assureon\_117117', 'System\_117117', 'Org01', 'Org02', and 'Org02FS01/02'. It lists metrics like 'Files', 'Files processed in the last hour', 'Files processed yesterday', 'Files read since 19/01/10 0:37', 'Files to dispose until yesterday', 'Safe shortcuts to create', and 'Transactions'.
- CPU & Memory:** Shows memory and CPU usage for F001-117117 (Memory % used: 34, CPU % used: 0) and F002-117117 (Memory % used: 17, CPU % used: 0).
- Folders:** Shows the state of folders.
- Services:** Shows the state of services, including 'Assureon Events Manager' which is 'Stopped'.
- Ingestion:** Shows the state of ingestion processes for F001-117117 and F002-117117, both 'Enabled'.
- Hardware:** Shows the state of hardware components like DIMM, Disk, and Fan, all 'Ok'.

### ▶ Assureon system state:

- **State** – The overall system state for the specified server.
- **Domain** – The domain the server belongs to.

- **CPU & Memory** – Whether CPU and memory use are within normal operating parameters. Capacity warnings and errors are generated based on configured threshold; see [Setting CPU and memory thresholds](#) on page 31.
- **Disks** – Whether disks have enough free space. Includes junction points. Capacity warnings and errors are generated based on configured threshold; see [Setting disk capacity thresholds](#) on page 26.
- **Folders** – Whether folders used for temporary processing are within normal operating parameters. Capacity warnings and errors are generated based on configured threshold; see [Monitoring the folders for Organizations](#) on page 32.
- **Queues** – Whether queue use is within normal operating parameters. Every queue has its own set of threshold parameters; see [Setting thresholds for message queues](#) on page 27.
- **Services** – Whether services are started.
- **Connectivity** – Whether the front-end server can connect to other sites (for plus configurations) or to the key server. Does not apply to back-end servers; see [Monitoring network connectivity](#) on page 28.
- **Ingestion** – Whether file system ingestion is enabled or disabled for the system. A check mark indicates ingestion is enabled. You can disable ingestion, if needed, by clicking the check mark, and then clicking the Change button; a red icon is displayed to indicate ingestion is disabled.
- **SQL Jobs** – Displays the status of database SQL jobs. A checkmark indicates that all SQL jobs that should be running have executed successfully. If they have not, you need to contact Nexsan Technical Support to investigate the issue.
- **Hardware** – Displays the overall status of hardware components.

The bottom section contains statistical information, as well as detailed information for the components contained in the summary table. The various panels may be collapsed or expanded by using the icon in the panel title. In the event of a problem, the yellow and red icons will appear in the title bar.

## Statistics panel

The statistics panel contains the following statistical information about the system. The information can be refreshed by clicking the refresh icon.

- **Files** – The total number of unique files archived on Assureon.
- **Files processed in the last hour** – The number of files processed on Assureon in the last hour (give or take 10 minutes).
- **Files processed yesterday** – The number of files processed, as of midnight the day before.
- **Files read since** – The number of files read or restored since the specified day and hour.
- **Files to dispose until yesterday** – The number of expired files as of midnight.
- **Transactions** – The total number of files sent to Assureon for processing.

## Disks panel

The disks panel displays all volumes on the system, including each volume's total disk capacity and percentage used.

## Queues panel

The queue panel displays the number of elements contained in the message queues. It only displays queues when they contain elements. For more information about queues, see [Monitoring Assureon Queues](#) on page 42.

## Connectivity panel

The connectivity panel displays network connectivity status from the server to other Assureon components, including the Key Server, Time Server, Windows Update Server, and so on.

## SQL Jobs panel

The SQL Jobs panel displays the status of each SQL job running for databases and reports. For more information about each SQL Job and to configure SQL Jobs thresholds, see [Setting SQL jobs thresholds on page 29](#).

## CPU & Memory panel

The CPU and Memory panel displays the percentage of CPU and memory consumed by the server.

## Folders panel

The Folders panel displays the total number of files in Assureon folders for each organization.

## Services panel

Displays the message "All services are running" or the name of the service that is stopped.

## Ingestion panel

The Ingestion panel indicates whether or not ingestion is enabled.

- **Show only Active File Systems** – Select this option to display information for active file systems only. Active file systems are those currently accepting files for archiving.

## Hardware panel

The Hardware panel displays the status of these components for each server:

- DIMM
- Disk
- Fan
- Processor
- PSU

To set up thresholds for hardware components, see [Setting hardware monitoring thresholds on page 33](#).

## Viewing overall system health

The System State page is automatically displayed when the System Administration user interface is accessed. It may also be accessed by clicking the Home icon at the top-right of every page or by clicking the Nexsan by Nexsan logo at the top-left of every page.

The top section contains three separate links for viewing the health of [Assureon](#) servers, [Clients](#), and [External Storage](#), with a status icon indicating the health of each component: a green check mark indicates that there are no issues; a yellow icon (warning) indicates a potential problem that needs to be investigated; a red icon (error) indicates a problem that needs to be addressed. By default, the System State page displays the health of the Assureon servers when you open the page.

## Clients

The **Clients** link compares the amount of data that was archived during the previous day (12:00am to 11:59pm) to the expected amount.

- A green checkmark indicates that everything is as it should be.
- A yellow icon (warning) indicates that the client archived less data than expected and this should be investigated.

The information in the table can be sorted in ascending or descending order by clicking on the column heading. To specify the Minimum Files values, see [About thresholds on page 41](#).

Figure 2-13: System State page – Status of Clients

The "Totals" view displays summary information for clients, including the total amount of data archived in a given date range. You can start or stop the Assureon FSW service on each client, and also initiate a new synchronization.

Today | Yesterday | Week | Month | Custom: [ ] to [ ] Go

Computer	Virtual Name	FSW Service Status	Sync	Status	Files Scanned	Files Archived	Bytes Archived	Bytes Shortcut	Action
EDGE001-117117	ASUEDGE	✔ Stop	○	✔	1,050,120	0	0.00 B	0.00 B	⚙
EDGE101-117117	ASUEDGE	✔ Stop	○	✔	9,450	0	0.00 B	0.00 B	⚙
F001-117117	F001-117117	✔ Stop	○	✔	0	0	0.00 B	0.00 B	⚙
					1,059,570	0	0.00 B	0.00 B	

Create Filter

Show Customization Window Save Layout

## External storage

The External Storage link displays the status of external storage systems associated with each Assureon server. The grid displays a status icon indicating the health of each external storage: a green checkmark indicates that there are no issues; a red icon (warning) indicates a potential problem that needs to be investigated. You can sort the information in ascending or descending order by clicking a column heading.

Figure 2-14: System State page – Status of External Storage

The screenshot shows the Nexsan Assureon System State page. The top navigation bar includes the Nexsan logo on the left and the Assureon logo on the right. Below the navigation bar, there are three tabs: System State (selected), Thresholds, and Tasks. The main content area is divided into a left sidebar and a main grid. The sidebar has sections for Files, Configuration, and Administration, each with a list of sub-items. The main grid displays a table with the following data:

Site	Status	Storage Hostname	Problem Summary
Site1	<IMG SRC=".\images\error16x16.png" />	172.21.16.117	: Enclosure (0) PSU (0) has no AC supply

At the top of the main grid, there are three status indicators: a red 'x' for Assureon, a green checkmark for Clients, and a red 'x' for External Storage. The table columns are Site, Status, Storage Hostname, and Problem Summary.

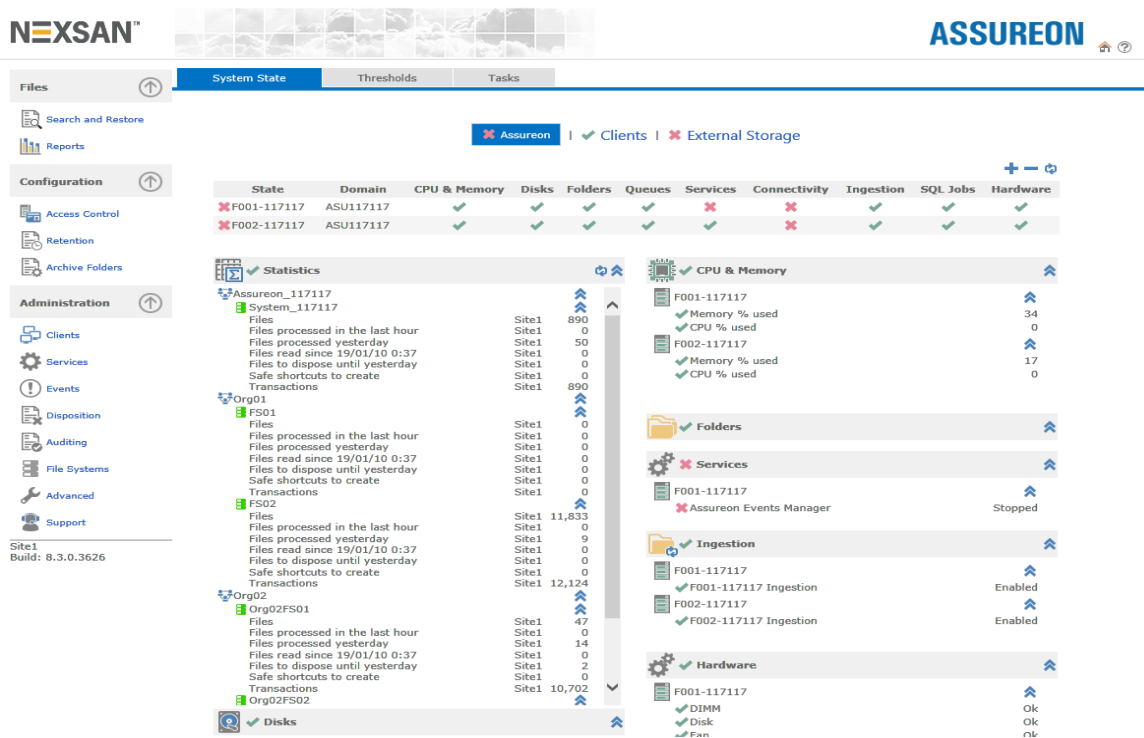
## Monitoring the System State

Use the System State page to monitor Assureon system activity. It is the default page when you open the System Administration user interface, and opens from the Home icon at the top right of the UI.

The System State home page has three tabs:

- [System State](#) – Displays the overall health of the system, including that of Clients and external storage connected to the server.
- [Thresholds](#) – Contains configurable monitoring thresholds for the system.
- [Tasks](#) – Displays running and completed tasks on the system.

Figure 2-15: System State page



Use the System State page to:

- monitor critical components and services of all Assureon servers;
- get an overview of the [Assureon](#) system health;
- view the status of [Clients](#) installed on other computers;
- display the health of [External Storage](#) for the server;
- configure monitoring thresholds for specific Assureon components.

**Note** For Replicated configurations, information is displayed for all sites.

Any warnings or errors should be resolved immediately. If you cannot resolve an issue, please contact [Nexsan Support](#). The system may also be configured to send system alerts, see [email alerts](#) for details.



## About thresholds

If a component reaches or exceeds a configured threshold value, the system displays the appropriate status icons on the main [System State](#) page, for the relevant component. For instructions, see [Setting thresholds on page 24](#)

In addition to specific configuration settings, for each threshold, you can configure whether to send email alerts when a threshold is reached or exceeded, and specify whether to ignore error and warning messages.

Figure 2-16: System State - Thresholds page

The screenshot shows the NEXSAN ASSUREON interface. The top navigation bar includes the NEXSAN logo on the left and the ASSUREON logo on the right. Below the navigation bar, there are three tabs: System State, Thresholds (which is active), and Tasks. On the left side, there is a vertical navigation menu with sections: Files (containing Search and Restore and Reports), Configuration (containing Access Control, Retention, and Archive Folders), and Administration (containing Clients, Services, Events, Disposition, Auditing, File Systems, Advanced, and Support). The main content area is titled 'Thresholds' and contains a descriptive text: 'Use this page to configure the default threshold settings for specific components of the Assureon system. You can also configure the refresh interval for monitoring each threshold.' Below this text is a grid of 12 threshold settings, each with a dropdown arrow. The settings are: Statistics, CPU, Disk Space, Memory, Queues, Folders, Connectivity, Services, Clients, Ingestion, SQL Jobs, and Hardware. At the bottom of the grid, there are two buttons: 'Save' and 'Restore Defaults'.

**Note** You can collapse or expand the various panels by using the icon in the panel title.

## Monitoring tasks

The **Tasks** tab displays a grid listing both active and completed tasks, including detailed information pertaining to each task. A task is defined as a long-running process or job that was started in the System Administration Web interface, such as a Disposition or Retention job.

Figure 2-17: Tasks page

This page lists all of the tasks that are in progress or that have completed recently. A task is a long-running action that was initiated by a user from the SysAdmin, such as changing the retention date of a list of files.

Job Name	Created By	Creation Date	Start Date	Completion Date	Status	Task Type	Organization	File System
Job Name: A1								
	ASU117117 \AssureonManager	2019/01/09 09:10:36	2019/01/09 09:10:36	2019/01/09 09:10:36	Completed	Allow Disposition	Org02	Org02FS02
	ASU117117 \AssureonManager	2019/01/09 09:10:36	2019/01/09 09:10:36	2019/01/09 09:10:36	Completed	Allow Disposition	Org02	Org02FS01
Job Name: C1								
	ASU117117 \AssureonManager	2019/01/09 09:11:39	2019/01/09 09:11:39	2019/01/09 09:11:39	Completed	Update Retention Date	Org02	Org02FS02
	ASU117117 \AssureonManager	2019/01/09 09:11:39	2019/01/09 09:11:39	2019/01/09 09:11:52	Completed	Update Retention Date	Org02	Org02FS01
Job Name: d								
	ASU117117 \AssureonManager	2019/01/09 09:14:17	2019/01/09 09:14:17	2019/01/09 09:14:18	Completed	Save Disposition	Org02	Org02FS02
	ASU117117 \AssureonManager	2019/01/09 09:14:17	2019/01/09 09:14:17	2019/01/09 09:14:20	Completed	Save Disposition	Org02	Org02FS01
Job Name: d2								
	ASU117117 \AssureonManager	2019/01/09 09:15:20	2019/01/09 09:15:20	2019/01/09 09:15:20	Completed	Save Disposition	Org02	Org02FS01
	ASU117117 \AssureonManager	2019/01/09 09:15:20	2019/01/09 09:15:20	2019/01/09 09:15:20	Completed	Save Disposition	Org02	Org02FS02
Job Name: G1								
	ASU117117 \AssureonManager	2019/01/09 09:23:16	2019/01/09 09:23:16	2019/01/09 09:23:16	Completed	Update Retention Date	Org02	Org02FS02
	ASU117117 \AssureonManager	2019/01/09 09:23:16	2019/01/09 09:23:16	2019/01/09 09:23:16	Completed	Update Retention Date	Org02	Org02FS01

By default, the contents of the grid are grouped by Job Name; you can add additional groupings by dragging any column heading to the top of the grid. For example, to group the information by both Job Name and Creation Date, drag the Creation Date column heading and drop it next to Job Name at the top of the grid; the system automatically reorganizes the information according to the specified grouping(s).

You can also filter the contents of the grid to display a specific task, or tasks. Simply click the filter icon in any column heading and select a filter criteria.

**Note** You cannot save layout changes; when you navigate away from the **Tasks** tab, the grid reverts to default display settings.

## Monitoring Assuranceon Queues

The Assuranceon system uses Microsoft Windows Message Queuing technology to handle system messages and file processing. The system uses queues to manage a list of files to be replicated to the other site.

The following is a brief description of the Assuranceon queues, along with their default System State warning and error thresholds; see [Monitoring the System State](#) on page 40. The default thresholds may be modified. For details, please contact Nexsan Support.

Queue Name	Description	Warning Threshold	Error Threshold
AuditQueue	Queue that contains lists of files to be audited; Used when auditing files across sites	10000	50000
cachenotification	[not currently used]	10000	50000
custinfoerrorqueue	Recovery queue for failed database requests	1000	5000
dispositionqueue	Queue that contains disposition requests	10000	50000
garbageerrorqueue	Recovery queue for failed requests to delete temporary files	1000	5000
keyserialnumbers	Queue that contains serial numbers of the encryption keys	20000	50000
manifestqueue	Queue that contains manifests to be sent to the key server	10000	50000
ORBQueue	Queue that contains commands or requests to replicate data across sites	20000	50000
storageErrorQueue	Recovery queue for failed storage requests	1000	5000
storagequeue	Recovery queue for failed storage requests	10000	50000
storagestatusqueue	Queue that contains storage transaction messages	10000	25000
storagetransportq1	[not currently used]	10000	50000
workfiledeleteq	Queue that contains the list of temporary files to delete after archiving has succeeded	20000	50000

## Searching for and restoring files

Use the **Search and Restore** page to search for files using advanced selection criteria and retrieve one or more files from the Assureon store.

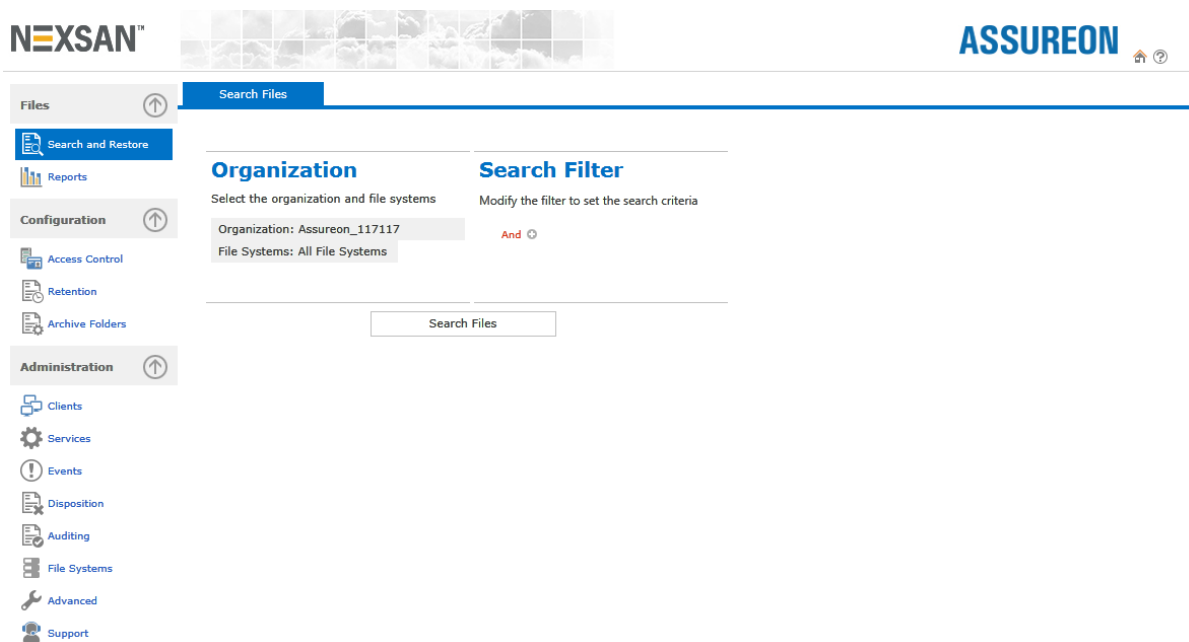
In order to retrieve a file, read access must not have been blocked, and you must have access permission. Access permission is controlled by assigning users to the security groups associated to the [access classification](#) by using Microsoft Active Directory.

**Note** Expired files are not listed. To view expired files, use the Disposition, [Override](#) page.

► **To access the Search and Restore page:**

- From the main menu, under **Files**, click **Search and Restore**.

Figure 2-18: Search and Restore page



When you access the Search and Restore page, you must first search for the files that you want to restore, by specifying the Organization and File System where the files are archived to, and if needed, specifying additional search criteria by activating the filters under Search Filter.

You can also display all files in a given Organization and all its File Systems, without filtering.

► **To search for files:**

1. Under **Organization**, click the Organization filter and select the organization where the files that you want to restore are archived.
2. Click the **File Systems** filter to select the relevant file system.

3. Under **Search Filter**, click the **And** link to build a filter that will search for specific files. It opens a drop-down list from where you can select operators and filter elements, or remove them.

Click the + icon after specifying an operator to start building your filter. You can build filters using multiple operators and criteria, giving you the flexibility to filter by computer name, file and folder name variations, ingestion and modified dates, a combination of all of these, and so on.

Depending on the type of search criteria selected, you must either enter an appropriate value in the text box, select from a list of available values, or select a date entry from the calendar that appears when you click the arrow in the text box.

4. Once you specify the desired search criteria, click the **Search Files** button to begin searching the store for files that meet the criteria.

The system searches the store for files and displays those that meet the specified criteria in a grid. If multiple, or All File Systems were selected as part of the search criteria, the grid displays files in the first file system specified.

To display files that match the search criteria in one of the other file systems you specified, select the corresponding file system in the File System to display drop-down list, at the top of the grid.

Similarly, for plus systems, search results are displayed for only one site at a time; to display search results on another site, click the corresponding site's radio button next to the Site to display field.

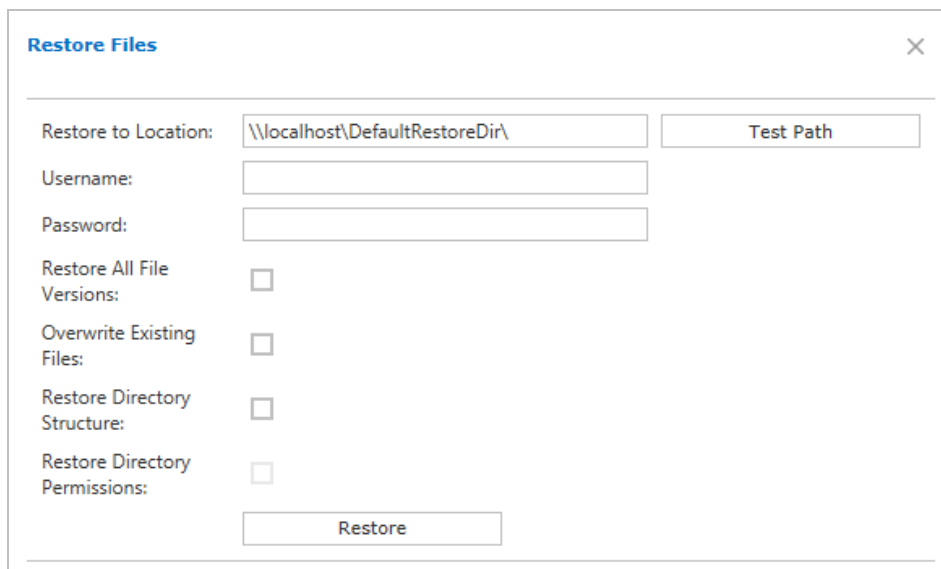
The grid displays these details for each file:

- **Signature ID** – The system-assigned file identification.
- **Start Transaction Time** – The date and time the file was stored.
- **File Name** – The name of the stored file.
- **Directory** – The name of the directory the file originated from.
- **computer Name** – The name of the computer the file originated from.
- **Retention Id** – The retention rule that was applied to the file when it was stored.
- **Retention Date** – The date after which the file becomes available for disposition. Calculated by the system based on the date the file was stored or as specified using the **Set Retention Date** button.
- **Read Access Allowed** – Whether the file has read access enabled
- **Block Disposition** – Whether the file is available for disposition and displayed in the disposition candidate list
- **Selection, Open File** – Click the link to open the file in the corresponding row.

► **To restore one or more files:**

1. Once you search for the files that you want to modify and they appear in Search Results, click the **Restore Files** button. The Restore Files dialog box displays:

Figure 2-19: Restore Files dialog box



This Restore Files dialog box has the following options:

- **Restore To Location** – The directory to which to restore the files. The location must already exist, be shared, and you must have write access. If you do not have write access, you can specify credentials on the fly using the User name and Password fields. The path can be in UNC format, or it can specify a local directory.
  - **Test Path** – Tests the directory path specified in the **Restore To Location** field.
  - **Izanami** – Specify the name of a user who has access to the share.
  - **Password** – Specify the password of the user specified in the Izanami field.
  - **Restore All File Versions** – Restores all versions of a file. For example, if a file named photo.pdf was saved 5 times with different content, all 5 versions of the file will be restored.
  - **Overwrite Existing Files** – Replaces existing files found in the restore location if they have the same name as restored files.
  - **Restore Directory Structure** – Restores files using the original directory structure.
  - **Restore Directory Permissions** – Restores folder security, if previously stored. Must be used with Restore Directory Structure option. For information about storing folder security, see [About the synchronization utility](#).
2. Specify the **Restore to Location** path and test it using the **Test Path** button.
  3. Select the **Restore All File Versions** and the **Overwrite Existing Files** options.
  4. To preserve the original directory structure, click the **Restore Directory Structure** option.
  5. Click **Restore**. The files are retrieved from storage and placed in the **Restore To Location** directory. If you restored using the **Restore Directory Structure** option, look for the files under the originating computer name.

When all versions of a file are restored, use the **Date Modified** information (displayed in Windows Explorer) to locate the version you want.

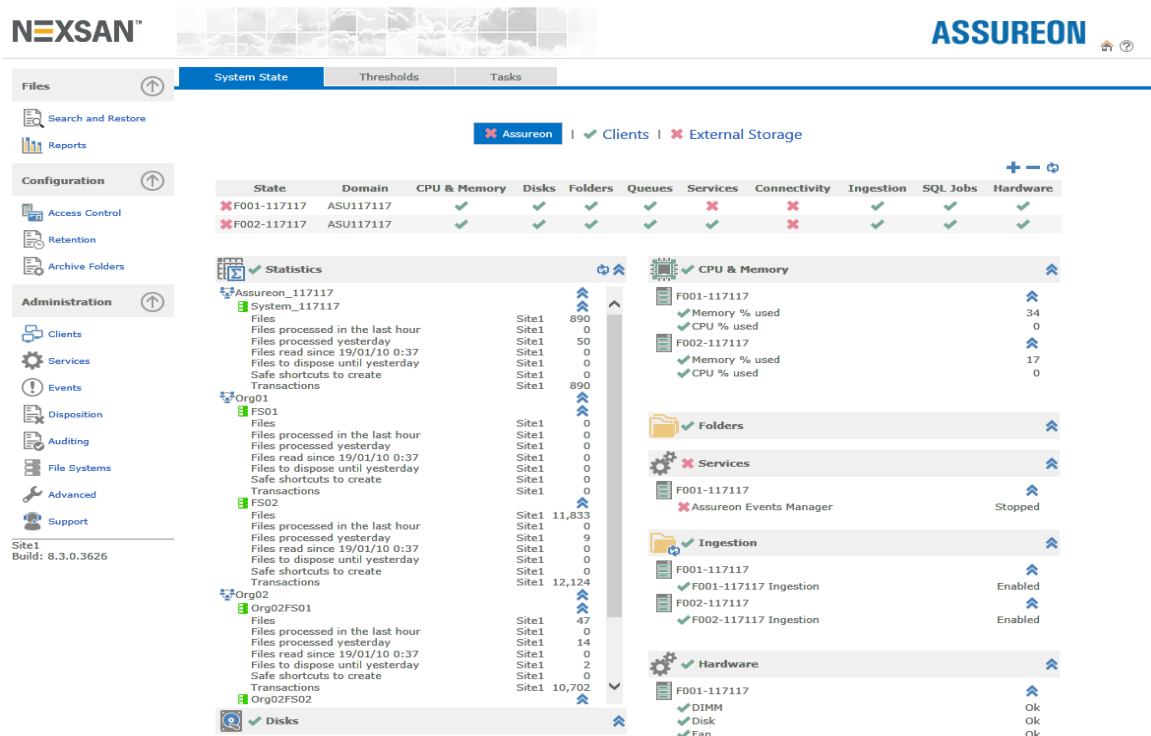
## Generating reports

Use the **Reports** page to view space consumption information, storage trends, and storage reports in both summary and date-specific views. This page is accessed by clicking Reports from the main menu. Access to reports may be controlled using [security groups](#).

The Reports home page has three tabs:

- [General Information](#) – Displays the overall space consumption of the system, including that of Clients and external storage connected to the server.
- [Client Trends](#) – Displays archiving stats over the last year, including total number of files, and average file size, either by client, or in total.
- [Advanced Reporting](#) – Displays storage reports in both summary and date-specific views.

Figure 2-20: System State page



Use the Reports page to:

- monitor critical components and services of all Assureon servers;
- get an overview of the [Assureon Server status](#);
- view the consumption and archiving of [Clients](#) installed on other computers;
- view a predictive analysis of monthly growth rates, and when the system will be full.

## Viewing space consumption, disposition details, and predictive analytics

The **General Information** tab provides information about space consumption within your system, as well as disposition information, and a predictive analysis of when your system will reach full capacity.

**Tip** Use the drop down menus to filter the display of information. For example to display only specific organizations or clients.

Figure 2-21: Reports page

The screenshot displays the Nexsan Assureon Administration interface. The top navigation bar includes 'Files', 'General Information' (selected), 'Client Trends', and 'Advanced Reporting'. The left sidebar contains various management tools. The main content area features several data panels:

- Organization Space Consumption:** A tree view showing space usage for 'Assureon\_999117' across 'Site1' and 'Site2'. Sub-organizations like 'CWOrg01', 'CWOrg02', and 'SysAdminOrg1' are listed with their respective usage.
- System Space Consumption:** A table showing space usage for 'AssureonSystem' and its sub-sites, including 'F001-999117' and 'F101-999117'.
- Disposition by Clients:** A table listing clients like 'ASUEDGE' and 'CLUSTERNAS' with their file counts, sizes, and disposition dates.
- Total Disposition:** A summary table of disposition data across sites.
- Predictive Analysis:** A panel indicating the system will be full on 'August 23, 2420' with a '0%' monthly growth rate.

Copyright © 2000-2017 Nexsan, Inc. All rights reserved.  
ASU999117AssureonManager

The following panels are displayed:

- **Organization Space Consumption** – The total amount of space being used by each site in the organization. Information is sub-divided by sites within your organization.
- **System Space Consumption** – The total amount of space being used by each server in the organization. Information is sub-divided by sites within your organization.
- **Disposition by Clients** – The number of files on each client that have passed their expiration date (as specified by the retention rule), and have become candidates for disposition (deletion).
- **Total Disposition** – The number of files on each site that have passed their expiration date (as specified by the retention rule), and have become candidates for disposition (deletion).
- **Predictive Analysis** – The estimated date that the system will reach full capacity. Also displayed is the monthly growth rate, as calculated by the system.



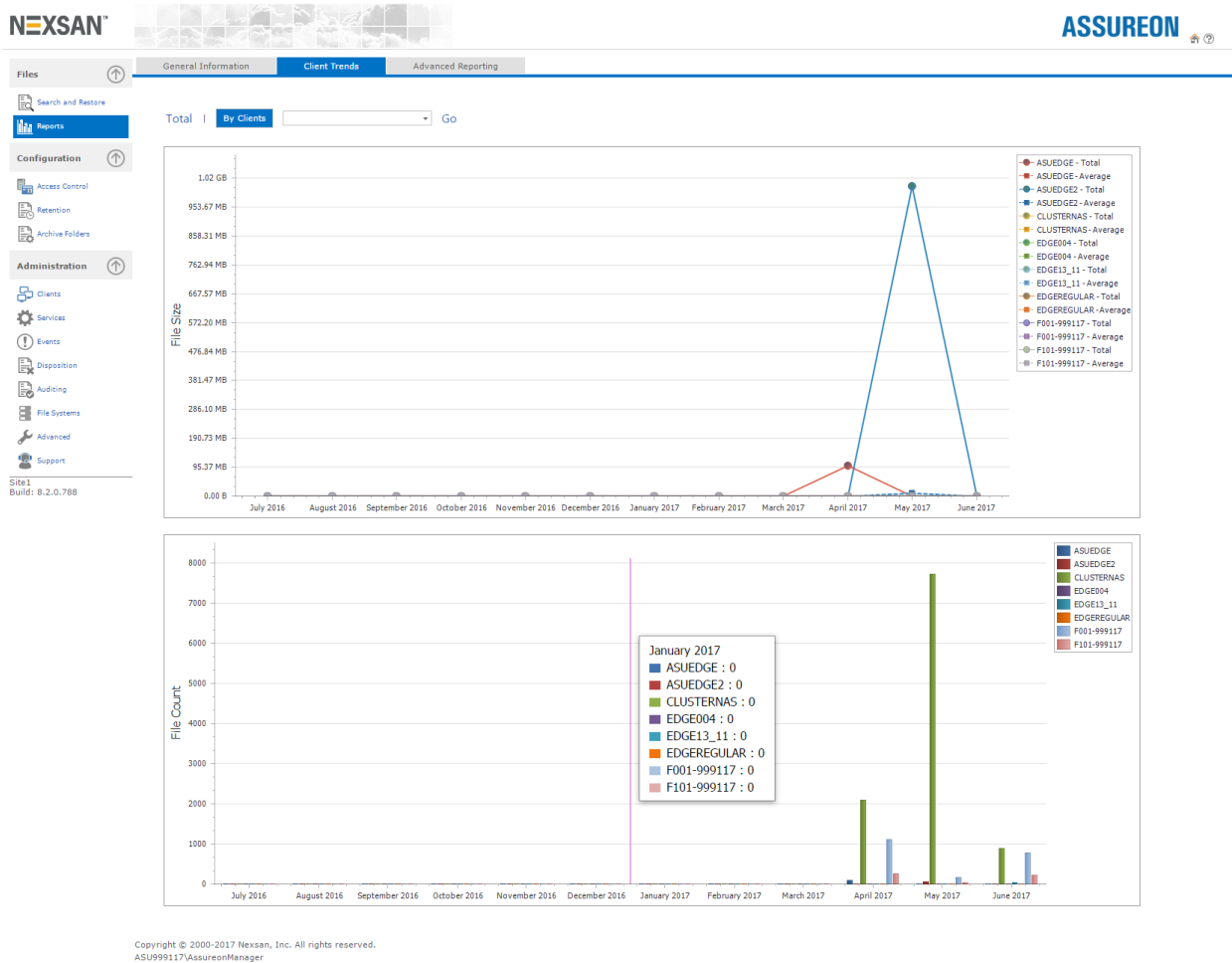
## Viewing client trends

Use the **Client Trends** tab to displays a graphical representation of the files that have been stored over the previous year. The following information is displayed:

- Total file size
- Average file size
- Total number of files

**Tip** Use the drop down menus to filter the display of information. For example to display only specific clients.

Figure 2-22: Client Trends



## Viewing summary and date-specific reports

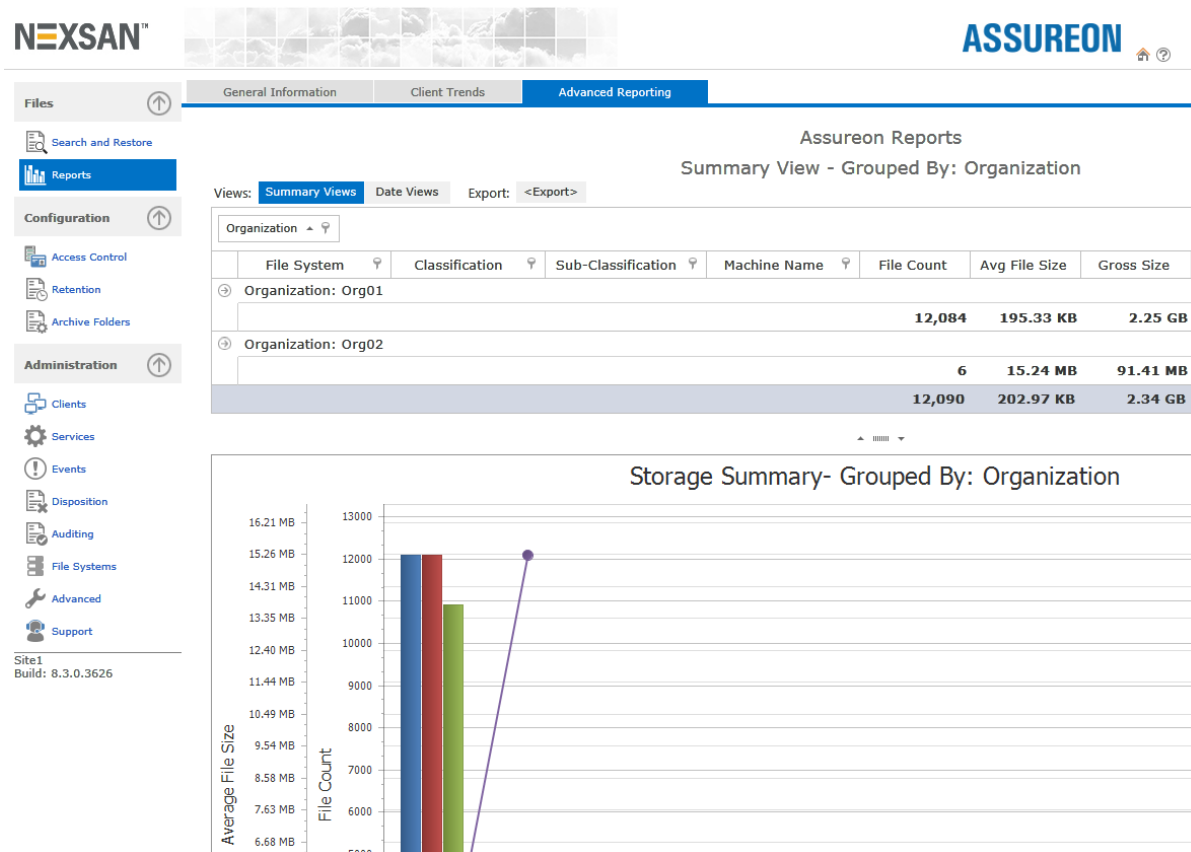
Use the **Reports** page to view storage reports in both summary and date-specific views. This page is accessed by clicking Reports from the main menu. Access to reports may be controlled using [security groups](#).

The information in the reports is automatically updated using report jobs that run daily. If you need the latest information, refresh the **Advanced Reporting** page, or switch between views to reload the data.

**Note** If you have a lot of data, the report job may take a while to complete.

Report jobs can also be run from the [Job Management](#) page.

Figure 2-23: Reports page



When you access the **Reports** page, the **Summary Views** report grouped by organization displays by default. You can display reports for specific time periods by clicking **Date Views**, and then selecting either **All** (all available time periods), This Month, 3 Months, 6 Months, or Custom. The Reports page displays both a tabular and graphical view for reports. You can export reports to PDF, Excel (XLS and XLSX), RTF, or CSV (comma-separated values) format.

**Note** Exported data appears in actual byte sizes, and not in unit multiples (for example, MB or GB).

File System	Classification	Sub-Classification	Machine Name	File Count	Avg File Size	Gross Size	Net Size	Savings	Saving Percent
<b>Organization: TestOrg01</b>									
TestOrg01FS01	EVERYONECL	EVERYONESC	ES2001110-001	735	1,045,714,079	768,599,848,180	768,599,848,180	0	0.00
				735	1,045,714,079	768,599,848,180	768,599,848,180	0	0.00
				735	1,045,714,079	768,599,848,180	768,599,848,180	0	0.00

You can also filter the contents of reports by Organization, File System, Classification, Sub-Classification, and computer Name.

### Changing the layout

- If you select an organization, the report will include all its file systems.
- Use the arrow icon in the reports to open or collapse a more detailed view.

- Drag any column heading to the top of the grid to create additional groupings of the information. For example, to group the information by both Organization and File System, drag the File System column heading and drop it next to Organization at the top of the grid; the system automatically reorganizes the information according to the specified grouping(s).
- Drag any column heading to the left or right to change the order of the information.

### **Working with reports**

By default, reports display summary information. To view the detail rows, "drill-down" by clicking the arrow icon to the right of each parent row. To "drill-up" from a detail, click the arrow again at the parent row to collapse the view.

#### ► **To filter reports:**

1. Click the filter icon in the column heading containing the desired filter criteria.
2. In the drop-down box, select the components, or components to filter by.
3. Click **OK**.

The system filters the report according to the specified criteria. The filter icon in the corresponding column heading(s) changes color to indicate filtering is active.

#### ► **To switch to Date Views reports:**

1. Click **Date Views**. The system displays data for all available dates.
2. To display data for a specific time period, choose of these options:
  - This Month
  - 3 Months
  - 6 Months
  - Custom; If you select **Custom**, you must specify a date range and then click **Go** to display the report.

#### ► **To export a report:**

1. Click **Export**.
2. Select the export format: PDF, Excel (XLS and XLSX), RTF, or CSV (comma-separated values).  
**Note** The application you are planning to view the exported file must be installed on the computer. You may also have to disable any Pop-up blockers.
3. You are prompted to save the file. Specify a file name and click **Save** to export the report to the specified format.

## Using the Access Control pages

This section provides information about these topics:

- [Classifying archived files - Access Classification page](#) below
- [Configuring read access](#) on the facing page
- [Reviewing file access logs](#) on page 56

### Classifying archived files - Access Classification page

Use the **Access Classification** page to classify archived files, for access and management purposes. When a file is placed under Assureon management, it is stored using classification and sub classification information. For example, the file `Building.jpg` originally on John Smith's computer in an archive folder called `jpegs`, may be classified using `JohnSmith1.JPEGImages`. Classifications allow you to control access to all of John Smith's files. They also provide an intuitive way to search, audit, and dispose of files.

When a classification is created, two security groups are created in Active Directory, providing a file access mechanism. For users to be able to access their files, they must be added as members of the `ASSUREONUsers` group and to the appropriate classification security groups.

For example, if John Smith is made a member of the `JohnSmith1` security group, he will be able to see all files stored in the `JohnSmith1` classification, no matter the sub-classification. If John Smith is made a member of one or more sub-classifications, but not to the classification, he will only have access to files stored under the sub-classifications.

To give a user access to everything, add them to the `ASSUREONUsers` and `ASSUREON` groups. By default, the `AssureonManager` and `AssureonAdmin` users are members of both these groups.

► **To access the Access Classification page:**

1. From the main menu, under **Configuration**, click **Access Control**.
2. Select the **Access Classification** tab.
3. Click the **Add Classification** button.

► **Access classification details:**

- **Organization** – The organization under which the classification will be created.
- **Classification** – The primary classification for the file. Maximum of 10 alphanumeric characters; no special characters allowed. Lower case characters are converted to upper case ones.
- **Subclassification** – A secondary or child classification for the file. Maximum of 10 alphanumeric characters. No special characters allowed; lower case characters are converted to upper case ones.
- **Active From** – The date the classification can first be used; files added to a watched directory before this date will not be added to the store. Default is the current date. Use the `yyyy-mm-dd` date format. Depending on your user, this field may not be displayed.
- **Active To** – The date after which the classification is no longer valid; files added to a watched directory after this date will not be added to the store. Use the `yyyy-mm-dd` date format. The default date is 2099-12-31. Depending on your user, this field may not be displayed.

- **Enable Flexible Retention** – Allows the retention period for files stored using the current classification to be shortened, with the exception of archive folders with [Compliant classifications](#). Flexible retention must be used with a [retention rule](#) where a **Minimum Retention Period** has been specified. To shorten or extend the retention period, use the [Disposition Override](#) page. Also used with the retention rule **Maximum File Versions** option to allow the disposition of excess file versions.
- **Date Created** – The date the classification was added.
- **Edit** – Modifies the **Active From**, **Active To** and **Enable Flexible Retention** options.
- **Delete** – Deletes the classification if it has not been used by the system. Classifications that are in use cannot be deleted.

► **To add new classification information:**

1. Specify a **Classification** and **Subclassification**.  
To use the default dates, from today to 2099-12-31, leave the date fields blank.
2. Click **Add**. The information is added to the table.

## Configuring read access

Use the **Read Access** page to control file read access. You can also use this page to retrieve a file.

► **To access the Read Access page:**

1. From the main menu, under **Configuration**, click **Access Control**.
2. Select the **Read Access** tab.

Figure 2-24: Access Control - Read Access page

The screenshot displays the 'Read Access' configuration page in the Nexsan Assureon interface. The page is divided into several sections:

- Organization:** Select the organization and file systems. Organization: 111111, File Systems: All File Systems.
- Search Filter:** Modify the filter to set the search criteria. Includes an 'And' button.
- Buttons:** Search Files, Block Read Access..., Allow Read Access...
- Search Results:** File System to display: 111111FS02, Site to display: Site1 (selected).

Signature Id	Start Transaction Time	File Name	Directory	Machine Name	Retention Id	Retention Date
EVERYONECL.EVERYONES.C.a.000002140	2018/12/19 08:37:58	VFTest000073.txt	D:\Sparse\VFTest	ASUEDGE	365daysEC	2019/12/19 08:37:58
EVERYONECL.EVERYONES.C.a.000002141	2018/12/19 08:37:58	VFTest000055.txt	D:\Sparse\VFTest	ASUEDGE	365daysEC	2019/12/19 08:37:58
EVERYONECL.EVERYONES.C.a.000002143	2018/12/19 08:37:58	VFTest000064.txt	D:\Sparse\VFTest	ASUEDGE	365daysEC	2019/12/19 08:37:58
EVERYONECL.EVERYONES.C.a.000002145	2018/12/19 08:37:58	VFTest000033.txt	D:\Sparse\VFTest	ASUEDGE	365daysEC	2019/12/19 08:37:58
EVERYONECL.EVERYONES.C.a.000002147	2018/12/19 08:37:58	VFTest000039.txt	D:\Sparse\VFTest	ASUEDGE	365daysEC	2019/12/19 08:37:58
EVERYONECL.EVERYONES.C.a.000002149	2018/12/19 08:37:58	VFTest000006.txt	D:\Sparse\VFTest	ASUEDGE	365daysEC	2019/12/19 08:37:58
EVERYONECL.EVERYONES.C.a.000002151	2018/12/19 08:37:58	VFTest000047.txt	D:\Sparse\VFTest	ASUEDGE	365daysEC	2019/12/19 08:37:58
EVERYONECL.EVERYONES.C.a.000002153	2018/12/19 08:37:58	VFTest000000.txt	D:\Sparse\VFTest	ASUEDGE	365daysEC	2019/12/19 08:37:58

**Block** and **Allow Read Access** controls whether a file can be retrieved from the archive. Once read access is blocked, a file cannot be retrieved until it is unblocked. Files that have been blocked from read access are still available for disposition.

When you open the **Read Access** page, you must first search for the files that you want to control read access for, by specifying the Organization and File System where the files are archived to, and if needed, specifying additional search criteria by activating the filters under Search Filter.

You can also display all files in a given Organization and all its File Systems, without filtering.

► **To search for files:**

1. Under Organization, click the Organization filter and select the organization where the files that you want to search for are archived.
2. Click the File Systems filter to select the relevant file system.
3. Under **Search Filter**, click the **And** link to build a filter that will search for specific files. It opens a drop-down list from where you can select operators and filter elements, or remove them.

Click the + icon after specifying an operator to start building your filter. You can build filters using multiple operators and criteria, giving you the flexibility to filter by computer name, file and folder name variations, ingestion and modified dates, a combination of all of these, and so on.

Depending on the type of search criteria selected, you must either enter an appropriate value in the text box, select from a list of available values, or select a date entry from the calendar that appears when you click the arrow in the text box.

4. Once you specify the desired search criteria, click the **Search Files** button.

The system searches the store for files and displays those that meet the specified criteria in a grid. If multiple, or All File Systems were selected as part of the search criteria, the grid displays files in the first file system specified.

To display files that match the search criteria in one of the other file systems you specified, select the corresponding file system in the File System to display drop-down list, at the top of the grid.

Similarly, for plus systems, search results are displayed for only one site at a time; to display search results on another site, click the corresponding site's radio button next to the Site to display field.

► **File details:**

- **Signature ID** – The system-assigned file identification.
- **Start Transaction Time** – The date and time the file was stored.
- **File Name** – The name of the archived file.
- **Directory** – The name of the directory the file originated from.
- **computer Name** – The name of the computer the file originated from.
- **Retention Id** – The retention rule that was applied to the file when it was archived.
- **Retention Date** – The date after which the file becomes available for disposition.
- **Read Access Allowed** – Whether the file can be accessed by someone with the correct credentials
- **Block Disposition** – Whether the file is available for disposition and displayed in the disposition candidate list.
- **Selection, Open File** – Opens the file specified on that row.

► **To block or allow read access:**

1. Once you search for the files that you want to modify and they appear in Search Results, click the **Block Read Access** or the **Allow Read Access** buttons. A popup displays prompting you for a name to assign to the task, which you can then monitor under the **Tasks** tab, on the System Stage page.
2. Specify a name and click **OK**.

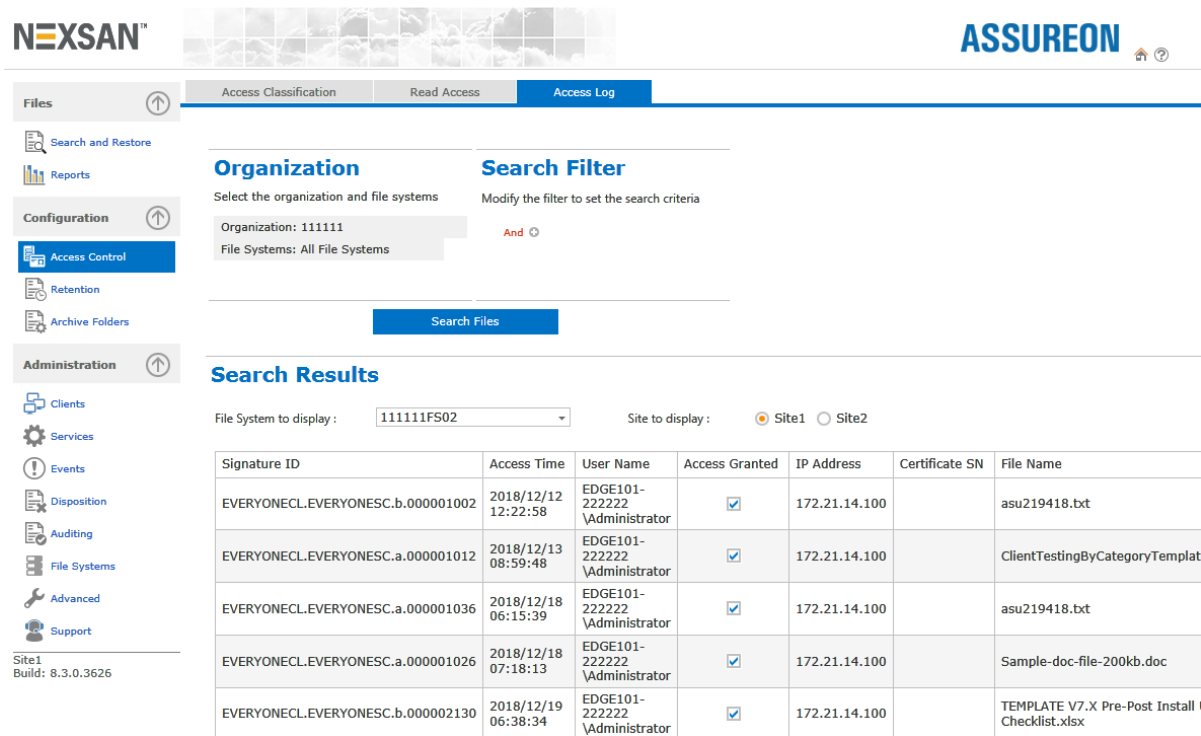
## Reviewing file access logs

Use the **Access Log** page to display requests to retrieve files from storage.

► **To access the Access Log page:**

1. From the main menu, under **Configuration**, click **Access Control**.
2. Select the **Access Log** tab.

Figure 2-25: Access Control - Access Log Page



When you open the Access Log page, you must first search for the access requests that you want to display, by specifying the relevant Organization and File System where access was requested, and if needed, specifying additional search criteria by activating the filters under Search Filter.

You can also display all requests in a given Organization and all its File Systems, without filtering.

► **To search for requests in the access log:**

1. Under Organization, click the Organization filter and select the organization you want to search in.
2. Click the File Systems filter to select the relevant file system.
3. Under **Search Filter**, click the **And** link to build a filter that will search for specific files. It opens a drop-down list from where you can select operators and filter elements, or remove them.

Click the + icon after specifying an operator to start building your filter. You can build filters using multiple operators and criteria, giving you the flexibility to filter by computer name, file and folder name variations, ingestion and modified dates, a combination of all of these, and so on.

Depending on the type of search criteria selected, you must either enter an appropriate value in the text box, select from a list of available values, or select a date entry from the calendar that appears when you



click the arrow in the text box.

4. Once you specify the desired search criteria, click the **Search Files** button to begin searching .

The system searches the store for files and displays those that meet the specified criteria in a grid. If multiple, or All File Systems were selected as part of the search criteria, the grid displays files in the first file system specified.

To display files that match the search criteria in one of the other file systems you specified, select the corresponding file system in the File System to display drop-down list, at the top of the grid.

Similarly, for plus systems, search results are displayed for only one site at a time; to display search results on another site, click the corresponding site's radio button next to the Site to display field.

► **Request details:**

- **Signature ID** – The name of the requested file.
- **Access Time** – The time, in UTC, that the file was requested.
- **User Name** – The name of the user that requested the file.
- **Access Granted** – Whether access to the file was granted
- **IP Address** – The IP address of the workstation from which the requested was made.
- **Certificate SN** – When security certificates are used for authentication, the serial number of the security certificate.
- **File Name** – The name of the requested file.
- **Directory** – The name of the directory the file was originally archived from.
- **Computer** – The name of the computer the file originated from.
- **Expiration Date** – The date after which the file becomes available for disposition.
- **Selection, Open File** – Click the link to open the file in the corresponding row.

## Working with retention rules

Use the **Retention Rules** page to view and add retention rules. Retention rules specify how long a file is kept under management, and whether the file is stored in encrypted or compressed format.

Retention rules are created to address specific regulatory requirements. Make sure the retention rules you create meet your legal and business requirements. It is best practice to create all rules with or without encryption. Should the same file be processed using two sets of rules, only one of which has encryption enabled, the file will be stored once using the first rule used.



**CAUTION:** Once created, retention rules cannot be modified or deleted.

► **To access the Retention Rules page:**

- From the main menu, under **Configuration**, click **Retention**.

Figure 2-26: Retention Rules page

Rule Name	Retention	Encrypt	Compress	Minimum Retention (Days)	Maximum File Versions	Use Custom Retention Date	Set Read-Only Lock	Reference Date	Last Saved
180days	180	False	False	0	0	False	False	Ingestion Date	
1DECV2	1	True	True	0	2	False	False	Ingestion Date	2018/12/12 7:28 PM
30Years	10958	False	False	0	0	False	False	Ingestion Date	
30YearsE	10958	True	False	0	0	False	False	Ingestion Date	
30YearsEC	10958	True	True	0	0	False	False	Ingestion Date	
365days	365	False	False	0	0	False	False	Ingestion Date	
365daysE	365	True	False	0	0	False	False	Ingestion Date	
365daysEC	365	True	True	0	0	False	False	Ingestion Date	

► **Retention rule details:**

- **Rule Name** – The name of the rule. Maximum of 10 alpha-numeric characters; no special characters allowed; not case-sensitive.
- **Retention** – The number of days to keep the file before it becomes available for disposition. Based on the retention period (years and days) specified when the rule was created. Also displays if **Use Read-Only Lock** or **Use Custom Retention Date** options were selected.
- **Encrypt** – Whether the stored files are encrypted.
- **Compress** – Whether the stored files are compressed.
- **Minimum Retention (Days)** – The minimum number of days to store files.

- **Maximum File Versions** – The maximum number of versions of a file to keep in storage.
- **Use Custom Retention Date** – Specifies whether the minimum number of days to store files is based on the retention period, or set manually.
- **Set Read-Only Lock** – Specifies whether the stored files are read-only.
- **Reference Date** – Whether retention is based on the modified or ingestion dates of the stored files.
- **Last Saved** – The date the retention rule was created or last modified.

Columns can be sorted by clicking the column heading.

## Adding a retention rule

### ► To add a retention rule:

1. Select an [organization](#). The rule will be created for that organization.
2. In the **Rule Name** field, specify a name for the retention rule.
3. In the [Initial Retention Period](#) field, specify the number of years or days, or combination of both, to keep the files and then click anywhere on the page to calculate the total number of days.
4. Select whether you want to encrypt and/or compress the file in the [Transform Options](#).
5. Specify whether to use a file's [ingestion date](#) or [modified date](#) when applying this retention rule to it.
6. In non-compliant (**Flexible retention**) situations where you want to be able to expire and delete files ahead of time, specify the minimum number of days to keep the files in the [Minimum Retention Period](#) field. In situations where you want to limit the number of versions of a file to keep in storage, specify a value in the [Maximum File Versions](#) field.
7. Click the **Add** button. The rule is added to the table. Rules are applied to archive folders using the [Archive Folder Editor](#) or the [Assureon Property Sheet](#).

The Add Retention Rule dialog box contains the following options.

### ► Retention rule options:

- **Organization** – The organization the retention rule will be created for.
- **Rule Name** – The name of the rule. Maximum of 10 alpha-numeric characters; no special characters allowed; not case-sensitive.
- **Initial Retention Period**
  - **Days** – The number of days to store the file before it becomes available for disposition. Leap years are taken into consideration when counting total days for years. The maximum number of years is 99; the minimum number of days is 1.
  - **Use Custom Retention Date** – Uses the date specified in the Archive Folders Editor, Include Rule, Retention date field as the file retention date.
  - **Use Read-Only Lock** – Files are processed only after the read-only file attribute is set. Uses the file's last accessed date, which has been set to a date in the future, as the file retention date. Supports the Snaplock protocol.

- **Transform Options**

- **Encrypt** – Whether to encrypt the stored file. Use this option to comply with regulations that require files at rest to be in an encrypted state; to enable the ability to destroy files that are stored offline or on WORM media; or to add an additional layer of security. This option consumes CPU resources which may impact overall system performance. This option is not displayed if encryption is disabled.
- **Compress** – Whether to compress the stored file. Will save storage space only if the file type can be effectively compressed. For example, there is no benefit to compressing JPEG files. This option consumes CPU resources which may impact overall system performance.
- **Reference Date** – Specifies whether to use a file's ingestion or modified date when applying this retention rule to it.
  - **Ingestion date** – Files are retained as of their ingestion date. For example, if a file with a 7-year retention rule is ingested on April 01, 2014, its retention date is set to April 01, 2021.
  - **Date modified** – Files are retained starting from the date they were last modified. For example, if a file with a 7-year retention rule is ingested on April 01, 2014, but was last modified on January 01, 2010, the file's retention date is set to January 01, 2017. This only applies to files that have a modified date no greater than 7 years, or however long you set retention. For example, if a file with a 7-year retention rule is ingested on April 01, 2014, but was last modified on February 01, 2000, the file's retention date is set to April 02, 2014.

- ▶ **Flexible Retention Options:**

- **Minimum Retention Period** – The minimum number of days to store files. You can specify whether to use the same value as the retention period or specify the number of days. When specified, the value must be less than the Retention Period. Minimum of 1 day.
- **Maximum File Versions** – The maximum number of versions of a file to keep in the store. When the specified value is exceeded, the oldest files can be disposed of; see [Disposing of Excess File Versions](#) for details. Used when Assureon is a backup appliance. In a compliance situation, this option should be ignored. A value of 0 means that the number of versions of a file to keep is unlimited.

## Using archive folders

This section provides information about these topics:

- [Setting archive folder rules](#) below. The **Archive Configuration** page is used to assign archiving rules, or predefined collections of rules to computers.
- [Using archive folder templates](#) on the next page. The **Templates** page enables you to create, edit and delete templates.
- [Using the Archive Folders Editor](#) on page 70. The **Archive Folders Editor** is used to create new archive folders for computers or for templates.
- [Archive Folders](#) on page 71

## Setting archive folder rules

Use the **Archive Configuration** page to assign archiving rules, or predefined collections of rules to computers. Rules are assigned per computer and specify the folders to monitor, as well as how files are archived. This section enables you to assign templates to computers and to edit configuration files. It may also be used to add or remove computers manually.

### ► To access the Archive Configuration page:

- From the main menu, under **Configuration**, click **Archive Folders**.

Figure 2-27: Archive Configuration

The screenshot shows the 'Archive Configuration' page in the Assureon interface. The page has a header with the Nexsan and Assureon logos. Below the header is a navigation sidebar with categories: Files, Configuration, and Administration. The 'Configuration' category is expanded, and 'Archive Folders' is selected. The main content area shows a table with the following data:

Domain Name	Machine Name
2016ASU021	F001-ASU021
2016ASU021	F101-ASU021
ASUEDGE	ASUEDGE
EDGEWIN10	EDGEWIN10

To the right of the table is a 'New' button and a 'Delete' button. Below the 'Delete' button is an 'Assign Template' button.

See also [Archive Folders](#) on page 71

### ► Archive configuration options:

- **Domain Name** – The name of the domain where the computer resides
- **computer Name** – The name of the computer where the Assureon Client Service is installed
- **New** – Opens the New Configuration box used to add a new computer

- **Edit** – Displays the Archive Folders Editor page, edits the configuration file assigned to the computer
- **Delete** – Deletes the watch file for the selected computer
- **Assign Template** – Assigns an existing template to the selected computer

**Note** When assigning a template the layout of any existing Assureon server can be used, and all existing Assureon servers are listed.

► **To add computers to the Configuration page list:**

1. Click **New** to open the New Configuration dialog box.
2. Enter the **Domain Name** and **Computer Name**.
3. (Optional) In the **Copy From** drop-down list, assign a Template or an existing archive configuration.
4. Click **Add**. The Domain\Computer is added to the list.

Figure 2-28: New Configuration popup

The image shows a 'New Configuration' dialog box. It has a title bar with the text 'New Configuration' and a close button (X). The dialog contains two text input fields: 'Domain Name:' and 'Computer:'. Below these is an 'Optional' section with a 'Copy From:' dropdown menu. At the bottom are 'Add' and 'Cancel' buttons.

► **To edit a configuration file for a computer:**

1. Select the computer from the list.
2. Click **Edit**. The [Archive Folders Editor](#) page appears.

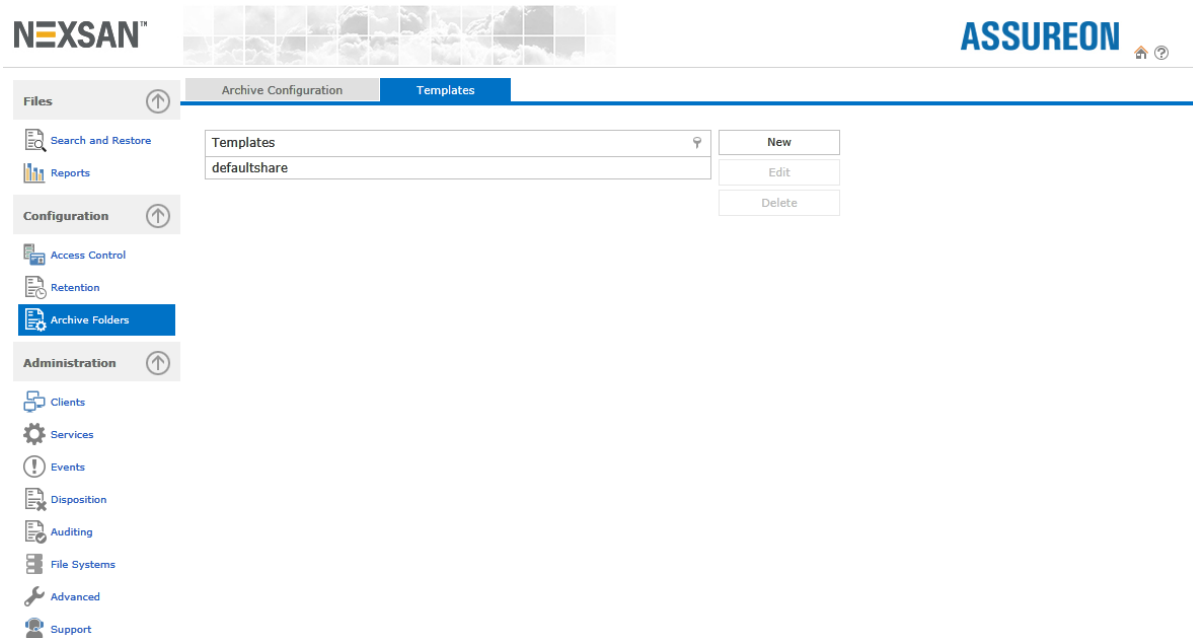
## Using archive folder templates

Use archive folder templates – predefined collections of rules – to ensure consistency for the rules applied across computers. After a template has been assigned to a computer, the template copy can be edited to include more folders, or to apply different retention or classification settings.

► **To access the Templates page:**

1. From the main menu, under **Configuration**, click **Archive Folders**.
2. Select the **Templates** tab.

Figure 2-29: Archive Folders - Templates



► **To create a template:**

1. Click **New** in the Templates page.
2. In the New Template dialog box, type a name for the new template.
3. Click **Add**. The new template is added to the template list.

► **To create a template based on an existing one:**

1. Click **New** in the Templates page.
2. In the New Template dialog box, type a name for the new template.
3. In the **Copy From Template** drop-down list, select the template you would like to base the new one on.
4. Click **Add**. The new template is added to the template list.

► **To modify a template:**

1. Select the template from the template list.
2. Click **Edit**. The Archive Folders Editor page appears. See [Using the Archive Folders Editor](#) on page 70.

## Using the Clients page

Use the **Clients** page to manage the Assureon client service installed on other computers, including starting and stopping synchronizations, viewing the status of currently executing synchronizations, and reporting the amount of data that was ingested by date for a given synchronization.

The **Clients** page enables you to:

- view file transfer totals for all clients by date;
- view daily summaries and synchronization information for all clients by date;
- start or stop a synchronization process for a client, or create a new synchronization;
- filter data;
- monitor file transfers.

Figure 2-30: Clients page

The screenshot shows the 'Clients' page in the Nexsan Assureon interface. The page has a sidebar with navigation options: Files, Configuration, and Administration. The 'Clients' option is selected under Administration. The main content area displays a 'Totals' view of client synchronization data. A text box explains that the 'Totals' view shows summary information for clients, including total data archived, and allows starting or stopping the service and initiating new synchronizations. Below this, there are tabs for 'Totals', 'Daily Summaries', and 'Synchronizations', and view options for 'Today', 'Yesterday', 'Week', 'Month', and 'Custom'. A table lists client data with columns for Computer, Virtual Name, FSW Service Status, Sync, Status, Files Scanned, Files Archived, Bytes Archived, Bytes Shortcut, and Action. The table shows three clients: EDGE001-117117, EDGE101-117117, and F001-117117. A summary row at the bottom shows totals: 776,818 files scanned, 1 file archived, 39.27 KB bytes archived, and 0.00 B bytes shortcut. There are also buttons for 'Show Customization Window' and 'Save Layout'.

Computer	Virtual Name	FSW Service Status	Sync	Status	Files Scanned	Files Archived	Bytes Archived	Bytes Shortcut	Action
EDGE001-117117	ASUEDGE	Stop	🔄	✓	769,993	1	39.27 KB	0.00 B	⚙️
EDGE101-117117	ASUEDGE	Stop	🔄	✓	6,825	0	0.00 B	0.00 B	⚙️
F001-117117	F001-117117	Stop	🔄	✓	0	0	0.00 B	0.00 B	⚙️
					776,818	1	39.27 KB	0.00 B	

► **To access the Clients page:**

- From the main menu, under **Administration**, click **Clients**. The Clients page contains the Totals, Daily Summaries, and Synchronization grids:

► **To display Totals for all clients by date:**

1. Click **Totals**; general information for all clients is displayed in the grid.
2. Click the Today, Yesterday, Month, or Custom view options to display information for a specific time period. For Custom, select the desired date range and click Go.

► **To start a new client synchronization:**

1. Click the **Action** icon for the corresponding client.
2. Select **Start New Sync**; the [Client Synchronization wizard](#) opens.



► **To stop or start an FSW:**

- To stop or start a client on another computer, click the Start or Stop link in the FSW Service Status column.

► **To display detailed information for a specific client.**

- Click the Action icon for the corresponding client and select More Details; the [Client Information](#) dialog box opens.

► **To display Daily Summaries for all clients by date:**

1. Click **Daily Summaries**; synchronization information grouped by date is displayed in the grid.
2. Click the Today, Yesterday, Month, or Custom view options to display information for a specific time period. For Custom, select the desired date range and click Go.
3. Drag any column heading to the top of the grid to create additional groupings of the information. For example, to group the information by both Date and Virtual Name, drag the Virtual Name column heading and drop it next to Date at the top of the grid; the system automatically reorganizes the information according to the specified grouping(s). Click Save Layout to save the new grouping layout; click Reset Layout to display the default grid layout.

► **To display Synchronization information for all clients by date:**

1. Click **Synchronizations**; synchronization information is displayed in the grid.
2. Drag any column heading to the top of the grid to create additional groupings of the information. For example, to group the information by both Date and Virtual Name, drag the Virtual Name column heading and drop it next to Date at the top of the grid; the system automatically reorganizes the information according to the specified grouping(s).
3. Click **Save Layout** to save the new grouping layout, or click **Reset Layout** to display the default grid layout.

You can also filter the contents of the Totals, Daily Summaries, and Synchronization grids, as well as customize the layout of the grids, by adding or removing columns.

► **To create a filter in a grid:**

1. Click **Create Filter** at the bottom of the grid; the Filter dialog box displays where you can create a custom filter using operators. The system automatically filters the currently active grid according to the specified filtering criteria.
2. Click **Save Layout** to save the filtered display.
3. Click **Clear** at the bottom right of the grid to remove the filter. Or, alternately, click **Reset Layout**.

You can also filter individual columns by clicking the filter icon in the corresponding column heading and selecting a specific value; for example, to filter the information by a specific computer, click the filter icon on the Computer column heading and select the relevant computer from the drop-down list.

► **To customize the layout of the grid:**

1. Click **Show Customization Window** to open a popup where you can select columns to add to the grid.
2. Drag any column from the popup and drop it in the desired location in the grid.
3. Click **Save Layout** to save the customized layout. Or, click **Reset Layout** to reset the layout to the default settings.

## Running a client synchronization

Use the Client Synchronization wizard to start a new file synchronization process on the selected client.

► **To launch the wizard:**

1. Click the **Action** icon for a Client Service on the [Clients](#) page.
2. Select **Start New Sync**.

Figure 2-31: Client Synchronization wizard



**NEXSAN™**

### Welcome to the Client Synchronization Wizard

Welcome to the Client Synchronization Wizard

This wizard will allow you to start a new synchronization on ASU117117\EDGE001-117117.

3. In the **Welcome** page, click the **Next** arrow to continue.
4. In the **Select Watch** page, select the watch to synchronize. You can select multiple watches, if needed.
5. In the **Select Synchronization Type** page, specify the synchronization type:
  - **Full** – Every file is scanned and compared to the Assureon server to determine whether it should be archived. This is the most comprehensive type of synchronization.
  - **Archive Bit** – The archive bit is an attribute in Windows. It is set on all new or modified files. This sync type allows only files that have the archive bit set to be considered for archiving. In most cases, this sync is recommended over a full sync. However, it is not recommended when another application is using the archive bit as it can cause the synchronization to miss files.
  - **Change Journal** – The Windows [change journal](#) is a database of new and modified files. This synchronization uses this database to determine which files need to be archived to the Assureon server.
6. The wizard has finished gathering information. Click the **Next** arrow to continue.
7. The wizard is configuring and displays the configuration process. When completed successfully, a message displays indicating that the sync has started successfully. Click the **Close Client Synchronization wizard** link.



## Displaying client Information

Use this procedure to display summary information about the selected client.

► **To access the Client Information dialog box:**

1. Under the **Actions** column, click an **Action** icon for a Client Service on the [Clients](#) page.
2. Select **More Details**.

Figure 2-32: Client Information dialog box

Client Information	
<b>ASUCPVM01\F001-CPVM01</b>	
Client configuration version	12
Server configuration version	12
Last checked	5/22/2015 10:15:17 AM
Status	Running
Client Version	8.1.0.42
Server Version	8.1.0.42
Number of files in journal folder	0
Path to journal folder	C:\Users\AssureonManager\AppData\Roaming\Nexsan Technologies\Assureon\Journal\
Available journal disk space	2.12 GB
Primary server	ilmclientlb.asucpvm01.net
Secondary server	
Security model	Access Classifications
 	
Save      Close	

► **Client Information dialog box information and icons:**

- **Client configuration version** – The version number of the Client Service configuration file on the client computer. When the configuration file is updated on the server, the client version will be updated within 30 seconds.
- **Server configuration version** – The version number of the Client Service configuration file on the server.
- **Last checked** – The last date and time the client status information was checked.
- **Status** – The status of the client, either *Running* (Started) or *Stopped*.
- **Client Version** – The version number of the Client Service software installed on the server.
- **Server Version** – The version number of the Assureon software installed on the cluster.
- **Number of files in journal folder** – The number of files stored in the journal directory. Files are stored in this directory in the event of a network problem; should always be 0.
- **Path to journal folder** – The location on the journal folder on the computer where the client is installed.
- **Available journal disk space** – The amount of disk space available to the journal folder.
- **Primary server** – The name or IP address of the primary Assureon server.
- **Secondary server** – The name or IP address of one or more secondary Assureon servers.
- **Security model** – Selects the security model for the client computer. Choose between [Access Classifications](#) or [NTFS Integrated](#)
- **Save icon** – Saves the change to the security model.
- **Close icon** – Closes the dialog box.

## Using the Assureon Services page

The following is a brief description of Assureon services:

- **Audit Server** – Verifies the integrity of archived files. Takes corrective action when required
- **Configuration Server** – Manages Assureon database configuration information
- **Customer Info Server** – Manages security, retention policies and assigns encryption keys
- **Disk Monitor** – Monitors available disk space
- **Disposition Manager** – Disposes of selected expired files
- **Events Manager** – Enables the Display of Assureon-related events in the System Administration Events page
- **Key Manager** – Along with the Key Server, handles encryption keys
- **Manifest Server** – Sends copies of the file manifests to the key server
- **Object File Server** – Deletes temporary files and manages the online cache option used with optical storage devices
- **Object Request Broker** – Handles file transfers between the FSW and the Assureon cluster
- **Read Server** – Handles read access to archived files
- **Restore Server** – Restores files from the store to a specified directory
- **Storage Server** – Handles the storage of meta data and files. Also handles compression and encryption of files.
- **Storage Web Services** – Web service that manages storage and read requests
- **System State** – Provides an overview of system health and statistical information
- **System State Web Services** – Provides access to the Assureon system for the System State service
- **Time Stamp Server** – Digitally signs Assureon meta data files with date and time information
- **Transaction Recovery Server** – A fail-safe mechanism that ensures that all file storage transaction requests are completed
- **Services Manager** – Starts and Stops Assureon services, taking into account dependencies

In a multi-node configuration, all services are installed on all servers. Only those services that are used by Assureon on a particular node are started.

### Managing services

The **Services** page enables you to start and stop Assureon-related services, including Web services and SQL Server services, that are distributed across all computers in the cluster.

In order to use this feature, the Services Manager service must be started (the default). Once started, services should not be stopped unless you are instructed to do so by Assureon customer support.

#### ► To access this page:

- From the main menu, under **Administration**, click **Services**. For a description of the services, see [Assureon Services](#).

Figure 2-33: Services page

The screenshot shows the Assureon Services page. The left navigation pane has 'Services' selected. The main content area contains a table of services. At the top of the table, there are instructions: 'Drag a column header here to group by that column'. The table has the following data:

Machine Name	Service	Status	Action	Auto Restart
F001-117117	OpenSM	Not Found	Start	<input checked="" type="checkbox"/>
F002-117117	OpenSM	Not Found	Start	<input checked="" type="checkbox"/>
F001-117117	SQL Server	Running	Stop	<input checked="" type="checkbox"/>
F002-117117	SQL Server	Running	Stop	<input checked="" type="checkbox"/>
F001-117117	SQL Server Agent	Running	Stop	<input checked="" type="checkbox"/>
F002-117117	SQL Server Agent	Running	Stop	<input checked="" type="checkbox"/>
F001-117117	Assureon Call Home Server	Running	Stop	<input checked="" type="checkbox"/>
F002-117117	Assureon Call Home Server	Running	Stop	<input checked="" type="checkbox"/>
F001-117117	Assureon Configuration Server	Running	Stop	<input checked="" type="checkbox"/>
F002-117117	Assureon Configuration Server	Running	Stop	<input checked="" type="checkbox"/>
F001-117117	Assureon Events Manager	Running	Stop	<input checked="" type="checkbox"/>
F002-117117	Assureon Events Manager	Running	Stop	<input checked="" type="checkbox"/>
F001-117117	Assureon Customer Info Server	Running	Stop	<input checked="" type="checkbox"/>
F002-117117	Assureon Customer Info Server	StartPending	Start	<input checked="" type="checkbox"/>
F001-117117	Assureon Authorization Manager	Running	Stop	<input checked="" type="checkbox"/>

#### ► Service commands and information:

- **Start All Services** – Starts all Stopped Assureon-related services in the cluster.
- **Stop All Services** – Stops all running Assureon-related services in the cluster. Make sure you clear the Enable Auto Restarts option (see below) if you do not want the services to automatically restart after a 5 second delay. This will not stop the SQL Server and SQL Server Agent services.
- **Refresh** – Refreshes the display with the latest information.
- **Enable Auto Restarts** – Enables the Auto Restart feature for all services.
- **computer** – The name of the server in the Assureon cluster.
- **Service** – The name of the service as it appears in the Windows Services dialog box.
- **Status** – Whether the server is running, stopped, not found or on stand by. It is normal for some services to be in Standing By mode.
- **Auto Restart** – Whether to automatically restart the service after a 5 second delay when the service stops.

#### ► To start or stop a service:

- To start a service that is stopped, click the **Start** link on the same row.
- To stop a service that is already running, click the **Stop** link on the same row.

## Using the Archive Folders Editor

Use the Archive Folders Editor page to create new archive folders for computers or for templates. An archive folder is composed of policy and rule information.

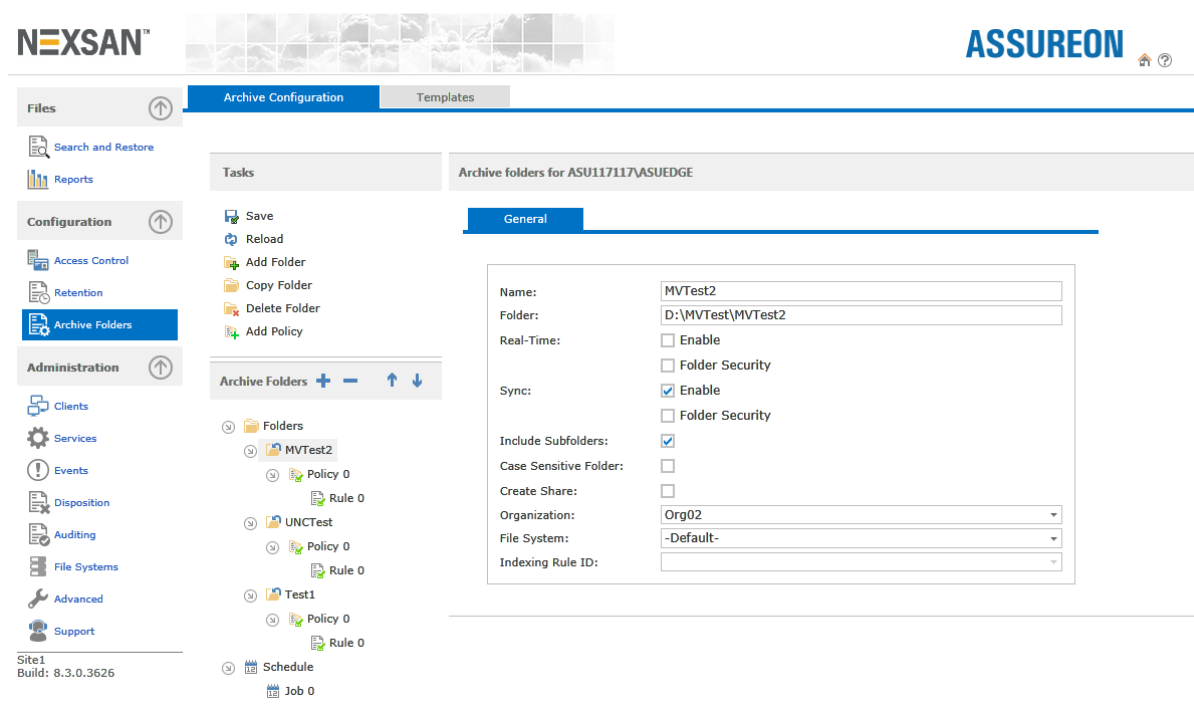
This page is divided into the following panels:

- [Tasks](#) on the facing page
- [Archive Folders](#) on the facing page
- [Archive Folders for](#) on page 75

**Note** Some of the options in the Archive folders for panel apply only to the Synchronization utility.

The **Show global archive folder** option displays the global archive, policy and rule information that is applied to all archive folders.

Figure 2-34: Archive Folders Editor



### ► To create a new archive folder:

1. Select a **Domain** or **computer Name** from the **Archive Configuration** list and click **Edit**.
2. Under the **Tasks** panel, click [Add Folder](#).
3. Specify a **Name** for the archive folder, as well as the folder location. If the archive folder is Real-Time Enabled, and the folder does not exist on the computer, it will be created.
4. Select an **Organization**. This will specify the classifications and retention rules available for the rule.
5. Click on [Policy](#). If you want the rule to apply only to a certain sub folder of the folder specified for the archive folder, specify it in the [Folder](#) match field.
6. Click on the [Include](#) rule and specify classification, retention rule, and processing options.

7. Optionally, click [Add Exclude](#) rule to create rules that exclude certain files from being processed.
8. Click **Save**. Make sure you see the save confirmation message.

► **To edit an archive folder:**

1. Select an archive folder from the Archive Folders list.
2. Make your changes.
3. Click **Save**.

## Tasks

**Tasks** – Saves the current settings and modifies the contents of the **Archive Folders** panel. Options will vary depending on what is selected in the Archive Folders panel.

- **Save** – Saves the archive folder, policies and rules to a configuration file. When saving, make sure you get the confirmation message.
- **Reload** – Reloads the last saved version. Works the same as a revert, any changes made since the file was last saved are lost.
- **Add folder** – Adds a new archive to the Archive Folders list
- **Copy folder** – Copies the selected archive folder
- **Delete folder** – Deletes the selected archive folder
- **Add policy** – Adds a new policy to the selected archive folder
- **Delete policy** – Deletes the selected policy
- **Add Include rule** – Adds an include rule to the selected policy
- **Add Exclude rule** – Adds an exclude rule to the selected policy
- **Delete rule** – Deletes the selected rule
- **Add scheduled job** – Creates an archive schedule
- **Copy scheduled job** – Copies the selected archive schedule
- **Delete scheduled job** – Deletes the selected archive schedule

## Archive Folders

**Archive Folders** – Displays archive folders, policies and rules for the current computer or template. To add archive folders, policies or rules, use the Tasks panel. To expand or collapse all the archive folders, use the + and - icons.

**Up and Down Arrows** – Changes the display and execution order of archive folders, policies and rules. Rules and policies are applied to an archive folder from the bottom up. So, for example, if you have an exclude rule and an include rule with the same selection criteria, and the exclude rule is displayed after the include rule in the Archive Folders panel, the exclude will be applied first.

### *Policy*

Displays policy information when a policy is selected in the Archive Folders panel:

- **Name** – The name of the policy
- **Enabled** – Whether the policy is enabled

- **Folder** – Applies the policy (and its rules) only to folders that match the name, or the regular expression variable specified in this field. For example, **test** will match 1test, test1, alltest, and so on. Blank means the policy is applied to all directories. More than one match may be specified. When specifying a directory structure using regular expression variables, select the Use Regular Expressions option to enable processing of regular expressions; for more information about regular expressions in the directory policy, see [Using regular expressions on page 80](#).
- **Use Regular Expressions** – Processes the variable(s) specified in the Folder field as a regular expression.

### **Rule—General settings**

Displays when you edit a rule.

- **Name** – The name of the rule
- **Access classification** – The classification to associate to the archived files.  
**Flexible classification** allows the retention period for files stored using the current classification to be shortened. For more information, see [Using the Access Control pages on page 52](#).  
**Compliant classification**, which you can specify in archive folder rules, prevents the retention date from ever being reduced. The minimum retention rule is ignored.

See also [Classifying archived files - Access Classification page](#)

- **Retention rule** – The retention rule to apply to the archived files. Retention rules are created in the [Retention Rules](#) page
- **Default retention date** – Specified a retention period for files when the archive folder uses a retention rule with the **Use Read-Only Lock option** and the file access dates are not set in the future. If the file dates are set in the future, then the future date is used as the retention date, and the Default retention date is ignored.
- **Retention date** – The retention date to apply to the archived files. All files stored using this option will expire on the same specified date. For example, you can set this date to 10 years after a project has completed. By using this option, you can be confident that all files for a project are disposed of in one disposition process.  
Can only be applied to files stored using a [retention rule](#) where the Use Custom Retention Date option has been selected.



- **After Storing Files** – Specifies what happens to the original file after it is placed in storage.
  - **Leave files** – Leaves files in their original location after they have been stored. Use this option if users need a local copy of the files for reference or if they plan to edit them.
  - **Delete files** – Deletes files from their original location after they have been stored. Files can only be read or restored using the [Restore Files](#) and [Search](#) pages or the [Assureon Explorer](#).
  - **Replace with shortcuts based on disk space** – Leaves files in their original location. Files are replaced with shortcuts after available disk space falls below a specified threshold. The oldest files are shortcutted first. Works with the shortcut management feature.
  - **Replace with shortcuts** – Shortcuts original files after they have been stored. The shortcut is placed in the same location as the original file. When a file is accessed via a shortcut, and modified, it must be saved under a different name.

The following "Days after" options turn original files that have been stored and left in their original location into shortcuts after a specified period and type of inactivity. To turn the inactive files into shortcuts, run the Synchronization utility after the specified number of days. One or both options may be specified.

- **Shortcut Settings**
  - **Use Regular Expressions** – Processes the variable(s) specified in the Folder field as a regular expression.
  - **Shortcuts To Include** – Specifies which files to shortcut. Criteria can be specified in one or more options. To specify more than one criteria per option, use a comma. Files that meet the criteria are processed.
  - **Shortcuts to Exclude** – Specifies which files to not shortcut. Criteria can be specified in one or more options. To specify more than one criteria per option, use a comma. Files that meet the criteria are processed.
  - **Minimum Shortcut Size** – Sets the minimum size for a shortcut.
  - **Maximum Shortcut Size** – Sets the maximum size for a shortcut.
  - **Days after modification** – Whether to replace the file with a shortcut if it is not modified for the specified number of days.
  - **Days after last access** – Whether to replace the file with a shortcut if it is not accessed for the specified number of days.
- **Process Files** – Specifies the delay in minutes after which a file is processed. One or more of the delay options may be specified. These option apply only to the Synchronization utility.
  - **Minutes after creation** – Whether to delay processing the file for the specified number of minutes based on the file's Date Created property
  - **Minutes after modification** – Whether to delay processing the file for the specified number of minutes based on the file's Date Modified property
  - **Minutes after last access** – Whether to delay processing the file for the specified number of minutes based on the file's Date Accessed property

### ***Rule—Include settings***

Displays rule information when an include rule is selected in the Archive Folders panel:

- **Name** – The name of the include rule
- **Include Files With** – Specifies file selection criteria. Criteria can be specified in one or more options. To specify more than one criteria per option, use a comma. Files that meet the criteria are processed.
- **Match pattern** – A match pattern. For example: \* or \*.\* or resources\*
- **Match pattern RegEx** – A .NET 2.0 regular expression. For example, \belvis\b.\*\balive\b will match elvis is alive but not elvis is dead. For more information about regular expressions, refer to third-party documentation, or to the Web.
- **File name extensions** – A file extension. Include the period in the extension name. For example: .exe.
- **Folder** – A full directory path. For example: c:\test.
- **Folder match** – A partial directory name. For example, **test** will match *1test*, *test1*, *alltestdfg*, and so on. To specify a specific directory, use the **Folder** field.
- **Files starting with** – One or more characters at the beginning of the file name. Files with these characters will be processed.
- **Files ending with** – One or more characters at the end of the file name (including the extension). Files with these characters will be processed.
- **File list** – The full path and name of the files to process. For example: *c:\test\file.txt*

### **Rule—Exclude settings**

Displays rule information when an exclude rule is selected in the Archive Folders panel. Files that match exclude rule criteria will **not** be processed. For examples, see **Include Files With** section (above).

- **Name** – The name of the exclude rule
- **Exclude Files With** – Specifies exclusion criteria. Files that meet the criteria are NOT processed. Criteria can be specified in one or more options. To specify more than one criteria per option, use a comma.
  - **Match pattern** – A match pattern.
  - **Match pattern RegEx** – A regular expression.
  - **File name extensions** – A file extension. Include the period in the extension name. Do not use wild cards.
  - **Folder** – A full directory path.
  - **Folder match** – A partial directory name. For example, **test** will match *1test*, *test1*, *alltestdfg*, and so on. To specify a specific directory, use the Folder field.
  - **Files starting with** – One or more characters at the beginning of the file name.
  - **Files ending with** – One or more characters at the end of the file name (including the extension).
  - **File list** – The full path and name of a file.

### **Schedule**

The Archive Folders Editor page enables you to create archive schedule jobs that you can assign to one or more folders.

- **Add scheduled job** – Creates an archive schedule
  - **Name** – The name of the scheduled job
  - **Enabled** – Whether the schedule is enabled
  - **Sync Type** – Specifies the synchronization type. See [In the Select Synchronization Type page, specify the synchronization type: on page 66.](#)

- **Watches** – Option to select all watches or select specific watches. See [Using Watch variables on page 77](#).
  - **Scheduled Start** – Specifies start of scheduled job
  - **Recur Every** – Specifies recurrence schedule
  - **Copy scheduled job** – Copies the selected archive schedule
  - **Delete scheduled job** – Deletes the selected archive schedule
- **To create a new scheduled job:**
1. Select Schedule in the Archive Folder.
  2. Click [Add scheduled job](#).
  3. Specify a Name for the scheduled job.
  4. Specify the [Sync type](#).
  5. Select the [watches](#) or folders to assign the scheduled job to. To select specific watches, click the Selected watches option, and then, select the individual watches to include in the job; click All watches to include all folders.
  6. Specify the Start date and time, as well as the recurrence.
  7. Click **Save**.

## Archive Folders for

**Archive folders for** – Displays archiving information when an archive folder is selected in the Archive Folders panel. In situations where Assureon is used for compliance purposes, both the Real-time Enabled and Sync Enabled options can be selected; new files will continue to be processed and the sync can be run at any time. When Assureon is used for backup purposes, the Real-time Enabled option should be disabled; New files will only be processed when the synchronization is performed.

- **Name** – The name of the archive folder
- **Folder** – The archive folder. The full directory path is required. If the directory does not exist, the Client Service will create it. UNC and administrative shares are supported; mapped drives are not supported. Assureon also provides watch variables that you can insert into the directory path. The FSW interprets the variables and processes the directory structure accordingly, before starting a sync. For more information about Assureon watch variables, see [Using Watch variables on page 77](#).
- **Real-time** – Specifies real-time options:
  - **Enable** – Whether files sent to the archive folder are processed in real time. To delay file processing, use the Sync Enabled option.
  - **Folder security** – Whether changes to **folder** NTFS security are recorded in real time.
- **Sync** – Specifies sync options:
  - **Enable** – Whether files sent to the archive folder are processed when the File Synchronization utility is run.
  - **Folder security** – Whether **folder** NTFS security is recorded when the File Synchronization utility is run using the Sync folder security option.
- **Include subfolders** – Whether to process files in sub-directories of the archive folder. When selected, files placed in subfolders will also be archived.

- **Case sensitive folder** – Whether to consider case when applying a rule to an archive folder. Applies to folder names and regular expressions. Disabled by default; enable this option when the archive folder is on UNIX (Solaris, RedHat, or Linux).
- **Organization** – The name of the organization to associate the archive folder to. Must be selected in order to apply asset classifications and retention rules to an archive folder.
- **Indexing rule ID** – When the Search Engine (see next topic) is installed, the name of the indexing rule to apply to the archive folder.
- **Stop Sync when updating config** – Displayed only when Show global archive folder is enabled, stops the [File Synchronization](#) utility if it is running when the configuration file is saved. Use this option if you want to apply changes to a sync that is in progress.

## The Search Engine

The **Search Engine** is an optional add-on component that enables you to search and retrieve files from the Assureon store using advanced selection criteria, including file content.

Once installed, the search page is accessed using the Assureon System Administration user interface, [Search and Restore](#) page. The Search Engine also enables file content searching in [Assureon Explorer](#).

The Search Engine uses an indexing rule to store file information, allowing the archived file to be located using content, retention rule and other criteria. Typically, files are assigned an indexing rule when they are archived, using the Indexing Rule ID field value specified for the archive folder (in the Archive Folders Editor page).

Use the Assureon [Indexing wizard](#) to assign an indexing rule to non-indexed files, making them available for advanced searches. For example, if you stored files using an archive folder where the Indexing rule ID was not specified, or if you installed the Search Engine after files were archived, you could run the wizard to assign the indexing rule to those files.

For more information about enabling this powerful option, please contact your Nexsan representative.

## The Indexing wizard

The [Search Engine](#) uses an indexing rule to store file information, allowing the file to be located using content, retention rule and other criteria. Typically, files are assigned an indexing rule when they are stored, using the Indexing Rule ID field value specified for the archive folder (in the [Archive Folders Editor](#) page).

The Assureon Indexing wizard is used to assign an indexing rule to non-indexed files, making them available for advanced searches. For example, if you stored files using an archiving rule where the Indexing rule ID was not specified, or if you installed the Search Engine after files were archived, you could run the wizard to assign the indexing rule to those files.

The wizard is available only if the Search Engine is installed.

► **To access the Indexing wizard in the Windows interface:**

- Select **Start> All Programs> Assureon> Indexing wizard**.

► **To run the Indexing wizard from a command prompt:**

1. Open a command prompt.
2. Change directory to where the wizard was installed and type one of the following commands.

**Note** In the following examples, IRID refers to the Indexing ID. To get the IRID, save an archive folder with Indexing enabled, and open the FSWConfig.XML in notepad. Find the archive folder with indexing. The IRID is the indexingID.

To...	Do this
display the help	<code>IndexWiz /?</code>
index everything	<code>IndexWiz /ALL /IRID &lt;number&gt;</code>
index a classification, for example, EVERTRUST1	<code>IndexWiz /CL EVERTRUST1 /IRID &lt;number&gt;</code>
index a classification and subclassification, for example, EVERTRUST1.RESEARCH01	<code>IndexWiz /CL EVERTRUST1 /SC RESEARCH01 /IRID &lt;number&gt;</code>
index classification EVERTRUST1.RESEARCH01, computer SVDPE01	<code>IndexWiz /CL EVERTRUST1 /SC RESEARCH01 /M SVDPE01 /IRID &lt;number&gt;</code>
index classification EVERTRUST1.RESEARCH01, computer SVDPE01, directory c:\temp	<code>IndexWiz /CL EVERTRUST1 /SC RESEARCH01 /M SVDPE01 /D c:\temp /IRID number</code>
index everything for computer SVDPE01	<code>IndexWiz /M SVDPE01 /IRID &lt;number&gt;</code>
index directory c:\temp from computer SVDPE01	<code>IndexWiz /M SVDPE01 /D c:\temp /IRID number</code>

## Using Watch variables

You can insert Watch variables into the directory path when specifying the archive folder name. The FSW interprets the variables and processes the directory structure accordingly, before starting a sync.

Many applications write data in a nested year/month/day type of structure. The layout of the data makes it obvious where the new data resides. Assureon watch variables allow the FSW to run synchronizations on specific directory sub-trees.

An Assureon watch variable is preceded by the \$( characters and finalized with the ) character. When a synchronization starts, it will expand the watch variable according to the current date and time. That path will be used until the next sync, even if the date changes.

You can have many variables within a single path; for example: `d:\data\$(yyyy)\$(MM)`

Assureon only supports watch variables for full and archive bit syncs. Real-time and change journal are not supported. The system will prevent you from enabling real time or run a change journal sync when the path contains a variable.

[Supported Watch variables](#) below

[Watch variable operators](#) on the facing page

[Examples of Watch variables in the folder path](#) on the facing page

For instructions about creating Watches, refer to the *Assureon Configuration Wizards Guide*, available from the [Assureon Documents & Downloads Web page](#).

### Supported Watch variables

All Assureon watch variables are derived from date variables following the standard Microsoft .Net date variables.

**Note** Variables are case sensitive.

Value	Description (Source: <a href="http://msdn.microsoft.com/en-us/library/8kb3ddd4.aspx">http://msdn.microsoft.com/en-us/library/8kb3ddd4.aspx</a> )	Value Assuming today's date is Monday, April 3, 2017
d	The day of the month, from 1 through 31.	3
dd	The day of the month, from 01 through 31.	03
ddd	The abbreviated name of the day of the week.	Mon
dddd	The full name of the day of the week.	Monday
M	The month, from 1 through 12.	4
MM	The month, from 01 through 12.	04
MMM	The abbreviated name of the month.	Apr
MMMM	The full name of the month.	April
y	The year, from 0 to 99.	17
yy	The year, from 00 to 99.	17
yyy	The year, with a minimum of three digits.	2017
yyyy	The year as a four-digit number.	2017
yyyyy	The year as a five-digit number.	02017

### Watch variable operators

In addition to variable expansion, Assureon supports addition and subtraction operations on watch variables. This is to allow the FSW to sync a directory structure using a point-in-time reference, such as, yesterday, last month, or last year.

For example, `d:\data\$(yyyy-1)` refers to the previous year.

#### Notes:

- You can use only **one** watch variable operator in the folder path.
- When using a watch variable similar to `$(yyyy)$(MM-1)`, where MM-1 represents the previous month, and the current month is January 2019, the system automatically interprets the variable as December 2018.

### Examples of Watch variables in the folder path

The examples listed in this table are based on a date of February 1st, 2019.

You can specify year, month, and day in any order.

Archive Folder	Match Folder
<code>d:\\$(dd)</code>	<code>d:\01</code>
<code>d:\\$(dd-2)</code>	<code>d:\31</code>
<code>d:\\$(MM-2)</code>	<code>d:\12</code>
<code>d:\\$(ddd-2)</code>	<code>d:\Mon</code>
<code>d:\\$(dddd-2)</code>	<code>d:\Monday</code>
<code>d:\\$(MM)</code>	<code>d:\02</code>
<code>d:\\$(MMM)</code>	<code>d:\Feb</code>
<code>d:\\$(MMMM)</code>	<code>d:\February</code>
<code>d:\\$(MM-2)</code>	<code>d:\12</code>
<code>d:\\$(yyyy) or d:\\$(yyy)</code>	<code>d:\2019</code>
<code>d:\\$(yyyy)\\$(MMMM)</code>	<code>d:\2019\February</code>
<code>d:\\$(yyyy)\\$(MMMM-2)</code>	<code>d:\2018\December</code>
<code>d:\\$(yyyy)\\$(MMMM-2)-\$(dddd)</code>	<code>d:\2018\December-Thursday.</code> This is interpreted as Thursday December 1st, 2018.
<code>d:\\$(yyyy)\\$(MMMM)-\$(dddd-2)</code>	<code>d:\2019\January-Monday.</code> This is interpreted as Monday January 31st, 2019.
<code>d:\\$(yyyy)\\$(MMMM-2)\\$(dddd)</code>	<code>d:\2018\December\Thursday</code>

Archive Folder	Match Folder
d:\\$ (yyyy) \\$ (MMMM) \$ (dddd)	d:\2019\FebruaryWednesday
d:\test\\$ (yyyy) \\$ (MMMM) \$ (dddd)	d:\test\2019\FebruaryWednesday
d:\test\\$ (yyyy) \\$ (MMMM-1)	d:\test\2019\January.
d:\test\\$ (yyy) \\$ (MMM) \$ (ddd)	d:\test\2019\FebWed
d:\test\\$ (yyy) \\$ (MMM) -\$ (ddd-2)	d:\test\2019\Jan-Mon. This is interpreted as Monday January 31st, 2019.
d:\test\\$ (yyy) \\$ (MM) -\$ (ddd-2)	d:\test\2019\01-Mon. This is interpreted as Monday January 31st, 2019.
d:\test\\$ (dd-2)	d:\test\31
d:\test\\$ (ddd-2)	d:\test\Mon
d:\test\\$ (dddd) \\$ (yyyy) \$ (MMMM)	d:\test\ Wednesday\2019February

### Using regular expressions

Regular expressions in the directory policy allow you to process directory paths that do not have a fixed data\date-type folder structure. Specifically, you can use regular expressions when the folder structure in the directory path contains multiple directories with different dates, as in this example:

```
D:\data\hsm00001\2019\05
D:\data\hsm00001\2019\06
...
D:\data\hsm00002\2019\06
D:\data\hsm00002\2019\07
...
```

One possible solution for the directory policy described above would be:

```
D:\data\hsm[0-9]{0,9}\$ (yyyy) \$ (mm) .
```

Where:

- Hsm is a literal string that matches hsm;
- [0-9] represents any character between 0 and 9;
- {0,9} represents anywhere from 0 to 9 occurrences of the characters 0 to 9 are allowed.

The FSW uses this regular expression to determine what folders to process; it will process these folders (assuming a date of May 17, 2019):

- D:\data (since it matches everything that is possible to match—nothing DOESN'T match)
- D:\data\hsm123
- D:\data\hsm123\2019\05
- D:\data\hsm123\2019\05\abc

The following directories do NOT match



- D:\data\hsm123\2019\06
- D:\data\exchange

Any directory that does not match is ignored—the sync will not browse deeper into that directory. This means that the FSW can very efficiently find the directories it needs to process and ignore all others.

## Unity Active Archive

When using Unity Active Archive in conjunction with an Assureon Server you now have the ability to set data retention policies to automatically offload stale data and release primary storage. This enables you to increase the performance of your primary storage without increasing its primary size.

If you require data retention policies for compliance and data management you now have the ability to leverage Nexsan tier one storage for your compliance needs. Archiving is useful if you want to:

- Use life-cycle management
- Utilize Assureon features to have better control of your corporate data
- Reduce risk of data loss or corruption
- Use Assureon to store sensitive data which would otherwise require a separate solution from your primary storage

## Using the Events page

This section provides information about these topics:

- [Working with event logs](#) below
- [Managing email alerts](#) on the facing page
- [Using the System Audit Trail](#) on page 85

### Working with event logs

The **Event Log** page monitors the Assureon, Microsoft IIS and Microsoft SQL Server event logs. It consolidates events sent to the Assureon error logs on all the computers in the cluster. The page automatically refreshes every 20 seconds or so. You can also manually refresh using the **Refresh** button. After 2000 events, the events are cleared and saved to file; to view past events, use the **Date Range** option.

► **To access the Event Log page:**

1. From the main menu, under **Administration**, click **Events**.
2. Select the **Event Log** tab.

Figure 2-35: Event Log page

The screenshot shows the Nexsan Assureon Administration interface. The 'Event Log' page is active, displaying a table of events. The table has the following columns: Type, Computer, Time Generated, Source, Message, Category, and Event ID. The event shown is an 'Information' type event from computer 'F001-117117.ASU117117.net' at '2019/01/11 16:02:44'. The source is 'AESystemState' and the category is '(10)'. The message describes monitoring parameters for drive F: and registered storage pool monitors for various storage IDs.

Type	Computer	Time Generated	Source	Message	Category	Event ID
Information	F001-117117.ASU117117.net	2019/01/11 16:02:44	AESystemState	Monitoring parameters for drive F: on F001-117117: Registered disk space monitor. Error if free disk space is less than 10% free. Warning if free disk space is less than 20% free. File ingestion will be stopped when free disk space is less than 2% free and will be resumed when free disk space is greater than 4% free. Registered storage pool monitor for storId 'b' and fsGuid '52aa1876-67ee-49b5-99e9-8f1ff447a80b'.The storId is currently enabled and is not active.The used space threshold for this pool is 95%. Registered storage pool monitor for storId 'b' and fsGuid '7d5efeda-3203-4cc6-ad90-5c0f9a3ce7c5'.The storId is currently enabled and is not active.The used space threshold for this pool is 95%. Registered storage pool monitor for storId 'b' and fsGuid '82c72bc1-e439-4d36-be91-3ba8eb4992'.The storId is currently enabled and is not active.The used space threshold for this pool is 95%. Registered storage pool monitor for storId 'b' and fsGuid 'd8095030-28f6-4137-94a1-7705be92b87e'.The storId is currently enabled and is not active.The used space threshold for this pool is 95%. Registered storage pool monitor for storId 'b' and fsGuid 'e1370c86-408a-422c-8565-d60cce3c7d3a'.The storId is currently enabled and is not active.The	(10)	430

► **Page options:**

- **Save and Clear** – Saves the content of the table to a file and then clears it. To view cleared logs, use the Date Range option.

- **Email Events** – Displays the Email Information dialog box, which enables you to send the current events to a specified email address. The events are sent as a zipped attachment.
    - **SMTP** – The name or IP address of the SMTP server to use to send the message.
    - **To** – The email address of the recipient. Use a semi-colon (;) between multiple recipients. Required.
    - **From** – Your email address. Required, but not validated.
    - **Subject** – A subject line for the email. Required.
    - **Body** – Additional information that you want to add to the email. Optional.
  - **Refresh** – Immediately refreshes the events listed in the table. Also applies the Event Filters.
  - **Auto Refresh** – Whether to refresh the page automatically.
  - **Current Events** – Displays the current event list.
  - **This Month** – Displays the event list for the current month.
  - **Three Months** – Displays the event list for the past three month.
  - **Six Months** – Displays the event list for the past six month.
  - **All** – Displays all saved events.
  - **Custom Date Range** – Displays saved events. **From\To**– Specifies the date range for the **Date Range** option.
- **Table columns:**
- **Type** – The type of message; error, warning, or information.
  - **Computer** – The name of the server in the cluster which generated the message.
  - **Time Generated** – The time, in UTC, when the message was generated.
  - **Source** – The name of the service (as displayed in the Windows Services console) that generated the message.
  - **Message** – The contents of the message sent to the Event Viewer.
  - **Category** – A number used for message tracking.
  - **Event ID** – A second number used for message tracking.

Except for **Message**, columns can be sorted by clicking the column heading.

## Managing email alerts

The **Email Alerts** page specifies whether email alerts containing event information should be sent and to whom they should be sent. In addition, it enables you to enable the **Daily Summary Email** mechanism, which automatically sends emails to inform you of overall system health including status information about external storage and statistical information about ingested data on [Clients](#).

The **Email Alerts** feature is optional, but recommended. This feature enables email alerts for the whole system, including the [System State](#) service.

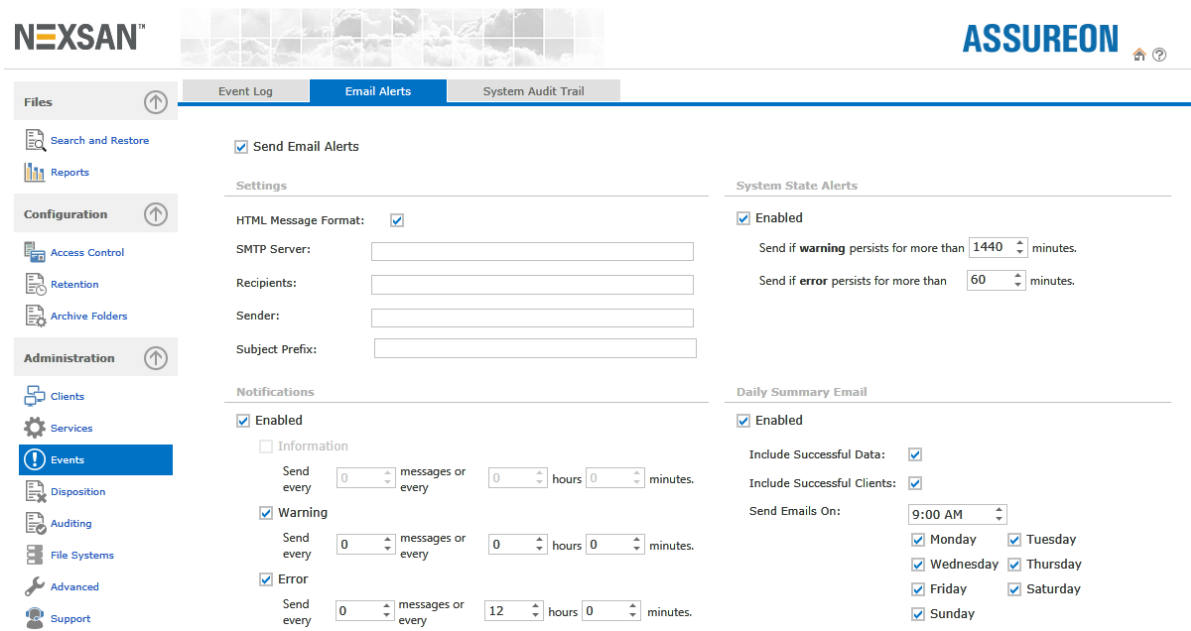
Notifications are sent based on an event count or time period, whichever occurs first. For example, if the Error Rule is configured to send email after 2 events or every hour, and 2 events occur within 15 minutes, an email containing the 2 events will be sent after 15 minutes. If only 1 event occurs during that time period, an email containing the 1 event will be sent after 1 hour. The time period is reset after the email is sent. If no count or time value is specified, the events are automatically sent as they occur.

The system state events are sent using a different set of criteria. If a warning or error occurs for a specified duration of time, a message is sent.

► **To access the Email Alerts page:**

1. From the main menu, under **Administration**, click **Events**.
2. Select the **Email Alerts** tab.

Figure 2-36: Email Alerts page



The page contains the following buttons and options:

**Send Email Alerts** – Whether email alerts should be sent.

**Settings**

- **HTML Message Format** – Whether to send the message using the HTML message format. Most email programs support this format, which allows the message to be formatted. If not enabled, Plain Text format will be used.
- **SMTP Server** – The name or IP address of your email SMTP server. If you do not specify a port, the typical default (:25) will be appended to the IP address.
- **Recipients** – The email addresses of the recipients. Multiple entries can be entered, separated with a semicolon (;) or comma (,).
- **Sender** – The email address of the sender.
- **Subject Prefix** – Adds additional information to the subject line of emails generated by Assureon. Optional.

**Notifications**

- **Notifications Enabled** – Whether to send general system email notifications:
  - **Information** – Whether to send information events. Not recommended. This option is disabled by default. To enable, please contact Nexsan Support.

- **Warning** – Whether to send warning events. Recommended.
- **Error** – Whether to send error events. It is highly recommended that this option be enabled.

### System State Alerts

- **Enabled** – Whether to send system state email notifications:
  - **Warning and Error** – The duration (in minutes) a warning or error condition must persist before an email alert is sent. For example, if you set the Warning duration to 30 minutes, and the CPU spikes for 35 minutes into the warning threshold level, an alert will be sent. This is to prevent unwanted messages which may occur during routine system use. Values must be specified. We recommend that the error value be less than the warning one, and that the warning one be a multiple of the error. For example, an error duration of 15 minutes and warning duration of 45 minutes.

### Daily Summary Email

**Note** The Daily Summary Email is always sent in HTML format, even if the HTML Message Format option is not selected.

- **Enabled** – Whether to send an email providing status on overall system health. The Daily Summary Email includes similar information to what is shown on the System State page, including status information about external storage and statistical information about ingested data on Clients.
  - **Include successful data** – Whether to include information for all statistics and counters on the System State page. If this option is not selected, only disk information and counters with errors are included.
  - **Include successful clients** – Whether to include statistics for all clients. If this option is not selected, only clients with errors are included.
  - **Send Email On** – Specifies the time and days of week to send the Daily Summary Email. The default is daily at midnight.
- **Save Settings** – Applies and saves the current email alert settings.

### Critical alerts

A critical alert is automatically sent to the recipients specified in the **Recipients** field when:

- A computer where the Client Service is installed gets low on disk space
- When a problem is detected on the server with the ignition key, monthly roll, available disk space or with the time synchronization of the Assureon server and the key server.

## Using the System Audit Trail

The **System Audit Trail** page tracks and logs all configuration changes to the Assureon system to facilitate auditing. The page displays all audit trail records available on the system, and provides options for searching and filtering through audit records.

#### ► To access the System Audit Trail page:

1. From the main menu, under **Administration**, click **Events**.
2. Select the **System Audit Trail** tab.

You can display audit trail records logged today, in the past week, in the past month, or all available records, by clicking the corresponding button. You can also filter the list by applying a filter to one or more columns in the table. In addition, you can build more advanced filters by clicking the **Create Filter** button on the bottom-left of the table.

You can also delete all audit records in the audit trail log, or export the records to a Microsoft Excel compatible spreadsheet file (.xsl).

► **To create a filter in the table:**

1. Click **Create Filter** at the bottom of the table; the Filter dialog box displays where you can create a custom filter using operators. The system automatically filters the list of records according to the specified filtering criteria.
2. Click **Clear** at the bottom right of the grid to remove the filter.

You can also filter individual columns by clicking the filter icon in the corresponding column heading and selecting a specific value; for example, to filter the list of audit records by a specific file system, click the filter icon in the Filesystem column heading and select the relevant file system from the drop-down list; the System Audit Trail page automatically filters the list of audit records as you type.

► **To delete all audit records in the log:**

1. Click the **Delete Logs** button.
2. Click **OK** to confirm the action.

► **To export the audit records as a Microsoft Excel compatible spreadsheet file (.xsl):**

1. Click the **Export Logs** button.
2. Click **Save** to specify the location to save the file, or **Open** to open the file.

## Managing disposition of files

Assureon provides extensive controls for file disposition. In Assureon records management, the term "disposition" refers to retention rules for permanent deletion of files.

This section provides information about these topics:

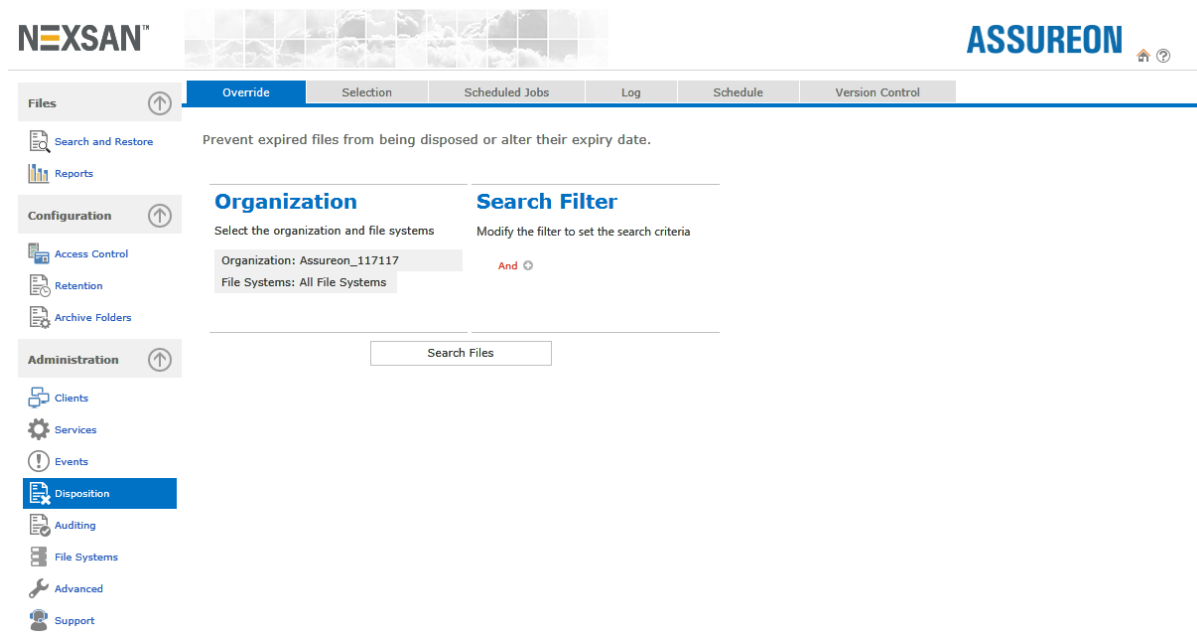
- [Setting disposition overrides](#) below
- [Selecting files for disposition](#) on page 89
- [Working with scheduled disposition jobs](#) on page 91
- [Viewing disposition logs](#) on page 92
- [Changing the disposition schedule](#) on page 93
- [Scheduling disposition of excess file versions](#) on page 94
- [Disposing of excess file versions manually](#) on page 95

### Setting disposition overrides

Use the **Disposition Override** page to prevent selected expired files from being disposed, and to set new retention dates. You can also use this page to retrieve a file.

When a stored file passes its retention date, it expires and automatically becomes a candidate for disposition. To prevent a file from being disposed, use the Block Disposition options described below. Files that have been blocked, will not be displayed in the [Disposition Selection](#) page. A file can be blocked from disposition at any time.

Figure 2-37: Disposition Override page



► **To access the Override page:**

1. From the main menu, under **Administration**, click **Disposition**.
2. Select the **Override** tab.

When you access the **Override** tab, you must first search for the files that you want to prevent disposition for, by specifying the Organization and File System where the files are archived to, and if needed, specifying additional search criteria by activating the filters under Search Filter.

You can also display all files in a given Organization and all its File Systems, without filtering.

► **To search for files:**

1. Under Organization, click the Organization filter and select the organization where the files that you want to prevent disposition for are archived.
2. Click the File Systems filter to select the relevant file system.

Under **Search Filter**, click the **And** link to build a filter that will search for specific files. It opens a drop-down list from where you can select operators and filter elements, or remove them.

Click the + icon after specifying an operator to start building your filter. You can build filters using multiple operators and criteria, giving you the flexibility to filter by computer name, file and folder name variations, ingestion and modified dates, a combination of all of these, and so on.

Depending on the type of search criteria selected, you must either enter an appropriate value in the text box, select from a list of available values, or select a date entry from the calendar that appears when you click the arrow in the text box.

3. Once you specify the desired search criteria, click the Search Files button to begin searching the store for files that meet the criteria.

The system searches the store for files and displays those that meet the specified criteria in a grid. If multiple, or All File Systems were selected as part of the search criteria, the grid displays files in the first file system specified.

To display files that match the search criteria in one of the other file systems you specified, select the corresponding file system in the File System to display drop-down list, at the top of the grid.

Similarly, for plus systems, search results are displayed for only one site at a time; to display search results on another site, click the corresponding site's radio button next to the Site to display field.

► **To block or allow disposition for the files displayed in the grid:**

1. Once you search for the files that you want to modify and they appear in **Search Results**, click the [Block Disposition](#) or the **Allow Disposition** buttons. A popup displays prompting you for a name to assign to the task, which you can then monitor under the **Tasks** tab, on the System State page.
2. Specify a name and click **OK**.

► **To set a new retention date for the files displayed in the grid:**

1. Once you search for the files that you want to modify and they appear in **Search Results**, click the **Change Retention Date** button. A popup displays prompting you for the retention date, as well as a name to assign to the task, which you can then monitor under the **Tasks** tab, on the System State page.
2. Specify the retention date and a name for the task, and then click **OK**.



► **File details:**

- **Signature ID** – The system-assigned file identification.
- **Start Transaction Time** – The date and time the file was stored.
- **File Name** – The name of the stored file.
- **Directory** – The name of the directory the file originated from.
- **computer Name** – The name of the computer the file originated from.
- **Retention Id** – The retention rule that was applied to the file when it was stored.
- **Retention Date** – The date after which the file becomes available for disposition. Calculated by the system based on the date the file was stored or as specified using the **Set Retention Date** button.
- **Read Access Allowed** – Whether the file has read access enabled.
- **Block Disposition** – Whether the file is available for disposition and displayed in the disposition candidate list.
- **Selection, Open File** – Click the link to open the file in the corresponding row.

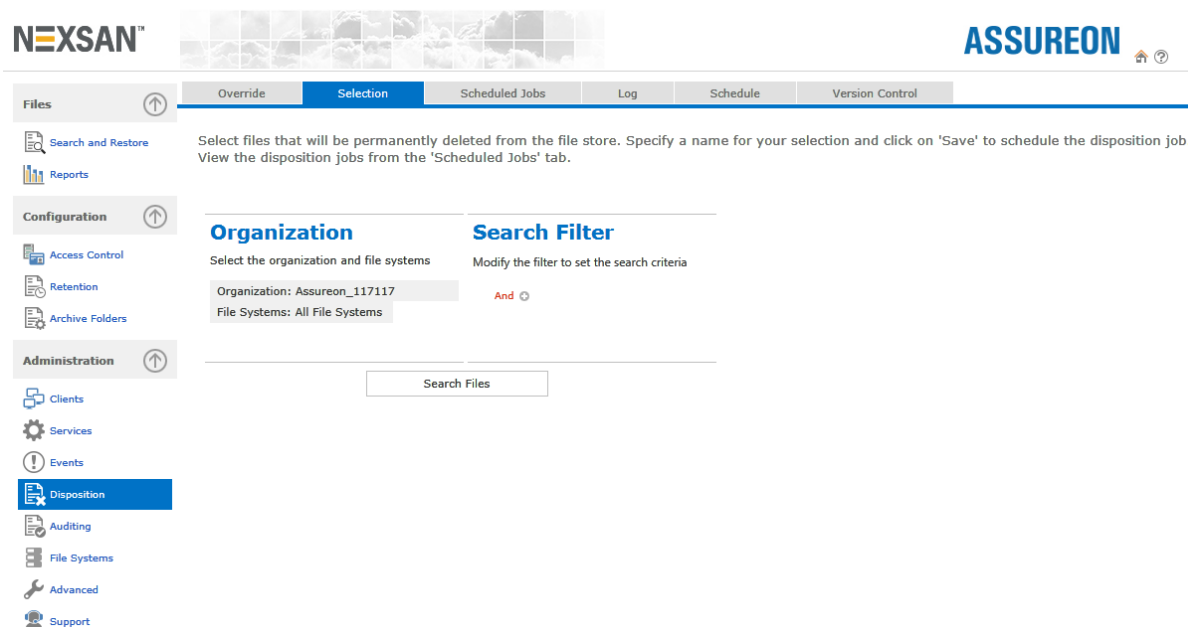
### Selecting files for disposition

Use the **Disposition Selection** page to select files that will be permanently deleted from the Assureon store. Only files that have passed their retention date are displayed. Once selected, the files will be disposed of as per the [disposition schedule](#) or by clicking **Dispose Now** in the [Scheduled Jobs](#) page.

► **To access the Selection page:**

1. From the main menu, under **Administration**, click **Disposition**.
2. Select the **Selection** tab. To block a file from disposition, or to set a new retention date, use the [Disposition Override](#) page.

Figure 2-38: Disposition Selection page



When you access the **Selection** tab, you must first search for the files that you want to permanently delete, by specifying the Organization and File System where the files are archived to, and if needed, specifying additional search criteria by activating the filters under Search Filter.

You can also display all files in a given Organization and all its File Systems, without filtering.

► **To search for files:**

1. Under Organization, click the Organization filter and select the organization where the files that you want to permanently delete are archived.
2. Click the File Systems filter to select the relevant file system.

Under **Search Filter**, click the **And** link to build a filter that will search for specific files. It opens a drop-down list from where you can select operators and filter elements, or remove them.

Click the + icon after specifying an operator to start building your filter. You can build filters using multiple operators and criteria, giving you the flexibility to filter by computer name, file and folder name variations, ingestion and modified dates, a combination of all of these, and so on.

Depending on the type of search criteria selected, you must either enter an appropriate value in the text box, select from a list of available values, or select a date entry from the calendar that appears when you click the arrow in the text box.

3. Once you specify the desired search criteria, click the **Search Files** button.

The system searches the store for files and displays those that meet the specified criteria in a grid. If multiple, or All File Systems were selected as part of the search criteria, the grid displays files in the first file system specified.

To display files that match the search criteria in one of the other file systems you specified, select the corresponding file system in the File System to display drop-down list, at the top of the grid.

Similarly, for plus systems, search results are displayed for only one site at a time; to display search results on another site, click the corresponding site's radio button next to the Site to display field.

► **To create a disposition list:**

1. Once you search for the files that you want to modify and they appear in Search Results, click the Save Disposition Job button. A popup displays prompting you for a name to assign to the task, which you can then monitor under the Tasks tab, on the System Stage page.
2. Specify a name and click OK. The job is created and displayed on the Scheduled Jobs page.

► **File details:**

- **Signature Id** – The system-assigned file identification.
- **Start Transaction Time** – The date and time the file was stored.
- **computer Name** – The name of the computer the file originated from.
- **Directory** – The name of the directory the file originated from.
- **File Name** – The name of the stored file.
- **Retention Date** – The date after which the file becomes available for disposition. Calculated by the system based on the date the file was stored or as specified using the [Disposition Override](#) page.

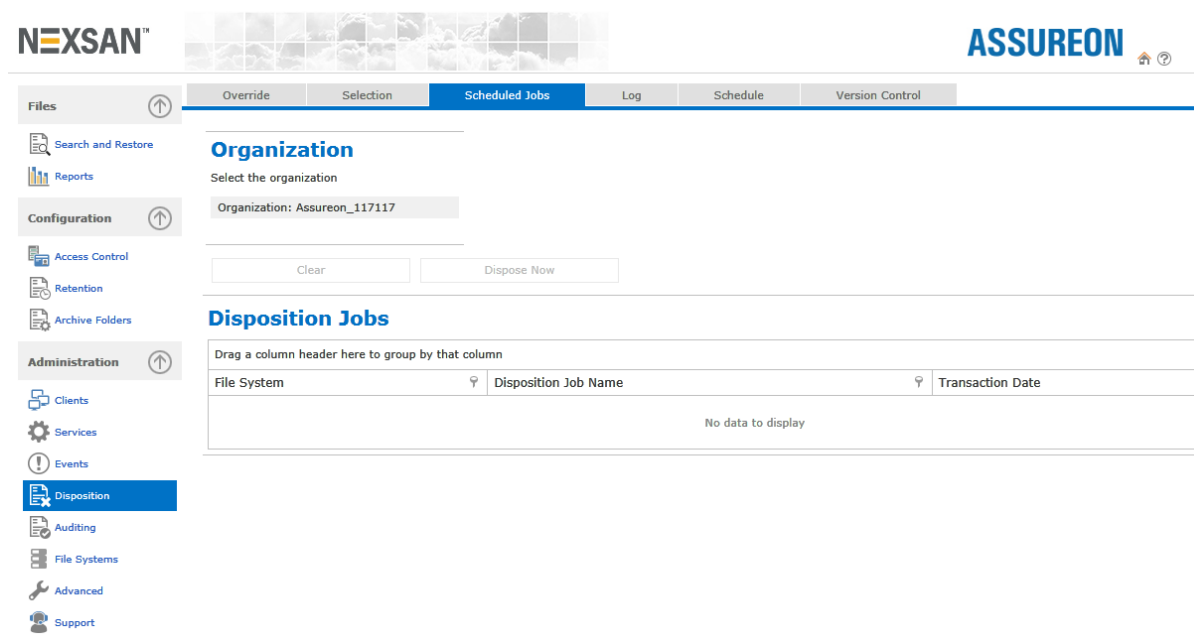
## Working with scheduled disposition jobs

Use the **Scheduled Jobs** page to remove existing disposition jobs or to perform a disposition. Disposition selections are created using the [Selection](#) page.

► **To access this page:**

1. From the main menu, under **Administration**, click **Disposition**.
2. Select the **Scheduled Jobs** tab.

Figure 2-39: Scheduled Disposition Jobs page



► **To clear pending jobs:**

- Select the disposition jobs and then click **Clear**.

► **To process disposition jobs:**

- To process jobs before the scheduled time, select them and then click **Dispose Now**.

The page contains the following buttons and table columns:

- **Organization** – The organization the files were selected for disposition from.
- **File System** – The file system within the specified organization the files were archived to.
- **Disposition Job Name** – The job created using the [Selection](#) page.
- **Transaction Date** – The date the job was created.
- **Clear** – Removes selected items from the table
- **Dispose Now** – Starts the selected disposition jobs immediately.

## Viewing disposition logs

The **Disposition Log** page displays the disposition logs generated by the Disposition Server for the selected date range. The Disposition Server is a service that permanently deletes expired files from storage using a disposition list created with the [Disposition Selection](#) page. The [Disposition Schedule](#) determines when files are deleted.

► **To access the Disposition Log page:**

1. From the main menu, under **Administration**, click **Disposition**.
2. Select the **Log** tab.

► **Disposition log options:**

- **Organization** – The organization the files were disposed from.
- **View Log** – Displays the disposition logs for the specified date.

► **To display the disposition logs:**

1. Select the Organization.
2. Specify a time frame: This Month, Three Months, Six Months, All or Custom.
3. Click the **View Logs** button.

► **Disposition Log table:**

- **File System** – The file system within the specified organization the files were disposed from.
- **ID** –The name of the Disposition Log file
- **Disposition Time** – The time, in UTC, the disposition started
- **Number of Files**– The number of files deleted
- **Disposed** – Whether the disposition completed successfully
- **Details** – Lists the files that have been disposed of, per disposition file. Allows you to verify that files have been disposed of.

Except for the **ID** column, columns can be sorted by clicking the column heading.

► **Details table:**

- **Asset Classification** – The classification, subclassification and serial number of the disposed file
- **Computer** – The name of the computer the files originated from
- **Directory** – The name of the directory the files originated from
- **File Name** – The name of the disposed file
- **Disposed Date** – The date the file was disposed

## Changing the disposition schedule

Use the **Disposition Schedule** page to modify the default disposition schedule. The schedule specifies the time of day when files selected for disposition are permanently deleted from storage. For information about how to select files for disposition, see [Disposition Selection](#).

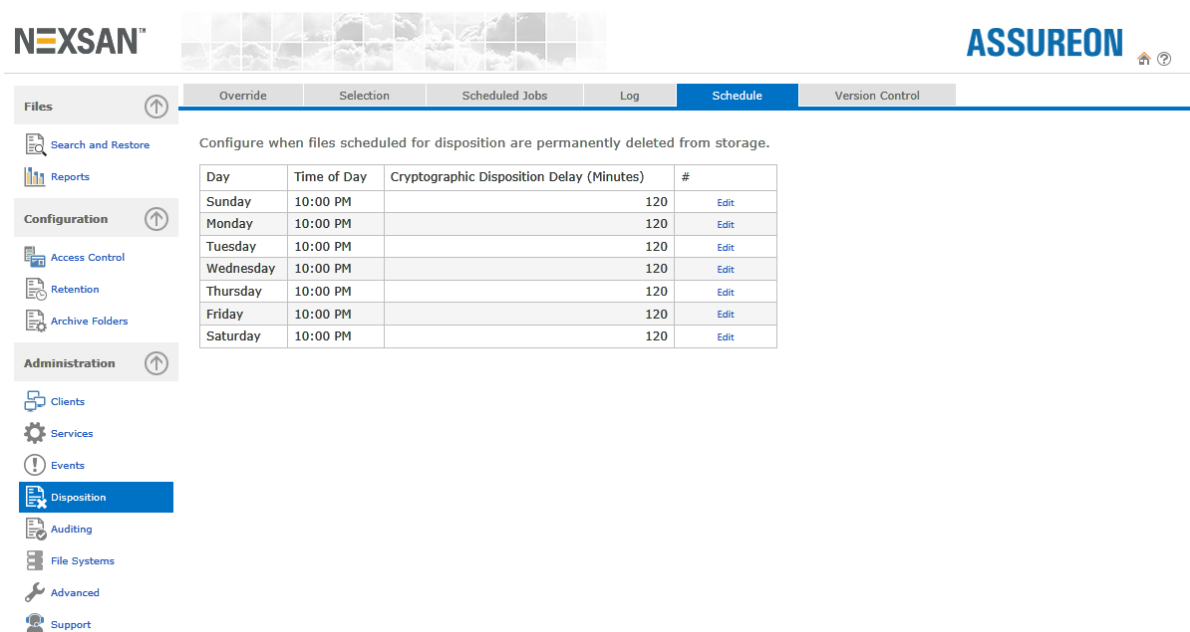
The time of day is local time. The new schedule takes effect the next day.

**Note** Only one disposition can be scheduled per day, so if you change the schedule after a disposition has started or completed, the new time will take effect only on the next day.

► **To access the Scheduled Jobs page:**

1. From the main menu, under **Administration**, click **Disposition**.
2. Select the **Scheduled Jobs** tab. Files can also be disposed of immediately, see the [Scheduled Jobs](#) Jobs page for details.

Figure 2-40: Disposition Schedule page



► **To edit the disposition schedule:**

1. Click the **Edit** link for the day of the week you want to modify.
2. Modify the disposition or delay time.
3. Click **Update**.

► **Disposition schedule details:**

- **Day** – The day of the week the disposition will occur.
- **Time of Day** – The time of day that the files in the disposition list are disposed of.
- **Cryptographic Disposition Delay (Minutes)** – The delay, in minutes, after the file has been disposed of, that the encryption keys associated with the file will be permanently destroyed. The default, recommended value is 120 minutes; the maximum value is 1380 minutes.

## Scheduling disposition of excess file versions

In non-compliance situations, where Assureon is used as a backup storage system, Assureon can be configured to dispose of excess versions of a file. By versions of a file, we mean a file stored using the same name, from the same directory and computer, but having different content.

The oldest files (those having an earlier **Date Modified** attribute) will be disposed of first.

► **To create an archive folder that uses this option:**

1. Access the Assureon System Administration console.
2. Click **Access Control** on the main menu to display the [Access Classification](#) page and create a classification that uses a flexible retention date.

3. Click **Retention** on the main menu to access the [Retention Rules](#) page and create a retention rule. Specify the maximum number of versions of a file to keep and then specify a Minimum Retention Period of 1 day if you want to be able to dispose of excess files as soon as possible after the maximum number of versions to keep is exceeded. If you want to keep excess files for a while, specify the minimum number of days to keep them.
4. Click **Archive Folders** on the main menu to access the [Configurations](#) page and then create an archive folder that uses the new classification and rule.

► **To delete the excess files:**

1. Excess file versions are automatically turned into disposition candidates every evening, right after the scheduled disposition has completed.  
You can also turn the excess file versions into disposition candidates manually, by using the [Disposition Version Control](#) page.
2. After the files have been turned into disposition candidates (either during the overnight process or manually), click **Disposition > Selection** to display the [Disposition Selection](#) page. Select the candidates and then save the disposition selection. The excess file versions, along with all other disposition candidates, will be disposed of at the next scheduled disposition time.

## Disposing of excess file versions manually

Use the **Disposition Version Control** page to manually turn excess file versions into disposition candidates. By default, Assureon performs this function every day after the scheduled disposition time.

► **To access the Version Control page:**

1. From the main menu, under **Administration**, click **Disposition**.
2. Select the **Version Control** tab.

Figure 2-41: Version Control page

The screenshot displays the Assureon Version Control page. At the top, there are navigation tabs: Override, Selection, Scheduled Jobs, Log, Schedule, and Version Control (which is currently selected). The page content includes a header with the NEXSAN and ASSUREON logos. Below the tabs, there is a section titled 'Organization' with a text input field containing 'Organization: Assureon\_117117' and a 'Start Version Control' button. A green message at the bottom of the main content area reads '0 excess file versions were turned into disposition candidates.' The left sidebar contains navigation menus for Files, Configuration, and Administration, with 'Disposition' highlighted under Administration.

► **To turn excess files into disposition candidates:**

1. Select an Organization.
2. Click **Yes**.

The process may take some time, depending on the number of files involved. After the files have been turned into disposition candidates, they may be disposed of using the disposition procedure.

## Using the Auditing page

This section provides information about these topics:

- [Managing integrity audits](#) below
- [Using the Scheduled Audit Configuration wizard](#) on page 98
- [Using the Manual Audit Configuration wizard](#) on page 99
- [Viewing integrity audit logs](#) on page 101
- [Viewing incomplete transaction logs](#) on page 102

## Managing integrity audits

Use the **Integrity Audit** page to view scheduled audit status and data, and to configure scheduled or manual audits. The audit servers are services that verify the integrity of files under management. On multi-node clusters, there is one audit server per Assureon server. For expediency, each server audits a section of the store.

When a file is stored in Assureon, it is copied to two locations, usually on two different storage devices (in Assureon Plus configurations, the second copy is on the other location). When an audit is performed and a file is determined to be corrupted, it is replaced with a good copy from the second location. Also, when a file is found in only one location, it is copied to the second. These corrective actions are described in the [integrity log](#).

To perform a file systems audit, you must first create and configure a schedule for automatic file system audits using the [Scheduled Audit Configuration wizard](#), which you access from the Integrity Audit page. You can also configure and perform a manual audit using the [Manual Audit Configuration wizard](#).

► **To access the Integrity Audit page:**

1. From the main menu under **Administration**, click **Auditing**.
2. Click the **Integrity Audit** tab.



Figure 2-42: Integrity Audit page

The screenshot shows the 'Integrity Audit' page in the Nexsan Assureon interface. The page is divided into three tabs: 'Integrity Audit' (selected), 'Integrity Logs', and 'Incomplete Transaction Log'. Below the tabs are two buttons: 'Configure Scheduled Audit' and 'Configure Manual Audit'. The main content area is titled 'Scheduled Audit Status' and lists two audits:

Audit ID	Status
F001-117117	Completed
F002-117117	Completed

For each audit, the following details are provided:

- Status:** Completed
- File system:** [Redacted]
- Current step:** [Redacted]
- Current object:** [Redacted]
- Number of objects processed:** 70720 (for F001) / 22388 (for F002)
- Number of objects to process:** 70720 (for F001) / 22388 (for F002)
- Date step started:** [Redacted]
- Date audit started:** 2019/01/09 00:09 (for F001) / 2019/01/08 00:42 (for F002)
- Date audit last completed:** 2019/01/09 00:12 (for F001) / 2019/01/08 00:45 (for F002)

At the bottom left, the site information is displayed: Site1, Build: 8.3.0.3626.

### ► Integrity Audit options:

- **Configure Scheduled Audit** – Starts the [Scheduled Audit Configuration wizard](#), where you create and configure an audit schedule.
- **Configure Manual Audit** – Starts the [Manual Audit Configuration wizard](#), where you create and configure a manual audit.
- **Manual Audit Status** – Displays the status of a manual audit currently configured on the system. This section displays the following options and controls:
  - **Start/Pause** button – Starts or suspends (pauses) a manual audit currently in progress; when you restart a manual audit after suspending it, the audit process resumes from the point at which it was suspended.
  - **Cancel** button – Stops a manual audit currently in progress. If you restart a manual audit after stopping it, the audit process restarts at the beginning.
  - **View Auditing Details** button – Displays configuration information for the manual audit; this launches the Manual Audit Configuration wizard where you can view read-only configuration settings for the manual audit.

- **Scheduled Audit Status** – Displays the status of a scheduled audit currently configured on the system. This section displays the following options and controls:
  - **Start/Pause** button – Starts or suspends (pauses) a scheduled audit currently in progress; when you restart a scheduled audit after suspending it, the audit process resumes from the point at which it was suspended. This button is not displayed if a scheduled audit is currently not in progress.
  - **Cancel** button – Stops a scheduled audit currently in progress.
  - **View Auditing Details** button – Displays configuration information for the scheduled audit; this launches the Scheduled Audit Configuration wizard where you can view read-only configuration settings for the scheduled audit.

## Using the Scheduled Audit Configuration wizard

Use the Scheduled Audit Configuration wizard to create and configure a schedule for automatic file system audits.



**CAUTION:** When you create a new scheduled audit, Assureon replaces the current scheduled audit, if it exists, with the new one.

► **To launch the Scheduled Audit Configuration wizard:**

1. From the main menu under **Administration**, click **Auditing**.
2. Click the **Integrity Audit** tab.
3. Click **Configure Scheduled Audit**.

Figure 2-43: Scheduled Audit Configuration wizard



**NEXSAN™**

### Welcome to the Audit Configuration Wizard

Welcome to the Audit Configuration Wizard

This wizard will configure the system audit process

4. In the **Welcome** page, click the **Next** arrow to continue.

5. In the **Organizations and File Systems** page, select organizations and file systems to audit:
  - **Audit all organizations and file systems** – Select this option to create an audit schedule for all organizations and file systems; this is the default selection.
  - **Audit all active file systems** – Select this option to create an audit schedule for active file systems only.
  - **Audit all inactive file systems** – Select this option to create an audit schedule for inactive file systems only.
  - **Customize organizations and file systems to audit** – Select this option to create an audit schedule for specific organizations and file systems; you are prompted to select the relevant organizations and file systems on the next page of the Scheduled Audit Configuration wizard.
6. In the **Organizations and File Systems** page 2, select organizations and file systems to audit. Some, or all, organizations and file systems on this page are automatically selected for auditing depending on the auditing option specified on the previous page.
7. In the **Auditing Options** page, set options and settings for the scheduled audit:
  - **Schedule** – Specify the interval, in days, between audit runs. The default interval is 14 days.
  - **File System Audit** – checks for missing files and for file corruption. Any problems are reported in the integrity log and corrective action is taken. Enabled by default.
    - **Audit Meta Data** – checks for [empty files](#). Problems are reported in the integrity log and corrective action is taken. Enabled by default.
    - **Audit Assets** – compares transaction information with archived files and meta data files; verifies that nothing has been deleted from the store. Enabled by default.
    - **Audit Database Records** – compares database records with archived files and meta data. Problems are reported in the integrity log and corrective action is taken. Disabled by default.
    - **Process Remote Audits** – on remote systems, compares files found on both sites. Disabled by default.
8. The wizard has finished gathering information. Click the **Next** arrow to continue. Assureon creates the audit schedule.
9. The wizard is configuring. The wizard displays the configuration process. Assureon informs you when the process completes. Click the **Close Audit Configuration wizard** link.

By default, scheduled audits run every evening at 9 PM (local time). On weekends, they run continuously. You can also start a scheduled audit manually by clicking the **Start/Pause** button in the **Scheduled Audit Status** section on the [Integrity Audit](#) page.

## Using the Manual Audit Configuration wizard

Use the Manual Audit Configuration wizard to configure and initiate a manual audit.



**CAUTION:** When you create a new manual audit, Assureon replaces the current manual audit, if it exists, with the new one.

### ► To launch the Manual Audit Configuration wizard:

1. From the main menu under **Administration**, click **Auditing**.
2. Click the **Integrity Audit** tab.

3. Click **Configure Manual Audit**.

Figure 2-44: Manual Audit Configuration wizard



NEXSAN™



---

## Welcome to the Audit Configuration Wizard

Welcome to the Audit Configuration Wizard

This wizard will configure the system audit process

---

4. In the **Welcome** page, click the **Next** arrow to continue.
5. In the **Organizations and File Systems** page, select organizations and file systems to audit:
  - **Audit all organizations and file systems** – Select this option to configure and initiate a manual audit on all organizations and file systems; this is the default selection.
  - **Audit all active file systems** – Select this option to configure and initiate a manual audit on active file systems only.
  - **Audit all inactive file systems** – Select this option to configure and initiate a manual audit on inactive file systems only.
  - **Customize organizations and file systems to audit** – Select this option to configure and initiate a manual audit on specific organizations and file systems; you are prompted to select the relevant organizations and file systems on the next page of the Manual Audit Configuration wizard.
6. In the **Organizations and File Systems** page 2, select organizations and file systems to audit. Some, or all, organizations and file systems on this page are automatically selected for auditing depending on the auditing option specified on the previous page.
7. In the **Auditing Options** page, set options and settings for the manual audit. Assureon has multiple audit levels:

**File System Audit** – checks for missing files and for file corruption. Any problems are reported in the integrity log and corrective action is taken. Enabled by default.

  - **Audit Meta Data** – checks for empty file sizes (size = 0). Problems are reported in the integrity log and corrective action is taken. Enabled by default.
  - **Audit Assets** – compares transaction information with archived files and meta data files; verifies that nothing has been deleted from the store. Disabled by default.
  - **Audit Database Records** – compares database records with archived files and meta data files. Problems are reported in the integrity log and corrective action is taken. Disabled by default.
  - **Process Remote Audits** – on remote systems, compares files found on both sites. Disabled by default.
8. The wizard has finished gathering information. Click the **Next** arrow to continue. Assureon creates the manual audit process.
9. The wizard is configuring. The wizard displays the configuration process. Assureon informs you when the process completes. Click the **Close Audit Configuration wizard** link.

Assureon runs the manual audit process as soon as you exit the Manual Audit Configuration wizard. If needed, you can start the manual audit at any time by clicking the **Start/Pause** button in the **Manual Audit Status** section on the [Integrity Audit](#) page.

## Viewing integrity audit logs

Use the **Integrity Logs** page to view the integrity audit logs generated by the [integrity audit](#) for the specified date range.

### ► To access this page:

1. From the main menu, under **Administration**, click **Auditing**.
2. Select the **Integrity Logs** tab.

Figure 2-45: Integrity Logs page

Drag a column header here to group by that column							
Audit Id	Level	Started On	Stopped On	Objects Audited	Errors	Actions Taken	
A11900000006	1	2019/01/09 03:12:20	2019/01/09 03:12:22	14	0	0	
A11900000005	0	2019/01/09 03:12:07	2019/01/09 03:12:20	6	0	0	
A11900000003	0	2019/01/08 03:44:45	2019/01/08 03:45:06	8	0	0	
A11900000002	1	2019/01/02 03:08:58	2019/01/02 03:08:59	14	0	0	
A11900000001	0	2019/01/02 03:08:45	2019/01/02 03:08:58	6	0	0	

### ► To display logs for the current month:

- Click the [View Logs](#) button.

### ► To display integrity logs for a specific date range:

1. Specify a From date.
2. Specify a To date.
3. Click the [View Logs](#) button.

### ► To view corrective action details:

When an error is encountered with a file under management, additional details may be viewed as follows:

1. Display the audit log as described above.
2. Click the [View Logs](#) button to display the report. The report is displayed below the integrity log.

### ► Integrity Logs buttons:

- **Organization** – The organization for which the audit was performed
- **File System** – The file system for which the audit was performed
- **Custom** – Enter the From date, or use the calendar to help specify the date

- **To** – The To date
- **View Logs** – Displays the audit logs for the specified date
- ▶ **Audit Logs table:**
- **Audit ID** –The name of the audit file
- **Level** – The diagnostic level. 0 indicates a file audit; 1 a meta data audit; 3 an integrity audit; 5 means a remote audit. See the [Integrity Audit](#) topic for details.
- **Started On** – The date and time the audit was started
- **Stopped On** – The date and time the audit was stopped
- **Objects Audited**– The number of files audited
- **Errors** – The number of errors encountered during the audit by the Audit Server
- **Actions Taken** – The number of corrective actions taken
- **View** – Displays detailed information about the error encountered and the corrective action taken

## Viewing incomplete transaction logs

Use the **Incomplete Transaction Log** page to monitor for failed or incomplete transactions. Incomplete transactions may occur in the event of a system malfunction, where the system cannot write a file to store.

If an incomplete transaction does occur, check the [Event Log](#) page for warnings or error messages, correct any problems and make sure the transaction completed successfully. To verify whether a transaction completed, use the [Restore Files](#) page to make sure the file mentioned in the log message was stored.

▶ **To access this page:**

1. From the main menu, under **Administration**, click **Auditing**.
2. Select the **Incomplete Transaction Log** tab.

Figure 2-46: Incomplete Transaction Log page

The screenshot shows the Nexsan Assureon Administration interface. The top navigation bar includes the Nexsan logo on the left and the Assureon logo on the right. Below the navigation bar, there are three tabs: Integrity Audit, Integrity Logs, and Incomplete Transaction Log (which is currently selected). The main content area is divided into two columns. The left column contains a sidebar with various navigation options: Files, Search and Restore, Reports, Configuration, Access Control, Retention, Archive Folders, Administration, Clients, Services, Events, Disposition, Auditing (highlighted in blue), File Systems, Advanced, and Support. The right column contains the 'Incomplete Transaction Log' page. It features a search filter section with 'Organization: Assureon\_117117' and a 'View Logs' button. Below this is a table titled 'Incomplete Transaction Logs' with columns: File System, Signature ID, Start Transaction Time, Stop Transaction Time, Computer, Directory, File Name, and md5 Hash. The table currently displays 'No data to display'.

► **Transaction Log Audit details:**

- **Organization** – The organization for which the check will be performed
- **File System** – The file system for which the check will be performed
- **Signature ID** – The system-assigned file identification.
- **Start Transaction Time** – The date and time (in UTC) that the transaction started.
- **Stop Transaction Time** – The date and time (in UTC) that the transaction stopped.
- **Computer** – The name of the computer the file originated from.
- **Directory** – The name of the directory the file originated from.
- **File Name** – The name of the file.
- **md5 Hash** – The md5 (Message-Digest algorithm 5) cryptographic hash of the file contents. Used for support purposes.
- **sha1 Hash** – The sha1 (Secure Hash Algorithm ) cryptographic hash of the file contents. Used for support purposes.

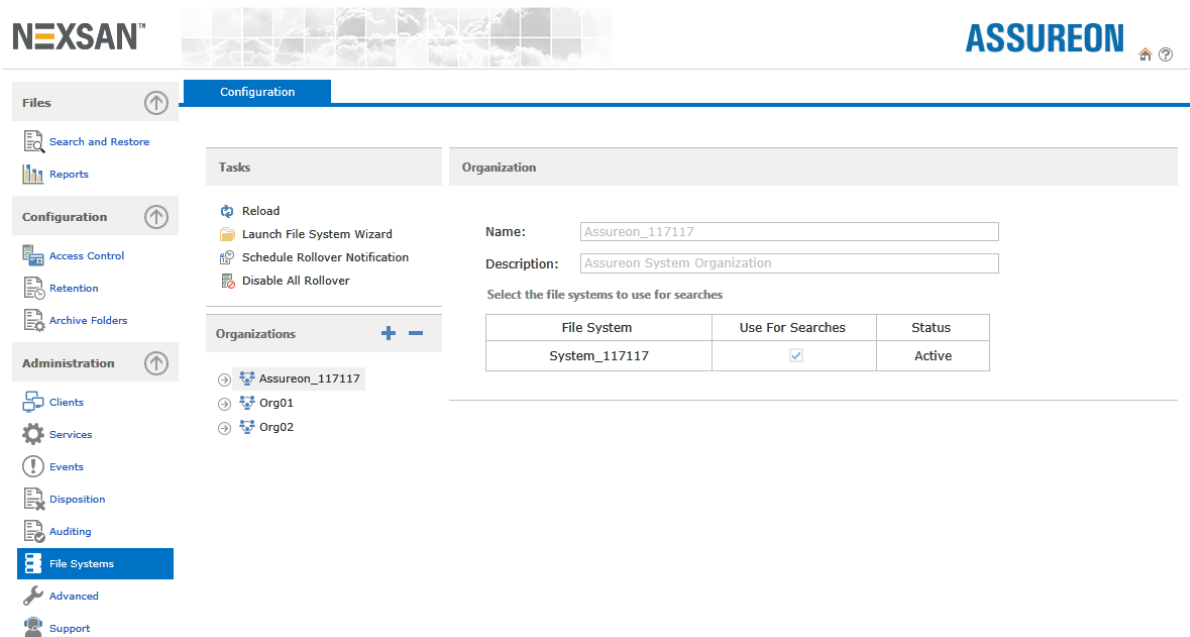
## Configuring File Systems and Organizations

Use the **File Systems** page to configure [Organizations and File Systems](#). An organization is composed of site and file system information. A file system is composed of Database and Storage information. File systems are created using the [File System wizard](#).

► **To access the File Systems page:**

- From the main menu, under **Administration**, click **File Systems**.

Figure 2-47: File System Editor



This page is divided into the following panels:

- [Tasks](#)
- [Organizations](#), and depending on what is selected, you will see this information:
  - [Organization](#)
  - [Site](#)
  - [File System](#)
  - [Database](#)
  - [Storage](#)

### Tasks

**Tasks** – Saves the current settings and modifies the contents of the Organizations panel. Options vary depending on what is selected in the [Archive Folders](#) panel.

- **Reload** – Reloads the last saved configuration. Works the same as a revert, any changes made since the file was last saved are lost.
- **Launch File System wizard** – Displays the [File System wizard](#).



- **Schedule Rollover Notification** – Displays the [Rollover Notification Scheduler](#) where you configure the time that notifications are sent after a rollover condition, that you specified on the [Rollover tab](#) for a file system, is met.
- **Disable All Rollover** – Disables roll over settings for all file systems.

## Organizations

**Organizations** – Displays organizations, sites and file system information. To expand or collapse all available organizations, use the + and - icons.

### Organization

**Organization** – Displays information about the organization selected in the Organizations panel tree. Except where indicated, the fields are for information purposes only, and cannot be modified.

- **Name** – The name assigned to the organization when it was created using the File System wizard.
- **Description** – The description assigned to the organization when it was created.
- **Select the file system to use for searches** – Selects the file systems that will be included when searching using an organization. For example, if a file system is de-selected on this page, it will not be searched when using the Restore Files page.

### Site

**Site** – Displays information about the site selected in the Organizations panel tree. Fields are for information purposes only, and cannot be modified.

- **ID** – A system-generated identification number for the site, created when Assureon was installed.
- **Name** – The name of the site, specified when Assureon was installed.

### File System

**File System** – Displays information about the file system selected in the Organizations panel tree. Some fields are for information purposes only, and cannot be modified. For standby or inactive file systems, none of the fields can be modified.

- **ID** – A system-generated identification number for the file system, created by the File System wizard.
- **Name** – The name of the file system assigned when it was created.
- **Description** – The description assigned to the file system when it was created.
- **Status** – Current status of the file system:
  - *Active* means that the file system is currently being used to store files.
  - *Read-only* file systems can only be used to read or restore archived files. A Read-only file system can be changed to *Active* by selecting **Active** and then clicking **Apply Status Change**. The change takes effect immediately; the previously Active file system is automatically made Read-only. Before making this change, stop all Assureon clients and make sure files are not being archived.
  - *Standby* means that file system is the standby file system in the organization. Assureon automatically rolls over to the standby file system when rollover criteria that you configure for the active file system are met. If an active file system already exists in the organization, and you do not set the new file system as read-only, Assureon automatically sets the file systems as standby.

- **Optimized** – This option adds indexing to specific database entries for the file system, in order to increase the speed of file system search queries. This option should typically only be enabled for read-only file systems as it may impact the performance of file system ingestion.

When you enable this option, Assureon launches the File System Read Optimization wizard, which performs read optimizations on the file system once you confirm the action. The optimization process may take a while to complete, depending on the size of the tables being indexed. While the tables are being indexed, archive files may not be available as the tables will be locked.

- **Default** – Indicates that the current file system is the default one, used for backward compatibility with pre version 6.0 Assureon systems.
- **Rollover tab** – Displays configuration setting and options for file system [rollover](#).

### Database

**Database** – Displays information about the file system database selected in the Organizations panel tree. Fields are for information purposes only, and cannot be modified.

- **Name** – The system generated name of the database.  
**Note** It includes the file system name.
- **Server Name** – The name of the server where the database resides.

### Storage

**Storage** – Displays information about the file system storage selected in the Organizations panel tree. The corresponding table shows information about storage pool mappings for the file system, if applicable, with details on the amount of storage capacity used by each storage location. Fields are provided for information purposes only, and cannot be modified.

- **Store ID** – An identifier for the storage pool
- **Enabled** – Whether or not the storage location is enabled
- **Active** – Whether or not the storage location is active
- **Store1 Server** – The first storage location for assets and metadata files. Specified when the file system was created using the File System wizard.
- **Store1 Volume** – The volume on the first storage location assigned to the file system. Specified when the file system was created using the File System wizard.
- **Store1 %Full** – The amount of disk space, in percentage, currently used by the file system on the first storage location by assets and metadata files.
- **Store1 Stop %** – The disk capacity threshold, in percentage, when, if reached, the system stops writing assets and metadata to the first storage location. The threshold is configured on the [Thresholds](#) page, under System State.
- **Store2 Server** – The second storage location for assets and metadata. On single-write systems this location is blank, as the second storage location is located on the remote site (site 2).
- **Store2 Volume** – The volume on the second storage location assigned to the file system. Specified when the file system was created using the File System wizard.
- **Store2 %Full** – The amount of disk space, in percentage, currently used by the file system on the second storage location by assets and metadata files.

- **Store2 Stop %** – The disk capacity threshold, in percentage, when, if reached, the system stops writing assets and metadata to the second storage location. The threshold is configured on the [Thresholds](#) page, under System State.

## About Organizations and File Systems

Although an Assureon Organization can have multiple File Systems, only one Organization is used to store files at a given time. This file system is designated as active. All other file systems are considered passive, but may be used to retrieve or query files. A new file system can be created at any time, whenever data isolation is required for security or performance reasons. Additionally, file systems may be created per quarter or per year, based on the number of files stored, or per project or per customer. A file system can store millions of objects. By using multiple file systems, the system can handle billions of files. File systems with old data (for example, from 2006) may also be moved to another storage device, typically one with Automatic Massive Array of Idle Disks (AutoMAID) energy saving technology.

Using the Assureon System Administration user interface, many operations can be performed for a single file system or several at a time. For example, you can search and retrieve files from the active and passive file systems, or limit your search to the active file system only.

Associating an archive folder on a client computer to an organization (and its active file system) is done when the archive folder is created, and can be modified at any point in time. The same client computer can have multiple archive folders pointing to different organizations and file systems.

For Plus configurations, organizations may be distributed across different geographic locations, called sites. Plus configurations are active - active and are available in non-ASP and two ASP topologies (see below for details).

### Active-Active Plus configurations

All Active-Active Plus configurations are active – active. That means that both sites can be used to store or read files. A file stored on site 1 is available to be read from site 2, and vice-versa. This feature provides both load balancing and failover capabilities. For example, the Assureon client service can be configured to round-robin between both sites to store files, distributing the processing load to more than one server. In the event of a disaster at one of the sites, the fail over feature will allow users to continue storing and reading files. And, once the site is back online, synchronization is automatically performed.

### Non-ASP model

In the traditional, non-ASP model, a company defines a single organization with 1 or more Assureon file systems, across 2 sites. Both sites are active, data added to site 1 is replicated to site 2 and vice versa.

### ASP fully-hosted model

Like the non-ASP model, the ASP fully-hosted model is active – active. The difference is that more than one organization is defined.

For example, a bank broker has 2 customers, banks ABC and DEF. For data redundancy purposes, the broker uses a Plus configuration, with site1 in New York, site 2 in San Francisco. Using the fully-hosted ASP model, the topology would look like the following diagram.

**Note** The number of organizations and file systems is practically unlimited with the addition of additional storage.

### ASP DR model

In the ASP DR model, multiple primary site 1s, all at different organizations and locations, are coupled with a central data center (acting like a collective site 2). For example, the bank broker has 3 customers, all with their own Assureon cluster on site. For data redundancy, the bank broker has created a site 2 that hosts all the secondary, or passive sites.

**Note** All organizations and file systems hosted at the DR site are completely isolated, both from hardware (they are on different volumes) and software perspective.

### Using the File System wizard

Use the **File System wizard** to create [organizations and file systems](#). An organization is composed of site and file system information. A file system is composed of Database and Storage information.

#### ► To launch the File System wizard:

1. From the main menu, under **Administration**, click **File Systems**.
2. Click the **Launch File System wizard** link.
3. In the **Welcome** page, click the **Next** arrow to continue.
  - **Delete Lock** – Deletes the wizard session lock. This option appears only if a lock exists; This may happen when the wizard is canceled and then restarted within five minutes.
4. In the **Organizations Options** page, create a new organization or to add a file system to an existing organization.

**Create new organization** – Creates a new organization

- **Name** – The name of the new organization. Will be displayed throughout the System Administration UI.
- **Description** – A description for the organization

**Use existing organization** – Adds a file system to an existing organization

- **Name** – The name of an existing organization, select one from the list.

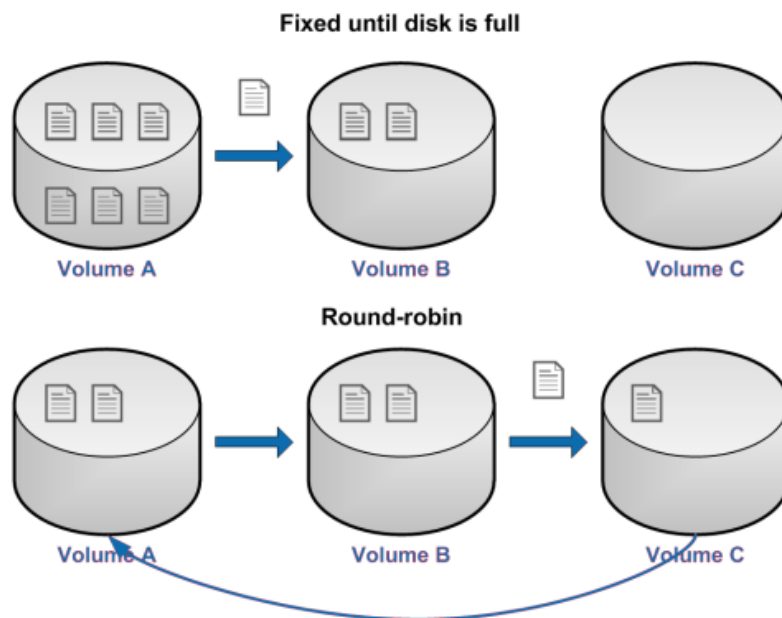
**Create a new File System** – Creates a file system for an organization.

5. In the **File System Options** page, specify the name and description for the file system, and the file system's status. On a remote configuration, this page appears twice: once for site 1 and then for site 2.
  - **File System Name** – A unique name for the file system. The name can contain up to 20 alphanumeric characters; the name is case insensitive. An organization cannot contain two file systems with the same name.
  - **Description** – A description. Maximum of 80 characters.
  - **File System State** – Specify the status of the file system:
    - **Active** – Indicates whether the file system should be the active file system in the organization. Active file systems can be used for archiving files. Only one default file system is allowed per organization; all other file systems are either read-only or standby.
    - **Standby** - Indicates whether the file system should be the standby file system in the organization. Assureon automatically rolls over to the standby file system when rollover criteria that you configure for the active file system are met. If an active file system already exists in the organization, and you do not set the new file system as read-only, Assureon automatically sets the file systems as standby.
    - **Read-only** - Indicates whether the file system should be set as a read-only file system.
  - **Default** – Indicates that the current file system is the default file system, used for backward compatibility with pre-version 6.0 Assureon systems.

- **Optimize:** Indicates whether the system should write round robin between storage writes. Each file is written on a different volume, with the next file going on the next volume. For example, file 1 goes to e:\, file 2 goes to f:\, file 3 goes to g:\, and so on. This results in an even distribution of files across volumes, which spreads out the load.

If this option is not selected, files are written onto one volume until it gets full, then they go on the next volume until it gets full, and so on.

Figure 2-48: Writes to disks—fixed versus round-robin



- In the **Storage Locations for Site** page, specify volumes and configure storage pools for the file system's storage location(s). Assureon enables you to create a storage pool for the file system by expanding the file system over multiple disk arrays (volumes). This enables for more efficient use of disk space and simplifies management. On a remote configuration, this page appears twice: once for site 1 and then for site 2.

For each storage location (Store 1 and Store 2 on systems with Dual-write enabled), configure the following settings:

- **Server** – Select the server where the volume(s) for the storage location exists.
  - **Volume** – Select the (primary) volume to use for the storage location.
  - If needed, modify the space consumption threshold at which Assureon starts writing to the next volume in the storage pool. The default value is 95%; this means that Assureon will write to the next volume in the storage pool when space consumption on the current volume reaches 95%. The space consumption threshold is applied to all volumes in the storage pool.
  - **Do not write to another volume** – Select this option if you do not want to expand the file system over multiple volumes.
  - **Write to** – Select this option if you want Assureon to expand the file system over multiple volumes. The File System wizard automatically suggests volume allocation for the storage pool, based on server configuration. Modify the list of volumes, if needed, by adding or removing volumes, or changing the write order for the volumes; for example, on a system with 3 volumes—`g: \`, `f: \`, and `h: \`—where `g: \` is the primary volume in the storage pool, you can specify the next volume to write to, either `g: /` or `h: /`, by changing the corresponding volume's position in the list using the up or down arrow button.
- In the **File System Volumes for Site** page, modify the volumes that the system automatically assigns to file system meta data, including cache and database files. Assureon automatically suggests optimal volume allocations, based on server configuration.

**Note** Do not modify the suggested volume allocations unless absolutely necessary.

- The wizard has finished gathering information. Click the **Next** arrow to continue. The organization or file system is created.
- The wizard is configuring and displays the configuration process. When completed successfully, a message displays. Click the **Close Assureon File System wizard** link.

## Applying Rollover settings

Use the **Rollover** tab to configure settings and options for file system rollover. Rollovers use a rule-based process to automatically switch to a new, pre-defined file system when the rollover criteria that you configure are met. This process enables the system to optimize when a new file system should be used without administrator intervention. This tab is only displayed for the active file system.

The system automatically checks the system twice a day to see if the rollover criteria that you specified for the file system have been met.

Assureon can roll over to a new file system based on any of the following criteria:

- Number of files archived
- Available disk space for the stores
- A specific date (for example, January 1, 2014)

For the rollover to occur, a new file system must have been created using the [Assureon File System wizard](#), **Stand By** option and selected using the **Select a File System** field on this page.

A warning threshold can be configured to notify administrators that a rollover is approaching. In the case where a rollover is due to the number of files archived, or to lack of disk space, the administrator can dispose of expired files to delay the rollover. An email will be sent to the administrator (if email notification has been configured) when the rollover occurs.

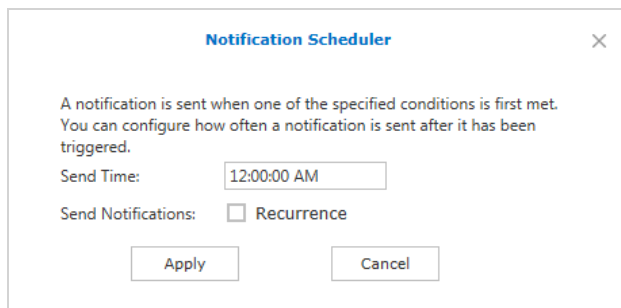
During the rollover, file ingestion will be paused. After the rollover, new files will be archived on the new file system.

- **Apply Template** – Applies the selected template. A template contains predefined information for the fields in this page and is created using the **Save as Template** feature (see below). Templates are a quick way of applying standardized criteria across multiple file systems.
- **Number of Files** – the total number of files archived on the file system
- **Send notification when number of files is more than** – Specifies the number of files, once reached, that will trigger a notification email
- **Roll over when number of files is more than** – Specifies the number of files, once reached, that will trigger the system to roll over to the stand by file system.
- **Available Space** – the amount of disk space used by the file system for the Assureon stores
- **Send notification when available space is less than** – Specifies the amount of disk space, once reached, that will trigger a notification email. Specifies as a percentage of available space.
- **Roll over when available space is less than** – Specifies the amount of disk space, once reached, that will trigger the system to roll over to the stand by file system.
- **Date**
  - **Send notification on** – Specifies a date, once reached, that will trigger a notification email
  - **Roll over on** – Specifies a date, once reached, that will trigger a roll over. For example, if you want to roll over with a new year, you would specify January 1, 2014.
- **Save As Template** – Saves the current information to a file. The Save As Template dialog box is displayed. Specify a name for the file and click **Save**. To apply the template, use the **Apply template** field at the top of the page.
- **Select A File System** – Select a File System that has been created with the File System wizard using the **Standby** option. If you do not already have a file system, you can launch the File System wizard by clicking **New**.

### Scheduling rollovers

Use the **Rollover Notification Scheduler** to configure the time that notifications are sent after a rollover condition, that you specified on the [Rollover tab](#) for a file system, is met.

Figure 2-49: Rollover Notification Scheduler





► **Notification Scheduler options:**

- **Send time** – Specify the time to send notifications.
- **Send Notifications: Recurrence** – Select this option to perform daily checks and resend notifications, as needed.

## Advanced system administration tasks

The **Advanced** menu has the following tabs:

- [Using the IIS Administration page](#) below
- [Using the Job Management page](#) on the facing page
- [Using the Storage Devices page](#) on page 117
- [Using the Authorization Management page](#) on page 117
- [Using the Organization Security page](#) on page 118
- [Using the Options page](#) on page 119

### Using the IIS Administration page

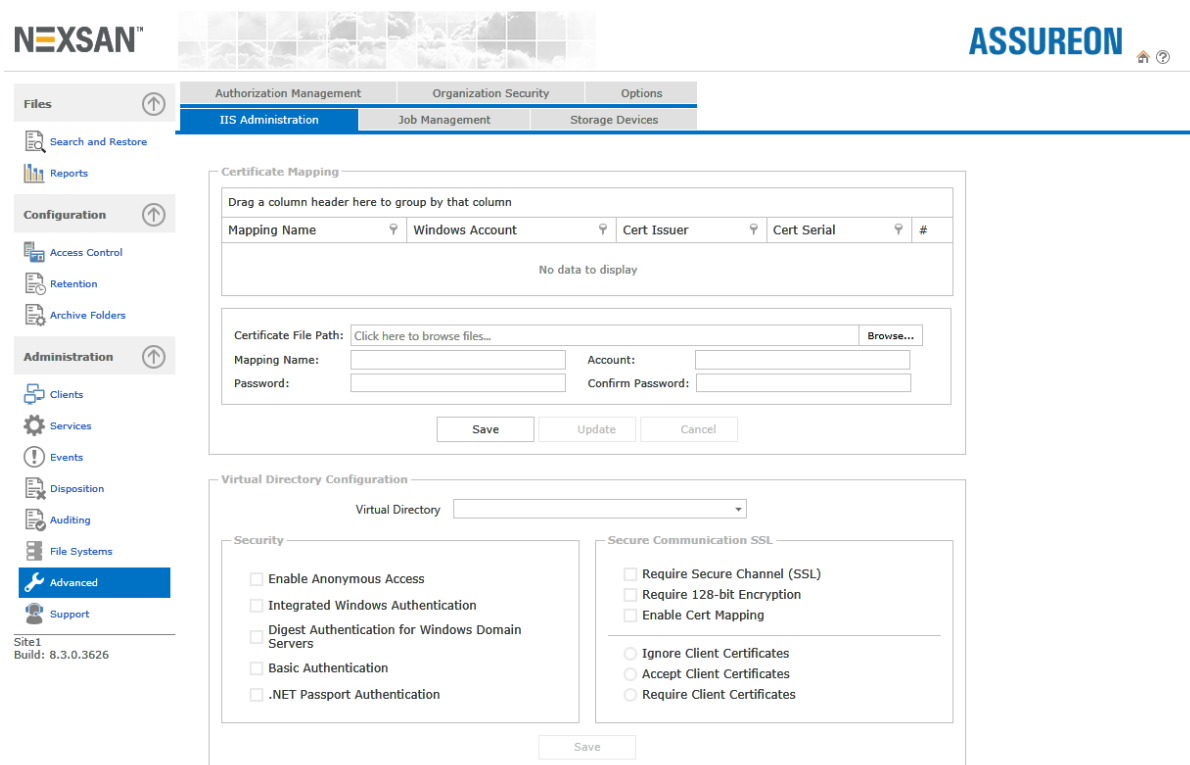
Use the IIS Administration page to configure virtual directory security and secure communications, certificate mapping, and DNS.

Specifically, this page is used when configuring [certificate-based authentication](#).

► **To access this page:**

1. From the main menu, under **Administration**, click **Advanced**.
2. Select the **IIS Administration** tab.

Figure 2-50: IIS Administration page



This page contains the following options and buttons:

- [Certificate mapping](#)
- [Virtual directory configuration](#)
- [IIS administration](#)
- [DNS records update](#)

### Certificate mapping

Maps issue user security certificates to Assureon security groups. For more information about security groups, see [access classification](#). For more information about how to use these fields, see [Using certificates for authentication](#) on page 154.

- **Certificate file path** – The path to the exported user certificate.
- **Mapping Name** – A name for the mapping. Suggestion: include the Client Service computer's name or a specific user's name as part of the mapping name, as this will help you administer the mappings.
- **Account** – The Assureon security group you want to map the Client Service computer or user to.
- **Password and Confirm Password** – The password for the Assureon security group.

### Virtual directory configuration

Modifies virtual directory security and secure communications options.

- **Virtual Directory** – The virtual directory to modify. Select a directory from the list, make your changes and then click **Save**.
- **Security**: For information about these fields, see [Using certificates for authentication](#).
- **Save** – Saves the changes.

### IIS administration

Displays the Assureon security certificate serial number and resets IIS.

- **Server SSL Certificate Serial Number** – The serial number of the AssureonWebServer security certificate. For display purposes only. When configuring Assureon to use certificate-based authentication, you can view and then copy the serial number from this location.
- **Reset IIS** – Stops and then starts the IIS service.

### DNS records update

Updates the Assureon Active Directory DNS with the specified values:

- **Host Name** – The DNS record to update.
- **IP Address** – The IP address to use. May be a comma-delimited list.
- **Update** – Updates the DNS with the change.

### Using the Job Management page

Use the **Job Management** page to monitor or start automated Microsoft SQL Server jobs run by Assureon. This page automatically refreshes every 10 seconds. Assureon uses a SQL Server database to store information about retention rules, classifications, dispositions, transactions, files and other system-related information.

Many maintenance tasks, such as backing up the database and transaction logs, are automated using scheduled jobs. Jobs are also used to update information in Assureon reports. The report jobs are scheduled to run consecutively every night, but can be run manually at any time.

Some report jobs are disabled by default at installation time. To enable them, click the **Disabled** link in the **Job State** column.

► **To access this page:**

1. From the main menu, under **Administration**, click **Advanced**.
2. Select the **Job Management** tab.

Figure 2-51: Job Management page

The screenshot displays the Job Management interface. At the top, there are navigation tabs for 'Authorization Management', 'Organization Security', and 'Options'. Below these are sub-tabs for 'IIS Administration', 'Job Management' (which is selected), and 'Storage Devices'. The main content area shows a table of jobs. The table is filtered by 'Job Type: Maintenance' and 'Job Type: Reports'. Each row represents a job with columns for 'Server Name', 'Job Name', 'Last Run Date', 'Last Run State', 'Current Status', and 'Scheduled'. The 'Scheduled' column contains checkboxes for enabling or disabling jobs. The 'Advanced' menu item in the left sidebar is highlighted.

Server Name	Job Name	Last Run Date	Last Run State	Current Status	History	Start	Scheduled
Job Type: Maintenance							
F001-117117	All databases check integrity	2019/01/05 01:00:00	✓	Idle	History	Start	✓
F001-117117	All databases differential backup	2019/01/11 05:00:00	✓	Idle	History	Start	✓
F001-117117	All databases disposition candidate generation	2019/01/11 00:04:00	✓	Idle	History	Start	✓
F001-117117	All databases file shrink	2019/01/11 02:30:00	✓	Idle	History	Start	✓
F001-117117	All databases full backup	2019/01/06 01:00:00	✓	Idle	History	Start	✓
F001-117117	All databases log backup	2019/01/11 07:00:00	✓	Idle	History	Start	✓
F002-117117	All databases check integrity	2019/01/05 01:00:00	✓	Idle	History	Start	✓
F002-117117	All databases differential backup	2019/01/11 05:00:00	✓	Idle	History	Start	✓
F002-117117	All databases disposition candidate generation	2019/01/11 00:04:00	✓	Idle	History	Start	✓
F002-117117	All databases file shrink	2019/01/11 02:30:00	✓	Idle	History	Start	✓
F002-117117	All databases full backup	2019/01/06 01:00:00	✓	Idle	History	Start	✓
F002-117117	All databases log backup	2019/01/11 07:00:00	✓	Idle	History	Start	✓
Job Type: Reports							
F001-117117	Report New - CAS Base Generation	2018/12/08 14:45:28	✓	Idle	History	Start	✓

► **Job management details:**

- **Job Type** – The type of reports shown in the table.
- **Job Name** – The name of the maintenance or report job.
- **Last Run Date** – The date and time the job was last run.
- **Last Run State** – Whether the job ran successfully.
- **Current Status** – Whether the job is currently running.
- **History** – Displays the last 15 messages generated by the job. For more details on a job, use the Microsoft SQL Server Enterprise Manager to check the SQL Server Logs.
- **Start/Stop** button – Manually starts or stops the job
- **Scheduled** – Whether a job is enabled or disabled. When enabled, it will run at the scheduled time.

For information about other database-related administrative tasks, such as how to track database disk space size, please refer to the SQL Server documentation installed with the software.

## Using the Storage Devices page

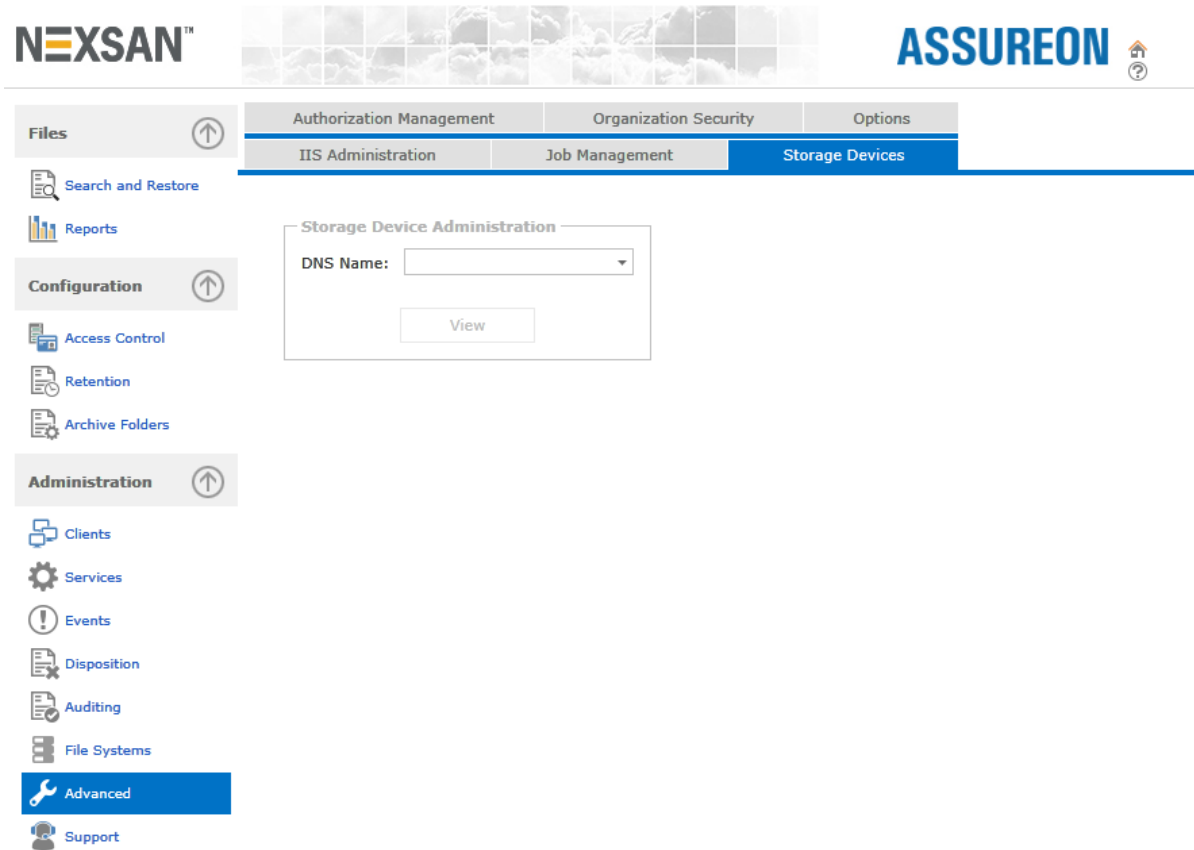
Use the Storage Devices page to monitor SATA storage devices. When configured, you can access the SATA device login page, and once logged in, the device web interface. The storage device IPs (more than one may be configured) are specified when Assureon is installed.

**Note** You must be logged on locally to the Assureon server in order to monitor the device.

### ► To access this page:

1. From the main menu, under **Administration**, click **Advanced**.
2. Select the **Storage Devices** tab.

Figure 2-52: Storage Devices page



### ► Storage devices details:

- **DNS Name** – Displays the DNS name of the device, pointing to the IP configured when Assureon was installed. The DNS names are generated by Assureon.
- **View** – Displays the SATA device login page.

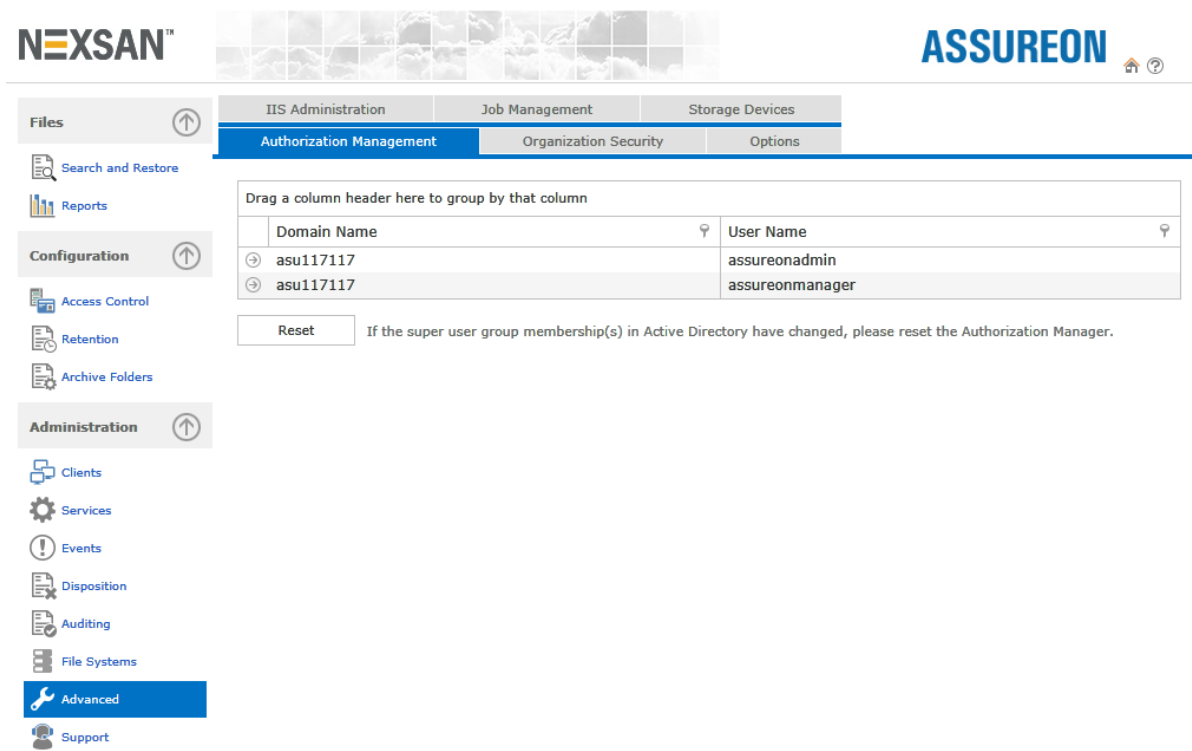
## Using the Authorization Management page

Use the **Authorization Management** page to view user group membership information. Use this page to check why a user does not have access to a specific file by getting the group memberships.

► **To access this page:**

1. From the main menu, under **Administration**, click **Advanced**.
2. Select the **Authorization Management** tab.

Figure 2-53: Authorization Management page



► **Authorization details:**

- **Get user** – Refreshes the list of users displayed in the User Name list.
- **User Name** – Displays users with group membership information stored in the Authorization Manager.
- **Get User Details** – Displays Security Group and Organization information for the selected user.
- **Security Groups panel** – Displays the Security groups that the user is a member of.
- **Organizations panel** – Displays the Organizations the selected user is a member of.
- **Reset** – Resets the authorization manager by reloading the user security information from the Assurance active directory and, if you are using a corporate [ADAM](#) instance, by deleting the security information provided by the Assurance Client on the servers where ADAM is installed.

## Using the Organization Security page

Use the **Organization Security** page to map an organization to a user security certificate, issued to a server using the ADAM security model.

► **To access this page:**

1. From the main menu, under **Administration**, click **Advanced**.
2. Select the **Organization Security** tab.

Figure 2-54: Organization Security page

The screenshot shows the Assureon web interface. At the top, there are logos for NEXSAN and ASSUREON. Below the logos is a navigation bar with tabs for IIS Administration, Job Management, and Storage Devices. Underneath, there are sub-tabs for Authorization Management, Organization Security (which is selected), and Options. The left sidebar contains a navigation menu with categories: Files (Search and Restore, Reports), Configuration (Access Control, Retention, Archive Folders), Administration (Clients, Services, Events, Disposition, Auditing, File Systems, Advanced), and Support. The main content area is titled 'Organization Security' and has a sub-section 'Organization' with the text 'Select the organization' and a dropdown menu showing 'Organization: Assureon\_117117'. Below this is an 'Add Certificate' button. The next section is 'Certificates', which contains a table with columns 'FS Organization', 'Allowed Certificates', and 'Action'. The table is currently empty, displaying 'No data to display'.

► **Organization security details:**

- **Organization** – The Organization to map to a user-specific digital certificate.
- **Certificate serial number** – The number of the certificate. Must be 20 alpha-numeric characters.

► **To obtain the certificate number:**

1. Launch the Certificate Authority on the Assureon server.
2. Browse to the **Issued Certificates**.
3. Double-click the user certificate.
4. Look in the **Details** tab.

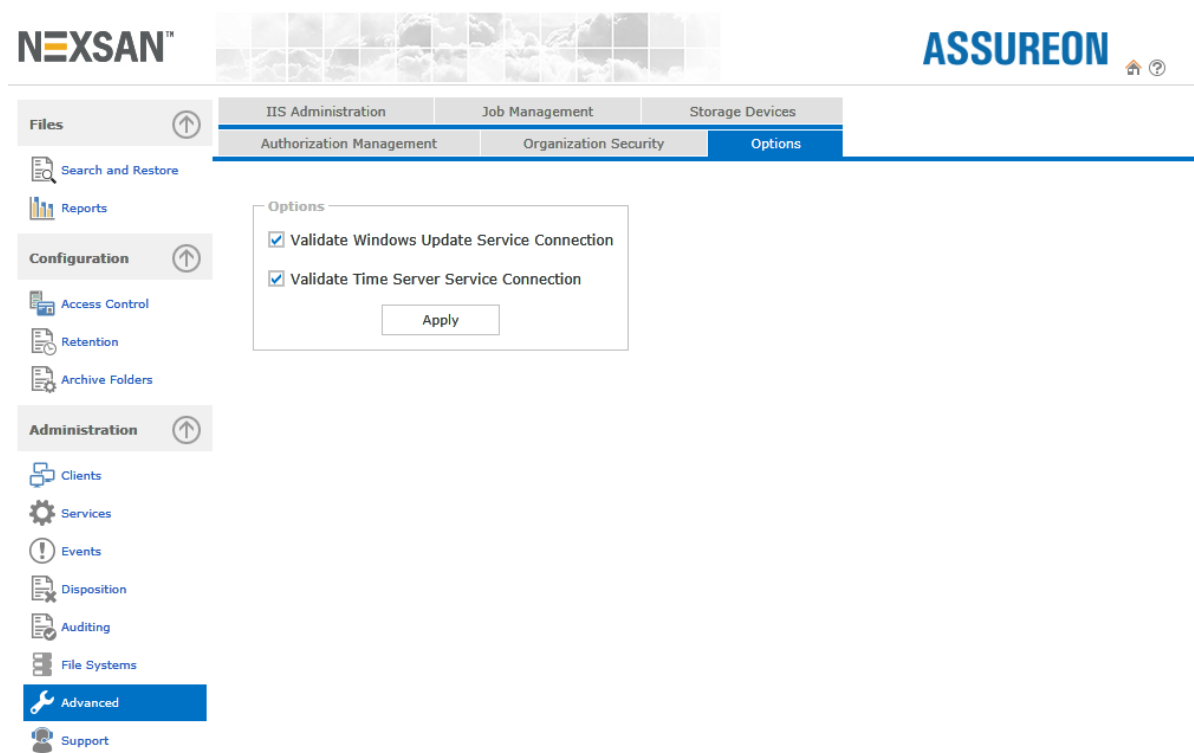
## Using the Options page

Use the **Options** page to enable or disable monitoring of network connectivity between the Assureon system and the Windows Update Server and between the Assureon system and the Time Server, by System State. When monitoring is enabled, the status of the connection to the relevant service is displayed on the [System State](#) page.

► **To access this page:**

1. From the main menu, under **Administration**, click **Advanced**.
2. Select the **Options** tab.

Figure 2-55: Options page



► **To enable or disable monitoring for a service:**

1. Click the check box corresponding to the service that you want to enable or disable monitoring for.
2. Click **Apply**.



## Using the Support page

Use the Support page to access support-related tools including the [Assureon Call-home service \(Remote Desktop\)](#), the [CallHome](#) feature, the [scheduled logs upload service](#), the automated [Assureon Upgrades](#) page, as well as [contact information](#) for Nexsan Support.

## Using Remote Desktop

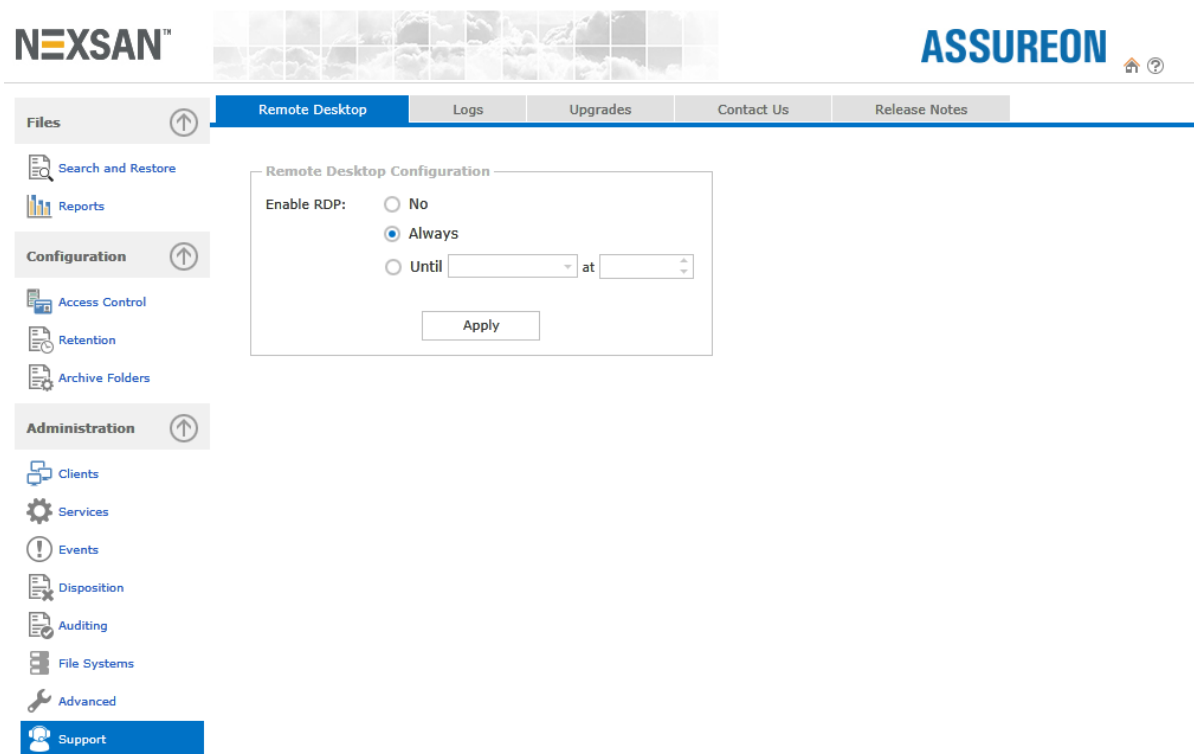
You can use **Remote Desktop** to enable or disable remote access to the server. This enables the Assureon Customer Support team to securely connect to the Assureon system and troubleshoot issues remotely without having to open up a manual support session or VPN connection.

By default, the remote desktop connection is disabled.

### ► To enable RDP:

1. Select one of these options:
  - **Always**
  - **Until** : Restrict access to a specific time frame by selecting a date and a time.
2. Click **Apply**.

Figure 2-56: Support—Remote Desktop page



## Using CallHome

Use the CallHome feature to send system logs when major issues are detected, based on events and diagnostics, including:

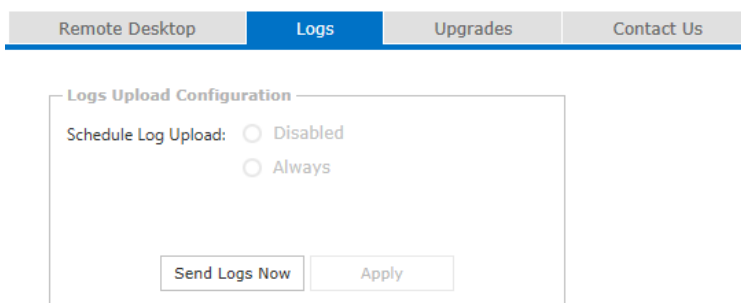
- The maximum object count is reached for the file system (in which case ingestion stops)
- Any hardware-related error (processor, fan, disk, power supply unit, or memory)

- The disk is full and ingestion gets turned off
- There are no more active storage pools and rollover failed
- The key server security check fails when trying to dispose files
- The Events Manager starts to discard events because it is receiving hundreds of errors per second
- The Root key is expired or is going to expire

## Logs

Allows the administrator to upload system logs to the Assureon support team for analysis. In some cases, automated log uploads are enabled. Please contact [Nexsan Support](#) for details.

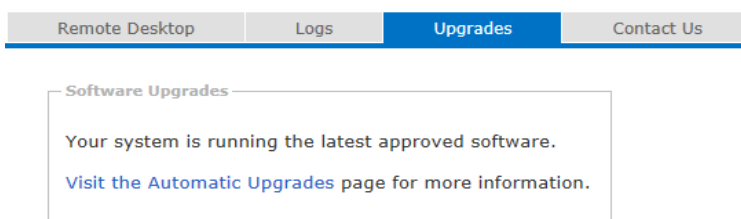
Figure 2-57: Support—Logs page



## Upgrades

Displays available upgrades, and provides access to the Assureon Automatic Upgrades page where you can upgrade the Assureon system to the latest version. The Assureon system intermittently checks the Assureon Upgrade Server for available upgrades. If a new version is available, an email notification is sent out. You can then trigger the start of the upgrade from the Assureon Automatic Upgrades page.

Figure 2-58: Support—Upgrades page



## Contact Us

Displays contact information for [Nexsan Support](#).

# Chapter 3

## The Client Service

---

This section provides information about these topics:

Installing the Client Service .....	124
Client Service taskbar icon .....	126
Assureon client options .....	126
Secure File Transfers .....	128
Client Service For Laptops .....	128
Assureon property sheet .....	128
Low disk space warning .....	129
Archive folder icons .....	129
Safe Shortcuts .....	129
About Sparse Files .....	129
About Virtual Shortcuts .....	130
About the Filter Driver .....	130
About empty files .....	131

## Installing the Client Service

The Client Service can be installed on a Windows 7 or 10 workstation or a Windows Server 2008R2, 2012, 2012R2, 2016. The client service installation utility may also be used to install an [ADAM](#) instance, or to point to an existing ADAM instance.

When installed on a Microsoft Windows Server, the Client Service can monitor and archive files from local drives, including drives that are SAN attached. Additionally, the server can monitor UNC paths on other Microsoft Windows Server or Windows XP workstations. Performance will vary depending on the deployment scenario.

- **Locally attached drives** – When the Client Service is operating in 'Real-time Enabled' mode, it can process nominally about 150,000 files per hour or a maximum of 50 gigabytes per hour. Performance will vary depending on server load, the speed of the computer, network traffic and the capacity of the Assureon system. If the system will sustain loads greater than the nominal maximums given, it is recommended that the Client Service operate in 'Sync Enabled' mode
- **UNC Mounted Drive Paths** – The Client Service can monitor folders mounted on UNC paths that are hosted on computers using NTFS. Notifications of the files to be archived and the archived files are transferred across the network to the server that hosts the Client Service before being transferred to Assureon. This will increase network traffic and the load on the local server hosting the Client Service. This feature is intended to be used to monitor folders that have a maximum of 100 new files per hour, with a maximum aggregate size of 20 gigabytes per hour across all monitored UNC paths. Over these limits, it is recommended that the Client Service be installed on the server/workstation that hosts the UNC path.

When the Client Service is installed, other client-related components such as the [Synchronization utility](#), [Assureon Explorer](#), [Filter driver](#), and the [Change Journal](#) are also installed. Also included with the Assureon FSW service are the Assureon Events Manager, Assureon Filter Driver Manager and the Assureon FSW Monitor services.

The following recommended procedure assumes that:

- The `FSWManager` user has been created in the corporate Active Directory, and has been added as a member of the Domain Admins group.
- The `FSWManager` user has been added to the Assureon Active Directory (Assureon.Net) as a member of the `FSWManagers` group.

► **To install the Client Service on a server:**

1. Log on to the server where you want to install the Client Service using the `FSWManager` user. This will create the required account on the server.
2. Using Windows Explorer, go to `\\<server name>\installers`, where `<server name>` identifies your Assureon server.
  - If the server is running a 32-bit operating system, choose `SetupFSW32`.
  - If the server is running a 64-bit operating system, choose `SetupFSW64`.
3. Double-click `Assureon FSW.exe`. The Welcome dialog box appears.
4. Click **Next**.
5. The Destination Folder dialog box appears. Accept the default location or click **Change** to modify it. Click **Next**.

6. The Cluster Information dialog box appears:
  - a. Select the applicable **Cluster** option.
  - b. Specify the **Virtual computer Name**.
  - c. Enter the **Virtual Domain Name**.
  - d. Specify the **Shortcut Type**.
  - e. Click **Next**.
7. The Setup Type dialog box appears. Select **Typical** and click **Next**.
8. The ADAM dialog box appears.

If...	Perform these steps
you are not using the ADAM security	<ol style="list-style-type: none"> <li>a. Select the <b>Do not use ADAM</b> option.</li> <li>b. Click <b>Next</b>.</li> </ol>
you are using the ADAM security	<ol style="list-style-type: none"> <li>a. Select the <b>Use an Existing ADAM Instance</b> option.</li> <li>b. Specify the <b>ADAM Server Address</b> and the <b>ADAM port</b>.</li> <li>c. Click <b>Next</b>.</li> </ol>

9. The Bogon Information dialog box appears.
  - a. Specify the `FSWManager` user using the @ format; for example, `FSWMANAGER@assureon.net`.
  - b. Enter the password.
  - c. Click **Next**.
10. This step modifies the service Log on account on the server to use the `FSWManager` user. Click **Next**.
11. The Ready to Install the Program dialog box appears. Click **Install**.

► **What's next:**

After the installation, perform these steps:

1. Launch Internet Explorer.
2. Click **Tools** and select **Internet Options**.
3. Select the **Security** tab.
4. Click the **Local intranet** icon.
5. Click **Sites**.
6. Add **F001** to the list of sites.
7. Click **OK**.

► **To uninstall the Client Service:**

1. On the server where the Client Service is installed, log on as the `FSWManager` user, and run the windows Add or Remove Programs dialog box.
2. Select **Assureon FSW** and click **Remove**.
3. Click **Yes** to confirm. The service is uninstalled. You may be prompted to restart your system.

► **To start the Client Service:**

To start the Client Service, you have a couple of options:



- Use the [Client Service taskbar](#)
- Use the Windows Services dialog box.

## Client Service taskbar icon

The Client Service taskbar icon provides a quick way to check the status of the Client Service, and to stop and start the service.

The icon is installed with the Client Service and may be viewed by expanding the notification icons at the bottom right of the taskbar. For example:



When the Client Service is running, the icon will appear with a green checkmark: . When stopped, the icon will appear with a red x: .

Right-click the Client Service taskbar icon to see the following options.

► **Menu options:**

- **Start Client Service** – Starts the Assureon Client Service
- **Stop Client Service** – Stops the Client Service
- **Restart Client Service** – Stops and then starts the Client Service
- **File Sync** – Displays the [File Synchronization dialog box](#)
- **Enable Filter Driver\Disable Filter Driver** – Starts or stops the [Filter Driver](#)
- **Options** – Displays the [Assureon Client Options](#) dialog box
- **Show at startup** – Whether to display the Client Service taskbar icon when the computer starts.
- **Exit** – Hides the Client Service taskbar icon. To redisplay the icon, double-click the file `ILMAgentTray.exe` in the `program files\nexsan technologies\assureon fsw` folder or restart the computer.

If you have a [Client Service for laptops](#) installed, you will also have the following options:

- **Resume Client Service Transfer** – The Client Service operates normally; any journalled files are processed. Use this option when connected to the network.
- **Pause Client Service Transfer** – Causes the Client Service to journal files on the laptop. Use this option when disconnected from the network.

## Assureon client options

The **Assureon Client Options** dialog box enables you to modify and enable various Client Service options.

After a change is made, the Client Service may be restarted. If the Client Service is already running and is currently processing files using the [File Synchronization Utility](#), the Client Service will NOT be restarted. If this happens, wait for the synchronization to finish and then restart.

► **To access the Assureon Client Options dialog box:**

1. Right-click the [Client Service taskbar](#) icon.
2. Select **Options**.

**General tab**

**Windows Change Journal** – Optional feature used for file synchronization

- **Enable** – Enables the [change journal](#) feature
- **Size (bytes)** – The size of the windows change journal. Modifies the default value set by the operating system to the specified value. Maximum of 512 MB.

**Folders tab**▶ **Journal Folder:**

- **Custom** – Specifies the location of the Client Service journal folder where files are temporarily stored when communication between the client and Assureon store is interrupted. If your c:\ drive has limited disk space, change this location
- **Default** – Resets the system to use the default journal location

▶ **Filter driver temporary folder:**

- **Custom** – Specifies the location of the temporary download folder used by the filter driver to retrieve files from the store. If your c:\ drive has limited disk space, and you are using the filter driver, change this location
- **Default** – Resets the system to use the default location

**Authentication tab**

**Client Certificate** – Optional feature used for secure authentication

- **Use Client Certificate** – Enables the use of certificates for authentication purposes.
- **Client certificate** – The security certificate to use for authentication. Certificates must be installed on the client prior to selection. See [Use Certificates for Authentication](#) for details.

**Shortcut Management tab**

Optional feature that is enabled by specifying the Replace with shortcuts based on disk space option for an archive folder. See [Archive Folder Editor](#) for details.

- **Shortcut files when free space is less than x**
- **Shortcut files until free space equals x**
- **Run Shortcut Manager once a day at** – Specifies the time the shortcutting utility is run, usually an off-peak time.

**Safe shortcuts**

- **Shortcut files after verifying that the files have been archived** – Shortcuts (or deletes) files in an archive folder only after verifying that they have been successfully stored. Adds an extra layer of verification. This option is disabled by default.
- **Verify every x minutes** – The verification time interval. The lower the value, the more frequent the checking, the quicker files will be shortcutted. A value of less than 5 minutes may impact system performance. Default is 5 minutes.

**Shortcut Type tab**

Specifies the type of shortcut to create.

- **Use sparse files for shortcuts** – When enabled, creates shortcuts using [sparse file](#) technology.
- **Use URL files for shortcuts** – Creates URL shortcuts. The following options apply only if the filter driver is installed and enabled.
  - **Display as shortcut** – Displays the shortcut as a shortcut even when the filter driver is enabled.
  - **Display as file** – Displays the shortcut as a file when the filter driver is enabled.
    - **Display as shortcut for Windows Explorer Only** – Displays the shortcut as a shortcut for Windows Explorer. For all other applications, the shortcut appears as a file.
- **Use virtual files for shortcuts** – Creates virtual file shortcuts. This option is only available for high-speed Assureon configurations with RoCE (RDMA over Converged Ethernet). When you enable this option, the Assureon Client creates virtual shortcuts that reside purely in memory, instead of on disk.

### ***File Sync Notification tab***

Specifies email options for the [File Synchronization Report](#).

- **Enabled** – Enables sending File Synchronization reports via email.
- **SMTP Server** – The name or IP address of the SMTP server to use to send the message.
- **From** – Text to prefix to the server name.
- **To** – The email address of the recipient. Use a semi-colon (;) between multiple recipients. Required.
- **Subject** – A subject line for the email. Required.
- **Attach details** – Attaches the log files to the email.
- **HTML Format** – Whether to send the message using the HTML message format. Most email programs support this format, which allows the message to be formatted. If not enabled, Plain Text format will be used.
- **Email criteria** – Specifies the criteria that when met will trigger an email notification.
- **Maximum size** – The maximum size for the email attachments, in megabytes.

## Secure File Transfers

For high-security installations, files can be signed or signed and encrypted during transfer from the Client Service to the Assureon server.

For more information about this optional feature, contact your Nexsan representative.

## Client Service For Laptops

The **Client Service for Laptops** is a special version of the Client Service designed for users who find themselves frequently disconnected from the network. Basically, the Client Service continues to monitor archive folders, and journals files. Once reconnected to the network, the files are processed by selecting the **Resume Client Service Transfer** option of the [Client Service taskbar](#).

For details on this version, contact your Nexsan representative.

## Assureon property sheet

The **Assureon property sheet** enables authorized users to quickly add or modify an archive folder on a server without having to use the Assureon System Administration user interface, Archive Folders Editor page. After an archive folder is created using the property sheet, it can also be edited using the [Archive Folder Editor](#).



To access the property sheet, right-click on a folder, and then the **Assureon** tab. If the Assureon tab is not displayed, make sure the user logged on to the server is a member of an [ILM security group](#).

The tab contains the following options:

### ***Do not archive this folder***

The Client Service does not monitor this folder for changes.

### ***Archive this folder***

The Client Service will monitor this folder. The following options may be modified (some options may not be available, depending on your system configuration):

- Real time
- Sync
- Include subfolders
- Organization
- Retention rule
- Access classification
- Indexing rule ID
- Match pattern
- Action

## Low disk space warning

The Client Service low disk space monitoring utility warns the user when disk space available falls below a specified threshold. The default value is 100 MB and is set in the ILM Tray Agent configuration file.

## Archive folder icons

Archive folders are displayed in Windows Explorer using Assureon icons, instead of the Windows folder one, allowing you to quickly identify archive folders. The real-time and Sync icons differ; an archive using both options will display the real-time icon.

## Safe Shortcuts

The Safe Shortcuts feature creates shortcuts to and deletes files from an archive folder only after verifying that they have been successfully stored on the Assureon server. This feature is disabled by default, but may be enabled from the Assureon Client Options dialog box, accessed from the [Client Services taskbar icon](#).

## About Sparse Files

Sparse Files are files that use file system space more efficiently. Sparse files are disabled by default. To enable them, right-click the Client Services taskbar icon, choose Options, Shortcut Management tab, and then select the Use sparse files as shortcuts option.

The advantages to using sparse files are:

- The shortcutted file opens with the correct application. For example, double-clicking on a .doc sparse file shortcut will open the document in Word.

- There is less network traffic, as only the required portion of a file is retrieved from the store when opening a file and only the modified portion sent to the store when modifying.

**Note** Assureon URL and sparse file shortcuts cannot be used on the same computer. In other words, the options are mutually exclusive.

Customers using URL shortcuts may convert them to sparse files, contact [Nexsan Support](#) for more information.

### Shortcut file attributes

On Windows Server 2008, Assureon sparse file shortcut file attributes may show the following in Windows Explorer: APLO

This means:

- A – Archive bit
- P – Sparse File
- L – Reparse Point
- O – Offline

## About Virtual Shortcuts

For high-speed Assureon configurations with RoCE (RDMA over Converged Ethernet), you can configure the Assureon Client to no longer create shortcuts to files on disk (by enabling the Use virtual files for shortcuts option in the Assureon Client Options dialog box; see [Assureon client options](#) on page 126.)

When you enable this option the Assureon Client creates virtual shortcuts that reside purely in memory as reference points to files. This means that there is zero recovery time in case the Assureon Client server goes down; you need only bring up another computer, install the Assureon Client on it and the files appear instantaneously.

Virtual shortcut features:

- Support for mount points – virtual shortcuts can reference files that are part of a mounted file system.
- Files can be downloaded to replace virtual shortcuts – you can configure Assureon to download the file reference by a shortcut, in order to replace the shortcut with the physical file.
- A file can be read entirely on the first read operation – you can configure Assureon to download a file in its entirety when it is first accessed using the corresponding shortcut. This can improve performance with read operations. By default, the Assureon server downloads files in 64 KB increments.

## About the Filter Driver

The Filter Driver resolves shortcuts to stored files for third party applications, such as email archiving tools. For example, if an application needs to open a file that has been archived and then replaced locally with a shortcut, the filter driver takes care of retrieving the file from the Assureon store and providing it to the requesting application. As far as the requesting application was concerned, the file was always local.

The filter driver can use sparse file or URL-based shortcuts. URL-based shortcuts are used by default. The filter driver is an optional component of the [Client Service](#), which is installed and enabled when the Client Service is installed. The filter driver runs as a Windows service and kernel driver and automatically monitors requests for files in folders where the archive policy is to replace files with shortcuts.

**Note** The Assureon 6 filter driver is only supported on Windows Server 2008R2 or higher.

► **To use sparse files:**

1. Right-click the [Client Services task bar](#) icon.
2. Select **Options**.
3. In the [Assureon Client Options](#) dialog box, select the **Shortcut Type** tab.
4. Select the **Use sparse files for shortcuts** option.

► **To disable the filter driver:**

1. Right-click the Client Services task bar.
2. Select **Disable filter** driver.

## About empty files

The Assureon server does not automatically archive empty files, that is, files without content and having a size higher than 0 KB. Instead, Assureon sends an email notification to inform you that a third-party application (such as an anti-virus application) may be intercepting files during a read/write operation and causing the files to become blank.

Empty files—files that have a size of 0 KB—are automatically archived.

You can configure the Assureon FSW configuration file (`fswconfig.xml`) to modify these settings:

- `skipZeroKFile`: This value archives 0 KB files when set to `false`. The default value is `false`.
- `skipBlankFile`: This value archives files that are blank (not 0 KB) when set to `false`. The default value is `true`.



# Chapter 4

## Assureon Explorer

---

This section provides information about these topics:

About Assureon Explorer .....	134
Restore options .....	135
Assureon Explorer command line .....	136

## About Assureon Explorer

Assureon Explorer extends Windows Explorer and enables you to explore, read and restore files (and directory structures) from the Assureon store.

The Explorer can be run from a command line, see [Assureon Explorer command line](#) on page 136 for details.

► **To access the Assureon Explorer, choose one of these options:**

- Double-click the Assureon Explorer desktop icon.
- Launch Windows Explorer and click on the **Assureon Explorer** folder.
- Launch Windows Explorer, right-click a file and select **View in Assureon Explorer**.

Multiple files can be selected using the mouse and the Shift and Ctrl keys. Expired and disposed of files are not displayed.

Assureon Explorer has the following options:

### *Filter*

- **Show All Versions** – Displays all the versions of a file with the same name in the store.
- **Show First Version Only** – When a file is stored more than once with the same name, it displays the oldest version of the file.
- **Show Last Version Only** – When a file is stored more than once with the same name, it displays the most recent version of the file.
- **My Computer** – Displays only the files stored from the current computer.
- **All Computers** – Displays files stored from other computers, if you have permission to view the files.

### *Restore*

Restores one or more files to a specified location. When a file has more than version with the same name, only the most recent file is restored. These options display the [Restore Options](#) dialog.

- **Restore files to original location** – Restores the file to its original location. You must be running Assureon Explorer on the source computer for this option to be available.  
**Note** Be careful using this option, if the folder is still an archive folder, the file will be reprocessed.
- **Restore files to alternate location** – Restores the file to a specified location.
- **Restore shortcuts to original location** – Creates shortcuts to their original location. You must be running the Assureon Client Service on the source computer for this option to be available.
- **Restore shortcuts to alternate location** – Creates shortcuts in a specified location.

### *Refresh*

Refreshes the display with the latest information about files in the store.

### *Search Engine*

Displays the [Search Engine](#) search page. Enabled only if the Search Engine is installed.

### *Resume Restore*

Allows you to resume failed restores that were started from the folder pane. Click on this option a dialog where you can specify whether to resume or discard (cancel) the restore.

► **To read a file:**

To read a file, double-click it or right-click and choose Open. The file will open in the correct application, based on the file extension.

► **To restore a file:**

To restore a file, click the Restore icon or right-click a file and choose a restore option.

## Restore options

Use the **Restore Options** dialog box to restore files from the Assureon Explorer to an original or alternate location.

► **To open the Restore Options dialog box:**

- Select a file restore option from [Assureon Explorer](#).

**Note** Version options are displayed only if you select a restore option from the Explorer folder list (the tree view to the left).

► **Restore options:**

- **Version options** – Specifies how files with more than one version in the store are restored. The version of a file is determined using its Date Modified file property.
  - **Restore last version** – Restores the last version of a file
  - **Restore first version** – Restores the first version of a file
  - **Restore all versions** – Restores all versions of a file.
  - **Restore to point in time** – Restores the closest version of a file found **before** the specified date and time based on the file modification date.
- **Replace options** – Specifies what happens when files are restored to a directory where files with the same name already exist.
  - **Rename** – Existing files are not modified; the restored files are renamed and then added to the directory. Files are renamed by inserting their modification date and time information into their file name.
  - **Replace** – Existing files are replaced with the restored ones.
  - **Skip** – Existing files are not modified; Files with the same name as those in the directory are not restored.
- **Directory**
  - **Restore the full directory structure** – Whether to restore the files keeping the original directory structure.
  - **Prefix Computer Name and Drive** – Whether to prefix the computer name and drive to the directory structure of the restored files.
  - **Restore folder security** – If available, original directory permissions will be restored to the restored folder. Applies only if the Restore the full directory structure option is selected.
  - **Prefix Organization and File System** – Whether to prefix the organization and file system names to the directory structure of the restored files. Applies only if the Prefix Computer Name and Drive option is selected.

## Assureon Explorer command line

Use the Assureon Explorer command line to restore files or shortcuts. The command line option is typically used to run a restore as a scheduled task. Files can also be restored using [Assureon Explorer](#).

### ► To use the Explorer command line:

1. Open a command prompt window.
2. Run the command from the Assureon Explorer folder in:

```
c:\Program Files\Nexsan Technologies
```

The command line syntax is, where the | indicates an option:

```
AEEexplorer.exe /restore shortcuts|files
```

### ► Optional arguments:

- /restorecomputer— Restores files that were archived on the specified computer. If not specified, all computers will be restored.
- /restoreTo— Restores files to the specified path. If not specified, files will be restored to the original location.
- /overwrite [skip|overwrite|rename] – Determines the action to take if the file already exists
- /verbose – Displays verbose messages to the UI
- /resume – Resumes the restore from the last file that was restored on the previous run
- /org [names|all] – Restores files for the specified organization
- /fs [all|active|readonly|hibernate|name] – Restores files for the specified file system or file system type. The readonly option refers to non-active or "passive" file systems. The hibernate option is currently not supported.
- /restoreFolder *folderPath*— Restores files that were archived to the specified folder
- /prefix [none|computer|organization] – Prefixes the originating computer name and drive
- /subdirectories [restore|skip] – Restores files using original subdirectory structure. Works with the /restoreFolder option.
- /restoreOption [all|first|last|pointInTime date] – Specifies the version of a file to restore. All restores all file versions. The date format of the pointInTime option is: year/05/10 (with the slashes). For example: 2008/05/10.
- /restoreFolderSecurity— Sets the security on the folders that are restored

### ► Examples:

Example 1: To restore files archived from SERVER1 to a specific folder:

```
AEEexplorer.exe /restore files /restorecomputer SERVER1 /restoreTo  
restoreFolder
```

Example 2: To restore all shortcuts to the original folder:

```
AEEexplorer.exe /restore shortcuts
```

### ► To schedule a restore using the Windows Scheduled Task wizard:

See the [File Synchronization Command Line](#) topic.



# Chapter 5


## The File Synchronization utility

---

Use the File Synchronization utility to archive new or modified data to the Assureon server using the configured archive folder settings.

Unlike the Client Service, which can archive the data in real-time, the File Synchronization utility is used to manually start a synchronization, either through the [File Synchronization application](#) (`FileSyncApp.exe`) or the [command line](#) (`FileSyncCmd.exe`). These tools can be found in <Installation path>\Assureon FSW (`c:\program files\nexsan technologies\Assureon FSW`).

► **To start the File Synchronization utility, choose one of these options:**

- Click the **Assureon File Sync** shortcut on the desktop;
- Click the Windows **Start** menu;
- From the system tray, right-click the **File System Watcher** icon  and select **File Sync**.

The real-time and synchronization modes can be enabled simultaneously. The real-time synchronization occurs whenever the Assureon FSW service is running. The synchronization mode must be either executed manually or scheduled using the scheduling features set using the [Archive Folders Editor](#) page in the System Administration Web interface.

► **To configure the Real-time and Sync Enabled options:**

- Right-click an **Assureon** folder in Windows Explorer, then select **Properties**, and click the **Assureon** tab.  
Or
- Open the [Archive Folder Editor](#) in the System Administration Web interface.

This section provides information about the following topics:

<a href="#">File Synchronization dialog box</a> .....	138
<a href="#">File Synchronization command line</a> .....	148
<a href="#">Change Journal</a> .....	149
<a href="#">File Sync Request Watcher</a> .....	150

## File Synchronization dialog box

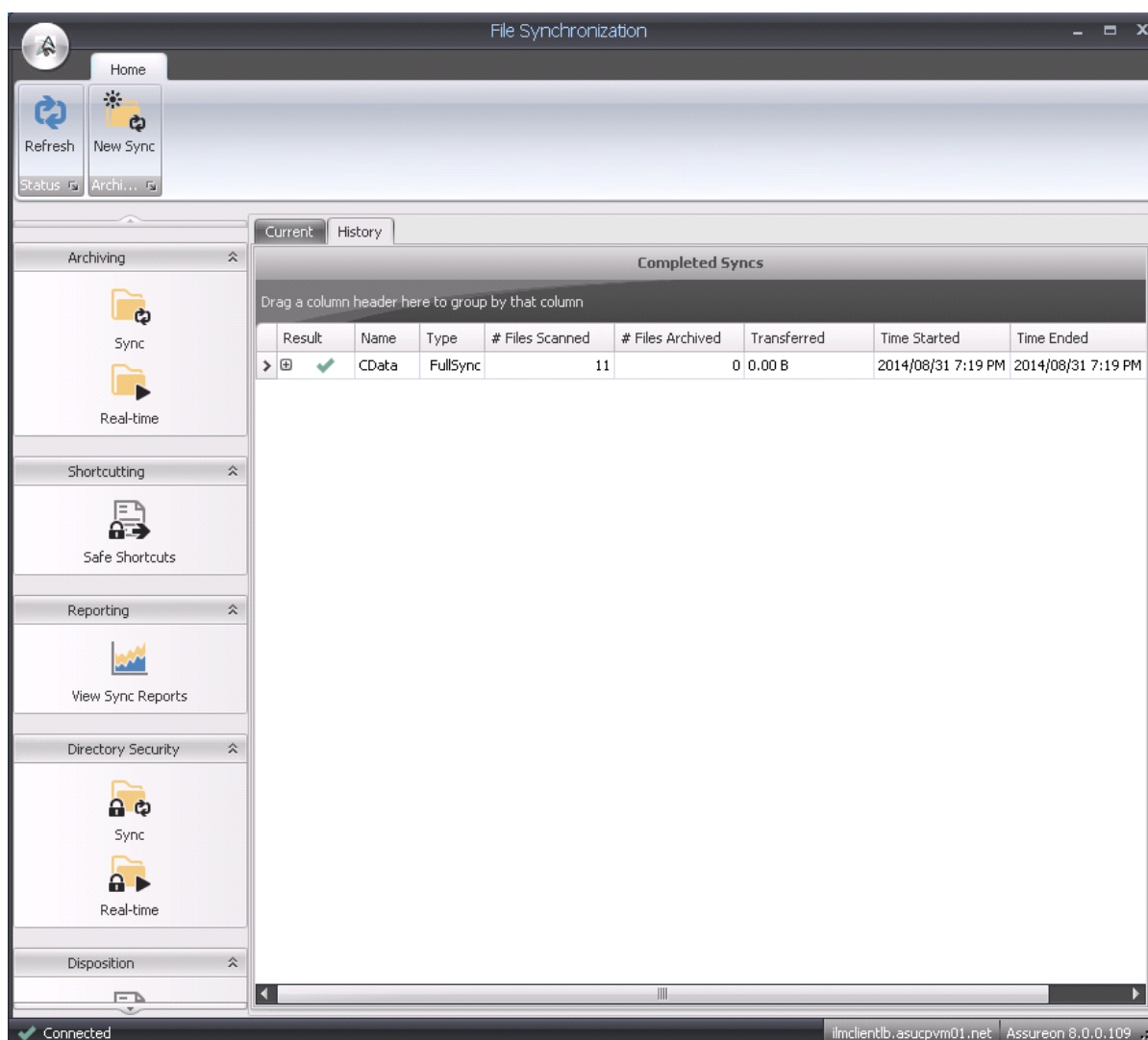
Use the File Synchronization dialog box to launch the [Assureon Synchronization utility](#) and perform a file synchronization.

► **To access this dialog box, choose one of these options:**

- From the desktop through the **Start** menu.
- Right-click the [FSW Agent task bar](#) and select **File Sync**.

**Note** File synchronization may also be performed from a [command line](#), although it is not the recommended approach.

Figure 5-1: File Synchronization dialog box



When opened, the dialog box reads and then displays archiving rules taken from the Client Service configuration file. If the rules are modified while the dialog box is open, click **Refresh** to display the latest information. A green checkmark in the bottom left shows connectivity to the FSW Client Service. The client version is displayed on the bottom right.

Use the File Synchronization dialog box to do the following:

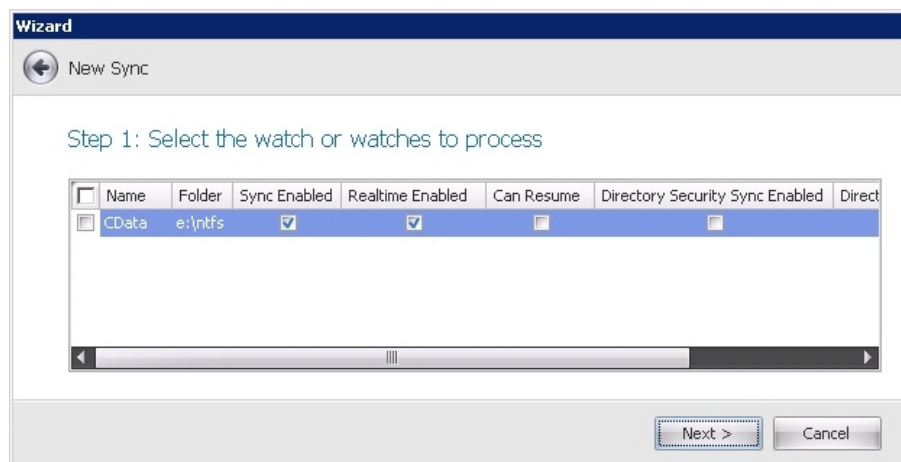
- [Starting a new file sync below](#)
- [Archiving Sync](#) on the next page
- [Shortcutting - Safe Shortcuts](#) on page 142
- [Reporting - View Sync Reports](#) on page 143
- [Directory Security - Sync](#) on page 145
- [Disposition - Delete disposed shortcuts](#) on page 146

## Starting a new file sync

The New Sync wizard is used to start one or several new syncs of any type; see [The File Synchronization utility](#) on page 137.

### ► To perform a new sync:

1. Right-click the Client Services task bar icon and select **File Sync**. The File Synchronization dialog box appears.
2. Click the **New Sync** button in the **Home** tab of the File Synchronization dialog box.  
The New Sync wizard opens.



3. Select the watch or watches you would like to sync. Scroll to the left to view which modes are enabled. Click **Next**.

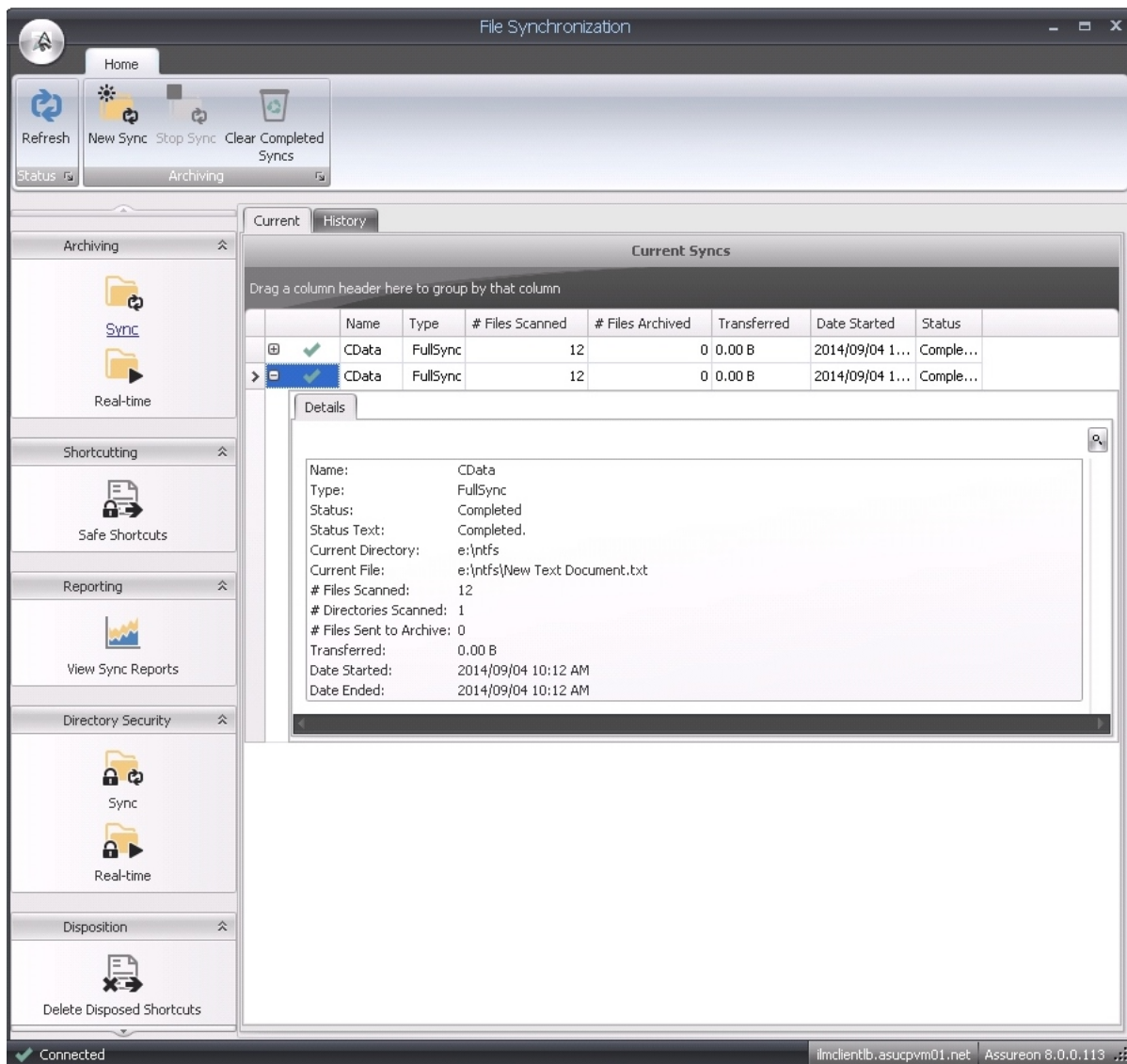
4. Select the synchronization type from the drop-down menu:
  - **Full** – Every file is scanned and compared to the Assureon server to determine whether it should be archived. This is the most comprehensive type of synchronization.
  - **Archive Bit** – The archive bit is an attribute in Windows. It is set on all new or modified files. This sync type allows only files that have the archive bit set to be considered for archiving. In most cases, this sync is recommended over a full sync. However, it is not recommended when another application is using the archive bit as it can cause the synchronization to miss files.
  - **Change Journal** – The Windows [change journal](#) is a database of new and modified files. This synchronization uses this database to determine which files need to be archived to the Assureon server.
  - **Directory Security** – This sync enables you to store the directory security. Applies only if Store folder security option is enabled for the archive folder, in the [Archive Folder Editor](#) page.
  - **Delete Disposed Shortcuts** – Whether to delete shortcuts that point to disposed files in the Assureon archive.
5. Click **Next**.
6. Confirm the details of the sync. Click **Start**.

## Archiving Sync

Use the Assureon File Synchronization Archiving Sync page to view details on a number of current or past syncs. The **Current** tab lists all syncs that are in the process of running, or have recently finished running. The **History** tab lists all syncs that have recently finished running.

Click on the **+** icon in the first column to view complete details on a specific sync.

Figure 5-2: Archiving - Current Sync page



### ► Current and History details:

- **Name** – The name of the archive folder. To select them all, check the box.
- **Type** – The synchronization type that was selected for the sync.
- **# Files Scanned** – The number of files that have been scanned during the sync.
- **# Files Archived** – The number of files that have been archived during the sync.
- **Transferred** – Total size of the data that has been transferred to the Assureon server so far.
- **Date Started / Date Ended** – The date and time the sync started and ended at.
- **Status** – Indicates the progress of the sync.

### Real-time

Use the Assureon File Synchronization Archiving Real-time page to monitor Real-time syncs. When Real-time sync is enabled for a folder, changes to the archive folder are automatically sent to the Assureon server.

To set a Real-time watch on a folder, see [Using the Archive Folders Editor](#) on page 70.

► **Real-time Watches details:**

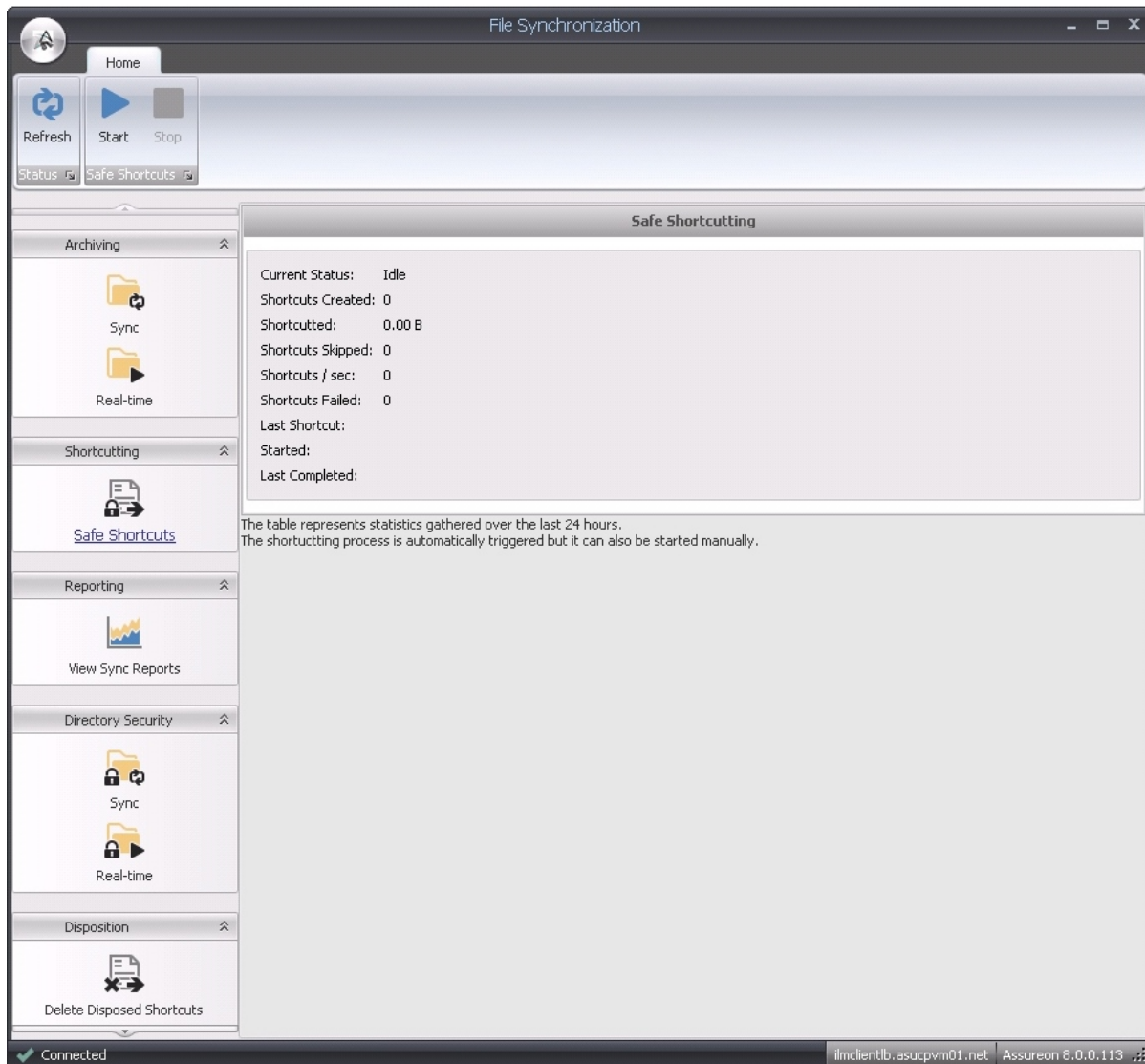
- **Name** – The name of the archive folder. To select them all, check the box.
- **# Files Archived** – The number of files that have been archived during the sync.
- **Transferred** – Total size of the data that has been transferred to the Assureon server so far.
- **Last File** – The last file to be processed.
- **Start Time** – The time the Real-time sync began.

## Shortcutting - Safe Shortcuts

If the **Safe Shortcuts** feature has been enabled for an archive folder, files within that folder will be shortcutted (or deleted) only after verifying that they have been successfully stored on the Assureon server; see [Assureon client options](#) on page 126.

The **Safe Shortcutting** page shows information collected over the past 24 hours. Once enabled, the shortcutting process is automatically triggered around every hour, although it can be started manually.

Figure 5-3: File Synchronization - Safe Shortcutting page



## Reporting - View Sync Reports

Use the **View Sync Reports** page to view the synchronization log files. The report will display errors first (if there are any), followed by warnings and then information messages. The top pane displays summary statistics related to skipped and transferred files.

### ► To view detailed information:

1. Select the log file.
2. Select one of the Log Data options:
  - Skipped Files
  - Transferred Files

3. Select one of the tabs:

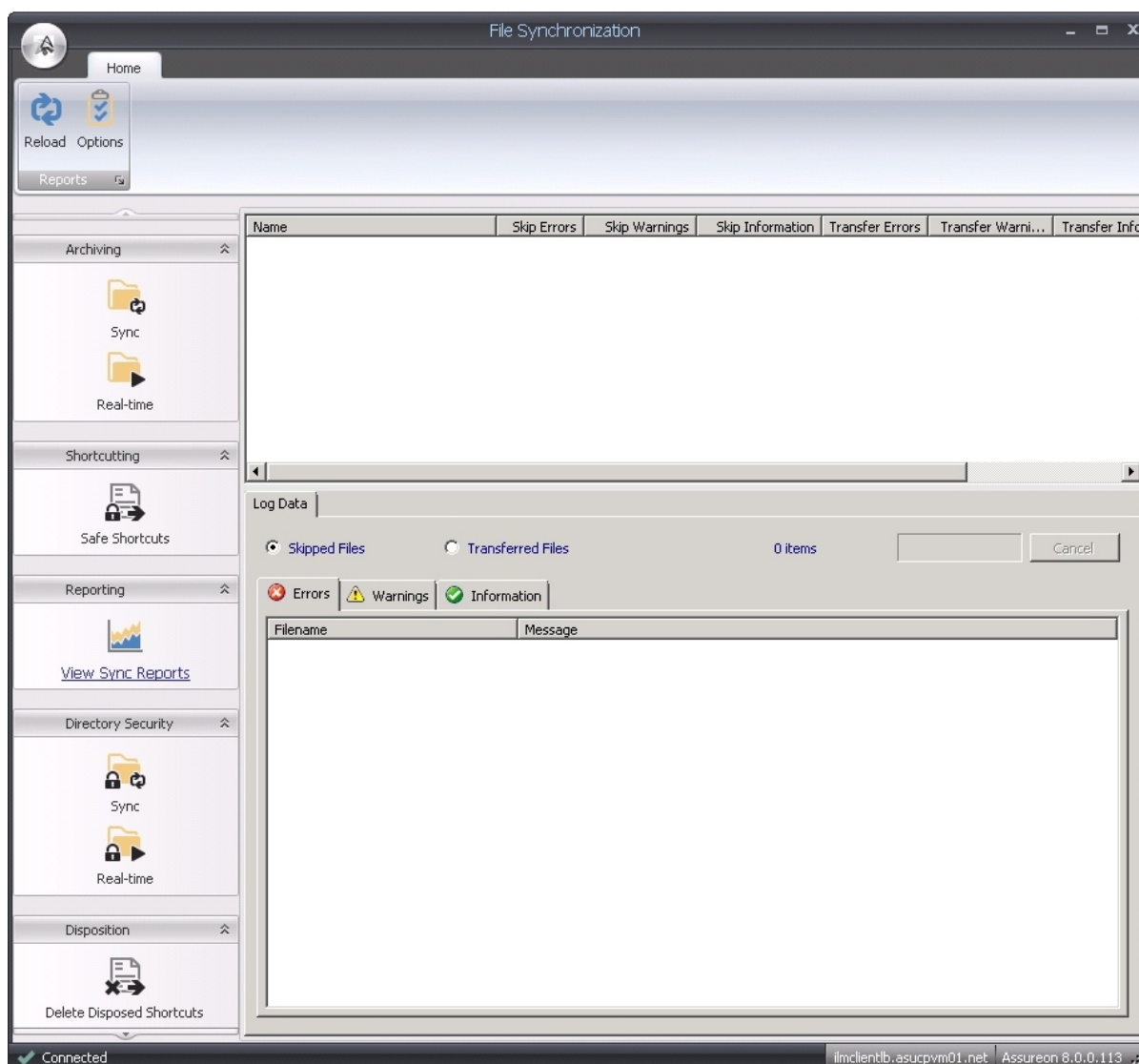
- Errors
- Warnings
- Information

► **To access this page:**

is accessed by clicking the View Sync Reports button in the [File Synchronization Utility](#) dialog box. The report is automatically displayed if there are any errors during a sync.

Reports can also be emailed to one or more recipients. To configure email options, use the [Assureon Client Options](#) dialog box.

Figure 5-4: File Synchronization dialog box - View Sync Reports page



► **Reports page details:**

- **Reload** – Refreshes the display. If new logs have been added to the folder while the Report is open, click this option to view them.

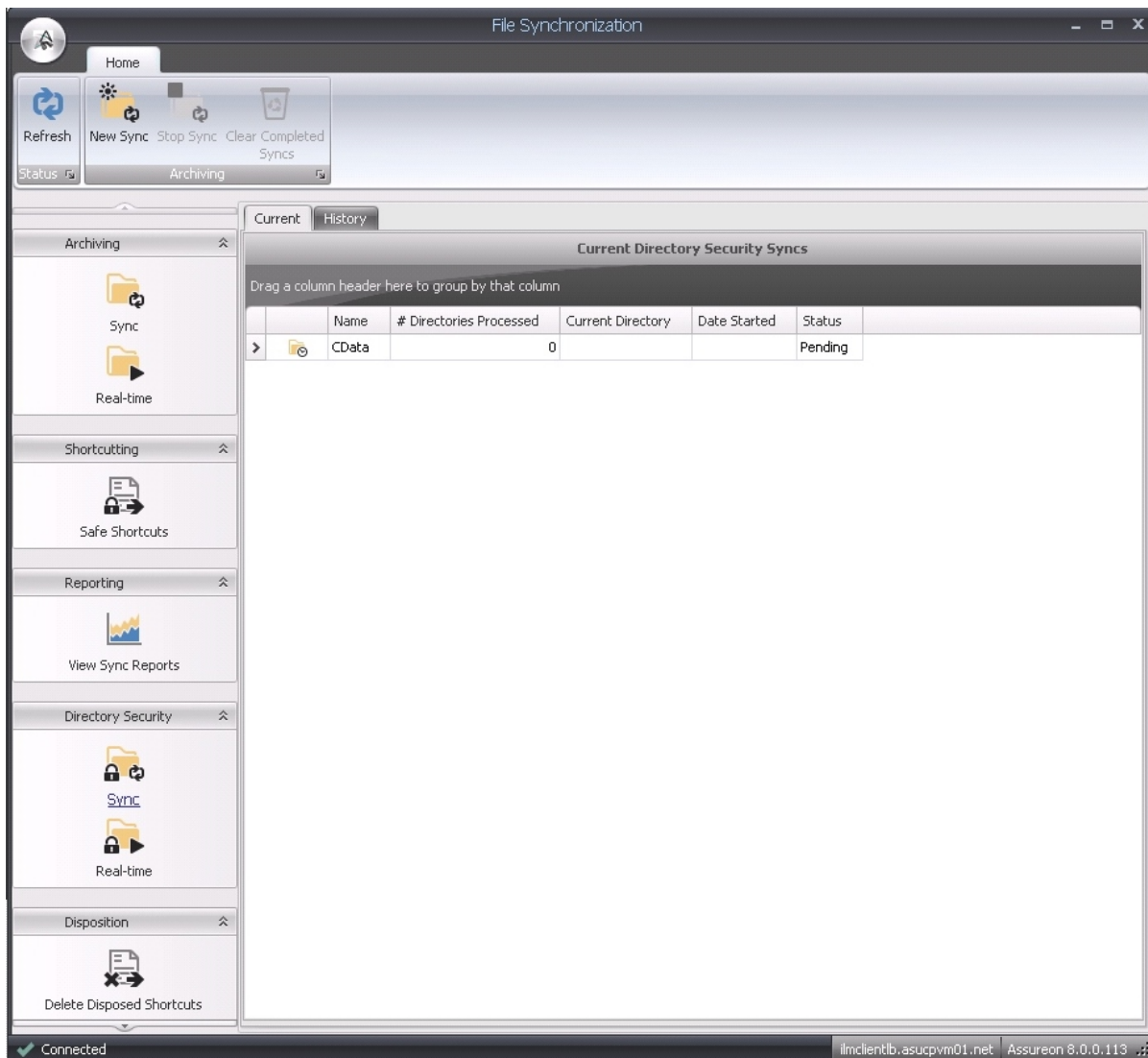


- **Options** – Specifies the location of the synchronization log files.
- **Name pane** – Displays the log files stored in the location specified in the Options dialog box.
- **Skipped Files \ Transferred Files** options – Displays the Error, Warning and Information messages contained in the log files. Select an option and then click the applicable tab.
- **Cancel** – Cancels the loading of a log file when it is selected. Use this option if you mistakenly select a very large log file.

## Directory Security - Sync

Use the **Directory Security Sync** page to view details of Sync Folder Security syncs. Changes to folder security are only sent to the server when the File Synchronization utility is run with the **Sync Folder Security** option enabled.

Figure 5-5: File Synchronization - Directory Security Sync page



► **Current and History details:**

- **Name** – The name of the archive folder. To select them all, check the box.
- **# Directories Processed** – The number of directories processed by the system during the sync.
- **Current Directory** – The directory that is being processed.
- **Date Started / Date Ended** – The date and time the sync started and ended at.
- **Status** – Indicates the progress of the sync.

**Real-time**

Use the **Security Real-time** page to monitor Real-time folder security syncs. When Real-time sync is enabled for folder security, changes to the archive folder are automatically sent to the Assureon server, within a 5-minute delay.

► **Real-time Directory Security Watches details:**

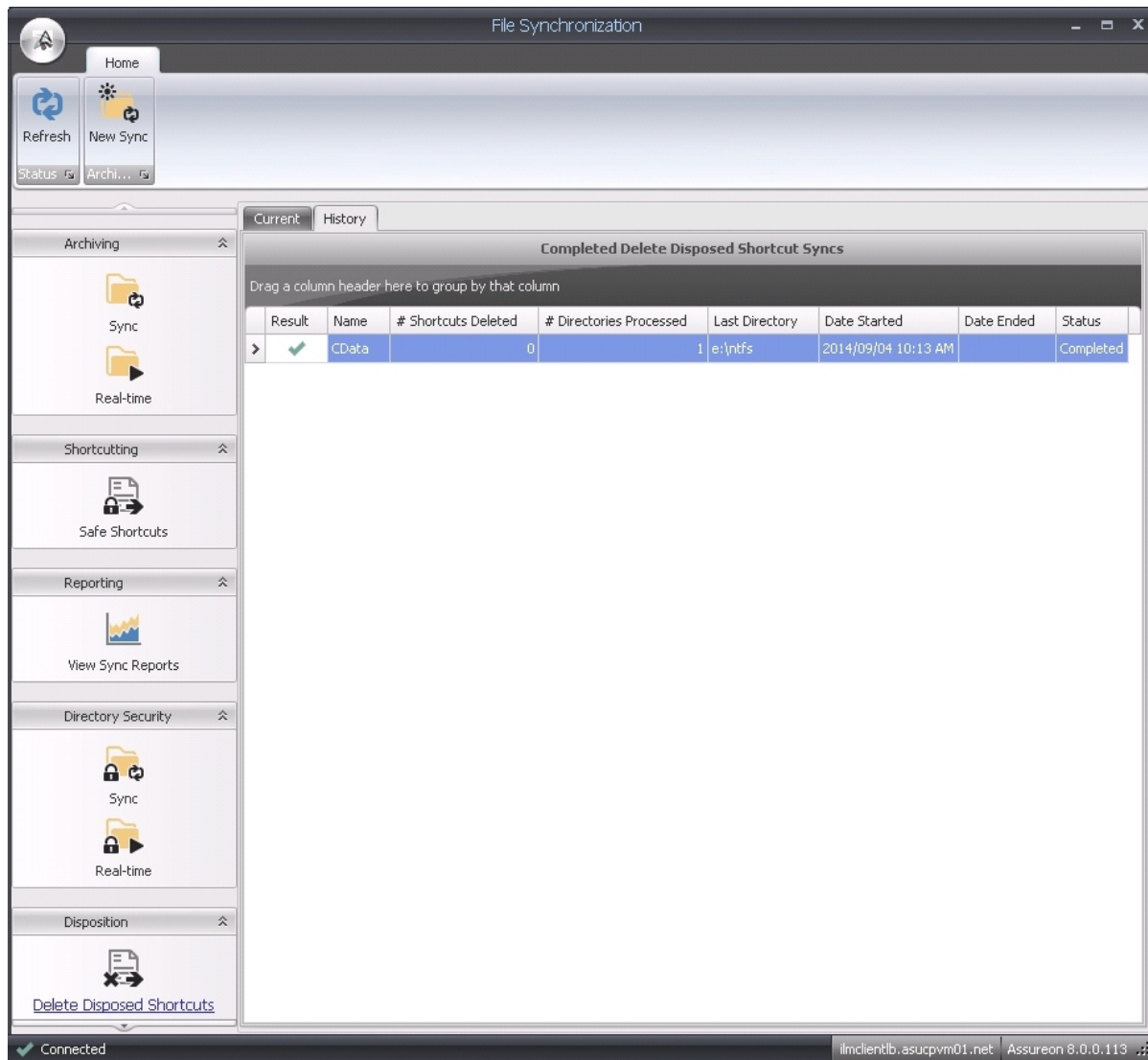
- **Name** – The name of the archive folder. To select them all, check the box.
- **# Directories Processed** – The number of directories processed by the system during the Real-time sync.
- **Last Directory** – The last directory to be processed.
- **Date Started** – The date and time the Real-time sync started at.

**Disposition - Delete disposed shortcuts**

Use the **Disposition** page to view details on the Delete Disposed Shortcuts syncs. The Delete Disposed Shortcuts sync deletes shortcuts that point to disposed files in the Assureon archive.

The **Current** tab lists all Delete Disposed Shortcuts syncs that are in the process of running, or have recently finished running. The **History** tab lists all Delete Disposed Shortcuts syncs that have recently finished running.

Figure 5-6: File Synchronization - Delete Disposed Shortcuts page



► **Current and History details:**

- **Name** – The name of the shortcutted folder. To select them all, check the box.
- **# Shortcuts Deleted** – The number of shortcutted files that have been deleted.
- **# Directories Processed** – The number of directories that have been processed throughout the sync.
- **Current Directory** – The directory that is currently being processed.
- **Date Started / Date Ended** – The date and time the sync started and ended at.
- **Status** – Indicates the progress of the sync.

## File Synchronization command line

The File Synchronization command line can be used to launch the [Assureon Synchronization utility](#) and perform a file synchronization. The command line option is typically used to run the file sync as a scheduled task, however it is not the recommended approach. Instead, we recommend that the sync be scheduled from the [Archive Folders Editor](#) in the System Administration Web interface.

The command line syntax is described in this table.

Syntax	Description
<code>-w "watchNames"</code>	The name of the archive folder to synchronize. <b>Names are case sensitive.</b> Required parameter, if <code>-all</code> is not used.
<code>-s syncType</code>	The sync type: <ul style="list-style-type: none"> <li>• <b>1</b> is a full sync (default);</li> <li>• <b>2</b> is a sync done using the archive bit;</li> <li>• <b>3</b> is a sync done using the change journal.</li> </ul> Required parameter.
<code>-f fileName</code>	The path to a configuration file containing archive folder information. Optional parameter. When not specified the <code>fswconfig.xml</code> file is used by the Client Service (in <code>C:\Documents and Settings\</code> ).
<code>-wf fileName</code>	A file containing a comma-separated list of watches.
<code>-all</code>	Synchronizes all archive folders specified in the configuration file where the Sync option has been enabled.
<code>-resume</code>	Resumes the synchronization process from where it left off.
<code>-shortcut</code>	Runs the safe shortcutting process, if enabled.

### Scheduling a synchronization process using the Windows Task Scheduler



**CAUTION:** This is not the recommended method. We recommend that synchronizations be scheduled from the [Archive Folders Editor](#) in the System Administration Web interface.

#### ► To schedule a sync using the Windows Task Scheduler under Windows Server 2008:

1. Click Start, Administrative Tools, Task Scheduler. The Task Scheduler appears.
2. In the Actions panel, click **Create Task**. The Create Task dialog box appears.
3. In the **General** tab, give the task a Name and Description. Then select the **Run whether the user is logged on or not** option.
4. Click on the **Triggers** tab and then click **New**. In the New Trigger dialog box, specify how often you want the task to run and then click **OK**.

5. Click on the **Actions** tab and then click **New**. In the New Action dialog box, browse to `FileSyncCmd.exe` (in `Nexsan Technologies\Assureon FSW`) and click **Open**.
  6. In the **Add arguments** field, add the `-all` or the `-w` parameter and the name of the archive folder to synchronize.
  7. Click **OK**, then **OK** to close the Task Scheduler. The new task will be listed in the Task Scheduler Library.
- **To schedule a sync using the Windows Task Scheduler under Windows Server 2003:**
1. Click Start, Control Panel, Scheduled Tasks, Add Scheduled Task. The Scheduled Task wizard appears.
  2. Click **Next** and then **Browse**. The Select Program to Schedule dialog box appears.
  3. Browse to `FileSyncCmd.exe` (in `Nexsan Technologies\Assureon FSW`) and click **Open**.
  4. Type a name for the task, choose when it should be performed, and click **Next**.
  5. Specify more options and click **Next**.
  6. Specify a user who has permission to access the `fswconfig` file, usually `fswmanager`, and the associated password, and then click **Next**.
  7. Check the **Open advanced properties for this task when I click Finish** option and then click **Finish**.
  8. On the Run line, add the `-all` option or the `-w` parameter and the name of the archive folder to synchronize.

## Change Journal

The Assureon **Change Journal** monitor uses the Windows change journal to track changes made to files in archive folders. When enabled, the File Synchronization utility queries the monitor to see which files have been modified; the sync does not have to traverse the entire directory structure looking for new or modified files.

The Change Journal monitor is a recommended approach.

- **To enable this feature:**
- Use the [Assureon Client Options](#) dialog box.

► **To change the Journal Size:**

When the Assureon change journal is enabled, the Windows change journal file size is determined and displayed in the Assureon Client Options dialog box. In some client installations, the default Windows change journal size may not be sufficient and changes made to files may be missed.

If more than 93 file changes per second per disk volume are handled by the server, this value will have to be increased. File changes include opening, closing, creating and deleting files, and include changes made to Windows system files. The recommended size of the journal is 134, 217, 728. You can customize the size using the following formula:

**Size in bytes** = 100 (bytes per record) \* 3 (system events per file change) \* **Number of changes to files per second** \* 60 (sec) \* 5 (minutes, default checking interval)

**Note** Assureon only uses the Windows change journal on the disk volume containing the archive folders.

## File Sync Request Watcher

The File Sync Request Watcher is a Windows service that monitors a folder for Assureon configuration files. When a configuration file is copied to the folder, files in the folder defined in the configuration file are processed using the file [synchronization utility](#).

This feature was developed for companies that cannot use the Assureon Client Service API because it is a .NET API.

For example, company ABC wants to control the retention date of the files they archive. To do this, they would normally use the Assureon Client Service Sync API and specify a list of files to archive with their respective retention dates. However, because the Assureon API requires .NET, they cannot call it from Java. The File Sync Request Watcher allows to specify a list of files to sync without calling any API.

### ► To use the File Sync Request Watcher:

1. Open the Assureon File Sync Request Watcher configuration file (by default in `Program Files\Nexsan Technologies\Assureon FileSync Request Watcher`).  
If you cannot find the folder, the service is not installed. If this is the case, run the Client Service installation utility and select this feature from the Custom dialog box.  
**Note** To see the feature expand the File System Watcher component.
2. Specify a folder for the **syncWatcherFolder** entry. This is the folder that will be monitored for configuration files.
3. Specify the same or another folder for the **syncManagerFolder** entry. This folder is used for administrative purposes. After a configuration file has been processed successfully, it is moved to the `syncManagerFolder\processed` folder.
4. Modify the other configuration settings as required:
  - `syncManagerProcessInterval`— The time interval, in seconds, when the service checks to see if there is a configuration file to process. Default is 5 seconds.
  - `syncManagerRetryInterval`— In the event that a file cannot be processed, the time interval, in seconds, when the file sync request watcher will retry to reprocess the file. During this interval, the file is moved to the `syncManagerFolder\retry` folder. Default is 300 seconds.
  - `syncManagerMaxTrials`— In the event of a problem, the maximum number of times the file sync request watcher will try to process a file. If a file cannot be processed, it will be moved to the `syncManagerFolder\error` folder. Default is 5 times.
  - `eventLogName` – The name of the Windows event log where messages (information, warning or errors) are sent. Default is `Assureon`.
  - `eventLogSource` – The name of the application displayed in the Source column of the Windows event log. Default is `FileSyncRequestWatcher`.
5. Save the file.
6. Start the service using the Windows services console.
7. Use the [Archive Configuration](#) page, to create a configuration, using a dummy Domain and Computer name.
8. Use the [Archive Folders Editor](#) to create a folder with the Name **api**.  
**Note** You must use this name.

9. Specify folder, policy and rule information. Make sure the folder is *Sync Enabled*, otherwise files will be ignored.
10. Save the archive folder.
  - ▶ **To test this feature:**
    1. Launch Windows Explorer and locate the `assureon\fswwconfig\dummy_domain\dummy_computer` folder.
    2. Copy the configuration file (`fswwConfig.exe`) to the folder specified in Step 2. The files in the watch will be processed.





# Appendix A

## Environment-specific configurations

---

This section contains information about the following environment specific configurations for Assureon:

Using certificates for authentication .....	154
Integration with Symantec EV .....	162
ADAM security model .....	164
Mac OS character support .....	166
Opened firewall ports .....	166
Windows updates .....	167
Read files from site 2 .....	167
NFS access .....	168
Creating a UNIX mount point .....	170

## Using certificates for authentication

Assureon can be configured to use certificate authentication. This mode encrypts the traffic between the Assureon Client and the server using an SSL certificate issued by the Assureon server. This certificate also determines the data that users have access to. In order to access files in the Assureon Explorer tool, users will need to have a certificate installed. Assureon shortcuts are protected using standard NTFS security. If the certificate allows access to the data in Assureon, then users who have access to the shortcuts will have access to the data.

**Note** Certificate authentication may also be used alongside Active Directory (AD) authentication. For example, some clients may use certificate authentication while others use AD authentication.

The Assureon server comes ready to support certificate authentication.

► **To configure the client to use the certificates:**

1. [Installing a certificate](#) below. You can reuse certificates across different clients, or you can issue a new certificate.
2. For new certificates, [map the certificate to a user](#). This determines what data the certificate has access to.
3. [Configure the client](#) to use the certificate.

## Installing a certificate

On the client, log on as the user who is running the Assureon client services.

**Note** To install the certificate for other users so they may access Assureon Explorer, log on as that user instead.

► **To create a new certificate:**

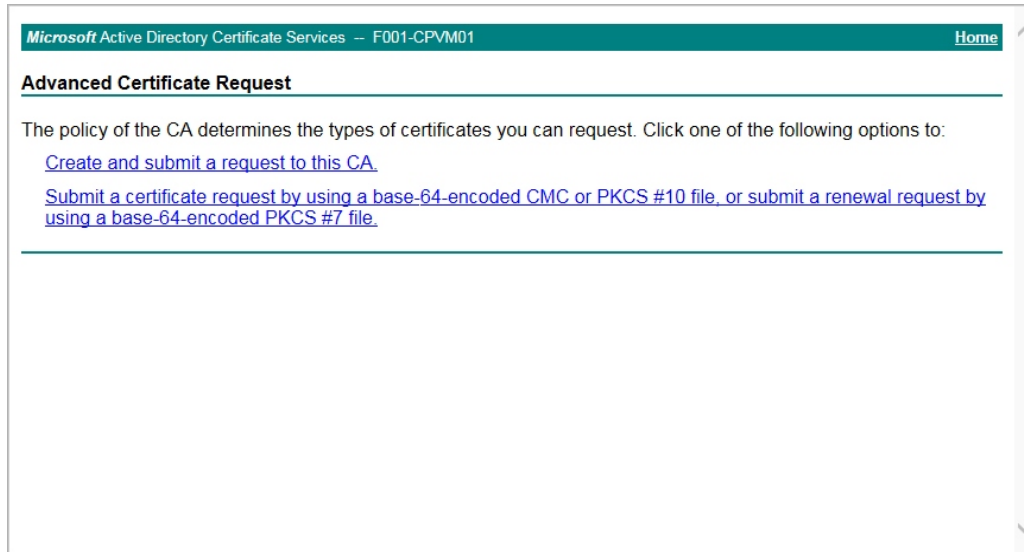
1. Launch IE and point to `https://<IP of F001 Assureon Server>/certsrv` to request a user certificate.
2. If prompted, enter the AssureonAdmin user and password. You will be redirected to the Welcome page. Click **Request a Certificate**.

**Note** If a security page appears stating "*There is a problem with this website's security certificate*", click **Continue** to this website. You will then be redirected to the **Request a Certificate** page.

3. Click **Advanced certificate request**. The Advanced Certificate Request page will open.

**Note** If the page does not appear and you instead get the **Submit a Certificate Request** or **Renewal Request** page, you must add the website IP to your browser's compatibility view settings before continuing. Once the IP address has been added, refresh your browser, click the **Home** button and repeat steps 1 through 3.

Figure A-1: Advanced Certificate Request page



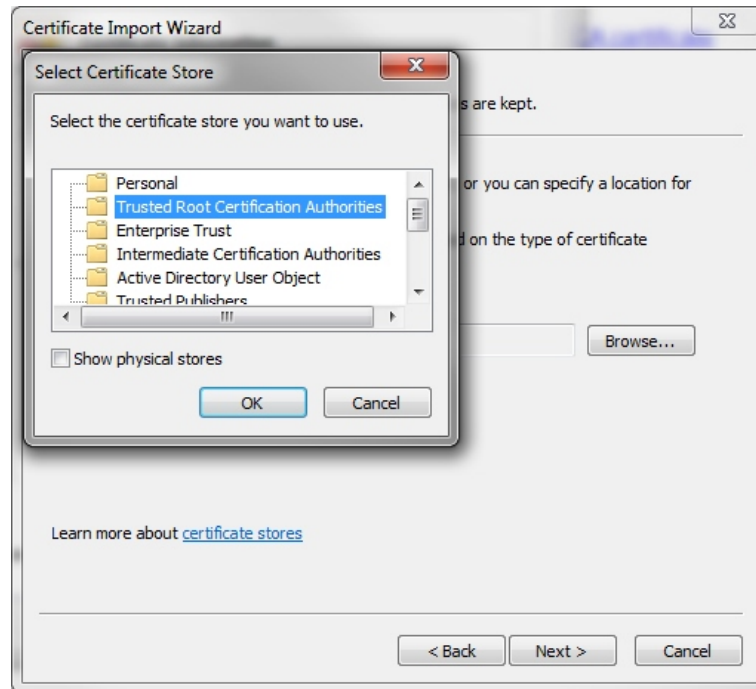
4. In the Advanced Certificate Request page, click **Create and submit a request to this CA**.
5. A Web Access Confirmation popup will appear, click **Yes**.
6. The Advanced Certificate Request page will open:
  - a. Specify a **Name** and **Friendly Name** for the certificate, often the same.
  - b. Select the **Mark keys as exportable** option under **Key Options**.
  - c. Do not enable any other options as it may cause an unsupported certificate configuration.
  - d. Click **Submit**.

**Note** If you did not use the IP address required, the following error message may display: *You did not come to this page as a result of a form submission. You may not bookmark this page.*

7. A Web Access Confirmation popup will appear, click **Yes**.
8. On the Certificate Issued page, click **Install this certificate**. A message stating the CA is not trusted will appear, click **Install this CA certificate**. Click **Open**.
9. A certificate popup will appear. Click **Install Certificate...**
10. The Certificate Import wizard will open. Click **Next**.
11. Select **Place all certificates in the following store** then click **Browse**.

12. Select the **Trusted Root Certification Authorities** folder, and click **OK**.

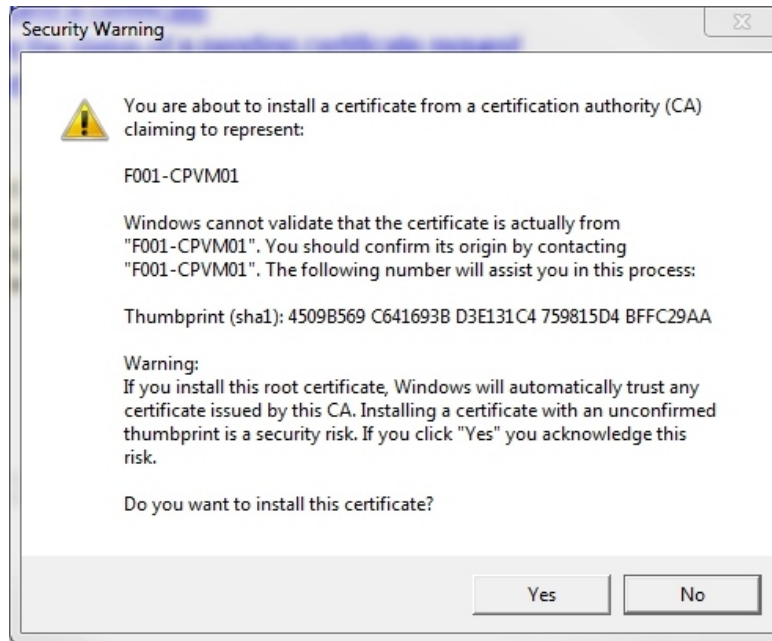
Figure A-2: Certificate Import wizard



13. Click **Next** then **Finish** to close the wizard.

14. A Security Warning popup will appear. Click **Yes** to install the certificate.

Figure A-3: Certificate Import wizard Security Warning



**Note** If no Security Warning appears, you must validate the certificate before it can be installed.

► **To validate the certificate in your Internet Explorer browser:**

- a. Open the **Tools** drop-down menu.
  - b. Select **Internet Options > Content > Certificates**.
  - c. Double-click the certificate.
  - d. Ensure that there is no warning in the top-left of the popup.
15. The Import was Successful popup appears. Click **OK**. You will be redirected to a Certificate Installed page stating that your new certificate has been successfully installed.
16. Continue by [exporting the certificate](#).
17. After exporting, [configure the Client Service to use the certificate](#) to complete the process.

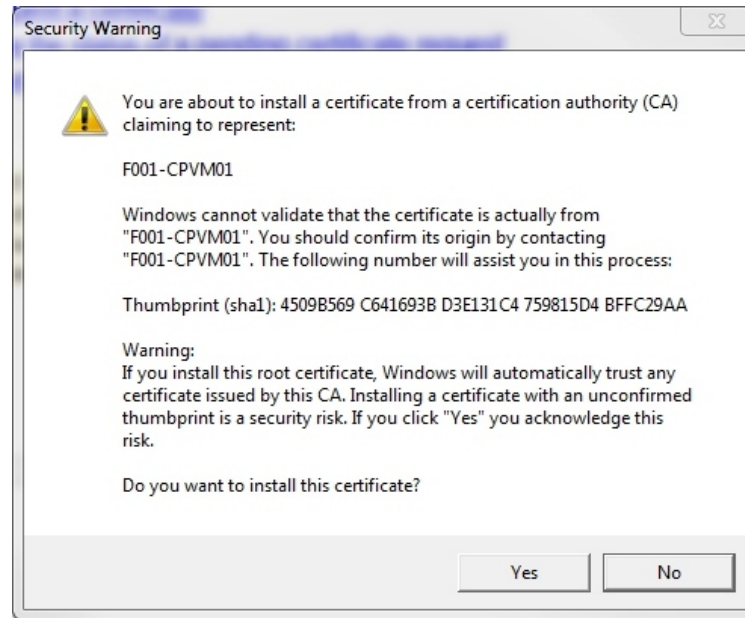
► **To use an existing certificate:**

You can use the certificate that is typically deployed in the "**Installers**" share found on the Assureon server, or you can re-use a certificate that you have stored from a different client.

1. Locate the certificate .pfx file that you would like to install.
2. Right-click the .pfx file and select **Install PFX**.
3. The Welcome to the Certificate Import wizard dialog box appears. Click **Next**.
4. On the File to Import page, click **Next** since the correct file is already selected.
5. Enter the **Password** for the certificate. This was set when the certificate was exported. For the certificate deployed with Assureon, the password is the same as for **AssureonAdmin**. Select the **Mark this key as exportable** option in addition to the **Include all Extended Properties** option. Click **Next**.
6. On the Certificate Store page, leave the default selection and click **Next**.

7. The Completed the Certificate Import wizard page appears. Click **Finish**.
8. A Security Warning popup appears. Click **Yes** to install the certificate.

Figure A-4: Certificate Import wizard Security Warning



**Note** If no Security Warning appears, you must validate the certificate before it can be installed.

► **To validate the certificate in your Internet Explorer browser:**

- a. Open the **Tools** drop-down menu.
  - b. Select **Internet Options> Content> Certificates**.
  - c. Double-click the certificate.
  - d. Ensure that there is no warning in the top-left of the popup.
9. The Import was Successful popup appears. Click **OK**.

## Exporting and mapping a new certificate

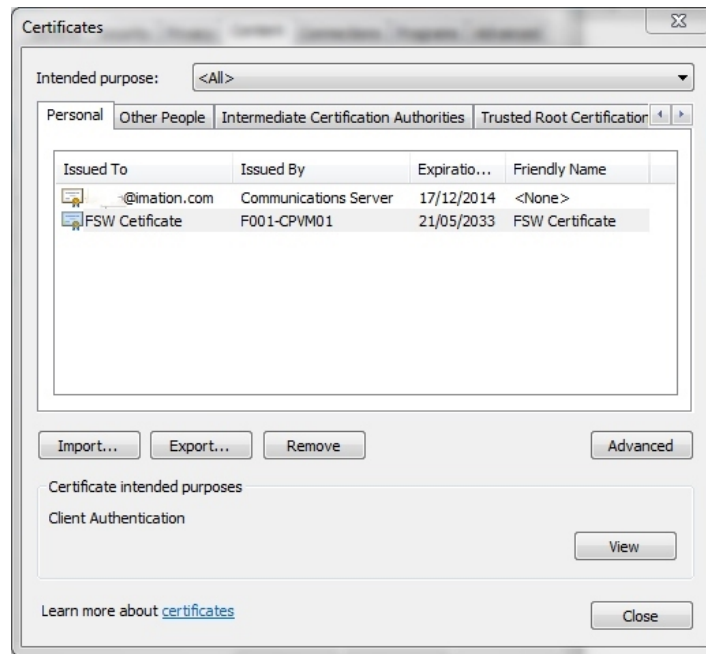
**Note** This procedure only applies if you would like to reuse the certificate for another client or user.

► **To export a new certificate for use on another computer:**

1. In *Internet Explorer*, select **Tools, Internet Options> Content> Certificates**. The Certificates dialog box opens.

- In the **Personal** tab, select the user certificate that you created (for example, FSW Certificate) and click **Export**.

Figure A-5: Exporting a certificate



- The Welcome to the Certificate Export wizard opens. Click **Next**.
- Select the **Yes, export the private key** option. Click **Next**.
- On the Export File Format page, select the **Include all certificates in the certification path if possible** option. Click **Next**.
- Specify a password and click **Next**.
- Specify a name for the exported file, click **Next** and then **Finish**.
- The Export was Successful popup appears. Click **OK** and then close.

### **Exporting a new certificate for mapping**

#### **► To export a new certificate for mapping:**

- In *Internet Explorer*, select **Tools, Internet Options > Content > Certificates**. The Certificates dialog box opens.
- In the **Personal** tab, select the Assureon Admin user certificate and click **Export**.
- The Welcome to the Certificate Export wizard opens. Click **Next**.
- Select **No, do not export the private key** option. Click **Next**.
- On the Export File Format page, select the **DER encoded binary X.509 (.CER)**. Click **Next**.
- Specify a File Name and the Assureon Installers location. Click **Next**.
- Click **Finish**. The Export was Successful popup appears.
- Click **OK** and then close.

## Mapping a certificate

User certificates must be mapped to an Assureon user account in order to access archived files.

### ► To map a new certificate:

1. Launch the Assureon System Administration user interface.
2. Click the **Advanced** button.
3. Select the **IIS Administration** tab.

Figure A-6: Advanced - IIS Administration page

The screenshot displays the Assureon IIS Administration interface. The top navigation bar includes 'Files', 'Authorization Management', 'Organization Security', and 'Options'. The 'IIS Administration' tab is selected, with sub-tabs for 'IIS Administration', 'Job Management', and 'Storage Devices'. The left sidebar contains various configuration and administration options, with 'Advanced' highlighted. The main content area is divided into two sections:

**Certificate Mapping**

Drag a column header here to group by that column

Mapping Name	Windows Account	Cert Issuer	Cert Serial	#
No data to display				

Certificate File Path:

Mapping Name:

Account:

Password:  Confirm Password:

**Virtual Directory Configuration**

Virtual Directory:

**Security**

- Enable Anonymous Access
- Integrated Windows Authentication
- Digest Authentication for Windows Domain Servers
- Basic Authentication
- .NET Passport Authentication

**Secure Communication SSL**

- Require Secure Channel (SSL)
- Require 128-bit Encryption
- Enable Cert Mapping

Ignore Client Certificates  
 Accept Client Certificates  
 Require Client Certificates

4. In **Certificate Mapping**, click **Browse** and open the user certificate folder on the local computer.
5. Type a **Mapping Name**, and then specify a user and password that is a member of one or more Assureon Active Directory Classifications. Typically, the `AssureonEdge` account is used if files are stored and read by an application, such as an email archive.

**Note** Include the domain name; it should be the netbios domain name (`Assureon\AssureonEdge`), in the **Account** field.

6. Click **Add**. The mapping is added to the table at the top of the page.



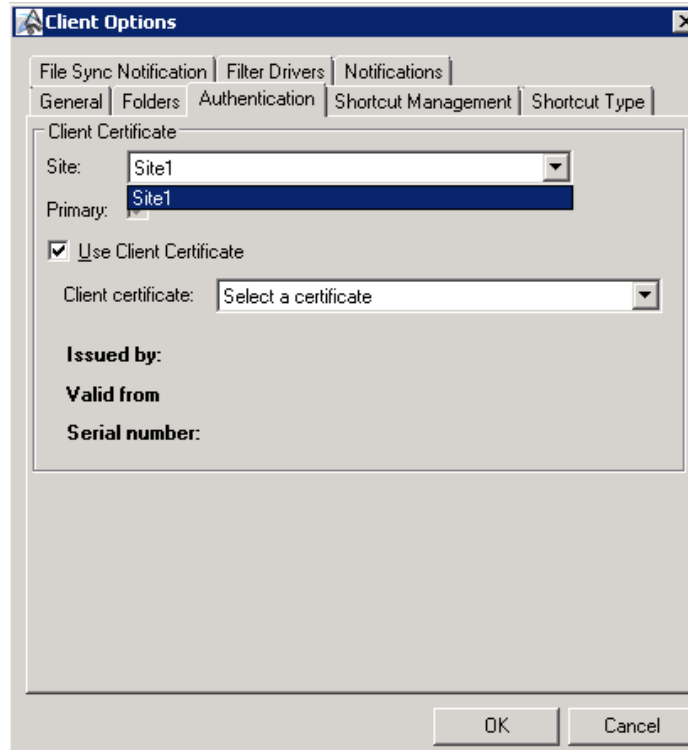
## Configuring the client to use a certificate

On the client, log on as the user who is running the Assureon client services.

### ► To Configure Client Service to use the Certificate:

1. On the client computer, right-click the Client Service taskbar icon and select **Options**. The Client Options dialog box opens.

Figure A-7: Client Service taskbar - Client Options



2. Select the **Authentication** tab.
3. Select the site from the drop-down list.
4. Select the **Use Client Certificate** option then select the friendly name of the certificate that you created; for example, *FSW Certificate*. Click **OK**.
5. A Restart services popup appears. Click **Yes**.
6. If applicable, repeat steps 3 through 5 to enable the Client Certificate for the other site.

## Integration with Symantec EV

Symantec EV is used to place files in a dedicated vault store partition, called Assureon Archive, where the SnapLock protocol has been implemented. When the files in the partition are marked as read-only, they are archived on the Assureon server and, depending on the archive policy, a shortcut created. In keeping with the SnapLock protocol, Assureon uses the last accessed date of the file as its retention date.

This topic assumes you are using an active directory trust between corporate server and the Assureon server for authentication. The EV client must be joined to the corporate domain and the trust established.

If you are using security certificates, see these topics:

- [Creating an Assureon Archive partition](#) below
- [Installing Assureon Client Services](#) on the facing page
- [Creating an Archive folder](#) on the facing page
- [Scheduling a Sync](#) on page 164
- [Security Certificate](#) on page 164

### Creating an Assureon Archive partition

For details on the options, please refer to your Symantec Enterprise Vault documentation.

► **To create the dedicated vault store partition:**

1. Log on to the Symantec EV client and select **Start> All Programs> Enterprise Vault> Administration Console**.
2. In the console, expand the tree on the left. Keep expanding until you see the **Vault Store Groups**.
3. Select the Vault Store Group you want to add the partition to, right-click in the right panel, and select **New> Partition**.
4. The New Partition dialog box, welcome page appears. Click **Next**.
5. The name and description page appears. Specify a name and description for the partition and then click **Next**.
6. The storage type page appears. Select **Assureon Archive** and then click **Next**.
7. The location page appears. Specify an existing location and click **Next**.
8. The partition rollover page is displayed. Specify a rollover and then click **Next**. This step is optional, depending on your site configuration.
9. The security ACLs page is displayed. Specify whether you want the partition created with security ACLs and click **Next**.
10. The secured options page appears. Specify your secured options and click **Next**.
11. The summary page appears. Click **Finish**.

#### *Disabling the last access update*

In order to use the SnapLock protocol, updates to the last date accessed file property from the Windows operating system must be disabled. If you are already using SnapLock, this should already be done. Please verify the following; if the change has not been done, please make it.

**Note** If you do make the change, a reboot of the system is required.

► **To disable last access update:**

1. Log on to the Symantec EV client, and select **Start> Run**.
2. In the Run dialog box, type `regedit` and then press Enter.
3. The Registry Editor dialog box appears. Expand this registry key:  
`HKEY_LOCAL_computer\SYSTEM\CurrentControlSet\Control\FileSystem.`
4. In the right panel, right-click **NtfsDisableLastAccessUpdate** and select **Modify**.
5. Make sure the **Value** data is set to **1**.
6. Click **OK** and then close the Registry Editor.
7. Reboot if you changed the value.

## Installing Assureon Client Services

For details on this step, please see [Installing the client service](#).

## Creating an Archive folder

To archive files, use the Assureon System Administration console to create a retention rule, access classification and archive folder. The following procedure is an overview; for detailed information, please see the [Archive Folders Editor](#) topic.

► **To create an Archive folder:**

1. On the Assureon Server, log on using the `AssureonAdmin` user.
2. Launch *Internet Explorer* and access the Assureon System Administration console.
3. In the main menu, click **Access Control**.
4. In the **Access Classification** tab, select an organization and then create a classification.
5. In the main menu, click Retention. Select an organization and create a retention rule. Be sure to select the Retention Period, Use Read-Only Lock option.
6. In the main menu, click **Archive Folders**. The Archive Folders, Configuration tab is displayed.
7. In the **Configured Computers** panel, **Domain** and **Computer** fields, specify the corporate domain and then the computer name. Then click **Add**.
8. Click **Edit** to display the Archive Folders Editor.
9. In the editor, click **Add folder** and define the archive folder. Be sure to specify name, folder, organization, access classification and retention rule information:
  - a. For **Folder**, specify the vault store partition location you specified above.
  - b. For EV, you should process files using a scheduled Sync. To do so, disable the Real-time option, make sure **Sync** is enabled, and see for details on scheduling the Sync.
  - c. For the **RetentionRule**, select the one you created in Step 4. Ignore the (0 days) part of the description. You can also specify a **Defaultretentionrule**, which will be applied if the last access date on the file is not set to a future date.
  - d. Click **Save**.

10. On the **Symantec EV client**, start the Assureon client service:
  - a. Right-click the **FSW Agent** icon on the system tray.
  - b. Select **Start Client Service**. If the FSW Agent tray icon has a green check-mark, it means the service has started successfully.

## Scheduling a Sync

The [Sync](#), short for Synchronization utility, is an Assureon utility used to archive files. For more information about running the Sync as a Windows scheduled task, please see the [File Synchronization Command Line](#) topic.

## Security Certificate

If you are using a digital certificate for authentication, please modify the procedures as follows:

- When [installing the Assureon client service](#), create the `FSWManager` user on the Assureon server.
- After the Assureon clients have been installed, configure them to use the digital certificate. For details, please refer to the *Assureon Installation Guide – Certificates*.
- After the Assureon client has been installed, use a text editor to add the following entries to the hosts file (in `c:\windows\system32\drivers\etc`) on the server. In the following examples, `IPofF001` is the IP of the primary Assureon Server, and `ASUxxxxxxx` is the name of the Assureon domain:`IPofF001.`

## ADAM security model

Assureon supports the ADAM (Active Directory Application Mode) security model. ADAM allows customers who do not have a trusted relationship between their corporate server and the Assureon server to manage user security.

Typically an ADAM instance is installed on an Assureon client. Users are added to the instance using a console application. Other Assureon clients installed on the same corporate domain can share the user information. Authentication between the clients and the Assureon server is automatically handled, allowing only authorized users to access files and the System Administration console.

### ► Installation overview:

The following is a summary of the steps required to install and use ADAM.

1. Install an ADAM instance and an Assureon client service using the Assureon client install
2. Install other Assureon clients, pointing to the existing ADAM instance
3. Install digital security certificates
4. Create a watch using the Assureon System Administration console
5. Add users to ADAM using the security console
6. Configure organization security

If you want to use ADAM, you can install it using the Assureon client installer.

### ► To install the ADAM Instance:

1. Launch FSW setup and then click **Next**.
2. Select a destination folder. Click **Next**.
3. Select the **Custom** setup type.

4. From the list of features, select **ADAM instance** and click **This feature will be installed on the local hard drive**. Click **Next**.
5. Enter a port for ADAM, and select **Do you want to open this port in the firewall?** if other clients will be connecting to this ADAM instance.
6. Specify a user name and password for the service. This user will also be the ADAM administrator. Click **Next**.
7. Click **Install**.

► **To install the Assureon client and configure it to use an existing ADAM instance:**

1. Launch FSW setup. Click **Next**.
2. Select a destination folder. Click **Next**.
3. Select the **Typical** setup type and click **Next**.
4. Select **Use an existing ADAM instance** and then type the server address where the corporate ADAM instance resides.
5. Specify a user name and password for the Assureon client service.
6. Click **Install**.

► **To install the required digital security certificates:**

ADAM requires the installation of digital security certificates between the FSW clients and the Assureon server.

1. From the client, request and install a user certificate from the Assureon server.
  2. Then, configure the Assureon client to use that certificate. For details, see the procedures in the [Using Certificates for Authentication](#) topic.
- Note** Only one certificate is required for ALL users. This is because ADAM is used for authentication.
3. On the Assureon server, use the Assureon System Administration console, [IIS Administration](#) page to create a mapping for the client user certificate to the `AssureonEdge` account.
  4. On the Assureon client, start the Assureon Web Server Proxy service.

► **To create a watch:**

1. On the Assureon Server, use the Assureon System Administration console, [Archive Folders](#) page to create the first watch.
2. Use the Assureon System Administration console, [Clients](#) page to make sure the new configuration is downloaded to the client.

► **To add users to ADAM:**

1. On the Assureon client where the ADAM instance has been installed, logon as the ADAM Administrator (the user used to install ADAM) and open the Security Console by double-clicking the Security Console icon located on the desktop.
2. Add users to the new groups that have been created in ADAM. This step will need to be repeated every time a watch is configured using a new organization.

► **To configure organization security:**

1. On the Assureon server, launch the Assureon System Administration console and click **Advanced**, and then the **Organization Security** tab.

2. Select the organization being used by the watch.
3. Enter the serial number of the user certificate issued to the client computer. You can see the serial number on the IIS Administration page.
4. Click **Add**.
5. If this is Plus system, repeat these steps on site 2.

► **To access the System Administration console from a client:**

- To access the Assureon System Administration console from a client computer running ADAM, enter `http://localhost:8080/AssureonSysAdmin/default.aspx`.

## Mac OS character support

Assureon supports archiving file names with Mac OS characters and restoring these files from Windows Explorer.

► **To enable Mac OS character support:**

1. The `foreignFileMap` configuration entry must be "uncommented" from the following configuration files (located by default in `\Program Files\Nexsan Technologies` folder):
  - `AEExplorer.exe.config` (in the Assureon Explorer or Assureon Explorer Server folder)
  - `AEShellExt.dll.config` (in the Assureon Explorer or Assureon Explorer Server folder)
  - `AssureonFSW.exe.config` (in the Assureon FSW folder)
  - `RestoreServerService.exe.config` (in the Assureon Restore Server folder)
2. After making the configuration file changes, restart the Client Service.

## Opened firewall ports

The following ports are opened on the Assureon server:

Description	Port	Protocol
Assureon HTTP	80	TCP
<b>The following port may be closed if certificate-based authentication is NOT used.</b>		
Assureon HTTPS	443	TCP
<b>All of the following object request broker ports are opened by default. For added security, you may close the ports that you do not use.</b>		
Assureon Object Request Broker Unsecure ( <b>default</b> )	65116	TCP
Assureon Object Request Broker Secure	65120	TCP
Assureon Object Request Broker Certificates	65129	TCP
<b>The following ports are opened in order to establish a trust between Assureon and a corporate server. They may be closed if anonymous or certificate-based authentication is used.</b>		
Assureon Active Directory TCP	389	TCP

Description	Port	Protocol
Assureon Active Directory UDP	389	UDP
Assureon Secure Active Directory	636	UDP
Assureon Active Directory Catalog	3268	TCP
Assureon Secure Active Directory Catalog	3269	TCP
Assureon Net Bios Name Service	137	TCP
Assureon RPC TCP	135	TCP
Assureon RPC UDP	135	UDP
Assureon RPC	1221	TCP
Assureon Kerberos TCP	88	TCP
Assureon Kerberos UDP	88	UDP
Assureon DNS TCP	53	TCP
Assureon DNS UDP	53	UDP
Assureon IP Security	500	UDP

The following applications and services are opened to the outside:

- Remote Desktop
- File and Print Sharing

In situations where you need to open ports for the Client Services (usually NOT required), here are the required ports:

- 65116 (default)
- 65120 (if using secure communications)
- 65129 (if you are using certificates)

## Windows updates

Windows updates to the Assureon cluster are automatically handled using a Nexsan-based Windows WSUS service. By default, updates are downloaded to the cluster at 11 PM (local time) every Friday. The updates must then be installed by an administrator. Some updates require a system reboot, so perform the updates only when files are not being processed.

## Read files from site 2

To configure Assureon Explorer to read files from site 2 of a Plus configuration, you need to modify your Assureon client workstation.

► **To read files from site 2:**

1. Make sure you can ping `ilmclientlb2.ASUxxxxxx.net`, where `ASUxxxxxx.net` corresponds to the Assureon domain.  
If you cannot ping the address, add an entry to your DNS server or local Hosts file.
2. With a text editor, open the `AEEExplorer.exe.config` and `AEShellExt.dll.config` files (in `c:\Program Files\Nexsan Technologies\Assureon Explorer`).
3. Modify the `primaryServer` and `primaryOrbServer` configuration file keys so that they point to `ilmclientlb2.ASUxxxxxx.NET`.

## NFS access

The [Assureon Filter Driver](#) may be used on a Windows-based workstation where NFS (Network File System) has been installed. Access to the NFS share is controlled using ANONYMOUS LOGON.

**Note** The ANONYMOUS LOGON option uses a digital security certificate issued by the Assureon server for authentication.

To configure your Windows workstation for use with Solaris, perform the following procedures.

► **To install Services for Network File System Role:**

1. Logon to the workstation where the Assureon Client Services will be installed.
2. Launch the Server Manager:  
Select **Start**> **Administrative Tools**> **Server Manager**.
3. In the tree view, click **Roles**.
4. In the right pane, click **Add Roles**.
5. The Add Roles wizard page appears. Click **Next**.
6. The Select Server Roles page appears. Select **File Services** and click **Next**.
7. The File Services page appears. Click **Next**.
8. The Select Role Services page appears. Select **Services for Network File System** and click **Next**.
9. The Confirm Installation Selections page appears. Click **Install**.
10. The Installation Results page appears. Click **Close**.

► **To create a shared folder using NFS sharing:**

1. Log in to the workstation running NFS Server.
2. Create the folder that will be used for the NFS share.
3. Right-click the NFS share folder, select **Properties** and then **NFS Sharing**.
4. Click **Manage NFS Sharing**.
5. Select the **Share this folder** option.
6. Perform one of the following actions:
  - For Windows Server 2008, select the **Allow anonymous access** option.
  - For Windows Server 2008 R2, select **Enabled unmapped user access** and the **Allow unmapped user UNIX access (by UID/GID)** options.
7. Click **Permissions**.



8. Change the **Type of access** to **Read-Write**.
  9. Select the **Allow root access** option.
  10. Click **OK**, and **OK** again.
  11. In the Properties dialog box, click the **Security** tab.
  12. Click **Edit**, and then **Add**.
  13. Add **ANONYMOUS LOGON** and then click **OK**.
  14. Give the ANONYMOUS LOGON user **Full Control**.
  15. Click **Edit**, and then **Add**.
  16. Add **Everyone** and then click **OK**.
  17. Give the Everyone user **Full Control**.
  18. Click **OK** and then **Close**.
- **To modify local group policy for anonymous:**
1. Click **Start**, type `gpedit.msc` in the Start Search text box, and then press Enter.
  2. The Local Group Policy Editor dialog box appears. In the console tree, open Computer Configuration, Windows Settings, Security Settings, Local Policies, and then click **Security Options**.
  3. In the middle pane, right-click **Network access: Let Everyone permissions apply to anonymous users**, and select **Properties**.
  4. To allow permissions that are applied to the Everyone group to apply to anonymous users, click **Enabled**.
  5. Click **OK**.
  6. Close the Local Group Policy Editor dialog box.
- **To configure the Solaris server:**
1. Logon to the Solaris server.
  2. Using a text editor (VI), open the NFS file in `/etc/default/` and add or modify the following line:  
`NFS_CLIENT_VERSMAX=3`
  3. Run the following mount command:  
`mount -F`
- **On the Assureon server:**
1. If your Edge devices are joined to the Assureon domain, create a new user called `clusteruser` in the Assureon domain.
  2. On the server, configure Assureon and the Assureon Client to use [digital security certificates](#).  
[Map the certificates](#) to the `clusteruser` user.
  3. Add the `clusteruser` user to the appropriate Assureon active directory organization and classification-based security groups.
  4. After doing so, launch the Assureon System Administration console and select **Advanced> Authorization Management> Reset**.

► **On the Assureon Client (Edge device):**

- Install the Assureon Services using the `clusteruser` user and configure the Assureon Client for certificates.

► **To remote desktop to the Edge devices, add AssureonAdmins to the local computer Administrator group:**

1. Click **Start**, right-click **Computer** and select **Manage**.
2. Expand **Configuration, Local User and Groups** and select **Groups**.
3. Right-click **Administrators**, select **Properties**.
4. Click **Add** to add the `AssureonAdmins` group.

## Creating a UNIX mount point

The Filter Driver is supported on Linux via NFS mount points. In this scenario, the Client Service is installed on a Windows Server 2003 workstation.

► **On the Client Service computer where NFS has been installed:**

1. Log on as an administrator.
2. Select **Start> All Programs> Administrative Tools> Microsoft Services for Network File System**.
3. Right-click **Microsoft Services for NFS** and select **Properties**.
4. Verify that **User Name Mapping Server** is set to `localhost` and then click **OK**.
5. Leave the NFS console open.

► **On the Linux computer:**

1. Log on as `root`.
2. Locate the user (`/etc/passwd`) and group (`/etc/group`) files and then copy them to the Client Service computer.

► **On the Client Service computer:**

1. In the NFS console, right-click **User Name Mapping** and select **Properties**.
2. Select the **Use Password and Group files** option.
3. Specify the file locations and click **OK**.
4. Right-click **User Maps** and select **Create Map**.
5. Click **List Windows Users** and then **List UNIX Users**.
6. Select the Windows User and then the UNIX User you want to map to. For example, `administrator` and `root`.
7. Click **Add** and then **Close**.

► **On the Linux computer:**

- Launch a command prompt and create a mount point by typing:

```
>mount ipAddressofFSW:/nameOfWatchOnFSWServer /directoryinLinux/Folder
```

Where:

- `ipAddressofFSW` – The IP address corresponding to the FSW computer
- `nameOfWatchOnFSWServer` – The watched folder
- `directoryinLinux/Folder` – The mount point on the Linux computer

► **On the Client Service computer:**

- Set the watched folder properties as follows.

Properties	Item	Setting
Security	Administrators	Full control
	Create Owner	Full control
	Systems	Full control
	Users	Full control
Sharing	Do not share this folder	
NFS Sharing	Share this folder	checked
	Share name	watched folder
	Encoding	ANSI
	Allow anonymous access	checked
	Permissions	Click on
NFS Share Permissions	Name	All computers
	Type of Access	Read-Write
	Encoding	ANSI
	Allow root access	checked
Assureon	Archive this folder	All settings should match those in Assureon System Administration console, Archive Folders Editor page



# Appendix B

## Advanced options

---

The following Advanced Assureon options required assistance from [Nexsan Support](#):

Backing up with a replicated configuration .....	174
Assureon server outage .....	174
Shutting down or restarting Assureon .....	174
Store data protection .....	174
Time synchronization .....	175
Clustered NAS .....	175
Database Transaction Log Shipping .....	175
NTFS security integration .....	176
Data Migration wizard .....	176

## Backing up with a replicated configuration

The best way to back up Assureon is to purchase a Replicated, or remote site, configuration. In this configuration, site 2 contains a copy of site 1, and site 1 a copy of site 2. Because the copy contains all files under management, retention rules, classifications, manifests, and so on, either site can continue operations in the event of a failure.

If a Replicated configuration is not an option, we recommend that you use the Windows backup utility, or a third-party backup software, to back up folders on the Assureon server. For more information, please contact [Nexsan Support](#).

## Assureon server outage

If an Assureon server becomes unresponsive, please contact [Nexsan Support](#).

On replicated systems, Assureon clients have automatic read failover enabled. In the case of an outage, shortcuts will continue to work by automatically reading from the second site. This means that shortcuts will continue to work by automatically reading from the second site in the case of an outage. Automatic write failover, however, is disabled by default.

Single site systems do not have any failover possibilities.

## Shutting down or restarting Assureon

### ► To shut down Assureon:

1. Stop all client services (FSW service) on the Assureon servers and workstations.
2. Wait for all private message queues to be empty (except for the `keyserialnumbers` one).
3. Disable the **Enable Auto Restarts** option in the System Administration console, [Services](#) page.
4. Using the System Administration console, Services page, stop all Services on all nodes.
5. Shut down the computers in the following order:
  - a. Back-ends first.
  - b. Then the front-ends.

**Note** You do not need to turn off storage hardware unless you are relocating storage.

### ► To restart Assureon, turn the computers back on in the following order:

1. Turn on all storage hardware (if shut down).
2. Turn on all front-ends, starting with F001, then F002, and so on.
3. Turn on all back-ends, starting with B001, then B002, and so on.
4. Enable the **Enable Auto Restarts** option in the System Administration console, [Services](#) page.
5. Using the System Administration console, Services page, verify that all services are started on all servers.
6. Start all client services (FSW service).

## Store data protection

Store data protection is an optional component installed on an Assureon cluster that adds an extra degree of protection to archived files (and meta data) kept in the Assureon archive. Once installed, files in the store cannot be modified or deleted, or the drive reformatted, even by a user with administrative passwords.

Data protection uses the Assureon Data Protection server as well as a specialized driver. When protection is enabled, the server handles file disposition. For more information about this option, please contact your Nexsan representative.

## Time synchronization

By default, Assureon is configured to synchronize its time with the following time servers:

- time.nrc.ca
- time.nist.gov
- time-a.nist.gov

Should you require to specify another time server, please contact [Nexsan Support](#) for details on how to do this.

## Clustered NAS

Clustered NAS is an optional Assureon component that provides a single archiving location distributed across multiple NAS servers. Using the latest hardware and software technologies, this configuration features:

- Windows Network Load Balancing clustering technology for high availability and scalability
- Ultra fast file archiving and file retrieval capabilities

For more information about this feature, please contact [Nexsan Support](#).

### Virtual Shortcuts with Clustered NAS

When using virtual shortcuts with clustered NAS, you can now set up multiple servers as an active/active cluster configuration. Each server has access to all files. You no longer need to deploy Microsoft clustering or Windows Enterprise.

## Database Transaction Log Shipping

The Assureon Database Transaction Log Shipping feature is an effective way to leverage an existing Assureon SX Plus configuration as a backup and restore mechanism for Microsoft SQL Server 2005 databases residing on servers.

The entire database backup and restore process is automated and is designed specifically for use over a wide area network (WAN). Should the primary, production database on site 1 go offline, the standby server on site 2 may be quickly activated.

The Assureon database transaction log shipping strategy is an economical option that can be easily implemented.

### ► **Process overview:**

- SQL scripts are used to perform a full backup of the production database
- The backup file is stored to an archive folder and then archived by Assureon FSW
- The backup file is replicated to site 2 by Assureon
- On site 2, Assureon Explorer and SQL scripts are used to restore the database
- Scheduled SQL jobs generate transaction log files on the SQL workstation
- The transaction log files are archived using Assureon FSW and replicated to site 2 using Assureon
- On site 2, Assureon Explorer and SQL scripts are used to restore the logs.

For more information about this feature, contact [Nexsan Support](#).

## NTFS security integration

Assureon has been integrated with Windows NTFS security. This security model may be used instead of or in conjunction with Assureon Access Classifications.

This model gives users read access to archived files (via shortcuts, Assureon Explorer, the System Administration console, and the Coveo search engine) based on NTFS folder security. You do not need to add corporate users to the access classification-based Assureon active directory security groups.

Access to the Assureon System Administration console, Restore Files and Search pages is automatically granted to NTFS-defined users; Users can only view and restore their own files. Full access to the Assureon System Administration console is controlled using Assureon AD access classification-based security.

This model requires a two-way active directory trust between the corporate and Assureon servers. Assureon clients are members of the corporate domain.

Security is set per client computer and enabled using the Assureon System Administration, Clients, [Client Information](#). Select the security model from the drop-down list.

Once enabled for a computer, the archive folders for that computer must be configured (with the System Administration, Archive Folders Editor page) to use the model with the Real-time or Sync Folder Security options:

- **Real-time Folder Security:** Changes to the folder security are automatically sent to the Assureon server, within a 5 minute delay.
- **Sync Folder security:** Changes to folder security are only sent to the server when the File Synchronization utility is run with the Sync folder security option.

## Data Migration wizard

Assureon systems are available in Single or Replicated configurations, where a second Assureon server (a mirror) is kept in another location.

Replicated configurations are active – active, meaning both sites can be used to store and retrieve files. Replicated configurations are recommended for customers who want to implement an effective disaster recovery strategy.

The Data Migration wizard can be used to migrate from a single to a replicated configuration. Options include:

- Upgrading to a Plus configuration using existing sites. Keeps all existing file systems.
- Rebuilding site 1 or 2 should the other site be irretrievably lost
- Backing up and restoring data from one site to another

The wizard is intended to be used by trained Assureon personnel only. Please contact [Nexsan Support](#) prior to using this component.



# Appendix C

## System messages

---

This section details common messages generated by Assureon. Included with each message is a detailed explanation and solution.

The messages are grouped by Assureon component:

Disposition messages .....	178
Key Manager messages .....	179
Key Server proxy messages .....	180
Manifest Server messages .....	181
Object Request Broker messages .....	181
Storage Server messages .....	185
Storage Web Services messages .....	186
Restore Server messages .....	186

## Disposition messages

<b>Source</b>	DispositionMgr
<b>Location</b>	DispositionManager
<b>Event ID</b>	101
<b>Event Type</b>	Error
<b>System Error Message</b>	Failed to get the log summary from the database. FSGUID: + fsGUID + ". System reports:" + ex.Message
<b>Cause</b>	An error occurred attempting to retrieve the disposition log from the database. Likely, the database server did not respond within the allowed period of time.
<b>Action</b>	The system will dispose of the files at the next scheduled time. If this error message occurs again, please contact <a href="#">Nexsan technical support</a> .
<b>Source</b>	DispositionMgr
<b>Location</b>	DispositionTrigger
<b>Event ID</b>	1390
<b>Event Type</b>	Error
<b>System Error Message</b>	There was a problem with the disposition. System reports: + ex.Message
<b>Cause</b>	The system could not process a scheduled disposition.
<b>Action</b>	No action is required. The service will automatically retry later. If this message occurs frequently, please contact <a href="#">Nexsan technical support</a> .
<b>Source</b>	DispositionMgr
<b>Location</b>	DispositionTrigger
<b>Event ID</b>	15007
<b>Event Type</b>	Error
<b>System Error Message</b>	Time is not in sync with Key Server. Latency: {0:0.00} seconds. Disposition will not take place.
<b>Cause</b>	An error occurred trying to contact the key server. The clock on the Assureon server may be inaccurate, and so it was not allowed to communicate with the key server for security reasons.
<b>Action</b>	Check connectivity to the key server using the <a href="#">System State</a> page. If there is

connectivity, please contact [Nexsan technical support](#) to verify the server clock.

## Key Manager messages

<b>Source</b>	KeyServerFileSystemManager
<b>Location</b>	DispositionTrigger
<b>Event ID</b>	876
<b>Event Type</b>	Error
<b>System Error Message</b>	Could not get code page list from key server during getAllMissingCodePage for file system: + this.fsGUID
<b>Cause</b>	An error occurred while attempting to retrieve code pages from key server. Likely, this is because the key server did not respond within the allowed period of time.
<b>Action</b>	System should automatically recover. Check the system state page for connectivity to key server, and troubleshoot the network connection if necessary. If this error message occurs again, please contact <a href="#">Nexsan technical support</a> .
<b>Source</b>	KeyServerFileSystemManager
<b>Location</b>	DispositionTrigger
<b>Event ID</b>	540
<b>Event Type</b>	Error
<b>System Error Message</b>	"Could not download codePageList from server for file system:" + this.fsGUID + "." + ex.Message
<b>Cause</b>	An error occurred getting code pages for the file system from the key server. Likely, the exception occurred either during authentication with the key server, the key server web service threw an exception while trying to connect, or the web service returned a null value.
<b>Action</b>	The system should automatically recover. Check the <a href="#">System State</a> page for connectivity to key server, and troubleshoot the network connection if necessary. If this message occurs again, please contact <a href="#">Nexsan technical support</a> .

## Key Server proxy messages

<b>Source</b>	KeySrvProxy
<b>Location</b>	AESStoreKeyService
<b>Event ID</b>	206
<b>Event Type</b>	Error
<b>System Error Message</b>	Could not get missing registered code page list. System reports: + ex.Message
<b>Cause</b>	An error occurred while attempting to retrieve code pages from key server. Likely, this is because the key server did not respond within the allowed period of time.
<b>Action</b>	The system should automatically recover. Check the <a href="#">System State</a> page for connectivity to key server, and troubleshoot the network connection if necessary. If this error message occurs again, please contact <a href="#">Nexsan technical support</a> .
<b>Source</b>	KeySrvProxy
<b>Location</b>	AESStoreKeyService
<b>Event ID</b>	304
<b>Event Type</b>	Warning
<b>System Error Message</b>	Key Server at " + ConfigInfo.KeyServiceURL + " is not responding. System reports: " + ex.Message
<b>Cause</b>	The key server did not respond to a ping within the allowed time.
<b>Action</b>	The system should automatically recover. Check the <a href="#">System State</a> page for connectivity to key server, and troubleshoot the network connection if necessary. If this message occurs again, please contact <a href="#">Nexsan technical support</a> .
<b>Source</b>	KeySrvProxy
<b>Location</b>	ConfigInfo
<b>Event ID</b>	1002
<b>Event Type</b>	Error
<b>System Error Message</b>	Cannot get key server url during proxy startup. System reports: + ex.Message
<b>Cause</b>	An error occurred as the proxy attempted to retrieve the real key server URL.

	This can happen when the proxy fails to contact the real key server due to connectivity or security issues.
<b>Action</b>	The system should automatically recover. Check the <a href="#">System State</a> page for connectivity to key server, and troubleshoot the network connection if necessary. If this message occurs again, please contact <a href="#">Nexsan technical support</a> .

## Manifest Server messages

<b>Source</b>	ManifestSrv
<b>Location</b>	ManifestTrigger
<b>Event ID</b>	1255
<b>Event Type</b>	Error
<b>System Error Message</b>	fsGUIDMessage + "could not process manifest recovery. System reports: " + ex.Message
<b>Cause</b>	An error occurred during the manifest recovery process. Likely, this happened while trying to list the files in the manifest recovery directory.
<b>Action</b>	No user action is required. The service will retry later. If this error message occurs frequently, please contact <a href="#">Nexsan technical support</a> .

<b>Source</b>	ManifestSrv
<b>Location</b>	ManifestTrigger
<b>Event ID</b>	140
<b>Event Type</b>	Error
<b>System Error Message</b>	Could not process manifest. System reports the following error. + ex.Message
<b>Cause</b>	An error occurred trying to process a local or remote manifest. Likely, the failure occurred trying to contact the database, accessing the manifest storage path, or sending the manifest to the key server.
<b>Action</b>	The system should automatically recover. Check the <a href="#">System State</a> page for connectivity between sites, and troubleshoot the network connection if necessary. If this message occurs again, please contact <a href="#">Nexsan technical support</a> .

## Object Request Broker messages

<b>Source</b>	ORBSrv
---------------	--------

<b>Location</b>	ConfigServerQuery
<b>Event ID</b>	22
<b>Event Type</b>	Warning
<b>System Error Message</b>	Failed to register for " + eventType.ToString() + " notifications. System reports: " + regex.Message
<b>Cause</b>	The ORB Server registers to be notified by the Configuration Server, if certain configuration changes occur. This registration failed, likely because the ORB Server could not contact the Configuration Server.
<b>Action</b>	Check status of the Configuration Server in SysAdmin, and start it if it is stopped. If this message occurs again, please contact <a href="#">Nexsan technical support</a> .
<b>Source</b>	ORBSrv
<b>Location</b>	ObjectRequestBrokerCommonLib.Client
<b>Event ID</b>	1
<b>Event Type</b>	Warning
<b>System Error Message</b>	The ORB client failed to connect to a host using a particular IP Address. This message is displayed only once per IP.
<b>Cause</b>	The ORB client failed to connect to a host using a particular IP Address. This message is displayed only once per IP.
<b>Action</b>	Check IP Addresses and network connectivity with the host mentioned. If there are no issues with IP addresses or connectivity, please contact <a href="#">Nexsan technical support</a> .
<b>Source</b>	ORBSrv
<b>Location</b>	OrbListener
<b>Event ID</b>	2
<b>Event Type</b>	Error
<b>System Error Message</b>	"Reading the request type from the client " + this.protocolParameters.ClientInfo.ClientIPAddress + " failed: " ***
<b>Cause</b>	A client request specified an invalid request type. The would occur if the message, method, or format is incorrect.
<b>Action</b>	The client and server may be running different versions of Assureon. Please contact <a href="#">Nexsan technical support</a> .

<b>Source</b>	ORBSrv
<b>Location</b>	ORBQueueManagement
<b>Event ID</b>	1
<b>Event Type</b>	Error
<b>System Error Message</b>	An error has occurred when sending a message.
<b>Cause</b>	The ORB Server failed to schedule a batch of files for processing.
<b>Action</b>	The system should automatically recover. If this message occurs again, please contact <a href="#">Nexsan technical support</a> .
<b>Source</b>	ORBSrv
<b>Location</b>	OrbTransferProtocol
<b>Event ID</b>	3
<b>Event Type</b>	Error
<b>System Error Message</b>	OrbListener.ERROR_MESSAGE + "An error has occurred"
<b>Cause</b>	An error occurred while transferring a batch of files from the client to the server. This can happen if the working folder is inaccessible, the metadata info is invalid, the system failed to receive a file, or the system failed to make a remoting call.
<b>Action</b>	Please contact <a href="#">Nexsan technical support</a> .
<b>Source</b>	ORBSrv
<b>Location</b>	OrbWrite
<b>Event ID</b>	5
<b>Event Type</b>	Warning
<b>System Error Message</b>	Various error messages.
<b>Cause</b>	The client failed to transfer a file to the server. Possible causes include: transfer protocol failure, files corrupted on the server, or when calling the audit server on the remote site failed because the service is not accessible.
<b>Action</b>	Check for network connectivity between the client and the server. Use the SysAdmin to check the status of all Audit Servers, and start them if they are stopped. If this message occurs again, please contact <a href="#">Nexsan technical</a>

	<a href="#">support.</a>
<b>Source</b>	ORBSrv
<b>Location</b>	ProcessRequestClient
<b>Event ID</b>	11
<b>Event Type</b>	Error
<b>System Error Message</b>	Requeueing the message in queue {0} has failed. The system reports: {1}
<b>Cause</b>	A batch of files could not be scheduled for reprocessing. This may be due to an error in the batch, or an error in the rescheduling mechanism.
<b>Action</b>	Please contact <a href="#">Nexsan technical support.</a>
<b>Source</b>	ORBSrv
<b>Location</b>	ProcessRequestClient
<b>Event ID</b>	6
<b>Event Type</b>	Warning
<b>System Error Message</b>	
<b>Cause</b>	A file transfer between a client and the server was not completed successfully. Likely, there was a network communication issue between the client and server during the transfer.
<b>Action</b>	No action is required. The message will be automatically rescheduled, and the transfer will resume. If this message occurs frequently, please contact <a href="#">Nexsan technical support.</a>
<b>Source</b>	ORBSrv
<b>Location</b>	Server
<b>Event ID</b>	25
<b>Event Type</b>	Error
<b>System Error Message</b>	The ORB will suspend sending files to the remote site {0} because the remote server is not responding.
<b>Cause</b>	The server has suspended sending files to the remote site because the remote server has not responded for a number of minutes.



<b>Action</b>	Use the system state page to ensure that the network connection with the remote site is operational. Use the SysAdmin to confirm that ORB server on the remote site is running, and start it if necessary.
---------------	--

## Storage Server messages

<b>Source</b>	StorageSrv
<b>Location</b>	StorageIOManager
<b>Event ID</b>	4502
<b>Event Type</b>	Error
<b>System Error Message</b>	Error transforming file. System will retry later.
<b>Cause</b>	The system encountered an error preparing a batch of files to be stored.
<b>Action</b>	The system will automatically retry. If this error occurs again, please contact <a href="#">Nexsan technical support</a> .

<b>Source</b>	StorageSrv
<b>Location</b>	TransformFiles
<b>Event ID</b>	801
<b>Event Type</b>	Error
<b>System Error Message</b>	"MD5 = " + md5 + "\nExisting MD5 = " + hB.MD5HashInHex + "\nFilename: " + filePath
<b>Cause</b>	An MD5 hash included in a file sent by a client was different than hash for the file received by the server. This indicates file may have been corrupted during transfer.
<b>Action</b>	If this message occurs again, please contact <a href="#">Nexsan technical support</a> .

<b>Source</b>	StorageSrv
<b>Location</b>	TransformFiles
<b>Event ID</b>	4
<b>Event Type</b>	Error
<b>System Error Message</b>	Source file " + tOut.uFIDOfWorkFile + "\n" + "was rejected because of corruption in transport.
<b>Cause</b>	File received by storage manager was corrupted. File may have been corrupted

	during transfer.
<b>Action</b>	If this occurs again, please contact <a href="#">Nexsan technical support</a> .

## Storage Web Services messages

<b>Source</b>	StorageWebServices
<b>Location</b>	TimeStampFile
<b>Event ID</b>	3
<b>Event Type</b>	Error
<b>System Error Message</b>	Time-Stamp server is down or not responding after {0} attempts. System reports: " + socketException.Message
<b>Cause</b>	There was a problem opening a connection to the Time Stamp Server.
<b>Action</b>	Check status of Time Stamp Server in the SysAdmin, and start it if it is stopped. If this error occurs again, please contact <a href="#">Nexsan technical support</a> .

## Restore Server messages

<b>Source</b>	RestoreSrv
<b>Location</b>	RestoreServerControl
<b>Event ID</b>	0
<b>Event Type</b>	Warning
<b>System Error Message</b>	Failed to show service startup message.\n\nSystem reports: + ex.Message
<b>Cause</b>	The restore server failed to show the startup message.
<b>Action</b>	Use the SysAdmin to check the status of the Restore Server. If server has started normally, this message can be disregarded. Otherwise, please contact <a href="#">Nexsan technical support</a> .

# Glossary

---

## A

### Active Directory

Microsoft Active Directory® is a directory service that stores directory information about a network and makes this information available to network users and administrators. AD stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information

### ADAM

(Active Directory Application Mode) security model. ADAM allows customers who do not have a trusted relationship between their corporate server and the Assureon server to manage user security.

### ASP model

Application Service Provider. In this model more than one organization is defined.

## B

### Bit

The smallest unit of digital data, representing a 0 or a 1. Abbreviated “b”.

## D

### Digital certificate

Used to grant certain users access to specific files over the internet. Use of certificates increases security for customers who do not have a corporate Active Directory.

### Disposition

The deletion of a file based on retention rules.

### DNS name

Domain Name System. Translates the domain name of the device to point to the configured IP address.

## E

### Event log

A record of system events that tracks informational, warning, and error events, such as when significant milestones are reached or when errors occur during activity.

## F

### Failover

The capability of a system to switch over automatically to a redundant or standby system upon the failure or abnormal termination of the previously active system. In Nexsan NST

appliances, failover describes one Controller Node taking over the host connections and storage pool control of the other Controller Node when that controller fails.

#### File System

An archive consisting of a database, storage location (the stores), manifest and audit files as well as replication options.

#### Filter Driver

Responsible for processing shortcut requests and making the shortcut appear transparent to the user or application attempting to read the data.

#### FSW

File System Watcher. Responsible for transferring data from the client to the server, as well as shortcutting data. Also known as Assureon Client Services.

#### FSW Monitor

Ensures that all clients are running properly. Also provides information to the server about the client and tells the FSW to update.

## G

#### Gb

Gigabit. Approximately one billion (1,000,000,000) bits.

## I

#### IIS

Internet Information Services. IIS is a web server software package.

#### ILM

Information Lifecycle Management. Refers to a range of policies and strategies for administering storage systems. Typically used to represent a storage solution that manages the file from its creation to disposition.

#### Ingestion

Synonymous with archiving. It is the process of moving data from the client to the server.

#### IP

(Internet Protocol) The network layer for the TCP/IP protocol suite widely used on Ethernet networks.

#### IP address

Internet Protocol address. A numerical label assigned to each device (such as a computer, printer, or Nexsan storage unit) on a computer network that uses TCP/IP for communication.

## M

#### Mb

Megabit. Approximately one million (1,000,000) bits.

## N

#### Network-attached storage (NAS)

File-level computer data storage connected to a computer network providing data access to clients on the network. Network-attached storage uses specialized hardware, software, or both, and is often a specialized device built from the ground up for storing and serving files.

#### NFS

Network File System. A protocol allowing a user on a client computer to access files over a network in a manner similar to how local storage is accessed. Used in most UNIX environments for folder or device sharing.

#### NTFS

New Technology File System. Developed by Microsoft, NTFS includes features that improve reliability such as automatically repairing hard drive errors, detailed transaction logs, and fault tolerance.

**O****Organization**

A group of Assureon file systems. Although an organization can have multiple file systems, only one is used to store files at a given time. This file system is designated as active. All other file systems are considered passive, but may be used to retrieve or query files.

**P****Pool**

A storage pool is a user-defined virtual grouping of volumes. Pools allow you to organize your storage into logical groups; expose file systems as shares to CIFS clients (Windows-based systems) and NFS clients (UNIX/Linux-based systems); and replicate all the data in the pool, or just a subset of it, for disaster recovery.

**Q****Queues**

A data structure that processes data or messages in a first in/first out order (FIFO). Typically, a queue is used to process data asynchronously.

**R****Reparse point**

An attribute of a file. It is used by NTFS to determine how to open the file.

**Replication**

A function of Nexsan Assureon that copies data to a secondary site to protect data in the event of a disaster. Assureon performs synchronous mirroring so that both sites always have the same content.

**Rollover**

An Assureon file system process that optimizes when a new file system should be used

without administrator intervention.

**S****SATA**

Serial Advanced Technology Attachment. A connection standard for fixed and removable hard disk drives.

**Server**

A computer system in a network that provides data to be shared with multiple users.

**SMTP**

Simple Mail Transfer Protocol. Used by a client (e.g. Outlook) to relay messages to the receiving mail server.

**SSL**

(Secure Sockets Layer) A commonly used protocol for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. The SSL protocol secures the following data: I/O, serial port, and VSIP communication; it does not apply to audio and video transmission.

**T****TCP/IP**

Transmission Control Protocol/Internet Protocol. The set of communications protocols used for the Internet and other similar networks. TCP provides reliable delivery of messages between networked computers. IP uses numeric IP addresses to join network segments.

**U****UNC paths**

Universal Naming Convention. A file name format that is used to identify the location of folders, files and other resources on a local-area network (LAN). A UNC path uses backslashes

or double slashes preceding the name of the computer.

## V

### Virtual Directory

There is an xml fragment representing the asset that is stored at the end of the asset itself.

### Volume

A volume represents a virtual subset of the aggregated disk space available.

## W

### WAN

(Wide Area Network) A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs).

### Watch

A rule that monitors changes to files based on folders, organization, and retention rules, updating the file system (archive) as required.

### Windows Service

An application that runs whenever the server is turned on, regardless of whether a user is logged in or not. Accessed by launching "services.msc".

# Index

---

## A

- Access control 53
- Access Log 56
- Accessing the administration console 20
- Active Directory Application Mode 164
- Active directory security groups 20
- ADAM 164
- ADAM instance 164
- ADAM security model 164
- Adding a retention policy 58
- Adding a retention rule 58
- Administration console 20
- Alerts 83
- Allow read access 54
- Archive bit 66, 140
- Archive Folders 61, 126, 128
- Asset protection 174
- Asset synchronization 138, 148
- Asset transfers 128
- Assets, restoring 135
- Assureon back up 174
- Assureon Explorer 135
- Assureon Property Sheet 128
- Assureon security groups 20
- Assureon services 68
- Attributes, file 129
- Audit all active file systems 99
- Audit all inactive file systems 99
- Audit all organizations and file systems 99
- Audit Assets; Asset Audit 99
- Audit Database Records; Database records audit 99
- Audit Log 96, 101
- Audit Meta Data; Meta Data Audit 99
- Audit schedule 99
- Authentication 127, 154

## B

- Back up 174
- Back ups 176
- Backing up 174, 176
- Backup software 174
- Backups 176

## C

- CA 154
- Cancel a disposition 89
- Certificate mapping 114
- Certificate serial number 115
- Certificates 115, 127, 154
- Certification Authority 154
- Change journal 66, 127, 140, 149
- Clearing a disposition list 91
- Clearing a manifest 91
- Client certificate 127
- Client Service 61, 75, 124
- Client Service for Laptops 124, 126, 128
- Client Service taskbar icon 126
- Client Synchronization Wizard 66
- Clustered NAS 175
- Clustering 175
- Command line 136, 148
- Compression 58
- Configuration file 150
- Configuring a watch 128
- Console access 20
- Console security 20
- Content search 76
- Copyright ii
- Corrective action 96, 102
- CPU use 40
- Create an archive folder 126
- Creating an archive folder 128

Critical updates 167  
Cryptographic disposition delay 94  
Customize organizations and file systems to  
audit 99

## D

Data Migration Wizard 176  
Database information 104  
Database Management 115  
Delayed processing 137  
Deleting extra file versions 94  
Directories 61  
Disaster recovery 175  
Disk space management 126  
Disk use 40  
Dispose now 92  
Disposing of expired files 89  
Disposing of extra versions 94  
Disposition 89, 93  
Disposition manifest 89  
Disposition selection 89  
Disposition selections 91  
Disposition version control 95  
DispositionMgr 178  
DMW 176  
DNS 114

## E

Editing a configuration 70  
Editing a template 70  
Email alerts 83  
Email archiving 130  
Email Events 83  
Email notification 112, 128  
Emailing reports 143  
Enabling the Filter Driver 126  
Encrypted file transfer 128  
Encryption 58  
Enterprise Vault 162  
Error messages 82, 177  
errors 177  
EV 162  
Event filters 83  
Event history 82  
Event Log 82  
Event log detail 83  
Event management 82  
Event Viewer 83  
Events 82, 177  
Exceptions 166  
Excess file versions 94  
Exclude files 74  
Expired files 89  
Explorer 134-135

Explorer command line 136  
Extended characters 166

## F

File attributes 130  
File compression 58  
File disposition 19  
File encryption 58  
File flags 129  
File integrity check 96, 101  
File sharing 168  
File Sync email 126  
File Sync Request Watcher 150  
File synchronization 138, 148-149  
File Synchronization report 143  
File Synchronization utility 137  
File System Audit 99  
File system backup 176  
File System Editor 104  
File systems 16, 104  
File transfers 128  
File versions 94-95  
Filename support 166  
Files processed 25, 36  
Files stored 40  
Files, restoring 135  
Filter Driver 126, 130, 168  
Firewall 166  
Folder security 176  
Foreign characters 166  
fswConfig.xml 150  
Full sync 66, 140

## I

Ignore files 70  
IIS reset 114  
IIS security 114  
ILM security groups 20  
Immediate disposition 91  
Include subdirectories 70  
Incomplete transactions 102  
Information messages 82  
Installing a client certificate 154  
Installing a server certificate 154  
Installing ADAM 164  
Installing the Client Service 124  
Installing the filter driver 130  
Integration with Enterprise Vault 162  
Integration with EV 162  
Integrity check 96, 101



**J**

Job management 115  
Jobs, SQL 115  
Journal folder 127

**K**

KeyServerFileSystemManager 179  
KeySrvProxy 180

**L**

Laptop 126, 128  
Laptops 124  
Log files 143  
Logs 56, 82, 96, 101

**M**

Mac character support 166  
Managing File Systems 104  
Managing Organizations 104  
Manifest 89, 91  
ManifestSrv 181  
Manual Audit Configuration Wizard 99  
Mapping certificates 114  
Maximum number of versions 95  
messages 177-181, 185-186  
Meta data protection 174  
Microsoft SQL Server 115  
Microsoft SQL Server Transaction Log Shipping 175  
Migrating 176  
Monitoring Assureon 40  
Monitoring CPU use 40  
Monitoring directories 61  
Monitoring disk space 126  
Monitoring disk use 40  
Monitoring services 68

**N**

NAS servers 175  
Network File System Access 168  
Network share 168  
NFS access 168  
Notification icon 126  
NTFS 176  
Number of files stored 40

**O**

Offline 130  
Open ports 167  
ORBSrv 181  
Organizations 16, 104  
OS updates 167  
Override read control 53

**P**

Plus configuration 167  
Policy options 70  
Policy rules 58  
Ports 166  
Process Remote Audits 99  
Processing a configuration file 150  
Processing after a delay in time 137  
Property Sheet 128

**Q**

Queue use 36

**R**

Read a file 135  
Read access 53  
Read control override 53  
Reading files from site 2 167  
Real-time folder security 176  
Reboot order 174  
Rebooting 174  
Rebuilding 176  
Rebuilding a site 176  
Recovery 174  
Reparse point 130  
Report, synchronization 143  
Reporting 143  
Request Watcher 150  
Resolving shortcuts 130  
Restarting Assureon 174  
Restarting servers 174  
Restarting the Client Service 126  
Restore a file 135  
Restore options 135  
RestoreSrv 186  
Restoring a site 176  
Restoring files 135-136  
Restoring shortcuts 136  
Retention period 59  
Retention rules 58, 76

Retrieve file 56, 134  
Retrieving a file 134  
Rule name 59  
Rules 58  
Running out of disk space 126

## S

SATA 117  
Save disposition manifest 89  
Scheduled Task Wizard 136, 149  
Scheduling a backup 148  
Scheduling dispositions 93  
Search Engine 76  
Search using content 76  
Searching 76  
Secure asset transfers 128  
Secure file transfers 128  
Security 20  
Security certificates 115, 126  
Security groups 20  
Security model 176  
Selection list 91  
Server updates 167  
Services 68  
Services Management 68  
Shares 126  
Sharing 168  
Shortcut 129  
Shortcut management 127  
Shortcut Manager 127  
Shortcuts 130  
Shortcutting files 126  
Shutting down Assureon 174  
Signed files 128  
Site backups 176  
Site rebuilding 176  
Sites 105  
Solaris 168  
Sparse file 129  
Sparse file attributes 129  
Special characters 166  
SQL Database 115  
SQL Server 68  
SSL 115  
Starting services 68  
Starting the Client Service 126  
Starting the Filter Driver 126  
State 40  
Statistics 35  
Stopping services 68  
Stopping the Filter Driver 126  
Storage devices 117  
Storage information 104  
Storage options 70  
StorageSrv 185  
StorageWebServices 186  
Store data protection 174

Store information 104  
Subdirectories 75  
Summary information 66  
Symantec Enterprise Vault 162  
Symantec EV 162  
Sync 149  
Sync folder security 176  
Sync report 143  
Synchronization 149  
Synchronization report 143  
Synchronization Type 66  
Synchronization utility 137  
Synchronizing 138, 148  
Synchronizing time 175  
System administration security 20  
system events 177  
System health 40  
System integrity 96, 101  
System message 186  
system messages 177-181, 185-186  
System recovery 174  
System statistics 40  
System updates 167

## T

Taskbar icon 126  
Technical reports 49  
Template 62  
Template configuration 70  
Time 175  
Time synchronization 175  
Trademarks ii  
Transaction log 102  
Transaction log shipping 175  
Transferring files 128

## U

Updating DNS 114  
Upgrading 176  
Using certificates for authentication 154  
Using EV 162  
Using Symantec 162

## V

Version 95  
Version control 95  
Versions of a file 94  
Viewing errors 82  
Viewing log files 143  
Viewing SATA devices 117  
Virtual directory 114

**W**

- warning messages 177
- Warnings 82, 177
- Watch Variables 77
- Watches 16
- Web services 68
- When server goes down 174
- Windows Change Journal 127
- Windows Explorer 130
- Windows Firewall 166
- Windows Network Load Balancing 175
- Windows scheduled task 136
- Windows shares 126
- Windows taskbar 126
- Windows updates 167
- WSUS service 167



#### **Nexsan Headquarters**

325 E. Hillcrest Drive, Suite #150  
Thousand Oaks, CA 91360 USA

#### **Nexsan Shipping**

302 Enterprise Street , Suite A  
Escondido, CA 92029 USA

Copyright © 2010—2019 Nexsan Technologies, Inc.. All rights reserved.

Nexsan® is a trademark or registered trademark of Nexsan Technologies, Inc..

The Nexsan logo is a registered trademark of Nexsan Technologies, Inc..

All other trademarks and registered trademarks are the property of their respective owners.

Document Reference: 20200127PM043148

#### **Nexsan Canada**

1405 Trans Canada Highway, Suite 300  
Dorval, QC H9P 2V9 Canada

#### **Nexsan UK**

Units 33–35, Parker Centre, Mansfield Road  
Derby, DE21 4SZ United Kingdom

This product is protected by one or more of the following patents, and other pending patent applications worldwide:

United States patents US8,191,841, US8,120,922;

United Kingdom patents GB2466535B, GB2467622B, GB2467404B,  
GB2296798B, GB2297636B

Firmware version: Version 8.3