# ASG-Live Navigator™
# User Guide

Version 3.1.2
Publication Number: ATL0200-312
Publication Date: June 2013

# Worldwide Customer Support

ASG provides support throughout the world to resolve questions or problems regarding installation, operation, or use of our products. ASG provides all levels of support during normal business hours and emergency support during non-business hours.

You can access support information at http://www.asg.com/support/support.asp.

**ASG Third-party Support.** ASG provides software products that run in a number of third-party vendor environments. Support for all non-ASG products is the responsibility of the respective vendor. In the event a vendor discontinues support for a hardware and/or software product, ASG cannot be held responsible for problems arising from the use of that unsupported version.

# Intelligent Support Portal (ISP)

The ASG Intelligent Support Portal (ISP) provides online support at http://isp.asg.com.

Log on to the ISP with this information:

Customer ID = *NNNNNNNNN*

Password = *XXXXXXXXXX*

where:

*NNNNNNNNN* is your customer ID supplied by ASG Product Distribution.

*XXXXXXXXXX* is your unique password supplied by ASG Product Distribution.

If you do not have your logon information, contact your local support center.

This table outlines the support response times you can expect:

| Severity | Meaning | Expected Support Response Time |
|---|---|---|
| 1 | Production down, critical situation | Within 30 minutes |
| 2 | Major component of product disabled | Within 2 hours |
| 3 | Problem with the product, but customer has work-around solution | Within 4 hours |
| 4 | "How-to" questions and enhancement requests | Within 4 hours |

# Product Support Policy

ASG fully supports the current release and one previous release of each of its products. ASG will temporarily support an older release, for up to six months, to provide time for you to upgrade.

Once programming support for a product release is withdrawn, ASG will no longer supply new fixes for problems nor accept enhancement requests for that release. When a vendor announces the end of support for system software or a hardware configuration on which ASG products rely, ASG will make a similar announcement regarding the support plans for its products. ASG's support for problems affected by system software release levels will terminate when the vendor no longer supports their hardware or software. Announcements regarding support plans for various products can be found on ASG's Web site.

Support for Field-developed Interfaces (FDIs) developed by ASG's Professional Services staff is described in *ASG Professional Services FDI Support Guide* that can be found on the ASG Support Web site in the Guide to Support section. This document describes how FDIs are supported by ASG Customer Support and ASG Worldwide Professional Services.

# ASG Documentation/Product Enhancements

Submit all product and documentation suggestions to ASG's product management team at http://www.asg.com/asp/emailproductsuggestions.asp.

Include your name, company, work phone, e-mail ID, and the name of the ASG product you are using. For documentation suggestions, include the publication number located on the publication's front cover.

## Atempo Copyrights

# Table of Contents

# Appendix A: Installing Live Navigator Agents . . . . . . . . . . . . . . . 37

# Appendix B: Glossary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 53

C H A P T E R   1

# Presenting Live Navigator

**1**

**Live Navigator** is a solution for the protection of file servers, laptops and workstations using a client/server architecture: a **Live Navigator** server protecting **Live Navigator** agents in a network.

# Features

| Feature | Description |
|---------|-------------|
| Continuous Data Protection and Flexible Recovery Point Objective | **Live Navigator** offers automatic and near continuous protection of user data. In contrast with traditional backup, there is no backup scheduling: instead, new or modified data is detected in real time and automatically transferred to the **Live Navigator** server, without user intervention. The time-intervals between transfers of data to protect is defined by the Recovery Point Objective (RPO). The RPO can vary from one minute to one day. |
| Block Level Deduplication | **Live Navigator** implements incremental backup and deduplication technology at block level. Network traffic is reduced since already protected blocks are not re-sent to the server. |
| "Self Service" Restore of Agent Data | A Restore Wizard lets the user restore files or directories at any time without administrator intervention. Data can be restored to its original place or to a new location.<br>Advanced Restore also allows to perform cross and distant restore, and restore from an alternate server. |
| Versioning | **Live Navigator** keeps historical logs of protected versions, letting you choose the protection date or version of the file or folder to restore. |
| Support of Open Files | For continuous protection of user data, **Live Navigator** protects open files. Applications such as Microsoft Outlook and Microsoft Office do not need to be closed, their files are protected while in use. |

| Feature | Description |
|---------|-------------|
| Support of Windows EFS | EFS (Encrypting File Systems) encrypt data on a machine to ensure its confidentiality. When **Live Navigator** protects the data on an EFS system, it is protected and restored in its encrypted form. |
| Network Management | **Live Navigator** agents automatically connect to the server as soon as a network connection is available.<br>**Live Navigator** lets you fine-tune data protection by defining, among other things, the behavior to adopt for different types of network, or the compression algorithm for data transfer. |
| Centralized Handling of the Server, Free Configuration of the Agent | Administrators of the **Live Navigator** server can oversee the entire IT environment of the company (file servers, workstations and laptops), applying common protection policies to groups of machines via a centralized Administration Console. They can define enterprise-wide protection policies such as exclusions and inclusions, and rights for **Live Navigator** agents. On the agents, users are free to set up their own protection policies, as allowed by their rights, as long as their customized policies do not conflict with the protection rules defined on the server. |

# Live Navigator Architecture and Components

## Live Navigator in a Stand Alone Configuration
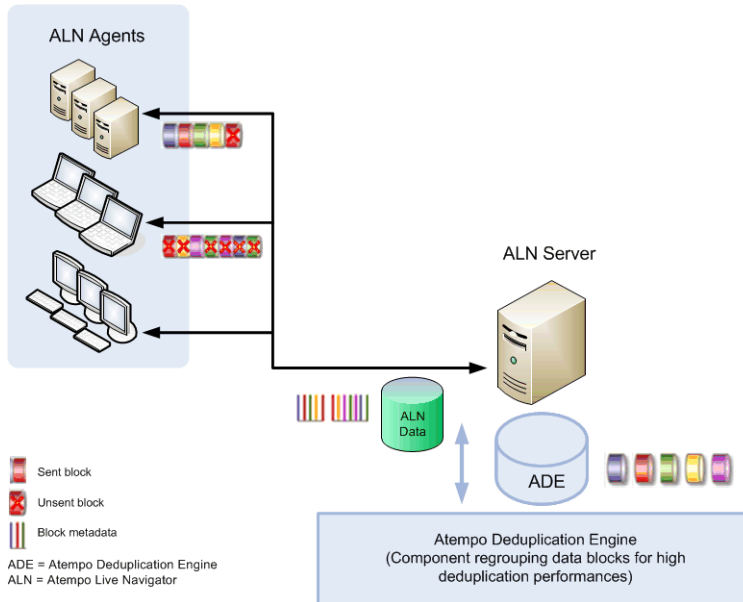


### The Live Navigator Server

- Stores protected data from the **Live Navigator** agents according to protection policies defined by the administrator and the user.

- Relies on the **ASG Deduplication Engine** (ADE) to store all the unique data blocks sent by the agents. The ADE database keeps track of all the data blocks stored, and the repository where data is actually stored.

### The Live Navigator Agent

- Detects new and modified data.

- Applies protection policies set on the server side by the administrator and on the agent side by the user.

- Sends unique blocks of protected data to the **Live Navigator** Server, according to the protection policies.

- Provides restore capability, via a restore wizard or Windows Explorer.

## Live Navigator with Hyperstream and Time Navigator
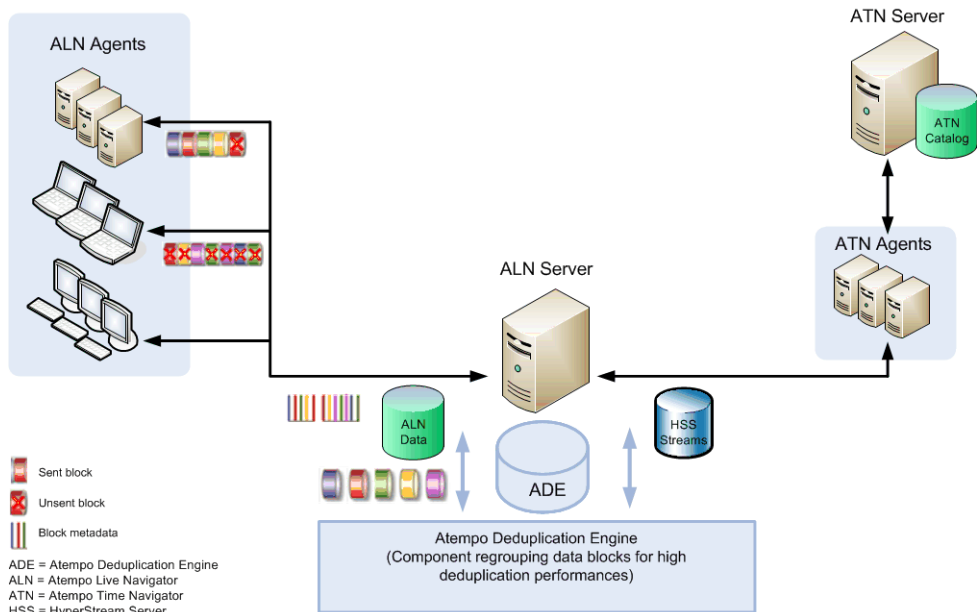


- **Live Navigator** and **HyperStream Server** share a common **ASG Deduplication Engine** and Administration Console for optimized integration.

- The integration with **Time Navigator** offers a complete protection solution for all your data.

# How does Live Navigator Work?

**Live Navigator** uses protection policies to determine what data to protect and how:

- Protection policies are defined on the server or on the agent.

- Data to protect is defined through **Protection Schemes**.

- Protection parameters are defined through **Strategies**.

## Defining Protection on the Server or the Agent

Protection policies can be defined at two levels:

- On the **Live Navigator** server, managed by the administrator. Defining policies on

the server is particularly useful if you have a large IT environment to manage, and if the location and type of data to protect is similar for groups of machines. The configuration is done only once on the server and applies to all the machines designated by the administrator.

■    On the **Live Navigator** agents, managed by the user. Defining policies on the agent allows the user some freedom in the choice of data to protect on his or her own machine. Policy definition on the agent is only possible if the administrator authorizes it.

Protection policies applied to the agents are a combination of administrator and user policies. Protection policies defined by the administrator on the **Live Navigator** Server take precedence over those defined by users on the **Live Navigator** agents.

# Defining Data to Protect

**Protection Schemes** define data to protect by supplying the following information:

■    The location of data to protect, in the form of a list of paths.

■    The type of files to protect, in the form of Protection Rules associating a category of files with an action. The action can be either inclusion or exclusion from protection.

### Principle for Creating a Protection Scheme:
According to the files you want to protect or exclude, you must define paths on which the Protection Rules can be applied, as illustrated below:



**Step 1**: Divide the computer in paths
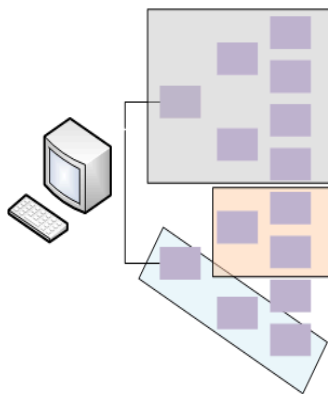
**Step 2**: Apply protection rules to the paths

Protection rule A:
• Include Office files
• Exclude multimedia files

Protection rule B:
• Exclude system files
• Include all other file types

Protection rule C:
• Include mail files
• Exclude all other file types
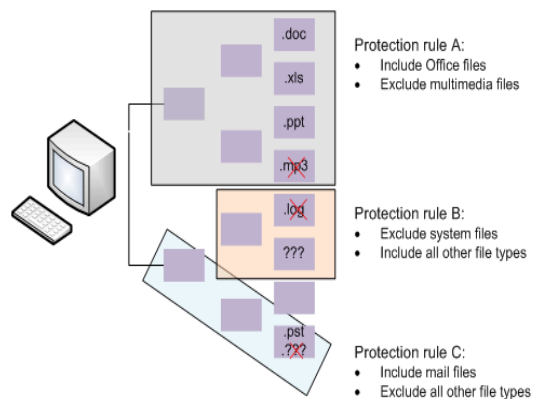
**Details of a Protection Scheme:**

To allow for the great variety of user environments and give the administrator flexibility for configuring protection, Protection Schemes are structured in the following manner:
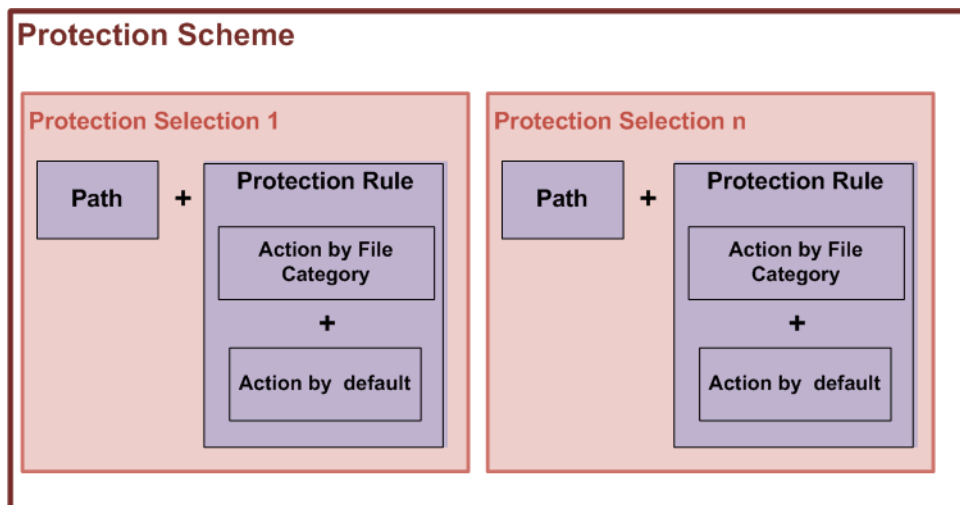


- A **Protection Scheme** is composed of a group of **Protection Selections**.

- Each Protection Selection contains a **path** associated with a Protection Rule.

- The **Protection Rule** includes a list of **File Categories** associated with **Actions**. It also necessarily includes a default action, to indicate what to do with file types not explicitly specified in a category.

- Action can either be **Include** or **Exclude** from protection. In addition you can decide whether the action is overwritable by the agent or not.

- The items that you can define freely are the paths and the file categories. The Protection Schemes, Selections and Rules are made up of existing elements.

## Unprotected Data

- **Live Navigator** own working files are always excluded from protection.

- Files and directories on network drives are not supported by **Live Navigator**.

## Defining Protection Parameters

After defining the data to protect in a Protection Scheme, the administrator must set up a **Strategy**. The Strategy contains the following protection parameters:

- **Retention Period**: how long the data must be stored

- **Rights**: is the user be authorized to modify his or her own protection parameters

- **Recovery Point Objective**: at what moment the data will be protected

- **Network**: data transfer mode, compression, encryption, etc.

If the administrator gives the user the possibility of choosing his or her own protection options, he/she can define retention, rights, Recovery Point Objective and Network.

C H A P T E R   2

# Configuring Protection on a Live Navigator Agent

**2**

Your administrator has already defined some policies that apply to all the agents in your network. You can also, if the administrator lets you and if you have the necessary rights, define your own protection policy.

Make sure that your customized policy does not conflict with the rules defined by your administrator on the server. If that is the case, the server rules take precedence. A validation is performed to indicate when the agent configuration is incompatible with the rules defined on the server.

---

Warning :     If you define your own protection policy and the administrator subsequently decides to terminate that right for users, your customized protection configuration will be lost.

---

# Including/Excluding Files and Directories

**To define protection on a file or directory**

1.    Right click on the **Live Navigator** agent icon in the taskbar and choose Settings.

---

Tip :         You can also run Start - All Programs - Live Navigator - Settings.

---

2.    Under the Data Protection tab, click on Folders and Files. The list of protections appears.

3.    Click on the + button. A file explorer appears.

4.    Select the file or directory and click on Open. The selected object is added to the list.

5.    In the Action column, select the action that you want to apply to this object in the pull-down list: Include or Exclude.

6.    In the Check column, the **Live Navigator** agent displays whether or not the protection is compatible with the rules defined on the **Live Navigator** server.

**Check Statuses**

| Status | Description |
|---|---|
| OK | The protection defined is compatible with the protection policies set on the **Live Navigator** server. |
| Server rules | The protection defined is incompatible with the protection policies set on the **Live Navigator** server, and the server rules prevail. |
| No effect | The protection defined is already in effect in the protection policies set on the **Live Navigator** server. |
| Syntax error | The path syntax is incorrect. You must check it. |
| Conflict | Two contradictory actions are defined for the same object. For example, you have chosen to exclude and include the same file in the same directory. |
| Unsupported | You have specified a path on a network drive. Files and directories on network drives are not supported by **Live Navigator**. |

7.    Click on OK to confirm the creation of your protection.

# Defining Files to Ignore

You can specify the file patterns to exclude from protection to the **Live Navigator** agent.

## Case of an Explicitly Protected File

If you previously explicitly defined protection on a file having an extension which you now exclude from protection, the file will in any case continue to be protected.

*Example*    A file movie001.avi is found in the directory D:\Movie Files containing only files with the extension "avi".

If:

- In the procedure "To define protection on a file or directory", page 9, you explicitly decided to protect the file
D:\Movie Files\movie001.avi

And if:

- You decide to exclude all files with the extension "avi" in the directory D:\Movie Files,

Then only the file movie001.avi in this directory will be protected.

### To exclude File Patterns from Protection

1. Right-click on the **Live Navigator** icon in the taskbar and choose Settings.

2. Under the Data Protection tab, click on Discardable Files. The list of patterns appears.

3. Click on the + button and enter the pattern for the file to exclude. For example:

   - *.avi to exclude all files with the extension "avi"

   - ~* to exclude all files beginning with " ~ "

   - SOFTWARE.LOG to exclude the "software.log" files in any protected directory.

4. The Check column shows whether the **Live Navigator** agent validates the syntax you entered. See "Check Statuses", page 10.

5. Click on OK to confirm the creation of your exclusion.

# Managing Volumes

You can view the volumes existing on your agent, whether they are protected or not, and for removable disk, enable or disable their protection. Only the removable disks supported by **Live Navigator** appear in the list. Currently, only USB disks are supported (see "Protecting Removable disks", page 13).

# Displaying the List of Protected Volumes

### To display the agent Volumes

1. Right-click on the **Live Navigator** icon in the taskbar and choose Settings.

2. Under the Data Protection tab, click on Volumes.

3.    In the Current Volumes tab, you see the list of the detected volumes. The following information is displayed:

| Parameter | Description |
| --- | --- |
| Support | The icon in this column is a green checkmark if the volume is supported and empty if it is not. |
| Protected | The checkmark in the Protected colum indicates that the volume is currently protected by **Live Navigator**. |
| Mount Path | Letter of the volume on Windows. |
| Name | Name of the volume. |
| Identifier | Identifier of the volume. |
| Display only supported volumes | Check/Uncheck this box to show only the volumes supported by **Live Navigator**, or to show all volumes. |
| Path | **This field appears only if multiple mount points are detected for a volume**. It indicates the mount points. |
| Reference Path | **This field appears only if multiple mount points are detected for a volume.** The reference path indicates the actual path taken into account to apply the protection scheme parameters, to decide what to protect on the volume. |

4.    In the Optional Volumes tab, you see the list of the offline volumes that are currently connected or have been protected at some point in the past. The following information is displayed:

| Parameter | Description |
| --- | --- |
| Activated | The icon in this column is a green checkmark if the volume is activated and empty if it is not. A volume that has already been protected is activated. |
| Name | Name of the volume. |
| Identifier | Identifier of the volume. |

5.    Click on Close to exit.

# Protecting Removable disks

### To protect a removable disk

1.    Connect the removable disk to the agent.

2.    Right-click on the **Live Navigator** icon in the taskbar and choose Settings.

3.    Under the Data Protection tab, click on Volumes.

4.    In the Current Volumes tab, check the option Protected for the removable disk.

The disk is now protected according to the Protection Scheme that applies to it.

## Protected vs. Activated

When you protect a removable disk, it is automatically activated. When you stop protecting your removable disk, namely when the disk is not connected to your agent, protection is suspended, but the disk remains activated. This guarantees that the next time the disk is connected to the agent, protection will resume.

### To stop protecting a removable disk

When you want to eject the removable disk while the **Live Navigator** protection is set, you must manually stop the protection.

1.    Right-click on the **Live Navigator** icon in the taskbar and choose Settings.

2.    Under the Data Protection tab, click on Volumes.

3.    In the Current Volumes tab, uncheck the option Protected for the removable disk.

On the other hand, when you deactivate a removable disk, not only is the volume no longer protected, but it will not be protected if it is reconnected to the agent at a later date. You will have to enable it as a new volume which will trigger a complete scan of the volume.

In addition, as soon as a volume is deactivated, the data retention starts, and data is deleted once the retention period is over.

### To deactivate a removable disk

1.    Right-click on the **Live Navigator** icon in the taskbar and choose Settings.

2.    Under the Data Protection tab, click on Volumes.

3.    In the Optional Volumes tab, uncheck the option Activated for the removable disk.

## Mac OS X Volumes

### Supported Volumes

- All HFS+ volumes are supported, whether internal disks, USB disks, FireWire disks, or Apple Disk Images.

- Network drives are not supported.

### Optional Volumes

All volumes but the system volumes are optional. To protect optional volumes:

1. Open Settings-Data Protection-Volumes-Current Volumes.

2. Select the checkbox in front of all the volumes you want to protect.

3. Close the Settings windows.

# Consulting the Server Rules

You can consult the rules set on the **Live Navigator** server which apply to your agent. This can be useful when you define protection on files and directories or exclude certain patterns.

### To consult the Server Rules

1. Right-click on the **Live Navigator** icon in the taskbar and choose Settings.

2. Under the Data Protection tab, click on Server rules. The list of Server rules appears.

3. Click on Close to exit.

## Understanding Server Rules

Sever rules are displayed in a tree structure, as in the example below:
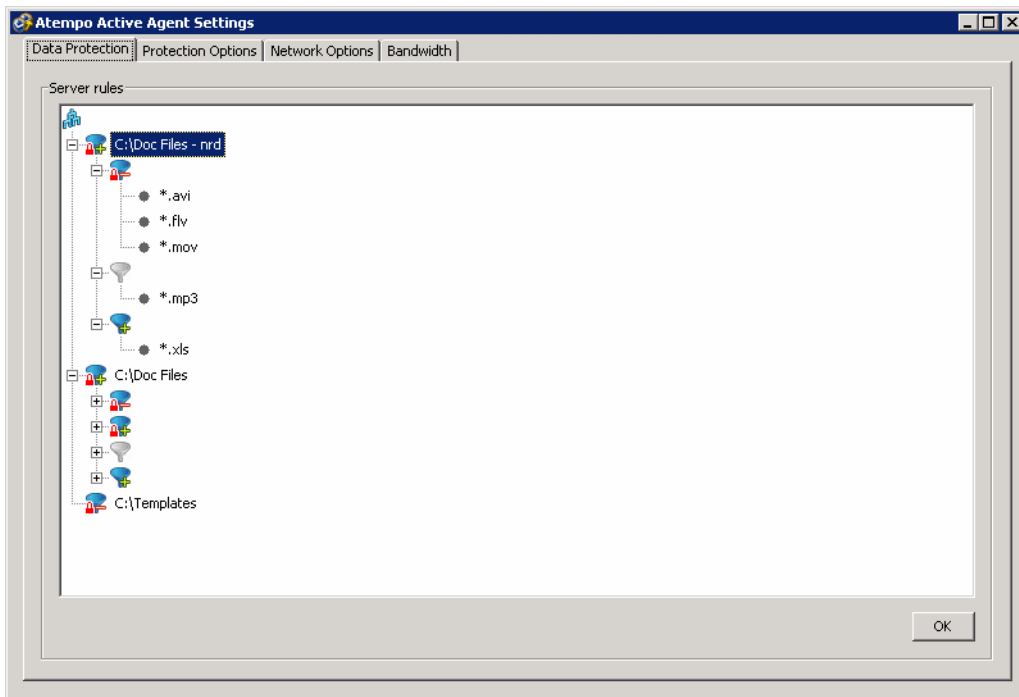


This tree structure comprises the following elements, all of which have been defined at server level:

- A list of paths. In our example, there are three paths:

  - `C:\Doc Files - nrd`

  - `C:\Doc Files`

  - `C:\Templates`

- Each path submits to a default action that may have exceptions. This default action is symbolized by an icon at the root of the path.

| Icon | Description |
|------|-------------|
|  | Include, cannot be modified: The objects are protected, and the user has no choice in the matter.. |
|  | Exclude, cannot be modified: The objects are not protected, and the user has no choice in the matter. |

| Icon | Description |
|------|-------------|
|  | **Include, can be modified:** The objects are protected unless the user decides otherwise. In that case, the user specifies the objects to include or exclude from protection, directly on his or her own machine. |
|  | **None, user defined:** The objects are not protected unless the user decides otherwise. |

In our example:

- `C:\Doc Files - nrd:` Include, cannot be modified
- `C:\Doc Files:` Include, cannot be modified
- `C:\Templates:` Exclude, cannot be modified

- An action which is not the default and which applies to a list of file extensions. In our example, for `C:\Doc Files - nrd` :

  - Exclude, cannot be modified: `*.avi, *.flv, *.mov`
  - Include, cannot be modified: `*. doc, *.docx`
  - Include, can be modified: `*.xls`
  - None, user defined: `*.mp3`

# Configuring Protection Behavior

Under the Protection Options tab, you can configure the general behavior of data protection on your **Live Navigator** agent, as well as the transfer of this data onto the **Live Navigator** server.

### Configuring the General Behavior of Protection

1. Right-click on the **Live Navigator** icon in the taskbar and select Settings.

2. Select the Protection Options tab to display the following settings:

| Setting | Description |
|---------|-------------|
| Pause protection | Lets you manually suspend or resume data protection on your **Live Navigator** agent. When the protection is paused, modifications on data are still monitored by the agent in the background. When protection is resumed, they will be transferred to the server. |

| Setting | Description |
| --- | --- |
| Boost mode | Lets your **Live Navigator** agent temporarily accelerate data protection. This can be useful if your agent is not connected to the **Live Navigator** server for a certain time and you need to protect data fast.<br>This mode should not be activated permanently because it draws very heavily on agent resources. |
| Recovery Point Objective | Defines the maximum time interval between two protection sessions, in other words the maximum admissible data loss if data is restored between the sessions.<br>**Note**: If the protection configuration is modified on the server or on the agent, protection is relaunched immediately, without waiting for the time specified in the Recovery Point Objective. |

# Configuring Network Options

From the Network Options tab, you can configure options relating to your network connection and encryption.

### Configuring Network Options

1.  Right-click the **Live Navigator** icon in the taskbar and select Settings.

2.  Select the Network Options tab to display the following settings:

| Settings | Description |
| --- | --- |
| Always connect to server | Lets your **Live Navigator** agent remain connected to the server through the network, whatever gateway or network interface is being used.<br>The gateway identification is performed as follows: first, we search if there is a gateway defined between the agent and the server. If not, we use the default gateway. |

| Settings | Description |
|---|---|
| Connect only when: | Lets you connect to the **Live Navigator** server through a network interface and gateway that you can define manually.<br>For the network interface, you can choose between:<br><br>■ Any<br><br>■ Wifi<br><br>■ Ethernet<br><br>■ VPN<br><br>■ Loopback<br><br>Then enter the name of your gateway and click on Apply. You can use the character * in the definition of the gateway name, and enter several gateways separated by a comma. |
| Always encrypt network | Permits activation of encryption on protected data during its transfer to the **Live Navigator** server. |
| Do not encrypt when gateway is: | Lets you enter the name of a gateway on which data encryption should not be activated. Once the gateway name is entered, click on Apply. You can use the character * in the definition of the gateway name, and enter several gateways separated by a comma. |

Here are two examples illustrating the possibilities of network settings:

*Example*    If you just want to protect data when you are at the office, whatever your connection interface, define the network options as follows:

   ■    Connect only when:

      ■    Interface is: Any

      ■    Gateway is: *.office.com

*Example*    If you want to protect your data only when you are at the office using an Ethernet connection, but do not want protection for connections via Wifi, define the network options as follows:

   ■    Connect only when:

      ■    Interface is: ethernet

      ■    Gateway is: *.office.com

# Configuring Bandwidth

Under this tab, you can configure the bandwidth allocation and compression algorithm for transferring your protected data to the **Live Navigator** server.

1.  Right-click on the **Live Navigator** icon in the taskbar and select Settings.

2.  Select the Bandwidth tab to display the following settings;

| Setting | Description |
|---|---|
| Adjust the amount of bandwidth used in KB/s | Lets you adjust the amount of bandwidth in kilobytes per second to be used for data transfer. Use the cursor to select a value or check the box Unlimited to use the maximum bandwidth at any given time. |
| Compression algorithm | Defines the compression algorithm to use on your protected data when it is transferred on the network:<br><br>■  ZLIB offers the best compromise between speed and compression. Recommended for all LAN connections.<br><br>■  LZMA offers better compression, but requires more processor power. Recommended for slow connections such as WAN. |

# Consulting Protection Activity on the Live Navigator Agent

## Monitoring

To access the Monitoring interface:

1.  Open a session on your **Live Navigator** agent.

2.  Right-click on the **Live Navigator** icon in the Taskbar and choose Monitoring. The Monitoring interface appears.

---

Tip:      Or, from the Windows Start menu, choose All Programs-Live Navigator-Active Agent and click on Monitoring.

---

3.  View the information available under the General and Current Activity tabs

# Status of the Live Navigator Agent

The icon of the **Live Navigator** application in the taskbar gives indications on the status of your agent:

| Status Icon | Description |
|---|---|
|  | **Live Navigator** is running. Your files and directories are protected. |
|  | Alert. Either **Live Navigator** is not running, or protection is not operative. |
|  | **Live Navigator** is not connected to the server. |
|  | **Live Navigator** is paused. |

# Protection Status of an Object

### To activate the display of the Protection status with Windows File Explorer overlay

On Windows agents, you can use the overlay feature to display the protection status of files and directories in the File Explorer.

1.  Right-click in the Windows File Explorer on any directory or file and select Atempo Live Navigator-Enable Shell Activated Protection Status.

    A green icon indicates that the directory of file is protected. A red one indicates that the directory or file is not protected.

2.  Refresh the File Explorer to see the icons.

3.  To disable the overlay, right-click on any directory or file and select Disable Shell Activated Protection Status.

| Note | **Live Navigator** uses six different overlay icons. By design, Windows only supports ten overlay icons. If other applications are already using overlay icons, you may not be able to see **Live Navigator** icons. Check the overlay used in the registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Explorer\Shell OverlayIdentifiers. If needed delete other applications overlay icons. |
|------|---|

**To view the detailed Protection status of an object:**

1.   Right-click in the Windows File Explorer on the directory or file for which you want to check the protection. Select Live Navigator- Check Protection.

2.   The window displays the path of the selected object as well as its protection status. The possible protection statuses, depending on the server and agent rules, are as follows:

| Protection Status | Server Rule | Agent Rule |
|---|---|---|
| **Excluded by System Rule** | Excluded by a system rule | Any |
| **Protected by Server Rule** | Protect all objects | Any |
| **Excluded by Server Rule** | Exclude all objects | Any |
| **Protected by Server Rule** | Protect all objects unless the user specifies otherwise | None |
| **Protected by Server Rule** | Protect all objects unless the user specifies otherwise | Protected |
| **Excluded by Agent Rule** | Protect all objects unless the user specifies otherwise | Excluded |
| **Not Protected** | Protect no object unless the user specifies otherwise | None |
| **Protected by Agent Rule** | Protect no object unless the user specifies otherwise | Protected |
| **Not Protected** | Protect no object unless the user specifies otherwise | Excluded |

## Date of Last Protection of Agent

Right-click on the **Live Navigator** icon in the taskbar to view the last protection date of the agent.

The last protection date is the last date at which you are able to restore data on your agent without loosing any information. It does not necessary mean that any data was backed up at that date. For instance, if no new data has been added since the last session at the time a new session is supposed to occur (according to the RPO parameter), the Last Protection Date is updated even though no new data has been protected.

C H A P T E R   3

# Restoring Data

**3**

The **Live Navigator** agent is equipped with a restore wizard which lets you restore any protected file or folder that has been corrupted, lost or accidentally overwritten. You can restore any version of the object backed up on the **Live Navigator** server, into the folder of your choice on your agent.

# Prerequisites

The agent onto which you want to restore data must be connected to the **Live Navigator** server through a network. Otherwise, no version will be available for restore.

# Restoring Files

## What Files Can I Restore?

### As an End User

You can restore any protected file provided that you have the following access permissions:

- Read-Write authorizations on the destination file.

- Authorization to modify access permissions on the source file.

Otherwise, you will get an Access Denied error during the restore.

### With Administrator Rights

You can use the option Restore as to restore any file, including files and folders requiring administrator level permissions.

An identification window to provide the user account to use for the restore appears when you use the Restore as option.

---

Note:    Access permissions to files and folders are retained at restore, whether you do a local or a cross-restore, as an end-user or as an administrator.

---

---

Note:    If the file to restore is a branch of a folder tree that has disappeared, the tree is restored at the same time as the file.

---

For additional information concerning restore permissions, see the Security Chapter in the Administrator Guide.

## How Can I Search for My Files to Restore?

The restore wizard lets you narrow down the list of files for restore by applying one or more of the following criteria:

| Criterion | Description |
| --- | --- |
| Location | You can indicate either the complete path to your file, or enter a parent folder and choose to include sub-folders in the search, if you are not exactly sure in what subfolder your file is located. |
| Type | The restore wizard will supply you with a list of all the file types present on your machine. You can choose the type of the file you want to restore. Only files of that type will be displayed. If you have also selected a location, the file type criterion is used in addition to the location. |
| Time Range | You can further reduce the list of files displayed in the restore wizard, by choosing a time range for the last modification of the file. Select a value and a unit. For example, 1 hour, or 3 days, or 1 week, etc. If you have also specified a location or a file type, the time range criterion is used in addition. |

Once the wizard has built a list of the files corresponding to your criteria, you can select your file in this list and display its available versions. Select the version and restore the file.

## Searching for the File to Restore



Search Criteria for Files to Restore

Search File A

File A

1. **Location**
Masks the files not at this location

2. **File Type**
Masks the files not of this type

3. **Time Range**
Masks the files last modified at a different time
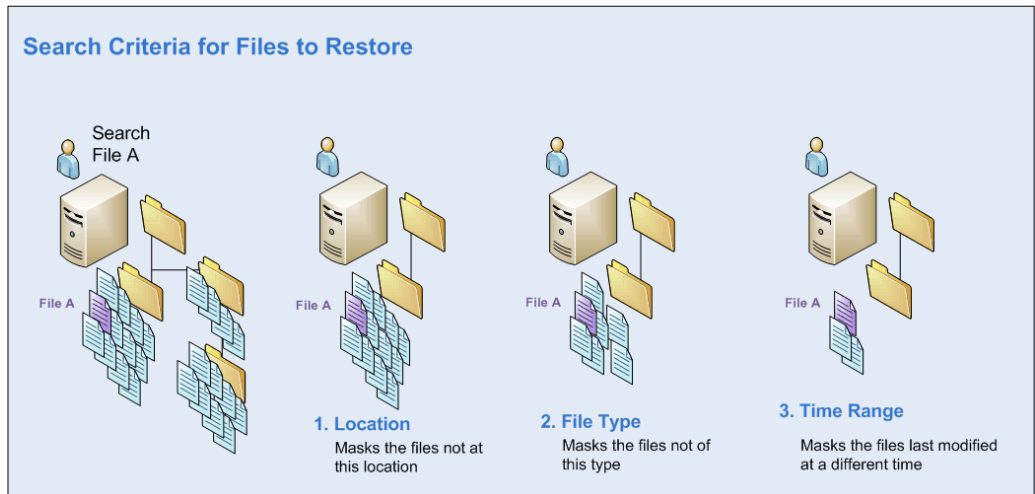
# What Options Do I Have for Restoring Files?

Once you have chosen the file to restore, you can choose among the following options:

- Version

- Restore destination: either restore to the original location, or specify a new destination

- Restore as Administrator lets you restore any file requiring adminstrator level permissions

- Behavior if the file already exists. The possible behaviors are:

    - Overwrite: The file is replaced by the restored file

    - Skip: The file is not restored

    - Rename: The file already present is renamed with the suffix `.bak`

---

**Note**    The file size information in the restore wizard is shown in decimal prefixes (1 MB is equal to 1000 KB) whereas file sizes in File systems is usually shown in binary prefixes (1 MB is equal to 1024 KB). As a result, you may notice a difference if you compare both sizes. The file in the wizard may appear to be bigger than on the file system, but they are actually of the same size.

---

# File Restore Scenarios

## Scenario 1: Restoring a Deleted File

In this scenario, you want to restore a file under the following conditions:

- The file has been deleted.
- You know the original folder of the file, and this folder is still present on your disk.
- You want to restore the file to its original location.
- You want to restore the last version of the file.

**To restore a deleted file**

1. Launch the Restore Wizard by right-clicking on the **Live Navigator** icon in the taskbar, and choosing Restore Wizard.

2. In the Introduction window, choose Restore a file.

3. In the Select Folder window, check the box My file was saved in the following folder. Uncheck Include Subfolders then click Browse to select the folder where the file to restore is found. Finally, click on Show Matching Files.

4. In the Matching Files window, click on the file to restore, then click on Continue.

   By default, the files are sorted by alphabetical order. If the list is too big and you want to limit it to just one file type:

   - Click on Go Back.
   - Returning in the Select Folder window, click on Continue.
   - In the Select File Type window, check the option Show me only files of the following type: and enter the file extension to display in the field to the right of the option.
   - Click on Show Matching Files and select the file to restore.

5. In the Available Versions window, choose the most recent version and click on Continue.

6. In the Restore Destination window, check the option Restore to the original location then click on Restore.

7.  Once the restore has been done, the Restore Status window lets you access your file by clicking on Open destination folder. Click on Finish to close the wizard.

## Scenario 2: Restoring a Deleted File Whose Location is Unknown

In this scenario, you want to restore a file under the following conditions:

- The file has been deleted.

- You do not know the original folder of the file.

- You want to choose the version of the file to restore.

- You want to restore the file to a new location.

### To restore a deleted file without knowing its location

1.  Launch the Restore Wizard by right-clicking the **Live Navigator** icon in the Taskbar, and choosing Restore Wizard.

2.  In the Introduction window, choose Restore a file.

3.  In the Select Folder window, check the box I do not know where my file is saved. Click on Continue.

4.  In the Select File Type window, check the option Show me only files of the following type. A list of file extensions is generated. Select the extension of the file you want to restore and click on Show Matching Files.

5.  By default, in the Matching Files window, the files are sorted by alphabetical order. You can also sort them by folder or by their date of mirroring by clicking on the header of the corresponding column.

    If you can find your file in the list, select it, click on Continue and proceed to step 8.

    If the list is too long and you would prefer to sort files according to their mirroring date, click on Go Back and continue from step 6.

6.  In the Define Time Range window, check My last save was within the last:, then indicate a value and a unit of time, for example 2 hours, or 3 days, etc., and click on Continue.

7.  In the Matching Files window, select the file to restore and click on Continue.

8.  In the Available Versions window, choose the version to restore and click on Continue.

9.  In the Restore Destination window, check the option Select the destination folder. Click on Browse and select a folder. Then click on Restore.

10. Once the restore has been done, the Restore Status window gives you the status of each restored item.

### Scenario 3: Restoring a Previous Version of a File

In this scenario, you want to restore a file under the following conditions:

- The file still exists but you want to recover it as it was at an earlier date.
- You know where the file is located.
- You want to restore the file to a new location.
- An earlier version already exists in the destination folder, and you want to rename the restored version.

**To restore a previous version of a file**

1. Right-click on the file in an Explorer and choose Live Navigator- Restore File.
2. In the list of Available Versions, choose the version to restore by selecting the desired date.
3. In the Restore Destination window, check the option Select the destination folder. Click on Browse and select a folder. In the field If the file already exists, select Rename, then click on Restore.
4. Click on Open destination folder. The already existing file appears with the extension .bak.
5. Click on Finish to close the wizard.

# Restoring Folders

## What Folders Can I Restore?

You can restore any protected folder for which you have Read-Write and Modify Authorizations access permissions. If you do not have these permissions, an Access Refused error will be raised when you try to restore.

## What Information Must I Provide to Restore a Folder?

To restore a folder, the Restore Wizard needs the following information:

- The location of the folder
- Whether you want to restore subfolders of the tree
- The date and time of the version to restore

- The location where you want to restore the folder: either in its original place, or in a destination that you specify.

- Whether you want to restore as an Administrator. Restoring as Administrator lets you restore folders for which Administrator-level permissions are required.

- The behavior to adopt with regards to existing files. The possible behaviors are:

  - Overwrite: The file is replaced by the restored file

  - Skip: The file is not restored

  - Rename: The file already present is renamed with the suffix .bak

# Folder Restore Scenarios

## Scenario 1: Restoring a Deleted Folder

In this scenario, you want to restore a folder under the following conditions:

- The folder has been deleted

- The folder contains subfolders that you also want to restore.

- You want to restore the last version of the folder.

- You want to restore the folder to its original place.

### To restore a deleted folder

1. Launch the Restore Wizard by right-clicking on the **Live Navigator** icon in the taskbar, and choosing Restore Wizard.

2. In the Introduction window, choose Restore a folder.

3. In the Select Folder window, check the box Include Subfolders. Hold down the Shift key and click on Browse to select the folder to restore. This will allow you to browse the **Live Navigator** catalog, *i.e.* the tree of protected folders, including deleted folders, rather than the tree currently on your disk.

4. In the Select Date and Time window, the last backup version is proposed by default. Click on Continue.

5. In the Destination Location window, check Restore to the original location, then click on Restore.

6.    Once the restore has been done, the Folder Restore Status window shows you the status of each restored item.

---

Note :    If the folder contains more than 10 000 files, for performance reasons, the list of restored files is not displayed in real time. Click on Get Status when the restore is finished, to view the complete list of restored objects.

---

## Scenario 2: Restoring a Previous Version of a Folder

In this scenario, you want to restore a folder under the following conditions:

- The folder still exists.

- The folder contains a tree of subfolders that you do not want to restore.

- You want to restore the folder to its original place.

- You only want to restore files that have disappeared.

### To restore a previous version of a folder

1.    Right-click in a file Explorer on the folder to restore, then select Live Navigator-Restore Folder.

2.    In the Select Folder window, uncheck Include Subfolders.

3.    In the Select Date and Time window, choose the time at wich you want to restore the folder. Choose a date and time and the folder will be restored in the state it was in, at that time. The Valid Time Range indicates the time between the first and last backups of your folder. The selected date must fall within this range.

4.    In the Destination Location window, check Restore to the original location. In the field If a file already exists:, choose Skip, then click on Restore.

5.    Once the restore is finished, the Folder Restore Status window displays the status of each restored item.

---

Note :    If the folder contains more than 10 000 files, for performance reasons, the list of restored files is not displayed in real time. Click on Get Status when the restore is finished, to view the complete list of restored objects.

---

# Advanced Restore

In addition to restoring your data on your own local machine, **Live Navigator** allows you to perform the following types of restore:

- Cross Restore
  Restore data to a computer other than the one where data was backed up.

- Remote Restore
  Launch the restore from a computer other than the one where data was backed up.

- Alternate Server Restore
  Restore data backed up by a server other than the one backing up your agent.

You can also combine the advanced restore modes, for instance perform a cross restore on a remote machine of data stored on a replicate server.

The required permissions to perform advanced restore are described in the Security Chapter in the Administrator Guide.

## Cross Restore

You can restore on your machine, files backed up on other machines protected by the same server as your machine. To do so, you need a password provided by your administrator, that authorizes you to perform cross restores.

Inter operating system restore is supported, for instance restoring Linux Files on a Windows computer. However, you may loose some attribute information, if the restore destination OS does not support the source OS attributes.
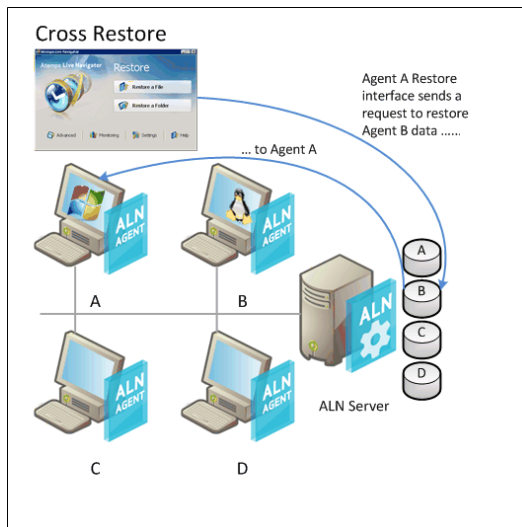


**Note**    When you perform a cross restore, the Browse feature that lets you search for the object to restore, displays the contents of the server catalog rather than the disk of the remote machine. You are not actually connecting to the remote machine.

**To perform a cross restore**

1.    Choose Start-All Programs-Atempo Live Navigator-Atempo Live Navigator Wizard.

2.    In the Restore Wizard window, click on Advanced.

3.    Check the option Restore files backed up on another computer.

4.    In the Restore Mode Window, check the option Cross Restore and provide the password for cross restore as indicated by your **Live Navigator** administrator.

**Note**    The option Restore agent files allows you to cancel the cross restore definition but continue with your parameter selection if you have selected other advanced restore options.

5.    In the Select the Source Computer window, select the machine where the data to be restored is located.

You can sort the list according to:

- Agent Name: Unique name of the computer. In most cases, the admin name is identical to the computer name. But if the computer name already exists, for example for a machine in a different domain, **Live Navigator** adds a suffix in the form -nnn (from 000 to 999) to the computer name to differentiate the machines.

- Computer Name: Name by which the computer is identified on the network.

- Operating System: Operating system of the machine.

If the list of machines is long, enter the name of the machine in the Search field. You can use the wildcard character *. For example, enter win* to find all the machines whose identifier begins with win.

6. Once you have selected the advanced restore parameters, click on Done. The restore source and destination information is displayed at the bottom of Restore Wizard.

You can now choose Restore a File or Restore a Folder and run your restore in the same way as if restoring from your local machine. Depending on the object to restore, see the restore scenarios:

- "Restoring Files", page 23
- "Restoring Folders", page 28

# Remote Restore

Remote restore allows you to launch a restore from a machine other than the one the data was backed up on.
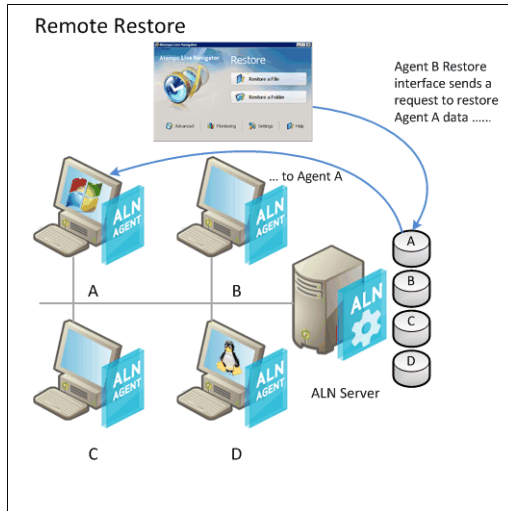


**To perform a remote restore**

1. Choose Start-All Programs-Atempo Live Navigator-Atempo Live Navigator Wizard.

2. In the Restore Wizard window, click on Advanced.

3. Check the option Restore to a different computer.

4. In the Select Agent Window, check the option Remote agent and provide the Fully Qualified Netwok Name of the remote agent to restore, and the user name and password to access the remote agent.

   > **Note** The option Local agent (user@agent) allows you to cancel the remote restore definion but continue with your parameter selection if you have selected other advanced restore options.

5. Once you have selected the advanced restore parameters, click on Done. The restore source and destination information is displayed at the bottom of Restore Wizard.

   You can now choose Restore a File or Restore a Folder and run your restore in the same way as if restoring from your local machine. Depending on the object to restore, see the restore scenarios:

# Restore from an Alternate Server

If the server where you backed up your agent initially is no longer available and a replica of the server exists, or if you want to restore data backed up by another server, use the Alternate Server Restore.
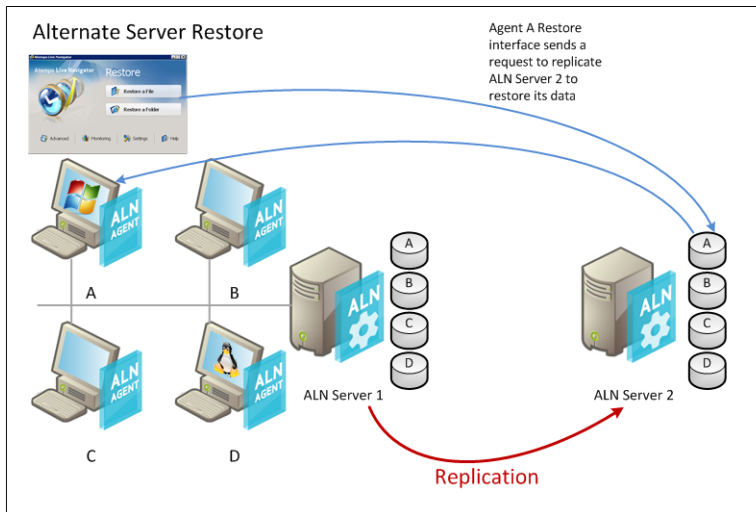


**To perform an alternate server restore**

1. Choose Start-All Programs-Atempo Live Navigator-Atempo Live Navigator Wizard.

2. In the Restore Wizard window, click on Advanced.

3. Check the option Restore from a different server.

4. In the Select the server window, provide the Fully Qualified Network Name of the server you want to restore from.

5. Once you have selected the advanced restore parameters, click on Done. The restore source and destination information is displayed at the bottom of the Restore Wizard.

   You can now choose Restore a File or Restore a Folder and run your restore in the same way as if restoring from your local machine. Depending on the object to restore, see the restore scenarios:

   - "Restoring Files", page 23

-

# Combined Advanced Restore

You can combine all advanced restore modes, for instance to perform a cross restore from a remote machine from the server replica.
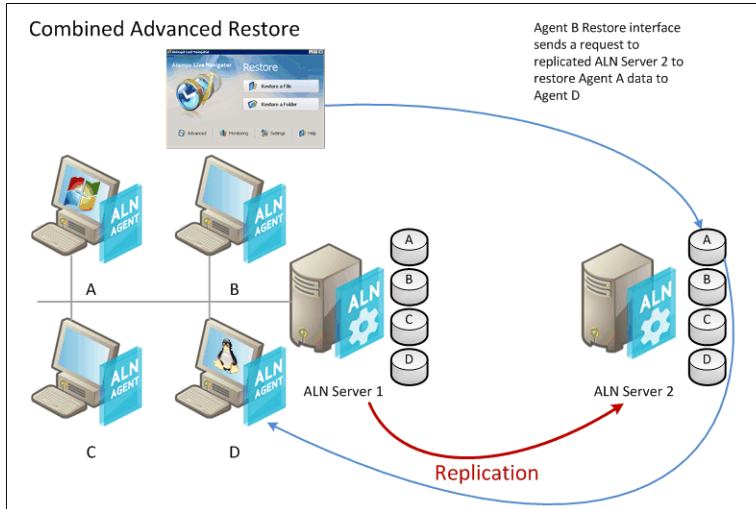


**To perform a combined advanced restore**

1.  Choose Start-All Programs-Atempo Live Navigator-Atempo Live Navigator Wizard.

2.  In the Restore Wizard window, click on Advanced.

3.  Check the three options and provide the restore parameters as described in the three sections above.

# Appendix A: Installing Live Navigator Agents

## Prerequisites to the Live Navigator Server Upgrade

| Prerequisites | Description |
|---|---|
| Product Download | Make sure you have downloaded the **Live Navigator** binaries from the ASG Web Portal at: http://isp.asg.com |
| User | |
| Update URL | If you intend to use the **Live Navigator** build-in mechanism to update your agents automatically (rather than using a tool such as GPO), make sure that you have set the Update URL parameter in the server Administration Console prior to upgrading the server. If not, agents may become unreachable after the server update, at which point you will be unable to push the URL to the agents. |

# Live Navigator Windows Agents Installation

## Prerequisites to Windows Agents Installation

| Prerequisite | Description |
|---|---|
| Operating System | ■  To find out the list of supported Operating Systems, please see the **Live Navigator** compatibility guide on the ASG Web site: http://www.asg.com/Collateral/Compatibility-Guide/ASG-Live-Navigator-Compatibility-Guide.aspx<br><br>■  At least one partition must be of NTFS type. |
| Memory | A minimum of 512 MB of RAM is required. |
| Database directory | The database requires around 10% of the volume of the protected data in disk space. |
| Product Download | Make sure you have downloaded the **Live Navigator** binaries from the ASG Web Portal at: http://isp.asg.com |
| Communication Port | If you want to connect to the Agent interface remotely, for instance to perform remote restores, Port 27261 must be open on your firewall. |
| Language | **Live Navigator** adopts the language set at this operating system level. Available languages are English, French, and German. Make sure you set the proper language for the OS. |

## Installing Live Navigator Windows Agents

### Installing a Live Navigator agent

1.  Make sure that the user who launches the install program has administration rights.

2.  Launch the program setup.exe on the agent from the directory corresponding to your operating system.

3.  Follow the on-screen instructions.

| Parameter | Description |
|---|---|
| License Agreement | Accept the License Agreement to install **Live Navigator**. |
| Destination Folder | Lets you choose a directory other than the default (C:\Program Files\Atempo\**Live Navigator**). Click on Change… and select a directory in the tree. |

| Parameter | Description |
|---|---|
| Database Folder | Lets you choose the path to install the database of the **Live Navigator** agent. To choose a directory other than the default (C:\HNDB\), click on Change... and select a directory in the tree. Make sure you have at least 10% of the volume of the data to protect in free disk space for the database. |
| Network fully qualified name of the server | Lets you enter a fully qualified name for the **Live Navigator** server where the protection policy of your **Live Navigator** agent will be defined. |

4.  Click on Install to finish installing.

5.  Close and reopen your session once the installation is complete to see the **Live Navigator** icon in the system tray.

## Updating Live Navigator Windows Agents

If the server to which your agent is attached is in automatic update mode, you will receive regular update notifications on your agent. These can be run immediately, or delayed for 10 minutes, one hour or eight hours.

## Uninstalling Live Navigator Windows Agents

> **Note**    Before uninstalling, make sure that there are no other users of **Live Navigator** currently connected to the machine.

### Uninstalling Live Navigator

1.  From the Windows Start menu, choose Control Panel-Add or Remove Programs-Change or Remove Programs.

2.  In the list of programs, select **Live Navigator** and click on Remove. A pop-up window asks you to confirm the uninstall.

3.  Restart your host to complete the uninstall.

## Installing/Upgrading Live Navigator Windows Agents in Silent Mode

The silent mode lets you install **Live Navigator** from the command line, without having to launch a graphical interface.

**Installing a Live Navigator agent in Silent Mode**

1. Make sure that the user who launches the install program has administration rights.

2. Launch a command line on your agent and navigate to the directory containing the setup.exe program of the **Live Navigator** agent.

---

**Note**  Select the 64 or 32-bit setup according to your agent type.

---

3. Enter the following command:

   ```
   setup.exe /s /v"/qn SERVERNAME=xxxx DATABASEDIR=xxxx
   INSTALLDIR=xxxx"
   ```

   For instance:

   ```
   setup.exe /s /v"/qn SERVERNAME=csc-data DATABASEDIR=E:\HNDB"
   ```

   where:

| Parameter | Description | Status |
|---|---|---|
| INSTALLDIR | **Live Navigator** installation path. | Optional, the default value is `C:\Program Files\Atempo\` **Live Navigator**`\` |
| DATABASEDIR | **Live Navigator** database path. | Optional, the default value is `C:\HNDB\` |
| SERVERNAME | Connection string of the **Live Navigator** Server where the agent data is going to be protected. The server connection string is in the form: `<servername>:<encrypted port>:<unencrypted port>` See "Agent Ports and Proxy Configuration", page 52, for details. | Mandatory. |
| - /l c:\logfile.log | Creates a log file in c:\logfile.log. | Optional |
| - /qb | The setup only displays a small window with progression information. | Optional |

| Parameter | Description | Status |
|-----------|-------------|--------|
| - /qn | The setup is hidden. | Optional |

**Live Navigator** is installed in silent mode and creates the following log file containing installation related information: TEMP%\setup_atempo_hnm_x86_32.log or %TEMP%\setup_atempo_hnm_x86_64.log.

### Updating a Live Navigator agent in Silent Mode

1.   Make sure that the user who launches the install program has administration rights.

2.   Launch a command line on your agent and navigate to the directory containing the setup.exe program of the **Live Navigator** agent.

---

**Note**   Select the 64 or 32-bit setup according to your agent type.

---

3.   Enter the following command:

```
setup.exe /s /v"/qn"
```

## Deploying Live Navigator Windows Agents

You can deploy **Live Navigator** agents through a network onto multiple agent using a software distribution and deployment tool such as Microsoft Group Policy Object (GPO), SCCM, LANDesk, Altiris, etc.

To use such tool, you need to create an `*.msi` deployment file from the **Live Navigator** agent install program. Then you can use the deployment tool on your domain to deploy this `*.msi` file on all required agents.

---

**Note**   When you configure your GPO for deployment, make sure you have the WMI 32 bit and 64 bit filters to deploy **Live Navigator** according to the operating system of your agent.

---

### Creating the Deployment File

The procedure below lets you create a deployment file for the **Live Navigator** agents containing the following default installation and database directories:

■   The default installation directory: `C:\Program Files\Atempo\`**Atempo**

**Live Navigator**\

■   The default database directory: C:\HNDB\

---

| Note | The only parameter that you will need to set later, either directly in the ALN.msi file or when deploying, is the name of the **Live Navigator** server that will protect the data on the agent, as there is no default value for this parameter. In addition you can also set the installation and database directory if the default value does not suit you. See "Deploying the Live Navigator Agents", page 43. |
|------|---|

---

### Creating the Deployment File for the Live Navigator Agent

1.   Launch a command line interface on your server and navigate to the directory containing the setup.exe program of the **Live Navigator** agent.

---

> **Note** Select the 64 or 32-bit setup according to your agent type.

---

2.   Enter the following command:

setup.exe /a

The flash screen of the setup program appears.

3.   Click on Next.

4.   In the Network Location window, enter the path where you want to create the **Live Navigator** deployment program.

5.   Click on Install. The installation program ALN.msi and the directory program files are created in the specified directory.

6.   Click on Finish to leave the installation program.

### Setting the Server Name Variable in the Deployment file

The server name can be set either by editing the ALN.msi file or directly as a parameter of the command launching the deployment (see "Deploying the Live Navigator Agents", page 43). To set the server name in the ALN.msi, proceed as follows:

1.   In the directory where you created the ALN.msi file, open the file C:\Program Files\Atempo\Atempo Live Navigator\Ref\CfgServerHost.def with a text editor.

2.   Replace the existing line with the connection string of the **Live Navigator** server that will protect the data of your agents.

The server connection string is in the form:

`<servername>:<encrypted port>:<unencrypted port>`

See "Agent Ports and Proxy Configuration", page 52, for details.

3.      Save and close the file.

You can now use the `ALN.msi` file to deploy **Live Navigator** on your agents. They will be protected by the **Live Navigator** server specified in the file `CfgServerHost.def`.

---

| **Note** | You must place the `ALN.msi` file as well as the `program files` directory on the domain server in order to be able to deploy using GPO. |
|---|---|

---

## Deploying the Live Navigator Agents

When deploying the `ALN.msi` file with a deployment tool, you can specify the following parameters:

| Parameter | Description | Status |
|---|---|---|
| INSTALLDIR | **Live Navigator** installation path. | Optional, the default value is `C:\Program Files\Atempo\`**Live Navigator**`\` |
| DATABASEDIR | **Live Navigator** database path. | Optional, the default value is `C:\HNDB\` |
| SERVERNAME | Connection string of the **Live Navigator** Server where the agent data is going to be protected. The server connection string is in the form: `<servername>:<encrypted port>:<unencrypted port>` See "Agent Ports and Proxy Configuration", page 52 for details. | Mandatory, except if defined in `CfgServerHost.def` file as described in "Setting the Server Name Variable in the Deployment file", page 42. |
| - /l* c:\logfile.log | Creates a log file in c:\logfile.log. | Optional |
| - /i | Command to install the `.msi` file | Mandatory |
| - /qb | The setup only displays a small window with progression information. | Optional |
| - /qn | The setup is hidden. | Optional |

For instance:
```
ALN.msi /qb /i INSTALLDIR="c:\Program Files\Atempo\testinstallaln"
DATABASEDIR="c:\Program Files\Atempo\testinstallaln\database"
SERVERNAME=ALNServer /l* c:\temp\logfile.log
```

## Retrieving a Server Name after Deployment

Once **Live Navigator** has been deployed and started on an agent, the agent retrieves the name of the server:

- First in the file `c:\HNDB\CfgServerHost`

- If this file cannot be found, the agent will search the Registry under the following key: `HKLM\SOFTWARE\ATEMPO\HN\, key servername`

- If the name of the server is not in the registry, the agent searches for it in the file `C:\Program Files\Atempo\HSX\Ref\CfgServerHost.def`

# Live Navigator Mac OS X Agents Installation

## Prerequisites

| Prerequisite | Description |
|---|---|
| Operating System | To find out the list of supported Operating Systems, please see the **Live Navigator** compatibility guide on the ASG Web site: http://www.asg.com/Collateral/Compatibility-Guide/ASG-Live-Navigator-Compatibility-Guide.aspx |
| Memory | A minimum of 512 MB of RAM is required. |
| Database Folder | The database requires around 10% of the volume of the protected data in disk space. |
| User's Right | The user performing the installation must have administrator's rights on the machine. |
| Product Download | Make sure you have downloaded the **Live Navigator** binaries from the ASG Web Portal at: http://isp.asg.com |
| Communication Port | If you want to connect to the Agent interface remotely, for instance to perform remote restores, Port 27261 must be open on your firewall. |
| Language | **Live Navigator** adopts the language set at this operating system level. Available languages are English, French, and German. Make sure you set the proper language for the OS. |

## Installing Live Navigator Mac OS X Agents

1. Unzip the file corresponding to Mac OS X, for instance: ALN_31_SP0_P5101_B8612.zip on the Mac OS X agent.

2. Double-click the Agent folder, then the macosx folder.

3. Double-click the LiveNavigator.dmg file, then the LiveNavigator.pkg file.

4. Follow the on-screen instructions.

| Parameter | Description |
|---|---|
| License Agreement | Accept the License Agreement to install **Live Navigator**. |
| Server Name | Enter the name of the machine hosting the **Live Navigator** server. |

| Parameter | Description |
|---|---|
| Database Folder | Lets you choose the path to install the database of the **Live Navigator** agent. To choose a folder other than the default (`/Library/Application Support/HN/DB`), click on Browse and select a folder in the tree.<br>Make sure you have at least 10% of the volume of the data to protect in free disk space for the database. |
| Login Information | Provide the name and password of the administrator. |

## Deploying Live Navigator Mac OS X Agents

The deployment is performed with the `LiveNavigator.pkg` file.

1.  In the same folder where the `LiveNavigator.pkg` is located, create a file named `AutoConfig.txt` containing the following line:

    `SERVERNAME = <server_connection_string>`

    Replace `<server_connection_string>` with your **Live Navigator** Server information. The server connection string is in the form:
    `<servername>:<encrypted port>:<unencrypted port>`
    See, for details.

2.  Launch the command:

    `installer -pkg LiveNavigator.pkg -target "/"`

    The installation will take place at the root of your disk. The installation location cannot be modified.

## Uninstalling Live Navigator Mac OS X Agents

1.  Double-Click /Application/Atempo/Live Navigator/Uninstall.

2.  Provide the password of the administrator and click OK.

# Live Navigator Linux Agents Installation

## Prerequisites

| Prerequisite | Description |
|---|---|
| Operating System | To find out the list of supported Operating Systems, please see the **Live Navigator** compatibility guide on the ASG Web site: http://www.asg.com/Collateral/Compatibility-Guide/ASG-Live-Navigator-Compatibility-Guide.aspx |
| Memory | A minimum of 512 MB of RAM is required. |
| Database directory | The database requires around 10% of the volume of the protected data in disk space. |
| Setup directory | The directory path where you launch the setup must not contain space characters as this is not currently supported. |
| Product Download | Make sure you have downloaded the **Live Navigator** binaries from the ASG Web Portal at: http://isp.asg.com |
| Communication Port | If you want to connect to the Agent interface remotely, for instance to perform remote restores, Port 27261 must be open on your firewall. |
| Language | **Live Navigator** adopts the language set at this operating system level. Available languages are English, French and German. Make sure you set the proper language for the OS. |

## Installing Live Navigator Linux Agents

Installing a Linux agent consists of installing the following components:

- **Live Navigator** Agent
- CDP (Continuous Data Protection), optional but strongly recommended to benefit fully from the **Live Navigator** protection.
- Nautilus (optional)

### To install a Live Navigator Linux Agent

1.  Open a terminal and log in as root.
2.  Go to the Agent/linux_modules directory on the product download directory.

3.  To install the **Live Navigator** agent, make sure that the script `install_module` is executable. If needed, set the permission with the command: `chmod +x install_module`. Depending on whether your Linux version requires DEB or RPM package, launch one of the following command:

    ▪ DEB
      `./install_module deb`

      or

    ▪ RPM
      `./install_module rpm`

    The script will find the package to install corresponding to your Linux version. If your particular Linux version is not present, contact ASG Customer Support.

4.  Define the following environment variables:

    ▪ `HN_SERVER_NAME` to define the **Live Navigator** server connection string. The connection string is in the form:
      `<servername>:<encrypted port>:<unencrypted port>`
      See "Agent Ports and Proxy Configuration", page 52 for details.

    ▪ `HN_WORK_DIR` to define home directory of the **Live Navigator** agent. The default value is `/opt/HNDB` but you can change it if you want.

    ---

    **Note** Make sure that the directory you specify exists.

    ---

5.  To install the **Live Navigator** agent, go to the Agent/linux directory of the product download. Choose amd64 if you want to install a 64-bit version or x86 for a 32-bit version. Depending on whether your Linux version requires DEB or RPM package, launch one of the following command and follow on screen instructions:

    ▪ DEB
      `dpkg -i livenavigator_3.x-<version>_<arch>.deb`

      or

    ▪ RPM
      `rpm -i livenavigator-3.x-<version>.<arch>.rpm`

    Where `arch` is the architecture of the agent, i386 or i686 for a 32-bit machine, and amd64 or x86_64 for a 64-bit machine.

6.  if you are using the Gnome file manager (Nautilus), you can install the **Live Navigator** extension for Nautilus to display a **Live Navigator** contextual menu. Go to the Agent/linux-nautilus directory on the product download directory, and launch the command corresponding to your OS version. For instance:

- - `livenavigatornautilus_<version>.debian6_amd64.deb` for a debian6 64-bit machine.

- - `livenavigatornautilus_<version>.ubuntu1110_i386.deb` for a Ubuntu11.10 32-bit machine.

- - `livenavigatornautilus-<version>.fc16.x86_64.rpm` for a Fedora 16 64-bit machine.

7. Close and reopen your session once the installation is complete to see the **Live Navigator** icon in the system tray.

**To install a Live Navigator Linux Agent in silent mode**

1. Define and export these environment variables:

   - `export HN_SERVER_NAME=<server_connection_string>`

     where `server_connection_string` is in the form:
     `<servername>:<encrypted port>:<unencrypted port>`
     See " for details.

   - `export HN_WORK_DIR=<directory_name>`

     where `directory_name` is the path of the **Live Navigator** Home directory.

2. Launch the installation

   - On debian distributions, run:
     `dpkg -i <packagename>.deb`

   - On rpm distributions, run:
     `rpm -i <packagename>.rpm`

**To launch the Live Navigator Linux Agent**

After the installation, the **Live Navigator** service is automatically launched on the agent. To manually stop or start the service, use the following command:

`/etc/init.d/hnagent {start|stop|restart|status}`

# Deploying the CDP Component

If the automatic update is configured on the server via the Update URL setting, the agent will receive notifications that the CDP component can be automatically installed.

| Note | To deploy CDP, you need to first install the **Live Navigator** component on the agent. |
|------|------|

# Updating Live Navigator Linux Agents

## CDP Component

**To manually update the CDP component**

1.  Open a terminal and log in as root.

2.  Copy the new version of the install_module script and the modules subdirectory.

3.  Relaunch the script:
    ```
    chmod +x install_module
    ./install_module
    ```

4.  Restart the agent when the update is complete.
    ```
    /etc/init.d/hnagent restart
    ```

## Live Navigator Component

**To manually update the Live Navigator component**

1.  Open a terminal and log in as root.

2.  Launch the command corresponding to your Linux version and follow on screen instructions:

    - DEB
      ```
      dpkg -i livenavigator_1.2-<version>_<arch>.deb
      ```

      or

    - RPM
      ```
      rpm -U livenavigator-1.2-<version>.<arch>.deb
      ```

    Where arch is the architecture of the agent, i386 or i686 for a 32-bit machine, and amd64 or x86_64 for a 64-bit machine.

## Automatic Updates

If the automatic update is configured on the server via the Update URL setting, the agent will receive notifications to perform updates of both **Live Navigator** and CDP components when necessary.

# Updating the Linux Kernel

After updating the Linux kernel on your agent, you need to:

- Restart the agent.

- Update the CDP component with the `install_module` script. See ".

# Uninstalling Live Navigator Linux Agents

### To uninstall the CDP component

1. Open a terminal and log in as root.

2. Launch the command corresponding to your Linux version:

- `dpkg --purge livenavigatormodule`

  or

- `rpm -e livenavigatormodule`

### To uninstall the Live Navigator component

1. Open a terminal and log in as root.

2. To uninstall the agent, launch the command corresponding to your Linux version and follow on screen instructions:

  - DEB
    `dpkg --remove livenavigator` to remove the program only.

    `dpkg --purge livenavigator` to remove the program and the local data, by default from the `/opt/HNDB` directory.

    or

  - RPM
    `rpm -e livenavigator` to remove the program and the local data, by default from the `/opt/HNDB` directory.

### To uninstall the Nautilus extension

1. Open a terminal and log in as root.

2. Launch the command corresponding to your Linux version:

- `dpkg --purge livenavigatornautilus`

  or

- ```
  rpm -e livenavigatornautilus
  ```

# Ports and Proxy Configuration

## Agent Ports and Proxy Configuration

The ports and proxy definition is integrated with the server command line as follows:

```
<server>:<port HTTPS>:<port HTTP>:<proxy host>:<proxyport>:<proxy
user>:<proxy passwd>
```

If a parameter is not specified, its default value is used.

- The most basic definition would be:
  ```
  <server>
  ```
- To redefine ports, use the command:
  ```
  <server>:<port HTTPS>:<port HTTP>
  ```
- To redefine the proxy and use default value for the port numbers, use the command:
  ```
  <server>:::<proxy host>:<proxyport>
  ```
- To redefine the proxy and proxy authentication and use default value for the port numbers, use the command:
  ```
  <server>:::<proxy host>:<proxyport>:<proxy user>:<proxy
  passwd>
  ```

For instance, if you are deploying **Live Navigator** on a Windows agent, the command is in the form:

```
setup.exe /vSERVERNAME=<server>:::<proxy host>:<proxyport>:<proxy
user>:<proxy passwd>
```

If you are using the graphical interface when you specify the server name, use a command in the form:

```
<server>:<port HTTPS>:<port HTTP>:<proxy host>:<proxyport>:<proxy
user>:<proxy passwd>
```

# Appendix B: Glossary

**action**

An action of protection or of exclusion that the **Live Navigator** administrator can apply to data on **Live Navigator** agents. There are two predefined actions:

- Include

- Exclude

**ASG Deduplication Engine**

**ASG Deduplication Engine** is a software component with which the Live Navigator server communicates. Its role is to gather all protected data blocks for implementation of data deduplication.

**CDP (Continuous Data Protection)**

A technology which intercepts modifications on objects at block level and stores this data in order to protect it. **Live Navigator** offers protection at near CDP level: thanks to the Recovery Point Objective feature, you can limit the number of backup sessions by postponing the next backup until a defined time interval has elapsed.

**group**

The intermediate level between an agent view and the **Live Navigator** agent. A view can be constituted by one or more groups in which agents are distributed.

**predefined path**

Path in which data to be protected is located. A certain number of paths exist in the software by default. These can be customized by the **Live Navigator** administrator.

**protection rule**

The protection rule is one of the components of a protection scheme. It comprises:

- Combinations of:

  - File categories, defined as a series of extensions or file patterns (*e.g.* ~*)

  - An action to apply to objects corresponding to the defined file types

- A default action for file types not explicitly specified by a category

**protection scheme**

The protection scheme determines what data is to be protected on **Live Navigator** agents.

**strategy**

A strategy is a feature used by the **Live Navigator** administrator to determine the method for protecting the data of **Live Navigator** agents.

**view**

The highest level in the organization of **Live Navigator** agents. A view permits listing of all the agents declared on the server and can be constituted of agent groups.

ASG Worldwide Headquarters Naples Florida USA | asg.com