Symantec™ Desktop and Laptop Option 7.5

Administrator's Guide

For Windows

Symantec.

Disclaimer

The information contained in this publication is subject to change without notice. Symantec Corporation makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Symantec Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

Legal Notice

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THEDOCUMENTATIONISPROVIDED”AS IS”ANDALLEXPRESSORIMPLIEDCONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BELEGALLYINVALID.SYMANTECCORPORATIONSHALLNOTBELIABLEFORINCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 “Commercial Computer Software - Restricted Rights” and DFARS 227.7202, “Rights in Commercial Computer Software or Commercial Computer Software Documentation”, as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

www.symantec.com

Third-Party Copyrights

Douglas C. Schmidt and his research group at Washington University and University of California, IrvineCopyright citation.
ACE (TM) is copyrighted by Douglas C. Schmidt and his research group at Washington University and University of California, Irvine,
Copyright (c) 1993-2002, all rights reserved.

Maarten Hoeben
ReportCtrl.h 2.0.1

Ronald L. Rivest
Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.
License to copy and use this software is granted provided that it is identified as the “RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing this software or this function.
License is also granted to make and use derivative works provided that such works are identified as “derived from the RSA Data Security, Inc.MD5 Message-Digest Algorithm” in all material mentioning or referencing the derived work.
RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided “as is” without express or implied warranty of any kind.
These notices must be retained in any copies of any part of this documentation and/or software.

Wei Dai
Compilation Copyright (c) 1995-2003 by Wei Dai. All rights reserved.
This copyright applies only to this software distribution package as a compilation, and does not imply a copyright on any particular file in the package.
The following files are copyrighted by their respective original authors, and their use is subject to additional licenses included in these files.mars.cpp - Copyright 1998 Brian Gladman.
All other files in this compilation are placed in the public domain by Wei Dai and other contributors.
I would like to thank the following authors for placing their works into the public domain:
Joan Daemen - 3way.cpp
Leonard Janke - cast.cpp, seal.cpp
Steve Reid - cast.cpp
Phil Karn - des.cpp
Michael Paul Johnson - diamond.cpp
Andrew M. Kuchling - md2.cpp, md4.cpp
Colin Plumb - md5.cpp, md5mac.cpp
Seal Woods - rc6.cpp
Chris Morgan - rijndael.cpp
Paulo Baretto - rijndael.cpp, skipjack.cpp,
square.cpp
Richard De Moliner - safer.cpp
Matthew Skala - twofish.cpp
Permission to use, copy, modify, and distribute this compilation for any purpose, including commercial applications, is hereby granted without fee, subject to the following restrictions:
1. Any copy or modification of this compilation in any form, except in object code form as part of an application software, must include the above copyright notice and this license.
2. Users of this software agree that any modification or extension they provide to Wei Dai will be considered public domain and not copyrighted unless it includes an explicit copyright notice.
3. Wei Dai makes no warranty or representation that the operation of the software in this compilation will be error-free, and Wei Dai is under no obligation to provide any services, by way of maintenance, update, or otherwise. THE SOFTWARE AND ANY DOCUMENTATION ARE PROVIDED “AS IS” WITHOUT EXPRESS OR IMPLIED WARRANTY INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL WEI DAI OR ANY OTHER CONTRIBUTOR BE LIABLE FOR DIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
4. Users will not use Wei Dai or any other contributor's name in any publicity or advertising, without prior written consent in each case.

5. Export of this software from the United States may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.
6. Certain parts of this software may be protected by patents. It is the users' responsibility to obtain the appropriate licenses before using those parts.
If this compilation is used in object code form in an application software, acknowledgement of the author is not required but would be appreciated. The contribution of any useful modifications or extensions to Wei Dai is not required but would also be appreciated.

Stac Electronics
Copyright (C) Stac Electronics 1993, including one or more U.S. patents No. 4701745, 5016009, 5126739 and 5146221 and other pending patents.

Birdstep Technology, Inc.
Copyright (c) 2001 Birdstep Technology Inc. All rights reserved.

Contents

Chapter 1 Symantec Desktop and Laptop Option

Chapter 2 Configuring the Desktop and Laptop Option

Chapter 4 DLO Command Line Interface Management Tools

Chapter 5 Administering the Desktop Agent

Chapter 1

Symantec Desktop and Laptop Option

About Symantec Desktop and Laptop Option

The Symantec Desktop and Laptop Option (DLO) provides automated file protection for desktops and laptops (collectively referred to as desktops). Protection is provided whether the computer is connected to the network or offline. When the desktop is not connected to the network, files are backed up to a user data folder on the desktop. When the computer reconnects to the network, files are backed up from the local desktop user data folder to the designated network user data folder. Users who have multiple computers can synchronize the data between their computers so the most up-to-date file versions are available on all their computers.

Deduplication feature is introduced with this version of Symantec DLO. Dedupe retains one copy of the attachment in a PST file, which multiple users or computers share. This process eliminates data duplication and increases efficiency in handling backup and storage.

Note: Symantec DLO product is intended to provide file-level protection for desktop user data and is not intended to provide a full system backup.

DLO Components

DLO contains the following components:

- DLO Administration Server
- DLO Dedupe Server
- DLO Administration Console
- DLO Database
- DLO Maintenance Server
- DLO Agent (Desktop Agent)

DLO Administration Server

The DLO Administration Server is a service running in the background. The DLO Maintenance Server, Storage Locations (File Server) and DLO Administration Console can reside on the Administration Server.

Dedupe Server

The Dedupe Server is web service hosted on Tomcat Web Server. It maintains the Global Hash Table and helps the Agent in identifying the data that already exists in the Dedupe Storage Location.

The Dedupe Server can also be installed on the same server where the other DLO components are installed.

DLO Administration Console

DLO Administration Console is the graphical user interface. From the DLO Administration Console, the Administrator can perform the following tasks:

- Create profiles for groups of users or computers. Profiles enable you to control the desktop user's level of interaction with the Desktop Agent, define the types of files that can be backed up, set the schedule for backups, and configure additional settings for the Desktop Agent.
- Create network user data folders. Network user data folders are locations on the network where data from protected desktops is stored.
- Create Automated User Assignments. Automated User Assignments determine the DLO Storage Location and profile to which users are assigned when they install the Desktop Agent.

Note: Automated User Assignments are not used if users are manually added to DLO.

- Add users manually to DLO. Instead of using Automated User Assignments, you can manually add users to DLO and assign a profile and DLO Storage Location to them. This is particularly useful when network shares already exist for user data storage. Users can be added individually or multiple users can be added at the same time by importing them from a list.
- View history log files, receive alerts, and restore files to a desktop from the Administration Console.
- Configure and manage Dedupe Server.

DLO Database

The DLO Database has two components: Configuration database and Dedupe database.

- **DLO Configuration Database:** DLO configuration database contains details related to the deployment of DLO components. For example, where the database is installed (on a remote machine or on the host), where the maintenance server exists, and so on.
- **Dedupe Database:** Dedupe database is the data store used by Dedupe Server for persisting the Dedupe related configuration and the Global Hash Table.

  The Dedupe database is always installed on the same server as the DLO Configuration database in all the supported configurations of the DLO Configuration database.

DLO Maintenance Server

The maintenance server is installed by default when DLO is installed.

Only one maintenance server is required. However, in large installations it may be more efficient to have one maintenance server for each Storage Location (File Server).

Desktop Agent

The Desktop Agent resides on the desktops and laptops that you want to protect. The desktop user’s level of interaction with the Desktop Agent can vary depending on how the Administrator has configured the profile assigned to the user. The Desktop Agent may run in the background, automatically protecting files. Alternatively, desktop users with full access to the Desktop Agent interface can do the following:

- Schedule backups
- Select which types of files to back up
- Restore files

- Synchronize file versions between different computers
- View the status of their backups

Related Topics:

"Configuring DLO" on page 72

"About DLO Profiles" on page 84

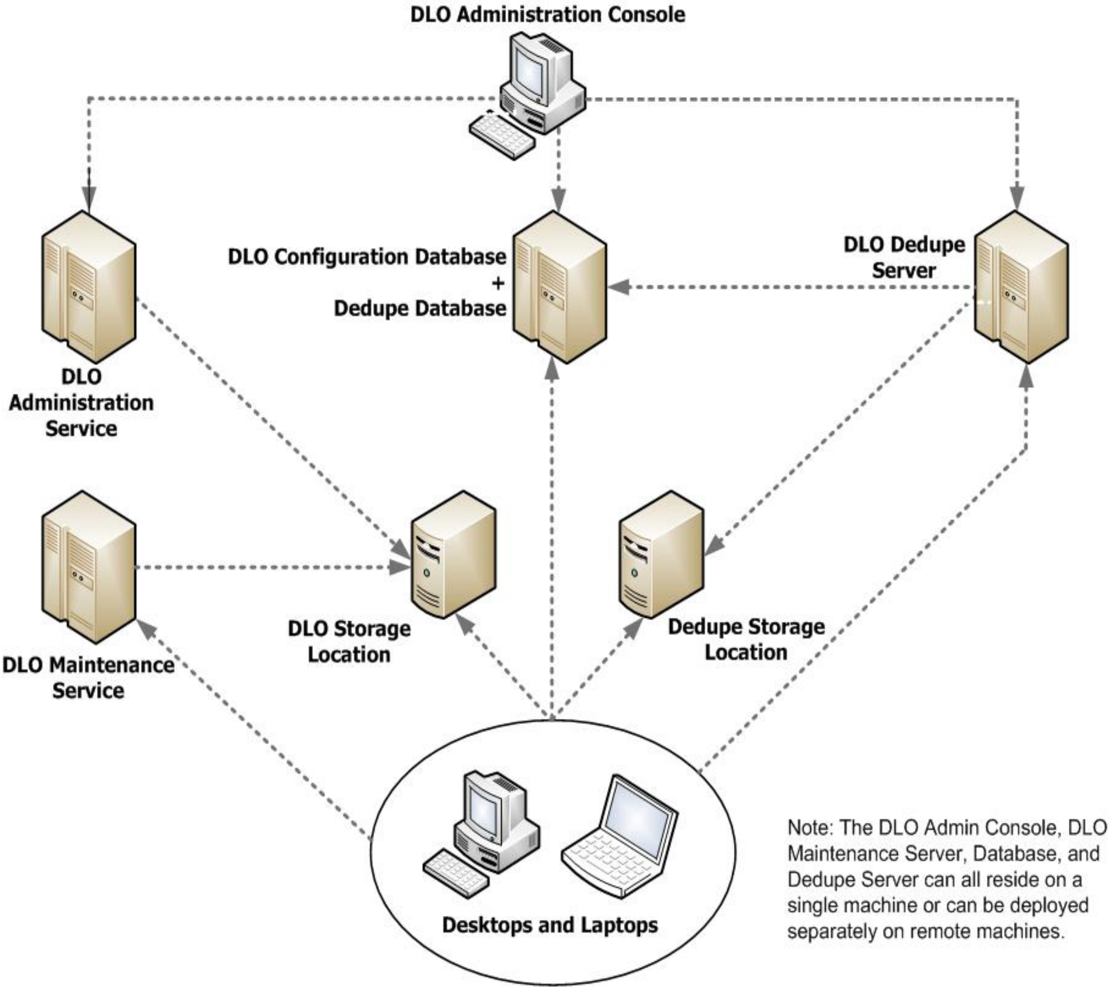
"About Backup Selections" on page 102

"About DLO Storage Locations" on page 121

"About Automated User Assignments" on page 129

"Configuring Dedupe Server" on page 73

Figure 1-1 Symantec Desktop and Laptop Option Components



Note: The DLO Admin Console, DLO Maintenance Server, Database, and Dedupe Server can all reside on a single machine or can be deployed separately on remote machines.

What's New in DLO

Symantec DLO 7.5 is an integrated backup solution that has source-side deduplication capability.

This section provides a brief introduction about the new features included in this release.

Global Source-side Deduplication

DLO 7.5 now supports deduped backups.

The following are the methods of deduplication supported:

- **Intelligent deduplication of files**
  - Dedupe the entire file for the very first time; that is, the very first backup revision of the file will be deduped.
  - If the file changes, then the backup modality automatically switches to "delta mode" from "dedupe mode" for that file, that is, delta will be applied from second revision of the backup file on a particular computer.
- **Content aware deduplication of PST**
  Global single instancing (SIS) of the attachments is achieved using content aware deduplication of PST.

This feature helps in improving the network usage and optimizes the storage requirements.

Windows 8 Desktop and Windows Server 2012 Support

- DLO Agent extends support to Windows 8
- DLO Administration Server extends support to Windows Server 2012

SQL Server 2012 Support

DLO extends support to SQL Server 2012.

Command Line Option to Delete Pending Users

DLO provides a new command-line option to delete pending users from the DLO database.

DLO Upgrade Support

DLO supports upgrades from the following previous versions:

- Symantec DLO 7.0

- BackupExec-DLO 2010 R3
- NetBackup DLO 6.1 MP7

For any existing customers with previous release of DLO (NetBackup DLO or BackupExec DLO) apart from the versions mentioned above, it will be a stepped upgrade support. That is, customers should first upgrade the existing version of DLO to Symantec DLO 7.0, and then upgrade to Symantec DLO 7.5. For more information, see “Upgrading to Symantec DLO 7.5” on page 50.

IPv6 Support

DLO supports versions 4 and 6 of the Internet Protocol (IP), which are commonly referred to as IPv4 and IPv6. You can use IPv4 and IPv6 in backup and restore networks. Support for IPv6 is dependent upon operating system support for the protocol, as well as proper network configuration.

Lotus Notes

DLO provides support to Lotus Notes version 8.5.3.

DLO Log Gather Utility

The DLO Log Gather tool is used to collect logs from various product install paths, log path, registry export, operating system, and from the installed applications. For more information, see “Symantec DLO Log Gather Tool” on page 242.

BitLocker Support

DLO provides support to volumes that run Windows BitLocker Drive Encryption.

Before You Install

Before you install DLO, you should consider the following described inTable 1-1.

:

Table 1-1 Pre-installation considerations

Item	Description
Domains and Active Directory	The DLO Administration Server, DLO Dedupe Server, and DLO Storage Locations must be in a Windows Domain or Active Directory. Computers running the Desktop Agent can be outside a Windows Domain or Active Directory, but they must authenticate with the domain or directory to access the DLO Administration Server or Storage Locations.
User Privileges for Installing DLO Components	

Table 1-1 Pre-installation considerations (continued)

Item	Description
Domain/User Credentials	Any user with local administrative rights can install the Symantec DLO components. In case the user account does not have the privileges, the administrator should grant local administrative rights to the user. **Note:** While installing the DLO database, and if the "Remote DB Install" option is selected, then the user account must have local administrative rights on the remote computer where SQL server is installed.
Authentication	DLO Administration Console The DLO Administration Console can be managed by any user who has full administrator rights on the DLO Administration Server where DLO is installed. The user's account must be a domain account and must have rights to create network shares and manage permissions of network shares and directories on any remote server used for Storage Locations or network user data folders. This is commonly accomplished by using a domain administrator account, or can be accomplished by granting a standard domain account with local administrative rights to the servers hosting the DLO resources. See "Managing Administrator Accounts" on page 37 for more information. Desktop Agent DLO requires domain accounts. Every Desktop Agent user must log in to DLO using a domain account. If you have users who log in using local accounts, they can still use DLO, but they must have domain credentials to authenticate with DLO. Dedupe Storage Location Access Credentials Dedupe Storage Location Access Credentials are domain user accounts having full control on the network storage locations configured as Dedupe Storage Locations. It is recommended to specifically create a low privilege domain user account only for accessing the Dedupe Storage Location. A user with administrator rights is not permitted to be configured as Dedupe Storage Location Access Credential account. See "About Dedupe Storage Locations" on page 128 for more information.

Table 1-1 Pre-installation considerations (continued)

Item	Description
Database Selection	By default DLO installs its own instance of SQL Server 2008 R2 Express SP1. DLO can also be manually configured to use an existing SQL Express 2005, SQL Server 2008, SQL Server 2005, or SQL Server 2008 R2. **Note:** If you use an existing database instance, named pipes must be enabled. If DLO installs its own SQL Express instance, named pipes will be enabled automatically.
Time Synchronization	All computers running the DLO Administration Console or the Desktop Agent should be set to a common time. This can be accomplished by configuring the Windows Time Synchronization service on the network. See www.microsoft.com for more information.
Firewalls	DLO is designed to work in firewall environments. For DLO to function properly in a firewall environment, network file shares must be visible after establishing a remote connection such as VPN. If file sharing is not allowed, then DLO will not be able to transfer files to or from the network user data folder. Desktop computer files will still be protected to the desktop user data folder, and will be transferred when the network user data folder is accessible.

System Requirements for the DLO Administration Server

The following are the minimum system requirements for running this version of DLO Administration Server.

Item	Description
Operating system	■ Microsoft Windows 2003 Server SP2 (32-bit, 64-bit, and R2) ■ Microsoft Windows 2008 Server SP2 (32-bit, 64-bit) ■ Microsoft Windows 2008 Server R2 SP1 ■ Microsoft Windows Server 2012 **Note:** Ensure that the operating system is updated with the latest service packs, to be able to install the DLO Administration Server. The Desktop Agent is not supported on any Windows Server class operating system.
CPU	2 x 1.5 GHz 32/64-bit
Processor	Xeon compatible

Memory	Minimum required: 4 GB RAM or more Recommended: 8 GB or more for better performance
Disk space	500 MB hard disk space required after Microsoft Windows is installed.

System Requirements for the DLO Dedupe Server

The following are the minimum system requirements for running the Dedupe Server.

Item	Description
Operating system	■ Microsoft Windows 2003 Server SP2 (32-bit, 64-bit, and R2) ■ Microsoft Windows 2008 Server SP2 (32-bit, 64-bit) ■ Microsoft Windows 2008 Server R2 SP1 ■ Microsoft Windows Server 2012 Recommended: Windows 2008 Server R2, 64-bit **Note:** Ensure that the operating system is updated with the latest service packs, to be able to install the Dedupe Server.
CPU	Quad core 64-bit
Processor	Xeon compatible
Memory	Minimum required: 4 GB RAM or more Recommended: 8 GB or more for better performance
Disk space	500 MB hard disk space required after Microsoft Windows is installed.

System Requirements for the DLO Maintenance Server

The following are the minimum system requirements for running this version of DLO Maintenance Server.

Table 1-2 Minimum system requirements

Item	Description
Operating system	■ Microsoft Windows 2003 Server SP2 (32-bit, 64-bit, and R2) ■ Microsoft Windows 2008 Server SP2 (32-bit, 64-bit) ■ Microsoft Windows 2008 Server R2 SP1 ■ Microsoft Windows Server 2012 **Note:** Ensure that the operating system is updated with the latest service packs, to be able to install the Maintenance Server.
CPU	2 x 1.5 GHz 32/64-bit
Processor	Xeon compatible
Memory	Required: 4 GB RAM Recommended: 8 GB or more for better performance
Disk space	200 MB hard disk space required after Microsoft Windows is installed

System Requirements for the DLO Database

The following are the minimum system requirements for running the DLO Database.

Table 1-3 Minimum system requirements

Item	Description
Operating system	■ Microsoft Windows 2003 Server SP2 (32-bit, 64-bit, and R2) ■ Microsoft Windows 2008 Server SP2 (32-bit, 64-bit) ■ Microsoft Windows 2008 Server R2 SP1 ■ Microsoft Windows Server 2012 **Note:** Ensure that the operating system is updated with the latest service packs, to be able to install the DLO database.
CPU	Quad core 64-bit
Processor	Xeon compatible

Table 1-3 Minimum system requirements (continued)

Item	Description
Memory	Required: 4 GB RAM Recommended: 8 GB or more for better performance
Disk space	10 GB hard disk space

DLO Installation Options

You can choose one of the following installation options based on the infrastructure in your organization.

- **Option 1:** Install each component on a different machine.
- **Option 2:** Install all components on one machine.
- **Option 3:** Install the DLO Administration Server and Dedupe Server on two different machines, and install the remaining components on another machine.

Installing the Symantec Desktop and Laptop Option

Review the topic "Before You Install" on page 19, which contains information that should be considered before installing DLO.

Note: The DLO Administration server must be in a domain.

To install the Symantec Desktop and Laptop Option

1. Run `setup.exe` to start the installation wizard.
2. Click **Next**.
3. Read the license agreement, and if you accept the terms, select I **accept the terms in the license agreement**.
4. Click **Next**.
5. Select the setup type from the following options.
    - **DLO Administration Console:** Installs only the DLO Administration Console. This selection is typically used to install an additional console on a separate computer.
    - **DLO Administration Service:** Installs the DLO Administration server on the system.
    - **DLO Maintenance Service:** Installs only the DLO maintenance server. The maintenance server supports delta file transmission and storage. For more information, see "About Delta File Transfer" on page 115.
    - **DLO Database Service:** Installs the DLO configuration database and Dedupe database on the system.
    - **Dedupe Server Service:** Installs the Dedupe Server on the system.
6. If you want to install to a different directory, click **Change**, select the new directory, and click **OK**.
7. Click **Next**.
8. Enter the DLO License key.
9. Click **Next**.

10 Select one of the following options for the DLO database.

SQL Server 2008 R2 Express SP1

On a 32-bit machine, the new local SQL Server 2008 R2 instance will be located at `C:\Program Files (x32)\Microsoft SQL Server\ MSSQL10_50.DLO` for DLO Database, and `C:\Program Files (x32)\Microsoft SQL Server\ MSSQL10_50.DEDUPE` for Dedupe database.

On a 64-bit machine, the new local SQL Server 2008 R2 instance will be located at `C:\Program Files (X86)\Microsoft SQL Server\ MSSQL10_50.DLO` for DLO database and `C:\Program Files (X86)\Microsoft SQL Server\ MSSQL10_50.DEDUPE` for Dedupe database.

Note: Each SQL instance requires minimum 2 GB hard disk space.

Existing SQL Server instance

The DLO Database and Dedupe database will be stored on an existing SQL Server 2005, SQL Server 2008, or SQL Server 2008 R2 Express instance on this computer. Select an instance from the list provided.

Note: If you use an existing database instance, named pipes must be enabled. If DLO installs its own SQL instance, then named pipes will be enabled automatically.

If you select this option, make sure that the SQL service is running under domain admin credentials, and provide the same user account credential that was used to install the SQL server, else the database connection fails.

Remote DB Install

The Symantec DLO console and SQL server are installed on two different machines. While installing DLO, provide the IP address or host name of the machine where SQL is installed. The DLO database is installed on the remote machine.

Note: Named pipes must be enabled on the machine where the SQL server is installed.

After enabling the named pipes, restart the SQL server and SQL server browser services. These services must be running with the domain admin credentials. Also, the computer browser services must be running.

Make sure that you provide the same user account credential that was used to install the SQL server, else the DLO Administration Console fails to launch.

11 Click **Next**.

12 Enter the account credentials, which will be used to create DLO Storage Locations and network user data folders. This account should be a domain

account that has local administrative rights on computers where backup data must be stored. See “Domain/User Credentials” on page 20.

13 Click **Next**.

14 Click **Install** to begin the installation.

15 When the installation is complete, click **Finish**.

Note: After installing the DLO components, to verify the status of the Dedupe Server, type the following URLs in your browser.
http://<dedupeserver_ip_or_hostname>:8080
https://<dedupeserver_ip_or_hostname>:8443
If the Dedupe Server is active, then the following message is displayed: *Dedupe Server Status: (20159) Active.*
If there is no response from Dedupe Server, then it indicates that the Dedupe Server is not initialized, and one of the reasons could be that the database connection is down.

Deploying the Desktop Agent

When you install DLO, the Desktop Agent install set is placed in a share in the installation directory and is available using a Uniform Naming Convention (UNC) path.

You can choose one of the following methods to deploy the Desktop Agent from the Desktop Agent install share to the desktop computer.

Table 1-4 Desktop Agent deployment methods

Deployment Method	Description
E-mail	Send a hypertext link to the install files or include the install files as an attachment.
Web page	Place the install files on your company's intranet.
Logon scripts	Create a file that includes commands for installing the Desktop Agent. Then assign the script to the User Properties for the employees who need to use DLO. The commands are executed automatically when the user logs on to the network. For more information about logon scripts, refer to your Microsoft Windows documentation.
Microsoft Systems Management Server (SMS)	Use this automated system to distribute the Desktop Agent install set to the desktop computers, which then initiate the installation. For more information about SMS, refer to your Microsoft documentation.
CD-ROM	To distribute the Desktop Agent installation files on a CD-ROM, place the contents of the `\\DLO Administration Server\DLO Agent` share on the CD-ROM. Users can then run `setup.exe` from the CD-ROM. The installed Desktop Agent will be correctly associated with the DLO Administration Server. See "Push Install Desktop Agent and Push Install DLO Maintenance Server" on page 31 for more information.

Related Topics

"Installing the Desktop Agent" on page 247.

Desktop Agent Installation Options

The Desktop Agent installation can be customized to meet specific needs. For example, it can run silently with no user interface displayed, or it can display either a basic or complete user interface. This and other customizations are accomplished by modifying the `SETUP.INI` file in the DLO Agent setup directory.

To customize the Desktop Agent installation

1. In the Desktop Agent `setup` directory, open the `SETUP.INI` file for editing.
2. Modify the value that begins `CmdLine= /qf`. The following options are available.

`Desktop Agent installation interface`

Modify the `/qf` term to change the interface that the Desktop Agent user sees during installation of the Desktop Agent.

`/qf`
: The full user interface is displayed, and a cancel button is provided.

`/qb`
: A basic progress dialog is displayed and the cancel button is enabled.

`/qb!`
: A basic user interface displayed. There is no cancel button.

`/qn`
: The installation will be silent installation.

Note: For a completely silent install, you must run the `"setup.exe /s"` after modifying the `SETUP.INI` file.

`Set the Default Media Server`

`DEFAULTMEDIASERVER` specifies the media server to which the Desktop Agent will attach after installation.

`Launch the Desktop Agent`

The `LAUNCHCLIENT` option specifies whether or not the Desktop Agent should be launched immediately following installation.

To launch immediately, set `LAUNCHCLIENT="1"`

To prevent immediate launch, set `LAUNCHCLIENT="0"`

`Suppress Reboot`

To suppress a reboot, even if one is required, add the following:

`REBOOT=ReallySuppress`

`Logging Options`	Logging options can be modified by changing the `l*v` variable. `l*v “%TEMP%\DLOAgentInstall.log”` Turns on verbose logging and create a log file at the specified location. **Note:** For additional Windows Installer logging options, see http://support.microsoft.com/kb/314852/EN-US/.

3 Save and close the `SETUP.INI` file.

Examples:

For a silent installation, edit `CmdLine` in the `SETUP.INI` file as follows:

Original:

```
CmdLine=/qf DEFAULTMEDIASERVER=”Desktop3” LAUNCHCLIENT=”1”
/l*v “%TEMP%\DLOAgentInstall.log”
```

Modified:

```
CmdLine=/qn DEFAULTMEDIASERVER=”Desktop3” LAUNCHCLIENT=”1”
/l*v “%TEMP%\DLOAgentInstall.log”
```

For an installation with a basic interface but no option to cancel the installation, edit `CmdLine` in the `SETUP.INI` file as follows:

Original:

```
CmdLine=/qf DEFAULTMEDIASERVER=”Desktop3” LAUNCHCLIENT=”1”
/l*v “%TEMP%\DLOAgentInstall.log”
```

Modified:

```
CmdLine=/qb! DEFAULTMEDIASERVER=”Desktop3” LAUNCHCLIENT=”1”
/l*v “%TEMP%\DLOAgentInstall.log”
```

Preparing for a Manual Push Deployment of the Desktop Agent

Complete the following steps before attempting a manual push deployment of the Desktop Agent.

1 From the `\\<`*`servername`*`>\DLOAgent` directory the following files are required:

- `*.mst`
- `*.cab`
- `DLOBuildInfo.ini`
- `*.msi`

2 Run the `msiexec` command using, as a base, the value in `setup.ini` from the cmdline key:

```
/qf DEFAULTMEDIASERVER="<From setup.INI File>"
DLODBINSTANCENAME="<FromSetup.INI File>" LAUNCHCLIENT="1"
TRANSFORMS="1033.mst" /l*v "%TEMP%\DLOAgentInstall.log"
```

The following are the default values.

DEFAULTMEDIASERVER	DLO Administration Server name. This value is assigned when DLO is installed and is the name of the computer on which the administration server is installed.
DLODBINSTANCENAME	Specifies the SQL instance name. It is recommended that you do not modify this value.
LAUNCHCLIENT	"1"
TRANSFORMS	"1033.mst"

3 For a silent installation, replace `/qf` with `/qn`.
To install without user interaction, but with a display of the installation progress, replace `/qf` with `/qb`.

4 TRANSFORMS should be set to one of the mst files, according to the language used by the desktop user:

```
1031.mst = German
1033.mst = English
1034.mst = Spanish
1036.mst = French
1040.mst = Italian
1041.mst = Japanese
1042.mst = Korean
2052.mst = Chinese (PRC) (Simplified)
1028.mst = Chinese (Traditional)
1046.mst = Portuguese Brazilian
1049.mst = Russian (Russia)
```

5 The specification of the TRANSFORMS property is required, and will affect the installer user interface and the start menu shortcuts. The DLO Agent is installed with support for all eleven languages, regardless of the transform chosen.

MSI 4.5 is required on the target systems. The MSI 4.5 (KB942288-v4) installer is included in the following file:

`\\<servername>\DLOAgent\WindowsInstaller.exe`

Push Install Desktop Agent and Push Install DLO Maintenance Server

You can install either the Desktop Agent or the Maintenance Server on a remote machine using the push install feature.

Prerequisites

To push-install DLO Desktop Agent to a computer that runs Symantec Endpoint Protection (SEP) version 11.0 or later, you must configure SEP to share files and printers. The file and printer sharing feature is turned off by default.

From the DLO Administration Console, you can install the following on remote computers:

- DLO Desktop Agent
- DLO Maintenance Server

Note: You can either push-install multiple Desktop Agents or Maintenance Servers at a time, but you cannot combine both the options.

Procedure to Push Install Desktop Agent and DLO Maintenance Server

---

Note: To push install Desktop Agent on to a Windows 8 Agent machine, the **remote registry services** should be enabled and started on that machine.

To push install Desktop Agent and push install DLO Maintenance Server on remote computers

1. Launch the DLO Administration Console.
2. On **Tools**, select **Install Agents and maintenance services on remote computers** and click **Next**.
3. On **Install Agent/Maintenance Server to Remote Computers** > **Select Component** to select any of the following components:
   - **Agent** - To push-install the Desktop Agent from the administration server to remote computers.
   - **Maintenance** - To push-install the DLO Maintenance Server from the administration server to remote computers.
4. Click **Add.**
5. In **Manual Entry of Remote Computer Name**, type the following:
   - **Name/IP Address**: Enter the computer name or IP address of the remote computer.
   - **Domain Name**: Enter the domain name of the remote computer.
   - **Browse**: Click **Browse**. In **Select Computer**, choose the required remote computer and click **OK**.

The **Name/IP Address** and **Domain Name** is updated. Also, **Remote Computer Logon Credentials** is displayed with the selected computer name and domain name.

6 Click **OK.**

7 In **Remote Computer Logon Credentials**, type the following:

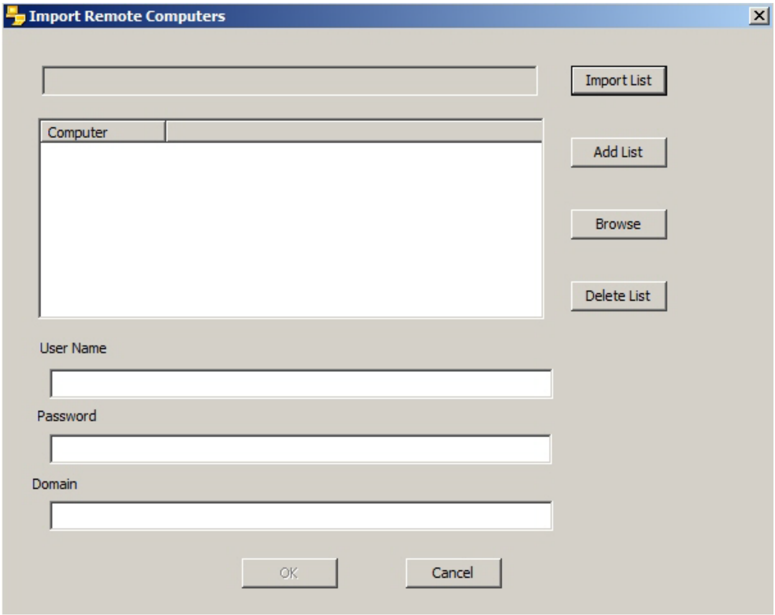
- **User Name:** Enter the user name for an account that has administrator rights on the remote computer.
- **Password:** Enter the password for an account that has administrator rights on the remote computer.
- **Domain Name:** The domain name is displayed based on the domain name you have entered in **Manual Entry of Remote Computer Name**.
- **Use this user name and password when attempting to connect to additional computers during the installation**: Select this option if you want to use the same user name and password during the next installation. By default, this option is not selected.

8 Repeat steps 4 to 6 for every remote computer for which you want to push-install the options.

9 You can also import the list of IP addresses of remote computers. To import the list, do the following:

- On **Install Agent/Maintenance Server to Remote Computers** > **Remote Computer Selection** window, click **Import Computers**.

- On the **Import Remote Computers** window, click **Import List**.



- Select the specific `.txt` file that contains all the IP addresses of remote computers.

Note: To generate a `.txt` file that contains the list of Desktop Agent machines, run the `DLOCommandu.exe -ListMachines` command. For more information, see "-ListMachines command" on page 236.

- To select a remote computer, click **Browse.**
- Click **Add List**. The IP address or the computer name is displayed in the **Computer** panel.
- Click the computer name or IP address and enter the details in these fields:
  - **User Name:** Enter the user name for an account that has the administrator rights on the remote computer.
  - **Password:** Enter the password for an account that has the administrator rights on the remote computer.
  - **Domain Name**: Enter the same domain name that you had entered in **Manual Entry of Remote Computer Name**.
- Click **OK**.

10 Click **Install**.

Based on the component (Desktop Agent or Maintenance Server) you have selected, the remote Desktop Agent or Maintenance Server is added.

11 To exit the wizard, click **Finish**.

To remove the remote Desktop Agent or Maintenance Server from the list

1 Select the remote Desktop Agent or the Maintenance Server.

2 Click **Remove**.

A **Confirmation Window** is displayed with the message: '*Do you want to Delete: <Component>*'.

> **Note:** *<Component>* refers to either Remote Desktop Agent or Maintenance Server, depending on the component you want to delete.

3 Click **Yes**.

The component is deleted from the list.

Post Installation Tasks

This section describes tasks that you should complete immediately after installation.

Setting a Recovery Password

When the DLO Administration console opens for the first time, the Recovery Password wizard opens. You must set a recovery password using this wizard or DLO will not run. If you upgraded from a previous revision and previously set a recovery password, you will not be prompted to set a recovery password. DLO will use the existing password.

The recovery password enables you to retrieve encrypted data that would otherwise be lost if the DLO database is damaged or corrupted.

Once set, this recovery password can only be changed using the DLO command-line interface tools.

Related Topics

"Checking Data Integrity" on page 35

"-SetRecoveryPwd command" on page 222

"-EmergencyRestore command" on page 222

Checking Data Integrity

The Data Integrity Scanner simplifies the process of scanning network user data from previous DLO backups to detect unrestorable backup data due to problems with the encryption keys. It verifies that all data is encrypted using the most recent user key, and ensures that all data has the correct recovery key for emergency restoration. This verification is applicable only to the user specific data in the DLO Storage Locations, and not for the shared data in the Dedupe Storage Locations.

When Desktop Agents are upgraded, they will automatically perform a data integrity check. When the DLO Administration console is opened, it identifies Desktop Agents that have not been checked for integrity. If any are found, a dialog will open stating that one or more computers have not yet been validated by the Data Integrity scanner and ask if they should be scanned.

To check data integrity

1. From the **Tools** menu, select **Wizards** and then **Data Integrity Scanner**.
2. Click **Next**.
3. If you want to set advanced options, click **Advanced Options**. Select the appropriate options and click **OK**.

Permanently remove previously quarantined data	Select this check box to cause all previously quarantined data to be deleted.
Quarantine data encrypted with outdated keys	Select this check box to quarantine all files with outdated keys. If this option is not checked, data is scanned without being quarantined. After data is quarantined, the Desktop Agent backs up a new version of the file with the correct encryption key.
Include computers that have already been validated	Select this check box to force all data to be rescanned, even if it has previously been validated.
Verbose output	Select this check box to receive detailed information from the scan.

4. Click **Start**.
5. Review the scan results.
   If the scan identified data encrypted with outdated keys but you did not choose to quarantine the data, you can run the scan again after setting advanced options to quarantine this data.
6. Click **Next**.
7. Click **Finish**.

Related Topics

"Setting a Recovery Password" on page 35

"-SetRecoveryPwd command" on page 222

"-EmergencyRestore command" on page 222

Changing DLO Service Credentials

When DLO is installed, you must specify account credentials to be used to run the DLO Administration Service. This account is used to create Storage Locations and network user data folders, and must have rights to create shares on any computers where backup data is to be stored. It is recommended to use a Domain Administrator account. To create Storage Locations in another domain, there must be appropriate trust relationships in effect.

To change DLO service credentials

1. On the **Tools** menu, select **Manage Service Credentials**.
2. Select **Change DLO Service Account Information**.
3. Enter the following account credentials.

Change DLO service account information	Select to change the DLO service account information.
User name	Type the user name for the account to be used.
Domain name	Enter the domain for this account.
Password	Type the password for this account.
Confirm password	Type the password again to confirm.

Managing Administrator Accounts

The DLO Administration Console can be managed by any user who has full administrative rights on the DLO Administration Server. The user’s account must be a domain administrator account and must have rights to create network shares and manage permissions of network shares and directories on any remote server used for DLO Storage Locations, Dedupe Storage Locations, or network user data folders.

When searching for files to restore, or when viewing history logs, the DLO Administration Console accesses the network user data folders using the credentials of the currently logged in user. If this user does not have the correct permissions to access a resource, then a message is displayed explaining this issue. If a DLO administrator attempts to access a network user data folder, but is not logged in with an account with rights to access this folder, DLO will prompt for credentials. If the administrator enters the credentials, then they will be used to access the folder, but will not be saved.

The DLO administrator also manages the Dedupe features such as configuring the Dedupe Server, creating Dedupe Storage Pools, Dedupe Storage Locations, and running the Garbage Collector utility.

Automated Permissions Management

To configure DLO to automatically manage permissions for accessing network user data folders, an administrator on the DLO Administration Server can create and configure DLO administrator accounts for users using the DLO Administrator Account Management dialog. Adding DLO Administrator accounts allows additional users to use the DLO console without adding them to the administrators group on the administration server.

You can manage DLO administrator accounts in one of the following ways:

- **Granting individual users administrative access to DLO**

  This is the default configuration for DLO account management. You can grant the rights to manage DLO, to a group of users. If you use a group of users, you can specify which users will have full restore rights, and which users will have limited restore rights.

  See "Creating and Configuring Individual Accounts to Manage DLO Permissions" on page 39 for instructions on configuring DLO to use a list of individual DLO administrators.

- **Using domain groups to manage DLO administrators**

  You can choose to specify domain groups to specify DLO administrators. If you specify domain groups, one group can be granted full restore privileges, and a second group can be granted limited restore privileges. The domain groups must already exist or must be created by a domain administrator. For DLO, we recommend using the groups `DLOFullAdmin` and `DLOLimitedAdmin`. The full administrator group is used to grant administrators read access to user's data, whereas the limited administrator group only supplies list access, thus protecting the user's data from unauthorized access.

  When accessing a network user data folder, the DLO console automatically checks the folder to ensure it can read the files and data within. If the Console is unable to access the folder, DLO uses the specified domain administrator group to set permissions on the files and folders it needs to access. By making these files and folders a member of the specified DLO administrator group, all DLO administrators are automatically granted permissions to access the necessary resources.

  See "Creating and Configuring Domain Groups to Manage DLO Permissions" on page 40 for more information.

Limited Restore

The purpose of the limited restore feature is to prevent restoration of data to an alternate location by unauthorized users. By default, DLO administrators cannot restore a desktop user's files to an alternate location, providing an additional level of data security. A DLO administrator can be granted full restore privileges, which allows the administrator to restore data to an alternate location. When a DLO administrator has limited restoration rights, there may be other administrative functions that they are not able to perform.

Creating and Configuring Individual Accounts to Manage DLO Permissions

An administrator on the DLO Administration Server can create and configure DLO administrator accounts for individual users. Accounts can be individually configured to specify full or limited restore rights as discussed in “Managing Administrator Accounts” on page 37.

Alternatively, DLO can be configured to use domain groups for permissions management. See “Creating and Configuring Domain Groups to Manage DLO Permissions” on page 40 for more information.

To configure DLO to use a list of individual accounts for permissions management

1 On the DLO navigation bar, select the **Network** menu, and select **Administrator Accounts**.

2 Click **Permissions**.

3 Ensure that the **Use domain groups to manage access to network user data folders** check box is not selected.

4 Click **OK**.

5 Do one of the following:

- To add a new DLO administrator account. click **Add**. Continue with step 6.
- To modify an existing DLO administrator account, click **Edit**. Continue with step 6.
- To delete an existing DLO administrator account. click **Remove**. Continue with step 7.

6 Define the following administrator account.

User name	Type the name of the user that must be assigned with administrative rights. Use the format *DomainName\UserName*
Description	Type a description for this administrator account.
Notes	Type any relevant notes regarding the administrator account.

Grant administrator full restore privileges	Select this check box to allow this DLO administrator full restore privileges, including the ability to restore desktop user data to an alternate location. **Note:** Allowing someone other than the desktop user who owns the data to restore files to an alternate location can compromise data security.

7 Click **OK** twice.

Creating and Configuring Domain Groups to Manage DLO Permissions

An administrator on the DLO Administration Server can create and configure DLO administrator accounts for users using the DLO Administrator Account Management dialog. One method of managing DLO administrative access is to use domain groups to specify who has rights to administer DLO. Two groups can be specified. The first group is granted full restore privileges. The second group has limited restore privileges as discussed in "Managing Administrator Accounts" on page 37.

Alternatively, DLO can be configured to use a list of accounts for permissions management. See "Creating and Configuring Individual Accounts to Manage DLO Permissions" on page 39 for more information.

To configure DLO to use domain groups for permissions management

1 On the DLO navigation bar, select the **Network** menu, and select **Administrator Accounts.**

The **Administrator Account Management** window appears.

2 Click **Permissions**.

3 Select the **Use domain groups to manage access to network user data folders** check box.

Note: When the **Use domain groups to manage access to network user data folders** option is selected, domain groups are listed on the Administrator Account Management dialog. When this option is not selected, individual user accounts are once again listed. If you change from one type of account management to another, the previous settings are retained for future use. For example, if you have a list of individual DLO administrators and then you change your configuration to use domain groups instead, the list of individual accounts is saved and will once again be used if the **Use domain groups to manage access to network user data folders** option is not selected.

4 Click **Browse** and select the appropriate option.

For DLO administrators with full restore privileges, use the domain group	To grant full restore privileges to DLO administrators in a specified domain group, including the ability to restore a desktop user's files to an alternate location, enter or browse to a fully qualified domain group. Example: `Enterprise\DLOFullAdmins`
For DLO administrators with limited restore privileges, use the domain group	To grant limited restore privileges to DLO administrators in a specified domain group that do not include the ability to restore a desktop user's files to an alternate location, enter or browse to a fully qualified domain group. Example: `Enterprise\DLOLimitedAdmins`

5 Click **OK** twice.

DLO Default Settings

When you start DLO for the first time, default settings are already configured during installation. You can adjust the default settings to meet the requirements of your environment. Default settings are available for profiles, backup selections and Global Settings. That is, you can run DLO to back up and restore desktop and laptop computers safely by using only the default settings.

You can change default settings for profiles, backup selections, and Global Settings.

Note: Changes to Global Settings take place immediately and apply globally to all Desktop Agents. Changes to the default profile and backup selection settings apply only to new profiles and backup selections and do not affect those that already exist.

Changing Default Profile Settings

The default DLO profile settings can be modified as follows:

To change default profile settings

1 On the DLO navigation bar, click **Setup**.

2 On the **Task** pane, under **Tool Tasks**, click **Options**.

3 In the **Properties** pane, under **New Profile Defaults**, click **General.**

4 Set the options as explained in "General Profile properties" on page 85.

5 In the **Properties** pane, under **New Profile Defaults**, click **User Settings.**

6 Set the profile user settings options as explained in “Profile User Settings options” on page 93.

7 In the **Properties** pane, under **New Profile Defaults**, click **Schedule.**

8 Set the profile schedule options as explained in “Profile User Settings options” on page 93.

9 In the **Properties** pane, under **New Profile Defaults**, click **Options**.

10 Set the profile options as explained in “Additional Profile tab options” on page 98.

Changing Default Backup Selection Settings

The default DLO backup selection settings can be modified as follows.

To change default backup selection settings

1 On the DLO navigation bar, click **Setup**.

2 On the **Task** pane, under **Tool Tasks**, select **Options**.

3 Under **New Backup Selection Defaults** in the Properties pane, click **Revisions** and set backup selection revision options as described in “Backup Selection Revision Control tab options” on page 109.

4 In the **Properties** pane under **New Backup Selection Defaults**, click **Options**.

5 Set the options as explained in “Backup Selection options” on page 111.

Changing Default Global Settings

The default DLO global settings can be modified as follows:

Note: These settings apply immediately to all Desktop Agents.

To change default global settings

1 On the DLO navigation bar, click **Setup**.

2 On the **Task** pane under **Tool Tasks**, select **Options**.

3 In the **Properties** pane under **Global Settings**, click **Options**.

4 Set global options. Table 1-5 describes the options.

Table 1-5 Global settings options

Item	Description
Disable	
All Desktop Agents	Select this check box to prevent all Desktop Agents from backing up.
Incremental backups of Outlook PST files	Select this check box to prevent the incremental backup of Microsoft Outlook PST files for all users. See "Backing up Outlook PST Files Incrementally" on page 265 for more information.
Incremental backups of Lotus Notes mail files	Select this check box to prevent the incremental backup of Lotus Notes files for all users. See "Backing up Lotus Notes NSF Files Incrementally" on page 267 for more information.
Reports	
Generate reports in PDF	Select this option to display reports in PDF if Adobe Reader is installed. If the Reader is not installed, then reports are displayed in HTML format.
Generate reports in HTML format	Select this option to display reports in HTML format.
Generate reports in XML format	Select this option to display reports in XML format.
Generate reports in XLS format	Select this option to display reports in XLS format.
Other	
Time to auto-refresh Administration Console	Enter the time in minutes. After the specified time, the Administration Console is automatically refreshed. The default value is 1 minute.

Table 1-5 Global settings options (continued)

Item	Description
Time to delay Desktop Agent startup after user logs in	Select this check box and enter the number of seconds to delay the start of the Desktop Agent after the user logs in. The Desktop Agent start is only delayed if this check box is selected and the Desktop Agent is started from the **Start** menu. The default value is 30 seconds.
Storage Threshold	
Desktop Agent low disk error threshold	Enter a value. Desktop Agent stops writing to the desktop user data folder when the available disk space drops below this level, and an error message is displayed. The default value is 3 %
Desktop Agent low disk warning threshold	Enter a value. A warning is displayed when the available disk space on the Desktop Agent drops below this value. The default value is 5%.
Network Storage low disk warning threshold	Enter a value. A warning is displayed when the available disk space on the network storage drops below this value. The default value is 5%.
Desktop Agent low quota warning threshold	Enter a value. A warning is displayed when the available disk quota on the Desktop Agent drops below this value. The default value is 10%. For example, if the desktop user data folder is limited to 30 MB and the low quota warning threshold is set at 10%, a quota warning is displayed when less than 3 MB space is available on the Desktop Agent.

Table 1-5 Global settings options (continued)

Item	Description
Network Storage low quota warning threshold	Enter a value. A warning is displayed when the available disk quota on the network storage drops below this value. The default value is 10%. For example, if the network user data folder is limited to 100 MB and the low quota warning threshold is set at 10%, a quota warning is displayed when less than 10 MB space is available on the network user data folder.

5 In the **Properties** pane under **Global Settings**, click **Desktop Agent Intervals**.

6 Set the Desktop Agent interval defaults. Table 1-6 describes the options.

Table 1-6 Desktop Agent interval options

Option	Description
How long to wait before retrying the backup of a previously busy file	Enter the number of minutes DLO waits before it retries the backup of previously busy file. If the wait time is reduced, Desktop Agent computers spend more CPU time and disk I/O trying to backup files if they are busy. If the time is set higher, files are backed up less frequently. The recommended default is 5 minutes.
How long to wait before retrying the backup of a previously failed file	Enter the number of minutes to wait before retrying the backup of a file that previously failed to back up. If the wait time is reduced, Desktop Agent computers spend more CPU time and disk I/O trying to backup files that previously failed to back up. If the time is set higher, files are backed up less frequently. The recommended default is 60 minutes.

Table 1-6 Desktop Agent interval options (continued)

Option	Description
How long to retain backups of files that have been removed from backup selections	Enter the number of days to retain backups of files that have been removed from backup selections. Increasing the retention time causes the files to be left on the server for a longer time after they have been removed from the backup selection. Setting a shorter retention time provides more space in the backup folders, but reduces the time during which users can restore files that have been removed from the backup selections. The recommended default is 30 days.
Minimum time between history updates	Enter the number of minutes to wait between history updates. If there is a lot of activity, a reduced time between updates causes the computers to spend more CPU time and disk I/O to update history. A higher wait time reduces the frequency of history updates. The recommended default is 15 minutes.
Minimum time between postings of the same alert	Enter the number of hours to wait between postings of the same alert. When there is a recurring alert, it is displayed only once during the specified time interval. If the time is set too low, the alert log can fill up with multiple postings of the same alert. The recommended default is 24 hours.
Minimum time between closing a job log and starting a new one	Enter the number of minutes to wait between closing a job log and starting a new one. When the time between job logs is reduced, more job logs appear. The recommended default is 30 minutes.

Table 1-6 Desktop Agent interval options (continued)

Option	Description
Minimum time between maintenance cycles	Enter the number of minutes to wait between maintenance cycles. A lower time between maintenance cycles means more CPU time and disk I/O is spent conducting maintenance. Maintenance cycles remove obsolete files and folders. The recommended default is 1440 minutes, which is 24 hours.
Minimum time between checking for changes to Lotus Notes e-mail files	Enter the number of minutes between checks for changes to Lotus Notes files. A lower time results in more CPU time and disk I/O is used to determine if Lotus Notes files have changed. The recommended default is 30 seconds.
Time during which Desktop Agents randomly respond to restart requests	Enter the number of minutes during which the Desktop Agents will randomly respond to restart requests. When a large number of Desktop Agents are restarted, for example when network user data folders are moved, the Desktop Agents are restarted randomly over a specified period of time. This prevents the potential for overloading DLO by starting a large number of Desktop Agents at the same time. The recommended default is 30 minutes.

7 In the **Properties** pane under **Global Settings**, click **User Activity Settings**.

8 Set the User Activity Settings defaults.

Enable user activity restrictions — Check **Enable user activity restrictions** to determine how DLO will perform tasks when users are interacting with their desktop computers. User activity is based on typing and mouse movement.

Limit network bandwidth usage to — Enter the maximum network bandwidth that DLO will use when the user is interacting with the desktop computer.

Restrictions will be removed when there has been no user activity for x seconds — Enter the number of seconds of user inactivity after which DLO will no longer restrict jobs.

Maximum scanner items per second	Scanner items per second limits the number of items processed per second during a file system scan. File system scans occur during the first backup of a desktop computer, after an abnormal system shutdown, or if the change journal is truncated. This setting reduces the impact of the scan on the desktop computer while the user is active.

9 In the **Properties** pane under **Global Settings**, click **LiveUpdate**.

10 Set the LiveUpdate defaults.

Enable Desktop Agent scheduled automatic updates	Select **Enable Desktop Agent scheduled automatic updates** to turn on scheduled automatic updates.
When checking for updates	Select one of the following: ■ Automatically download and install all available Desktop Agent updates ■ Only notify Desktop Agents of available updates (these updates will not be installed or downloaded)
Frequency	Select one of the following options to check for updates: ■ Once ■ Daily ■ Weekly ■ Monthly
Interval	Select the time to check for updates. The specific options available will vary with the frequency selected.

Configuring DLO to Use a Specific Port for Database Access

You may want to configure DLO to use a specific port for database access. This may be necessary, for example, if a fixed port is already being used for the SQL Server, you may need to configure DLO to use the same port to access the DLO database.

To configure DLO for alternate database access through a specific port

1 Select a unique port number for the DLO database and then use `svrnetcn.exe` to set the new port number.

2 On computers that run the DLO Administration Console from outside the firewall, create the following registry key as a DWORD value if it does not exist and set the DBUseTCP flag to 1:

```
HKLM\Software\Symantec\Symantec DLO\AdminConsole\DBUseTCP
```

3 On computers that run the Desktop Agent from outside the firewall, create the following registry key as a DWORD value if it does not exist and set the DBUseTCP flag to 1:

`HKCU\Software\Symantec\Symantec DLO\Client\DBUseTCP` or

`HKLM\Software\Symantec\Symantec DLO\Client\DBUseTCP`

4 Set the `DBTcpPort` on the computers modified in steps 2 and 3 to the port number you set in step 1.

5 Restart the modified computers.

Configuring Dedupe to Use a Specific Port for Database Access

You may want to configure the Dedupe Server to use a specific port to access the database. This may be necessary in scenarios where a fixed port is being used for the SQL Server, and SQL Server Browser service is disabled.

To configure Dedupe Server for database access through a specific port

Add the specific port number in the `context.xml` file located at this path:

```
C:\Program Files\Symantec\Symantec DLO\Dedupe
Server\Tomcat\webapps\DedupeServer\META-INF\context.xml
```

Sample context.xml where the port number is specified:

```
<?xml version="1.0" encoding="UTF-8"?>
<Context path="/DedupeServer" docBase="DedupeServer" debug="5"
   reloadable="true" crossContext="true">
   <Resource name="jdbc/dedupedb" auth="Container"
   type="javax.sql.DataSource"
   maxActive="100" maxIdle="30" maxWait="10000"
   factory="com.middleware.db.DBConnectionPoolFactory"
   driverClassName="com.microsoft.sqlserver.jdbc.SQLServerDrive
   r" removeAbandoned="true"
   removeAbandonedTimeout="300" logAbandoned="true"
   validationQuery="select 1"
   autoReconnect="true"
   url="jdbc:sqlserver://;serverName=172.22.68.180;instanceName
   =DLO;portNumber=1445;DatabaseName=dedupedb;integratedSecurit
   y=true" />
</Context>
```

Note: After changing the values in the `context.xml` file, you must restart the Dedupe Server.

If you are running SQL Server as a named instance and you are not using a specific TCP/IP port number in your connection string, then you must enable the SQL Server Browser service to allow for remote connections.

To configure a SQL server to listen on a specific TCP port, refer to the instructions at http://msdn.microsoft.com/en-us/library/ms177440(v=sql.105).aspx

Upgrading to Symantec DLO 7.5

To upgrade from a previous version of DLO to Symantec DLO 7.5, follow these steps:

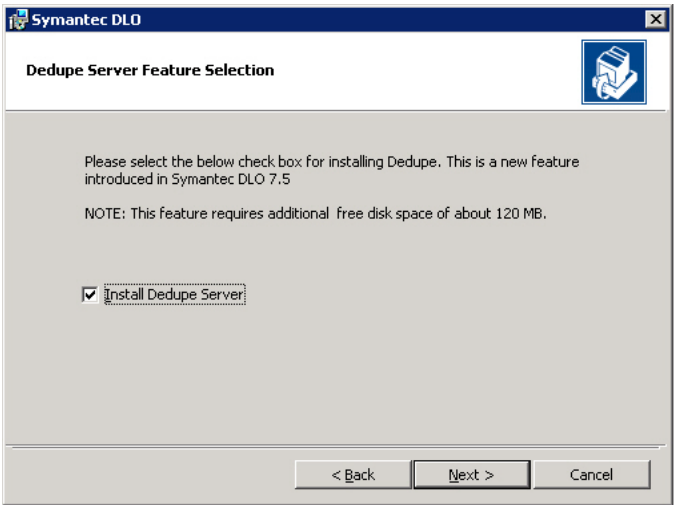
1 Run **setup.exe** to start the installation wizard.

2 Click **Next**.

3 Read the license agreement, and if you accept the terms, select **I accept the terms in the license agreement**.

4 Click **Next**.

5 As DLO 7.5 comes with Dedupe feature, the following screen appears.



Symantec DLO

Dedupe Server Feature Selection

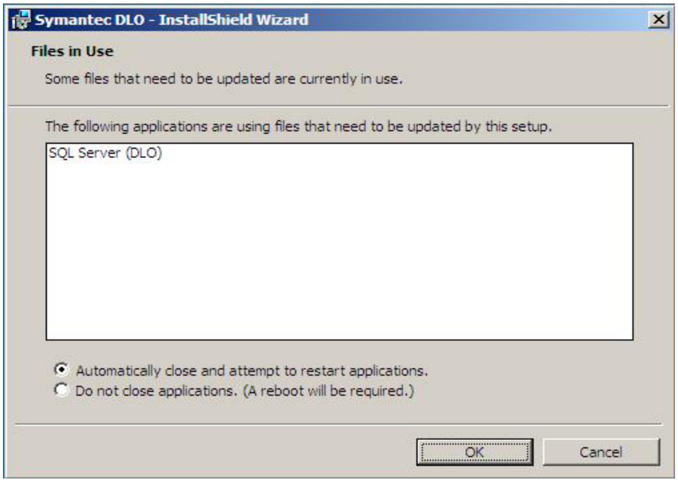
Please select the below check box for installing Dedupe. This is a new feature introduced in Symantec DLO 7.5

NOTE: This feature requires additional free disk space of about 120 MB.

☑ Install Dedupe Server

6 Select the **Install Dedupe Administration Service Feature** check box and click **Next**.

7 During upgrade, the following screen may appear in some scenarios.



Symantec DLO - InstallShield Wizard

Files in Use

Some files that need to be updated are currently in use.

The following applications are using files that need to be updated by this setup.

SQL Server (DLO)

● Automatically close and attempt to restart applications.

○ Do not close applications. (A reboot will be required.)

8 Select the **Do not close applications** option and click **OK**.

Note: Reboot is not required after upgrade.

9 Proceed with the installation steps.

10 When the installation is completed, click **Finish**.

Updating Symantec DLO

Updates to DLO are periodically provided by Symantec as website downloads or on CD. Updates to the Desktop Agent install set are included, although the Desktop Agent updates are not automatically installed. Symantec LiveUpdate will be used to deliver selected security patches to the DLO Administration Server and Desktop Agents.

Updating Symantec DLO with LiveUpdate

Symantec LiveUpdate, which provides updates, upgrades, and new versions of Symantec DLO, is installed manually. You can access LiveUpdate from several locations in Symantec DLO. However, you cannot access it from the Windows **Start** menu.

Symantec DLO installs the latest version of LiveUpdate. If a previous version of LiveUpdate is detected on the computer, Symantec DLO upgrades it. You can view any hot fixes or service packs that are installed on the media server. When LiveUpdate installs updates on the Symantec DLO media server, it also determines if computers on which the Remote DLO Agent for Windows Systems have the latest updates. You can push-install or manually install those updates to Symantec DLO Remote Agents. Symantec Live Update will take care of the Dedupe Server update.

You can use the LiveUpdate Administrator utility with LiveUpdate. The LiveUpdate Administrator utility allows an administrator to modify LiveUpdate so that network users can download program and virus definition updates from an internal server rather than going to the Symantec LiveUpdate server over the Internet.

Go to
ftp://ftp.symantec.com/public/english_us_canada/products/symantec_scan_engine/5.1/manuals/LuAdmin.pdf

Running LiveUpdate Manually

You can run LiveUpdate manually at any time to check for updates. You can configure LiveUpdate to run in either Interactive mode or Express mode. Interactive mode gives you the flexibility to choose which updates you want to install. Express mode automatically installs all of the Symantec DLO updates. For information about how to change the LiveUpdate mode, refer to the LiveUpdate documentation.

Note: By default, LiveUpdate is configured for Interactive mode. If you change it to Express mode, then you must cancel the LiveUpdate session and restart it before the change takes place.

To run LiveUpdate manually

1. On the DLO Administration Console, go to **Tools**, click **LiveUpdate**.
2. In **LiveUpdate**, do the following:
   - To apply the updates, upgrades, and new versions of Symantec DLO, click **Start**.
   - To decline the updates, upgrades, and new versions of Symantec DLO, click **Cancel**.

Updating the DLO Administration Console

The default installation directory for Symantec DLO version 7.0 and later is:

`C:\Program Files\Symantec\Symantec DLO`

If upgraded from NetBackup (NBU) DLO or BackupExec (BE) DLO, then the install path is `C:\Program Files\Symantec\Symantec DLO`

Previous versions of DLO used the following default installation directories:

```
C:\Program Files\VERITAS\NetBackup DLO
C:\Program Files\Symantec\NetBackup DLO
```

To update the DLO Administration Console

1. Install the DLO Administration Console as directed in “Installing the Symantec Desktop and Laptop Option” on page 25.
2. Start the DLO Administration Console and set a recovery password using the Recovery Password Wizard, which automatically starts the first time DLO is opened after installation. For more information on the Recovery Password Wizard, see “Setting a Recovery Password” on page 35.
3. If you are updating from DLO version 5.0, run the Data Integrity Scanner to detect DLO backup files that are no longer being used, verify that all data is encrypted with the most recent user key, and ensure that all data has the correct recovery key for emergency restoration. See “Checking Data Integrity” on page 35 for more information.

Updating the Desktop Agent

As soon as the DLO Administration Server is updated, either through a full install or Maintenance Pack release, the Desktop Agents should be updated in one of the following ways:

1. Update the Desktop Agent from the Desktop Agent Computer
2. Update the Desktop Agent using the **Install Agents and Maintenance Services on Remote Computers** option on the DLO Administration Console. See “Procedure to Push Install Desktop Agent and DLO Maintenance Server” on page 32 for more information.
3. Update the Desktop Agent from the Command-Line Interface

Note: Command line option does not work for Windows Vista and later. In this case, you can use either the first or second option.

Updating the Desktop Agent from the Desktop Agent Computer

To manually update the Desktop Agents, from the Desktop Agent computer, run the following:

```
\\<DLO Administration Server>\DLOAgent\setup.exe
```

Updating the Desktop Agent from the Command-Line Interface

The DLO Command-Line Interface tool can automatically offer updates to the Desktop Agents using the publish command.

To upgrade Desktop Agents from the DLO Administration Console using the command-line interface

1. Update the DLO Administration Server as explained in the update documentation.
2. From the command line on the DLO Administration Server, change to the DLO installation directory.
   Default installation directory:

   Example `C:\Program Files\Symantec\Symantec DLO`
3. Run `DLOCommandu.exe` with the update option to add the configuration file and make note of the ID number returned when this command is run:

   ```
   DLOCommandu -update -add -f
   "DLOAgent\update_7.5\DLOAgentUpdate_NBU.ini"
   ```

   Note: If the configuration file has been moved or renamed, you will need to specify the full path and file name in the command above.

   Sample output:

   ```
   ID=3
   Name=7.5 Update
   Updates Symantec DLO Desktop Agent to 7.5
   Version=7.5
   PromptUser=Yes
   ExitAfterLaunch=No
   Build=7.50.25a
   srcPath=\\a2symms14907\DLOAgent\update_7.5
   cmdName=AutomatedAgentUpgrade.exe
   cmdArgs=
   cmdPath=%DOWNLOADDIR%
   ```
4. Run `DLOCommandu.exe` with the `publish` command to make the update available to Desktop Agent users.

   ```
   DLOCommandu -update -publish -UI y -U UserName
   DLOCommandu -update -publish -UI y -P ProfileName
   ```

   The **y** indicates the ID number returned when the `add` command was run in step 3. Using an asterisk in place of `UserName` or `ProfileName` will publish the update to all users.

   When this command is executed, it will return a list of all users targeted for update. Users will be updated the next time the Desktop Agent application is started.

Note: For more information on the `-update` command and additional command options, see "-Update command" on page 219.

Related Topics

"DLO Command Line Interface Management Tools" on page 209

Running the Desktop Agent Upgrade Silently

Desktop Agents can be upgraded silently. During a silent upgrade, users will not be prompted to download and start the upgrade, but they will still be prompted to confirm that they want to actually perform the upgrade.

To run the Desktop Agent upgrade silently

1. From the Desktop Agent upgrade folder, open the `DLOAgnetUpdate_NBU.ini` file for editing.
2. Set `PromptUser=0`.
3. Save and close the file.
4. Run the upgrade using one of the methods described in "Updating the Desktop Agent" on page 53.

Upgrading from NetBackup Professional to DLO

The NetBackup Professional (NBUP) to Desktop Agent upgrade is only available for NBUP customers running version 3.51.20 or later. If you are not running 3.51.20, consider upgrading your NBUP server and clients before upgrading to the Desktop Agent.

This mechanism installs the Desktop Agent onto desktop computers that are currently running the NBUP client. You can remove the NBUP client when installing the Desktop Agent or leave the NBUP client installed and run both applications concurrently. These two options will appear as separate upgrades in the NBUP Console, so you can remove NBUP from some profiles and continue to run NBUP for other profiles.

The upgrade from NBUP to DLO requires two additional components that are distributed with the Desktop Agent install set:

- A DLO Client (Remove NBUP).VPK file that contains instructions and an executable to upgrade the system to DLO Tasks bar and remove NBUP at the same time.

- A DLO Client (Leave NBUP).VPK file that contains instructions and an executable to upgrade the system to DLO and leave NBUP installed but increment the version number so that it appears NBUP was upgraded.

To upgrade from NetBackup Professional to DLO

1. Contact Technical Support to receive the NBUP to Desktop Agent upgrade. The two files that you need are `DLOAgent_LeaveNBP.vpk` and `DLOAgent_RemoveNBP.vpk`.
2. From the NBUP server, or any computer with the NBUP console installed, launch the appropriate file; `DLOAgent_LeaveNBP.vpk` or `DLOAgent_RemoveNBP.vpk`. This will upload the upgrade package to the NBUP server. Repeat this process for the other `vpk` file to make both the leave and remove NBUP options available for selection in various profiles.
3. Create a folder entitled `DLOAgent` in `C:\Program Files\Veritas NetBackup Professional\Upgrades`, or in the appropriate location if you installed NBUP in a location other than the default.
4. Copy the entire contents of the `DLOAgent` share on the DLO Administration Server into the `DLOAgent` folder on the NBUP server.
5. Launch the NBUP Console.
6. Open the profile properties and select the **Upgrades** tab. Select the appropriate upgrade (leave NetBackup Professional or remove NetBackup Professional) and enable it by selecting the **Enable this upgrade** check box. Select the other options you want for this upgrade.
7. Repeat the steps through step 6 for each NBUP Profile you want to upgrade to DLO.
8. Follow the standard procedure for upgrading NBUP ("Check for upgrade now" in the console or refresh the client). See the *NetBackup Professional Administrator's Guide* for more information.
   If the Desktop Agent installation is successful, the NBUP version number in the NBUP administration console will change to 9.1.0.0 for computers that still have NetBackup Professional installed or 0.0.0.1 for computers on which NetBackup Professional was removed.

Upgrading the DLO Database on Remote SQL Server

If an existing installation is NetBackup 6.1 MP7, and if the DLO Database is installed on a remote SQL server, then follow this procedure to upgrade the DLO Database.

1. Before uninstalling the older version of DLO Database component on the database machine, ensure that the correct version of the new utility `DLODBRegcreateU.exe` (available in `x86/x64` version) is executed. The

`DLODBRegcreateU.exe` creates a registry key-value (string) `HKLM\Software\Symantec\Symantec DLO\DB\OldDLODBPath`

Note: You must have administrator privileges to run the `DLODBRegcreateU.exe` utility.

2 Next, uninstall the existing DLO Administration Server and the DLO Database component.

3 Upgrade to Symantec DLO by using the **Remote DLO Database Installation** option, during installation.

Note: If you have installed Symantec DLO 7.0 with remote database setup, then while upgrading to Symantec DLO 7.5, select the “Remote DLO Database Installation” option.
Similarly, for BE-DLO 2010 R3 with the remote database setup, select the “Remote DLO Database Installation” option while migrating to Symantec DLO 7.5.

Changing the License Key

This section explains how to change the license key.

To change the license key

Option 1:

1 On the main menu, select **Help > About Symantec Desktop and Laptop Option**.

2 Click **Change the License Key**.

3 Enter the DLO License Key.

4 Click **Change**.

Option 2:

1 On the main menu, select **Help > Change License Key**.

2 Enter the DLO License Key.

3 Click **Change**.

Option 3:

Use the command-line utility to add or change the license key.

1 Open the command prompt.

2 From the command line on the DLO Administration Server, change to the DLO installation directory.
Default installation directory:

Example `C:\Program Files\Symantec\Symantec DLO`

3 Run the following command:

```
DLOLicenseCLI.exe. <-list>|<-add> <license key
number>|<-delete>|
```

Option	Description
-list	Lists the installed license key
-add	Adds a license key
-delete	Deletes the license key

BackupExec (BE)-DLO Migration

Symantec DLO 7.5 is a unified and independent version of BackupExec (BE)-DLO and NetBackup (NBU)-DLO. BE-DLO users need to install Symantec DLO 7.5 on their systems, as the latest version of BE (BE 2012) does not contain DLO as an optional plug-in.

This section explains the procedure to migrate from BE-DLO to Symantec DLO 7.5.

Prerequisites

BackupExec (BE) customers need to have BE-DLO installed and BE DLO option enabled.

Migrating a Standalone BE-DLO to Symantec DLO

This section explains the procedure for migration, when all components are running on the same machine.

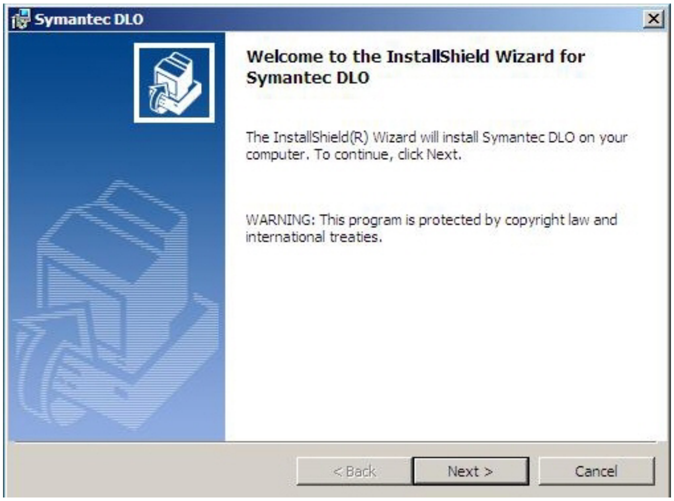
Note: While doing migration, make sure that the SQL service is running under domain admin credentials, else the database connection fails.

While doing migration, you can select BE SQL database instance (“XYZ”) or local SQL database instance, or local database instance shipped by Symantec DLO or any other pre-existing SQL database instance. After migration you will not be able to launch DLO from the BE console.

We recommend that you DO NOT select the “Remote DLO Database” option, to avoid loss of data.

To migrate from BE-DLO to Symantec DLO

1 Run the DLO 7.5 `setup.exe` on the BE-DLO installed machine to start the installation wizard.



Symantec DLO

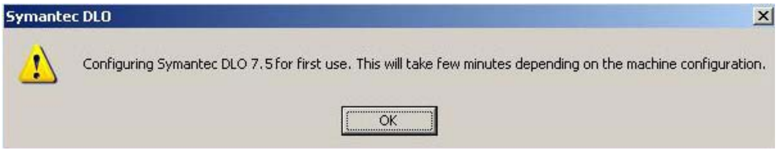
Welcome to the InstallShield Wizard for Symantec DLO

The InstallShield(R) Wizard will install Symantec DLO on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Figure 1-2 Installation wizard

2 When the migration is complete, cleanup of BE-DLO will start. Click **OK**.

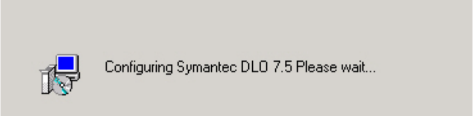


Symantec DLO

Configuring Symantec DLO 7.5 for first use. This will take few minutes depending on the machine configuration.

Figure 1-3 Cleanup message

3 Next the following message appears.



Configuring Symantec DLO 7.5 Please wait...

Figure 1-4 Cleanup in progress

4 When the cleanup of BE-DLO is complete, launch the Symantec DLO Administration Console.

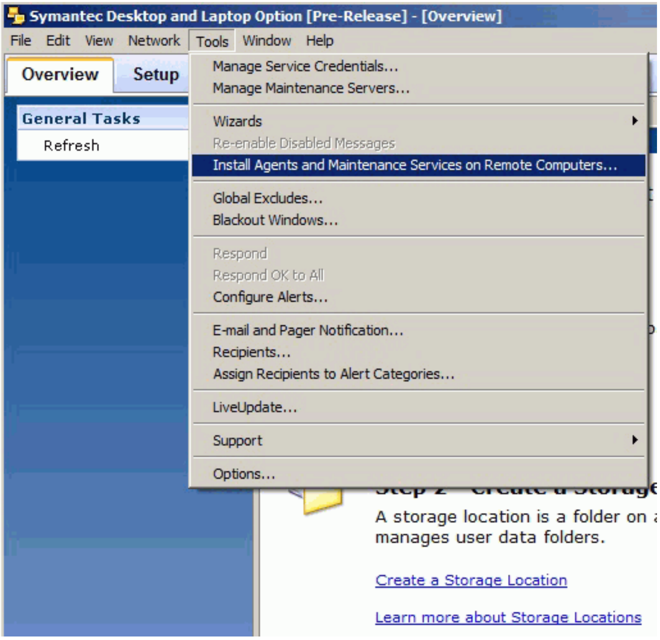
When the Symantec DLO Administration Server migration completes, check whether all the data that was created before migration is retained after migration.

Migrating BE-DLO Agent to Symantec DLO

You can use one of the following methods to migrate the BE-DLO Agent to Symantec DLO.

Option 1:

On **Tools**, select **Install Agents and Maintenance Services on Remote Computers** or access the remote machine where DLO Administration Server is installed and run the `setup.exe`. See “Procedure to Push Install Desktop Agent and DLO Maintenance Server” on page 32 for more information.


Symantec Desktop and Laptop Option [Pre-Release] - [Overview]
File
Edit
View
Network
Tools
Window
Help
Overview
Setup
General Tasks
Refresh
Manage Service Credentials...
Manage Maintenance Servers...
Wizards
Re-enable Disabled Messages
Install Agents and Maintenance Services on Remote Computers...
Global Excludes...
Blackout Windows...
Respond
Respond OK to All
Configure Alerts...
E-mail and Pager Notification...
Recipients...
Assign Recipients to Alert Categories...
LiveUpdate...
Support
Options...
Step 2 Create a Storage
Create a Storage Location
Learn more about Storage Locations

A storage location is a folder on a
manages user data folders.

Figure 1-5 Install Agents and Maintenance Services on Remote Computers option

Option 2:

Using the remote desktop connection, access the remote machine where DLO Agent is installed. Run the `setup.exe` that is within the DLO Agent folder.

```
C:\Program Files\Symantec\Symantec DLO\DLO Agent\setup.exe
```

Note: If BE-DLO Agent does not respond to the profile changes when it is not yet migrated to Symantec DLO version of Agent, then update BE-DLO Agent to Symantec DLO Agent.

To migrate BE-DLO Agent to Symantec DLO Agent through the `DLOcommandu.exe CLI` options, run the following commands in the same order:
Run `DLOcommandu.exe -ChangeDB`. See "-ChangeDB command" on page 213.
Run `DLOcommandu.exe -Update -add.` See "-Update command" on page 219.
Run `DLOcommandu.ext -Update -publish`. See "-Update command" on page 219.

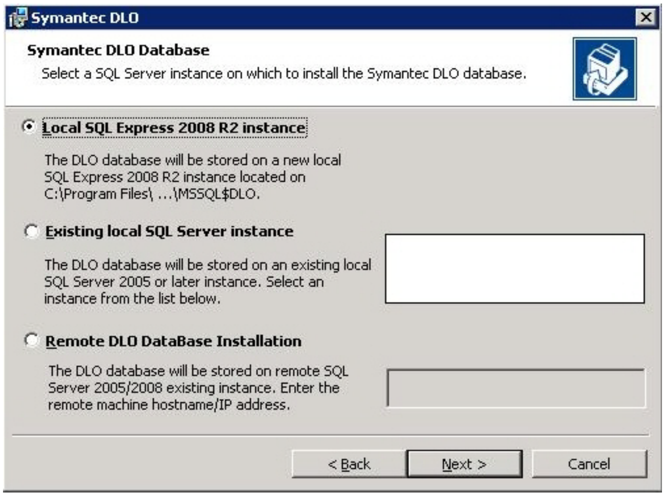
Migrating BE-DLO in a Distributed Configuration to Symantec DLO

To migrate from BE-DLO in a distributed configuration to Symantec DLO

1 Run the DLO 7.5 `setup.exe` on the BE-DLO installed machine to start the installation wizard.

2 When prompted to select the database, select the **Remote DLO Database Installation** option.

3 Enter the IP address or the host name of the machine where BE-DLO Database is installed.


Symantec DLO

Symantec DLO Database

Select a SQL Server instance on which to install the Symantec DLO database.

● Local SQL Express 2008 R2 instance

The DLO database will be stored on a new local SQL Express 2008 R2 instance located on C:\Program Files\ ...\MSSQL$DLO.

○ Existing local SQL Server instance

The DLO database will be stored on an existing local SQL Server 2005 or later instance. Select an instance from the list below.

○ Remote DLO DataBase Installation

The DLO database will be stored on remote SQL Server 2005/2008 existing instance. Enter the remote machine hostname/IP address.

Figure 1-6 Remote DLO Database Installation option

Note: This machine should have been selected as the remote database (DB) even while installing BE. Otherwise, this migration process will fail.

---

4 When the migration completes, cleanup of BE-DLO will start.

5 When the cleanup of BE-DLO completes, launch the Symantec DLO Administration Console.

When the Symantec DLO Administration Server migration completes, check whether all the data that was created before migration is retained after migration.

Migrating BE-DLO in a Cluster Environment to Symantec DLO

To migrate BE-DLO in cluster environment to Symantec DLO 7.5

1 Uncluster the BE-DLO cluster configuration by running the `Clusconfig.exe.` This utility exists in the installation directory: `C:\Program Files\Symantec\Symantec DLO\Clusconfig.exe.`

Note: Ensure that you complete this process, otherwise Symantec DLO installation will fail, and the following error message is displayed: "*Symantec DLO cannot be installed on the same machine as the Backup Exec DLO Console is clustered*".

---

2 During unclustering, ensure that you select the database to overwrite the data that was stored in the original install path (default - `C:\Program Files\Symantec\Backup Exec\Data`) with the data from the shared disk location (where DLO Database files are hosted.)

Note: Also, while unclustering BE-DLO by using the wizard, two pop-up dialogs appear:
To confirm if the data from the shared disk should be removed
To confirm if the data should be available to the local node
Click **Yes** in both the cases.
This will ensure that the database files are copied back to the original install path.

---

3 In case you do not select the database, then manually copy the `BE_DLO.mdf` and `BE_DLO.ldf` files from the shared disk folder to the new location where Symantec DLO is being installed. `C:\Program Files\Symantec\Symantec DLO\Data`.

4 Continue with the Symantec DLO installation.

5 When the installation completes, reconfigure the BE environment by running the `Clusconfig.exe` provided by BE.

6 Configure the Symantec DLO cluster environment by running the `DLOClusconfig.exe` provided by Symantec DLO. The executable file is located in `C:\Program Files\Symantec\Symantec DLO\DLOClusconfig.exe`. See "Configuring DLO on a Microsoft Cluster Server" on page 205 for more information.

Migrating BE-DLO Agent in Cluster Environment to Symantec DLO

On **Tools**, select **Install Agents and Maintenance Services on Remote Computers** or access the network share based on the virtual host name, and run the `setup.exe`. See "Procedure to Push Install Desktop Agent and DLO Maintenance Server" on page 32 for more information.

Chapter 2

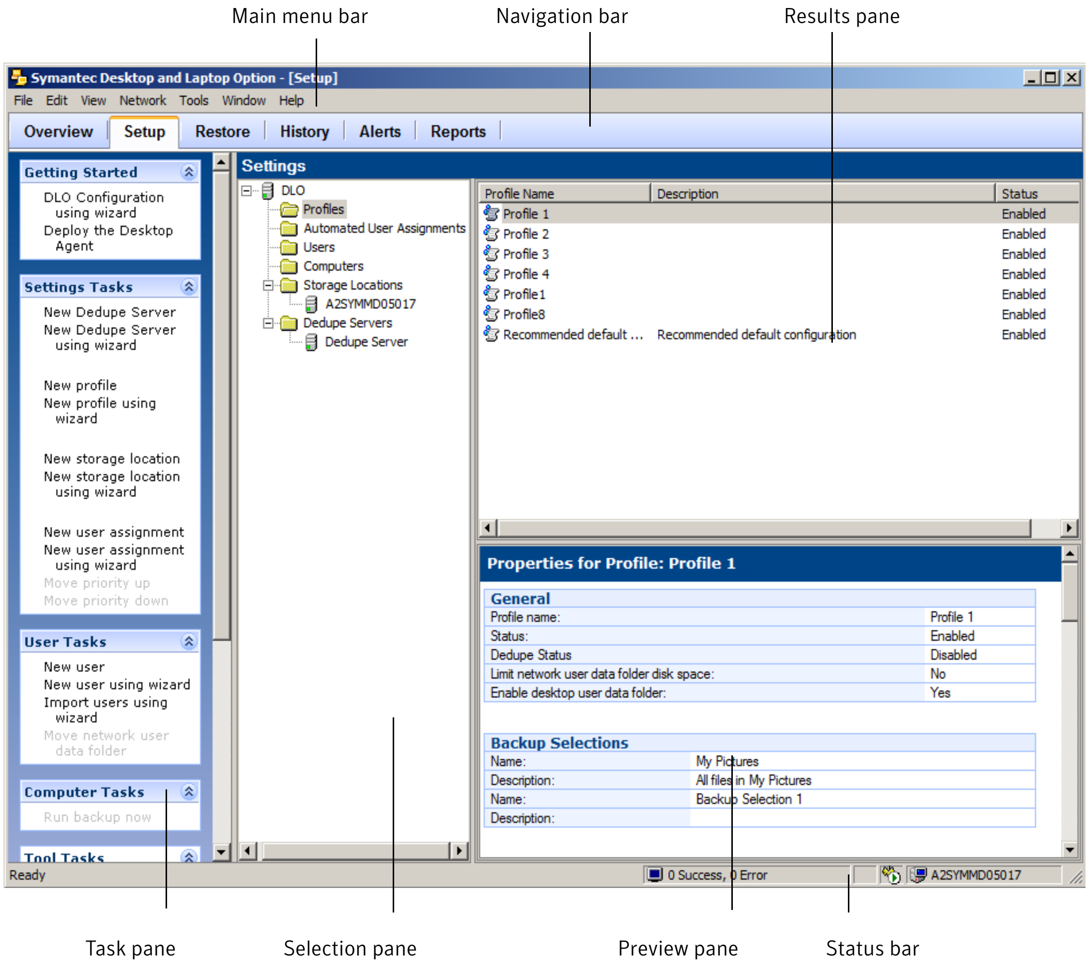
Configuring the Desktop and Laptop Option

This section contains the following topics:

Using the DLO Administration Console

When you launch DLO, the DLO Administration Console appears. From the console, you can configure DLO and manage desktop backup and restore operations.

Figure 2-1 Symantec DLO Administration Console



Profile Name	Description	Status
Profile 1		Enabled
Profile 2		Enabled
Profile 3		Enabled
Profile 4		Enabled
Profile1		Enabled
Profile8		Enabled
Recommended default ...	Recommended default configuration	Enabled

Properties for Profile: Profile 1

General

Profile name:	Profile 1
Status:	Enabled
Dedupe Status	Disabled
Limit network user data folder disk space:	No
Enable desktop user data folder:	Yes

Backup Selections

Name:	My Pictures
Description:	All files in My Pictures
Name:	Backup Selection 1
Description:	

Showing the Task Pane

The **User Tasks** pane (hereafter referred to as **Task pane**) appears on the left side of the DLO Administration Console. Actions can be initiated from the Task pane, and these actions vary with the selected view.

To show the Task pane

From the **View** menu, verify that **Task pane** is selected, or select it.

Using the DLO Overview View

The DLO Overview view provides two options: Getting Started view and System Summary view.

Getting Started View

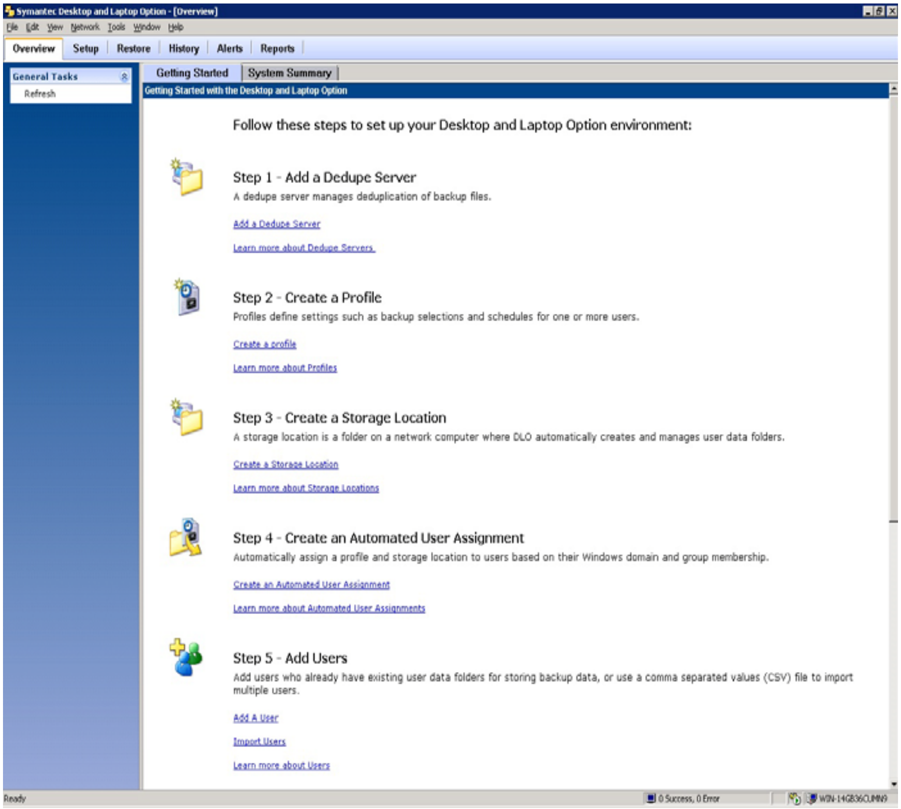
The Getting Started view provides convenient links to help you set up and manage DLO. From this page, you can easily perform the following tasks or access the help associated with these tasks.

- Add a Dedupe Server
- Create a Profile
- Create a Storage Location
- Create an Automated User Assignment
- Add Users
- Deploy the Desktop Agent
- Set Preferences and Default Settings
- Manage Alerts and Notifications
- Run Reports

To access the getting started view

1. On the DLO navigation bar, click **Overview**.
2. Click the **Getting Started** tab.

Figure 2-2 Symantec Getting Started view


Symantec Desktop and Laptop Option - [Overview]
File Edit View Network Tools Window Help
Overview
Setup
Restore
History
Alerts
Reports
General Tasks
Refresh
Getting Started
System Summary
Getting Started with the Desktop and Laptop Option
Ready
0 Success, 0 Error
WIN-14GB36CUMN9

Follow these steps to set up your Desktop and Laptop Option environment:

Step 1 - Add a Dedupe Server

A dedupe server manages deduplication of backup files.

Add a Dedupe Server

Learn more about Dedupe Servers

Step 2 - Create a Profile

Profiles define settings such as backup selections and schedules for one or more users.

Create a profile

Learn more about Profiles

Step 3 - Create a Storage Location

A storage location is a folder on a network computer where DLO automatically creates and manages user data folders.

Create a Storage Location

Learn more about Storage Locations

Step 4 - Create an Automated User Assignment

Automatically assign a profile and storage location to users based on their Windows domain and group membership.

Create an Automated User Assignment

Learn more about Automated User Assignments

Step 5 - Add Users

Add users who already have existing user data folders for storing backup data, or use a comma separated values (CSV) file to import multiple users.

Add A User

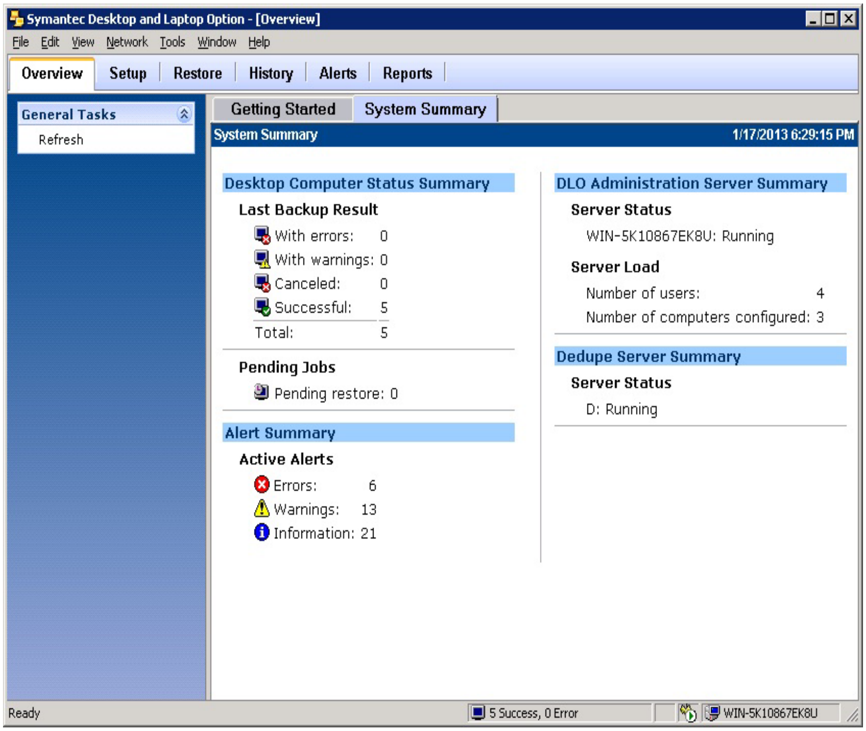
Import Users

Learn more about Users

System Summary view

The System Summary overview provides the DLO administrator with a summary of the current state of desktop backups, server status, and alerts.

Figure 2-3 DLO Overview System Summary view



System Summary 1/17/2013 6:29:15 PM

Desktop Computer Status Summary

Last Backup Result

With errors: 0
With warnings: 0
Canceled: 0
Successful: 5
Total: 5

Pending Jobs

Pending restore: 0

Alert Summary

Active Alerts

Errors: 6
Warnings: 13
Information: 21

DLO Administration Server Summary

Server Status

WIN-5K10867EK8U: Running

Server Load

Number of users: 4
Number of computers configured: 3

Dedupe Server Summary

Server Status

D: Running

5 Success, 0 Error

WIN-5K10867EK8U

To access the DLO system summary view

1 On the DLO navigation bar, click **Overview**.

2 Click the **System Summary** tab.

Table 2-1 shows the information available in the System Summary view.

Table 2-1 DLO System Summary options

Item	Description
Desktop Computer Status Summary	
Last Backup Result	Summarizes the completion status of the last operation performed on each computer protected by DLO. Totals are provided for the number of computers that completed the last job successfully, with errors, with warnings, or for which the last job was cancelled. ■ With Errors: The last operation was completed, but errors were generated. ■ With Warnings: The last operation was completed, but warnings were generated. ■ Canceled: The job was cancelled or refreshed by the user during the job. ■ Successful: The job was successfully completed without warnings or errors, and it was not cancelled or refreshed by the user during the job. **Note:** Errors take precedent over warnings, so if there are both errors and warnings, the last backup result displays **With Errors**.
Pending Jobs	Lists restore jobs requested by the DLO administrator that have not yet been run.
Alert Summary	
Active Alerts	Lists alerts that have not been cleared by the DLO administrators and have not yet been removed by the alert grooming process.
Server Summary	
Server Status	Lists the status of each DLO server. Server status can be Running or Stopped.
Server Load	Lists the number of desktops being protected by DLO and the total number of installed Desktop Agent users. These numbers may not be the same if some users are protecting multiple computers with DLO. Both online and offline users are counted.

Connecting to DLO on a Different DLO Administration Server

To connect to DLO on a different administration server, the user account needs to have full administrator rights to the server and it must also be a domain account.

To connect to DLO on a different DLO administration server

1 On the DLO Administration Console main menu, click **Network**, and select **Connect to DLO Administration Server**.

2 Select the appropriate options.

Server	Enter the name of the DLO Administration Server you want to connect to, or select a server from the drop-down menu.
User name	Type the user name for an account with administrator access to the DLO Administration Server.
Password	Type the password for this account.
Domain	Enter the domain for this account.

3 Click **OK**.

Related Topics
"Managing Administrator Accounts" on page 37

Using DLO Administration Server on VMware ESXi

DLO supports the administration server and the DLO database on VMware ESXi server 4.x and 5.0. Symantec recommends that you install the maintenance server on a physical system.

Installing the maintenance server on VMware may lead to performance issues.

For optimum performance, Symantec recommends that you locate the maintenance server in either of the following locations:

- On the same computer as the file server
- On the same network as the file server

Symantec recommends that the DLO Storage Locations and Dedupe Storage Locations should be located on a physical system and not in a VMware environment. Having DLO and Dedupe Storage Locations on VMware may lead to performance issues. Intensive Input/Output activities such as data migration or reporting may take a longer time than expected.

Ensure that your virtual environment meets all the hardware requirements and the recommendations that VMware specifies. Hardware that VMware does not support may cause unknown issues.

For example, DLO may not function correctly if your virtual machine hardware does not support VMware. See the *VMware documentation* for information on supported configuration.

Configuring DLO

For DLO to back up user data, you must set up these options in the following order:

1. Add a Dedupe Server, and configure the Dedupe Storage Pools and Dedupe Storage Locations. For more information, see "Adding Dedupe Server" on page 73.
2. Create a profile, which determines what files are backed up, when the files are backed up, and the level of interaction the desktop user has with the Desktop Agent. For more information, see "About DLO Profiles" on page 84.
3. Create Storage Locations where user data will be stored on the network. DLO requires an individual user data folder on the network for each desktop user. If Storage Locations are used, they will automatically create network user data folders for each new Desktop Agent user. If network data storage folders already exist for each user, they can be added to DLO individually or many users can be imported at one time using a list. For more information, see "About DLO Storage Locations" on page 121 and "Managing Desktop Agent Users" on page 149.
4. Create an Automated User Assignment to automatically assign a DLO Storage Location and profile to new users, or configure new users manually. For more information, see "About Automated User Assignments" on page 129.

Configure DLO Using the Configuration Wizard

You can set up DLO by using the configuration wizard or by setting options manually. The DLO configuration wizard provides a series of wizards that help you set up DLO in the correct order.

The configuration wizard appears when the DLO Administration Console is opened unless the **Always show this wizard at startup** box is not selected.

The configuration wizard can also be accessed as follows:

To access the configuration wizard

1. On the DLO navigation bar, click **Setup**.
2. On the **Task** pane under **Getting Started**, select **DLO Configuration using wizard**.

3 If you want the Configuration Wizard to display each time the DLO Administration Console is started, select **Always show this wizard at startup** check box.

Related Topics

"About DLO Storage Locations" on page 121

"About Automated User Assignments" on page 129

"Managing Desktop Agent Users" on page 149

Configuring Dedupe Server

Configure the Dedupe Server in the following order:

1 Add the Dedupe Server to the DLO Administration Server using the DLO Admin Console. For more information, see "Adding Dedupe Server" on page 73.

2 Create Dedupe Storage Pools. For more information, see "Adding Dedupe Storage Pool" on page 75.

3 Create Dedupe Storage Locations. For more information, see "Adding a Dedupe Storage Location" on page 76.

4 Assign the Dedupe Storage Locations to an existing or a newly created DLO Storage Location. For more information, see "Creating DLO Storage Locations" on page 123.

5 Create a Dedupe Enabled Profile. For more information, see "Creating a New Profile" on page 85.

6 Assign the Dedupe Enabled Profile and DLO Storage Location to the user.

Adding Dedupe Server

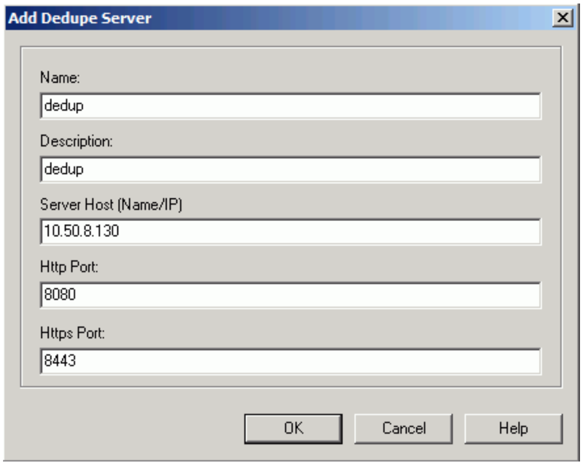
To add a Dedupe Server

1 Launch the Symantec DLO Admin console.

2 On the DLO navigation bar, click **Setup**.

3 In the **Settings** pane, right-click **Dedupe Server**, and select **New Dedupe Server** or **New Dedupe Server using Wizard**.
OR
In the **Task** pane, under **Setting Tasks**, click **New Dedupe Server** or **New Dedupe Server using Wizard**

The **Add Dedupe Server** window appears.



Name: dedup

Description: dedup

Server Host (Name/IP) 10.50.8.130

Http Port: 8080

Https Port: 8443

4 Enter the following details:

Field	Description
Name	Enter a name for the Dedupe Server. This is just for identification purpose.
Description	Enter a description to identify the Dedupe Server.
Server Host Name/IP	Enter the host name or IP address where the Dedupe Server is installed.
HTTP Port	Enter the HTTP port number of the Dedupe Server host. This port will be used by the DLO components to connect to the Dedupe Server. Default value is 8080.
HTTPS Port	Enter the HTTPS port number of the Dedupe Server host. This port will be used by the DLO components to connect to the Dedupe Server. Default value is 8443.

5 Click **OK**.

Note: After adding Dedupe Server, you can verify the status of the Dedupe Server. Type the following URLs in your browser.
http://<dedupeserver_ip_or_hostname>:8080
https://<dedupeserver_ip_or_hostname>:8443
If the Dedupe Server is active, then the following message is displayed: *Dedupe Server Status: (20159) Active.*
If there is no response from Dedupe Server, then it indicates that the Dedupe Server is not initialized, and one of the reasons could be that the database connection is down.

Adding Dedupe Storage Pool

Dedupe Storage Pool is a group of Dedupe Storage Locations across which deduplication is performed.

To add a new Dedupe Storage Pool

1 On the DLO navigation bar, click **Setup**.

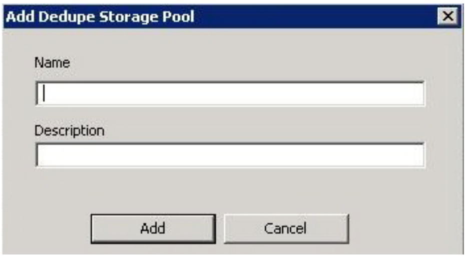
2 In the **Settings** pane, double-click the **Dedupe Server**.
The name of the Dedupe Server is displayed.

3 Right-click the Dedupe Server name and select **Manage**.

4 On the **Dedupe Storage Pool** tab, click **Add**.

5 In the **Add Dedupe Storage Pool** window, enter the **Name** and **Description** for the Dedupe Storage Pool.

Note: The name of the Dedupe Storage Pool is a just logical name used to identify the group of Dedupe Storage Locations.



6 Click **Add**.
The Dedupe Storage Pool is created, and a confirmation message appears.

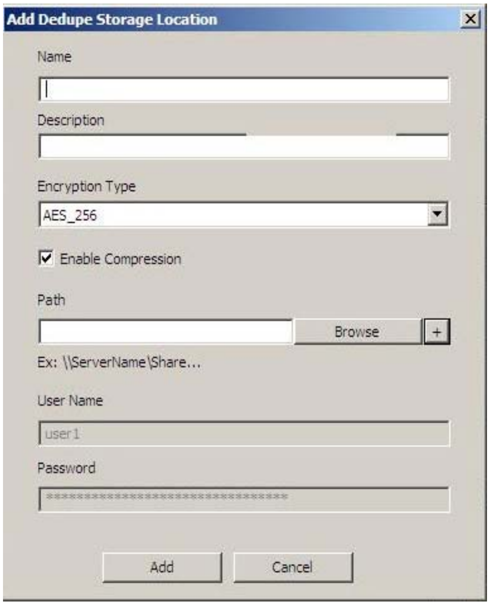
Adding a Dedupe Storage Location

The administrator defines an ID to identify the Dedupe Storage Locations. Multiple Dedupe Storage Locations cannot refer to the same DLO Storage Location. Multiple user groups can use the same Dedupe Storage Locations. For more information, see "About Dedupe Storage Locations" on page 128.

Note: At least one Dedupe Storage Pool must be created first before creating and adding a Dedupe Storage Location.
Before adding a Dedupe Storage Location, the DLO administrator should create a shared folder on the system where DLO Administration Console is installed, and grant access rights to specific users.

To add a Dedupe Storage Location

1. On the DLO navigation bar, click **Setup**.
2. In the **Settings** pane, double-click the **Dedupe Server**.
   The name of the Dedupe Server is displayed.
3. Right-click the Dedupe Server name and select **Manage**.
4. By default, the **Dedupe Storage Pool** tab is selected.
5. Select the **Dedupe Storage Location** tab.
6. Click **Add**.
7. In the **Add Dedupe Storage Location** dialog, enter the following details:



Add Dedupe Storage Location

Name

Description

Encryption Type
AES_256

☑ Enable Compression

Path

Ex: \\ServerName\Share...

User Name
user1

Password
****

Field	Description
Name	Enter a name for the Dedupe Storage Location. Ensure that the name does not contain any special characters, including blank space.
Description	Enter the description to identify this Dedupe Storage Location.
Encryption Type	Select the encryption type from the drop-down list. AES_256 is recommended. This encryption algorithm is to used to encrypt the data in the Dedupe Storage Locations.
Enable Compression	This option is selected by default. Clear the check box to disable compression. If enabled, data in the Dedupe Storage Locations will be stored in compressed format.

Field	Description
Path	Enter the path of the existing shared folder or click **Browse** and locate the required folder. Make sure that the user creating the Dedupe Storage Location has full control to the folder and subfolders of this shared folder. To set the permissions: 1 Right-click the shared folder and select **Properties**. 2 Select the **Sharing** and **Security** tabs, and provide the permissions. You can also create a shared folder as follows: ■ Click the '**+**' icon. ■ Enter the machine name and the path of the folder or click **Browse** to locate the machine and folder. ■ Click **Create**. The folder path is displayed in this field. Note: This path should not be the same as the NUDF folder path of the DLO Storage Location. For more information, see "About Dedupe Storage Locations" on page 128.
User Name	Enter the name of the domain user that has read-write (RW) access to the shared folder. This user name has to be a non- administrator account.
Password	Enter the password.

8 Click **Add**.
A confirmation message appears, indicating that the Dedupe Storage Location is created successfully.

Note: After configuring the Dedupe Server, creating Dedupe Storage Pools, and Dedupe Storage Locations, you can create new DLO Storage Locations and assign these Dedupe Storage Locations. For existing DLO Storage Locations, you should first assign the specific Dedupe Storage Locations and then enable Dedupe for that profile. For more information, see "Creating DLO Storage Locations" on page 123.

Modifying Dedupe Server

You may want to change the port numbers of the Dedupe Server, or when the Dedupe Server is not working, you need to set up another Dedupe Server. In such cases, modify the configuration details of the Dedupe Server.

To modify the Dedupe Server

1. On the DLO navigation bar, click **Setup**.
2. In the **Settings** pane, double-click the **Dedupe Server**.
   The name of the Dedupe Server is displayed.
3. Right-click the Dedupe Server name and select **Edit**.
4. Change the details as required.
5. Click **OK**.

Modifying a Dedupe Storage Pool

You can modify the properties of a Dedupe Storage Pool only when the Dedupe Server is in maintenance mode. Backup and restore jobs will stop during the maintenance period.

To modify a Dedupe Storage Pool

1. On the DLO navigation bar, click **Setup**.
2. In the **Settings** pane, double-click the **Dedupe Server**.
   The name of the Dedupe Server is displayed.
3. Right-click the Dedupe Server name and select **Manage**.
4. Select the **System** tab.
5. To set the maintenance schedule, enter the time in the **Timeout** field.
6. Click **Start**.
7. On the **Dedupe Storage Pool** tab, select the specific row from the list and click **Modify**.
8. Change the properties as required.
9. Click **Modify**.
   The properties of the Dedupe Storage Pool are updated.

Viewing Dedupe Storage Pool Statistics

Dedupe Storage Pool statistics is updated when the deduped data size is more than 100 MB or when the Desktop Agent is closed and launched again.

To view the Dedupe Storage Pool statistics

1. Follow **steps 1 to 3** as explained in the section "Modifying a Dedupe Storage Pool" on page 79.
2. On the **Dedupe Storage Pool** tab, select the required row.
3. Click **Statistics**.
   The total data size, storage space used on the disk, and the deduplication savings are displayed.

Modifying a Dedupe Storage Location

You can modify the properties of a Dedupe Storage Location only when the Dedupe Server is in maintenance mode. Backup and restore jobs will stop during the maintenance period.

Note: You can change the storage path for a Dedupe Storage Location. After changing the path, you should move all the data in the previous path to the new storage path.

To modify a Dedupe Storage Location

1. On the DLO navigation bar, click **Setup**.
2. In the **Settings** pane, double-click the **Dedupe Server**.
   The name of the Dedupe Server is displayed.
3. Right-click the Dedupe Server name and select **Manage**.
4. Select the **System** tab.
5. To set the maintenance schedule, enter the time in the **Timeout** field.
6. Click **Start**.
7. On the **Dedupe Storage Location** tab, select the specific row from the list.
8. Click **Modify**.
9. In the **Modify Dedupe Storage Location** dialog, change the required values.
10. Click **Modify**.
    The properties of the Dedupe Storage Location are updated.

Changing Credentials

You should change the credentials when the password used to create the Dedupe Storage Location has been changed, or when the user account has expired.

To change the credentials of users

1. On the DLO navigation bar, click **Setup**.
2. In the **Settings** pane, double-click the **Dedupe Server**.
   The name of the Dedupe Server is displayed.
3. Right-click the Dedupe Server name and select **Manage**.
4. Select the **System** tab.
5. To set the maintenance schedule, enter the time in the **Timeout** field.
6. Click **Start**.
7. On the **Dedupe Storage Location** tab, click **Change Credentials**.
8. Change the user name and password.
   Click **OK**.

Deleting a Dedupe Storage Location

You can delete the Dedupe Storage Location only when the Dedupe Server is in maintenance mode. Backup and restore jobs will stop during the maintenance period.

Note: As long as the Dedupe Storage Location is active (listed in the DLO Administration Console), admin should not delete any data in the Dedupe Storage Location. Deleting this data will lead to corrupted backups for the users of the Dedupe Storage Pool to which this Dedupe Storage Location belongs. One of the scenarios where the administrator would delete the data in the Dedupe Storage Location is when a specific user is deleted or migrated to some other Dedupe Storage Pool. Even in this scenario, the administrator **should not delete the data within the Dedupe Storage Location**.

Note: A Dedupe Storage Location **cannot** be deleted if it is being used by any of the DLO Storage Locations.

To delete a Dedupe Storage Location

1. On the DLO navigation bar, click **Setup**.

2 In the **Settings** pane, double-click the **Dedupe Server**.
The name of the Dedupe Server is displayed.

3 Right-click the Dedupe Server name and select **Manage**.

4 Select the **System** tab.

5 To set the maintenance schedule, enter the time in the **Timeout** field.

6 Click **Start**.

7 On the **Dedupe Storage Location** tab, select the specific row from the list.

8 Click **Delete**.

9 In the confirmation dialog, click **Yes**.
The Dedupe Storage Location is deleted.

Deleting Dedupe Server

While deleting the Dedupe Server, ensure that the Dedupe Storage Location is not associated with any DLO Storage Location.

1 On the DLO navigation bar, click **Setup**.

2 In the **Settings** pane, double-click the **Dedupe Server**.
The name of the Dedupe Server is displayed.

3 Right-click the Dedupe Server name and select **Delete**.

4 A confirmation prompt appears, asking you to confirm the delete operation.

5 Click **Yes**.
The Dedupe Server is deleted from the DLO configuration.

Dedupe Server Maintenance

The administrator can modify the properties of the Dedupe components only when the Dedupe Server is in the maintenance mode. The administrator can perform configuration changes, maintenance operations, and add new admin users.

Note: Backup or restore operations cannot be performed during the maintenance mode.

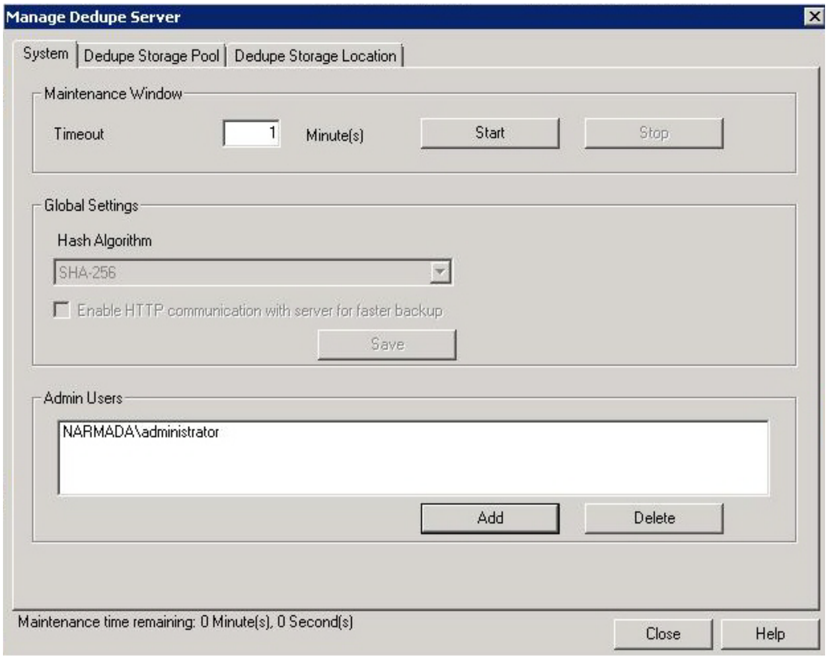
To set the maintenance schedule

1 On the DLO navigation bar, click **Setup**.

2 In the **Settings** pane, double-click the **Dedupe Server**.
The name of the Dedupe Server is displayed.

3 Right-click the Dedupe Server name and select **Manage**.

4 Select the **System** tab.



Timeout: 1 Minute(s)

Hash Algorithm: SHA-256

□ Enable HTTP communication with server for faster backup

NARMADA\administrator

Maintenance time remaining: 0 Minute(s), 0 Second(s)

5 To set the maintenance schedule, enter the time in the **Timeout** field.

6 Click **Start**.

7 To change the configuration, select the required encryption type from the **Hash Algorithm** field.

8 **Enable HTTP communication to server for faster backup**: Select this check box if required.

9 To add admin users, click **Add**.

10 In the **Add Admin Users** window, enter the user name in this format: `domain name\user name`.

11 Click **Add**.

A confirmation message appears, indicating that the operation was successful.

Command Line Option to Schedule Maintenance Window

The `DdAdminCU.exe` command is used to schedule, stop, or check the status of a Maintenance Window.

Syntax

Schedule the Maintenance Window

```
DdAdminCU.exe -ScheduleMaintenance |-SCM <DedupeServerName>
<HTTPS PortNumber> <Maintenance Timeout Value> [-i]
```

Stop Maintenance Window

```
DdAdminCU.exe -StopMaintenance |-STM <DedupeServerName> <HTTPS
PortNumber> [-i]
```

Check the status of Maintenance Window

```
DdAdminCU.exe -IsMaintenanceActive |-IMA <DedupeServerName>
|<HTTPS PortNumber> [-i]
```

Command Options

Option	Description
-ScheduleMaintenance |-SCM	Schedules the Maintenance Window
<Dedupe Server Name>	Name of the Dedupe Server. Default: localhost
<HTTPS Port Number>	Port Number of the Dedupe Server. Default: 8443
<Maintenance Timeout Value>	Duration of the schedule Default: 9999 minutes
-StopMaintenance|-STM	Stops the Maintenance Window
-IsMaintenanceActive|-IMA	Checks the status of the Maintenance Window
-i	The command is run in interactive mode Default: silent mode

About DLO Profiles

Profiles are used to customize settings for specific groups of similar users. For example, a group of highly technical users may require the option to modify the backup selections and schedules while less experienced users may require a fully automated backup service.

In a profile, you can set the following:

- Backup file and folder selections
- Desktop and network user data folder storage limits
- Backup schedules
- The desktop user’s level of interaction with the Desktop Agent
- Logging options
- Network bandwidth usage options for backup and restore operations
- Dedupe backup

You cannot modify settings for individual Desktop Agent users from the DLO Administration Console unless an individual user is the only user assigned to a profile. However, you can grant permission to Desktop Agent users to modify their own settings.

Creating a New Profile

New profiles can be created to meet the specific needs of desktop users, and to support the existing IT environment.

To create a new profile

1. On the DLO navigation bar, click **Setup**.
2. In the **Settings** pane, click **Profiles**.
3. In the **Task** pane under **Settings Tasks**, click **New Profile**.
4. From the **General** tab in the **New Profile** dialog box, select the appropriate options. Table 2-2 describes the fields.

Table 2-2 General Profile properties

Item	Description
Profile Name	Type the name of the new profile that you want to create. The profile name cannot contain any of the following characters: \”@#$%^&*()=+|/{}[]’
Description	Type a description for the profile.
Enable Profile	Profiles are enabled by default. To disable the profile, clear this check box.

Table 2-2 General Profile properties (continued)

Item	Description
Enable Dedupe	This option is selected by default. **Note:** When Dedupe is enabled, all deduped backups is handled by the Dedupe engine, and data is stored in the Dedupe Storage Locations. In case you have already created a profile, you can enable Dedupe when you choose to modify the profile. **Note:** When Dedupe is enabled, DLO-based Encryption or Compression options cannot be configured for this profile. However, Dedupe-based encryption and compression will be applicable to the data. **Note:** To enable Dedupe backup for a profile, the Dedupe Server must be installed and added to the DLO configuration. Otherwise, the **Enable Dedupe** option is disabled in the **Profile Properties** window. For more information, see "Configuring Dedupe Server" on page 73.
Storage Limits	
Limit network user data folder to (MB)	Limits the disk space available on the network to store DLO backup files and type the amount of space you want to use for storage.

Table 2-2 General Profile properties (continued)

Item	Description
Enable desktop user data folder	Enables the use of the desktop user data folder. When **Enable desktop user data folder** is selected, files are copied to the desktop user data folder first, and then they are copied to the network user data folder from the desktop user data folder. This is true even when DLO is configured to keep zero revisions in the desktop user data folder. When **Enable desktop user data folder** is not selected, files are copied straight to the network user data folder from the original location. *Advantages of enabling the desktop user data folder*: ■ Offline protection is provided because revisions can be stored locally as well as on the network. ■ Because files are more quickly saved to the local computer than to the network, the time a file is held open for backup is reduced. *Advantages of disabling the desktop user data folder*: ■ If local revisions are not required, this option will prevent backup files from being stored in the desktop user data folder. No revisions are saved in the desktop user data folder even if backup selections specify that a certain number of revisions should be stored locally. ■ Works well for desktop users with very limited disk space. ■ When the DLO administrator disables the desktop user data folder or the number of revisions retained in this folder is set to zero, DLO will still create empty place holders in the desktop user data folder. The place holders can be seen in the Desktop User data folder, but contain no data. They indicate which files and folders have been backed up and saved to the network user data folder.

Table 2-2 General Profile properties (continued)

Item	Description
Limit desktop user data folder to	Limits the disk space available to store DLO backup files. **A percentage of the total disk space (%)** Select this option and enter a percentage to limit the amount of disk space used for storing backup files in the desktop user data folder to a percentage of the local drive. **A size (MB)** Select this option and enter a size in MB to limit the desktop user data folder to a specific maximum size. **Note:** While limiting available disk space for the desktop user data folder can prevent overloading of the desktop hard drive, backups can fail to run if the desktop user data folder space limit is reached.
My Default Desktop User Data Folder Path	The default desktop user data folder path is the user's local application data path. To override this location for newly deployed Agents, select the **Override default desktop user data folder path** check box, and type the new path.

5 On the **Backup Throttling** tab, select the **Basic Throttling** tab.

Note: These options are disabled if no Agents with DLO versions prior to 6.1 MP3 are registered.

Select the appropriate options as described in Table 2-3.

Table 2-3 Basic Throttling Profile Properties

Item	Description
Limit network bandwidth usage to (KB/sec)	Limiting the bandwidth for DLO data transfer is a means to manage the trade-off between backup speed vs. the impact of backups on the local computer, network, and server. The default limit is meant to be a conservative setting to minimize the impact of backups, but many factors come into play, such as network speed, connection type, the amount of data backed up and the total number of computers backing up to DLO. If computer performance is not impacted, but DLO data transfer is slow, a higher bandwidth setting may be more suitable. If computer performance is noticeably impacted during backups, a lower value will reduce the impact of backups on computer performance, but backups will take longer to complete. Select the **Limit network bandwidth usage to (KB/sec)** check box, and enter a specific maximum bandwidth setting to control the rate at which data is sent to the network user data folder. Data transfer is only limited when data is written to the network user data folder, not when it is written to the desktop user data folder. Data transfer is not limited during the incremental backup of Outlook PST files or Lotus Notes NSF files.

Table 2-3 Basic Throttling Profile Properties (continued)

Item	Description
Yield bandwidth to other programs	Enables DLO to reduce data transfer over the network when other applications on the desktop computer are transferring data. DLO automatically resumes normal data transfer rates when other applications are not using this resource. The yield bandwidth option monitors network traffic on the desktop computer. If DLO is using more than 90% of the total current traffic, DLO is not throttled. When DLO traffic drops below 90% of the total network traffic on the desktop, and total traffic is over 60% of the maximum traffic seen on the connection, then DLO throttles itself to use only the otherwise unused portion of the connection. For example, if there was 70% total usage, DLO will throttle itself to 30% of maximum. **Note:** Selecting this option can improve system performance when other network-intensive applications are running at the same time. Data transfer is only limited when data is written to the network user data folder, not when it is written to the desktop user data folder.

6 On the **Backup Throttling** tab, select the **Enhanced Throttling** tab.

7 Select the appropriate options for each of the three network bandwidth categories: **Low bandwidth setting**, **Medium bandwidth setting**, and **High bandwidth setting**.

Table 2-4 describes the options.

Table 2-4 Enhanced throttling properties for bandwidth on backups

Item	Description
Bandwidth range	Enter a bandwidth range for this category in KB/sec.
No network throttling	Select this option to disable all network throttling for this category.
Limit network bandwidth usage to	Select this option and then select a specific percent of available network bandwidth to control the rate at which data is sent to the network user data folder.
Limit network bandwidth statically	

Table 2-4 Enhanced throttling properties for bandwidth on backups (continued)

Item	Description
Limit usage to	Select this option and enter a specific maximum bandwidth setting (in KB/sec) to control the rate at which data is sent to the network user data folder. Data transfer is only limited when data is written to the network user data folder, not when it is written to the desktop user data folder. Data transfer is not limited during the incremental backup of Outlook PST files or Lotus Notes NSF files.
Yield bandwidth to other programs	This option enables DLO to reduce data transfer over the network when other applications on the desktop computer are transferring data. DLO resumes normal data transfer rates when other applications are not using this resource.
Disable network backup	Select this option to not use the network for backups. This option is generally used for the low bandwidth network category. When network backups are disabled, files do not get backed up to the network user data folder. However, backups to the local user data folder still occur.

8 On the **Restore Throttling** tab, select the appropriate options for each of the three network bandwidth categories: **Low bandwidth setting**, **Medium bandwidth setting**, and **High bandwidth setting**.

Table 2-5 Restore throttling properties

Item	Description
Bandwidth range	Enter a bandwidth range for this category in KB/sec.
No network throttling	Select this option to disable all network throttling for this category.
Limit network bandwidth usage to	Select this option and then select a specific percent of available network bandwidth to control the rate at which data is sent to the network user data folder.
Limit network bandwidth statically	

Table 2-5 Restore throttling properties

Item	Description
Limit usage to	Select this option and enter a specific maximum bandwidth setting (in KB/sec) to control the rate at which data is sent to the network user data folder. Data transfer is only limited when data is written to the network user data folder, not when it is written to the desktop user data folder. Data transfer is not limited during the incremental backup of Outlook PST files or Lotus Notes NSF files.
Yield bandwidth to other programs	This option enables DLO to reduce data transfer over the network when other applications on the desktop computer are transferring data. DLO resumes normal data transfer rates when other applications are not using this resource.

9 From the **Backup Selections** tab, select the backup selections that you want to apply to users of this profile.

You can add, modify, and delete backup selections for a profile from this dialog box. When a new backup selection is created, it is available for selection in all profiles. Changes made to a backup selection in one profile will impact all other profiles that use the backup selection. Similarly, when a backup selection is deleted, the change impacts all profiles that use the backup selection. For more information, see “About Backup Selections” on page 102.

10 From the **User Settings** tab, select the appropriate options.

Note: When a user is given the option to change any of the following settings, the new settings will apply only to that user and not to other users assigned to the same profile.

Table 2-6 describes the options.

Table 2-6 Profile User Settings options

Item	Description
Desktop Agent display settings	Select one of the following options to determine the desktop user's level of interaction with the Desktop Agent: ■ Display the complete interface. Select this option to enable desktop users to access all Desktop Agent options. ■ Display only the status. Select this option to enable desktop users to view the status of backup jobs. With this option, desktop users cannot change settings for the Desktop Agent or access any options other than the status. Desktop users can right-click the system tray icon to open the status view or exit the program. ■ Display only the system tray icon. Select this option to display the Desktop Agent icon in the system tray in the lower right corner of the screen. Desktop users can right-click the system tray icon to exit the program. ■ Do not display anything. Select this option to run the Desktop Agent in the background. The desktop user cannot view the Desktop Agent.
Allow Users to	Select the options below to enable desktop users to configure the following features of the Desktop Agent. These options are only available if **Display the complete interface** was selected above.
Restore data	When selected, users in this profile can restore their backed up files. For more information, see "Restoring Files Using the Desktop Agent" on page 286.

Table 2-6 Profile User Settings options (continued)

Item	Description
Add user-defined backup selections	Enables users in this profile to create and modify backup selections. This option does not allow users to modify backup selections made by the DLO administrator in the profile. **Note:** With this option selected, users can add a backup selection that will back up a folder that is excluded from the profile backup selections. The only way to prevent users in a profile from backing up a specific folder is to deselect this option. For more information, see "About Backup Selections" on page 102, "Modifying Backup Selections in the Standard View" on page 258 or "Modifying Backup Selections in the Advanced View" on page 264.
Modify profile backup selections	Enables users in this profile to modify backup selections created by the DLO administrator for the profile. For more information, see "About Backup Selections" on page 102 or "Modifying Backup Selections in the Advanced View" on page 264.
Customize backup selection revision policy settings	Enables users in this profile to modify the revision policy settings. Users cannot change these settings if this option is not selected. For more information, see "Backup Selection Revision Control Dialog Box" on page 261.
Change backup selection encryption settings	Enables users in this profile to turn encryption of backup files on or off. For more information, see "Backup Selection options" on page 111.
Change backup selection compression settings	Enables users in this profile to turn compression of backup files on or off. For more information, see "Backup Selection options" on page 111.
Customize profile logging settings	Enables users in this profile to customize profile logging settings. For more information, see "Setting Customized Options" on page 271.
Customize profile e-mail settings	Enables users in this profile to customize mail settings in the profile. For more information, see "Setting Customized Options" on page 271.
Move local user data folder	Enables users in this profile to move the local user data folder to a new location. For more information, see "Moving the Desktop User Data Folder" on page 273.

Table 2-6 Profile User Settings options (continued)

Item	Description
Change groom policy settings	Enables users in this profile to customize grooming settings. For more information, see "Setting Customized Options" on page 271.
Synchronize files	Enables users in this profile to synchronize data across all of their computers that run the Desktop Agent. For more information, see "Synchronizing Desktop User Data" on page 277.
Customize local disk quota	Enables users in this profile to limit the amount of disk space that can be used to store backup files in the desktop user data folder. For more information, see "Setting Customized Options" on page 271.
Modify backup schedule	Enables users in this profile to modify the schedule on which their files are backed up. For more information, see "Changing Backup Job Schedule Options" on page 269.
Customize connection policies	Enables users in this profile to customize connected based policies. For more information, see"Customizing Connection Policies" on page 274.
Cancel scheduled or manual jobs	Enables users in this profile to cancel both scheduled and manually initiated jobs. Scheduled jobs will run again at the next scheduled time. Manual jobs must be restarted manually. For more information, see "Suspending or Cancelling a Job" on page 283.
Suspend jobs	Enables users in this profile to suspend jobs for a specified amount of time. For more information, see "Suspending or Cancelling a Job" on page 283.
Disable Desktop Agent	Enables users in this profile to disable the Desktop Agent from the tray icon. They will also have the ability to re-enable the Desktop Agent once it has been disabled.
Work Offline	Enables users in this profile to set the Desktop Agent to work offline. For more information, see "Changing your Connection Status" on page 251.

Table 2-6 Profile User Settings options (continued)

Item	Description
Save encrypted passwords used by DLO	Allows users to automatically authenticate to the media server or storage location in the event of an authentication failure. This could happen, for example, when the desktop user logs in using a local or cross-domain account. Keeping this option unchecked will cause DLO to prompt the user to enter a password each time DLO authenticates to a DLO resource while using an account which requires domain credentials in order to authenticate to a DLO resource.
Suppress errors and warnings	Prevents error and warning messages from being displayed when a user is not interacting with the Desktop Agent.
When user goes offline, automatically go back online after	Enter the time after which a user will automatically go back online after they have manually placed the Desktop Agent in an offline state.
When user suspends a job or disables the Desktop Agent, automatically resume or enable after	Enter the time after which a job will be resumed or the Desktop Agent enabled after the user suspends a job or disables the Desktop Agent.

11 On the **Schedule** tab, select the appropriate options. Table 2-7 describes the options.

Table 2-7 Profile Schedule options

Item	Description
Run backups	
Whenever a file changes	Select this option to back up files whenever they change. On NTFS drives, backups will occur automatically whenever a file changes. For FAT drives, you must enter a backup interval in the **Back up changed files every** field.
According to a schedule	Select this option to back up files according to a customized schedule. Click **Edit schedule** to configure the backup schedule. The backup schedule is configured in step 12.
When initiated by the user	Select this option to enable desktop users to determine when to back up their files.

Item	Description
Logout/Restart/Shutdown options	
Do nothing	Select this option to proceed with a logout, restart or shutdown even when there are files that require backup. **Note:** If a job is already running, a prompt asks if the user would like to log out, restart or shut down when the job is complete.
Prompt user to run job	Select this option to display a prompt and ask the user if a backup should be run before proceeding with the logout, restart, or shutdown. **Note:** If a job is already running, a prompt asks if the job should be cancelled before proceeding with the logout, restart or shutdown.
Run job immediately	Select this option to back up waiting files without prompting before proceeding with a logout, restart or shutdown. **Note:** If a job is already running, a prompt asks if the job should be cancelled before proceeding with the logout, restart or shutdown.
Run job at next login	Select this option to run a backup job when the user logs in the next time. **Note:** If a job is already running, a prompt asks if the job should be cancelled before proceeding with the logout, restart, or shutdown.
Run as scheduled	Select this option to run the backup job according to a schedule when the user is logged out. **Note:** If a job is already running, a prompt asks if the job should be cancelled before proceeding with the logout, restart, or shutdown.

12 If you selected **Edit schedule** in the previous step, select the appropriate options, and click **OK**. Table 2-8 describes the options.

Table 2-8 Backup Schedule tab options

Item	Description
Run on these days	Select the days on which you want to back up files.

Table 2-8 Backup Schedule tab options (continued)

Item	Description
Run once at	Select this option to run a single backup on the days you selected at the time specified.
Run every	Select this option to run backups at the specified time interval on the days you selected.
From	If you selected **Run every**, select the beginning of the time interval over which you want backups to begin.
Until	If you selected **Run every**, select the end of the time interval over which you want backups to begin. **Note:** This field specifies the end of the time period within which backups will begin. If a backup is in progress at this time, it will continue to run to completion.
Start backup jobs over a period of	Select this option to stagger start times for backup jobs. Rather than starting all backup jobs at exactly the time indicated, DLO will distribute the start times over the specified interval to better distribute the demands on the server and network.

13 Click the **Options** tab and select the appropriate options.

Note: Events such as file copies, file grooms, errors and warnings are logged by DLO and can be viewed as discussed in “Monitoring Alerts on the DLO Administration Console” on page 177.

Table 2-9 describes the options.

Table 2-9 Additional Profile tab options

Item	Description
Log file maintenance	
Keep log files for a minimum of (days)	Specify the minimum number of days to keep log files. Log files will not be deleted until they are at least as old as specified. **Note:** Log files will not be deleted until their combined size exceeds the setting for the combined size of all log files, which is discussed below.

Table 2-9 Additional Profile tab options (continued)

Item	Description
After minimum number of days, delete oldest log files when combined size exceeds (MB)	Enter the maximum combined size of all log files to be retained before the oldest log files are deleted. **Note:** You may have more than the specified number of MB of log files stored if none of the log files is as old as specified in the **Keep log files for a minimum of (days)** setting.
Logging options	
Log groom messages	Select this check box to create logs for grooming operations.
Log information messages for backup	Select this check box to create logs for all backup operations.
Log warning messages	Select this check box to create logs for all operations that generate warnings.
Mail options	
Enable incremental backups of Outlook PST files	Select this check box to enable incremental backups of Microsoft Outlook Personal Folder (PST) files. Incremental backups must be enabled to allow PST files to be backed up while they are open. If this option is not selected, PST files that are configured in Outlook will be fully backed up each time the PST file is saved, which generally occurs when Outlook is closed. When Outlook PST files are backed up incrementally, only one revision is maintained regardless of the number of revisions set in the backup selection. **Note:** Microsoft Outlook must be your default mail application for DLO to perform incremental backups of PST files. **Note:** Synchronized files cannot be backed up incrementally. For more information, see “Backing up Outlook PST Files Incrementally” on page 265.
Enable VSS Backups of Outlook PST Files after every 30 minutes	Select this check box to enable VSS backups of Microsoft Outlook Personal Folder (PST) files. **Note:** This feature is applicable to 6.1 MP5 or later versions of DLO Agent.

Table 2-9 Additional Profile tab options (continued)

Item	Description
Enable incremental backups of Lotus Notes e-mail files	Select this check box to enable incremental backups of Lotus Notes e-mail files. Additional configuration may be necessary. For more information, see “Backing up Lotus Notes NSF Files Incrementally” on page 267. When Lotus Notes NSF files are backed up incrementally, only one revision is maintained regardless of the number of revisions set in the backup selection.

14 Click the **Connection Policies** tab to disable or limit backups for specific connection types. Click **Add** to create a new connection policy. Table 2-10 describes the options available to configure the policy.

Table 2-10 Connection Policies tab Add button options

Item	Description
Connection Type	
Dialup	Select this option to limit or disable backups when using a dialup connection.
IP address range	Select this option to limit or disable backups for a specific IP address range. Specify whether you want the connection policy to apply to computers that **are** or **are not** in the IP address range you specify. Select IPv6 or IPv4 and enter the IP address range for the connection policy. **Note:** IPv6 addresses are only supported on Windows XP and later operating systems and will not be enforced for Desktop Agents running on Windows 2000. An additional connection policy using IPv4 addresses may be desired for Desktop Agents on Windows 2000 computers.
Active Directory	Select this option to limit or disable backups using Active Directory. Select Configure to configure the Active Directory settings. See “Customizing Connection Policies” on page 274 for details on configuring connection policy settings for Active Directory.
Desktop Agent Behavior	

Table 2-10 Connection Policies tab Add button options

Item	Description
Disable network backup	Select this option to prevent users from backing up to the network user data folder. Backups will continue to the desktop user data folder.
Disable network backup for files greater than	Select this option to prevent users from backing up files larger than a specified size based on the connection type. Enter a files size in KB.
Limit network bandwidth usage to	Enter a value in KB/sec to restrict the usage of network bandwidth to the specified value.
Enforce policy according to scheduled window	Select this option to enable the connection policy to apply only during the specified period of time. Click **Schedule** to set the time during which the policy will be in affect. Schedules can be set to run weekly or for a specific date range.

15 Click **OK**.

Related Topics

"About Backup Selections" on page 102

"Monitoring Alerts on the DLO Administration Console" on page 177

"Modifying Desktop Agent Settings" on page 268

Copying a Profile

When you create a new profile, we recommend that you begin with a copy of an existing profile with a configuration similar to that required for the new profile. You can then modify the copy as required, to meet the needs of a new group of desktop users.

To copy a profile

1 On the DLO navigation bar, click **Setup**.

2 In the **Settings** pane, click **Profiles**.

3 Right-click on the profile you want to copy.

4 Click **Copy**.

5 Type a name for the new profile.

6 Type a description of the new profile.

7 Click **OK**.

Modifying a Profile

Profiles can be modified as required to meet the changing needs of user groups.

Note: Modifications to a profile will cause users of that profile to cancel jobs, load settings, restart backup engines and scan their backup selection tree.

To modify a profile

1. On the DLO navigation bar, click **Setup**.
2. In the **Settings** pane, click **Profiles**.
3. In the **Results** pane, select the profile you want to modify.
4. In the **Task** pane, under **General Tasks**, click **Properties**.
5. To enable Dedupe, on the **General** tab, select the **Enable Dedupe** check box.

   Note: If any of the users associated with this profile uses a DLO Storage Location without Dedupe Storage Location, then the Dedupe option cannot be enabled for those users.

6. Modify the profile properties as needed.
7. Click **OK**.

Disabling Dedupe for a Profile

If you disable the Dedupe option for a profile, then DLO manages the backup and restore operations normally, using the Encryption, Compression, and Delta file options. Deduped data that was previously backed up can be restored.

In case you want to enable Dedupe again after some days, then the list of users associated with this updated profile is checked. If any user has a Storage Location without a Dedupe Storage Location defined, then a message prompts you to define a Dedupe Storage Location for that specific user.

About Backup Selections

Backup selections specify which files and folders you want to back up on desktops. Backup selections created by DLO administrators within profiles are called profile backup selections. Desktop users can also create backup selections or modify profile backup selections if the DLO administrator has provided them with sufficient rights.

Backup selections are easily customized to meet a wide variety of needs. With in each backup selection you can do the following:

- Specify the path to be backed up
- Choose to include or exclude subfolders, file types, or specific folders
- Set the number of revisions retained for each file in the backup selection, the frequency with which they are saved, and instructions on how long to retain backup files
- Configure the backup selection to transfer only the changed portions of files
- Compress or encrypt the files for transmission and storage
- Specify how long to retain backup files after the source files are deleted

Caution: Symantec strongly recommends that you consider disk space when choosing backup selections for desktops and laptops. A large number of local copies may cause the Desktop Agent user's computer to run out of disk space. For example, you may want to avoid selecting entire drives for backup or synchronization.

Related Topics

“Default Backup Selections” on page 103

“Removing Default Backup Selections from a Profile” on page 104

“Adding a Backup Selection” on page 105

“Defining General Backup Selection Properties” on page 106

“Including and Excluding Files or Folders from a Backup Selection” on page 107

“Revision Control” on page 108

“Setting Options for a Backup Selection” on page 111

“Using DLO Macros in Backup Selections” on page 112

“Modifying a Backup Selection” on page 114

“Deleting Backup Selections” on page 117

Default Backup Selections

DLO is configured to back up commonly used files and folders by default. You can add additional backup selections or cancel the use of default backup selections. The following are backed up by default.

Table 2-11 describes the default selections for backups.

Table 2-11 Default backup selections

Item	Description
My Documents	All files in My Documents
My Favorites	Internet Explorer Favorites
Outlook PST Files	PST files in the default location
My Desktop	All files on the Desktop
Notes Files (Multi-user)	Lotus Notes data for multiple user install
Notes Archive (Multi-user)	Lotus Notes archive for multiple user install
Notes Files (Single-user)	Lotus Notes data for single user install
Notes Archive (Single-user)	Lotus Notes archive for single user install
My Music	All files in My Music
My Pictures	All files in My Pictures
My Videos	All files in My Videos
Outlook 2010 PST Files	Outlook 2010 PST files in default location
Notes (ver. 8 and above) Files (Single-user)	Notes (ver. 8 and above) data for single user install
Notes (ver. 8 and above) Archives (Single-user)	Notes (ver. 8 and above) archive for single user install

Note: Backup selections assume applications are using default paths. If custom paths were used during installation or modified thereafter, you will need to customize the backup selections to insure they work properly. See “Modifying a Backup Selection” on page 114 for more information.

Removing Default Backup Selections from a Profile

Default profile backup selections are appropriate for most DLO installations. In some cases, it may be desirable to remove or replace default backup selections.

To remove default backup selections from a profile

1 On the DLO navigation bar, click **Setup**.

2 In the **Settings** pane, click **Profiles**.

3 In the **Results** pane, select the profile you want to modify.

4 In the **Task** pane, under **General Tasks**, click **Properties**.

5 Click the **Backup Selections** tab.

6 Deselect those backup selections you do not want to use.

7 Click **OK**.

Adding a Backup Selection

When a new backup selection is created for a profile, that profile backup selection is available for selection in all other profiles.

To add a backup selection

1 On the DLO navigation bar, click **Setup**.

2 In the **Settings** pane, click **Profiles**.

3 In the **Results** pane, select the profile for which you want to add a backup selection.

4 In the **Task** pane, under **General Tasks**, click **Properties**.

5 Click the **Backup Selections** tab in the **Profile Properties** dialog box.

6 Click **Add**.
A dialog box explains that if you customize NTFS permissions or directory attributes such as compression or encryption for backed up files or folders, these settings will not be backed up. You must reapply these settings after restoring the files. If you use a password for a Microsoft Outlook PST file, you must reset the password after restoring a PST file.

7 Read the message that displays, and then click **OK**.

8 Do any of the following to customize the backup selection properties:

- To set general backup selection properties including the name, description and folder to be backed up, see “Defining General Backup Selection Properties” on page 106.
- To include or exclude specific files from this backup selection, see “Including and Excluding Files or Folders from a Backup Selection” on page 107.
- To set revision control for this backup selection, see “Setting Revision Control for a Backup Selection” on page 109.
- To set Delta File Transfer, encryption and compression options for this backup selection, see “Setting Options for a Backup Selection” on page 111.

9 Click **OK** twice.

Defining General Backup Selection Properties

When a backup selection is created, the name, description and path to be backed up are specified in the backup selection general dialog box. Once the backup selection is created, the name, description and backup path can be modified as needed.

1. Open the **Backup Selection** dialog box as described in one of the following procedures:
   - "Adding a Backup Selection" on page 105
   - "Modifying a Backup Selection" on page 114
2. From the **General** tab in the **Backup Selection** dialog box, select the appropriate options. Table 2-12 describes the options.

Table 2-12 Backup Selection General tab

Item	Description
Name	Type a descriptive name for the backup selection.
Description	Type a clear description of the backup selection. This description may include, for example, the folder selected, the group of users it was created for, or the purpose for creating the backup selection.
Folder to back up	
Type a folder name	Select this option to add a specific folder to the backup selection. Type the path to the folder, including the folder name. For example, to add a folder named MyData on drive C, type `C:\MyData`. **Note:** See "Using DLO Macros in Backup Selections" on page 112 for information on using macros to define the folders backed up by a backup selection.
Select a pre-defined folder	Select this option to choose a pre-defined folder from the list provided. **Note:** See "Using DLO Macros in Backup Selections" on page 112 for information on the macros used to define the pre-defined folders.
Include subfolders	Select this option to also back up all subfolders in the specified directory. This option is selected by default.

3. Click **OK**.

Including and Excluding Files or Folders from a Backup Selection

Each backup selection can be configured to either include all files and folders, or to include or exclude specific files and folders. In addition, specific file types or folders can be specified for inclusion or exclusion using wildcards.

Files and folders can also be excluded from all backups for all users using global exclude filters. Several file types are excluded by default. These global excludes can be viewed or modified in the Global Excludes dialog box.

Related Topics

"DLO Default Settings" on page 41

"Configuring Global Exclude Filters" on page 134

To include or exclude files or folders from a backup selection

1. Open the **Backup Selection** dialog box as described in one of the following procedures:
   - "Adding a Backup Selection" on page 105
   - "Modifying a Backup Selection" on page 114
2. From the **Include/Exclude** tab in the **Backup Selection** dialog box, select the appropriate options.
   - **Include all file types:** Select this option to include all the file types in this backup selection.
   - **Include and exclude only the items listed below:** Select this option to include or exclude only specific files or file types. When this option is selected, a wildcard include is added to back up all files not specifically excluded.
3. To add a filter to the **Include/Exclude** list, verify that you selected **Include and exclude only the items listed below** in step 2, and click **Add Include** or **Add Exclude**.
4. If you selected **Add Exclude**, you will be notified that all previously backed up files matching this exclude will be deleted from this backup selection. Click **Yes** to continue or **No** to cancel.
5. Select the appropriate options.

Table 2-13 describes the options.

Table 2-13 Add Include Filter or Add Exclude Filter options

Item	Description
Filter	Type the name of the file or the folder that you want to include or exclude. You can use wildcards. For example, type `*.mp3` to either include or exclude all files with the file extension .mp3, or type `unimportant.txt` to include or exclude all files in the backup selection with this specific file name. Click **Extensions** to select a predefined filter to either include or exclude all files with a given file extension.
Description	Type a description of this include or exclude filter.
Apply to	Select one of the following: ■ **Files** to apply this filter to files ■ **Folders** to apply this filter to folders ■ **Files and Folders** to apply this filter to both files and folders

6 Click **OK**.

Revision Control

Revisions are versions of a file at a specific point in time. You configure revision settings when you create a backup selection. When a file is changed and backed up, DLO stores a new revision. DLO will store and maintain a specific number of revisions for all files in a backup selection. Because backup selections are configured separately, the number of revisions retained in each backup selection can vary.

When the number of revisions is exceeded, DLO removes the oldest revision, maintaining only the specified number of revisions in the Desktop and network user data folders.

You can limit the number of revisions retained in a given period of time. If you are working on a document and backing it up frequently, all of your revisions could potentially be just a few minutes apart. By specifying that you want to retain only two revisions every 24 hours, at least 120 minutes apart, you can retain older revisions for a longer period of time. While some intermediate versions will not be retained, it does support situations in which returning to an older revision is needed.

Another consideration in determining the number of revisions to retain is the amount of storage space required to store the data. The amount of space required for backups can be estimated by multiplying the number of revisions retained by the amount of data protected.

Example `If you are retaining three revisions of each file and have 10 MB of data to back up, approximately 30 MB of disk space are required if file sizes remain consistent between revisions.`

Although compression can improve the space utilization, it varies significantly with file type and other factors. Typical compression ratios are approximately 2:1, so in the previous example, the maximum disk space usage might be reduced to approximately 15 MB.

File Grooming

The Desktop Agent grooms revisions based on backup selection settings and does this as new revisions are created. The oldest revision is deleted when a new revision is created that exceeds the limit. See step 2 on page 109 for revision control settings.

Maintenance grooming is the process of removing backups of deleted files. It occurs at most once every 24 hours. Maintenance grooming occurs during the first backup that runs after 24 hours have passed since the last maintenance grooming.

Setting Revision Control for a Backup Selection

The number of revisions retained in the desktop user data folder and network user data folder are specified for each backup selection and can be customized to meet specific user requirements. In addition, the time between revisions can be specified.

To set revision control for a backup selection

1 Open the **Backup Selection** dialog box as described in one of the following procedures:
   - "Adding a Backup Selection" on page 105
   - "Modifying a Backup Selection" on page 114

2 From the **Revision Control** tab in the **Backup Selection** dialog box, select the appropriate options for both the Desktop and network user data folders.
   Table 2-14 describes the options.

Table 2-14 Backup Selection Revision Control tab options

Item	Description
Number of revisions	

Table 2-14 Backup Selection Revision Control tab options (continued)

Item	Description
Desktop user data folder	Type the number of revisions to keep in the desktop user data folder for each file in the backup selection. **Note:** When Outlook PST files or Lotus Notes NSF files are backed up incrementally, only one revision is maintained regardless of the number of revisions set in the backup selection.
Limit to	Select this option to limit the number of revisions retained in a given amount of time, and specify the following: ■ **Revisions:** Select the number of versions to retain. ■ **Within the last x hours:** Select the time period during which you want to retain the versions. ■ **At least x minutes apart:** Select the minimum amount of time that must elapse between backups in this backup selection. **Note:** The oldest revision is deleted when a new revision is created that exceeds one of these limits.
Network user data folder	Select the number of revisions to keep in the network user data folder for each file in the backup selection.
Limit to	Select this option to limit the number of revisions retained in a given amount of time, and specify the following: ■ **Revisions:** Select the number of versions to retain. ■ **Within the last x hours:** Select the time period during which you want to retain the versions. ■ **At least x minutes apart:** Select the minimum amount of time that must elapse between backups in this backup selection. **Note:** The oldest revision is deleted when a new revision is created that exceeds one of these limits.
Revision Age	
Discard all revisions in the desktop user data folder older than	Enter the number of days after which all revisions in the desktop user data folder will be deleted. **Note:** The most recent revision will not be discarded.

Table 2-14 Backup Selection Revision Control tab options (continued)

Item	Description
Discard all revisions in the network user data folder older than	Enter the number of days after which all revisions in the network user data folder will be deleted. **Note:** The most recent revision will not be discarded.

Setting Options for a Backup Selection

DLO backup selections can be further customized by settings options for Delta File Transfer, Compression and Encryption. In addition, you can specify how long to keep backup files after the original source files are deleted.

1 Open the **Backup Selection** dialog box as described in one of the following procedures:

- "Adding a Backup Selection" on page 105
- "Modifying a Backup Selection" on page 114

2 From the **Options** tab in the **Backup Selection** dialog box, select the appropriate options. Table 2-15 describes the options.

Note: For Dedupe enabled profile, Delta File Transfer option is selected by default, and is applicable only for non-PST files. For PST files, Delta File Transfer parameters are forcibly applied whether the option is selected or not selected.

Table 2-15 Backup Selection options

Item	Description
Delta File Transfer	Each time a file is backed up, only the part of the file that has changed is transferred and stored in the network user data folder. In addition, delta file transfer uses compression. Enabling this option requires that you have installed and configured a maintenance server. See"Adding a New Maintenance Server" on page 117 for more information.

Table 2-15 Backup Selection options (continued)

Item	Description
Compression	Each time a file is backed up, files in this backup selection will be compressed for data transfer over the network and for storage in the Desktop and network user data folders. This affects files created after this feature is activated. Previously stored files will not be compressed. Delta File Transfer also uses compression.
Encryption	Select this option to encrypt files for transfer and to store files from this backup selection in an encrypted format in the network user data folder. This affects files transmitted and stored after this feature is activated. Previously stored files will not be encrypted. The Advanced Encryption Standard (AES) and a 256 bit key length are used. If enabled, versions are stored unencrypted in the desktop user data folder, and encrypted in the network user data folder. Transfer over the network is encrypted.
When source files are deleted, delete the backed up files from the:	
Desktop user data folder after	Indicate the number of days after which DLO will delete all file versions from the desktop user data folder after the source file has been deleted from the desktop.
Network user data folder after	Indicate the number of days after which DLO will delete all file versions from the network user data folder after the source file has been deleted from the desktop.

3 Click **OK** to save the backup selection.

Using DLO Macros in Backup Selections

You can type macros into the **Type a folder name** field of the backup selection dialog box to automatically back up specific folders. For more information on configuring the **Type a folder name** field, see “Backup Selection General tab” on page 106.

The following table describes the macros that are supported.

Table 2-16 Folder Macros for use with backup selections

Backup Selection Macro	Folders backed up
%LOCALFIXEDDRIVES%	All local fixed drives. **Note:** DLO is not designed to back up removable media. Attempting to back up a floppy disk or CDROM may result in errors.
%MACHINENAME%	Represents the desktop user's computer name. Example: `C:\documents\%machinename%` represents `C:\documents\UsersMachineName`.
%CURRENTUSERNAME%	Represents the username of the currently logged-on user. Example: If the local administrator is logged on to the computer, `C:\documents\%currentusername%` represents `'C:\documents\Administrator'`
%CURRENTUSERPROFILE%	All files and folders in the C:\Documents and Settings\current user profile directory.
%CURRENTUSERMYDOCS%	The My Documents directory for the user who is logged on.
%CURRENTUSERFAVORITES%	The Favorites directory for the user who is logged on.
%CURRENTUSERPRINTHOOD%	The Printers directory for the user who is logged on.
%CURRENTUSERNETHOOD%	The Network Locations directory for the user who is logged on.
%CURRENTUSERDESKTOP%	The Desktop directory for the user who is logged on.
%CURRENTUSERRECENT%	The Recent Files directory for the user who is logged on.
%PROGRAMFILES%	The Windows Program Files directory. Example: `%PROGRAMFILES%\lotus\notes\data\archives`
%LOCALAPPDATA%	The Windows local application data directory: `Documents and Settings\<user_name>\Local Settings\Application Data”`

The following additional pre-defined folder macros are available for selection in the backup selection dialog box.

Table 2-17 Macros for pre-defined folders in the Backup Selection dialog

Folder Name	Pre-Defined Folder Macro	Folders Backed Up
My Documents	`%CURRENTUSERMYDOCS%`	The My Documents directory for the user who is logged on.
Desktop	`%CURRENTUSERDESKTOP%`	The Desktop directory for the user who is logged on.
Favorites	`%CURRENTUSERFAVORITES%`	The Favorites directory for the user who is logged on.
PrintHood	`%CURRENTUSERPRINTHOOD%`	The Printers directory for the user who is logged on.
NetHood	`%CURRENTUSERNETHOOD%`	The Network Locations directory for the user who is logged on.
Recent	`%CURRENTUSERRECENT%`	The Recent Files directory for the user who is logged on.
All local fixed drives	`%LOCALFIXEDDRIVES%`	All local fixed drives.

Note: When you enter a path that uses a macro, a backslash is automatically added immediately following the macro. For example, if you type %LOCALFIXEDDRIVES%\Documents, an extra backslash is added and it appears as "x:\\Documents" in the Desktop Agent backup selection advanced view. It does not show at all in the Desktop Agent backup selection Standard view. The correct way to type this macro is %LOCALFIXEDDRIVES%Documents. This properly resolves to x:\Documents.

Modifying a Backup Selection

Profile backup selections can be modified from the DLO Administration Console.

To modify a backup selection

1 On the DLO navigation bar, click **Setup**.

2 In the **Settings** pane, click **Profiles**.

3 In the **Results** pane, click the profile you want to modify.

4 In the **Task** pane, under **General Tasks**, click **Properties**.

5 Click the **Backup Selections** tab.

6 Select the backup selection you want to modify, and click **Modify**.

Note: The **Type a folder name** field in the **General** tab is grayed out in this view. If the path in this field is longer than the display, hold the curser over the path for a moment to display the entire path.

7 Click **OK** to indicate that you read the message stating that modifying this backup selection will change all profiles that are using this selection.

8 Change the backup selection as described in the following topics:
"Defining General Backup Selection Properties" on page 106
"Including and Excluding Files or Folders from a Backup Selection" on page 107
"Setting Revision Control for a Backup Selection" on page 109
"Setting Options for a Backup Selection" on page 111

9 Click **OK** twice.

About Delta File Transfer

The Delta File Transfer feature enables incremental transfer and storage of backup data. When this option is enabled, the initial backup requires transfer of the entire file. Subsequent backups require only the transfer of the parts of the file that have changed, reducing the bandwidth required and improving backup speed.

Note: For Dedupe enabled profiles, Delta File Transfer option is applicable only for non-PST files. For PST files, Delta File Transfer parameters are forcibly applied whether the option is selected or not selected.

Excluding files from delta file transfer

Delta File Transfer is not limited to certain programs or file types, but does offer the ability to exclude certain file types. Default excludes are configured for Delta File Transfer because these file types do not benefit from this technology. This is usually because the file types are already highly compressed. See "Configuring Global Exclude Filters" on page 134 for more information.

Working Offline

Delta File Transfer is only used to transfer and store backup files on in the network user data folder. Backup files stored in the Desktop User Data Folder are not stored using deltas. If a Desktop Agent user is working offline, the local revisions are stored in their entirety in the desktop user data folder. When the user is once again working online, Delta File Transfer is used to transfer data to the network user data folder.

Requirements for Delta File Transfer

Delta File Transfer requires the use of the DLO maintenance server. The maintenance server manages the deletion of previous delta revisions from storage locations. The maintenance server is only required when the Delta File Transfer option is enabled, but it is installed by default when DLO is installed. Only one maintenance server is required, but in large installations it may be more efficient to have one maintenance server for each Storage Location host (that is File Server).

The maintenance server is installed on the DLO Administration Server by default when DLO is installed. If the administration server is also the Storage Location host, then no additional steps are required to configure the maintenance server.

Maintenance Server Technical Information and Tips

The Desktop Agent uses Windows RPC over named pipes to communicate with the maintenance server. For the maintenance server to function, named pipe traffic must not be blocked at any point between the DLO Client and the maintenance server.

The rolloff operation for delta revisions can require significant bandwidth. For this reason, the maintenance server should be installed on the computer that is hosting the Storage Location.

However, there are situations where the maintenance server cannot be installed on the same computer as the Storage Location server. For example, the maintenance server cannot be installed on a NAS device. In this case, the maintenance server should be installed on a computer with a high bandwidth connection to the Storage Location.

A maintenance server can manage one or more Storage Locations. A maintenance server will always manage the Storage Locations located on same computer as the maintenance server. The maintenance server can be configured to manage additional Storage Locations hosts, that is, File Servers, from the DLO Admin console. The maintenance server uses delegation to access remote Storage Locations. See "Configuring a Maintenance Server for Delegation" on page 118 for more information.

Enabling Delta File Transfer for a Backup Selection

Delta File Transfer is off by default. It can be enabled for a given backup selection by selecting **Delta** in the **Backup Selection Options** tab as explained in "About Delta File Transfer" on page 115.

In addition, if a maintenance server manages file servers that are on a target other than itself, the maintenance server must be configured for delegation as explained in "Configuring a Maintenance Server for Delegation" on page 118.

Delta File Transfer can also be selected as the default compression type by changing the application default settings for compression. If the default compression setting is changed to **Delta**, all new backup selections will use Delta compression by default. See “DLO Default Settings” on page 41 for more information.

Deleting Backup Selections

Before you can delete a backup selection, you must be sure that it is not in use by any profiles. When you delete a backup selection from one profile, DLO deletes it from every profile.

When you delete a backup selection, the backup versions are deleted in the same manner as when source files are deleted. They will be groomed after the number of days specified in the backup selection.

To delete a backup selection

1. On the DLO navigation bar, click **Setup**.
2. In the **Settings** pane, Click **Profiles**.
3. In the **Results** pane, click the profile that contains the backup selection you want to delete.
4. In the **Task** pane, under **General Tasks**, click **Properties**.
5. From the **Backup Selections** tab, select the backup selection you want to delete.
6. Click **Delete**.
7. Click **Yes**.

Related Topics

“Backup Selection options” on page 111

About Maintenance Servers

Adding a New Maintenance Server

After you install a new maintenance server, you must add the maintenance server to DLO. After adding the maintenance server to DLO, you can then specify which file servers it is to manage as explained in “Reassigning a File Server” on page 120.

To add a new maintenance server

1. Verify that the new maintenance server has been installed.

Note: A default maintenance server is installed with DLO. A stand-alone maintenance server can also be installed by selecting **Maintenance Server** as the installation type as described in "Installing the Symantec Desktop and Laptop Option" on page 25.

2 From the DLO Console, on the DLO navigation bar, click **Setup**.

3 In the **Task** pane, under **Manage Tasks**, click **Maintenance servers**.

4 Click **Add**.

5 Navigate to the computer where the maintenance server is installed.

6 Select this computer.

7 Click **OK**.

Configuring a Maintenance Server for Delegation

When a maintenance server is configured to manage Storage Locations hosted by a different computer, they must be configured to access these locations on behalf of desktop users running the Desktop Agent. This configuration is managed using the Active Directory.

Note: For detailed information on delegating Active Directory administration, see the Microsoft website:
http://technet.microsoft.com/en-us/library/cc773318(v=ws.10).aspx

To configure a maintenance server for delegation

1 Verify that the following conditions are met:

- Domains are Windows 2000 or later. NT 4 domains are not supported.
- Both the Desktop Agent user's account and the maintenance service's account must be in the same domain.
- Desktop Agent user and computer accounts must be in mutually trusted domains.
- Desktop and server operating systems must be Windows 2000 or later.

2 Confirm that the desktop user account is configured for delegation. See "Confirming the Desktop User's Account is Configured for Delegation" on page 119.

3 Confirm that the server process account is trusted for delegation."Confirming the Server Process Account is Trusted for Delegation" on page 119.

Confirming the Desktop User's Account is Configured for Delegation

This process verifies that the Desktop Agent user's account can be delegated.

To confirm that the desktop user's account is configured for delegation

1. Log on to the domain controller using a domain administrator account.
2. On the **Task** bar, click **Start> Programs > Administrative Tools> Active Directory Users and Computers**.
3. Under the domain, click the **Users** folder.
4. Right-click the user account to be delegated and click **Properties**.
5. Click the **Account** tab.
6. In the **Account options** list, verify that the **Account is sensitive and cannot be delegated** is not selected.
7. Click **OK**.

Confirming the Server Process Account is Trusted for Delegation

This process verifies that the account used to run the maintenance server process is allowed to delegate client accounts.

To confirm that the server process account is trusted for delegation

Example: On a Windows Server 2003 machine

1. Log on to the domain controller using a domain administrator account.
2. On the **Task** bar, click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
3. Right-click the **Computers** folder and click **Properties**.
4. Right-click the computer on which the maintenance server runs and then click **Properties**.
5. On the **General** tab, click **Trust computer for delegation**.
6. Click **OK**.

Changing the Default Maintenance Server

When DLO is installed, a maintenance server is installed and set as the default maintenance server. New storage locations are automatically assigned to the default maintenance server when they are created. If you want new storage locations to be assigned to a different maintenance server by default, you must change this setting.

To change the default maintenance server

1. From the DLO Console, on the DLO navigation bar, click **Setup**.
2. In the **Task** pane, under **Manage Tasks**, click **Maintenance servers**.
3. In the **Maintenance Servers** list, select the check box for the maintenance server you want to set as the default.
4. Click **OK**.

Deleting the Maintenance Server

When you uninstall a maintenance server, the entry for the maintenance server still remains on the Administration Console.

The entry for the maintenance server must be manually deleted from the Administration Console.

To delete the entry for a maintenance server

1. Select **Tools> Manage Maintenance Servers**.
2. Select the check box for the maintenance server you want to delete.
3. Click **Delete**.

Note: The entry for the default maintenance server cannot be deleted from the Administration Console.

Similarly, once you add a maintenance server from the Administration Console, you must install the maintenance server software on the computer to begin maintenance processes.

Reassigning a File Server

You can reassign a file server to another maintenance server that is recognized by DLO. For example, when you create a new storage location, it is automatically assigned to the default maintenance server. You may want to reassign it to a different maintenance server.

To reassign a file server

1. Verify that the new maintenance server has been installed and configured.
2. On the DLO navigation bar, click **Setup**.
3. In the **Task** pane under **Manage Tasks**, click **Maintenance servers**.
4. Select the maintenance server currently manages the file server.

5 Click **Edit**.

6 Select the file server you want to reassign.

7 Click **Reassign**.

8 Select the new maintenance server from the drop-down menu.

9 Click **OK** three times.

About DLO Storage Locations

Storage Locations are locations on network computers where network user data folders are automatically created. DLO stores each user’s data in two places. First, data is stored in the desktop user data folder on the user's computer to provide protection and restore capabilities even when the computer is disconnected from the network. The data is then additionally stored in a network user data folder, which is located on the network. This provides an additional level of protection, and enables the files to be backed up to secondary media when the server is backed up.

When a user is automatically added to DLO using an Automated User Assignment, a network user data folder is created in a DLO Storage Location as specified in the Automated User Assignment. If network shares already exist for desktop users, they can be specified as network user data folders when users are manually added to DLO. If existing network shares are used as network user data folders, Storage Locations are not used.

DLO supports the use of hidden shares (for example; “Share$”) as Storage Locations on NTFS volumes or as network user data folders for FAT32 volumes, but they cannot be created with the DLO Administration Console. They must be created and configured manually. See “Using Hidden Shares as Storage Locations” on page 122 for more information.

Supported Storage Location Configurations

The following table summarizes supported configurations for DLO Storage Locations.

Table 2-18 Storage Location Configuration Support

Description	Supported	Not Supported
All DLO Administration Server platforms	X	
Windows 2000 NAS/SAK NAS devices	X	
Local DLO Administration Server direct-attached storage	X	

Table 2-18 Storage Location Configuration Support (continued)

Description	Supported	Not Supported
SAN	X	
Windows-networking accessible NAS Devices (Quantum, Network Appliance, etc.)	X	
FAT, FAT32 and NTFS partitions are supported as Storage locations, although FAT and FAT32 are not recommended. NTFS is the preferred file system for Storage Locations	X	
NetWare 3.1x, 4.x, or E-Directory Storage Locations		X
UNIX file systems or SAMBA shares on UNIX systems		X

Using Hidden Shares as Storage Locations

DLO supports the use of hidden shares (for example; “Share$”) as Storage Locations on NTFS volumes or as network user data folders for FAT32 volumes, but these shares must be manually created and configured. They cannot be created with the DLO Administration Console. Hidden shares cannot be used for FAT based Storage Locations.

The following table provides information about the permission settings for hidden shares.

Table 2-19 Permission Settings for Hidden Shares

Drive Type	User or Group	Permissions
Share Permissions on NTFS Volumes		
	Administrator	Allow Full Control, Change, Read
	Everyone	Allow Full Control, Change, Read
Security Permissions on NTFS Volumes		
	Administrator	Full control
	Everyone	Allow Read & Execute Allow List Folder Contents Allow Read

Table 2-19 Permission Settings for Hidden Shares (continued)

Drive Type	User or Group	Permissions
	Special security permissions or advanced settings	Allow Traverse Folder/Execute File Allow List Folder/Read Data Allow Read Attributes Allow Read Extended Attributes Allow Read Permissions
Advanced Security Permissions on NTFS Volumes		
	Administrator	Allow Full Control
	Everyone	Allow Traverse Folder / Execute File Allow List Folder / Read Data Allow Read Attributes Allow Read Extended Attributes Allow Read Permissions
Share Permissions on FAT Volumes		
	Administrator	Allow Full Control, Change, Read
	Owner	Allow Full Control, Change, Read
	Full Admin Group	Allow Full Control, Change, Read
	Limited Admin Group	Allow Read

Creating DLO Storage Locations

A DLO Storage Location should be used by only one DLO Administration Server. If you set up multiple administration servers to use the same DLO Storage Location and the DLO Storage Location is deleted from one administration server, the other administration server will no longer be able to access it.

Storage Locations must be in a Windows Domain or Active Directory. Computers running the Desktop Agent can be outside a Windows domain or Active Directory, but they must authenticate with the domain or directory to access the DLO Administration Server or Storage Locations. Users are prompted to provide domain credentials when the Desktop Agent is launched.

If your original files reside on an NTFS volume, then the desktop user data folder and the network user data folder should also be NTFS. If your original files are on NTFS and either the desktop user data folder or network user data folder are on a FAT or

FAT32 volume, you may see duplicate entries in the Restore and Restore Search screens. If duplicates do appear, you can select either file to restore.

Once created, Storage Locations cannot be modified, but they can be deleted if there are no users or Automated User Assignments assigned to them. You can move users to new Storage Locations. For more information, see “Moving Desktop Agent Users to a New Network User Data Folder” on page 154.

Note: If you receive errors when creating Storage Locations, verify that the login account for the service named MSSQL$DLO has sufficient rights to create directories and change permissions for the Storage Locations. Use the Windows Service Control Panel to change the login account for the MSSQL$DLO instance. You can avoid these problems if you specify a domain account when you install DLO.

To create DLO storage locations

Note: After you create Storage Locations, you cannot modify them.

1. On the DLO navigation bar, click **Setup**.
2. Select one of the following options to create a new DLO Storage Location.
    - In the **Selection** pane, right-click **Storage Locations** and select **New Storage Location** or **New Storage Location using Wizard**.
    - In the **Task** pane, under **Settings Tasks**, click **New Storage Location**.
3. Select the appropriate options as described in the following table.

Table 2-20 New Storage Location Dialog Box

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Computer name</b></td><td>Type a computer name or browse to a computer on which to create the Storage Location.</td></tr>
<tr><td><b>Path</b></td><td>Type or browse to a location on the computer where the Storage Location will be created.
<b>Note:</b> Storage Locations should be in the same domain as the DLO Administration Server or in a domain that trusts the administration server’s domain.</td></tr>
<tr><td><b>Storage Location name</b></td><td>Type a name for the new DLO Storage Location. The name cannot contain any of the following characters: \”@#$%^&*()=+|/{}[]’</td></tr>
</table>

Table 2-20 New Storage Location Dialog Box (continued)

Item	Description
Dedupe Storage Location	Select a Dedupe Storage Location from the drop-down list. For more information about how to add a Dedupe Storage Location, see "Adding a Dedupe Storage Location" on page 76. **Note:** Once you choose a Dedupe Storage Location for a DLO Storage Location, you cannot change the Dedupe Storage Location later.
Summary	This field automatically displays the location and format of network user data folders that will be created for new users assigned to this Storage Location. Network user data folders are automatically created in the Storage Location. DLO uses the %USERDOMAIN% and %USERNAME% variables to determine the actual folder path for each user who is assigned to a DLO Storage Location. DLO uses the user's domain and user name to create a unique network user data folder name for that user. If the user is logged on with credentials that do not allow access to the DLO Storage Location, the user will be prompted to enter alternate domain credentials. The network administrator can access this folder, but cannot configure the variables.

4 Click **OK**.

Configuring Remote Windows Share or NAS Device for DLO Storage Locations

You can create DLO Storage Locations on remote Windows shares or network attached storage devices.

Case 1

To create storage locations when the DLO administration service is a full administrator on the remote system

1 Validate that DLO 5.1 MP1 or later is installed.

2 Ensure that the account credentials used for DLO services have full administrator rights to the remote storage location or NAS device.

3 Make sure that the volume desired to be used for DLO has been assigned a drive letter on the remote storage location or NAS device.

Note: See hardware vendor documentation on share creation and naming.

4 Create a new DLO Storage Location as explained in the section "Creating DLO Storage Locations" on page 123. Use the **Browse** feature to select a location on the computer where the DLO Storage Location should be created. This will insure that the path and the DLO service account are valid.

Case 2

The DLO administration service does not run as an administrator level user, but the DLO administration groups have been assigned the appropriate permission levels on a pre-existing share.

To configure storage locations using non-administrator case

1 Configure DLO to use existing domain groups to automatically manage access to network user data folders as explained in "Managing Administrator Accounts" on page 37. Check the Automatically grant DLO Administrators access to network user data folders checkbox and provide the required domain groups. Provide two groups: a group for full-DLO administrators and a group for limited-DLO administrators.

2 From the Administrator Account Management dialog, add the appropriate domain user accounts to the account manager. If the user will have full administrator rights, check the "Grant administrator full restore privileges" checkbox in the Add Administrator Account dialog. In addition to other users, be sure to grant the DLO Administration Service full restore privileges.

3 Create a folder on the remote storage location using an administrator, or administrator equivalent user.

4 Share the new folder. Ensure that 'Everyone' has full-access to the share.

5 Modify the folder's security permissions such that the full-DLO administrator group has full-control of the folder and that the limited-DLO administrator group has modify-control of the folder.

6 Using the DLO console, create a new DLO Storage Location. Specify the machine name, drive and path, and share name for the folder just created.

Note: Do not click the Browse buttons at any point while creating the DLO Storage Location because using the Browse feature will cause the process to fail.

7 Once the required fields are completed, click **OK.**

8 Storage Locations manually created when the DLO Admin Service does not have full administrator rights to the server hosting the DLO Storage Location cannot be deleted from the DLO Administration Console. Attempting to do so will result in an error.

9 To manually remove the DLO Storage Location:

  a Move or delete all users in the DLO Storage Location.

  b Manually remove the DLO Storage Location share and folder from the server.

  c Delete the DLO Storage Location from the DLO Administration Console.

Deleting DLO Storage Locations

Before you can delete DLO Storage Locations, you must delete or reassign users and Automated User Assignments that use the DLO Storage Location. The DLO Storage Location associated with a user or Automated User Assignment is listed when you select **Users** or **Automated User Assignments** from the **Setup** view.

Note: When a DLO Storage Location is created using an existing share on a remote computer and DLO does not have full computer rights, the DLO Storage Location cannot be deleted from the DLO Administration Console. To remove the DLO Storage Location, first delete the DLO Storage Location share and then delete the DLO Storage Location from the DLO Administration Console.

To delete DLO storage locations

1 On the DLO navigation bar, click **Setup**.

2 In the **Selection** pane, to expand the file servers list, click the '+' icon next to File Servers.

3 In the **Selection** pane, click the File Server on which the DLO Storage Location resides.

4 In the **Results** pane, right-click the DLO Storage Location name and click **Delete**
OR
In the **Task** pane, under **General Tasks**, click **Delete**.

5 Click **Yes**.

Related Topics

"Managing Desktop Agent Users" on page 149

"Modifying Automated User Assignments" on page 132

"Deleting Automated User Assignments" on page 133

About Dedupe Storage Locations

The Dedupe Storage Location is a Common Internet File System (CIFS) network share location where data is stored as part of deduplication process. A logical group of Dedupe Storage Locations across which deduplication is performed is called a Dedupe Storage Pool.

Dedupe Storage Locations hold shared data that is common across and is shared by all or a subset of users in the system. So the users pointing to Dedupe Storage Locations (through Storage Location Mapping) in the same Dedupe Storage Pool need to have read/write access to all the Dedupe Storage Locations in the Storage Pool.

For security reasons, read/write access to the Dedupe Storage Locations is not granted to all the users even though they need to read and write data from the Dedupe Storage Locations. Instead, while creating the Dedupe Storage Location, the administrator configures a new user account called “Dedupe Storage Location Access Credential”, which will be used by the Desktop Agent to access the Dedupe Storage Location.

Hence it is recommended that the administrator specifically creates a low privilege domain user account as “Dedupe Storage Location Access Credential” for accessing the Dedupe Storage Location, and for security reasons.

In addition, the administrator should ensure that the password for this user account does not expire frequently. If the password expires, then the administrator should reset the password for the domain user.

All types of CIFS network shares supported by DLO Storage Location are supported by Dedupe Storage Locations also.

The following are some important facts about Dedupe Storage Locations:

- The Dedupe Storage Location name has to be unique across groups.
- The same network share should not be assigned to more than one Dedupe Storage Location.
- All network shares assigned to Dedupe Storage Locations in a Dedupe Storage Pool should have the same “Dedupe Storage Location Access Credential”.
- Only the administrator and users with “Dedupe Storage Location Access Credential” account should have access to the network share location used as a Dedupe Storage Location.
- The “Dedupe Storage Location Access Credential” account should not have administrator rights.
- The Dedupe Storage Location path should not be the same as the NUDF folder path.

- After the Dedupe Storage Location is associated with a DLO Storage Location, and a deduped backup is performed, in case the Dedupe Storage Location should be moved, then make sure to use the `-MigrateSL` command.
- The Dedupe Storage Location user should have the “Allow log on locally” policy set in the domain controller group policy object. To set this policy, do the following:
  - After logging on locally with domain admin account, run `gpmc.msc` (Group Policy Management).
  - Double-click the Domain name.
  - Expand **<Group Policy Objects>** and right-click **<Default domain controllers policy>**.
  - Click **Edit**.
  - Expand **<Computer Configurations> <Policies> <Windows Settings> <Security Settings> <Local Policies> <User Rights Assignment>.**
  - Right-click **<Allow log on locally>** and click **Properties**. Change as required.
  - Run **gpupdate** and wait for the confirmation: "*user policy update has completed succesfully*" (default gpupdate without switches should only apply the changes).

About Automated User Assignments

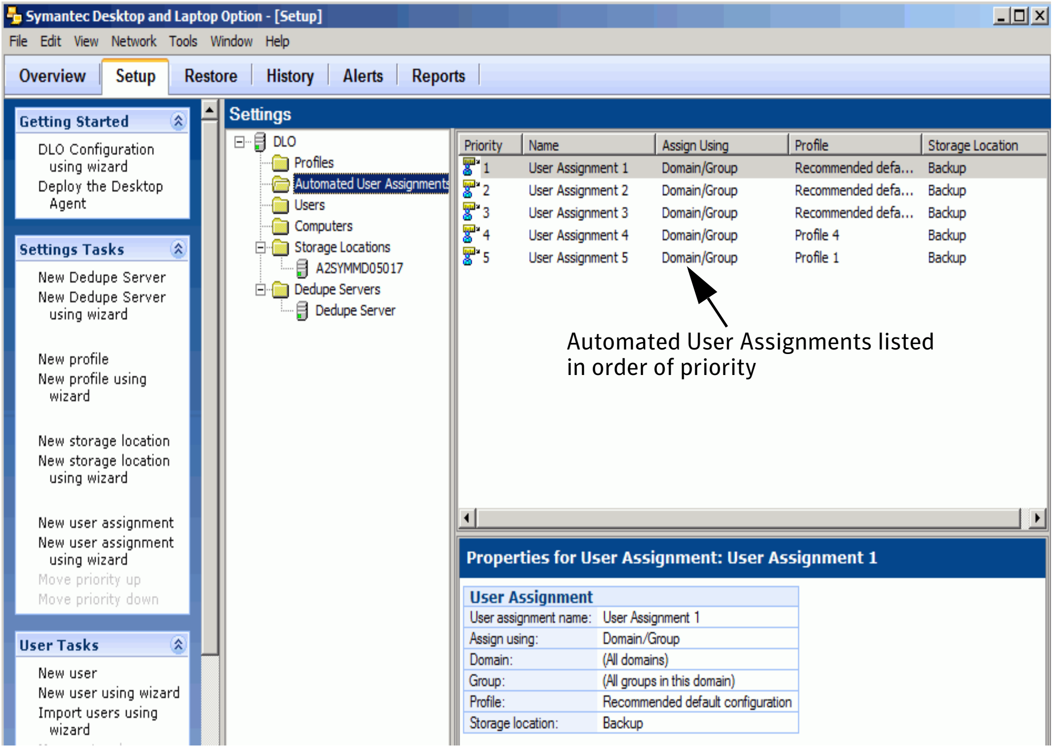
Automated User Assignments are instructions that are applied when the Desktop Agent is first run on a desktop. The Automated User Assignment assigns a profile and network user data folder to each user who is automatically configured by DLO. These settings can be changed from the DLO Administration Console at a later time if necessary.

Note: If a user is added manually to DLO, a Storage Location and profile are selected by the DLO administrator. The Automated User Assignment will not be used. For more information, see “Managing Desktop Agent Users” on page 149.

Automated User Assignments are assigned to desktop users based either on their domain and group, or using Active Directory settings. Because users may match the criteria for more than one Automated User Assignment, the Automated User Assignments are prioritized. When the Desktop Agent is run for the first time, the Desktop Agent user’s domain and group credentials are checked against those of the Automated User Assignment starting with the highest priority assignment. When a match is made, the share and profile specified in that Automated User Assignment are assigned to the new user.

Modifying Automated User Assignments does not affect users who have already been configured. Only new users configured with the Automated User Assignment will use the new settings.

Figure 2-4 Viewing automated user assignments



Priority	Name	Assign Using	Profile	Storage Location
1	User Assignment 1	Domain/Group	Recommended defa...	Backup
2	User Assignment 2	Domain/Group	Recommended defa...	Backup
3	User Assignment 3	Domain/Group	Recommended defa...	Backup
4	User Assignment 4	Domain/Group	Profile 4	Backup
5	User Assignment 5	Domain/Group	Profile 1	Backup

Automated User Assignments listed in order of priority

Properties for User Assignment: User Assignment 1

User Assignment	
User assignment name:	User Assignment 1
Assign using:	Domain/Group
Domain:	(All domains)
Group:	(All groups in this domain)
Profile:	Recommended default configuration
Storage location:	Backup

For information on modifying Automated User Assignment priorities, see “Changing the Priority of Automated User Assignments” on page 133.

Creating Automated User Assignments

Automated User Assignments are assigned to Desktop Agent users based either on domain and group settings or Active Directory settings. The Automated User Assignment determines which Storage Location and Profile are assigned to the user.

To create a new automated user assignment

1 On the DLO navigation bar, click **Setup**.

2 In the **Settings Tasks** pane, click **New User Assignment**.

3 Or in the **Settings** pane, right-click **Automated user assignment** and select **New User Assignment**.

The **New User Assignment** window appears.

4 Select the appropriate options as described in the following table.

Table 2-21 New Automated User Assignment Dialog Box Options

Item	Description
User Assignment	
User assignment name	Type a name for the Automated User Assignment. The Automated User Assignment name cannot contain the following characters: \”@#$%^&*()=+|/{}[]’
Assign using Domain and Group	Select this option to match Desktop Agent users to Automated User Assignments based on their domain and group.
Domain	Select the domain to which this Automated User Assignment will apply.
Group	Select the group to which this Automated User Assignment will apply.
Assign Using Active Directory	Select this option to match Desktop Agent users to Automated User Assignments based on Active Directory settings.
Configure	Click the Configure button to configure the User Assignment using Active Directory. See step 5 below for information on configuring the Active Directory settings.
Storage Location/Profile	
Storage Location	Select a Storage Location to be assigned to the users in the selected domain and group.
Profile	Select a profile to be assigned to the users in the selected domain and group. **Note:** When you select a profile that has Dedupe enabled, make sure that the Storage Location associated to this profile has a Dedupe Storage Location defined. If it is not defined, then you will not be able to create an automated user assignment.

5 If you chose to use Active Directory to configure the User Assignment in step 4, configure the Active Directory settings as follows:

Table 2-22 Active Directory Object Dialog

Item	Description
Object	For Automated User Assignments, the only option is **User**.
In LDAP Directory	Type or browse to the LDAP directory. **Note:** When selecting Active Directory user accounts, you must select the specific directory that holds the user accounts. Be sure not to select the user groups directory. Browse to or type the exact path of the specific user accounts directory for which you are creating this rule.
All objects in this directory	Select this option to apply the connection policy to all objects in the specified directory.
Only the objects in this directory that match the criteria below	Select this option to apply the connection policy only to those objects in the specified directory that match the criteria entered.
Attributes	Select an attribute from the drop-down menu or type a custom attribute.
Condition	Select the appropriate condition. Available options include =, <, <>, and >.
Value	Type a value to complete the criteria that will be used to determine matches. Wildcards can be used to specify the value.

6 Click **OK**.

Modifying Automated User Assignments

Modifying an Automated User Assignment affects only users added to the assignment after it has been modified. Existing Desktop Agent users are unaffected.

Settings for existing Desktop Agent users can be modified from the **Setup** view of the DLO Administration Console. For more information see “Modifying Desktop Agent User Properties” on page 152.

To modify an automated user assignment

1 On the DLO navigation bar, click **Setup**.

2 In the **Selection** pane, click **Automated User Assignments**.

3 In the **Results** pane, select the Automated User Assignment you want to modify.

4 In the **Task** pane, under **General Tasks**, select **Properties**.

5 Modify the Automated User Assignment properties.

Changing the Priority of Automated User Assignments

When you create an Automated User Assignment, DLO assigns a priority to it so that when a user is a member of more than one domain and group, it is clear which Automated User Assignment will be used. The most recently created Automated User Assignments have the lowest priority. You can change the priority of Automated User Assignments.

To change the priority of automated user assignments

1 On the DLO navigation bar, click **Setup**.

2 In the **Selection** pane, click **Automated User Assignments**.

3 In the **Results** pane, select the Automated User Assignment for which you want to change the priority.

4 In the **Task** pane, under **Settings Tasks**, select **Move priority up** or **Move priority down**.

Viewing Automated User Assignment Properties

To view automated user assignments

1 On the DLO navigation bar, click **Setup**.

2 In the **Selection** pane, click **Automated User Assignments**.

3 In the **Results** pane, select an Automated User Assignment.

4 In the **Task** pane, under **General Tasks**, select **Properties**.

Deleting Automated User Assignments

You can delete Automated User Assignments when you no longer need them.

To delete an automated user assignment

1 On the DLO navigation bar, click **Setup**.

2 In the **Selection** pane, click **Automated User Assignments**.

3 Click the Automated User Assignment to be deleted.

4 In the **Task** pane, under **General Tasks**, click **Delete**.

5 Click **Yes**.

Related Topics

"Moving Desktop Agent Users to a New Network User Data Folder" on page 154

"Modifying Desktop Agent User Properties" on page 152

Configuring Global Exclude Filters

DLO global exclude options enable you to specify the attributes of files that you want to exclude from all backups, or that you do not want to compress, encrypt, or back up with Delta File Transfer. You can also exclude attachments to e-mails or specific e-mail folders from backup. Global excludes apply to both Profile backup selections and user created backup selections for all Desktop Agent users who back up to the DLO Administration Server on which the excludes are configured.

The files you exclude are listed on the **Include/Exclude** tab in the advanced view on the Desktop Agent and on the **Include/Exclude** tab for a profile's backup selection on the DLO Administration Console. Items configured for the global exclude list are not available for selection on the selection list.

Caution: Adding a global exclude will cause all previous backups matching the global exclude to be deleted.

To configure global excludes, see the following procedures:

"Specifying Files and Folders to Exclude from all Backups" on page 135

"Specifying E-mail to Exclude from all Backups" on page 136

"Specifying Files and Folders to Exclude from Compression" on page 137

"Specifying Files and Folders to Exclude from Encryption" on page 138

"Specifying Files and Folders to Exclude from Delta File Transfer" on page 139

"Using DLO Macros to Define Global Excludes" on page 141

Specifying Files and Folders to Exclude from all Backups

File and Folder global excludes are used to specify which files and folders, or file and folder types, are to be excluded from all backups for all users.

To specify files and folders to exclude from all backups

1. From the **Tools** menu in the DLO Administration Console, select **Global Excludes**.
2. Select the **Files/Folders** tab. Default Files/Folders global excludes are listed.
3. To exclude all files greater than a specific size, select the **Exclude all files greater than** check box and enter a size in KB.
4. To exclude all files modified before a specified date, select the **Exclude all files modified before** check box and enter a date.
5. To add a new Files/Folders global exclude, click **Add** and configure as described in the following table.

Table 2-23 Add Global Exclude Filter Dialog

Item	Description
Filter	The filter determines which files or folders will be excluded from backup by the global exclude. Type a file name, wildcard, or macro for the files you want to exclude. Examples: Wildcard: *.tmp File name: pagefile.sys Macro: %WINDIR% **Note:** When using wildcards, you must use the asterisk (*) wildcard. For example, `*.tmp` will return all results with the `.tmp` extension while `.tmp` will return only files explicitly named `.tmp`.
Description	Type a description of the global exclude.
Apply to	Indicate whether this global exclude should apply to files, folders, or both files and folders.

6. Click **OK**.
7. To edit a global exclude filter, click **Edit** and configure as described in the step 5.
8. To delete a global exclude filter, click the filter to be deleted and click **Delete**. Click **Yes** to delete the filter or **No** to cancel.
9. Click **OK**.

Specifying E-mail to Exclude from all Backups

E-mail global excludes are used to specify the type of e-mails to be excluded from all backups for all users.

Note: Lotus Notes e-mails cannot be filtered by attachment size or type.

Note: E-mail global excludes does not apply for VSS based PST backups.

To specify e-mail attachments to exclude from all backups

1. From the **Tools** menu in the DLO Administration Console, select **Global Excludes**.
2. Select the **E-mail** tab.
3. To exclude from all backup attachments greater than a specific size, select the **Exclude all attachments greater than** check box and enter a size in KB. This feature does not apply to Lotus Notes e-mails.
4. To exclude from all backup messages received before a specified date, select the **Exclude all messages received before** check box and enter a date.
5. To add a new e-mail global exclude, click **Add** and configure as follows.

Table 2-24 Add Global E-mail Exclude Filter Dialog

Item	Description
Attachment file type	The filter determines which attachment file types will be excluded from backup by the global exclude. **Note:** Lotus Notes e-mails cannot be filtered by attachment type. Filters can be file names or wildcards. Examples: Wildcard: *.tmp File name: pagefile.sys **Note:** When using wildcards, you must use the asterisk (*) wildcard. For example, *.tmp will return all results with the .tmp extension while .tmp will return only files explicitly named .tmp.
Mail folder name	Type the name of the mail folder you would like to exclude from backup.
Description	Type a description of the global exclude.

6 Click **OK**.

7 To edit a global e-mail filter, click the filter you want to change. Click **Edit** and configure as described in table 2-24, "Add Global E-mail Exclude Filter Dialog".

8 To delete a global e-mail filter, click the filter to be deleted and click **Delete**. Click **Yes** to delete the filter or **No** to cancel.

9 Click **OK**.

Specifying Files and Folders to Exclude from Compression

Compressed file global excludes are used to specify the type of files or folders to be excluded from compression for all users.

Note: Compression global excludes is not applicable for Dedupe enabled backups.

To specify files and folders to exclude from compression

1 From the **Tools** menu in the DLO Administration Console, select **Global Excludes**.

2 To exclude files or folders from compression, select the **Compressed Files** tab. Default compressed files global excludes are listed.

3 To exclude all files greater than a specific size from compression, select the **Exclude all files greater than** check box and enter a size in KB.

4 To add a new compressed file global exclude, click **Add** and configure as follows.

Table 2-25 Add Global Compression Exclude Filter Dialog

Item	Description
Filter	The filter determines which files or folders will be excluded from compression by the global exclude. Filters can be file names, wildcards or macros. Examples: Wildcard: *.tmp File name: pagefile.sys Macro: %WINDIR% **Note:** When using wildcards, you must use the asterisk (*) wildcard. For example, *.tmp will return all results with the .tmp extension while .tmp will return only files explicitly named .tmp.
Description	Type a description of the global exclude.

Table 2-25 Add Global Compression Exclude Filter Dialog (continued)

Item	Description
Apply to	Indicate whether this global exclude should apply to files, folders, or both files and folders.

5 Click **OK**.

6 To edit a global exclude filter, click the filter you want to change. Click **Edit** and configure as described in the "Add Global Compression Exclude Filter Dialog" table above.

7 To delete a global exclude filter, click the filter to be deleted and click **Delete**. Click **Yes** to delete the filter or **No** to cancel.

8 Click **OK**.

Specifying Files and Folders to Exclude from Encryption

Encrypted file global excludes are used to specify which files or folders, or file and folder types, are to be excluded from encryption for all users.

Note: Encryption global excludes is not applicable for Dedupe enabled backups.

To configure encrypted file global excludes

1 From the **Tools** menu in the DLO Administration Console, select **Global Excludes**.

2 To exclude files or folders from encryption, select the **Encrypted Files** tab. Default encrypted files global excludes are listed.

3 To exclude files greater than a specific size from encryption, check the **Exclude all files greater than** check box and enter a size in KB.

4 To add a new encrypted file global exclude, click **Add** and configure as follows.

Table 2-26 Add Global Encryption Exclude Filter Dialog

Item	Description
Filter	The filter determines which files or folders will be excluded from encryption by the global exclude. Filters can be file names, wildcards or macros. Examples: Wildcard: *.tmp File name: pagefile.sys Macro: %WINDIR% **Note:** When using wildcards, you must use the asterisk (*) wildcard. For example, *.tmp will return all results with the .tmp extension while .tmp will return only files explicitly named .tmp.
Description	Type a description of the global exclude.
Apply to	Indicate whether this global exclude should apply to files, folders, or both files and folders.

5 Click **OK**.

6 To edit a global encryption exclude filter, click the filter you want to change. Click **Edit** and configure as described in table 2-26, “Add Global Encryption Exclude Filter Dialog”.

7 To delete a global encryption exclude filter, click the filter to be deleted and click **Delete**.
Click **Yes** to delete the filter or **No** to cancel.

8 Click **OK**.

Specifying Files and Folders to Exclude from Delta File Transfer

Delta File Transfer global excludes are used to specify which files or folders, or file and folder types, are to be excluded from Delta File Transfer for all users.

Note: Delta File Transfer global excludes is not applicable for Dedupe enabled backups.

To specify files and folders to exclude from delta file transfer

1 From the **Tools** menu in the DLO Administration Console, select **Global Excludes**.

2 To exclude files or folders from Delta File Transfer, select the **Delta File Transfer** tab. Default Delta File Transfer global excludes are listed. File types excluded by default from Delta File Transfer are generally file types that do not benefit from this technology.

Note: Files and Folders backed up using Delta File Transfer are also compressed with standard compression. If a file is in a backup selection that uses Delta File Transfer, but is excluded from Delta File Transfer using a global excludes filter, it is still compressed with standard compression unless it is also excluded from standard compression using another global excludes filter.

3 To exclude files greater than a specific size from Delta File Transfer, select the **Exclude all files greater than** check box and enter a size in KB.

4 To exclude files smaller than a specific size from Delta File Transfer, select the E**xclude all files less than** check box and enter a size in KB.

5 To add a new Delta File Transfer global exclude, click **Add** and configure as follows.

Table 2-27 Add Global Delta File Transfer Exclude Filter Dialog

Item	Description
Filter	The filter determines which files or folders will be excluded from Delta File Transfer by the global exclude. Filters can be file names, wildcards or macros. Examples: Wildcard: *.tmp File name: pagefile.sys Macro: %WINDIR% **Note:** When using wildcards, you must use the asterisk (*) wildcard. For example, *.tmp will return all results with the .tmp extension while .tmp will return only files explicitly named .tmp.
Description	Type a description of the global exclude.
Apply to	Indicate whether this global exclude should apply to files, folders, or both files and folders.

6 Click **OK**.

7 To edit a global Delta File Transfer exclude filter, click the filter you want to change. Click **Edit** and configure as described in table 2-27, “Add Global Delta File Transfer Exclude Filter Dialog”.

8 To delete a global Delta File Transfer exclude filter, click the filter to be deleted and click **Delete**.
To delete the filter, click **Yes**, and to cancel, click **No**.

9 Click **OK**.

Excluding Files that are Always Open

On desktop computers running Windows XP and Windows 2000, the following folders and file types are generally always open and DLO is unable to back up these files. Adding these files to the Global Excludes list, or backup selection exclude list will prevent them from always being listed in the pending files list on the Desktop Agent.

- C:\Windows\System32\Config
- registry hives and logs, including *.DAT.LOG, *.LOG and the files system, SECURITY, default, SAM, and software
- C:\Windows\System32\wbem
- *.EVT
- *.LOG (in particular, STI_Trace.log, WIADEBUG.LOG, WIASERVC.LOG)
- *.DAT (in particular, NTUSER.DAT, USRCLASS.DAT)

Related Topics

“About Backup Selections” on page 102

“Configuring Global Exclude Filters” on page 134

Using DLO Macros to Define Global Excludes

The following macros are typically used for excluding files using the global exclude option, but can also be used in backup selections.

Table 2-28 Global Exclude Macros

Macro	Folder
%TEMP%	The temp directory for the user who is logged on.
%WINDIR%	The Windows directory. Example: `C:\Windows or C:\Winnt`

Table 2-28 Global Exclude Macros (continued)

Macro	Folder
%WEBTEMP%	The web cache for the user who is logged on.
%RECYCLED%	Recycle bins
%SYSTEM%	The Windows system directory. Example: `C:\Windows\system or C:\Winnt\system`

Symantec DLO Firewall Ports

You may have special port requirements for Symantec DLO if you use a firewall. Firewalls sometimes affect system communications between administration servers and remote systems that reside outside the firewall environment.

Symantec DLO uses the following ports:

Table 2-29 Symantec DLO Ports

Service or Process	Port	Port Type
Server Message Block (SMB) communication	135-139	TCP/UDP
Server Message Block (SMB) communication without NETBIOS	445	TCP/UDP
SQL	1434	TCP/UDP
SymantecDLOAdminSvcu.exe (DLO admin service)	3999 in listening mode	TCP/UDP
Additional ports	135 1037 441 1125 3527 6101 6103 6106	TCP
The default or any other port number specified during installation	8443	HTTPS
The default or any other port number specified during installation	8080	HTTP
SQL Server Port number if SQL Server is installed on a machine where Dedupe Server is not installed.		TCP

Service or Process	Port	Port Type
SQL Server Browser service port number if SQL Server is installed on a machine where Dedupe Server is not installed.	1434	UDP

Note: In a remote DB setup, if the database is installed on a Windows 2008 R2 server or on a Windows Server 2012 machine, while adding the ports 1434 UDP and 1433 TCP, select the **Domain** check box for the Profile.

Add firewall exceptions for the following:

- File and printer sharing
- Remote service management
- Windows management instrumentation

For Windows XP and Windows 2003 server machines, since Windows Management Instrumentation is not listed under Firewall settings, follow this procedure to enable firewall exception:

1. Run `gpedit.msc`.
   The **Local Group Policy Editor** window opens.
2. In the left pane, click **Computer Configuration.**
3. In the right pane, double-click **Administrative Templates > Network > Network Connections > Windows Firewall**.
4. If the computer is in the domain, then double-click **Domain Profile**, else double-click **Standard Profile**.
5. Click **Windows Firewall: Allow remote administration exception**.
6. On the **Action** menu, select **Properties**.
7. Click **Enable**, and then click **OK**.

The default instance of the SQL Server Database Engine listens on TCP port 1433. Named instances of the Database Engine are configured for dynamic ports. That is, an available port is selected when the SQL Server service is started. While connecting to a named instance through a firewall, configure the Database Engine to listen on a specific port, so that the appropriate port can be opened in the firewall.

How to configure the SQL Server to listen on a specific TCP port

To configure the SQL Server, refer to the instructions provided at

http://msdn.microsoft.com/en-us/library/ms177440(v=sql.105).aspx

How to find the port number for a particular named instance of SQL Server

1. Click **Start > Programs > Microsoft SQL Server > Configuration Tools > SQL Server Configuration Manager**.
2. Expand **SQL Server Network Configuration** and select **Protocols** for <instance name>.
3. Right-click **TCP/IP** and select **Properties**.
4. In the **TCP/IP Properties** window, select the **IP Addresses** tab.
   The port used by the SQL Server instance can be found either in the TCP Dynamic Ports for a dynamic port, or in the TCP Port for a static port.
5. You can also find the port number using the registry entry:
   `HKLM\Software\Microsoft\Microsoft SQL Server\<name of the instance>\MSSQLServer\SuperSocketNetLib\TCP`

Special Considerations for Installing Symantec DLO on Remote Computers

Before you install Symantec DLO to remote computers, the following must be considered:

Table 2-30 Special considerations for installing Symantec DLO on remote computers

Item	Description
Windows XP/Windows Server 2003	To push-install to a Windows XP/Windows Server 2003 computer, you must enable File and Printer Sharing on the Windows Firewall Exceptions list for the following ports: ■ 135 (RPC) ■ 1037 ■ 441 (RPC) For more information about the Windows Firewall Exception list, refer to the Microsoft Windows documentation. During the installation process, Symantec sets the Remote Launch and Remote Access security permissions for the Administrator’s group. You should enable the “Allow remote administration exception” group policy for the computer to which you push the installation.

Table 2-30 Special considerations for installing Symantec DLO on remote computers

Item	Description
Windows Vista/Windows 7/Windows Server 2012	To push-install to a computer that runs Windows Server 2008, you must enable certain items on the destination computer's Windows Firewall Exceptions list. You must enable the following items: ■ File and Printer Sharing ■ Windows Management Instrumentation (WMI) ■ Remote Service Management For more information refer to the Microsoft Windows documentation.
Symantec Endpoint Protection (SEP)11.0 or later	To push-install to a computer that runs Symantec Endpoint Protection (SEP) version 11.0 or later, you must configure SEP to share files and printers. The file and printer sharing feature is turned off by default.

IPv6 Support

Deploying Dedupe Server on IPv6 Network

To deploy the Dedupe Server on IPv6 network, the attribute value of the protocol for the different connector elements must be modified in the server.xml file.

The server.xml file is located at this path:

```
C:\Program Files\Symantec\Symantec DLO\Dedupe
\Tomcat\conf\server.xml
```

Modify the following lines in the file:

Change the protocol's attribute value in the following lines:

1 *Existing attribute value for protocol:*

```
<Connector connectionTimeout="20000" port="8080"
protocol="HTTP/1.1" redirectPort="8443" server=" "/>
```

Change to:

```
<Connector connectionTimeout="20000" port="8080"
protocol="org.apache.coyote.http11.Http11Protocol"
redirectPort="8443" server=" "/>
```

2 *Existing attribute value for protocol:*

```
<Connector SSLEnabled="true" SSLProtocol="TLS"
clientAuth="false" keystoreFile="dedupeserver.jks"
keystorePass="dedupeserver" maxThreads="200" port="8443"
```

```
protocol="org.apache.coyote.http11.Http11NioProtocol"
scheme="https" secure="true" server=" "/>
```

Change to:

```
<Connector SSLEnabled="true" SSLProtocol="TLS"
clientAuth="false" keystoreFile="dedupeserver.jks"
keystorePass="dedupeserver" maxThreads="200" port="8443"
protocol="org.apache.coyote.http11.Http11Protocol"
scheme="https" secure="true" server=" "/>
```

3 *Existing attribute value for protocol:*

```
<Connector port="8009" protocol="AJP/1.3"
redirectPort="8443"/>
```

Change to:

```
<Connector port="8009"
protocol="org.apache.coyote.ajp.AjpProtocol"
redirectPort="8443"/>
```

After you modify the values in the server.xml file, restart the Dedupe Server.

Chapter 3

Managing and Monitoring DLO

This section contains the following topics:

Managing Desktop Agent Users

The DLO Administrator manages Desktop Agent users from the DLO Administration Console. From this interface, users or groups of users can be manually added to DLO, enabled or disabled, moved to a new network share, or assigned a different profile.

Desktop Agent users are added to DLO either automatically using Automated User Assignments, or manually from the DLO Administration Console.

Related Topics

"About Automated User Assignments" on page 129

"Adding a Single Desktop User to DLO" on page 151

"Importing Multiple Users who have Existing Network Storage" on page 152

"Viewing a List of Desktop Agent users" on page 156

"Modifying Desktop Agent User Properties" on page 152

"Enabling or Disabling DLO Access for a Desktop User" on page 153

"Deleting a User from DLO" on page 153

"Moving Desktop Agent Users to a New Network User Data Folder" on page 154

Manually Creating New Network User Data Folders

If network shares already exist for desktop user backups, they can be added to DLO as network user data folders, or new shares can be created and added to DLO for this purpose. To create or use an existing network share as a network user data folder, the folder must have the appropriate security attributes.

To manually create network user data folders and set security attributes

1. Create or locate a network share on the computer where backup files will be stored.
2. Right-click the share you created in step 1, and then select **Properties**.
3. Click the **Sharing** tab.
4. Verify that **Share this folder** is selected.
5. Click **Permissions**.
6. Select the following permissions for user Everyone: Full Control, Change, Read
7. Click **OK**.
8. Click the **Security** tab.
9. Click **Advanced**.
10. Verify that the **Inherit from parent the permission entries that apply to child objects** check box is not selected.
11. Add Administrator and Everyone and give them full control permissions.
12. In this share, create a data folder for each user who will use this DLO Storage Location, or verify that a data folder already exists.
13. Right-click the data folder for a user.
14. Select **Properties**.
15. Select **Security**.
16. Verify that the **Inherit from parent the permission entries that apply to child objects** check box is not selected.

17 Add Administrator and the user who will be assigned to the user data folder to the share permission list.

18 Set full permission for Administrator and the user.

Adding a Single Desktop User to DLO

Desktop users can be configured manually rather than with Automated User Assignments (see "About Automated User Assignments" on page 129). This allows the use of existing network folders that are dedicated to storing backup data for specific users. These network folders become the DLO network user data folders.

When a single desktop user is added to DLO, the user data folders are added manually so DLO Storage Locations are not required, but they can be used if it is desirable to place the network user data folder in this location.

After adding a desktop user manually, the settings that you assign (the user data folder and the profile) are applied the first time the desktop user runs the Desktop Agent.

To add a single desktop user

1. On the DLO navigation bar, click **Setup**.
2. In the **Selection** pane, click **Users**.
3. In the **Task** pane, under **User Tasks**, click **New User**.
4. Select the appropriate options as described in the following table.

Table 3-1 New User Properties

Item	Description
Enable User	Select this option to enable this user to use the Desktop Agent, or clear it to prevent the user from using the Desktop Agent.
User	Browse to the user name or type it in the form DomainName\UserName.
Profile	Select the profile that you want to assign to this user.
User data folder	Do one of the following:

Table 3-1 New User Properties (Continued)

Item	Description
Network user data folder	Select this option and type the path or browse to an existing network user data folder where this desktop user's backup files will be stored. This must be an existing folder, and the security attributes must be set for the folder according to your organization's needs. For example, determine which users can access the folder. **Note:** A DLO Storage Location is not required when an existing network share is used as the network user data folder.
Storage Location	Select this option to choose an existing Storage Location. The network user data folder for the new user will be placed in this Storage Location.

Importing Multiple Users who have Existing Network Storage

If you want to configure multiple new desktop users who already have an existing location on the network to store data, you can import a list of the users using a comma separated values (CSV) file. This feature cannot be used to import network user data folders for existing Desktop Agent users.

The file must be in the following format and have the following information for each user:

user name, domain, profile, user data folder

Example `JSmith,enterprise,Default,\\Server1\Userdata\jsmith`

To import multiple desktop users from a file

1 On the DLO navigation bar, click **Setup**.

2 In the **Selection** pane, click **Users**.

3 In the **Task** pane, under **User Tasks**, click **Import users using wizard**.

4 Follow the instructions in the wizard.

Modifying Desktop Agent User Properties

1 On the DLO navigation bar, click **Setup**.

2 In the **Selection** pane, click **Users**.
Users are listed in the **Results** pane.

3 Select the user you want to modify.

4 In the **Task** pane, under **General Tasks**, select **Properties**.

5 Select the appropriate options as described in the following table.

Table 3-2 User Properties

Item	Description
Enable User	Select this option to enable this user to use the Desktop Agent, or clear it to prevent the user from using the Desktop Agent.
User	The name of the user. This field cannot be edited.
Profile	Select a profile to apply to this user.
network user data folder	This is the location where the user's backup files are to be stored. It cannot be modified. To move a user to a new location, see "Moving Desktop Agent Users to a New Network User Data Folder" on page 154.

Enabling or Disabling DLO Access for a Desktop User

This option allows to you either allow or prevent a user from using the Desktop Agent.

To enable or disable DLO access for a desktop user

1 On the DLO navigation bar, click **Setup**.

2 In the **Selection** pane, click **Users**. Users are listed in the results pane.

3 Select the user you want to modify.

4 In the **Task** pane, under **General Tasks**, select **Properties**.

5 Do one of the following:

- Clear the **Enable user** check box to prevent the desktop user from backing up data with the Desktop Agent
- Select the **Enable user** check box to allow the desktop user to back up data with the Desktop Agent

Deleting a User from DLO

If you want to permanently remove a user from the DLO database, you can delete the user's entry from DLO. Before deleting the user from the DLO Administration Console database, you should uninstall the Desktop Agent from the user's desktop. Otherwise, the user will automatically be re-added if the Desktop Agent is run by the user and a matching user assignment exists in DLO. If you cannot uninstall the Desktop Agent from the user's computer, disable the user. For more information, see "Enabling or Disabling DLO Access for a Desktop User" on page 153.

To delete a user from the DLO database

1 Uninstall the Desktop Agent from the user's computer.

2 On the DLO navigation bar, click **Setup**.

3 In the **Selection** pane, click **Users**.

4 Click the user or users you want to delete.

5 In the **Task** pane, under **General Tasks**, click **Delete**.

6 To delete the data stored in the user data folder, select the **Delete data stored in the user data folder** option. When you select this option, backup data is deleted from the network user data folder, but not from the desktop user data folder. When the Desktop Agent is uninstalled from the desktop computer, an option is provided to delete the desktop user data folder.

7 To delete the user, click **Yes** or **Yes to All**.

Note: If you delete a user from the DLO Administration Console without first uninstalling the Desktop Agent from the user's desktop, the Desktop Agent on that user's computers will close automatically.

Moving Desktop Agent Users to a New Network User Data Folder

When Desktop Agent users are moved to new network user data folders, the contents of each network user data folder is moved to a new directory. The new directories can be existing DLO Storage Locations or other directories on the network.

When the network user data folder is moved to a UNC location (for example, `\\myserver\userdata\username`) rather than an existing DLO Storage Location, permissions on the new location may need to be modified. The local administrator group and the owner of the files must have read and change permissions for the network user data folder, and the Everyone group should be removed.

For more information on using existing directories on the network as network user data folders, see "Manually Creating New Network User Data Folders" on page 150.

After the data is successfully moved, data in the old network user data folders is deleted. Subsequent backups will be stored in the new location for each user.

To move one or more Desktop Agent users to a new network user data folder

Note: When the transfer is complete, each affected Desktop Agent will shut down and then automatically restart within a 30 minute window.

1 On the DLO navigation bar, click **Setup**.

2 In the **Selection** pane, click **Users**.

3 Select one or more user to be moved.

4 In the **Task** pane, under **User Tasks**, click **Move network user data folder**.

5 Select the appropriate options as described in the following table.

Table 3-3 Move User

Item	Description
User	Lists the domain and user name of the selected user or users.
From	Lists the current network user data folder location.
Destination	
Move the user data folder to an existing Storage Location	Select this option to choose an existing Storage Location from the drop-down list. A new network user data folder will be created in the new Storage Location for each user who is moved.
Move the contents of the user data folder to an alternative location	Select this option to specify a new Storage Location. Type the path in the box provided, or click **Browse** and navigate to the new location. A new network user data folder will be created in the new Storage Location for each user who is moved.

6 Click **Start** to begin the data transfer.

Migrating a Desktop User to a New Computer

When a desktop user receives a new computer, DLO can be used to migrate user data to the new computer. DLO accomplishes this task by staging a user's backed up data on the new computer using a restore process. When the user logs in, the data is restored to the same location it occupied on the original computer. The final restoration of data occurs automatically when the user logs in and does not require a connection to the DLO Administration Server.

To migrate a desktop user to a new computer

1 Restore the user data as described in "Restoring Files and Folders from the DLO Administration Console" on page 162.

2 In step 8, select "Stage this user data on an alternate computer for a new DLO installation." The data is staged on the new computer.

When the owner of the staged data logs in to the new computer, DLO moves the staged data to the same location it occupied on the original computer, completing the data migration process.

Viewing a List of Desktop Agent users

To view the list of desktop agent users

1. On the DLO navigation bar, click **Setup**.
2. In the **Selection** pane, click **Users** to list users in the **Results** pane.

Managing Desktop Computers

Desktop computers can be easily managed from the DLO Administration Console. You can view and modify computer properties as well as enable, disable or delete computers from the console. In addition, an immediate backup can be run on one or more selected computers.

Modifying Computer Properties

Computer properties can be viewed and modified from the DLO Administration Console. Computer properties are based on the profile to which the desktop computer owner is assigned. Computer properties can also be changed by the desktop user if that user has sufficient rights assigned in the profile.

To view and modify computer properties

1. On the DLO navigation bar, click **Setup**.
2. In the **Selection** pane, click **Computers**.
3. Right-click the computer for which you want to modify properties, and click **Properties**.
4. To modify the backup schedule for the computer, click the **Schedule** tab.
5. Configure the schedule as described in the following table.

Table 3-4 Profile Schedule Dialog Box

Item	Description
Use Profile schedule	Select this option in the drop-down menu to use the scheduling options specified in the profile. **Note:** If this option is selected, additional settings on the **Schedule** tab cannot be modified.
Use customized schedule	Select this option in the drop-down menu to specify a customized schedule that differs from the profile schedule.
Run jobs	

Table 3-4 Profile Schedule Dialog Box (Continued)

Item	Description
Whenever a file changes	Select this option to back up files whenever they change. On NTFS drives, backups will occur automatically whenever a file changes. For FAT drives, you must enter a backup interval in the **Back up changed files every** field.
According to a schedule	Select this option to back up files according to a customized schedule. Click **Edit schedule** to configure the backup schedule. The backup schedule is configured in step 12 of “Creating a New Profile” on page 85.
Manually	Select this option to require that the DLO Administrator or desktop user initiate backups manually.
Log on/off options	
Automatically run jobs when logging on	Select this option to begin a backup after the desktop user logs on to the computer.
Automatically run jobs when logging off	Select this option to begin a backup when the desktop user logs off the computer.

6 To modify computer options, click the **Options** tab and configure the computer options as described in the following table.

Table 3-5 Additional Profile Options

Item	Description
Use Profile options	Select this option in the drop-down menu to use settings specified in the profile. **Note:** If this option is selected, additional settings on the **Options** tab cannot be modified.
Use customized options	Select this option in the drop-down menu to specify settings that differ from the profile options. **Note:** This option must be selected to enable access to additional settings on the **Options** tab.
Limit disk space usage on my computer to	Select this check box to limit disk space usage on the desktop computer. To limit the usage to a percent of drive space, select **%** and type the maximum percentage of drive space to use. To limit the usage to a specific size, select **MB** and type the maximum number of MB to use on the local drive.
Log file maintenance	

Table 3-5 Additional Profile Options (Continued)

Item	Description
Keep log files for a minimum of (days)	Type the minimum number of days to keep log files. Log files will not be deleted until they are at least as old as specified. **Note:** Log files will not be deleted until their combined size exceeds the setting for the combined size of all log files, which is discussed below.
After minimum number of days, delete oldest log files when combined size exceeds (MB)	Type the maximum combined size of all log files to be retained before the oldest log files are deleted. **Note:** You may have more than the specified number of MB of log files stored if none of the log files are as old as specified in the **keep log files for a minimum of (days)** setting.
Logging options	
Log groom messages	Select this check box to create logs for grooming operations.
Log information messages for backup	Select this check box to create logs for all backup operations.
Log warning messages	Select this check box to create logs for all operations that generate warnings.
Mail options	
Enable incremental backups of Outlook PST files	Select this check box to enable incremental backups of Microsoft Outlook Personal Folder (PST) files. Incremental backups must be enabled to allow PST files to be backed up while they are open. If this option is not selected, then PST files that are configured in Outlook will be fully backed up each time the PST file is saved, which generally occurs when Outlook is closed. When Outlook PST files are backed up incrementally, only one revision is maintained regardless of the number of revisions set in the backup selection. **Note:** DLO is unable to perform incremental backups of Outlook PST files unless Outlook is your default mail application. When you restore Microsoft Outlook PST files, the restored PST file will differ from the original PST file as explained in “Restoring Microsoft Outlook Personal Folder Files” on page 289. **Note:** Synchronized files cannot be backed up incrementally. For more information, see “Backing up Outlook PST Files Incrementally” on page 265.

Table 3-5 Additional Profile Options (Continued)

Item	Description
Enable incremental backups of Lotus Notes email files	Select this check box to enable incremental backups of Lotus Notes e-mail files. Additional configuration may be necessary. See “Backing up Lotus Notes NSF Files Incrementally” on page 267. When Lotus Notes NSF files are backed up incrementally, only one revision is maintained regardless of the number of revisions set in the backup selection.

7 To view the computer backup folders, click the **Backup Folders** tab.

8 To modify the computer backup selections, click the **Backup Selections** tab.
See “Adding a Backup Selection” on page 105. Profile backup selections are not listed, and can only be modified directly in the profile as described in “Modifying a Backup Selection” on page 114.

9 To view synchronized selections for a computer schedule, click the **Synchronized Selections** tab.
Synchronized selections can only be viewed from the Administration Console. They are configured on the Desktop Agent as described in “Synchronizing Desktop User Data” on page 277.

10 To view and modify connection policies, click the **Connection Policies** tab.
Profile defined connection policies can only be modified in the profile. See “Customizing Connection Policies” on page 274.

Enabling or Disabling a Desktop Computer

When a computer is disabled, the Desktop Agent remains on the desktop computer. The Desktop Agent can be used to restore files and view history, but backups are disabled and the user cannot modify Desktop Agent settings.

To enable or disable a desktop computer

1 On the DLO navigation bar, click **Setup**.

2 In the **Selection** pane, click **Computers**.

3 In the **Results** pane, select one or more computers to be enabled or disabled.

4 Right-click the selected computers and click **Enable** to enable the Desktop Agent to run on the selected computers, or click **Disable** to prevent the Desktop Agent from running on the selected computers.

Deleting a Desktop Computer from DLO

Deleting a desktop computer from DLO removes the computer from the DLO database and deletes the backed up files. This feature is most commonly used for a desktop computer that is no longer in use. Deleting a computer does not disable the Desktop Agent software. If subsequent backups are performed by the Desktop Agent, the computer entry will be added back to DLO. To prevent further backups from the computer, disable the computer rather than deleting it.

To delete a desktop computer from DLO

1 On the DLO navigation bar, click **Setup**.

2 In the **Selection** pane, click **Computers**.

3 In the **Results** pane, select one or more computers to be deleted.

4 In the **Task** pane, under **General Tasks**, click **Delete**.

5 When asked if you want to delete each selected computer and all backup files, click **Yes**.

Backing up a Desktop from the Administration Console

The DLO Administration Console can be used to run an immediate backup on one or more desktop computers. This allows the administrator to force a backup of a computer running in manual or scheduled mode.

To run an immediate backup on a desktop computer

1 On the DLO navigation bar, click **Setup**.

2 In the **Selection** pane, click **Computers**.

3 In the **Results** pane, select one or more computers on which to run an immediate backup.

4 In the **Task** pane, under **Computer Tasks**, click **Run backup now**.

Setting Blackout Windows

DLO can be configured to stop backups at specific times to selected file servers, or to file servers managed by a specific maintenance server. This is done by configuring blackout windows. When a blackout window is configured for a selected resource, backups to network user data folders are suspended during the specified period.

Blackout windows are specific to the resource for which they are created. To use the same schedule for two different resources, you must configure them separately.

To configure a blackout window for a network resource

1 On the DLO navigation bar, click **Setup**.

2 In the **Task** pane, under **Tool Tasks**, click **Blackout windows**.

3 From the **File Server** list, select a network resource for which you want to configure a blackout window.

4 Do one of the following:

- To edit an existing schedule, select it from the drop-down menu.
- To create a new schedule click **New**.

5 Configure the schedule as described in the following table.

Table 3-6 Blackout Window Schedule

Item	Description
Enable Schedule	Select this check box to activate this schedule.
Occurs	Select the frequency of occurrence. Selections include **on a specific date** and **weekly**.
Starts at	Enter the start time for the blackout window. For a blackout window on a specific date, enter the date on which the blackout window is to start. For a weekly blackout window, select the day of the week on which the blackout window is to start.
Ends at	Enter the end time for the blackout window. For a blackout window on a specific date, enter the date on which the blackout window is to end. For a weekly blackout window, select the day of the week on which the blackout window is to end.

6 Click **OK**.

Deleting a Blackout Window Schedule

To delete a blackout window schedule

1 On the DLO navigation bar, click **Setup**.

2 In the **Task** pane, under **Tool Tasks**, click **Blackout Windows**.

3 Under **Schedules**, select the schedule to be deleted.

4 Click **Delete**.

5 Click **OK**.

Restoring Files and Folders from the DLO Administration Console

The administrator can restore files and folders to a desktop computer from the DLO Administration Console.

Note: DLO can overwrite a file which is in use by staging the file to be restored when the desktop computer restarts. Using this feature requires that the currently logged on user of the desktop computer has administrative rights on the desktop computer. Alternatively, the file can be restored by first closing the application which is using the file, or by restoring the file to an alternate location.

To restore files and folders from the DLO administration console

Note: Outlook should be installed on the machine where DLO Administration Console exists, and on the machine from where the emergency restore is done

1. On the DLO navigation bar, click **Restore**.
2. In the **Computer** pane, click the desktop from which the data to be restored originated.
3. In the **Backup Folder** pane tree view, select the folder containing the files you want to restore.
4. To restore the entire folder, check the folder in the **Backup Folder** pane.
5. To restore specific files, check the files in the **File Version** pane.
6. If multiple versions exist for a file, select the radio button for the file version you want to restore.

   Note: When a desktop user deletes an original file, the backup files are retained until they are deleted by the file grooming process. If an original file has been deleted, but backup files are still available, the icon for the file in the restore view will have a small red ‘x’ to indicate the deletion of the original file. See “File Grooming” on page 257 for more information.

7. In the **Task** pane, under **Restore Tasks**, click **Restore files** to open the Restore dialog.

8 Select the appropriate options from the following table.

Table 3-7 Restore Dialog Box

Item	Description
Restore destination	
Restore to original computer	Select this option to restore the selected files or folders to the computer from which they were originally backed up. **Note:** When files or folders are restored to the original desktop computer, the job is submitted to the Desktop Agent and is run when the Desktop Agent connects to the DLO Administration Server. The job may run immediately if the desktop computer is currently on the network, or the job may be pending for some time if the desktop computer is not connected to the network.
Restore to original folder	Select this option to restore the file or folder to its original location.
Redirect the restore to an alternate folder	Select this option to restore the file or folder to a different location on the original desktop. Click **Browse** to browse to the folder where you would like to restore the file.
Restore to an alternate computer	Select this option to restore the selected items to a network or local drive on a computer other than the one from which they were originally backed up. **Note:** When files or folders are restored to a folder on an alternate computer, the restore job is processed immediately from the network user data folder by DLO. The job is not queued to the Desktop Agent.
Redirect the restore to a folder on an alternate computer	Select this option to restore the data to a selected folder on an alternate computer.
Stage this user data on an alternate computer for a new DLO installation	Select this option to migrate user data to a new computer. See "Migrating a Desktop User to a New Computer" on page 155 for more information.
Preserve folder structure	Select this check box to restore the data with its original directory structure intact. If you clear this option, all data (including the data in subdirectories) is restored to a single folder in the path you specify.

Table 3-7 Restore Dialog Box (Continued)

Item	Description
Restore Options	
If file already exists:	Select **Do not overwrite** to cancel the restoration of files that already exist in the destination folder. Select **Prompt** to be prompted before overwriting the file if it already exists in the destination folder. Select **Overwrite** to overwrite the file without prompting if it already exists in the destination folder.
Restore deleted files	Select this option if you want to restore files even though the original files have been deleted.
Preserve security attributes on restored files	Select P**reserve security attributes on restored files** to preserve security information in restored files. You may need to uncheck this box to successfully restore a file if the source file security conflicts with the destination security. Unchecking this option causes the security information to be removed from the restored file.

9 Click **OK**.

Note: If you customize NTFS permissions or directory attributes, such as compression or encryption for files or folders, you must reapply these settings after restoration. If you use a password for your PST file, you must reset the password after restoring your PST file.

10 In the **Restore Summary** dialog box, review the selected restore settings, and do one of the following:

- Click **Print** to print a copy of the restore summary
- Click **Restore** to continue with the restore

11 Click **OK** when the restore job completes.

Searching for Files and Folders to Restore

To search for desktop files and folders to restore

1 On the DLO navigation bar, click **Restore**.

2 In the **Computer** pane, click the desktop on which you would like to search for files to restore.

3 In the **Task** pane, under **Restore Tasks**, click **Search for files to restore**.

4 Select the appropriate options as described in the following table.

Table 3-8 Search Dialog Box Options

Item	Description
Search for file names with this text in the file name	Type all or part of the name of the file or folder you want to find. Wildcard entries are accepted, for example *proj.doc.
Modified	Select this option to search for files that were modified during a specific time frame, and then select the time frame.
Today	Select this option to search for files modified on the current calendar day.
Within the past week	Select this option to search for files modified in the last calendar week.
Between	Select this option to search for files modified during a range of days.
Of the following type	Select this check box to select a file type from the list provided.
Of the following size	Select this check box and then enter information as follows: ■ Select from **equal to**, **at least,** or **at most** in the first drop-down menu ■ Type a file size ■ Select **KB**, **MB,** or **GB**

5 Click **Search**.

6 In the **Results** pane, check the items to be restored.
In some cases the Restore Search view may contain duplicate entries for the same file. If this occurs, you can select either file to restore and receive the same outcome.

7 Click **Restore**.

8 Select the appropriate options as outlined in "Restoring Files and Folders from the DLO Administration Console" on page 162.

9 Click **OK**.

Backup and Recovery of DLO Servers and User Data

DLO stores information in two major locations: the DLO Administration Server and the File Server. The DLO Administration Server stores the configuration database and the File Server stores the user data. The following recovery scenarios are discussed:

- "Recovering Data for a Single User Emergency Restore" on page 167
- "Recovering Data for a Single User Without DLO Emergency Restore" on page 168
- "Recovering a Damaged or Corrupted DLO Administration Server" on page 168
- "Recovering a Damaged or Corrupt File Server" on page 169

This topic assumes that both the DLO Administration Server and File Server are periodically backed up to another disk, tape, or other media. Also note that for many DLO installations the administration server and file server are on the same computer.

About Encrypted User Data

DLO encrypts user data using a user-specific, randomly generated encryption-key. The encryption-keys are stored in DLO's configuration database on the DLO Administration Server. The encryption-keys are also stored, in encrypted form, on the File Server, as detailed in the next section.

About DLO Emergency Restore and Recovery Passwords

DLO's Emergency Restore feature is used to recover Desktop Agent user data from the File Server in the event that the configuration database is lost. Emergency Restore can also simplify the task of restoring user data for users that have been deleted using the DLO Console. To use the Emergency Restore feature, a Recovery Password must have been established before the database was lost or the user was deleted. If user data is restored from another media then the Recovery Password that was in effect when the user data was backed up must be used to recover the data.

A Recovery Password is established when the DLO Console is first launched. For older versions of DLO, a recovery password had to be manually established using the DLO command line interface. The recovery password is used to encrypt each user's encryption-key so the key can safely be stored on the File Server. The Emergency Restore feature prompts the administrator for the Recovery Password, which is used to decrypt the user's encryption-key. The encryption-key is then used to decrypt the user's data. If a recovery password has not been established the Emergency Restore feature cannot be used to restore encrypted user data.

Changing Recovery Passwords

If the Recovery Password must be changed the administrator must be aware that the former Recovery Password will still be in effect for former backups of the File Server.

The Recovery Password should only be changed if mandated for security reasons, such as a compromised password. If possible the Recovery Password should never be changed. Changing or establishing a Recovery Password will never aide in restoring existing user data. In fact, it can make it more difficult: changing the Recovery Password can result in multiple Recovery Passwords being in use at the same time.

For example, consider the case where a recovery password “pwd1” is established when DLO is installed. Each user's encryption-key is encrypted with the Recovery Password stored on the File Server. When the File Server is backed up, the backup copies all use the Recovery Password “pwd1”. If the recovery password is subsequently changed to “pwd2”, the user encryption-keys on the File Server will be changed to be encrypted with the new Recovery Password. Subsequent backups of the File Server will use the Recovery Password “pwd2”. Now there are backups of the File Server using both “pwd1” and “pwd2” as the Recovery Password. When the Emergency Restore feature is used, the administrator will have to use the Recovery Password that was in affect at the time the File Server was backed up.

Deleting a User using the DLO Console

When a user is deleted using the DLO Console, all data associated with the user is deleted. This includes the configuration data stored on the DLO Administration Server, and the user data stored on the File Server. The method for restoring data for a deleted user depends on whether a Recovery Password has been created or not.

Recovering Data for a Single User Emergency Restore

The Emergency Restore feature can be used to restore data for a deleted user if the user data can be restored from a backup of the File Server and a Recovery Password was established prior making the backup. See the section “About DLO Emergency Restore and Recovery Passwords” on page 166 for more information on Recovery Passwords.

To recover data for a single user emergency restore

1. Restore the user data to its original location on the File Server or to any other temporary location.
2. Run the `-emergencyrestore` command to restore the data to DLO.

   ```
   dlocommandu -emergencyrestore <usersharepath> -w
   <RecoveryPassword> -ap <destination-path>.
   ```

Note: If a user account that does not have administrator privileges is used to restore data, then open the command prompt by selecting the **Run as Administrator** option, and then run the command. Else, the files will not be restored.

Recovering Data for a Single User Without DLO Emergency Restore

If the Recovery Password was not established or has been lost, restoring data for a deleted user requires that both the DLO Administration Server and the File Server be restored to a single point in time before the user was deleted.

1. Take both the File Server and DLO Administration Server offline.
2. Back up both servers. Ensure that the backup includes the DLO configuration database and the all user data. This backup will be used to restore DLO back to its current state once the data is recovered. If any DLO data is not backed up it may be impossible to return to the current state.
3. Restore the user data to the File Server. If possible, restore just the data for the user being restored. If unsure, the entire volume on the File Server can be restored, provided that precaution was taken in step 2 to ensure the entire volume was backed up.
4. Restore the configuration database to the DLO Administration Server. The default database path is `C:\Program Files\Symantec\Symantec DLO\Data.`
5. Restart the DLO Administration Server.
6. Use the DLO Console to restore the user's data. Select “**Restore to an alternate computer**” and restore the data to a temporary location.
7. Restore both the File Server and DLO Administration Server back to the most recent state.

Recovering a Damaged or Corrupted DLO Administration Server

There are two cases for recovering a damaged or corrupted DLO Administration Server.

Case 1

A non-system disk on the administration server fails or is otherwise corrupted.

The recovery procedure for Case 1 is as follows

1. Fix or replace the failed disk.

2 Restore the entire disk from the backup copy.

3 Restart the computer.

Case 2

The administration server's system hard drive fails, or the server’s computer needs to be replaced with a new computer then the recovery procedure is as follows:

The recovery procedure for Case 2 is as follows

1 Setup the computer with the operating system software. Be sure to use the same computer name as the failed DLO Administration Server.

2 Install DLO on the new administration server. Be sure to use the same version of DLO as was installed on the failed server.

3 Restore the DLO database files, overwriting the database files created when DLO was installed. The default database path is `C:\Program Files\Symantec\Symantec DLO\Data.`

4 Restart the computer.

Recovering a Damaged or Corrupt File Server

If a non-system disk on the File Server fails or is otherwise corrupted the recovery procedure is as follows:

1 Fix or replace the failed disk.

2 Restore the entire disk from the backup copy.

3 Restart the computer.

If the File Server's system hard drive fails, or the file server computer needs to be replaced with a new computer then the recovery procedure is as follows:

1 Setup the computer with the operating system software. Be sure to use the same computer name as the failed File Server.

2 If the File Server had the DLO Maintenance Server installed, then install the DLO Maintenance Server on the computer. Be sure to use the same version of DLO as was installed on the failed File Server.

3 Restore the DLO file data.

Backing up and Restoring the DLO File Server and Database

Note: This process is applicable to the setup where only DLO components are installed and configured.

You can use Symantec DLO to back up the DLO Storage Locations, network user data folders, and the DLO database.

To back up Desktop Agent user data, create a backup job and include the DLO Storage Location or network user data folder in the backup selection. To restore Desktop Agent user data from DLO, restore the data from DLO to a DLO Storage Location or network user data folder, and then use the DLO Administration Console to restore data to the desktop user data folder.

To back up the DLO database, use the `-backup` command as described in "DLO Database Maintenance" on page 238 to create a copy of the database, and then create a backup job in DLO to back up this copy of the database. Use the `-restore` command to restore the database from a specific backup file.

Backing up and Recovering Data in a DLO-Dedupe Setup

Note: This recovery process is applicable to the setup where the DLO and Dedupe components are installed and configured together.

When a DLO Admin server is configured with a Dedupe Server, the following components form a single logical entity in time.

- DLO configuration database
- Dedupe Server database files
- DLO file data in file server
- Dedupe Storage Location data

Hence, the backup and restore of these components should be performed together at a single logical point in time (PIT).

PIT across all the components requires the data writes to be stopped on all the components. The data writes can be stopped by disconnecting the individual components from the network or the Dedupe Server can be switched to maintenance mode by scheduling a Maintenance Window from the DLO Administration Console.

Backup

- Schedule a Maintenance Window with sufficient time out for backing up all components. If backup time cannot be estimated in advance, then a time out of '9999' minutes can be specified.
- Back up all the components and tag them together for easy identification of the same Point in Time for all the components.
- Stop the Maintenance Window from the DLO Administration Console.

For more information on scheduling or stopping a Maintenance Window using the DLO Administration Console, see “Dedupe Server Maintenance” on page 82.

You can also use the command line option for scheduling a Maintenance Window. For more information, see “Command Line Option to Schedule Maintenance Window” on page 83.

Restore

In case of a disaster, data of all the components should be restored to a suitable logical PIT backup.

To restore the data, follow these steps:

1. Shut down the Dedupe Server if it is running.
2. Restore all components data to the same logical Point in Time.
3. Run the following command:

   ```
   DDAdminCU.exe -ConfirmDR <HTTPS Port Number>
   ```
4. Start the Dedupe Server.

It is recommended to follow this procedure for backup and restore operations, and thus prevent data loss or any issue related to data integrity.

Monitoring DLO Job Histories

Use the History view on the DLO Administration Console to view information about the status of Desktop Agent jobs. These jobs include backup, restore, synchronization, and move user jobs. History logs are generated by each desktop running the Desktop Agent and are viewed in either the DLO Administration Console or the Desktop Agent Console. You can filter history logs so that old or less important logs are not displayed, or so that only backup or restore job logs display.

Viewing the DLO Job History

By default, the history logs are updated when a job runs and an hour has passed since the last update. However, if the job's status changes, the history log is updated immediately to reflect the new status.

To display the history view in the DLO administration console

- ◆ On the DLO navigation bar, click **History**.

  The History view includes a computer history and a job history for each desktop that is displayed. The History pane displays all desktops that are backed up with the Desktop Agent and provides the summary of information as described in the following table.

Table 3-9 Computer History pane

Item	Description
User	The user name of the user who is logged on to the desktop that generated the message.
Computer	The name of the desktop that generated this message.
Last Backup Result	The outcome of a completed backup, for example, Success, Warnings, Failed, Cancelled. For descriptions of possible backup outcomes, see "DLO System Summary options" on page 70.
Profile	The name of the Profile to which the desktop user who is logged on to the desktop belongs. For more information on profiles, see "About DLO Profiles" on page 84
Backup Mode	The backup mode specified in the profile. Backup modes include: ■ Continuous: The backup occurs whenever a file changes ■ Scheduled: The backup occurs according to a schedule ■ Manual: The backup occurs when initiated by the desktop user
Desktop Data Folder Size	The current size of the desktop user data folder.
Network Data Folder Size	The current size of the network user data folder.
Network Data Folder Path	The location of the network user data folder.

The Job History pane displays information as described in the following table.

Table 3-10 Job History pane

Item	Description
Start Time	The time the job was started.
End Time	The time the job ended.
Operation	The operation performed in this job, such as backup or restore.
Status	The current status of the job, such as active, completed, completed with errors, completed with warnings, cancelled, or failed.

Table 3-10 Job History pane (Continued)

Item	Description
Files Protected (Desktop)	The number of files copied to the desktop user data folder during the job.
Size Protected (Desktop)	The total bytes of data copied to the desktop user data folder during the job.
Files Protected (Network)	The number of files copied to the network user data folder during the job.
Size Protected (Network)	The total bytes of data copied to the network user data folder during the job.
Errors	The number of errors, if any, that were generated during the job.

Setting Job History View Filters

The job history view can be filtered to show only the type of jobs you wish to view. You can filter jobs by type, alerts received during the job, or by the time period in which the job was run.

To set job history view filters

1. On the DLO navigation bar, click **History**.
2. Click the desktop for which you want to view the history.
3. On the **Task** pane, under **Job History View Filters**, select one of the following options.

Table 3-11 Type of Jobs Viewed in the History View

Item	Description
List all jobs	Lists history logs for all jobs that have run on the selected desktop. These may include backup, synchronization, restore, or move user jobs.
List backup jobs only	Lists history logs only for backup jobs that have run on the selected desktop.
List restore jobs only	Lists history logs only for restore jobs that have run on the selected desktop.

4 To filter job history logs based on alerts received, select one or more of the following options.

Table 3-12 Selections to Filter Job Histories Based on Alerts Received

Item	Description
Show successful jobs	Lists history logs for all successful jobs on the selected desktop.
Show jobs with warnings	Lists history logs for all jobs that generated warnings on the selected desktop.
Show jobs with errors	Lists history logs for all jobs that generated errors on the selected desktop.
Show cancelled jobs	Lists history logs for all jobs that were cancelled on the selected desktop.

5 To set a time frame for filters to be displayed, select one of the following options.

Table 3-13 Time Frame for Job Histories viewed

Item	Description
Show last 24 hours	Lists history logs that have been generated in the last 24 hours, and that meet all other filtering criteria.
Show last 7 days	Lists history logs that have been generated in the last 7 days, and that meet all other filtering criteria.
Show all	Lists all history logs that also meet all other filtering criteria.

Viewing History Logs

History logs are listed for each job on a desktop computer. They are viewed in the DLO Administration Console History view.

To view a history log in the DLO administration console

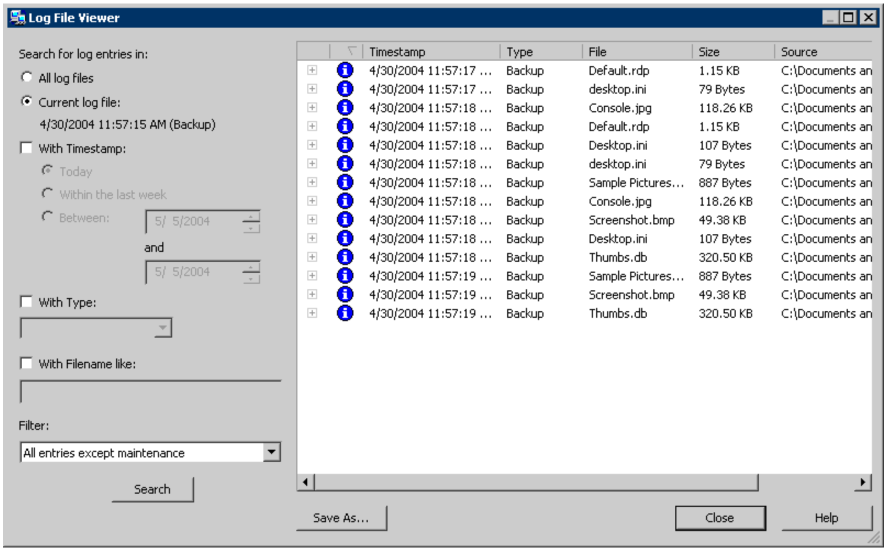
1 On the DLO navigation bar, click **History**.

2 In the **History** pane, select the computer for which you want to view a history log.

3 In the **Job History** pane, click the log you want to view.

4 In the **Task** pane, under **General Tasks**, click **View history log file** to display the log file viewer with all log messages for this job.

Log file viewer



Log File Viewer

Search for log entries in:

○ All log files

● Current log file:

4/30/2004 11:57:15 AM (Backup)

□ With Timestamp:

● Today

○ Within the last week

○ Between: 5/ 5/2004 and 5/ 5/2004

□ With Type:

□ With Filename like:

Filter: All entries except maintenance

Timestamp	Type	File	Size	Source
4/30/2004 11:57:17 ...	Backup	Default.rdp	1.15 KB	C:\Documents an
4/30/2004 11:57:17 ...	Backup	desktop.ini	79 Bytes	C:\Documents an
4/30/2004 11:57:18 ...	Backup	Console.jpg	118.26 KB	C:\Documents an
4/30/2004 11:57:18 ...	Backup	Default.rdp	1.15 KB	C:\Documents an
4/30/2004 11:57:18 ...	Backup	Desktop.ini	107 Bytes	C:\Documents an
4/30/2004 11:57:18 ...	Backup	desktop.ini	79 Bytes	C:\Documents an
4/30/2004 11:57:18 ...	Backup	Sample Pictures...	887 Bytes	C:\Documents an
4/30/2004 11:57:18 ...	Backup	Console.jpg	118.26 KB	C:\Documents an
4/30/2004 11:57:18 ...	Backup	Screenshot.bmp	49.38 KB	C:\Documents an
4/30/2004 11:57:18 ...	Backup	Desktop.ini	107 Bytes	C:\Documents an
4/30/2004 11:57:18 ...	Backup	Thumbs.db	320.50 KB	C:\Documents an
4/30/2004 11:57:19 ...	Backup	Sample Pictures...	887 Bytes	C:\Documents an
4/30/2004 11:57:19 ...	Backup	Screenshot.bmp	49.38 KB	C:\Documents an
4/30/2004 11:57:19 ...	Backup	Thumbs.db	320.50 KB	C:\Documents an

5 To filter the results, select the appropriate options as described in the following table.

Table 3-14 Log File Viewer Filtering Options

Item	Description
Search for log entries in	
All log files	Select this option to show all log entries in the log file viewer.
Current log file	Select this option to search only those log entries in the current log file.
With timestamp	Select this check box to search only those log entries within a specified time period. The options include: ■ Today: Show only log files that were created today ■ Within the last week: Show all log files created in the last week ■ Between dates: Show all log files created between the dates entered

Table 3-14 Log File Viewer Filtering Options (Continued)

Item	Description
Of the following type	Select this check box to show only logs of the indicated type. The available selections will vary depending on the log file, but may include the following: ■ Backup ■ Restore ■ Move User ■ Maintenance ■ Dedupe
With File names containing	Select this check box to enter a file name, or file type. Wildcard entries are supported. Example: *gold.doc **Note:** When using wildcards you must use the '*' wildcard. For example, *.tmp will return all results with the .tmp extension while .tmp will return only files explicitly named .tmp.
Limit search to	Select this check box to limit the log files displayed to one of the following types of log entries: ■ Informational entries only ■ Error and warning entries only ■ Error entries only ■ Warning entries only ■ Local data folder entries only ■ Local data folder error entries only ■ Network data folder entries only ■ Network data folder error entries only

6 Click **Search**.

7 Double-click a log entry to view additional details.

8 Click **Close**.

Searching History Logs

History log files are easily searched using the Log File Viewer. This enables you to refine the list of jobs to only those of interest.

To search for log files using the DLO administration console

1 On the DLO navigation bar, click **History**.

2 In the **Task** pane, under **General Tasks**, click **Search log files** to display the log file viewer.

3 Set filtering options as discussed in step 5 on page 175.

4 Click **Search**.

5 Double-click a log entry to view additional details.

6 Click **Close**.

Monitoring Alerts on the DLO Administration Console

Alerts appear in DLO when the system needs administrator attention. Alerts help the DLO administrator understand the current condition of DLO jobs by displaying information on jobs.

Alerts can be generated to provide general information, or they can be in response to a problem. When an alert is generated due to a problem, the alert contains information about the problem, and in some cases, recommendations on how to fix it.

The DLO Administrator can choose to display all alerts, or limit the type of alerts that appear.

Active alerts display the alerts that are active in the system and need a response from the operator. Alert history displays alerts that have been responded to or alerts that have been automatically cleared from the system.

In addition, the status bar at the bottom of the screen displays an alert icon. The icon that displays in the status bar is for the most severe type of alert in the Active alerts list. Therefore, if the current or most recent alert is not the most severe, the icon in the status bar will not match the icon for the most recent alert in the alert list.

The Desktop Agent filters the alerts to minimize the load on DLO. By default, alerts are limited to one of each type in 24 hours. For example, you will see only one "*Local Out of Disk Condition*" alert in a 24-hour period from a desktop running the Desktop Agent.

Note: "*Backup/Restore complete*" alerts cannot be filtered. If you enable these alerts, they are generated each time a backup or restore job completes.

Active alerts that are older than a specified number of days are cleared and moved into the alert history. The alerts in the history will be deleted if they have been cleared for more than a specified number of days.

If an alert is manually cleared, it is moved into the alert history. Deleting an alert manually removes it permanently.

You can set up DLO to notify recipients when alerts occur. See "Configuring Alerts for Notification" on page 183 for more information.

The following table describes the alert types.

Table 3-15 Alert Categories

Alert Type	Description
Informational	Notifies you that an expected action has occurred, such as the successful completion of a backup or restore job.
Warning	Notifies you of a potential issue. For example, an alert is generated when a backup has not been completed on a desktop within a given time frame, or if the disk quota limitations are being approached.
Error	Notifies you of an active or pending danger to the application or its data. An error would be generated, for example, if a backup failed to complete, or if a desktop has exceeded its disk quota limitations.

The following table describes the possible alerts.

Table 3-16 DLO Alerts

Type	Name	Description
Errors		
	A backup job has completed with errors	A backup job has completed, but errors were generated.
	A restore job has completed with errors	A restore job has completed, but errors were generated.
	An error has occurred on the file server	
	Desktop user data folder disk space full	The volume containing the desktop user data folder is full. There is insufficient free disk space to back up the current file. The file will be copied directly to the network user data folder.
	Desktop user data folder storage limit has been reached	The specified disk storage limit was reached when attempting to add a new revision to the desktop user data folder.

Table 3-16 DLO Alerts (Continued)

Type	Name	Description
	File name, directory name, or volume label syntax is incorrect.	Indicates either a storage system problem that requires attention, or a file name denied by SRM software. If the latter, these files should be added to DLO's global exclude list. See "Configuring Global Exclude Filters" on page 134 for more information.
	Network user data folder disk space full	The volume containing the network user data folder is full. There is insufficient free disk space to back up the current file.
	Network user data folder storage limit has been reached	The specified disk storage limit was reached when attempting to add a new revision to the network user data folder.
	Unable to configure the Desktop Agent	A new user has connected, but for an unknown reason, cannot be configured properly.
	Suspend backup and alert administrator on throttling failure	The backup job has been suspended because of a throttling failure.
	Throttling failed during backup	A throttling job has failed during backup.
Warnings		
	A backup job has completed with warnings	A backup job has completed, but warnings were generated.
	A restore job has completed with warnings	A restore job has completed, but warnings were generated.
	A restore job has not completed in 1 hour	A restore job was submitted, but an hour has passed and the restore job is not complete.
	A restore job has not completed in 12 hours	A restore job was submitted, but 12 hours have passed and the restore job is not complete.
	A restore job has not completed in 24 hours	A restore job was submitted, but 24 hours have passed and the restore job is not complete.
	Desktop user data folder approaching storage limit	The amount of stored backup data in a user's desktop user data folder is approaching the specified size limit.
	Desktop user data folder disk space low	The volume containing the desktop user data folder is running low.

Table 3-16 DLO Alerts (Continued)

Type	Name	Description
	Evaluation period daily reminder	This reminder specifies the number of days remaining in the evaluation period for the Symantec Desktop and Laptop Option.
	Evaluation period has expired	The DLO evaluation period has expired. A license is required to continue to use DLO.
	Network user data folder approaching storage limit	The amount of stored backup data in a user's network user data folder is approaching the specified size limit.
	Network user data folder disk space low	The volume containing the network user data folder is running low.
	No backups in 14 days	A desktop computer has not performed a backup for 14 days.
	No backups in 28 days	A desktop computer has not performed a backup for 28 days.
	No backups in 7 days	A desktop computer has not performed a backup for 7 days.
	No matching automated user assignment	A new user connected, but no matching Automated User Assignment was found.
Informational		
	A backup job has completed	A backup job has completed successfully.
	A restore job has been queued	A restore job was initiated from the DLO Administration Server.
	A restore job has completed	A restore job has completed successfully.
	PST file was skipped because it is not configured in Outlook	A PST file on the desktop computer was not backed up because it was not configured in Microsoft Outlook.
	User was configured	A new user connected and was successfully configured.
	Dedupe synchronization has started	Dedupe synchronization task has been initiated.
	Dedupe synchronization has stopped	Dedupe synchronization task has completed.

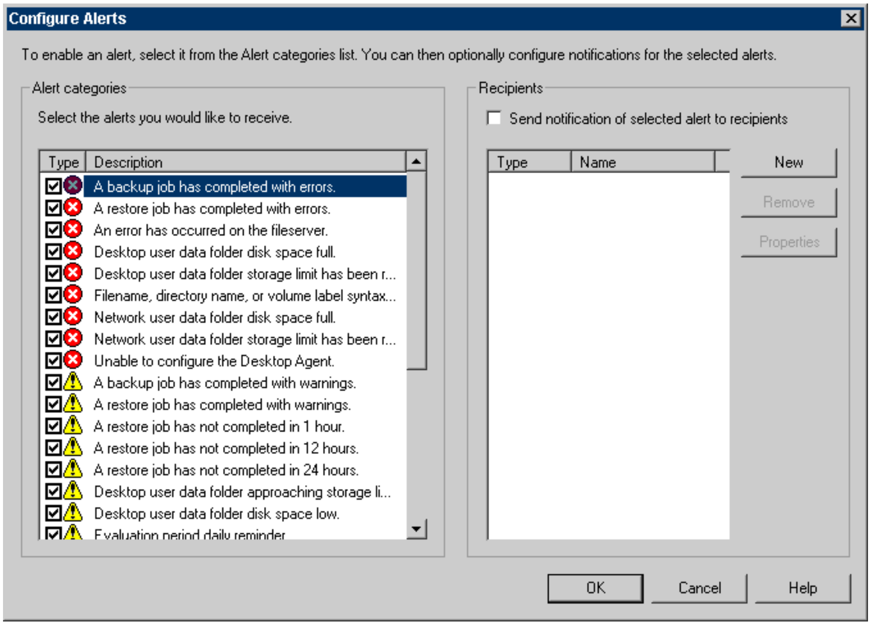
Configuring Alerts

To configure alerts

1 On the DLO navigation bar, click **Alerts**.

2 In the Task pane, under **Alert Tasks**, click **Configure alerts**.

3 Select the alerts you want to receive, and clear the check boxes for the alerts you do not want to receive.



Configure Alerts

To enable an alert, select it from the Alert categories list. You can then optionally configure notifications for the selected alerts.

Alert categories

Select the alerts you would like to receive.

Type	Description
☑ ⊗	A backup job has completed with errors.
☑ ⊗	A restore job has completed with errors.
☑ ⊗	An error has occurred on the fileserver.
☑ ⊗	Desktop user data folder disk space full.
☑ ⊗	Desktop user data folder storage limit has been r...
☑ ⊗	Filename, directory name, or volume label syntax...
☑ ⊗	Network user data folder disk space full.
☑ ⊗	Network user data folder storage limit has been r...
☑ ⊗	Unable to configure the Desktop Agent.
☑ ⚠	A backup job has completed with warnings.
☑ ⚠	A restore job has completed with warnings.
☑ ⚠	A restore job has not completed in 1 hour.
☑ ⚠	A restore job has not completed in 12 hours.
☑ ⚠	A restore job has not completed in 24 hours.
☑ ⚠	Desktop user data folder approaching storage li...
☑ ⚠	Desktop user data folder disk space low.
☑ ⚠	Evaluation period daily reminder

Recipients

☐ Send notification of selected alert to recipients

Type	Name

4 To send notification to recipients when the selected alerts are generated, do the following:

Note: Alerts must be configured for notification before selecting recipients. See “Configuring Alerts for Notification” on page 183 and “Configuring Recipients for Notification” on page 187 for more information.

- Select one or more alerts from the list. To select multiple alerts, click one item and press <Ctrl> or <Shift> while clicking the other items
- Check the **Send notification of selected alert to recipients** check box
- Click **Recipients**
- Select the recipients to receive notification of the alerts
- Click **OK**

5 Click **OK**.

Managing DLO Alerts

From the Alerts view in the DLO Administration Console, you can view a subset of alerts, clear alerts, and move alerts to a history log.

To view DLO alerts

1. On the DLO navigation bar, click **Alerts**.
2. Select **Active alerts** to view active alerts, or **Alert history** to view alerts that have been cleared.

   Note: Alerts that are older than a specified number of days are cleared and moved into alert history.

3. To filter alerts by type, select one or more options from **Active Alerts View Filters** or **Alert History View Filters** in the task pane as described in the following table.

   Table 3-17 Active Alerts View Filters

Item	Description
Show errors	Lists error alerts for the selected view.
Show warnings	Lists warning alerts for the selected view.
Show information	Lists informational alerts for the selected view.

4. To view the properties of an alert, right-click the alert in the **Active Alerts** or **Alert History** list and select properties.
5. If a log file is associated with the alert, a link is provided to the log file. Click this link to view the log file.
6. Click **Close** to close the Alert Information dialog.

Clearing DLO Alerts

Alerts are set by default to move to the alert history after a specified time; however, some alerts may appear frequently and fill the Active alerts pane. You may want to clear these alerts to the Alert history pane before they are automatically moved by the system.

To clear DLO alerts

1. On the DLO navigation bar, click **Alerts**.
2. If needed, filter the **Alerts** view as described in “To view DLO alerts” on page 182.

3 From the alert list, select one or more alerts that you want to clear.

4 In the **Task** pane, under **Alert Tasks**, do one of the following:

- Select **Respond** to clear only the selected alerts
- Select **Respond OK to all** to change the status of all alerts to cleared

Configuring Alerts for Notification

DLO has several methods to notify you of alerts:

- SMTP
- MAPI
- Lotus Notes e-mail
- Pagers
- Printers
- Net Send

To use notifications you must perform the following:

- Configure the methods you want to use to notify the recipient. Printer and Net Send notification methods do not require pre-configuration
- Configure recipients. Recipients are individuals, computer consoles, printers, or groups. They can be configured to use one or more of the notification methods
- Assign the recipients to alerts or jobs for notification

Configuring Alert Notification Methods

DLO can be configured to notify individuals of specified alerts by using the following methods:

- SMTP email Notification. See “Configuring SMTP Email for Notification” on page 183
- MAPI email Notification. See “Configuring MAPI Email for Notification” on page 185
- VIM (Lotus Notes) email Notification. See “Configuring VIM Email for Notification” on page 186
- Pager Notification. See “Configuring a Pager for Alert Notification” on page 186

Configuring SMTP Email for Notification

You must have an SMTP-compliant email system, such as a POP3 mail server to receive alert notification messages using the SMTP notification method.

To configure the SMTP email notification method

1. From the **Tools** menu, click **Email and Pager Notification**.
2. Click the **SMTP Configuration** tab.
3. Select the appropriate options as described in the following table.

Table 3-18 SMTP Configuration dialog box

Item	Description
Enable	Select this check box to activate the notification method.
SMTP mail server	Type the name of an SMTP mail server on which you have a valid user account. DLO will not check the server name or the email address for validity.
SMTP port	Defaults to a standard SMTP port. In most cases, the default should not have to be changed.
Sender Name	Type the name of the user from whom the notification message will be sent.
Sender email address	Type the email address of the user from whom the notification message will be sent. The email address should contain a name that identifies the user to the mail server, followed by an at sign (@) and the host name and domain name of the mail server. For example, john.smith@company.com.
Enable SMTP Authentication	Select this check box to enable SMTP authentication.
SMTP server login	Type the SMTP server login credentials.
Sender password	Type the password for this login.
Confirm password	Re-type the password to confirm.

4. Click **OK**.

Related Topics

"Configuring Recipients for Notification" on page 187

Configuring MAPI Email for Notification

You must have a MAPI-compliant email system, such as Microsoft Exchange to receive alert notification messages using the MAPI notification method.

Note: If you install Outlook after installing DLO, you must stop and restart the DLO Administration Service for MAPI email notification to work and to save the MAPI configuration settings.

To configure MAPI alert notification

1. From the **Tools** menu, click **Email and Pager Notification**.
2. Click the **MAPI Configuration** tab.
3. Select the appropriate options as described in the following table.

Table 3-19 MAPI Configuration dialog box

Item	Description
Enable	Select this check box to activate the notification method.
Mail server name	Type the name of the Exchange server. You must use an Exchange server to which the DLO service account has access.
Mailbox name of sender	Type the mailbox from whom the notification message will be sent, for example, John Smith. The name appears in the From field in the message and does not require a full address. **Note:** The DLO services must be running under a domain account that has rights to the Exchange mailbox used for MAPI notification to save the MAPI configuration settings.

4. Click **OK**.

Related Topics

"Configuring Recipients for Notification" on page 187

Configuring VIM Email for Notification

You must have a VIM (Lotus Notes) compliant email system to receive alert notification messages using the VIM notification method.

To configure VIM alert notification

1. From the **Tools** menu, click **Email and Pager Notification**.
2. Click the **VIM Configuration** tab.
3. Select the appropriate options as described in the following table.

Table 3-20 VIM Configuration dialog box

Item	Description
Enable	Select this check box to activate the notification method.
Notes client directory	Type the path of the directory in which the Notes client is located.
Mail password	Type the password that enables you to connect to the Notes client.
Confirm mail password	Re-type the password that enables you to connect to the Notes client.

4. Click **OK**.

Related Topics

"Configuring Recipients for Notification" on page 187

Configuring a Pager for Alert Notification

You can configure DLO to page you with alert notification messages. You must have a modem set up on your system to use the pager notification method. You must be sure that the modem you are using can communicate properly with your paging service in order for pager notification to work properly. Before you set up pager notification, contact your paging service for information about the recommended brand of modem to use with your paging service.

1. From the **Tools** menu, click **Email and Pager Notification**.
2. Click the **Pager Configuration** tab.

3 Select the appropriate options as described in the following table.

Table 3-21 Options for Pager Configuration

Item	Description
Enable	Check Enable to activate this alert notification method.
Select a modem for sending pages	Select a modem from the list. Only modems that are recognized in Windows appear in the list.

4 Click **OK**.

Configuring Recipients for Notification

Recipients are individuals with a predefined notification method, computer consoles, printers, or groups. Recipient configuration consists of selecting a notification method and defining notification limits. After you create entries for the recipients, you can assign them to alerts or jobs. The following types of recipients can be configured for notifications:

- Person: An individual that has a predefined method of notification such as SMTP, MAPI, or VIM email, or a pager. You must configure the notification method before you can enable it for the recipient.
- SNMP Trap: SNMP Traps are sent to a computer that is configured to receive them.
- Net Send: A computer that serves as a notification recipient.
- Printer: A specific printer to which notifications can be sent.
- Group: A group of one or more recipients, including person recipients, Net Send recipients, and other groups.

Related Topics

"Configuring Alerts for Notification" on page 183

Configuring SMTP Mail for a Person Recipient

You can configure a person recipient to receive SMTP email notification messages if you have configured the SMTP notification method.

To configure SMTP mail for a person recipient

1. From the **Tools** menu, click **Recipients**.
2. Click **New**.
3. Click **Person**.
4. Click **OK**.
5. In the **Name** field, type the name of the recipient that you want to configure.
6. Click the **SMTP Mail** tab.
7. Select the appropriate options as described in the following table.

Table 3-22 SMTP Mail dialog box

Item	Description
Enable	Select this check box to activate this notification method for the recipient.
Address	Type the email address of the person to whom the notification message will be sent. For example, john.smith@company.com.
Test	Enables you to test the notification configuration for the recipient.
Limit the number of notifications sent	
Enable	Select this check box to activate the option.
Notify me a maximum of *x* times within *y* minutes	Type the total number of notifications that can be sent to the recipient for all alerts that are generated within a specified number of minutes. After the specified number of notifications have been sent, additional notifications are not sent until the specified minutes have been reached. The maximum number of minutes you can set is 1440, which is the number of minutes in a day.
Reset the notification limits after *x* minutes	Select this check box to enter the number of minutes that must be reached before the notification limits are reset. When the time limit has been reached, the number of notifications that are sent is reset to zero.
Limit when notifications can be sent	

Table 3-22 SMTP Mail dialog box (Continued)

Item	Description
Enable	Select this check box to activate the option and configure the length of time the recipient is available for notification.
Schedule	Enables you to select the days and times when notifications can be sent to the recipient. For more information, see “Scheduling Notification for Recipients” on page 198.

8 Click **OK**.

Configuring MAPI Mail for a Person Recipient

You can configure a person recipient to receive MAPI email notification messages if you have configured the MAPI notification method.

To configure MAPI mail for a person recipient

1 From the **Tools** menu, click **Recipients**.

2 Click **New**.

3 Click **Person**.

4 Click **OK**.

5 In the **Name** field, type the name of the recipient that you want to configure.

6 Click the **MAPI Mail** tab.

7 Select the appropriate options as follows described in the following table.

Table 3-23 MAPI Mail dialog box

Item	Description
Enable	Select this check box to activate this notification method for the recipient.
Mailbox	Type the email address or mailbox name of the recipient to whom the notification message will be sent. For example, john.smith@company.com or John Smith.
Test	Enables you to test the notification configuration for the recipient.
Limit the number of notifications sent	
Enable	Select this check box to activate the option.

Table 3-23 MAPI Mail dialog box (Continued)

Item	Description
Notify me a maximum of *x* times within *y* minutes	Type the maximum number of notifications sent to the recipient for all alerts generated within the specified number of minutes. After the specified number of notifications have been sent, additional notifications are not sent until the specified minutes have been reached. The maximum number of minutes that can be set is 1440, which is the number of minutes in a day.
Reset the notification limits after *x* minutes	Select this check box to enter the number of minutes that must be reached before the notification limits are reset. When the time limit has been reached, the number of notifications sent is reset to zero.
Limit when notifications can be sent	
Enable	Select this check box to activate the option and configure the length of time the recipient is available for notification.
Schedule	Enables you to select the days and times when notifications can be sent to the recipient. For more information, see "Scheduling Notification for Recipients" on page 198.

8 Click **OK**.

Configuring VIM Mail for a Person Recipient

You can configure a person recipient to receive VIM email notification messages if you have configured the VIM notification method.

To configure VIM mail for a person recipient

1 From the **Tools** menu, click **Recipients**.

2 Click **New**.

3 Click **Person**.

4 Click **OK**.

5 In the **Name** field, type the name of the recipient that you want to configure.

6 Click the **VIM Mail** tab.

7 Select the appropriate options as described in the following table.

Table 3-24 VIM Mail dialog box

Item	Description
Enable	Select this check box to activate this notification method for the recipient.
Address	Type the email address of the recipient to whom the notification message will be sent. For example, JohnSmith@company.com.
Test	Enables you to test the notification configuration for the recipient.
Limit the number of notifications sent	
Enable	Select this check box to activate the option.
Notify me a maximum of *x* times within *y* minutes	Type the total number of notifications sent to the recipient for all alerts generated within the specified number of minutes. After the specified number of notifications have been sent, additional notifications are not sent until the specified minutes have been reached. The maximum number of minutes that can be set is 1440, which is the number of minutes in a day.
Reset the notification limits after *x* minutes	Select this check box to enter the number of minutes that must be reached before the notification limits are reset. When the time limit has been reached, the number of notifications sent is reset to zero.
Limit when notifications can be sent	
Enable	Select this check box to activate the option and configure the length of time the recipient is available for notification.
Schedule	Enables you to select the days and times when notifications can be sent to the recipient. For more information, see "Scheduling Notification for Recipients" on page 198.

Configuring a Pager for a Person Recipient

You can configure a person recipient to receive notification messages by pager if you have configured the pager notification method.

To configure a pager for a person recipient

1 From the **Tools** menu, click **Recipients**.

2 Click **New**, and then click **Person.**

3 Click **OK**.

4 In the **Name** field, type the name of the recipient that you want to configure.

5 Click the **Pager** tab.

6 Select the appropriate options as described in the following table.

Table 3-25 Pager dialog box

Item	Description
Enable	Select this check box to activate this notification method for the recipient.
Carrier Phone	Type the area code and phone number to access the paging service provider's modem. The paging service number may be different from the number you enter to manually send a page.
Country/region name and code	Enter the country or region name and country code in which the pager is located.
Pager Pin	Type the pager identification number provided by the paging service provider. You will have a pin if you use TAP services and in most cases, the number is the last seven digits of the pager's phone number.
Advanced Pager setup options	
Advanced	Enables you to configure additional settings for the pager. For more information about the options, see "Advanced Pager Information dialog box" on page 193.
Test	Enables you to test the notification configuration for the recipient.
Limit the number of notifications sent	
Enable	Select this check box to activate the option.
Notify me a maximum of *x* times within *y* minutes	Type the total number of notifications sent to the recipient for all alerts generated within the specified number of minutes. After the specified number of notifications have been sent, additional notifications are not sent until the specified minutes have been reached. The maximum number of minutes that can be set is 1440, which is the number of minutes in a day.
Reset the notification limits after *x* minutes	Select this check box to enter the number of minutes that must be reached before the notification limits are reset. When the time limit has been reached, the number of notifications sent is reset to zero.

Table 3-25 Pager dialog box (Continued)

Item	Description
Limit when notifications can be sent	
Enable	Select this check box to activate the option and configure the length of time the recipient is available for notification.
Schedule	Enables you to select the days and times when notifications can be sent to the recipient. For more information, see “Scheduling Notification for Recipients” on page 198.

7 Click **Advanced** to configure advanced pager setup options and select the appropriate options as described in the following table.

Table 3-26 Advanced Pager Information dialog box

Item	Description
Pager Configuration	
Password	Type the password for the pager, if one is required.
Message Length	Type the maximum number of characters you want to use for messages. The number is determined by the paging service provider.
Retries	Type the number of times you want the paging service provider to retry the page. The number is determined by the paging service provider.
Pager type	
Numeric	Select this option if you are configuring a pager that accepts only numbers.
Alpha-numeric	Select this option if you are configuring a pager that accepts letters and numbers.
Modem Configuration	
Modem Baud Rate	Select the speed of the modem. The speeds that appear are limits set by the paging service; select the appropriate speed regardless of the modem speed rating.
Data bits, Parity, Stop bit	Select the communication protocol. In most cases, you should use the Windows default.

8 Click **OK** to save the settings in the Advanced Pager Information dialog box, and then click **OK** to save the pager configuration settings.

Configuring a SNMP Trap Recipient

To configure a SNMP trap as a recipient

1 From the **Tools** menu, click **Recipients**.

2 Click **New**.

3 Click **SNMP Trap**.

4 Click **OK**.

5 Select the appropriate options as described in the following table.

Table 3-27 SMTP Mail dialog box

Item	Description
Name	Type a name for the SNMP Trap recipient.
Host	Type the name of the SNMP host computer.
Port	Enter the SNMP port number. The default SNMP port is 162.
Limit the number of notifications sent	
Enable	Select this check box to activate the option.
Notify me a maximum of *x* times within *y* minutes	Type the total number of notifications sent to the recipient for all alerts generated within the specified number of minutes. After the specified number of notifications have been sent, additional notifications are not sent until the specified minutes have been reached. The maximum number of minutes that can be set is 1440, which is the number of minutes in a day.
Reset the notification limits after *x* minutes	Select this check box to enter the number of minutes that must be reached before the notification limits are reset. When the time limit has been reached, the number of notifications sent is reset to zero.
Limit when notifications can be sent	
Enable	Select the check box to activate the option and configure the length of time the recipient is available for notification.

Table 3-27 SMTP Mail dialog box (Continued)

Item	Description
Schedule	Select the days and times when notifications can be sent to the recipient. For more information, see "Scheduling Notification for Recipients" on page 198.

6 Click **OK**.

7 Click **Close**.

Configuring a Net Send Recipient

You can configure Net Send to send notification messages to a target computer or user.

Note: If the target computer has Internet pop-up advertisement blocking software installed, the Net Send notification message will not display.

To configure a net send recipient

1 From the **Tools** menu, click **Recipients**.

2 Click **New** and then click **Net Send.**

3 Click **OK**.

4 Select the appropriate options as described in the following table.

Table 3-28 Net Send Recipient Properties dialog box

Item	Description
Name	Type the name of the recipient for whom you are configuring the notification.
Target Computer or User Name	Type the name of the computer or user to whom you are sending the notification. You should enter a computer rather than a user because the Net Send message will fail if the user is logged off the network. **Note:** If the target computer has Internet pop-up advertisement blocking software installed, the Net Send notification message will not display.
All Computers	Select **All Computers** to send the notification to all the computers in the network.

Table 3-28 Net Send Recipient Properties dialog box (Continued)

Item	Description
Test	Enables you to test the notification configuration for the recipient.
Limit the number of notifications sent	
Enable	Select this check box to activate the option.
Notify me a maximum of *x* times within *y* minutes	Type the total number of notifications sent to the recipient for all alerts generated within the specified number of minutes. After the specified number of notifications have been sent, additional notifications are not sent until the specified minutes have been reached. The maximum number of minutes that can be set is 1440, which is the number of minutes in a day.
Reset the notification limits after *x* minutes	Select this check box to enter the number of minutes that must be reached before the notification limits are reset. When the time limit has been reached, the number of notifications sent is reset to zero.
Limit when notifications can be sent	
Enable	Select this check box to activate the option and configure the length of time the recipient is available for notification.
Schedule	Select the days and times when notifications can be sent to the recipient. For more information, see “Scheduling Notification for Recipients” on page 198.

5 Click **OK**.

Configuring a Printer Recipient

You can select installed printers as a notification method for recipients; however, fax printer devices are not supported by DLO. Only printers that were configured using the same username and password as the DLO service account can be selected.

To configure a printer recipient

1 From the **Tools** menu, click **Recipients**.

2 Click **New** and then click **Printer.**

3 Click **OK**.

4 Select the appropriate options as described in the following table.

Table 3-29 Printer Recipient Properties dialog box

Item	Description
Name	Type the recipient for whom you are configuring the notification. You cannot use a fax printer device to receive the notification.
Target Printer	Select the name of the printer to which the notification message will be sent.
Test	Enables you to test the notification configuration for the recipient.
Limit the number of notifications sent	
Enable	Select this check box to activate the option.
Notify me a maximum of *x* times within *y* minutes	Type the total number of notifications sent to the recipient for all alerts generated within the specified number of minutes. After the specified number of notifications have been sent, additional notifications are not sent until the specified minutes have been reached. The maximum number of minutes that can be set is 1440, which is the number of minutes in a day.
Reset the notification limits after *x* minutes	Select this check box to enter the number of minutes that must be reached before the notification limits are reset. When the time limit has been reached, the number of notifications sent is reset to zero.
Limit when notifications can be sent	
Enable	Select this check box to activate the option and configure the length of time the recipient is available for notification.
Schedule	Select the days and times when notifications can be sent to the recipient. For more information, see "Scheduling Notification for Recipients" on page 198.

Configuring a Group Recipient

Groups are configured by adding recipients as group members. A group contains one or more recipients and each recipient receives the notification message. Members of the group can be a combination of individual persons, computers, printers, or other groups.

To configure a group recipient

1 From the **Tools** menu, click **Recipients**.

2 Click **New** and then click **Group.**

3 Click **OK**.

4 In the **Group Name** field, type the name of the group for whom you are configuring the notification.

5 Do one of the following as described in the following table.

Table 3-30 Configuring a Group Recipient

Item	Description
To add members to the group	Select recipients from the **All Recipients** list, and then click **Add** to move them to the **Group Members** list.
To remove members from the group	Select recipients from the **Group Members** list, and then click **Remove** to move them to the **All Recipients** list.

6 Click **OK**.
The new group can be added to other groups.

Scheduling Notification for Recipients

During the recipient configuration process, you can enable the **Limit when notifications can be sent** option to select the times of the day and the days of the week the recipient is available to receive the notification messages. You can modify the schedule after the recipient is configured by editing recipient notification properties.

See "Configuring Recipients for Notification" on page 187 for more information on the recipient configuration process.

To configure the notification schedule for recipients

1 On the **Recipient Properties** dialog box, under the **Limit when notifications can be sent** group box, click **Enable** to activate the option.

Note: To access the Recipient Properties dialog box, click **Recipients** from the Tools menu. Click **New** to create a new recipient or select an existing recipient and then click **Properties**.

2 Click **Schedule**.

3 Do any of the following as described in the following table.

Table 3-31 Scheduling Notification

Item	Description
Include work days	Clear the **Include work days** check box to exclude Monday through Friday from 8 A.M. to 6 P.M.
Include weeknights	Clear the **Include weeknights** check box to exclude Monday through Friday from 6 P.M. to 8 A.M.
Include weekends	Clear the **Include weekends** check box to exclude Saturday and Sunday, 24 hours a day.

Note: You can select any combination of **Include work days**, **Include weeknights**, or **Include weekends**, or click any single hour of the chart to select or clear that hour.

4 Click **OK**.

Editing Recipient Notification Properties

You can edit the recipient notification properties at any time and change the recipient information, such as an email address, telephone number, or schedule.

To edit the recipient notification properties

1 From the **Tools** menu, click **Recipients**.

2 Select the recipient you want to edit.

3 Click **Properties**.

4 Edit the properties for the selected recipient.
You can edit any of the properties except for the recipient name in the **Name** field. To modify the recipient name, you must create a new recipient, and then delete the old one.

5 Click **OK**.

Editing Recipient Notification Methods

You can configure new notification methods or edit existing notification methods after you configure recipients.

To edit notification methods

1. From the **Tools** menu, click **Recipients**.
2. Select the recipient to be edited and click **Properties**.
3. Edit notification properties for the following types of notification methods:
   - SMTP Configuration. See “SMTP Configuration dialog box” on page 184
   - MAPI Configuration. See “MAPI Configuration dialog box” on page 185
   - VIM Configuration. See “VIM Configuration dialog box” on page 186
   - Pager Configuration. Click **Enable** to activate or clear the notification method, and then select a modem from the **Configured Modems** list
4. Click **OK**.

Removing Recipients

You can delete recipients that do not want to receive notification messages; however, the recipient is permanently removed upon deletion. If you want to keep the recipient, but do not want the recipient to receive notifications, clear the **Enable** check box in the recipient properties.

To remove a recipient

1. From the **Tools** menu, click **Recipients**.
2. Select the recipient you want to delete, and then click **Remove**.
3. Click **OK**.
4. You can start the job after configuring the new recipients or edit recipient properties or select other options from the **Properties** pane.

DLO Reports

DLO provides a variety of reports that show detailed information about your DLO operations. These reports can be viewed from the DLO Console or generated and saved using the new report command (see “-Report command” on page 226).

When you generate a report, you can specify filter parameters for the data that you want to include in the report. The filters that are enabled are specific to each report.

You can use the DLO global settings to set the default report format. The default formats are only used by the reports viewed from the console. See “Changing Default Global Settings” on page 42 for more information.

If the default report format is set as PDF and Adobe Acrobat is installed on the system, reports are displayed in Adobe Portable Document Format (PDF). If Adobe Acrobat is not detected, the reports are displayed in HTML format.

All report formats can be saved and printed.

To view the list of available reports

- The following reports are available on the **Reports** view.

Table 3-32 DLO Reports

Report Name	Description
Active Alerts	A list of all currently active alerts arranged chronologically.
Active Alerts by Computer	A list of all currently active alerts sorted by computer name.
Active Alerts by User	A list of all currently active alerts from all computers sorted alphabetically by Desktop Agent user name.
Alert History	A chronological list of alerts that have been sent by all computers in the past.
Alert History by Computer	A list of alerts that have been sent by all computers in the past, sorted by computer name.
Alert History by User	A list of alerts that have been sent by all computers in the past, sorted by Desktop Agent user name.
Failed Backups	A chronological list of computers that have a failed status for the last backup.
Failed Backup by Computer	A list of computers that have a failed status for the last backup, sorted by computer name. **Note:** Only the last backup result is stored in the DLO database, so it is only possible to report the last backup result for each desktop computer and not a complete history of failed jobs.
Failed Backup by User	A list of computers that have a failed status for the last backup, sorted by Desktop Agent user name. **Note:** Only the last backup result is stored in the DLO database, so it is only possible to report the last backup result for each desktop computer and not a complete history of failed jobs.
Last Backup Status	A chronological list of the last backup status for all Desktop Agent computers.
Last Backup Status by Computer	A list of the last backup status for all Desktop Agent computers, sorted by computer name.

Table 3-32 DLO Reports (Continued)

Report Name	Description
Last Backup Status by User	A list of the last backup status for all Desktop Agent computers, sorted by Desktop Agent user name.
Storage Consumption per User	This report shows the storage consumption used (in MB) per user on the Network User Data folder.
Last Backup Status by Profile	This report displays backup failures, successes, and warnings for machines and is grouped by profile name.
No Backups	This report shows the machines that have not been backed up in the past X days. The value for days is specified using the days filter. Only those machines whose last completed backup time is greater than X days are displayed. If no days filter is specified, all the cancelled and failed backup jobs are displayed.
Backups Status Dashboard	This report shows the status of all clients associated with a storage location. The report provides the total number of backup successes, warnings, cancellations, and errors for the associated clients.

Related Topics

"Changing Default Global Settings" on page 42

"Viewing Report Properties" on page 203

"Running a Report" on page 202

Running a Report

When you run a report, you can specify filtering criteria to determine which items will be included in the report. After the report is generated, only the items that match the entered criteria appear in the report. If no criteria are entered, all available entries are included in the report.

To run a report

1. On the navigation bar, click **Reports**.
2. On the **Reports** pane, select the report you want to run.
3. In the **Task** pane, under **Reports Tasks**, click **Run report now**.

4 Select the appropriate filters for the data you want to include in the report from the following available filters. Some of these filters are disabled depending on the report selected.

Table 3-33 Report Filters

Item	Description
Computer	Select this filter to create a report for a specific computer, and then enter a desktop computer name.
User	Select this filter to create a report for a specific desktop user, and then enter the user's name.
Profile	Select this filter to create a report for a specific profile, and then enter a profile name.
Days	Select this filter to create a report for a specific number of days, and then enter the number of days.

5 Click **OK** to run the report. The report can be printed or saved before it is closed.

6 Click **OK** to close the report.

Viewing Report Properties

Report properties provide a summary of information about each report. The properties can be viewed, but not edited.

To view report properties

1 On the navigation bar, click **Reports**.

2 On the **Reports** pane, select the report for which you want to view properties.

3 In the **Task** pane, under **General tasks**, click **Properties**.
The Report dialog box provides the following information.

Table 3-34 Report Properties

Item	Description
Title	The name of the report.
Description	The type of data that is included in the report.

Table 3-34 Report Properties (Continued)

Item	Description
Category	Classification for the report. Available report categories include: ■ Alerts ■ Last Backup Status ■ Failed Jobs
Author	The creator of the report.
Subject	The version of the product for which the report was created.
Keywords	The primary information used to categorize the report.
File name	The file name of the report template. Report templates are specified in Report Definition Language (RDL) and are structured XML schemas that specify the report definition.
File size	The size of the report template.
Creation Date	The date the report was installed on the system.

4 Click **OK**.

About DLO and Clusters

In a server cluster, Symantec DLO can protect data on local disks and shared disks. Clustered servers provide high availability of applications and data to users. In a clustered server, several servers (nodes) are linked in a network. The Microsoft Cluster Service (MSCS) allows every node to access the shared disks only when it becomes active. If a node is unavailable, cluster resources migrate to an available node (failover). The shared disks and the virtual server are kept available. During failover, you experience only a short interruption in service.

DLO Administration service, DLO Database service, Dedupe Server service, and Dedupe Database service are supported in the cluster environment.

Requirements for Installing DLO on a Microsoft Cluster Server

The following are the pre-requisites to install DLO Administration Server on a Microsoft cluster:

- Two-node clusters are supported with DLO on Microsoft Windows Server 2003, 2008, 2008 R2, and 2012.

- DLO clusters can be configured on Microsoft Windows Server 2003, 2008, 2008 R2, and 2012 majority node configurations. However, there must be a shared disk in the configuration for DLO to share the database files between the nodes.
- The controlling node and designated failover nodes must be online when installing Admin DLO server into the cluster.
- A unique IP address and a unique network name are required for configuring DLO service on a MSCS cluster.
- While configuring DLO service on a MSCS cluster, it is mandatory that the user executing the DLO Cluster configuration utility from the active node must be the owner of the shared disk and the active node.
- Use the domain admin account for DLO services on all nodes in the cluster. If nodes in a cluster use DLO and have different accounts, change the services to use the domain admin account.
- While clustering the machine using domain user account, which is part of domain admin group, then provide additional rights/privileges to this user account on the “Computer” container in Domain Controller for performing cluster operations. The user account should have the following privileges:
    - Create Computer Object
    - Read All Properties

  If the user is added to a different group other than the domain admin group, then provide the above two privileges to this specific user or group. Also, this user should be a local administrator on the computers that will be part of cluster. For more information, refer to the Microsoft Technet link.

  http://blogs.technet.com/b/askcore/archive/2010/06/02/rights-needed-for-user-account-to-create-a-cluster-name-object-cno-on-windows-server-2008-r2-failover-cluster.aspx

Configuring DLO on a Microsoft Cluster Server

To configure DLO on a Microsoft Cluster Server:

1. Install DLO on all the nodes.
2. Go to **Start** > **Programs** > **Symantec** > **Symantec DLO** > **DLOCluster Configuration Utility**.
3. In the **Symantec Cluster Configuration Wizard**, click **Next**.
4. In **Cluster Group Information**, type the following:
    a. In **Type a unique name for the Symantec DLO cluster group, or use default** - enter the required name or use Symantec DLO (default name).

- b In **Select a network adaptor card for this node, or use the default** - select the public option.

  Note: The private option is selected for using clusters internally.

- c To select the drive, click **Change**.

  Note: The MSCS Quorum drive <disk> is not supported.

- d In **Change Location of Application Data**, select a new location for Symantec DLO's application data and click **Next**.

Note: Ensure that you select the shared disk drive only.

The changed location is displayed in the **Cluster Group Information** window.

5 Click **Next**.

6 In **Virtual Server Information**, type the following:

- a In **Enter a name for the Symantec DLO virtual server or use the default** - enter the required server name or use DLOVRS (default name).
- b In **Type the IP Address of the Symantec DLO virtual server** - enter the virtual IP address of the virtual server.
- c In **Type the subnet mask of the Symantec DLO virtual server** - enter the subnet mask of the virtual server.
- d Click **Next**.

7 In **Add or Remove Nodes**, click **Add** to add the nodes to the Symantec DLO cluster group.

8 Click **Next**.

9 In **Ready to Configure the Cluster**, click **Configure**.
The cluster is configured successfully.

10 In **Summary**, the summary of changes that are made to the cluster configuration are displayed.

11 To exit the wizard, click **Finish**.

Unclustering DLO

Pre-requisites for Unclustering DLO

Before unclustering DLO, ensure that you complete the following tasks:

1 Create a new Dedupe Storage Location on the local disk.

2 Create a new DLO Storage Location on the local disk and assign the Dedupe Storage Location that was created on the local disk to this DLO Storage Location.

3 Move the network user data folder from the virtual server to the newly created DLO Storage Location on the local disk.

4 Run the `-ChangeDB` command to change the existing database on the shared disk to a database on the local disk.

```
DLOCommandu.exe -ChangeDB -DBServer <DB Server Name>
-DBInstance <DB Instance Name> -DBName <DLO Database Name>
-DBDataFile <DLO data file name> -DBLogFile <DLO log file>
```

For more information about the command, see “-ChangeDB command” on page 213.

5 Run the `-ChangeServer` command to change the existing media server on the shared disk to a media server on the local disk.

```
DLOCommandu.exe -ChangeServer -M <Media server name> -A
```

For more information about the command, see “-ChangeServer command” on page 214.

To uncluster Symantec DLO:

1 Go to **Start** > **Programs** > **Symantec** > **Symantec DLO** > **DLOCluster Configuration Utility**.

2 In **Symantec Cluster Configuration Wizard**, click **Next**.

3 In **Add or Remove Nodes**, select the nodes that must be removed from the cluster and click **Remove**.

The selected nodes are moved to **Nodes not in the Symantec DLO cluster group**.

4 Click **Next**. A warning message stating ‘*You have chosen to remove all nodes. Do you wish to remove the data off the shared drive?*’ is displayed.

5 Click **Yes**. A warning message stating ‘*Do you wish to make the data from the shared drive available for use by this local node after removal of the cluster group?*’ is displayed.

6 Click **Yes**.

7 In **Ready to Configure the Cluster,** click **Configure** to apply the settings to the cluster configuration.

After the cluster is removed successfully, the **Summary** screen displays the summary of changes that are made to the cluster configuration.

8 To exit the wizard, click **Finish**.

Note: After unclustering DLO, ensure that you change the Dedupe Server's host name to the local host name. For more information about editing the Dedupe Server details, see "Modifying Dedupe Server" on page 79.

Upgrading DLO on a Microsoft Cluster Server

This section explains the procedure to upgrade from DLO 7.0 cluster environment to DLO 7.5.

Pre-requisites

Before unclustering DLO, ensure that you complete the following task.

1. From the DLO 7.5 installer package, extract the binaries (`DLOClusconfig.exe` and `DLOCluster.dll`) from the `clusterpatch.zip` file.
2. Replace the DLO 7.0 cluster binaries with the extracted binaries, only on the machine where DLO will be unclustered.

   The binary files are located at this path:

   `C:\Program Files\Symantec\Symantec DLO\DLOClusconfig.exe.`

   `and`

   `C:\Program Files\Symantec\Symantec DLO\DLOCluster.dll.`

To upgrade DLO on a Microsoft cluster server

1. To uncluster the existing DLO on the server, follow the procedure explained in the section, "Unclustering DLO" on page 206.

   Note: Upgrade process will fail if DLO is not unclustered.

2. Upgrade to DLO 7.5 on the server.
3. To re-configure DLO 7.5 on the Microsoft cluster server, follow the procedure explained in the section "Configuring DLO on a Microsoft Cluster Server" on page 205.

DLO Command Line Interface Management Tools

DLO provides a number of powerful command line system tools to manage DLO server operations as explained in the following sections:

- "DLO Command Syntax" on page 209
- "Commands in Detail" on page 210

DLO Command Syntax

DLO Command Line Interface commands are run from the installation directory and are executed with the *DLOCommandu* command.

Note: The default installation directory for Symantec DLO version 7.0 and later is:
`C:\Program Files\Symantec\Symantec DLO`
If Symantec DLO is upgraded from a previous version, it will remain in the original installation directory. Previous versions of DLO used the following default installation directories:

```
C:\Program Files\VERITAS\NetBackup DLO
C:\Program Files\Symantec\NetBackup DLO
```

DLOCommandu is executed as follows:

```
DLOCommandu [remote-server-options] command
[command-options-and-arguments] [log-file-option]
```

Remote server options allow you to specify the name of the remote server on which you want to run a command. You can also enter your username and password if required.

Remote server options are described in the following table.

Table 4-1 Remote Server Options

Option	Description
–C <computer>	Remote computer name, default to local computer
–N <user>	Fully qualified user name, e.g. `Enterprise\GFord`. The default is the current user
–W <password>	User password if –n is specified
-DB <dbname>	Specifies the name of the database on the remote server
-DBInst <instance>	Specifies the name of the database instance on the remote server
-DBDataFile <db data file>	Specifies the name of the database data file on the remote server. The default value is `DLO.mdf`
-DBLogFile <db log file>	Specifies the name of the database log file on the remote server. The default value is `DLO_log.mdf`

Commands in Detail

See the following topics for detailed information on available commands:

- “`-AssignSL` command” on page 211
- “`-EnableUser` command” on page 212
- “`-ChangeDB` command” on page 213
- “`-ChangeServer` command” on page 214
- “`-KeyTest` command” on page 215
- “`-ListProfile` command” on page 216
- “`-ListSL` command” on page 217
- “`-ListUser` command” on page 218
- “`-LogFile` command” on page 218
- “`-Update` command” on page 219
- “`-EmergencyRestore` command” on page 222

- “-SetRecoveryPwd command” on page 222
- “-NotifyClients command” on page 223
- “-InactiveAccounts command” on page 223
- “-RenameDomain command” on page 224
- “-RenameMS command” on page 224
- “-LimitAdminTo command” on page 224
- “-IOProfile command” on page 225
- “-Report command” on page 226
- “-ListReport command” on page 227
- “-MigrateDomain command” on page 227
- “-ChangeProfile command” on page 227
- “-MigrateUserSL command” on page 228
- “-MigrateUser command” on page 231
- “-ListMachines command” on page 236
- “-DeletePendingUser command” on page 236

-AssignSL command

The *–AssignSL* command is used to assign a new to existing users when the existing DLO Storage Location is no longer available. The new DLO Storage Location must be managed by the same DLO Administration Server.

Caution: If the existing DLO Storage Location is accessible, use the -MoveUser command to move users to a new DLO Storage Location. See “Moving Desktop Agent Users to a New Network User Data Folder” on page 154 for more information.

Desktop Agent users can be assigned to new DLO Storage Locations based on User account name, profile name, profile ID, DLO Storage Location, DLO Storage Location ID, and File server.
The Desktop Agent that is being moved will be disabled until the administration server is notified that the move is complete.

Note: This command does not move the user’s data. To assign a new DLO Storage Location to existing users and move the associated data, use the “-MigrateDomain command” on page 227.

Syntax:

```
DLOCommandu -AssignSL -NI [-A | -F | -P | -PI | -S | -SI |
-U]
```

Note: Wildcard matches (*) are permitted in profile, Storage Location and user names.
Quotation marks are required around names if the name contains a space or colon.

Command options

Table 4-2 –AssignSL Options

Option	Description
–NI <new SLID>	The -NI option is used to specify the name of the new Storage Location.
–A	Assigns a new Storage Location to all users.
–F <file server>	Assigns a new Storage Location to users with Storage Locations on the named file server.
–P <profile name>	Assigns a new Storage Location to users with named profile.
–PI <profile ID>	Assigns a new Storage Location to users with given profile ID.
–S <SL name>	Assigns a new Storage Location to users with named Storage Location.
–SI <SL ID>	Assigns a new Storage Location to users with the given Storage Location ID.
–U <user>	Assigns a new Storage Location to named user account only.

Examples:

```
DLOCommandu -AssignSL -NI DLO_SL02 -A
DLOCommandu -AssignSL -NI DLO_SL03 -U mmouse
```

-EnableUser command

The *-EnableUser* command is used to enable or disable a user.
Use this command if you want to force the desktop computer to refresh from the DLO Administration Server.

Syntax:

```
DLOCommandu -EnableUser [-E | -D] [-A | -F | -P | -PI | -S |
-SI | -U]
```

Note: Wildcard matches (*) are permitted in profile, Storage Location and user names.
Quotation marks are required around names if the name contains a space or colon.

Command options

Table 4-3 –EnableUser Command Options

Option	Description
-E	Enables a user account. The default value is to enable a user.
-D	Disables a user account.
-A	Enables or disables all users on the DLO Administration Server.
-F <file server>	Enables or disables users with storage locations on the named file server.
-P <profile name>	Enables or disables users with the specified profile name.
-PI <profile ID>	Enables or disables users that are assigned to the specified profile.
-S <SL name>	Enables or disables users assigned to the specified Storage Location.
-SI <SL ID>	Enables or disables users in the specified Storage Location.
-U <user>	Enables or disables only the user with the specified user name.

Examples:

```
DLOCommandu -EnableUser -E -A
DLOCommandu -EnableUser -D -U mmouse
```

-ChangeDB command

This command is used to change the existing database to another DLO database.

Syntax:

```
DLOCommandu -ChangeDB -DBServer <DB server name> -RemoteDB
-DBInstance <DB instance name> -DBName <DLO database name>
-DBDataFile <DLO data file name> -DBLogFile <DLO log file>
```

Command options

Option	Description
–DBServer	The name of the new database server
-RemoteDB	The name of the remote database server. Use this option when the DLO Administration Server and the DLO database server are installed on different machines.
–DBInstance	The name of the database instance. **Note:** Specify "" in case of a blank database instance.
–DBName	The name of the database. Default value is DLO
–DBDataFile	The name of the database file. Default value is DLO.mdf
–DBLogFile	The name of the log file. Default value is DLO_log.ldf

-ChangeServer command

The *-ChangeServer* command is used to reassign users to another DLO Administration Server.

Each desktop user must back up data to a network user data folder that is managed by the same administration server to which the user is assigned. If a matching automated user assignment is available on the new DLO Administration Server, the user is automatically assigned a profile and Storage Location. If a matching automated user assignment is not available, the user can be manually configured.

When a Desktop Agent user is reassigned from one administration server to another, the user's current profile settings and existing backup files are not moved. They remain on the original file server.

Syntax:

```
DLOCommandu -ChangeServer -M <DLO Administration Server> [ -A | -F
<file server> | -P <profile name> | -PI <profile id> | -S <SL name>
| -SI <SL id> | -SP <SL path> | -U <user> ]
```

Note: Wildcard matches (*) are permitted in profile, Storage Location, and user names.
Quotation marks are required around names if the name contains a space or colon.

Command options

Table 4-4 –ChangeServer Command Options

Option	Description
–A	Switches all users (default).
–F <file server>	Switches users with Storage Locations on the named file server.
–M <DLO Administration Server>	The new DLO Administration Server name.
–P <profile name>	Switches users based on profile name.
–PI <profile ID>	Switches users based on profile ID.
–S <SL name>	Switches users based on Storage Location name.
–SI <SL ID>	Switches users based on Storage Location ID.
–SP <SL path>	Switches users based on Storage Location path.
–U <user>	Switches users based on user name.

Examples:

```
DLOCommandu –ChangeServer –M sunshine –P Desktop*
DLOCommandu –ChangeServer –M sunshine –SP \\moonlight\EngDept
DLOCommandu –ChangeServer –M sunshine –SP
\\moonlight\EngDept\Enterprise–MNoel
```

-KeyTest command

The *-KeyTest* command scans network user data to identify encrypted data that cannot be restored with the current encryption key.

Syntax:

```
DLOCommandu –KeyTest
```

Command options

The following options can be used independently or in combination.

Table 4-5 –KeyTest Command Options

Option	Description
-f	The -f option forces a full scan for all users even if the data has already been validated.
-quar	The -quar option quarantines any unrestorable data encountered. Data that cannot be restored with the current encryption key is quarantined in the `.dloquarantine` folder in the user's network user data folder. If this option is not specified the data will be scanned and reported but will not be quarantined.
-purge	The -purge option deletes any previously quarantined data.

Examples:

Check for unrestorable data that has not previously been validated, or that was backed up by an old version of the Desktop Agent:	`DLOCommandu –keytest`
Scan all data, even if it has been previously validated, to identify unrestorable data. Quarantine unrestorable data.	`DLOCommandu –keytest -f -quar`

-ListProfile command

The *-ListProfile* command is used to list profiles of Desktop Agent users.

Syntax:

```
DLOCommandu –ListProfile [-A | -P ]
```

Note: Wildcard matches (*) are permitted in profile, Storage Location and user names.
Quotation marks are required around names if the name contains a space or colon.

Command options

Table 4-6 –ListProfile Command Options

Option	Description
–A	Lists settings for all profiles (default).
–P <profile name>	Lists settings for only the specified profile.

Examples:

```
DLOCommandu -ListProfile -A
DLOCommandu -ListProfile -P <yourprofile>
```

-ListSL command

The *-ListSL* command is used to list the DLO storage locations.

Syntax:

DLOCommandu –listsl [–A | –F | –S]

Note: Wildcard matches (*) are permitted in profile, Storage Location and user names.
Quotation marks are required around names if the name contains a space or colon.

Command options

Table 4-7 –ListSL Command Options

Option	Description
–A	Lists all storage locations (default)
–F <file server>	Lists storage locations for the named server
–S <SL name>	Lists only the named storage location.

Examples:

```
DLOCommandu -listsl -A
DLOCommandu -listsl -F yourserver
DLOCommandu -listsl -S yourSL
```

-ListUser command

The *-ListUser* command is used to list by All, file server, profile name, profile ID, DLO Storage Location name, DLO Storage Location ID, or user name.

Syntax:

```
DLOCommandu -listuser [-A | -F | -P | -PI | -S | -SI | -U]
```

Note: Wildcard matches (*) are permitted in profile, Storage Location, and user names.
Quotation marks are required around names if the name contains a space or colon.

Command options

Table 4-8 –ListUser Command Options

Option	Description
–A	Lists settings for all users (default)
–F <file server>	Lists settings for users with storage locations on the named file server
–P <profile name>	Lists settings for users by profile name
–PI <profile ID>	Lists settings for users by profile ID
–S <SL name>	Lists settings for users by Storage Location name
–SI <SL ID>	Lists settings for users by Storage Location ID
–U <user>	Lists settings for users by user name

Examples:

```
DLOCommandu -listuser -A
DLOCommandu -listuser -P yourprofile
DLOCommandu -listuser -U mmouse
DLOCommandu -listuser -U m*
```

-LogFile command

The *-LogFile* command allows administrators to change the path or name of the LogFile. And, since every command overwrites the LogFile, to track all events (logs), you must change the path\name of the next LogFile to retain older versions.

The default path is the “\Logs” folder under the installed path:

```
C:\Program Files\Symantec\Symantec DLO\Logs
```

If DLO was upgraded from a previous version, the original directory structure is used. The default path for the “\Logs” folder in previous releases was:

```
C:\Program Files\VERITAS\NetBackup DLO\Logs
```

Syntax:

```
-LogFile <path\file>
```

Note: Wildcard matches (*) are permitted in profile, Storage Location and user names.

Quotation marks are required around names if the name contains a space or colon.

Command options

Table 4-9 –LogFile Command Options

Option	Description
<path>	Specifies the path to the new LogFile
<file>	Specifies the filename for the new LogFile

Examples:

```
DLOCommandu -logfile test.log
DLOCommandu -logfile “c:\test.log”
```

-Update command

The *-Update* command is used to list, add, remove, and publish Desktop Agent updates. See “Updating Symantec DLO” on page 51 for detailed information on updating the Desktop Agent software.

Syntax:

```
DLOCommandu -update [-list | -add | -remove | -publish]
```

Subcommands:

The following subcommands allow you to list, add, remove or publish updates. See "Command options" on page 221 for a description of the available options for each command.

Table 4-10 –Update Sub commands

Sub Command	Description
–List [-A|–UI <update ID>]	Lists settings for previously used updates.
–Add –F <file name>	Adds an "update definition file" to the updates list and assigns it a unique update ID number. The update ID number is used when the update is published with the -publish command.
–Remove [-UI <update ID>|–A]	Removes a file or files from the update list.
–Publish [-R] –UI <update ID> [–P <profile name>|–PI <profile ID>|–U <user>]	Makes the specified updates available to users. Users can be identified by using the following options: **-P** Profile name **–PI** Profile RecordID. To obtain the profile RecordID, run the -listprofile command. **–U** User name

Command options

Table 4-11 –Update Command and Sub-Command Options

Option	Description
–A	Updates all
–F <file name>	Specifies a text file that contains update records
–U <user name>	Specifies a fully qualified user name, such as `Enterprise\JFord`
–P <profile name>	Specifies a profile name
–PI <profile ID>	Specifies a profile record ID
–R	Designates to un-publish
–UI <update ID>	Specifies an update record ID

Note: Wildcard matches (*) are permitted in profile, DLO Storage Location and user names.
Quotation marks are required around names if the name contains a space or colon.

Examples:

- To list published updates:

  Lists settings for all published updates

  ```
  DLOCommandu -update -list -A
  ```

  To list details of a specific update:

  ```
  DLOCommandu -update -list -UI <updateID>
  ```

- To add a file to the update list and assign it an ID number

  Prepares an update file to be published and assigns it a unique Record ID number. The Record ID number is returned when the following command is executed:

  ```
  DLOCommandu -update -add -f cntlfile.txt
  ```

- To publish an update to make it available to Desktop Agents

  Makes updates available to users. You can specify whether to make this available to all users, specific users, or users in a profile. You can also use wildcards to specify profile and user names.

  To publish an update for a profile:

  ```
  DLOCommandu -update -publish -UI <updateID> -P <profile
  name>
  ```

```
DLOCommandu -update -publish -UI 63 -P yourprofile
```

To publish an update for a specific user:

```
DLOCommandu -update -list -UI <updateID> -U <username>
```

To publish an update for all users:

```
DLOCommandu -update -list -UI <updateID> -U *
```

- To remove a file from the update list

  Removes a file from the update list. If the file was previously published, it must be unpublished before removing it.

  To unpublish:

  ```
  DLOCommandu -update -publish -R -UI 33
  ```

  To remove:

  ```
  DLOCommandu -update -remove -UI 3
  ```

-EmergencyRestore command

The *-Emergency Restore* command uses the DLO administrator's recovery password to restore user data that would otherwise be unavailable if the DLO database is damaged or corrupted. The recovery password must be known to execute this command. The data will be restored to the specified location in the original data structure, but it will no longer be encrypted. See "Setting a Recovery Password" on page 35 for more information.

Syntax:

```
DLOCommandu -EmergencyRestore <usersharepath> -W <recovery
password> -AP <destination path>
```

Command options

Table 4-12 –EmergencyRestore Command Options

Option	Description
<usersharepath>	Specifies the full path to the user share directory
-W <recovery password>	Specifies the recovery password
-AP <destination path>	Specifies the path to which data will be restored

-SetRecoveryPwd command

The *-SetRecoveryPwd* command is used to change the recovery password, which enables you to retrieve encrypted data that would otherwise be lost if the DLO database is damaged or corrupted. The -SetRecoveryPwd command now updates the password for existing users as well as new users.

Once set, this recovery password can only be changed using the DLO command line interface tools.

See “Setting a Recovery Password” on page 35 for more information.

Syntax:

```
DLOCommandu -SetRecoveryPwd <password>
```

-NotifyClients command

The *-NotifyClients* command forces the Desktop Agents to refresh the profile settings immediately, or the next time the Desktop Agent connects if it is offline.

Syntax:

```
DLOCommandu -notifyclients
```

-InactiveAccounts command

The *-InactiveAccounts* command is used to list and delete accounts that have not been used in a specified number of days.

To list inactive accounts

```
dlocommandu -inactiveaccounts -list -days <#days>
```

This command returns a list of inactive accounts. The list includes the following information, which is used to delete specific accounts:

- computer name
- computer ID
- domain\user name
- user ID

To delete specific inactive accounts

```
dlocommandu -inactiveaccounts -delete -U <domain\user name>
-M <computer name> -days <#days>
dlocommandu -inactiveaccounts -delete -UI <userID> -MI
<computer ID> -days <#days>
```

Where `-U` and `-M` are used to delete the user and computer by name and `-UI` and `-MI` are used to delete the user and computer by ID.

To delete ALL accounts inactive for a specified number of days

```
dlocommandu -inactiveaccounts -delete -a <#days>
```

-RenameDomain command

The *-RenameDomain* command is used after a Windows NT domain has been renamed. Running the -RenameDomain command changes each Desktop Agent user's record to reflect the new domain name and changes the path for the network user data folder. It also notifies each Desktop Agent of the change.

Syntax:

```
DLOCommandu –RenameDomain <OldDomainName> <NewDomainName>
```

-RenameMS command

The *-RenameMS* command is used when an administration server has been renamed. Running the -RenameMS command updates the installation share, DLO Storage Location paths and network user data folder paths. It also notifies each Desktop Agent of the change.

Syntax:

```
DLOCommandu –RenameMS <OldServerName> <NewServerName>
```

-LimitAdminTo command

The *-LimitAdminTo* command limits administration of DLO to the specified group or user.

Syntax:

```
DLOCommandu –LimitAdminTo -NAU <domain\NewAdminName>
DLOCommandu –LimitAdminTo -NAU <domain\NewAdminGroup>
```

Command options

Table 4-13 -LimitAdminTo Command Option

Option	Description
-NAU	The -NAU option is used to add a new DLO administrator or to add a group that can be used of DLO administrators.
-DAU	The -DAU option is used to delete a DLO administrator or a DLO administration group.
-L	The -L option lists all of the current DLO administrators and groups.

`-IOProfile` command

The *`-IOProfile`* command enables a profile to be exported from one DLO Administration Server, and then imported to another administration server. An option is also provided to import global settings.

Note: When a profile is imported, it does not initially have any users assigned to it, so there is no immediate impact. When global settings are imported, they immediately apply to all Desktop Agent users assigned to the server.

- To export a profile:
  ```
  DLOCommandu -C <master server name> -IOProfile -DBF <export
  file name> -E <profile name>
  ```
  This exports the requested named profile (-E) from the specified server (-C) into the named file (-DBF). It is not necessary to specify the master server name with the -C option if the profile is on the same server where the command is run.
- To import a profile:
  ```
  DLOCommandu -C < server name> -IOProfile -DBF <export file
  name>
  ```
  This imports the profile in the given file (-DBF) into the named server (-C.)
- To import the console settings for DLO administrator account management in addition to the profile, use the IPRCS option as follows:
  ```
  DLOCommandu -C < server name> -IOProfile -DBF <export file
  name> -IPRGCS
  ```
- To import the global settings in addition to the profile, use the IPRGS option as follows:
  ```
  DLOCommandu -C < server name> -IOProfile -DBF <export file
  name> -IPRGS
  ```

-Report command

This command generates and saves one of the predefined DLO reports. To generate a report you must specify the name of the .rdl file associated with the report.

For a list of all available reports and their corresponding .rdl file names, use the "-ListReport command" on page 227 or use the file name available when selecting Reports > *report_name* > Properties from the DLO Console UI.

Any filter criteria and the output path where the report is stored are optional.

The report format is also optional. By default the report is generated and saved in PDF. The default report format in the DLO global settings is not used by this command.

Syntax:

```
DLOCommandu -Report -RDL <RDL File Name> [-O <Output Path>]
[-FC <Computer Name>] [-FU <User Name>] [-FD <Days>] [-T
<PDF | HTML | XML | XLS>]
```

Command options

Table 4-14 -Report Command Option

Option	Description
-RDL <RDL File Name>	The name of the .rdl file associated with the required report. Report templates are specified in Report Definition Language (RDL). An RDL file name is required.
-O <Output Path>	Path for storing the generated report. If a path is not specified, the report is stored in the current directory.
-FC <Computer name>	Filter specifying the name of a computer.
-FU <User name>	Filter specifying the name of a user.
-FD <Number of days>	Filter specifying the number of days.
-T <PDF or HTML or XML or XLS>	The format of the report. If a report format is not specified, PDF is used.

Examples:

```
DLOCommandU -Report -RDL DLOactiveevents_en.rdl -FD 3 -FC MyDesktop -O
C:\DLOReports -T PDF
```

This sample command generates a report of the Active Alerts for the machine named MyDesktop in the past 3 days and stores the report in `C:\DLOReports` folder.

For unique report identification, generated reports have a name which is the `.rdl` file name appended by a time stamp. The time stamp includes year, day, month, hours and minutes.

In this example, if the command is executed at 10.28 AM on 25 May 2012, it generates the report file in the folder `C:\DLOReports`, with the name as `DLOactiveevents_en_201225051028.pdf.`

-ListReport command

This command lists all of the reports available in DLO and the names of the corresponding RDL files. The command does not accept any options.

Use this command to determine the RDL file name used as input to the "`-Report` command" on page 226.

Syntax:

```
DLOCommandu -ListReport
```

-MigrateDomain command

This command is used to migrate a user from an old domain to a new domain in trust.

Syntax:

```
DLOCommandu -MigrateDomain -OD <OldDomainName> -ND <NewDomainName> -U
<UserName>
```

Command options

Table 4-15 -MigrateDomain Command Option

Option	Description
-OD	The name of the old domain.
-ND	The name of the new domain.
-U	The name of the user, with or without wildcard.

-ChangeProfile command

This command is used to change the profile assigned to the user(s). Here multiple users can be assigned with the same profile.

Syntax:

```
DLOCommandu -ChangeProfile -NP|-NPI [-A|-F|-P|-PI|-S |-SI|-U]|-UF
```

Note: Wildcard '*' match is permitted in profile, Storage Location, and user names. Quotations around name are required if name contains a space or colon.

Command options

Table 4-16 Change Profile Command Options

Options	Descriptions
-NI <new SL ID>	New Storage Location ID
-NPI <new SL path>	Fully qualified UNC path to new network user data folder
-A	Migrate all users
-F <file server>	Migrate users with storage locations on the named file server
-P <profile name>	Migrate users with named profile
-PI <profile ID>	Migrate users with given profile ID
-S <SL name>	Migrate users with named storage location
-SI <SL ID>	Migrate users with given storage location ID
-U <user>	Migrate named user
-UF <text file name>	Migrate user listed in the given text file. **Note:** While running the above command, the text file should be placed in the path `C:\Program Files\Symantec\Symantec DLO`.

Examples:

```
DLOCommandu -ChangeProfile -NP newprof -A
```

-MigrateUserSL command

This command migrates an existing DLO user's NUDF from one storage location to another location. Users are moved to the new storage location along with their data. A storage location should be a CIFS-based network user data folder. A CIFS-based network user data folder can be present on a Windows server and on certified NAS devices that support CIFS.

Users are disabled during a migration until the client computer is notified that the migration is complete. On successful migration, the DLO client automatically restarts, the user is enabled and their profile is updated to point to the new storage location. User’s data is not deleted from the old storage location. This deletion of data needs to be done manually.

The command also monitors and reports on the progress of the migration (the Migration status report). The command logs the operation updates and progress in a log file and also displays the progress in a command window.

The following user status is used to show user’s NUDF migration to a new storage location.

Data Migration in progress

This message shows the status of the user when the user’sNUDF migration to a new storage location is in progress.
In case the migration process is specifically interrupted, the user status remains as Data Migration in Progress.
See “What happens if the migration process fails or is interrupted?” on page 230. On successful migration the user is enabled and their profile is updated to point to the new storage location. User’s data is not deleted from the old storage location. This deletion of data needs to be done manually.

Desktop Agent users can be migrated to new network storage locations based on the following filter options:

- User account name
- Profile name
- Profile ID
- Storage location
- Storage location ID
- File server name

A new network storage location (the -NI or -NP options) and one of the eight filter options for the user must be specified.

Syntax:

```
DLOCommandu -MigrateUserSL [-NI <new SL id>|-NP <new SL path>] [-A|-F
<file server>|-P <profile name>|-PI <profile id>|-S <SL name>|-SI <SL
id>|-U <user>|-UF <text file path>]
```

Note: Wildcard '*' match is permitted in profile, Storage Location, and user names. Quotations around name are required if name contains a space or colon.
To get a list of all storage locations use the `-ListSL` command.

Command options

Table 4-17 Migrate USer SL Command Options

Options	Descriptions
-NI <new SL ID>	New profile to assign
-NP <new SL path>	New profile to assign (by ID)
-A	All users
-F <file server>	Users with storage locations on the named file server
-P <profile name>	Users with named profile
-PI <profile ID>	Users with given profile ID
-S <SL name>	Users with named storage location
-SI <SL ID>	Users with given storage location ID
-U <user>	Named user account only

Examples:

The following examples show you how to use the command options:

```
DLOCommandu -MigrateUserSL -NI DLO_SL02 -A
DLOCommandu -MigrateUserSL -NI DLO_SL03 -U SUS\mmouse
```

About the Migration Status Report

A status report is generated for each migration operation. The default location for this report is `C:\Program Files\Symantec\Symantec DLO\Logs`. The name of the report file is `DLOSLMigrationReport.log`.

What happens if the migration process fails or is interrupted?

If a migration process fails or is interrupted, there is no data loss. The original storage location continues to contain all the data.

The following scenarios can occur if the migration process fails or is interrupted:

Case 1

Migration process fails due to issues such as data size mismatch on the source and destination administration servers.

If the migration process fails due to issues like network outage, the partially migrated files are deleted from the new storage location. Any new backups are stored in the original storage location. All the data needs to be recopied again.

The migration procedure must be followed again to migrate the NUDF to another storage location.

Case 2

Migration process is specifically interrupted.

If you interrupt the migration process with a kill command or a system shutdown, the user status appears as Data Migration in Progress. The status of the computer user is also disabled. The partially migrated files remain on the new storage location.

In this case, this user and the respective computers must be enabled using the DLO Administration Console. The partially migrated files should also be removed from the new storage location.

The migration procedure must be followed again to migrate the NUDF to another storage location.

-MigrateUser command

This command migrates single or multiple users from one Administration Server to another Administration Server. The user's data can now be accessed from the destination Administration server. All user-specific settings such as customized backup selection and policies are migrated along with the user.

The command also monitors and reports on the progress of the migration (the User Migration Status Report). The command logs the operation updates and progress in a log file.

The user that is migrated is disabled until the client computer is notified that the migration is complete. Upon successful migration, the DLO client automatically restarts and connects to the new Administration Server.

The following are the status messages for user migration:

User Migrated	Indicates the status of the user on the source administration server after the user is successfully migrated.
User Migration in progress	Indicates the status of the user on the source administration server while the user is migrated. If the migration process is specifically interrupted, the user status appears as *User Migration in Progress*.

Prerequisites for Migrating Users across Administration Servers

The following prerequisites must be met before you can migrate users across Administration Servers:

Domain — The source and the destination administration servers must be on the same domain or on trusted domains.

Administrative Rights — The Administrator of the source Administration server must have administrative rights on the destination Administration server.

DLO Versions — The source and the destination administration servers must have the same DLO versions and same patch levels.

Shared Clients — The user that is migrated must not share the client computer with any other user.

Storage Locations — On the destination administration server, configure the same storage location that is present on the source administration server.

The name of the storage location on the destination administration server must be exactly the same as the storage location on the source administration server.

Profile — On the destination Administration server, create the same profile that is present on the source Administration server. This profile is used by the user that is to be migrated. The profiles can be migrated to the destination Administration server by using the

-IOProfile command. For more information, see "-IOProfile command" on page 225.

Dedupe Server — The source and destination Dedupe Servers must be on the same domain or on a trusted domain.

Dedupe Storage Pools — On the destination administration server, configure the same Dedupe Storage Pool that is present on the source administration server.

The name of the Dedupe Storage Pools on the destination administration server must be exactly the same as the Dedupe Storage Pools on the source administration server.

Dedupe Storage Locations — On the destination administration server, configure the same Dedupe Storage Location that is present on the source administration server.

The name of the Dedupe Storage Location on the destination administration server must be exactly the same as the Dedupe Storage Location on the source administration server.

Migrating Users across Administration Servers

Before you start the migration process, review the section “Prerequisites for Migrating Users across Administration Servers” on page 232.

To migrate users across Administration Servers

1. On the destination administration server, configure the same storage location that is present on the source administration server. The name of this storage location must be exactly the same as the storage location on source administration servers. For example, the storage location name on the source administration server is *storage1*. The destination server must also contain a storage location with the name *storage1*.

2. On the destination administration server, create the same profile for the user. The profile can be migrated to the destination server with the `-IOProfile` command. The profile name must be exactly the same on both the source and the destination servers. For more information, see “`-IOProfile` command” on page 225.

3. On the source administration server, enter the following command:

   ```
   DLOCommandu -MigrateUser -M <media server>[-A|-F <file
   server>|-P <profile name>|-PI <profile id>|-S <SL name>|-SI
   <SL id>|-U <user>|-UF <text file path>]
   ```

   Note: Wildcard '*' match is permitted in profile, Storage Location, and user names.
   Quotations around name are required if name contains a space or colon.
   To get a list of all storage locations, use the `-ListSL` command.

Command options

Migrate User Command Options

Options	Descriptions
-M <media server>	New media server name
-A	Migrate all users
-F <file server>	Migrate users with storage locations on the named file server
-P <profile name>	Migrate users with named profile
-PI <profile ID>	Migrate users with given profile ID
-S <SL name>	Migrate users with given storage location
-SI <SL ID>	Migrate users with given storage location ID
-U <user>	Migrate named user only
-UF <text file path>	Migrate users listed in the given text file.

Optional parameters for destination DB

Options	Descriptions
-DB server <DB server>	Default: same as media server
-DBInstance <DB instance>	Default: DLO
-DBName <DB name>	Default: DLO
-DBDataFile <DB data file>	Default: DLO.mdf
-DBLogFile <Db log file>	Default: DLO_log.mdf

Note: For the `-DBInstance` option, specify “” in case of a blank instance.

The following are examples of using this command:

```
DLOCommandu -MigrateUser -M MARY.CAF.dlo.com -P Profile1
DLOCommandu -MigrateUser -M MARY.CAF.dlo.com -U CAF\ummouse
```

On the source administration server, the user’s status changes to *User Migrated* once the migration is successful. Delete this user from the Administration Console.

User Migration Status Report

A status report is generated for each migration operation. The default location for this report is `C:\Program Files\Symantec\Symantec DLO\Logs`. The name of the report file is `DLOUserMigrationReport.log`.

Troubleshooting during migration process

What happens when the migration process is interrupted?

The migration process may fail due to any number of issues.

Case 1

Migration process fails due to issues such as network outage.

In a multiple-user migration process, only one user is migrated at a time.

A rollback operation occurs if the migration process fails due to the following issues:

- Network outage
- Sharing of the client computer by multiple users during the migration

In these cases, the following takes place:

- Migrated users are not affected. These users are successfully migrated to the destination administration server. The status for these users appears on the source administration server as User Migrated.
- Users that are not migrated still exist on the source administration server. See the migration procedure in the preceding sections to migrate these users to the new administration server.
- Users that were in the process of migration are affected. A rollback operation follows and the particular user on the source administration server rolls back to its previous status (Enabled/Disabled). Also, the user profile points only to the source administration server.

The migration procedure must be followed again to migrate this user to the new administration server.

Case 2

Migration process is specifically interrupted:

In a multiple-user migration process, only one user is migrated at a time.

If the migration process is specifically interrupted say by issuing a kill command or system shutdown, the following takes place:

- Migrated users are not affected. These users are successfully migrated to the destination administration server.
- Users that were not migrated still exist on the source administration server. See the migration procedure to migrate these users to the new administration server.

Users in the process of migration are affected. The status for this particular user appears on the source administration server as User Migration in Progress. The computers and the users of those computers are also disabled. The user and the respective computers for that user must be enabled on the source administration server by using the DLO Administration Console. Then, migrate the user with the migration procedure.

-ListMachines command

This command lists all the DLO Agent machines that are connected to the DLO Administration Console.

Syntax:

```
DLOCommandu -ListMachines |-v | -v <product version>
```

If you do not specify any parameters, by default, all machines connected to the current DLO Administration

console is displayed at the command prompt.

To store the list in a file, provide a file name when you run the command.

```
DLOCommandu -ListMachines <file path>
```

Example `DLOCommandu -ListMachines > C:\MachineList.txt`

Optional parameters

Options	Descriptions
-V	Displays all machines with product version
-V <product version>	Displays machines with the specified product version

-DeletePendingUser command

The `-DeletePendingUser` command deletes only those users that are in the “DeletePending” state. This command does not delete the users’ NUDF data.

Syntax

```
DLOCommandu -DeletePendingUSer [-U]
```

Note: Wildcard ‘*’ match can be used with user name. Quotations around the user name are required if the name contains a space or colon.

Example `DLOCommandu -DeletePendingUser -U user 1`

Optional parameters

Option	Description
-U	Deletes users in pending state

DLO Command Line Interface Database and License Tools

DLO provides a number of command line system tools that enable you to perform configuration and maintenance operations.

DLO Command Line Interface Database and License tool commands are run from the installation directory and are executed with the `DLODBUtils` command.

Command Line Options

The command-line options enable you to set specific parameters when performing a maintenance or management function with the command-line tools.

Server

`-server <computername>`

Use this command to specify the computer on which DLO command-line functions will take affect. You must have sufficient privileges on the specified computer to perform functions remotely.

Example `DLODBUtils -server server1 -backup`

Verbose

`-verbose`

Use this command to turn on verbose mode and display additional detail when DLO command-line operations are performed.

Example `DLODBUtils -verbose -backup`

DLO Database Maintenance

The following commands perform database maintenance functions. The options outlined in “Command Line Options” on page 237 may be used with these commands.

Check database

```
-check
```

This command performs a consistency check of the DLO database. If there are any consistency errors, you should run the Repair Database command. See “Repair database” on page 239.

Backup database

```
-backup -dir <backup directory>
```

This command allows you to back up the DLO database to a specified directory.

Example `DLODBUtils -backup -dir "c:\backups\DLODatabase"`

IDR

This command copies and recovers DLO Intelligent Disaster Recovery (IDR) MSDE database files.

```
-setupidr
```

Makes a copy of the MSDE database files.

Example `DLODBUtils -setupidr`

```
-idr
```

Restores the MSDE database files saved with the -setupidr command. The computer must be restarted following the execution of this command to make the changes effective.

Example `DLODBUtils -idr`

Restore database

```
-restore -databasefile
```

This command restores the database from a specific backup file.

Example

```
DLODBUtils -restore -databasefile
"c:\backup\DLO.bak"
```

Note: Exclusive database access is required to run the `-restore` command.

Routine Maintenance

The following commands are used to perform routine maintenance. The options outlined in “Command Line Options” on page 237 may be used with these commands.

Compact database

`-compact`

Compresses the database by removing a database’s unused space.

Example `DLODBUtils -compact`

Rebuild index

`-rebuildindex`

Rebuilds the index for the DLO database.

Example `DLODBUtils -rebuildindex`

Repair database

`-repair`

Repairs the DLO database

Example `DLODBUtils -repair`

Groom alerts

-groomalerts *days*

Removes alerts older than a specified number of days.

Example `DLODBUtils -groomalerts` *`5`*

Database Management

Attach database

The attach command makes the DLO database available to the database engine.

Note: Exclusive database access is required to run the -attach command. Stop the DLO Administration Service before running this command and then restart the services after running the command.

-attach -datafile <*database file name*> -logfile <*database log file name*>

Example

```
DLODBUtils -attach -datafile "c:\backup\DLO.mdf"
-logfile "c:\backup\DLO.ldf"
```

Detach database

Note: Exclusive database access is required to run the -detach command. Stop the DLO Administration Service before running this command and then restart the services after running the command.

Use this command to detach the database.

Example `DLODBUtils -detach`

License Management

These command-line tools enable license management from the command line.

List licenses

`-list`

Lists current DLO licenses.

Example `DLOLicenseCLI.exe -list`

Add licenses

`-add <`*`license key`*`>`

Adds the specified license key.

Example `DLOLicenseCLI.exe -add <`*`license key`*`>`

Delete licenses

`-delete <license key>`

Deletes the specified license key.

Example `DLOLicenseCLI.exe -delete <`*`license key`*`>`

DLO Logging Command Line Interface Tool

DLO provides a command-line tool that enables logging with different logging levels for all the DLO binaries.

These `DLOLoggingu` command is run from the installation directory.

```
C:\Program Files\Symantec\Symantec DLO\DLOLoggingu.exe
```

Syntax

```
DLOLoggingu -E <DLO component Executable name> [Options [-L |
-LS]]
```

Note: In a distributed DLO environment, the DLO Logging command-line tool will be deployed in each machine where individual DLO component is installed.

Table 4-18 DLOLoggingu options

Options	Descriptions
-E	This option is used to specify the DLO component's executable name for which logging is to be enabled. Example: To enable logging for DLO console component, specify `DLOConsoleu.exe` as parameter for the -E option. `DLOLoggingu -E "DLOConsoleu.exe"` It is mandatory to specify the DLO component's executable name. Else, the command execution will not proceed.
-L	This option is used to specify the logging level with which the logging should be enabled. Specify one of the following parameters along with the -L option. ■ Verbose (**V**): In this level, all Errors, Warnings, Traces and Function Entry/Exit traces are printed. ■ Common (**C**): In this level, only Errors, Traces and Warnings are printed to the log file. ■ Disable (**D**): In this level, all warnings and errors are printed to log files. This value is set as default if no logging is specified in the command line. If you do not specify any parameter for this option, then by default logging level is set to Disable, that is "**D**". Example: `DLOLoggingu -E "DLOConsoleu.exe"`
-LS	This option enables to specify the size of the log files. **Note:** The value specified with this option is common for all the DLO components for which logging will be enabled. This value will not set the log size for individual DLO component. If no log size is specified while running this utility for the first time, then the default log size will be considered as 10 MB. Example: `DLOLoggingu -E "DLOAdminsvcu.exe" -L "V"` Once the log size is set, this value remains the same until you explicitly change the log size using this option again.

Note: After you run the `DLOloggingu` command, for the new changes to take effect, ensure that you restart or relaunch the DLO console, DLO client and the DLO services for which logging is enabled.

Example

To enable verbose logging for DLO Administration service, run the following command:

```
DLOLoggingu -E “DLOAdminsvcu.exe” -L “V” -LS “20”
```

After executing this command, restart the DLO administration service for the new changes to take effect.

Symantec DLO Log Gather Tool

The Symantec DLO Log Gather tool enables you to collect logs from various product install paths, log path, registry export, operating system, and from the installed applications.

Note: `DLOGatherU.exe` gathers product logs from Symantec DLO 7.0 onwards.

Note: The tool also depends on `DLODBUtils.exe` to collect the DB backup, and `DLOCommandu.exe` to collect information about users, profiles, and computers. Therefore, check whether the machine on which DLO is installed is 32-bit or 64-bit, and then run the appropriate version of the tool on that machine.

To gather the logs

1. Navigate to the following path:
   `C:\Program Files\Symantec\Symantec DLO`
2. Double-click the `DLOGatherU.exe` tool.
3. Select the appropriate check boxes to gather the required logs.
   - DLO Installation Logs
   - DLO Application Logs
   - Operating System Logs
   - DLO Database
   - Dedupe Logs

4 Enter the path of the directory or click **Browse** to select the output directory where the gathered logs should be saved.

5 In the **Additional files to gather** field, enter the file names or click **Browse** to select the additional files to be gathered.

6 Click **Add Files**.

7 Click **Gather** to start collecting the selected logs.

Once the process is completed, a file is created in the selected output directory in the following format: `IncidentNumber_MachineName_CurrentTime.cab`

Troubleshooting

When you are using Windows 2003 server, the operating system logs of installed applications that will be stored in the `installed_apps.txt` file is empty.

Solution

In Windows 2003 server, you must install the WMI Windows Installer Provider.

1 In the Windows Control Panel, select **Add or Remove Programs**.

2 Select **Add/Remove Windows Components**.

3 In the **Windows Components** Wizard, select **Management and Monitoring Tools** and then select **Details**.

4 In the **Management and Monitoring Tools** dialog box, select **WMI Windows Installer Provider**.

5 Click **OK**.

6 Click **Next.**

7 Follow the instructions in the wizard.

Garbage Collection Utility

Garbage Collection (GC) is an administrative job that needs to be scheduled in the Dedupe Server machine. GC reclaims the Dedupe Storage Location storage space used by unreferenced data.

This is a time-bound process that runs as per the maximum duration specified in the command.

Note: During garbage collection, Dedupe Server automatically switches to maintenance mode, and you cannot perform backup or restore operations.

The Garbage Collection tool tries to accomplish as much as possible in the specified duration, and exits once the time limit is reached. If the job is not completed in the specified duration, then the tool continues the job from where it was stopped in the previous run.

If the garbage collection process completes before the specified duration, then the tool immediately exits, and the Dedupe Server resumes with backup and restore operations.

The administrator can do regular scheduling of garbage collection by using the Windows Task Scheduler.

To run the garbage collection utility

1. Open the command prompt.
2. Change to the DLO installation directory.

   ```
   C:\Program Files\Symantec\Symantec DLO
   ```

3. Run the `DDGC.exe` utility.

   ```
   DDGC.exe <ServerName with port number>|<MaintenanceTime in
   minutes>
   ```

   Server name with port number: Enter the server name and the port number in this format: `<https://><Server Name>:<Port Number>`

   Maintenance Time: Enter the maximum duration (in minutes) for the server to be in maintenance mode.

   Example code for 30 minutes GC:

   ```
   DDGC.exe https://10.45.50.5:8443 30
   ```

   Dedupe Server’s IP is 10.45.50.5 (machine name can also be used instead of IP).

   Default HTTPS port for Dedupe server is 8443.

Administering the Desktop Agent

This section contains the following topics:

About the Desktop Agent

The Desktop Agent is the component of the Symantec DLO that protects files on desktop and laptop computers (collectively referred to as desktops) by backing up data to the desktop's local drive and to a Storage Location on the network. The DLO administrator initially configures the Desktop Agent. If the DLO administrator has set your profile so that you can view the complete Desktop Agent and modify settings, then you can restore files, synchronize files between multiple desktops, configure backup selections, set schedules, view history and more.

Your profile determines the level of interaction between you and the Desktop Agent. The administrator may also configure the Desktop Agent to run without a user interface, with a fully functional user interface, or somewhere in between.

Features and Benefits of the Desktop Agent

The Desktop Agent provides the following features:

- **Data Protection:** Selected files on the desktop are automatically copied to user data folders on the desktop's local drive and on the network. The Desktop Agent can be configured so that no user interaction is required. Files are protected automatically when the desktop is online or offline.
- **Data Availability:** A user can access data from multiple desktops in multiple locations if they are using the same login credentials on each desktop. Users can also restore previous file revisions, even when the desktop is offline, if they are saving at least one file revision in the desktop user data folder.
- **Synchronization:** A user that accesses multiple computers with the same login credentials can configure folders to be synchronized on each of the computers. When a synchronized file is changed on one computer, the updated file is copied to the network user data folder and also to the desktop user data folder on all other computers that are configured for synchronization.

System Requirements for the Desktop Agent

The following are the minimum system requirements for running this version of the Desktop Agent.

Table 5-1 Minimum System Requirements

Item	Description
Operating System	■ Microsoft Windows XP 32-bit, Service Pack 3 ■ Microsoft Windows XP 64-bit, Service Pack 2 ■ Microsoft Windows Vista (32-bit and 64-bit) Service Pack 2 ■ Microsoft Windows 7 (32-bit and 64-bit) ■ Microsoft Windows 8 Desktop
CPU	1.5 GHz 32/64-bit
Processor	Pentium, Xeon, AMD, or compatible
Memory	Required: 1 GB MB RAM Recommended: 2 GB (or more for better performance).

Table 5-1 Minimum System Requirements (continued)

Item	Description
Disk Space	100 MB hard disk space

Installing the Desktop Agent

The DLO administrator determines who installs the Desktop Agent. It can be either the administrator or the desktop user. Administrator rights are required to install the Desktop Agent. After the Desktop Agent is installed on a desktop, anyone who logs on to that desktop can use the Desktop Agent. The logged on user will only have access to DLO backup files associated with the logged on account.

All computers running the DLO Administration Console or the Desktop Agent should be set to a common time. This can be accomplished by configuring the Windows Time Synchronization service on the network. See www.microsoft.com for more information.

Note: You must have administrative rights to the desktop on which you want to install the Desktop Agent. If you need to restart the desktop during installation, you must use the same administrator login again to ensure that the installation completes successfully.

To install the Desktop Agent

1. From the desktop on which you want to install the Desktop Agent, browse to the network server where the installation files for the Desktop Agent are stored. The default location is `\\<DLO Administration Server name>\DLOAgent`. If you are unsure of the location, contact the administrator.
2. Double-click the file **setup.exe**.
3. On the Welcome screen, click **Next**.
4. Read the license agreement, and then click **I accept the terms in the license agreement**.
5. Click **Next**.
6. Do one of the following:
   - a To change the location on the desktop's local drive where the Desktop Agent will be installed, click **Change** and enter the alternate location, then click **OK**.
   - b To install the Desktop Agent in the default location, continue with step 7.

The default installation location is `C:\Program Files\Symantec\Symantec DLO\DLO`.

7 Click **Next**.

8 Click **Install**.

9 Click **Finish** to install the Desktop Agent.

Configuring the Desktop Agent

The following topics are useful for reference when configuring the Desktop Agent:

- "Connecting to the DLO Administration Server" on page 248
- "Using Local Accounts on Desktop Computers" on page 249
- "Using Alternate Credentials for the Desktop Agent" on page 249
- "Resetting Dialog Boxes and Account Information" on page 251
- "Changing your Connection Status" on page 251
- "Disabling the Desktop Agent" on page 252
- "Enabling the Desktop Agent" on page 252

Connecting to the DLO Administration Server

The Desktop Agent communicates with the DLO database and services on the DLO Administration Server during normal operation. When using the Desktop Agent, you must connect to the administration server using a domain account.

Note: If you connect to the administration server with one set of credentials, and then attempt to connect to the server with a different set of credentials, authentication may fail. Restart the computer to reconnect.

When new information is available for the Desktop Agent, the Desktop Agent receives a notification of this new information and retrieves it. This will happen, for example, when settings or synchronized files change or if a software update is available. The Desktop Agent and the DLO Administration Server do not contact each other directly.

Caution: If you attempt to connect to a server using characters in the share name that do not exist on the code page for the local system, the connection will fail. Code pages map character codes to individual characters, and are typically specific to a language or group of languages.

Using Local Accounts on Desktop Computers

You can log in to your desktop with a local account. If you log on to your desktop with a local account, the Desktop Agent prompts you for your user name and password for your domain account.

The following should be considered when using local accounts on desktops that run the Desktop Agent:

- You can only use a set of domain credentials with one local account. If you use more than one local account on a desktop or laptop computer, you should either disable DLO for other accounts or have unique domain credentials for each account. See "To log on with alternate credentials or to disable accounts" on page 250 for more information.

  Example `If you usually log on to the desktop computer as ‘myusername’, you should have a domain account to use for DLO with this account. If you also occasionally log on as ‘administrator’, DLO can be disabled when you are logged on to this account. Alternately, you can provide a unique set of domain credentials to use for DLO when you are logged on as ‘administrator’.`

- Multiple users of the same desktop computer can all use DLO, but must provide unique credentials for the desktop computer and unique domain credentials for connection with the Desktop Agent.

- DLO does not support the Fast User Switching feature of Windows XP.

Using Alternate Credentials for the Desktop Agent

The account used by the Desktop Agent is the logon account by default, but could be an alternate account if one has been specified, such as when connecting across domains.

If you are logged on with credentials that are not recognized by the Desktop Agent, you can specify alternate credentials for Desktop Agent operation and save the account information for future sessions. If you prefer, you can disable an account for Desktop Agent operations so that the Desktop Agent will not run when you are logged on with the account currently being used. This dialog allows you to save this account info for future connections.

Note: If you have a previously established network connection to the administration server and it does not match the account the Desktop Agent is using, the Desktop Agent will attempt to reconnect as the Desktop Agent user. If this fails, the following error displays: “Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again.The account used by the Desktop Agent is the logon account by default, but could be an alternate account if one has been specified; for example, to connect across domains.

Using alternate credentials to work across domains

In a cross-domain configuration where there is no trust relationship, if multiple users are running the same Desktop Agent, each user must provide a unique user name and password in the DLO Administration Server domain. If different users use the same credentials, DLO displays an error message stating that the user is already connected to the administration server.

Note: For information on resetting accounts that have been disabled for Desktop Agent operation, see “To reset dialogs and account information” on page 251.

To log on with alternate credentials or to disable accounts

1 When you are logged on to the desktop computer with an account that is not recognized by the Desktop Agent, the **Alternate Credential** dialog box will appear.

2 Specify Desktop Agent logging options as described in the following table.

Table 5-2 Alternate Credentials

Item	Description
Use this account	Select this option to enable the Desktop Agent to run when you are using the account under which you are currently logged on.
User name	Enter the user name for an account that is authorized for Desktop Agent operation.
Password	Enter the password for the account to be used for Desktop Agent operation.
Domain	Type the domain for the account to be used for Desktop Agent operation.

Table 5-2 Alternate Credentials (continued)

Item	Description
Save my password	Select this option to have DLO save and use this password in the future to automatically authenticate to the media server or storage location in the event of an authentication failure. **Note:** This option will only appear if the DLO administrator has enabled this option. On newly-deployed Desktop Agents, this option will not show until the second time the Desktop Agent connects to the media server.
Disable this account	Select this option to prevent the Desktop Agent from running when you are using the account under which you are currently logged on.

3 Click **OK**.

Resetting Dialog Boxes and Account Information

While you can suppress dialogs by selecting the **Don’t show me this message again** check box. These dialogs can be reset so they will once again be displayed. If passwords and account information are cleared, the Desktop Agent will prompt for this information if it is required to access a resource.

To reset dialogs and account information

1. From the **Tools** menu, click **Options**.
2. If you want to reset any information dialogs suppressed by the **Don’t show me this message again** check box, click **Reset dialogs**.
3. Click **Yes** when prompted to reset the dialogs.
4. If you want to clear any passwords and account information that the Desktop Agent has stored, click **Reset accounts**.
5. Click **Yes** when prompted to clear the accounts.
6. Click **OK**.

Changing your Connection Status

When you are using the Desktop Agent, your connection status is displayed in the lower right corner of the Desktop Agent Console. When the Desktop Agent is in offline mode, the following are true until you choose to work online again:

- Files are not transferred to the network user data folder. Pending files remain in the pending files list with a status of “Pending network”
- Job logs are not copied up to the network user data folder
- Alerts are not posted to the DLO Administration Server

To change your connection status

1 Click the connection status on the lower right corner of the Desktop Agent.

2 Do one of the following:

- Click **Work Offline** to place the Desktop Agent in offline mode
- Click **Work Online** to place the Desktop Agent in online mode

Note: The DLO Administrator sets a maximum time after which the Desktop Agent will automatically be returned to the online mode, assuming a network connection is available.

Disabling the Desktop Agent

If your Profile allows it, you can disable the Desktop Agent.

To disable the Desktop Agent

1 From the Windows system tray, right-click the Desktop Agent icon.

2 Click **Disable**. This option will be grayed out if you do not have permission to take this action.

Enabling the Desktop Agent

If the Desktop Agent has been disabled, and your Profile allows it, you can re-enable the Desktop Agent.

To enable the Desktop Agent

1 From the Windows system tray, right-click the Desktop Agent icon.

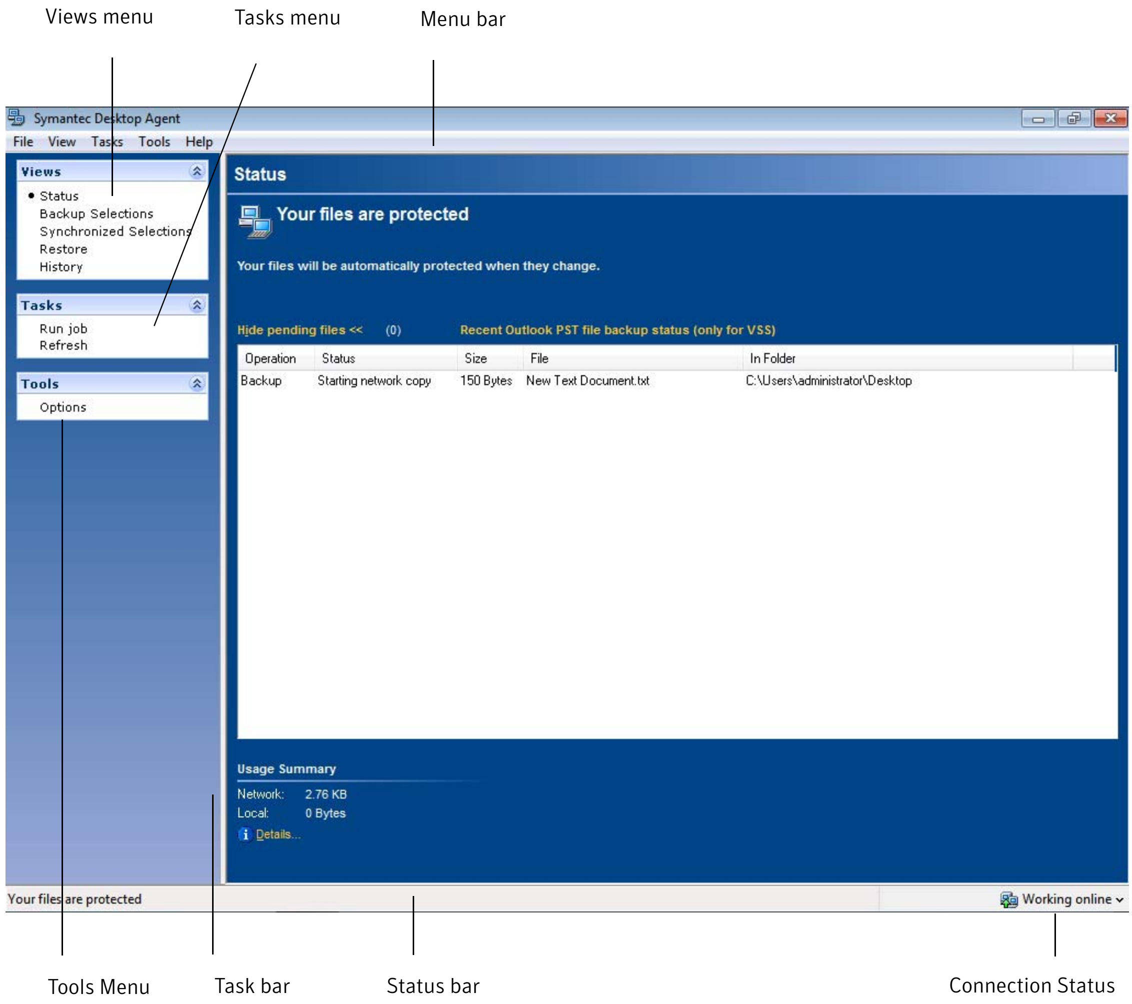
2 Click **Enable**. This option will be grayed out if you do not have permission to take this action.

About the Desktop Agent Console

The Desktop Agent Console is the user interface for the Desktop Agent. Access to the Desktop Agent Console is controlled by the DLO administrator. The DLO administrator may choose from the following:

- Display the complete interface: Enables desktop users to access all Desktop Agent options
- Display only the status: Enables desktop users to view the status of backup jobs, but they cannot change Desktop Agent settings or access options other than status. Desktop users can right-click the system tray icon to open the status view or exit the program
- Display only the system tray icon: The desktop user sees only the Desktop Agent icon in the system tray in the lower right corner of the screen. Desktop users can right-click the system tray icon to exit the program
- Do not display anything: The Desktop Agent runs in the background. The desktop user cannot view the Desktop Agent

Figure 5-1 Symantec DLO Desktop Agent console



Status

Your files are protected

Your files will be automatically protected when they change.

Hide pending files << (0) Recent Outlook PST file backup status (only for VSS)

Operation	Status	Size	File	In Folder
Backup	Starting network copy	150 Bytes	New Text Document.txt	C:\Users\administrator\Desktop

Usage Summary

Network: 2.76 KB
Local: 0 Bytes
Details...

Your files are protected

The Desktop Agent Console has the following components.

Table 5-3 Desktop Agent Console Features

Item	Description
Menu bar	The menu bar appears across the top of the screen. To display a menu, click the menu name. Some menu items are not available until an item is selected from the console screen.
Tasks bar	The Tasks bar appears on the left side of the Desktop Agent Console. To hide the Tasks bar, from the **View** menu, select **Tasks bar**. Actions are initiated from the Tasks bar, and these actions vary with the selected view.
Views menu	The Views menu appears in the Tasks bar and enables you to navigate to the following views:
Status	Provides job status, lists pending jobs, and summarizes recent backup activity. See “Viewing the Desktop Agent Status” on page 281 for more information.
Backup Selections	Enables you to define what data is protected by the Desktop Agent. See “Using the Desktop Agent to Back up Your Data” on page 256 for more information.
Synchronized Selections	Enables you to configure the Desktop Agent to maintain a user’s selected files and folders on multiple computers so that the most recent backed up version is always available to the user. See “Synchronizing Desktop User Data” on page 277 for more information.
Restore	Enables the user to restore backed up data and search for backed up files. See “Restoring Files Using the Desktop Agent” on page 286 for more information.
History	Displays Desktop Agent error, warning, and informational messages.
Tasks menu	Actions are initiated from the tasks menu. These actions vary with the selected view.
Tools menu	
Options	Enables you to do the following: ■ Reset dialogs that have been suppressed by the **Don’t show me this message again** check box ■ Clear passwords and account information that the Desktop Agent has stored. See “Resetting Dialog Boxes and Account Information” on page 251 for more information

Note: To ensure that you have the latest status and settings at any time while using the Desktop Agent, from the **Tasks** menu, click **Refresh**.

Using the Desktop Agent to Back up Your Data

When data is backed up by the Desktop Agent, it is transferred to the user data folder on the desktop's local drive. Then, the data is transferred to a network user data folder, which is assigned by the DLO Administrator. Network user data folders are typically also backed up by Symantec DLO, which provides an additional level of protection.

Caution: If you attempt to connect to a server using characters in the share name that do not exist on the code page for the local system, the connection will fail. Code pages map character codes to individual characters, and are typically specific to a language or group of languages.

For information on backing up and restoring Microsoft Outlook PST files, see "Backing up Outlook PST Files Incrementally" on page 265 and "Restoring Microsoft Outlook Personal Folder Files" on page 289.

Select files that you want to protect from the **Backup Selections** view. Backup selections are initially assigned by the administrator, but if the DLO administrator has set your profile so that you can view the complete Desktop Agent and modify settings, then you can choose your backup selections.

You can change Desktop Agent settings and backup selections when you are working offline. The settings will be stored until you are once again working online, at which time they are automatically transferred. If the administrator has also made changes that conflict with the changes made on the Desktop Agent, the changes made by the administrator will be used.

You can view and modify backup selections using two views: standard and advanced. The standard view lists the contents of your local drives, allowing you to check off files and folders to be backed up. It also uses default backup selection settings to add new selections. The advanced view provides more configuration options for selections.

A backup selection consists of:

- A folder or list of folders
- Criteria for the files to be included or excluded from the backup
- Limits on the number of file revisions to retain
- Settings for compression, backup file deletion, and encryption

Managing Revisions

Revisions are versions of a file at a specific point in time. When a file is changed and backed up, DLO stores a new revision. DLO stores and maintains a specific number of revisions for all files in a backup selection. Because each backup selection is configured separately, the number of revisions retained can vary for different backup selections.

When the number of revisions is exceeded, DLO removes the oldest revision, maintaining only the specified number of revisions in the desktop and network user data folders.

You can limit the number of revisions DLO retains in a given period of time. If you are working on a document and backing it up frequently, all of your revisions could potentially be just a few minutes apart. By specifying that you want to retain only 2 revisions every 24 hours, at least 120 minutes apart, you can retain older revisions for a longer period of time. While some intermediate versions will not be retained, it does support situations in which returning to an older revision is needed.

Another consideration in determining the number of revisions to retain is the amount of storage space required to store the data. The amount of space required for backups can be estimated by multiplying the number of revisions retained by the amount of data protected.

Example `If you are retaining three revisions of each file and have 10 MB to back up, approximately 30 MB of disk space will be required.`

Although compression can improve the space utilization, it varies significantly with file type and other factors.

Alternate stream backup

DLO protects all of the alternate streams for a file, including security streams. If a new version of a file contains only alternate stream data modifications, the new version replaces the old version without impacting the revision count.

Related topics

"Modifying Backup Selections in the Standard View" on page 258

"Adding Backup Selections in the Advanced View" on page 259

"Backing up Outlook PST Files Incrementally" on page 265

"Restoring Microsoft Outlook Personal Folder Files" on page 289

"Restoring Files with Alternate Stream Data" on page 290

File Grooming

The Desktop Agent grooms revisions based on backup selection settings and does this as new revisions are created. The oldest revision is deleted when a new revision is created that exceeds the limit.

Maintenance grooming is the grooming off of deleted files. It occurs at most once every 24 hours. Maintenance grooming occurs during the first backup that runs after 24 hours have passed since the last maintenance grooming.

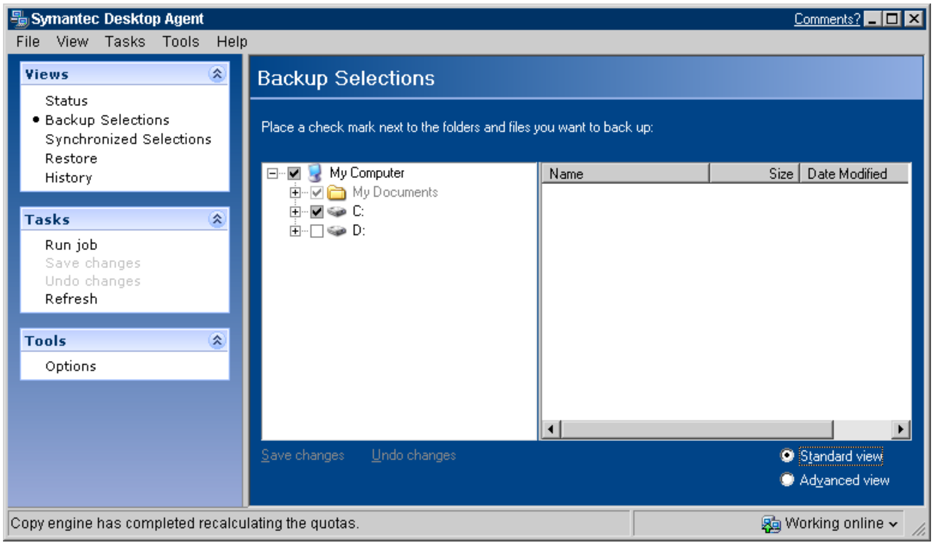
Modifying Backup Selections in the Standard View

Backup selections in the Standard view provides a list of drives, folders, and files that you can select for backup.

Note: *Profile backup selections* are those that were specified by the DLO administrator in your profile. You cannot modify profile backup selections in the Standard view. You can only modify the backup selections that you create on the Desktop Agent. Profile backup selections are displayed in the Standard view with gray check boxes. They can be modified in the Advanced view if the administrator has granted you sufficient rights. See "Modifying Backup Selections in the Advanced View" on page 264 for more information.

When you create new backup selections in the standard view, the default backup selection settings are used. When you add new sub folders and files to the backup selection using the standard view, these new backup selections will have the same settings as the main folders.

Figure 5-2 Standard view



Place a check mark next to the folders and files you want to back up:

Copy engine has completed recalculating the quotas.

In the Desktop Agent Backup Selection Standard view, files and folders are represented in a tree view where users can select or deselect files and folders for backup. When the check box next to a file or folder is grayed out, the selection was defined by the administrator and can only be changed if the administrator has granted this right in the profile definition. When a red 'X' appears in the check box next to a file or folder, this item has been globally excluded from all backups by the administrator and cannot be selected.

To modify backup selections in the backup selections standard view

1 Under **Views** in the Desktop Agent Tasks bar, click **Backup Selections**.

2 Click **Standard view**.

3 Select the folders and files you want to back up.

Expand selections by clicking the plus sign (+) and collapse selections by clicking the minus sign (-).

Note: To return to the last saved settings at any time, click **Undo changes**.

4 Click **Save changes** to save the new settings or **Undo changes** to return to the last saved settings.

After clicking Save, previously backed-up selections that were not selected are treated like deleted backup selections and will no longer be backed up. The backup files for this selection will be deleted after the number of days specified in the backup selection settings. The source files for the deleted backup selection will not be deleted by the Desktop Agent.

Selected folders that were not previously selected are added to the backup selections for this desktop.

Adding Backup Selections in the Advanced View

To add a backup selection in the backup selections advanced view

1 Under **Views** in the Desktop Agent Tasks bar, click **Backup Selections**.

2 Click **Advanced view**.

3 Click **Add**.

4 From the **General** tab in the **Backup Selection** dialog box, select the appropriate options as described in the following table.

Table 5-4 Backup Selection General Dialog Box

Item	Description
Name	Type a descriptive name for the backup selection.
Description	Type a clear description of the backup selection. This description may include, for example, the folder selected, the group of users it was created for, or the purpose for creating the backup selection.

Table 5-4 Backup Selection General Dialog Box (continued)

Item	Description
Folder to back up	
Type a folder name	Select this option to add a specific folder to the backup selection. Type the path to the folder, including the folder name. For example, to add a folder named MyData on drive C, type `C:\MyData`. **Note:** Once a backup selection is created, the folder cannot be modified.
Select a pre-defined folder	Select this option to choose a pre-defined folder from the list provided.
Include sub folders	Select this option to also back up all sub folders in the specified directory. This option is selected by default.

5 From the **Include/Exclude** tab, select the appropriate options as described in the following table.

Table 5-5 Backup Selection Include/Exclude Dialog Box

Item	Description
Include all file types	Select this option to include all file types in this backup selection.
Include and exclude only the items listed below	Select this option to include or exclude only specific files or file types.

6 To add a filter to the **Include/Exclude** list, verify that you selected **Include and exclude only the items listed below** in step 5, and click **Add Include** or **Add Exclude**.

7 If you selected **Add Exclude**, you will be notified that all previously backed up files matching this exclude will be deleted from this backup selection. Click **Yes** to continue or **No** to cancel.

8 Select the appropriate options as described in the following table.

Table 5-6 Add Include Filter or Add Exclude Filter Dialog Box Options

Item	Description
Filter	Type the name of the file or the folder, or a wildcard description of the file or folder that you want to include or exclude from backup selections. For example, type `*.mp3` to either include or exclude all files with the file extension .mp3 in this Backup selection, or type `unimportant.txt` to include or exclude all files in the backup selection with this specific file name. Click **Extensions** to select a predefined filter to either include or exclude all files with a given file extension.
Description	Type a description of this include or exclude filter.
Apply to	Select one of the following: ■ **Files** to apply this filter to file ■ **Folders** to apply this filter to folders ■ **Files and Folders** to apply this filter to both files and folders

9 Click **OK.**

10 From the **Revision Control** tab, select the appropriate options for both the Desktop and network user data folders as described in the following table. Table 5-7 describes the options.

Table 5-7 Backup Selection Revision Control Dialog Box

Item	Description
Number of Revisions	
desktop user data folder	Type the number of revisions to keep in the desktop user data folder for each file in the backup selection. **Note:** When Outlook PST files are backed up incrementally, only one revision is maintained regardless of the number of revisions set in the backup selection.

Table 5-7 Backup Selection Revision Control Dialog Box (continued)

Item	Description
Limit to	Select this option to limit the number of revisions retained in a given amount of time, and specify the following: ■ **Revisions**: Select the number of versions to retain. ■ **Within the last x hours:** Select the time period during which you want to retain the versions. ■ **At least x minutes apart:** Select the minimum amount of time that must elapse between backups in this backup selection. **Note:** The oldest revision is deleted when a new revision is created that exceeds one of these limits.
network user data folder	Select the number of revisions to keep in the network user data folder for each file in the backup selection.
Limit to	Select this option to limit the number of revisions retained in a given amount of time, and specify the following: ■ **Revisions:** Select the number of versions to retain. ■ **Within the last x hours:** Select the time period during which you want to retain the versions. ■ **At least x minutes apart:** Select the minimum amount of time that must elapse between backups in this backup selection. **Note:** The oldest revision is deleted when a new revision is created that exceeds one of these limits.
Revision Age	
Discard all revisions in the desktop user data folder older than	Enter the number of days after which all revisions in the desktop user data folder will be deleted. **Note:** The latest revision will not be discarded.
Discard all revisions in the network user data folder older than	Enter the number of days after which all revisions in the network user data folder will be deleted. **Note:** The latest revision will not be discarded.

11 From the **Options** tab, select the appropriate options as described in the following table.

Table 5-8 Backup Selection Options

Item	Description
Delta File Transfer	If you choose Delta File Transfer, each time a file is backed up, only the part of the file that has changed is transferred and stored in the network user data folder. In addition, Delta file transfer uses compression. Enabling this option requires that the DLO administrator has installed and configured a maintenance server.
Compression	When you select compression, each time a file is backed up, files in this backup selection will be compressed for data transfer over the network and for storage in the Desktop and network user data folders. This affects files created after this feature is activated. Previously stored files will not be compressed. Delta File Transfer also uses compression.
Encryption	Select this option to encrypt files for transfer and to store files from this backup selection in an encrypted format in the network user data folder. This affects files transmitted and stored after this feature is activated. Previously stored files will not be encrypted. The AES (Advanced Encryption Standard) and a 256 bit key length are used. If enabled, versions are stored without encryption in the desktop user data folder, and encrypted in the network user data folder. Transfer over the network is encrypted.
When source files are deleted, delete the backed up files from the	
desktop user data folder after	Indicate the number of days after which DLO will delete all file versions from the desktop user data folder after the source file has been deleted from the desktop. The default setting is 60 days.
network user data folder after	Indicate the number of days after which DLO will delete all file versions from the network user data folder after the source file has been deleted from the desktop. The default setting is 60 days.

12 Click **OK** to save your changes.

Modifying Backup Selections in the Advanced View

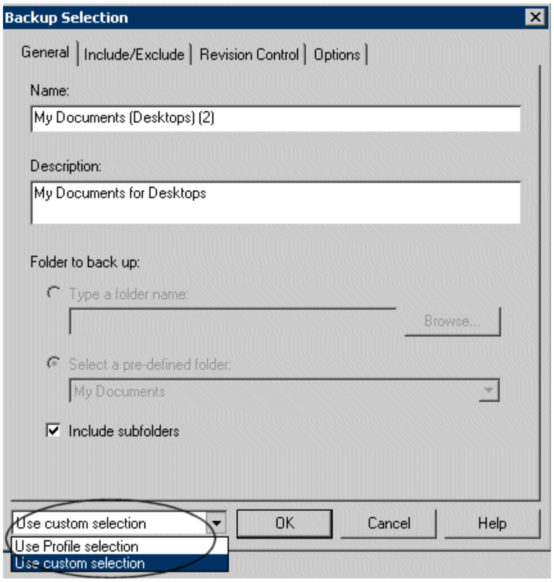
From the advanced view, backup selections created on the Desktop Agent and those created by the DLO administrator in the profile can be modified if the profile grants sufficient rights to the Desktop Agent user.

1 Under **Views** in the Desktop Agent Tasks bar, click **Backup Selections**.

2 Click **Advanced view**.

3 Select the backup selection you want to change, and then click **Modify**.

4 Profile backup selections are those set by the DLO administrator. If the backup selection is a profile backup selection, and if the user has been granted sufficient rights, it can be modified by selecting **Use custom selection** in the drop-down menu. Once this option is selected, your backup selection will no longer be updated when the administrator updates the profile backup selection.
You can return to the profile backup selection settings at any time by selecting **Use Profile selection** in the drop-down menu. Once you select this option, your profile will be updated if the DLO administrator modifies the profile backup selection.



Backup Selection

Name: My Documents (Desktops) (2)

Description: My Documents for Desktops

Folder to back up:

○ Type a folder name:

● Select a pre-defined folder: My Documents

☑ Include subfolders

Use custom selection

5 Modify the backup selection properties as needed. For detailed information on backup selection settings, review the instructions for setting up a backup selection beginning with step 4 on page 259.

6 Click **OK**.

Deleting Backup Selections in the Advanced View

When you delete a backup selection, the backup files are deleted after the number of days specified in the backup selection. See “Backup Selection Options” on page 263 for more information.

To delete a backup selection

1. Under **Views** in the Desktop Agent Tasks Bar, click **Backup Selections**.
2. Click **Advanced view**.
3. Select the backup selection you want to delete.
4. Click **Remove**.
5. Click **Yes** to verify that you want to delete this backup selection, or click **No** to cancel.

Backing up Outlook PST Files Incrementally

DLO is configured to back up PST files incrementally by default. Incremental backup of PST files is controlled by the administrator in the Profile, or by the desktop user in Options dialog if the desktop user has been granted sufficient rights.

Note: Outlook must be the default mail application to perform incremental backups of Outlook PST files.

The following limitations should be considered when backing up Outlook PST files incrementally:

- Some of the DLO options are not used, even if they are enabled. These options include Delta File Transfer, Compression, and Encryption.

  DLO relies on Microsoft's Messaging Application Programming Interface (MAPI) code to perform the actual backup of PST files. Using MAPI does not allow the use of these DLO options during an incremental backup.

  This is a limitation of the way the incremental backups are performed and is normal behavior for backups of Outlook `*.pst` files. This limitation only applies to incremental backups and does not apply to non-incremental PST backups.
- When Outlook PST files are backed up incrementally, only one revision is maintained regardless of the number of revisions set in the backup selection.
- When you restore Microsoft Outlook PST files, the restored PST file will differ from the original PST file as explained in Restoring Microsoft Outlook Personal Folder Files on page 289.
- Synchronized files cannot be backed up incrementally.

- When a DLO profile is configured to limit the bandwidth usage during data transfer to the network user data folder, bandwidth is not limited during the incremental transfer of PST files.

Related topics

"Setting Customized Options" on page 271

Setting outlook as the default email application

DLO is unable to perform incremental backups of Outlook PST files unless Outlook is your default mail application.

To specify outlook as your default mail application in your internet options

1. Open Internet Explorer.
2. On the **Tools** menu, click **Internet Options.**
3. Select the **Programs** tab.
4. Select **Microsoft Office Outlook** in the **email** list.

Note: If you do not intend to use Outlook as your default mail application, you can disable the warning message about incremental backups in the Desktop Agent by selecting **Settings** in the **Views** menu, and by clearing the **enable incremental backups of Outlook PST files** check box in the **Options** tab.

Pending PST files

When an Outlook PST file is included in a DLO backup selection, it will appear in the Desktop Agent pending queue whenever the PST file is closed. Because PST files are a shared resource, opening and closing of PST files is controlled by a process called MAPI. Both DLO and Outlook access PST files using the MAPI process. MAPI opens a PST upon request from the application. MAPI may or may not, depending on the version in use, close a PST in response to the following:

- An application such as DLO or Microsoft Outlook detaches from the PST, such as when Outlook is closed
- DLO startup
- After 30 minutes of inactivity in the PST

When the PST is closed DLO does one of the following. If the PST is being handled incrementally by MAPI (see section on incremental PST) DLO determines if the PST has been backed up in its entirety. If it has already been backed up then the entry is simply removed from the Desktop Agent pending queue because DLO knows the PST is in sync. If the PST is not being handled incrementally, the PST will be backed up in its entirety at this time.

Related topics

"Restoring Microsoft Outlook Personal Folder Files" on page 289

Backing up Lotus Notes NSF Files Incrementally

The following types of Lotus Notes NSF Files can be backed up incrementally.

Table 5-9 NSF Files That Can Be Backed Up Incrementally

File Name	Location	Description
BOOKMARK.NSF	Notes\Data directory	Contains saved bookmarks and Welcome Page information.
NAMES.NSF	Notes\Data directory	This file contains contacts, connections, locations and Personal Address Book information.
A_<name>.NSF		This is an e-mail archive file. E-mail must be archived to be incrementally backed up by DLO. See Lotus Notes documentation for more information on archiving e-mail.

When a file is backed up incrementally, there is no progress indicator in the Desktop Agent Status view, and only one revision is retained.

Note: When a DLO profile is configured to limit the bandwidth usage during data transfer to the network user data folder, bandwidth is not limited during the incremental transfer of Lotus Notes NSF files.

Lotus Notes must already be installed before the Desktop Agent is installed. If Lotus Notes is installed after the Desktop Agent, you must run the Desktop Agent installer again to repair the installation. Additionally, if Lotus Notes is open during the Desktop Agent installation, Lotus Notes must be restarted.

Lotus Notes email files can only be backed up incrementally with DLO if the e-mails have been archived. Once emails are archived, the resulting archive file can be backed up incrementally. See the Lotus Notes documentation for information on archiving e-mails.

To configure the Desktop Agent for incremental backup of Lotus Notes files

1 Verify that Lotus Notes was installed before the Desktop Agent was installed, or that the Desktop Agent installer was run again after Lotus Notes was installed to repair the installation.

2 Verify that emails to be backed up have been archived in Lotus Notes.

3 Verify that the Lotus Notes NSF files to be backed up have been selected in the appropriate backup selection. See "Using the Desktop Agent to Back up Your Data" on page 256 for more information on backup selections.

4 Under **Tools** in the Desktop Agent Tasks bar, click **Options.**

5 Select the **Options** tab.

6 Check **Enable message level incremental backups of Lotus Notes email files**.

7 Click **OK**.

Using the Desktop Agent when Lotus Notes is not Configured

When a user logs in to a computer that has both DLO and Lotus Notes installed, but that user is not yet configured in Lotus Notes, a debugging DOS-window may appear which contains the following errors:

```
<time_date_stamp> Created new log files as C:\Documents and
Settings\<user_name>\Local Settings\Application
Data\Lotus\Notes\Data\log.nsf.
<time_date_stamp> A previous process with the process ID <####> failed
to terminate properly.
```

The DOS-window cannot be closed without manually exiting the DLO process. If you configure the current user for Lotus Notes, the errors are no longer generated at login for that user.

Deleting Lotus Notes Email Files

If a Lotus Notes Email message is deleted before it is backed up by DLO, it will not be backed up.

Modifying Desktop Agent Settings

If the DLO administrator has set your profile so that you can view the complete Desktop Agent and modify settings, you can use the **Settings** view to modify the following:

- Backup job schedule options
- Desktop user data folder location
- Desktop user data folder disk space limits
- Log file disk space limits
- Logging level
- Bandwidth usage

The Desktop Agent will continue to use settings specified in the profile until you specifically elect to use customized schedules or options as described in “Changing Backup Job Schedule Options” on page 269 and “Setting Customized Options” on page 271.

You can change Desktop Agent settings and backup selections when you are working offline. The settings will be stored until you are once again working online, at which time they are automatically transferred. If the administrator has also made changes that conflict with the changes made on the Desktop Agent, the changes made by the administrator will be used.

Note: Changing settings on one Desktop Agent causes settings to be loaded on other Desktop Agents that use the same authentication. This will cancel and restart any running jobs.

Changing Backup Job Schedule Options

You can change backup job schedule options if the DLO administrator has set your profile so that you can view the complete Desktop Agent and modify settings.

To change backup schedule options

1. On the **Tasks** bar, under **Tools**, click **Options**.
2. Click the **Schedule** tab.
3. Select the appropriate options as described in the following table and then click **OK**.

Table 5-10 Job Schedule Options

Item	Description
Use Profile schedule	Select this option to use the scheduling options specified in the profile. **Note:** If this option is selected, additional settings on the **Schedule** tab cannot be modified.
Use custom schedule	Select this option to specify a customized schedule that differs from the profile schedule.

Table 5-10 Job Schedule Options (continued)

Item	Description
Run jobs:	
Whenever a file changes	Select this option to back up files automatically whenever they change. **Note:** Automatic backup whenever a file changes is available only for NTFS file systems. For FAT file systems, type a number of minutes or hours between backups in the **Back up changes files every** field.
According to a schedule	Select this option to back up files according to a schedule. The default is to run a backup at 11:00 P.M. every Monday, Tuesday, Wednesday, Thursday, and Friday. To change this default, click **Modify...**.
Manually	Select this option to run a backup only when you initiate it.
Logout/Restart/Shutdown options	
Do nothing	Select this option to proceed with a logout, restart or shutdown even when there are files that require backup. **Note:** If a job is already running, a prompt asks if the user would like to log out, restart or shut down when the job is complete.
Prompt user to run job	Select this option to display a prompt that asks if a backup should be run before proceeding with the logout, restart or shutdown. **Note:** If a job is already running, a prompt asks if the job should be cancelled in order to continue with the logout, restart or shutdown.
Run job immediately	Select this option to back up waiting files without prompting before proceeding with a logout, restart or shutdown. **Note:** If a job is already running, a prompt asks if the job should be cancelled in order to continue with the logout, restart or shutdown.

Table 5-10 Job Schedule Options (continued)

Item	Description
Run job as scheduled	Select this option to proceed with a logout, restart or shutdown and back up files according to the schedule. **Note:** If a job is already running, a prompt asks if the job should be cancelled in order to continue with the logout, restart or shutdown.
Run job at next login	Select this option to proceed with a logout, restart or shutdown without prompting, and run a job the at the next login. **Note:** If a job is already running, a prompt asks if the job should be cancelled in order to continue with the logout, restart or shutdown.

Setting Customized Options

You can change additional Desktop Agent settings, such as disk space used by the desktop user data folder, if the DLO administrator has set your profile so that you can view the complete Desktop Agent and modify settings.

To set customized options

1. On the **Tasks** bar, under **Tools**, click **Options**.
2. Click the **Options** tab.
3. Select **Use custom options** from the drop-down menu.
4. Select the appropriate options as described in the following table and then click **OK**.

Table 5-11 Options Dialog Box

Item	Description
Use Profile options	Select this option to use the scheduling options specified in the profile. **Note:** If this option is selected, additional settings on the **Schedule** tab cannot be modified.
Use customized options	Select this option to specify a customized schedule that differs from the profile schedule. **Note:** This option must be selected to enable access to additional settings on the **Options** tab.

Table 5-11 Options Dialog Box (continued)

Item	Description
Limit disk space usage on my computer to:	Select this option to limit the amount of space used on the computer to store backup files. **%** Select **%** to enter a percentage of the hard disk space that can be used to store backup files. **MB** Select **MB** to enter the maximum number of megabytes of disk space that can be used to store backup files.
Log file maintenance	
Keep log files for a minimum of (days)	Specify the minimum number of days to keep log files. Log files will not be deleted until they are at least as old as specified. **Note:** Log grooming occurs each time a log is created. Log files will not be deleted until the minimum age has been reached and, when the combined size of all log files, is also reached.
After minimum number of days, delete oldest log files when combined size exceeds	Enter the maximum combined size of all log files to be retained before the oldest log files are deleted. **Note:** You may have more than the specified number of MB of log files stored if none of the log files are as old as specified in the **Keep log files for a minimum of (days)** setting.
Logging options	
Log groom messages	Select this option to create logs for grooming operations.
Log information messages for backup	Select this option to create logs for all backup operations.
Log warning messages	Select this option to create logs for all operations that generate warnings.

Table 5-11 Options Dialog Box (continued)

Item	Description
Enable message level incremental backups of Outlook PST files	Select this option to enable incremental backups of Microsoft Outlook Personal Folder (PST) files. Incremental backups must be enabled to allow PST files to be backed up while they are open. If this option is not checked, PST files that are configured in Outlook will be fully backed up each time the PST file is saved, which generally occurs when Outlook is closed. For more information, see "Backing up Outlook PST Files Incrementally" on page 265.
Enable message level incremental backups of Lotus Notes email files	Select this check box to enable the configuration of DLO for incremental backup of certain Lotus Notes NSF files. Additional steps may be necessary to insure backup of these files. See "Backing up Lotus Notes NSF Files Incrementally" on page 267 for more information. To prevent the incremental backup of Lotus Notes files, clear this check box.

Moving the Desktop User Data Folder

You can change the location of the desktop user data folder if the DLO administrator has configured your profile so that you can view and modify the complete Desktop Agent and modify settings.

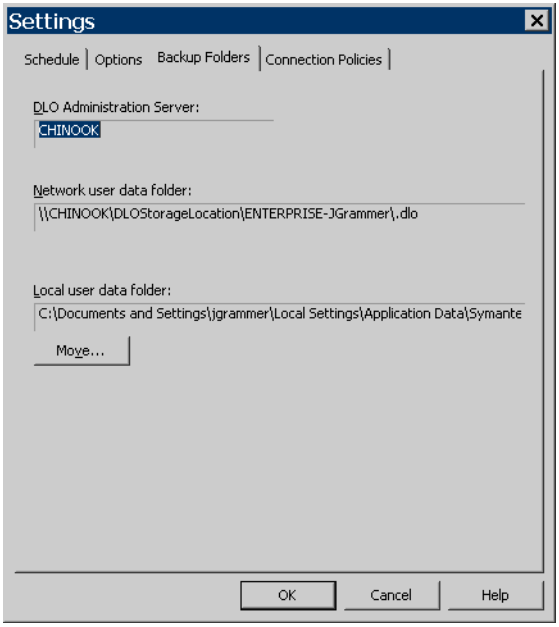
To move the desktop user data folder

1 In the **Tasks** bar, under **Tools**, click **Settings.**

2 Click the **Backup Folders** tab.

3 Click **Move**.

Figure 5-3 Settings



DLO Administration Server: CHINOOK

Network user data folder: \\CHINOOK\DLOStorageLocation\ENTERPRISE-JGrammer\.dlo

Local user data folder: C:\Documents and Settings\jgrammer\Local Settings\Application Data\Symante

4 In the **Browse for folder** dialog box, choose a new location for the desktop user data folder.

5 Click **OK**.

6 When prompted to continue, click **Yes**.

7 Click **OK**.

Customizing Connection Policies

The Desktop Agent can be configured to disable or limit backups for certain connection types. For example, if the DLO administrator has granted you sufficient rights, you can choose to disable backups when you are connected using a dialup connection, and continue backing up when you are connected to a higher speed connection.

When backups are limited by a connection policy, files are backed up to the desktop user data folder. Files are transferred to the network user data folder when connection policies are no longer limiting backups. If the desktop user data folder is disabled, no offline protection is provided.

When connection policies are created using Active Directory settings to define the policies, and two or more policies match a specific user or computer, the most restrictive policy is used.

Example:

One connection policy that matches a specific user or computer disables backups to the network user data folder of all files over 500 KB. A second connection policy that also matches the computer or user disables all backups to the network user data folder. The second policy will be used because it is more restrictive to limit all backups than just backups of large files.

To customize connection policies

1. Under **Tools** in the Desktop Agent Tasks bar, click **Settings**, and then click the **Connection Policies** tab.
2. Select the appropriate options as described in the following table and then click **OK** .

Table 5-12 Add/Edit Connection Policy

Item	Description
Connection Type	
Dialup	Select this option from the drop-down menu to limit or disable backups when using a dialup connection.
IP address range	Select this option to limit or disable backups for a specific IP address range. Specify whether you want the connection policy to apply to computers that **are** or **are not** in the IP address range you specify. Select IPv6 or IPv4 and enter the IP address range for the connection policy. **Note:** IPv6 addresses are only supported on Windows XP and later operating systems and will not be enforced for Desktop Agents running on Windows 2000. An additional connection policy using IPv4 addresses may be desired for Desktop Agents on Windows 2000 computers.
Active Directory	Select this option to limit or disable backups using Active Directory. Select Configure to configure the Active Directory settings. See step 3 on page 276 for details on configuring connection policy settings for Active Directory.
Desktop Agent Behavior	
Disable network backup	Select this option to prevent users from backing up to the network user data folder. Backups will continue to the desktop user data folder.

Table 5-12 Add/Edit Connection Policy

Item	Description
Disable network backup for files greater than	Select this option to prevent users from backing up files larger than a specified size based on the connection type. Enter a file size in KB.
Limit network bandwidth usage to	Select this option and enter a value in KB/sec to restrict the usage of network bandwidth to the specified value.
Enforce policy according to scheduled window	Select this check box to enable the connection policy to apply only during the specified period of time. Click **Schedule** to set the time during which the policy will be in affect. Schedules can be set to run weekly or for a specific date range.

3 If you selected Active Directory in step 2 above, configure the Active Directory settings as described in the following table and click **OK**.

Table 5-13 Active Directory Object Dialog

Item	Description
Object	Select the Active Directory Object you want to use to configure the connection policy. You can select either **Computer** or **User**.
In LDAP Directory	Type or browse to the LDAP directory.
All objects in this directory	Select this option to apply the connection policy to all objects in this directory.
Only the objects in this directory that match the criteria below	Select this option to apply the connection policy only to those objects in the directory that match the specified criteria.
Attributes	Select an attribute from the drop-down menu or type in a custom attribute.
Condition	Select the appropriate condition. Available options include =, <, <>, and >.
Value	Type a value to complete the criteria that will be used to determine matches. Wildcards can be used to specify the value.

4 Click **OK** to close the **Add/Edit Connection Policy** dialog.

5 Click **OK** to close the **Settings** dialog.

Synchronizing Desktop User Data

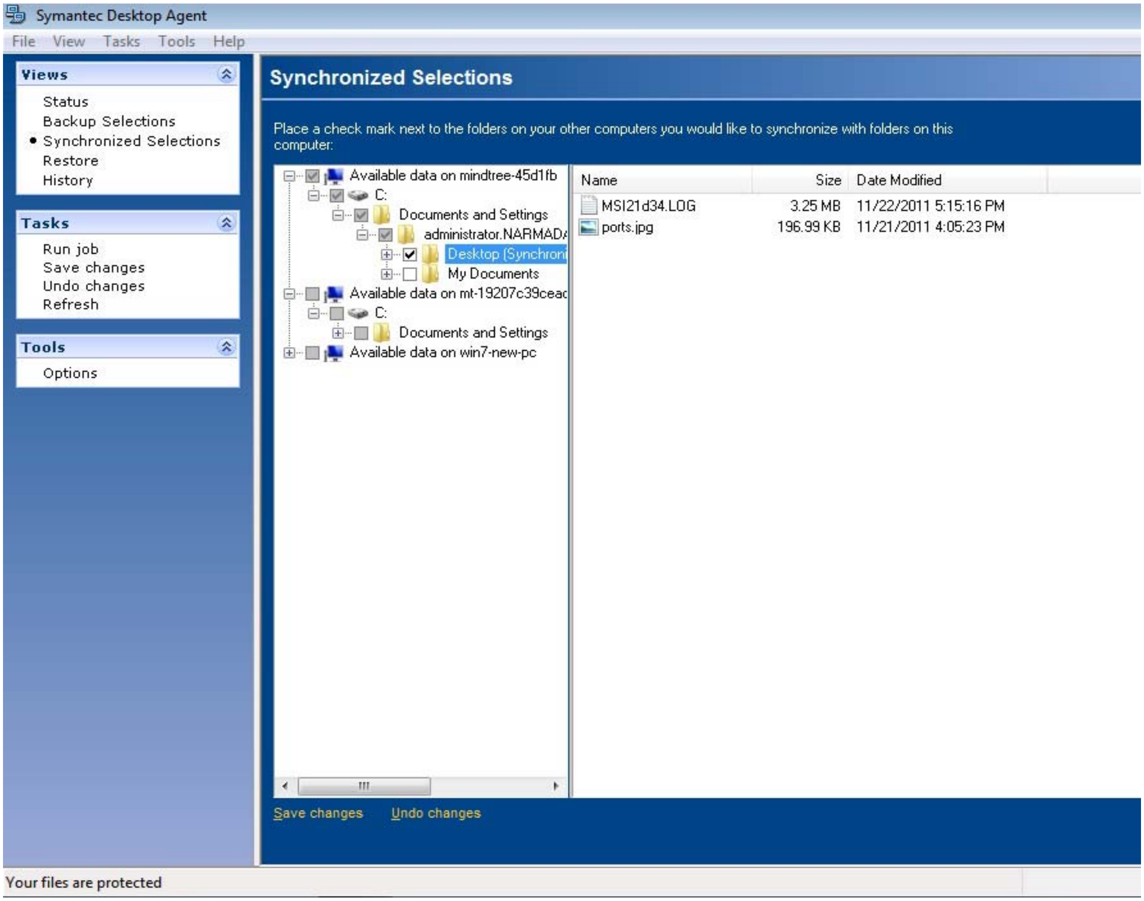
Your backed up data is stored in the desktop user data folder on the local drive of each desktop running the Desktop Agent, and in the network user data folder. If you have multiple desktops, your network user data folder contains copies of backed up files from each desktop. When a folder is synchronized using the Desktop Agent, only one copy of the folder and its contents is included in the network user data folder. When the file is changed on one desktop, it is stored in the desktop user data folder on that computer, and then uploaded to the network user data folder the next time a DLO job is run. It is then available for download to another synchronized desktop computer the next time that computer runs a job.

After a folder is synchronized, the Desktop Agent checks the network user data folder each time the desktop is connected to the network and a job is run. If new file versions are available in any of the synchronized folders, the Desktop Agent downloads the new version to the user data folder on the desktop. If you change a file on your current desktop and change the same file on one of your other backed up computers without synchronizing the files, a conflict will occur and you will be prompted to select which file revision to use.

By synchronizing backed-up data, you can work on a file on any of your desktops with the assurance that you are working on the most recent version.

The **Synchronized Selections** view displays folders backed up on your other desktops that are available for synchronization. Select any of these folders that you want to synchronize with the current desktop computer.

Figure 5-4 Synchronized selections view



Place a check mark next to the folders on your other computers you would like to synchronize with folders on this computer:

```
☑ Available data on mindtree-45d1fb
  ☑ C:
    ☑ Documents and Settings
      ☑ administrator.NARMAD/
        ☑ Desktop (Synchroni
        □ My Documents
□ Available data on mt-19207c39ceac
  □ C:
    □ Documents and Settings
□ Available data on win7-new-pc
```

Name	Size	Date Modified
MSI21d34.LOG	3.25 MB	11/22/2011 5:15:16 PM
ports.jpg	196.99 KB	11/21/2011 4:05:23 PM

Your files are protected

Note: If you customize NTFS permissions or folder attributes for compression or encryption, you must reapply these settings after restoration or synchronization.

How Synchronization Works

When a DLO job runs, DLO does the following to back up and synchronize files:

- Backs up files that changed on the desktop
- Makes synchronized files available to the other computers with which the desktop is synchronized

- Downloads synchronized files that were changed on another computer and uploaded since the last DLO job ran
- Retains all conflicting versions of files. You can then choose which version to use

When you back up files, you can set various filters, such as which types of files to include, exclude, compress or encrypt. When you synchronize files between computers, the filters are combined. For example, if one of the synchronized files is compressed and encrypted, all synchronized files will be compressed and encrypted automatically. If the original backup selection backed up only `.jpg` files, the synchronized file set will include only.jpg files.

If the settings for a synchronized folder are changed after the folder is synchronized, and the folder is later unsynchronized, the folder will revert to the original backup selection settings. For example, if the original backup selection backed up only `.jpg` files and the folder is later synchronized and set to back up all files, if the folder is then unsynchronized, it will once again backup only `.jpg` files.

If the number of files backed up on different computers varies, DLO synchronizes the largest number of files. For example, if you back up three files on computer A and back up five files on computer B, DLO synchronizes five files.

Synchronized selections are subject to limitation by global excludes in the same manner as backup selections. See "Configuring Global Exclude Filters" on page 134 for more information.

You can manage synchronization using the following options:

- **Standard view**: Enables you to create new synchronization sets
- **Advanced view:** Enables you to modify settings for each synchronization set

---

Note: To use the synchronization feature, all synchronized computers must be running the same version of the Desktop Agent and the clocks on all the user's computers must be synchronized.
In case you upgrade the Desktop Agent from a previous version, all previously synchronized backups will be displayed as normal backups. So, do the synchronization again.

To synchronize a folder across multiple desktops

1. Under **Views** in the Desktop Agent Tasks bar, click **Synchronized Selections**.
2. Click **Standard view**.
   Desktops available for synchronization appear in the **Remote Computers** pane.

Note: A desktop must have the same owner and must be backed up with the Desktop Agent to appear in the Synchronized Selections view. Only backed up folders are available for synchronization.

3 Select the folders that you want to synchronize.

4 When the **Choose Local Folder** dialog box appears, type or browse to the location where the synchronized files are to be stored.

5 Click **OK**.

6 Click **Save changes** to save the selections or **Undo changes** to return to the last saved settings.

To view or change a synchronized folder

1 Under **Views** in the Desktop Agent Tasks bar, click **Synchronized Selections**.

2 Select the **Advanced view** radio button.

3 Click the folder to be viewed or modified.

4 Click **Modify**.
The **General** tab in the **Synchronized Folder** dialog box identifies the location where synchronized files from this selection will be stored, and also lists other computers synchronizing with the selected folder.

5 Configure the synchronization folder settings as described for backup selection configuration, beginning with step 5 on page 260.

6 Click **OK**.

To remove a synchronized folder

Note: When a synchronized selection is deleted, the backup files are deleted in the same manner as when source files are deleted. They will be groomed away after the number of days specified in the backup selection.

1 Under **Views** in the Desktop Agent Tasks bar, click **Synchronized Selections**.

2 Click the **Advanced View** radio button.

3 Click the synchronization selection to be deleted.

4 Click **Remove**.

5 When prompted, if you want to delete the backup selection, click **Yes** to continue or **No** to cancel.

Resolving Conflicts with Synchronized Files

If a synchronized file is modified on more than one computer without updating the file with the Desktop Agent, a conflict will occur and you will be prompted to determine which file version to keep. For example, a conflict will occur if the same file is modified on both your desktop computer and your laptop and your laptop is disconnected from the network. When your laptop is subsequently connected to the network, the conflict will be detected.

To resolve a conflict with a synchronized file

1. Under **Views** in the Desktop Agent Tasks bar, click **Status**.
   If a conflict is identified, a **resolve conflicts** button will appear in the Status view.
2. Click the **Conflicts have been found** link to open the **Resolve Conflicts** wizard.
3. Review the information on synchronization conflicts and click **Next**.
4. Select the file you wish to resolve.
5. Click the **Open Folder** button.
6. Manage the revisions as required.
   For example, to keep an older revision, you can delete the newer revision and rename the conflicting revision back to it's original name.
7. Click **Finish**.

Viewing the Desktop Agent Status

The Desktop Agent Status view provides a summary of Desktop Agent operations that includes the items described in the following table.

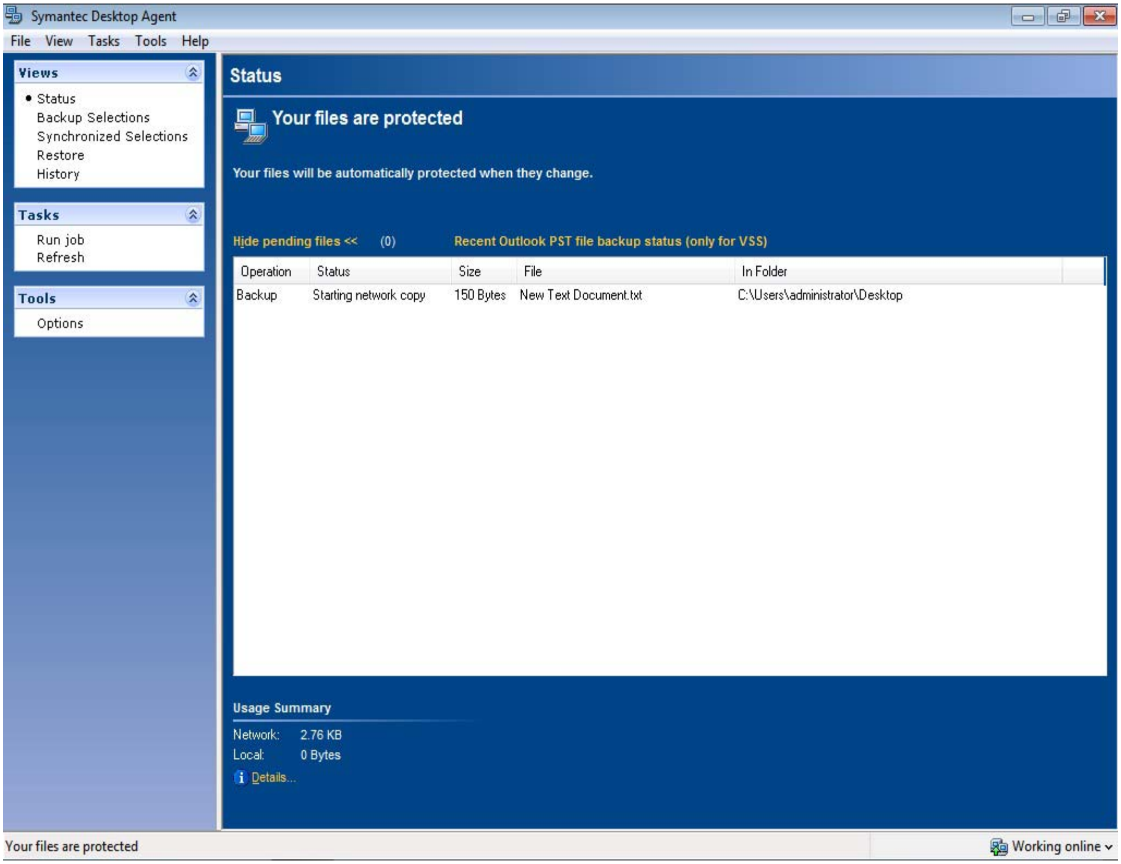
Desktop Agent Operations

Item	Description
Status	Displays the current state of Desktop Agent jobs, displays when backups will run, and summarizes the results of the last backup.
Details	This link is located just below the status summary if a backup selection has been made for a FAT drive. It provides scheduling details based on current Desktop Agent settings.
Show/Hide Pending Files	Hides or displays pending files. This selection toggles between **Hide pending files** and **Show pending files** when you click the link.
Usage Summary	

Desktop Agent Operations (continued)

Item	Description
Network Usage	Displays the total amount of data stored in the network user data folder for this computer.
Local Usage	Displays the total amount of data stored in the desktop user data folder on this computer.
Details	This link is located just below the status summary and provides detailed information on folder usage for user data. For more information, see "Viewing Usage Details" on page 283.

Figure 5-5 Desktop Agent status view



Your files are protected

Your files will be automatically protected when they change.

Hide pending files << (0)
Recent Outlook PST file backup status (only for VSS)

Operation	Status	Size	File	In Folder
Backup	Starting network copy	150 Bytes	New Text Document.txt	C:\Users\administrator\Desktop

Usage Summary

Network: 2.76 KB

Local: 0 Bytes

Starting a Pending Job in the Status View

To run a pending job from the status view

1. Under **Views** in the Desktop Agent Tasks bar, click **Status**.
2. Under **Tasks** in the Desktop Agent Tasks bar, click **Run job**.
   All pending jobs will be run, such as backup, synchronization or restore jobs.

Suspending or Cancelling a Job

If the DLO administrator has set your profile so that you can suspend and cancel jobs, you can do this by pressing the **Suspend** button. The available options depend on the type of job being suspended. When you click **Suspend**, a dialog opens specifying the options available.

Note: The DLO administrator sets the maximum time after which a suspended job will resume.

Table 5-14 Options for Suspending Jobs

Type of Job Running	Options
Continuous	■ Suspend the job and resume after a specified number of minutes
Manual	■ Suspend the job and resume after a specified number of minutes ■ Cancel the job until it is started again manually
Scheduled	■ Suspend the job and resume after a specified number of minutes ■ Cancel the job until it is scheduled to run again

Viewing Usage Details

The Desktop Agent Status view provides a summary of information on both local and network disk space used to store your data. Additional usage details and a grooming function are available in the Usage Details dialog:

- Total disk space currently used on the network and desktop computer to store your backup data
- Quotas, or maximum allowed storage space which can be used to store your data on the network and desktop computers

- The disk space available on the network and desktop computer for storing your data
- An option to immediately delete old revisions and deleted files
- Links to additional information and help

Note: The link to usage details is only available when the Desktop Agent is idle. It will not be shown when a job is running.

To view usage details and groom files

1. Under **Views** in the Desktop Agent Tasks bar, click **Status**.
2. Under **Usage Summary** in the Status pane, click **Details** to open the Usage Details dialog.
3. Review the usage information and take the appropriate actions as described in the following table.

Table 5-15 Usage Details

Item	Description
Usage	
Local	Summarizes disk space usage on the desktop computer for storing your data. The following information is provided: *Using*: The total disk space on the desktop computer currently being utilized to store your backup data. *Quota*: The maximum amount of disk space you can use to store your backup data on the desktop computer. The quota limit is set by the administrator in the profile, but can be modified from the Desktop Agent **Settings** view if you have been given rights to modify settings. For more information, see “Modifying Desktop Agent Settings” on page 268. *Available*: The amount of free disk space available on the desktop computer for storing your data without exceeding a quota. If there is no quota, the Desktop Agent will reserve a small amount of disk space so the drive will not fill completely with backup data.

Table 5-15 Usage Details (continued)

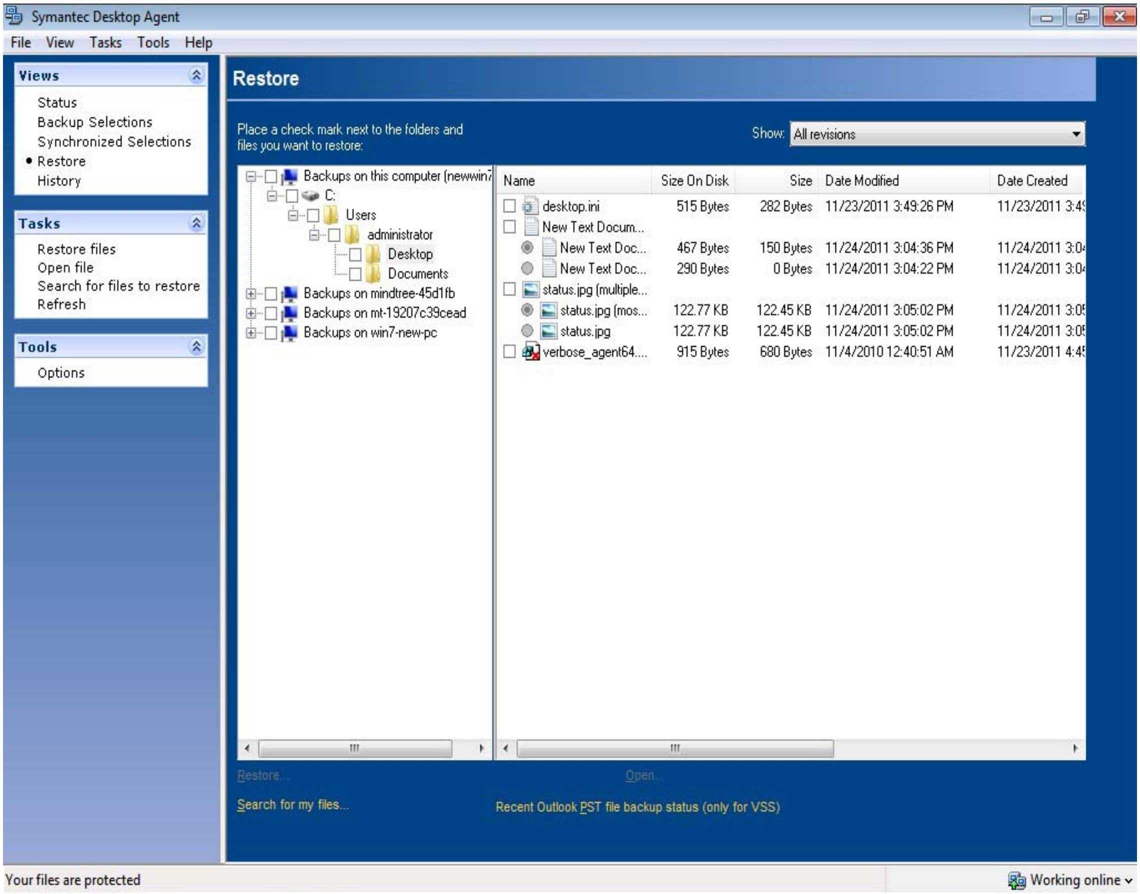
Item	Description
Network	Summarizes disk space usage on the network for storing your data. The following information is provided: *Using:* The total disk space on the network currently being utilized to store your backup data. *Quota*: The maximum amount of disk space you can use to store your backup data on the network. *Available*: The amount of free disk space available on the network for storing backup data for the current user without exceeding a quota.
Synchronized Files	Summarizes disk space usage for storing synchronized data. The following information is provided: *Using*: The total disk space on the network currently being utilized to store your synchronized data.
Remove deleted files	Select this option to immediately and permanently delete all files that are marked as deleted in your Network and desktop user data folders. The periodic maintenance cycle will otherwise delete these files after the amount of time specified in your assigned profile. Click this button to open the **Remove Deleted Files** dialog. Choose from the following options: ■ **Remove only the deleted files that currently meet the backup selection deleted files criteria** ■ **Remove all deleted files** Select the **Remove files from the network user data folder** check box to additionally groom deleted files from the network user data folder.
Additional information	
View last job log	Click the button to open the Log File Viewer. For more information on the log file viewer, see "Monitoring Job History in the Desktop Agent" on page 290.

Restoring Files Using the Desktop Agent

If the DLO administrator has set your profile to include restoring files, then you can use the Desktop Agent to restore files to the original or an alternate directory. If a Desktop Agent user has more than one desktop computer running DLO, files can be selected from all available backups on each of the user's desktops, but can only be restored to the current desktop computer.

For information on backing up and restoring Microsoft Outlook PST files, see "Backing up Outlook PST Files Incrementally" on page 265 and "Restoring Microsoft Outlook Personal Folder Files" on page 289.

Figure 5-6 Restore view



Place a check mark next to the folders and files you want to restore:

Show: All revisions

Name	Size On Disk	Size	Date Modified	Date Created
□ desktop.ini	515 Bytes	282 Bytes	11/23/2011 3:49:26 PM	11/23/2011 3:4
□ New Text Docum...				
● New Text Doc...	467 Bytes	150 Bytes	11/24/2011 3:04:36 PM	11/24/2011 3:0
○ New Text Doc...	290 Bytes	0 Bytes	11/24/2011 3:04:22 PM	11/24/2011 3:0
□ status.jpg (multiple...				
● status.jpg (mos...	122.77 KB	122.45 KB	11/24/2011 3:05:02 PM	11/24/2011 3:0
○ status.jpg	122.77 KB	122.45 KB	11/24/2011 3:05:02 PM	11/24/2011 3:0
□ verbose_agent64....	915 Bytes	680 Bytes	11/4/2010 12:40:51 AM	11/23/2011 4:4

If you customize NTFS permissions or directory attributes, such as compression or encryption for files or folders, you must reapply these settings after restoration.

If you disconnect from the network while the Desktop Agent is running, you may encounter a slow response when browsing the Restore view. From the **Tasks** menu, select **Refresh** to fix this problem.

Note: DLO can overwrite a file which is in use by staging the file to be restored when the computer restarts. Using this feature requires administrative rights on the Desktop Agent computer. Alternatively, the file can be restored by first closing the application which is using the file, or by restoring the file to an alternate location.

To restore data

1 Under **Views** in the Desktop Agent Tasks bar, click **Restore**.

2 In **Show**, select one of the following revision display options.

Table 5-16 Restore File Version Display Options

Item	Description
All revisions	All file revisions will be displayed and available as restore selections.
Latest revision	Only the latest file revision will be displayed and available as a restore selection.
Revisions modified on or after	If selected, enter a date and time after which revisions will be displayed and available as restore selections, then click **OK**.

3 Select the items you want to restore.
In some cases the Restore Search view may contain duplicate entries for the same file. If this occurs, you can select either file to restore and receive the same outcome.

Note: When you delete a file, the backup files are retained until they are deleted by the file grooming process. If an original file has been deleted, but backup files are still available, the icon for the file in the restore view will have a red ‘x’ to indicate the deletion of the original file. See “File Grooming” on page 257 for more information.

4 Click **Restore**.

5 Select the appropriate options as described in the following table and then click **OK**.

Table 5-17 Restore Dialog Box Options

Item	Description
Restore to the original folders on this computer	Select this option to restore files and folders to their original location.
Redirect the restore to an alternate folder on this computer	Select this option to restore files and folders to an alternate folder on the same computer.
Preserve folder structure	Select this option to restore the data with its original directory structure. If you clear this option, all data (including the data in subdirectories) is restored to the path you specify.
Options	
If file already exists	Select one of the following: ■ Do not overwrite ■ Prompt ■ Overwrite
Restore deleted files	Select this option if you want to restore files even though the source file has been deleted.
Preserve security attributes on restored files	Select **Preserve security attributes on restored files** to preserve security information in restored files. You may need to clear this check box to successfully restore a file if the source file security conflicts with the destination security. If you do not select this check box, then the security information is removed from the restored file.

Searching for desktop files to restore

To search for desktop files and folders to restore

1 Under **Views** in the Desktop Agent Tasks bar, click **Restore**.

2 Click **Search for files to restore** under **Tasks** in the Desktop Agent Tasks bar to open the **Search** dialog box.

3 Select the appropriate options as described in the following table and then click **OK**.

Table 5-18 Search Dialog Box Options

Item	Description
Search for file names with this text in the file name	Type all or part of the file name or folder you want to find.
Modified	Select this option to search for files that were modified during a specific time frame. Then specify the time frame.
Today	Select this option to search for files modified on the current calendar day.
Within the past week	Select this option to search for files modified in the last calendar week.
Between	Select this option to search between calendar dates.
Of the following type	Select this check box to select a file type from the list provided.
Of the following size	Select this check box and then enter information as follows: ■ Select from **equal to**, **at least** or **at most** in the first drop-down menu ■ Type a file size ■ Select **KB**, **MB,** or **GB**

Restoring Microsoft Outlook Personal Folder Files

When you restore Microsoft Outlook Personal Folder (PST) files, the following differences will exist between the restored PST and the original PST:

- The file size will be different
- Any rule that points to a folder inside a PST file will no longer work. You must edit the rule to point to the correct folder
- Restored `PST` files will have Inbox, Outbox, and Sent Items folders, even if the original files did not have them
- If you use a password for your PST file, you must reset the password after restoring your PST file

Related topics

"Backing up Outlook PST Files Incrementally" on page 265

Restoring Deleted E-mail Messages

The default behavior when deleting a message from a mail archive may differ depending on the mail application. With Lotus Notes, there is a “soft delete” feature that allows a message to be maintained in a special folder, the “Trash,” for a measured interval (default is 48-hours). After that, the message is permanently deleted. Outlook behaves in much the same manner. Deleted messages are moved to the “Deleted Items” folder but there is no time limit associated with this action. Outlook will permanently delete a message when the user empties the Deleted Items folder.

In either case, the Desktop Agent will replicate the delete during the next backup operation. In the event a user accidentally deletes a message from a mail archive, they will need to recover that file from the appropriate folder assuming the file has not been permanently deleted by the mail application. Because there are no versions maintained for e-mail archives, permanently deleted messages will be unavailable after the time limit has expired or the user has manually emptied the folder.

Restoring Files with Alternate Stream Data

DLO protects all of the alternate streams for a file, including security streams. If a new version of a file contains only changes to alternate stream data, the file replaces the previous version and does not impact the revision count. Only revisions with actual data changes are treated as new revisions.

FAT partitions do not use alternate data streams. If a file is restored from an NTFS partition to a FAT partition, the alternate steam data will not be included in the restored file.

When a file is restored, one of the options is to preserve the security attributes on restored files. If this option is not checked, the security attributes are removed from the restored file. This option is set in the restore dialog box. See “Restore Dialog Box Options” on page 288 for more information.

Monitoring Job History in the Desktop Agent

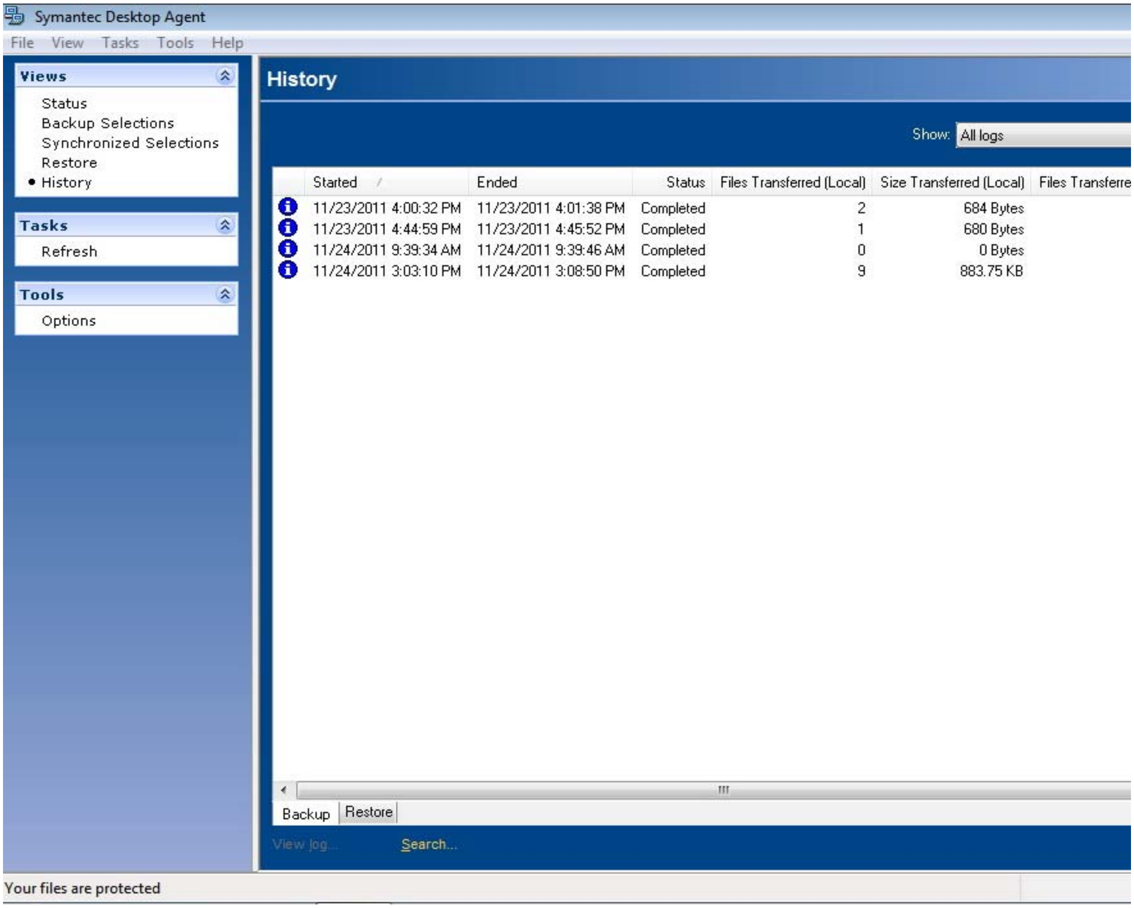
When a backup, restore, or synchronization operation takes place, details of that operation are stored in log files. Log files can be viewed, searched and saved as text files. The History View summarizes the following information and provides access to the full logs.

You can choose to view the backup history or restore history by selecting the appropriate tab at the bottom of the History window.

Table 5-19 Job History View Information

Item	Description
Started	The date and time the operation started.
Ended	The date and time the operation ended.
Status	The status of the job, such as Active, Completed, Cancelled or Failed.
Files Transferred (Local)	The total number of files transferred to the desktop user data folder during the listed job.
Size Transferred (Local)	The total number of bytes of data transferred to the desktop user data folder during the listed job.
Files Transferred (Network)	The total number of files transferred to the network user data folder during the listed job. This information is only available for the backup history, not the restore history.
Size Transferred (Network)	The total number of bytes of data transferred to the network user data folder during the listed job. This information is only available for the backup history, not the restore history.
Errors	The number of files that failed to copy and produced errors.

Figure 5-7 History view



Show: All logs

	Started	Ended	Status	Files Transferred (Local)	Size Transferred (Local)	Files Transferre
ℹ	11/23/2011 4:00:32 PM	11/23/2011 4:01:38 PM	Completed	2	684 Bytes	
ℹ	11/23/2011 4:44:59 PM	11/23/2011 4:45:52 PM	Completed	1	680 Bytes	
ℹ	11/24/2011 9:39:34 AM	11/24/2011 9:39:46 AM	Completed	0	0 Bytes	
ℹ	11/24/2011 3:03:10 PM	11/24/2011 3:08:50 PM	Completed	9	883.75 KB	

Your files are protected

Viewing Log Files

To view history logs

1 Under **Views** in the Desktop Agent Tasks bar, click **History**.

2 To view backup logs, select the **Backup** tab, or to view restore logs, select the **Restore** tab.

3 Select the appropriate History view filter option from the **Show** drop-down menu:

- **All logs:** All history logs are displayed.

- **All logs with errors:** History logs for all jobs that generated errors are displayed.
- **Logs filtered by date:** All logs generated after a specified date and time are displayed. Enter the date and time after which logs are to be displayed in the **Filter by date** dialog box and click **OK.**

4 Click the job history entry for which you want to view the history log.

5 To open the log file viewer, click **View Log**.

6 If required, click **Save As** to save the log file as a text file.

7 To exit the log file viewer, click **Close**.

Searching for Log Files

The Log File Viewer has a powerful search mechanism to help you locate the log files you want to view.

To search for log files

1 Under **Views** in the Desktop Agent Tasks bar, click **History**.

2 In the **History** pane, click the **Search** link, to open the Log File Viewer.

3 Enter filtering parameters as described in the following table.

Table 5-20 Log File Viewer Filtering Options

Item	Description
Search for log entries in	
All log files	Select this option to show all log entries in the log file viewer.
Current log file	Select this option to search only those log entries in the current log file.
With timestamp of	Select this check box to search only those log entries within a specified time period. The options include: *Today*: Show only log files that were created today. *Within the last week:* Show all log files created in the last week. *Between dates*: Show all log files created between the dates entered.

Table 5-20 Log File Viewer Filtering Options (continued)

Item	Description
Of the following type	Select this check box to show only logs of the indicated type. You may select one of the following types: ■ Backup ■ Restore ■ Move User ■ Maintenance ■ Error ■ Warning
With Filenames containing	Select this check box and enter a filename, or file type. Wildcard entries are supported. Example: *gold.doc **Note:** When using wild cards, you must use the '*' wildcard. For example, *.tmp will return all results with the .tmp extension while .tmp will return only files explicitly named .tmp.
Filter	
Informational entries only	Select this option to display only informational entries.
Error and warning entries only	Select this option to display both error and warning entries.
Error entries only	Select this option to display only error entries.
Warning entries only	Select this option to display only entries for warnings.

4 Click **Search**.

5 To view detailed information for a log file entry, expand the tree view for the entry and click the '+' check box.

6 If required, click **Save As** to save the log file as a text file.

7 Click **Close** when finished.

Log File Grooming

Log grooming occurs each time a log is created. Log files are not deleted until they have reached both the minimum age and maximum combined size of all log files settings. If the administrator has granted you sufficient rights in your profile, you can modify these settings in the Desktop Agent settings Options tab as described in "Setting Customized Options" on page 271.

Agent Repair Installation Scenarios

The Desktop Agent repair installation is required in the following scenarios.

If the repair installation is not done, the Outlook PST file backup will not work. The Desktop Agent repair installation ensures that compatible versions (x86 or x64) of the Desktop Agent binaries are installed and the Desktop Agent works as expected.

Note: The user should have local administrator privileges or should log in with domain administrator credentials to be able to perform the Agent repair installation.

Complete the repair installation for the following situations:

Table 5-21 Agent repair scenarios

Scenario	Solution
A Desktop Agent computer is running with no mail client and Outlook 2010 (x64) is installed later.	For all these scenarios, and depending on the availability of VS 2005 SP1 x64 redistributable, an error message is displayed: "*Install VS2005 SP1 x64 redistributable and perform the Agent repair again. If this does not solve the issue, please contact your DLO administrator.*" For all these scenarios, and depending on the availability of VS 2010 SP1 x64 redistributable, an error message is displayed: "*Install VS2010 SP1 x64 redistributable and perform the Agent repair again. If this does not solve the issue, please contact your DLO administrator.*"
Outlook 2010 (x86) is uninstalled and Outlook 2010 (x64) is installed on an existing Desktop Agent computer.	
Outlook 2003/2007 is uninstalled and Outlook 2010 (x64) is installed on an existing Desktop Agent Computer.	
Outlook 2010 (x64) and the Lotus Notes mail client co-exist and Outlook 2010 (x64) is uninstalled by making the Lotus Notes client the default mail client.	
The Lotus Notes mail client exists as the default mail client and Outlook 2010 (x64) is used. Lotus Notes is uninstalled and Outlook 2010 (x64) is set as the default mail client.	

Table 5-21 Agent repair scenarios

Scenario	Solution
Outlook 2010 (x64) is uninstalled and Outlook 2010(x86) is installed on an existing Desktop Agent computer.	For all these scenarios, and depending on the availability of VS2005 SP1 x86 redistributable, an error message is displayed: *“Install VS2005 SP1 x86 redistributable and perform the Agent repair again. If this does not resolve the issue, please contact your DLO administrator.”* For all these scenarios, and depending on the availability of VS2010 SP1 x86 redistributable, an error message is displayed: *“Install VS2010 SP1 x86 redistributable and perform the Agent repair again. If this does not resolve the issue, please contact your DLO administrator.”*
Outlook 2010 (x64) is uninstalled on an existing Desktop Agent computer.	
On an existing Desktop Agent computer, Outlook 2010 (x64) and the Lotus Notes mail client co-exist and the default mail client is toggled between Outlook 2010 (x64) and Lotus Notes.	
Outlook 2010 (x64) is uninstalled and Outlook 2003/2007 is installed on an existing Desktop Agent Computer.	

Troubleshooting

This section contains the following topics:

Using DLO with other Products

The following are known compatibility issues.

Symantec Storage Exec

Symantec Storage Exec is a policy-based storage resource manager for controlling file and application disk usage in Microsoft Windows environments. DLO and Storage Exec are compatible, but care must be taken to avoid conflicts between DLO backup selections and Storage Exec policies. If DLO is configured to back up a specific file type and Storage Exec is set to prevent this file type from being copied to the server, a conflict will result. DLO will attempt to back up the file, but the operation will fail. The DLO history log will indicate that the file failed to copy to the network user data folder.

To prevent this conflict, DLO backup selections and Storage Exec policies must be reviewed to identify any potential conflicts. If a conflict is found, the policies must be manually revised to eliminate the conflict.

WinCVS

When DLO runs concurrently with WinCVS, permission denied errors are sometimes generated when checking out source. This error can be avoided by excluding any directories named cvs using global excludes or backup selection excludes.

Windows XP Service Pack 2

If you are using Windows XP with Service Pack 2 you must enable file sharing to use the Browse button in the DLO Administration Console Restore view.

Troubleshooting the DLO Administration Console

This topic contains frequently asked questions that you may encounter while running the DLO Administration Console, and provides answers for these questions.

I modified an Automated User Assignment, but the change isn't reflected for existing Desktop Agent users.

Automated User Assignments are only used once to assign a profile and Storage Location to a new Desktop Agent user. An Automated User Assignment can be modified to change the profile and Storage Location settings, but these changes will only apply to new users. Users that have already been configured will not be affected by subsequent changes in the Automated User Assignment.

This also applies to existing users who install the Desktop Agent on another desktop. The new installation will use the existing user settings and will store data in the user's existing user data folder. Automated User Assignment changes will not affect an existing user, even if the Desktop Agent installation is on a new computer.

Settings for an existing desktop user can be changed by modifying the profile to which the user is assigned, or by reassigning that user to a new profile or Storage Location.

Related topics

"Modifying Desktop Agent User Properties" on page 152

"Managing Desktop Agent Users" on page 149

"About Automated User Assignments" on page 129

"About DLO Profiles" on page 84

"Moving Desktop Agent Users to a New Network User Data Folder" on page 154

A desktop user ran the Desktop Agent and received an error indicating "Unable to configure the Desktop Agent. No settings found for the current user and no automatic user assignments match." What does this indicate?

This message means that DLO could not find the user or an Automated User Assignment that matched the user's domain and group.

Users are added to DLO either by an Automated User Assignment or by manually adding them.

In the first case, you use an Automated User Assignment that matches the user's domain and group. The Automated User Assignment assigns a profile and Storage Location to the Desktop Agent and adds the user to DLO. Check that you have created Automated User Assignments that match the domain and group to which the user belongs who is running the Desktop Agent.

You can also create an Automated User Assignment that covers all domains and all groups. This method catches any users who might not match a more specific Automated User Assignment. Such a "catchall" Automated User Assignment would typically be set to the lowest priority.

The other option is to manually add users to DLO. This process requires that you assign a profile and assign either a Storage Location or a user data folder to the new user.

Before running the Desktop Agent, be sure that the user has a matching Automated User Assignment, or is added manually.

Related topics

"About Automated User Assignments" on page 129

When do I need a network user data folder, and when do I need a Storage Location?

Every Desktop Agent user must have a network user data folder, which is used to store backup data. Storage Locations are locations on the network where network user data folders are automatically created and maintained. They are not required if existing network shares are used to store user data.

If you want DLO to automatically create network user data folders, use a Storage Location. When new users are added to a Storage Location, network user data folders are automatically created for them within the Storage Location.

Alternatively, if you would like to use existing network shares as network user data folders, or if you want to create network user data folders manually, then do not use Storage Locations.

Related topics

"Configuring DLO" on page 72

I'm trying to create a Storage Location on a remote file server, and I am receiving an error indicating the MSDE Database Instance for the Desktop and Laptop Option needs to have access to the remote file server. What do I need to do?

To create Storage Locations on a remote file server, you must use an account that has administrative rights on the remote file server. For details about creating the Storage Location, see "Changing DLO Service Credentials" on page 37.

I manually added a new user and assigned the user to an existing Storage Location. I don't see a new user data folder for the new user in this Storage Location. Isn't it supposed to create one?

User data folders are created only after the Desktop Agent is both installed on the desktop and run by the new user.

How do I prevent a user from backing up data?

1 On the Navigation bar, click **Setup**. In the **Settings** pane, click **Users**.

2 Select the user you do not want to be able to perform backups.

3 Under **General Tasks** in the **Task** pane, select **Properties**.

4 Clear the **Enable user** check box.

5 Select **OK**.

The user's status will display as `Disabled`.

In a backup selection, I selected to encrypt or compress my user's data. However, data that has already been backed up is not encrypted or compressed. Why is this?

DLO does not retroactively apply changes to encryption and compression settings to user data that is already backed up. Any data backed up after these settings have changed will use the new settings.

I would like to prevent files of specific types from being backed up. How can I set up DLO to always exclude files like *.mp3 or *.gho?

On the **Tools** menu, select **Global Excludes**. In this dialog box, you can add specific file types that will be excluded in all backup selections for all profiles.

Backups do not seem to be running for all users, or specific files are not being backed up.

If backup jobs are not running for a group of users, check the profile for these users to verify that backups are scheduled.

If specific files are not being backed up, review the backup selections in the profile to verify that the files are selected for backup.

I just tried to restore a file, but it doesn’t appear to have been restored.

When restoring existing files to their original location, verify that you have selected **Prompt** or **Overwrite** in the **Restore** dialog box to replace the file. If you select **Do not overwrite**, the file will not be restored.

In a profile, I configured backup selections to encrypt files. Now I need to recover files for a user. Do I need an encryption key to restore this data?

As an Administrator running the DLO Administration Console, you can redirect a restore of encrypted user data to an alternate computer or location, and it will be decrypted during the restore.

I would like to restore data to a user's computer, but that user is out of the office. Do I have to wait until that user returns to the office before I can start the restore?

DLO can queue restore jobs to desktops. If the user is offline now, you can queue a restore job through the **Restore** view in the DLO Administration Console.

Another option is to restore the data to an alternate location, such as the administration computer or a network drive.

How can I protect open files?

DLO does not protect open files. It will attempt to back up files when they are closed or saved. If a file cannot be backed up because it is open (for example, a Word document you are editing) it will remain in the Desktop Agent's pending list. The Desktop Agent will attempt to back up the file at the next backup time. This also means that certain files opened by the operating system will not be backed up, they never close when the operating system is running. The exception to this is protection of open PST files. The Desktop Agent is designed to protect open PST files if they are part of the profile or user's backup selections. Incremental backups must be enabled for open file backups of PST files.

See “Excluding Files that are Always Open” on page 141 for more information.

The History view in the DLO Administration Console doesn't show the most recent backup for all users.

The DLO Administration Console is automatically updated when a job runs, but not more than once per hour.

I am not able to run either the -emergencyrestore, -migrateuser, or the -migrateSL command.

The error occurs because these commands should be run with a user account that has administrator privileges.

If the user account does not have administrator privileges, then open the command prompt by selecting the "*Run as Administrator*" option, and then run the specific command.

When I am clustering DLO Admin Service using domain user account, which is part of "Domain Admin" group, the following error message is displayed: "*This software will not run on a machine that is not part of cluster.*"

To resolve this issue, make sure that all the required rights/privileges are provided to this user account or group. Also this user account should be local administrator on all computers that are part of MSCS cluster or failover clustering.

For more information on configuring a user account for failover cluster, refer to the link: http://technet.microsoft.com/en-us/library/cc731002%28WS.10%29.aspx

After installing DLO 7.5, when I migrate the DLO server from one domain to another domain, I am unable to launch the DLO Administration Console.

SQL Server 2008 R2 that is shipped with DLO 7.5 does not support migration from one domain to another domain.

When a BE 2012 or BE 2012 R2 product co-exists on the machine where DLO 7.5 is installed, and when I try to launch the report from the DLO 7.5 Administration Console, a .rdl error occurs and the report does not launch.

To resolve this issue, the `DLORegKeySettingForReportU.exe` must be run, which is now available with DLO 7.5.

In a standalone setup, do the following:

Navigate to the product install path (example: `C:\Program Files\Symantec\Symantec DLO`) and run the `DLORegKeySettingForReportU.exe`. This tool resolves the .rdl error and you can launch the reports.

In a distributed environment setup, do the following:

On the DLO server machine, navigate to the path where DLO Administration service is installed (example: `C:\Program Files\Symantec\Symantec DLO`), and run the `DLORegKeySettingForReportU.exe.` This tool resolves the .rdl error and you can launch the reports.

Troubleshooting the Desktop Agent

This topic contains frequently asked questions that you may encounter while running the Desktop Agent, and provides answers for these questions.

I installed the Desktop Laptop Option, but I do not know how to install the Desktop Agent on users' computers.

The Desktop Agent can be installed by running the installation program from the share where DLO is installed as described below.

The Desktop Agent installation program is located in a share where you installed DLO. This share will have a name in the following format: `\\<Server>\DLOAgent`.

Using Windows Explorer, browse to this share from the desktop that you want to protect with the Desktop Agent. Run `Setup.exe` from this share. You must be an administrator on the desktop to install the Desktop Agent software.

Symantec recommends that DLO administrators run the Configuration Wizard to familiarize themselves with the application.

You can also install the Desktop Agent by using the "Push Install Desktop Agent" option. See "Procedure to Push Install Desktop Agent and DLO Maintenance Server" on page 32 for more information.

Can I install the Desktop Agent on Windows Servers or DLO Administration Servers?

Because the Desktop Agent is designed to protect user data rather than critical server data, it cannot be installed on Windows Servers or DLO Administration Servers.

I am receiving the following error while authenticating through the Desktop Agent to the DLO Administration Server: "Failed to Initialize database. 0x800A0E7D"

You attempted to connect to the DLO Administration Server with an account that is not in the same domain, or a trusted domain, as the administration server. For DLO to function properly, the DLO Administration Server must be in a Windows Domain.

I have a desktop and a laptop computer protected by the Desktop Agent. Why can't I move my laptop to a new Storage Location?

When a user has multiple computers running the Desktop Agent, all backup data is stored in the same network user data folder. If you want to move your data to a new Storage Location, you must move the entire network user data folder for all of your computers to that new location.

I am trying to synchronize files between my desktop and laptop computers, but I cannot see my other computer in the Synchronization View in the Desktop Agent.

To synchronize data between two computers, the same user account must be used when running the Desktop Agent on each computer. For example, the user `Domain\MyUser` must have backed up data on Computer A and Computer B in order for synchronization to take place between these two computers.

If you are sure you have backed up data while running the Desktop Agent under the same user account on both of your computers, select **Refresh** in the Desktop Agent's Synchronization View to make the synchronization selections available. If this is not successful, **Exit** from the File menu and restart the Desktop Agent application.

What files or folders can I synchronize between my computers?

Any data backed up by a backup selection are eligible for synchronization. These backup selections may be defined by the DLO Administrator in the profile or in a backup selection created with the Desktop Agent.

I would like to share my synchronized data with my co-workers. How can I do this?

DLO does not provide functionality for sharing files between users. Synchronization is designed to share files between a single user's computers.

DLO backup of Outlook PST files is slow during “Copying local” phase of the backup job.

When DLO performs a backup of an Outlook PST file, DLO copies the snapshot of the PST to the Local User Data Folder (LUDF), and then it copies the file to the Network User Data Folder (NUDF). During the first stage, the “Status” column in the Desktop Agent window displays the status as “Copying *local (x%)*”. Sometimes, this “*Copying local*” phase can be very slow.

To find out if DLO is introducing a sleep mechanism, enable DLO Agent logging and capture the slow backup job in the log.

Cause:

The “Copying local” phase can be slow due to one of the following reasons:

- The PST file is very large. The snapshot still occurs on the entire PST file, even if it is only doing a “Message level incremental”.
- The local AntiVirus application may be slowing down the process. Try disabling AntiVirus and observe the performance of the next backup job.
- DLO may be doing disk throttling. DLO monitors the LogicalDisk Performance Counter called “`Current Disk Queue Length`”. If the queue length exceeds 2 (default value of 2), DLO introduces a sleep mechanism during the “Copying local” phase of the backup jobs. This is to prevent DLO from consuming disk cycles that other applications might need.

To enable Desktop Agent Logging:

1. Launch the Desktop Agent GUI.
2. Select **Tools > Support > Enable Verbose Logging.**
3. Restart the Desktop Agent.

Once a slow backup has been captured, locate the newly created `DLOClient.log` file:

The `DLOClient.log` will be located here:

On Windows 7: `C:\Users\<UserName>\AppData\Local\Symantec\DLO\.settings`

On XP: `C: \Documents and Settings \<UserName> \Local Settings \Application Data\Symantec\DLO\.settings`

Example:

In the log file, look for lines such as:

diskthrottle.cpp(228) Read queue: 8.73956, sleeping for 2000ms

diskthrottle.cpp(228) Read queue: 4.50836, sleeping for 1254ms

diskthrottle.cpp(228) Read queue: 11.5639, sleeping for 2000ms

diskthrottle.cpp(228) Read queue: 3.54665, sleeping for 773ms

diskthrottle.cpp(228) Read queue: 2.85208, sleeping for 426ms

In the above example, it can be observed that DLO is introducing a sleep mechanism to prevent over-throttling of the physical disk.

The average of the sum of the queue length above is 6.625. Rounding up = 7.

If logs suggest the performance delays are associated with disk throttling (as seen above) and you have determined that it is alright for DLO to consume additional disk resources, these registry adjustments will increase the threshold at which DLO engages disk throttling:

Note: DLO will divide the specified registry value by 10, so take the observed average queue length and multiply by 10 to determine the value that you must implement in the registry.

1 Open **regedit**

2 Navigate to `HKLM\Software\Symantec\DLO\3.0\Client.`

3 Create a new DWORD value named `DiskQueueLimit`.

4 Type the value as 70 decimal.

5 Navigate to `HKCU\Software\Symantec\DLO\3.0\Client.`

6 Create a new DWORD value named `DiskQueueLimit`.

7 Type the value as 70 decimal.

8 Restart the Desktop Agent (do not just minimize and maximize it).

Note: The value of 70 was obtained by calculating the average read queue length during a slow backup event and multiplying by 10. The value of 70 may not necessarily apply to all desktop environments. Follow the logging example as explained above, to determine the average queue length experienced on the problematic host, and apply the observed adjusted average to the `DiskQueueLimit` registry key.

When I upgrade the Desktop Agent from 7.0 to 7.5 by using a different user account (instead of the administrator account that was used to log on to the machine and install Desktop Agent 7.0 version), and when I try to access the existing desktop user data folder, the Desktop Agent goes to disabled state with the following error: *"Access denied. Failed to create recovery key."*

The error occurs because the user account may not have the privileges to access the existing desktop user data folder.

To resolve this issue, follow these steps:

1 Right-click the desktop user data folder, and select **Properties**.

2 Select the **Security** tab and add the user account.

3 Click **Apply**.
The recovery key is created.

Before unclustering DLO from a cluster setup, the network user data folder (NUDF), DLO database, and media server are moved from the virtual server disk to a local disk on the Desktop Agent. After this process, when I launch the Desktop Agent, the following error message is displayed: "*Failed to load configuration settings*".

This error occurs because the DLO Administration server is down, and the notification has not been updated in the Desktop Agent machine.

Note: This error may also occur for desktops and laptop users in a non-clustered setup.

To resolve this issue, manually update the registry keys of the NUDF, media server, and database in the Desktop Agent machine.

1. Open **Registry Editor**.
2. Navigate to `HKEY_LOCAL_MACHINE\Software\Symantec\DLO\Client.`
3. Double-click the `DefaultMediaServer`, and change the name of the media server from virtual server name to the host name of media server.
4. Navigate to `HKEY_LOCAL_MACHINE\Software\Symantec\DLO\Client\UserShare`
5. Double-click the user name and change the path of the network user data folder.
6. Navigate to `HKEY_LOCAL_MACHINE\Software\Symantec\DLO\DB`
7. Double-click the `DBServer`, and change the name of the database server from virtual server to host name of DB server.

   Note: Complete step 7 only when standalone DLO components are clustered. In case a remote DB setup was used for clustering DLO, then step 7 is not required.

When I install Desktop Agent on a BitLocker enabled drive and later if I lock the drive and try to launch the Agent, the following error message is displayed: “*Access denied*”.

To resolve this issue, unlock the drive and then launch the Agent.

Similarly, for NUDF and LUDF, ensure that you unlock the drive and then access the data.

Remote DLO Agent and Push Install Maintenance Server

I am receiving the following error: “*Remote Install Error: Credentials not found for machine.*”

You must ensure that the “Windows Management Instrumentation” and “Remote Registry” services are running on the remote machine and has execute permission for “Windows Management Instrumentation” service.

Remote installation of DLO Agent or Maintenance Server is failing.

On the ‘Installation Status’ screen, right-click the remote computer for which installation is failing, select the ‘View Push log’ or ‘View Install Log’ option and look for the error.

The “*Administration services are down*” error is displayed after launching the console with Remote DB.

You must ensure that ‘Symantec DLO SQL services’ and ‘SQL browser services’ on remote database are started. If the error still persists, then start the ‘Symantec DLO administration services’.

Troubleshooting the Dedupe Server

Dedupe Server is installed but the following error message is displayed: "The server host or port details you have entered is invalid or there is no Dedupe Server running at the specified location."

This error could occur if some other application and Dedupe Server are using the same default HTTPS port number 8443.

After installing the Dedupe Server, change the HTTP and HTTPS port numbers in the `server.xml` file located at this path:

```
C:\Program Files\Symantec\Symantec DLO\Dedupe
Server\Tomcat\conf\server.xml.
```

For example, if the HTTP port number is 8181, and the HTTPS port number is 8445, modify the server.xml file as explained here:

1 *Existing value:*

```
<Connector connectionTimeout="20000" port="8080"
protocol="HTTP/1.1" redirectPort="8443" server=" "/>
```

Change to:

```
<Connector connectionTimeout="20000" port="8181"
protocol="HTTP/1.1" redirectPort="8445" server=" "/>
```

2 *Existing value:*

```
<Connector SSLEnabled="true" SSLProtocol="TLS" clientAuth="false"
keystoreFile="dedupeserver.jks" keystorePass="dedupeserver"
maxThreads="1000" port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
scheme="https" secure="true" server=" "/>
```

Change to:

```
<Connector SSLEnabled="true" SSLProtocol="TLS" clientAuth="false"
keystoreFile="dedupeserver.jks" keystorePass="dedupeserver"
maxThreads="1000" port="8445"
protocol="org.apache.coyote.http11.Http11NioProtocol"
scheme="https" secure="true" server=" "/>
```

3 *Existing value:*

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"/>
```

Change to:

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8445"/>
```

4 After changing the values in the `server.xml` file, add these port numbers in the firewall exceptions.

5 Restart the Dedupe Server services.

Scenario 1:

While installing only the Dedupe Server on a machine, if I provide a different user account (instead of the administrator account that was used to log on to the machine) for the SQL service,

I am not able to add the Dedupe Server and the following error message is displayed: ***"The Dedupe details you have entered is invalid or there is no Dedupe Server running at the specified location."***

Scenario 2:
While upgrading from Symantec DLO 7.0 to Symantec DLO 7.5, if I provide a different user account for the SQL service, I am able to add Dedupe Server, but cannot manage the Dedupe Server.

For these two scenarios, ensure that both SQL service and Dedupe Server service run with the same user account.

To resolve this issue, follow these steps:

1. Change the Dedupe Server service's user account to match the SQL service account.
2. To grant administrator rights to the user account that was used for SQL service, run the following command.

   Example

   ```
   sqlcmd.exe -E -l 60 -S <SERVERNAME>\SQlEXPRESS -d DedupeDB -Q "EXEC
   sp_addsrvrolemember 'testdomain\DBAdmin1', 'sysadmin'"
   ```

3. To update the `dedupedb user_info` table with the DLO administrator account, run the following command:

   ```
   sqlcmd.exe -E -S <SERVERNAME>\<INSTANCENAME> -l <TIMEOUT>-d DedupeDB
   -Q "UPDATE user_info SET user_name='<DOMAIN\USERNAME>'"
   ```

   Example

   ```
   sqlcmd.exe -E -S A2SYMMD14906\SQLEXPRESS -l 60 -d dedupedb -Q
   "UPDATE user_info SET user_name='<DOMAIN\USERNAME>'"
   ```

Options

-E: Uses a trusted connection instead of prompting for a password.

-l: The duration (in seconds) when the `osql` login is active.

-Q: Query.

Note: After adding the Dedupe Server, in case the user account does not have the privileges to manage the Dedupe Server, then the following error message is displayed: *"Could not authenticate user."* In such a scenario, follow the same procedure to grant the administrator rights.

On a Windows 2008 R2 machine, I have installed Symantec DLO 7.0 with administrator account. While upgrading to Symantec DLO 7.5, if I use the domain administrator account, Dedupe database is not getting attached, and the error message is displayed: ***"Unable to connect to server. DLO Administration service is not running. Would you like to check the service credentials."***

To resolve this issue, follow these steps:

1. Log on to the Windows 2008 R2 machine using an administrator account. Example: <domain>\administrator
2. Install the SQL Server and SQL instance using the same administrator account.
3. Install DLO 7.0 choosing existing SQL instance.
4. Add the domain user account (<domain>\<user name>) to local admin group.

5. Change the “SQL Server”, “SQL Agent” and “SQL Browser” services credentials to the domain user account.
6. Set the SQL administrator role to the domain user by running the following command:

   ```
   sqlcmd.exe -E -S <SERVERNAME>\<INSTANCENAME> -Q "EXEC
   sp_addsrvrolemember 'testdomain\DBAdmin1','sysadmin'"
   ```

   Example

   ```
   sqlcmd.exe -E -S MachineName\SQLEXPRESS -Q "EXEC
   sp_addsrvrolemember 'testdomain\DBAdmin1','sysadmin'"
   ```

7. Log off from the machine and log on with the domain user account.
8. Upgrade to DLO 7.5 by providing the domain user account in the “SQL Service Account” and “DLO Administrator Account” screens.
   The Dedupe database and all other components work properly.

In a remote DB scenario, the DLO server and DLO database machines are running with two different login credentials. When I upgrade this remote DB setup from DLO 7.0 to DLO 7.5, I am not able to configure the Dedupe Server and the following error message is displayed: “*Failed to authenticate server. Do you want to retry?*”

To resolve this issue, manually add the user name to the “UserInfo” table in the Dedupe database.

1. To add the domain user name to the `DedupeDB user_info` table, run the following command:

   ```
   sqlcmd.exe -E -S .\<INSTANECENAME> -d DedupeDB -Q "insert into
   user_info values (5,'<DOMAINNAME\USERNAME>',NULL,1)"
   ```

2. Configure the Dedupe Server.

After installing the DLO components, how do I verify the status of the Dedupe Server?

Type one of the following URLs in your browser.

http://<dedupeserver_ip_or_hostname>:8080

or

https://<dedupeserver_ip_or_hostname>:8443

Response	Remark
StoreSmart Dedupe Server Status: (20159) Active	Dedupe Server is up and running after installation.
StoreSmart Dedupe Server Status: (20157) Garbage Collection In Progress	Dedupe Server is up and running and GarbageCollection is in progress.
StoreSmart Dedupe Server Status: (20158) Under Maintenance	Dedupe Server is up and running and MaintenanceWindow is active.
No response	Dedupe Server is not initialized.

If there is no response from the Dedupe Server, then it indicates that the Dedupe Server is not initialized, and one of the reasons could be that the database connection is down. This issue will be logged in the `dedupeserver.log` file located at this path: `C:\Program Files\Symantec\Symantec DLO\DedupeServer\Tomcat\logs`.

I want to modify a Dedupe Storage Location but it is disabled in the DLO Administration Console.

You can modify the Dedupe Storage Location only when the Maintenance Window is scheduled.

For more information about scheduling the Maintenance Window see “Dedupe Server Maintenance” on page 82.

When I try to initialize the Desktop Agent in offline mode I get an error 23522: “*Dedupe Engine is failed to initialize in offline mode*.”

This error may occur if the metadata files are deleted from the local machine and the Desktop Agent is initialized in offline mode. This issue is resolved when the Agent goes online.

Accessibility

Symantec products meet federal accessibility requirements for software as defined in Section 508 of the Rehabilitation Act:

http://www.access-board.gov/508.htm

Keyboard shortcuts are available for all graphical user interface (GUI) operations and menu items. Symantec products are compatible with operating system accessibility settings as well as a variety of assisting technologies. All manuals also are provided as accessible PDF files, and the online help is provided as HTML displayed in a compliant viewer.

The following topics explain the accessibility features and compliance in DLO:

Keyboard Navigation and Shortcuts in DLO

All program functions and menu items are accessible using the keyboard exclusively. DLO uses standard operating system navigation keys and keyboard shortcuts. For its unique functions, DLO uses its own keyboard shortcuts, which are documented in "Keyboard Shortcuts" on page 314.

Items in the task pane that do not have keyboard shortcuts can be accessed by using the operating system's "mouse keys", which allow you to control the mouse through the numerical keyboard.

To see a table of the standard Microsoft navigation keys and keyboard shortcuts, select your version of Microsoft Windows from the table at:

http://www.microsoft.com/enable/products/keyboard.aspx

General Keyboard Navigation within the GUI

You can navigate and use DLO with only the keyboard. In the GUI, the current active tree or table has a dark blue highlight, and the current active tab, radio button, or check box is enclosed within a rectangle formed by dotted lines. These areas are said to have *focus* and will respond to commands.

All Symantec GUIs use the following keyboard navigation standards:

- The TAB key moves the focus to the next active area, field, or control, following a preset sequence. SHIFT+TAB moves the focus in the reverse direction through the sequence
- CTRL+TAB exits any Console area that you internally navigate with the TAB key
- UP and DOWN ARROW keys move focus up and down the items of a list
- The ALT key in combination with the underlined mnemonic letter for a field or command button shifts the focus to that field or button
- Either ENTER or the SPACEBAR activates your selection. For example, after pressing the TAB key to select Next in a wizard panel, press the SPACEBAR to display the next screen
- SHIFT+F10 provides access to context menus

Keyboard Navigation within Dialog Boxes

Dialog boxes contain groups of controls necessary to set options or settings for programs. Here are some general rules about dialog box navigation:

- The TAB key moves focus between controls within the dialog box along a preset sequence
- Controls displaying a mnemonic (an underlined letter) can be selected regardless of focus by typing ALT and the underlined letter
- A dark border indicates the default command button. Press ENTER at any time to choose the button with a dark border
- ESC chooses the **Cancel** button if one exists
- SPACEBAR chooses a control you select with the TAB key
- SPACEBAR changes the state of a check box that has focus. Typing a mnemonic (if one is available) will move the focus to the check box and change its state
- Arrow keys move focus within radio buttons, list boxes, sliders, groups of option controls, or groups of page tabs
- Items that cannot be changed are not visited by the TAB key sequence. Options that are unavailable are grayed-out and can neither be selected nor given focus

While the controls described here are typically found in dialog boxes, they also can occur in other contexts. The same navigation standards will apply.

Tabbed Dialog Boxes

Some dialog boxes use tabbed pages to subcategorize groups of many options. Each tabbed page contains different groups of controls. Use TAB to move the focus between tabbed pages within a dialog box. Typing the mnemonic for a tab also moves the focus to the tabbed page and displays its page of controls.

The following table lists keyboard navigation rules within tabbed dialog boxes.

Table 7-1 Keyboard Navigation within Tabbed Dialog Boxes

Keyboard input	Result
CTRL+PAGE DOWN or CTRL+TAB	Switches to the next tab and displays the page.
CTRL+ PAGE UP	Switches to the previous tab and displays the page.
RIGHT ARROR or LEFT ARROW	When the focus is on a tab selector, chooses the next or previous tab in the current row and displays the page.

List Boxes

List boxes display a column of available choices. Different types of list boxes are available with additional navigation conventions:

- Drop-down list boxes by default show only the selected item. A small button to the right of the control shows a downward-pointing arrow. Select the arrow to display more items from the list box. If there are more choices than can fit in the preset list box area, a slider appears along the side of the list box. Show or hide the list using ALT+DOWN ARROW, ALT+UP ARROW, or F4. The TAB key selects an item.
- Extended selection list boxes support selecting single items, blocks of items, or combinations of the two. After selecting an item, hold down CTRL+navigation keys to select or clear additional items or blocks of items.

Keyboard Shortcuts

All menu items can be selected by using accelerator or mnemonic keyboard shortcuts. An accelerator is a key combination that provides shortcut access to a GUI function. A mnemonic (sometimes referred to as a “hot key”) is a single-key equivalent (used in combination with the ALT key) for selecting GUI components such as menu items. The mnemonic “hot key” letter is underlined in the GUI.

Routine functions such as opening, saving, and printing files can be performed using the standard Microsoft keyboard shortcuts. Other menu items are unique to DLO.

The following table lists the shortcut keys in the Desktop Laptop Option Administration Console.

Table 7-2 Keyboard Shortcuts Unique to Backup Exec Desktop and Laptop Option Administration Console

Accelerator	Mnemonic	Result
ALT	F	The **File** menu expands. From the **File** menu, you can create new profiles and Storage Locations, and add users.
ALT	E	The **Edit** menu expands. From the **Edit** menu, you can restore files, search for files to restore, manage alerts, and delete items.
ALT	V	The **View** menu expands. From the **View** menu, you can change the information that displays on the screen.
ALT	N	The **Network** menu expands. Use the Network menu to work with administrator accounts, connect to the DLO Administration Servers on the network, or to reconnect to a local DLO Administration Server.
ALT	T	The **Tools** menu expands. Use the **Tools** menu to set global excludes, access all DLO wizards, and manage service credentials.
ALT	W	The **Window** menu expands. Use the **Window** menu to move to a new window or view.
ALT	H	The **Help** menu expands.Use the **Help** menu to access documentation and various Symantec web sites.

The following table lists the shortcut keys in the Desktop Agent:

Table 7-3 Keyboard Shortcuts Unique to Desktop Agent

Accelerator	Mnemonic	Result
ALT	F	The **File** menu expands. From the **File** menu, you can minimize or exit the Desktop Agent.
ALT	V	The **View** menu expands. From the **View** menu, you can change the information that displays on the screen.

Table 7-3 Keyboard Shortcuts Unique to Desktop Agent

Accelerator	Mnemonic	Result
ALT	K	The **Tasks** menu expands. Use the **Tasks** menu to run a job or refresh the view.
ALT	O	The **Tools** menu expands. Use the **Tools** menu to reset dialog boxes and accounts.
ALT	H	The **Help** menu expands. Use the **Help** menu to access the online help for the Desktop Agent.

Select secondary menu items by opening the main menu and using the UP or DOWN ARROW key until the required item is highlighted. Press the RIGHT ARROW key to open a submenu, and ENTER to select your choice.

Keyboard shortcuts are not case-sensitive. Mnemonic keystrokes may be pressed either sequentially or simultaneously. All menu items have mnemonics, but not all menu items have accelerators.

Support for Accessibility Settings

Symantec software responds to operating system accessibility settings.

Symantec products are compatible with Microsoft's accessibility utilities. In Windows 2000, accessibility options involving keyboard responsiveness, display contrast, alert sounds, and mouse operation can be set through the Control Panel.

To set accessibility options

1 On the **Start** menu, select **Settings**, and then select **Control Panel.**

2 Select **Accessibility Options**.

Note: You can also set accessibility options through the Accessibility Wizard. On the **Start** menu**,** select **Programs**, and then select **Accessories**. Select **Accessibility**, and then select **Accessibility Wizard**.

Though all graphics in Symantec documentation can be read by screen readers, setting your screen reader to ignore graphics may improve performance.

Glossary

Administrator
The user that configures DLO using the Symantec DLO Administration Console. This user must have administrative rights to operate the console.

Authentication
The process of validating a user's credentials.

Automated User Assignments
Rules that assign profiles and Storage Locations to a specified group of desktop users. Settings are applied the first time a user runs the Desktop Agent.

Compression
A method of reducing data to expedite transmission time or storage volume.

Chunk
Uniquely identified data block.

Chunk Retrieval Information (CRI)
Location of data in the Dedupe Storage Location where it was written during backup. CRI is used to read back the data during restore.

Chunk Signature
Hash value of the data block.

Dedupe Storage Location
A shared storage location on the network where data is stored.

Dedupe Storage Pool
Groups of Dedupe Storage Locations across which deduplication is performed.

DLO Administration Console
The administrator's interface with the Desktop and Laptop Option.

DLO Backup Selection
The files and folders on a desktop or laptop that are selected for backup by the DLO Administrator or desktop user.

DLO Database
The location where policy settings and status information are stored.

DLO File Server
The computer that hosts DLO Storage Locations.

Dedupe Database
Data store used by Dedupe Server for storing the configuration and Global Hash Table.

Delta File Transfer
Delta File Transfer is a compression process that allows only the changed portion of a file to be transferred once the complete original file is backed up. Delta File Transfer reduces bandwidth use and disk storage requirements.

Desktop Agent Install Share

The network share where the Desktop Agent install files are located. This folder is set up on the DLO Administration Server when DLO is installed, and facilitates the installation of the Desktop Agent on desktops.

Desktop Agent

The DLO software that runs on desktop and laptop computers.

Desktop Agent Console

The user interface for the Desktop Agent software.

Encryption

A process used to ensure data security of files and folders on disk and during data transfer.

Global Hash Table

Table that maps data signature to CRI for the data that is stored in the Dedupe Storage Locations.

Open File Handling

The process by which files currently in use can be backed up.

Optimization

The process of reducing network traffic and file storage through technologies such as compression.

Profile

DLO settings configured by the administrator and that apply to users or groups of users.

Revision

A version of a file at a specific point in time.

Storage Location

A shared location on the network in which network user data folders and backup files are stored.

Synchronization

The process that maintains the most recent version of selected files and folders belonging to the same user on multiple desktops. Synchronization is available for files and folders that are backed up by DLO.

Task

An accessible program function that varies with the view selected in the DLO Administration Console or Desktop Agent console.

User

The person who operates the desktop or laptop computer on which the Desktop Agent is run.

User Data Folder

The folder in which user backup data is stored. There is a user data folder on each desktop that is protected by the Desktop Agent, and one user data folder on the network for each Desktop Agent user.

User Name

The user name used for Windows authentication.

View

The main navigational interface in the DLO Administration Console.

Index