# Veritas™ Desktop and Laptop Option 9.4

# README

VERITAS

Veritas Desktop and Laptop Option: README

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice



Veritas Technologies LLC

2625 Augustine Drive

Santa Clara, California 95054, U.S.A

http://www.Veritas.com/

# Technical Support

Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within the company to answer your questions in a timely fashion.

Our support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about our support offerings, you can visit our website at the following URL:

www.veritas.com/support

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

## Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.veritas.com/support

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
- Error messages and log files
- Troubleshooting that was performed before contacting Technical Support
- Recent software configuration changes and network changes

## Licensing and registration

If your product requires registration or a license key, access our technical support Web page at the following URL:

www.veritas.com/support

## Customer Service

Customer service information is available at the following URL:

www.veritas.com/support

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Advice about technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

## Support Agreement Resources

If you want to contact us regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

| | |
|---|---|
| Worldwide (except Japan) | CustomerCare@veritas.com |
| Japan | CustomerCare_Japan@veritas.com |

# Contents

# What’s New in DLO 9.4

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

## Simplified data restore of users who have left the organization

DLO now enhances the administrator experience with the ability to perform seamless data restore from the console, of users who have left the organization and have been deleted from the Active Directory.

## Usability Enhancements

DLO now provides key usability enhancements, in terms of Improved User machine mapping and enhanced Audit Trail reports.

## Mac Encryption Support

DLO now supports the FileVault2 encryption for Mac endpoints.

# Key Features from Previous Releases

This section provides an overview of the key features of the previous releases:

## Rollback Capabilities

The Rollback capabilities have been provided considering the rise in ransomware attacks that are impacting the endpoints in the organizations. From a ransomware protection strategy perspective, the rollback capabilities consist of two parts - first being the backup strategy in order to be prepared for the ransomware attack and next, the restore capabilities in case an actual attack occurs.

In terms of the backup strategy, DLO's scheduled backup capability and revision control policy can be leveraged to create multiple revisions that the customer can restore from. For maintaining day-wise revisions, a certain number of days can be configured as the Rollback Window by the administrator. The latest revision of the respective days will be maintained in the network user data folder.

In case of an attack, the files may get encrypted resulting in a file change that will be backed up. Hence the administrator may want to prevent further backups before proceeding with restores, for which the Disable options can be used.

For restore capabilities, in addition to a simplified restore UI, a point in time restore of the backed up data can be initiated by selecting a date from the restore dialog, to restore the latest revision of the file on that particular date. Once the restore activities are completed, the detailed summary can be viewed.

**Note**: Rollback capabilities are not supported for Windows and Mac endpoints with DLO versions prior to 9.1. Configuring Rollback Window is not supported on Mac endpoints.

## Active Directory Scan for Auto User Deletion

The Active Directory Scan option provides the administrator with the ability to configure automated and manual scans of the Active Directory to identify and auto delete users who have quit the organization.

# Downloading Veritas DLO

To download Veritas DLO 9.4, perform the following:

1. Download the appropriate files into a temporary directory:
- `Veritas_Desktop_and_Laptop_Option_9.4_xxxxxx_64-bit.zip`

   where, xxxxxx is the build number.
2. To extract the files, double-click the `.zip` file.

   This helps to create a number of files that include `x64.README` and `setup.exe`.

# Prerequisites for Installing Veritas DLO

| Item | Description |
|---|---|
| Domains and Active Directory | The DLO Administration Server, DLO Dedupe Server, DLO Edge Server, DLO IO 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.<br><br>Note: From the DLO 9.2 version onwards, DLO can be deployed in a Domain Trust Independent architecture, where the DLO Server and Agents are in different domains. For more information, refer *Domain Trust Independent Solution* document available here. |
| User privileges for installing and managing DLO | Following are the accounts required for installing and managing DLO Components:<br><br>**Domain User or Domain Administrator account for:**<br>• Veritas DLO Administration Server: This user should have local administrator privilege on DLO Administration Server machine, Storage Server and SQL Server. This user should have read and write access to the registry on the DLO Administration Server machine.<br>• Mindtree Storesmart Dedupe Server service: This user should have local administrator privilege on the DLO Administration Server machine. This account should be the same as DLO Administration Server service account.<br>• SQL Server (instance): This user should have local administrator privilege on DLO Administration Server, SQL Server machine and Storage Server.<br>• SQL Server Browser: This user should have local administrator privilege on the SQL Server machine.<br>• Veritas DLO Web Server Service: This user should have local administrator privilege on DLO Administration Server machine. This account should be the same as DLO Administration Server service account.<br>**Local System Account for:**<br>• Veritas DLO Edge Server Service<br>• Veritas DLO Maintenance Server<br><br>**Domain User account for:**<br>• Accessing Dedupe Storage Location. This low privilege domain user account is also known as “Dedupe Storage Location Access Credential” and will be used by the Desktop Agent to access the Dedupe Storage Location. A user account with administrator rights is not permitted to be configured as Dedupe Storage Location Access |

| | |
|---|---|
| | Credential account. The administrator needs to ensure that the password for this user account does not expire frequently. If the password expires, then reset the password for the domain user. This user should have the 'Allow log on locally' policy set in the domain controller group policy object. |
| User privileges for DLO Agents Users | • Impersonation privilege is required for the logged on user on the desktop agent machine for impersonating as the Dedupe Storage Location user in order to write the deduped data to the Dedupe Storage Location.<br>• A local system account for the Volume Shadow copy service is required. This service should be up and running in order to provide backup statistics for generation of the Backup Status Report. |
| Database Selection | By default DLO installs its own instance of SQL Server 2014 Express SP3. DLO can be manually configured to use an existing local SQL Server instance. The DLO Database Service requires minimum 6 GB hard disk space.<br>Note: Ensure to manually install the *Microsoft® SQL Server® 2014 SP3 Latest Cumulative Update* available here.<br><br>For more information on the supported versions, refer the *Veritas DLO Software Compatibility List* document available here.<br><br>Note: When you use an existing local or remote database instance, TCP/IP and named pipes must be enabled. Refer the link https://msdn.microsoft.com/en-us/library/ms191294.aspx. |
| Firewalls | DLO is designed to work in firewall environments. The DLO Desktop Agents can be installed on endpoints that are connected either over the corporate network or in the Backup Over Internet (BOI) mode using the private internet connection. The details of the port configuration for the DLO Server components and DLO Clients in a firewall environment are defined for the following three deployment scenarios:<br>• **Non BOI Deployment**: For organizations having endpoints that are always within the organization premises and are connected over the corporate network.<br>• **Exclusive BOI Deployment**: For organizations having endpoints that are always outside the corporate network and connect only using internet connection.<br>• **Occasional BOI Deployment**: For organizations having endpoints that are occasionally outside the organization premises, during which they connect using internet connection, but are otherwise within the organization premises connecting over the corporate network.<br>For details on configuring the ports for the specific deployments, refer the *Port Requirements for Veritas Desktop and Laptop* document available here. |
| Certificates | This is required for the Backup Over Internet (BOI) capability. In order to configure the BOI capability, an SSL certificate procured from a Trusted CA is a pre-requisite. This certificate is required for the Desktop Agents to communicate with the DLO Edge Server over a public URL. However, for product evaluation scenarios, an inbuilt self-signed certificate is provided in the DLO Installer package for validating the BOI capability.<br>**Note**: It is recommended to use a SSL certificate procured from a Trusted CA when deploying in production. |
| Remote Install Considerations | For remote installation of the DLO Maintenance Server and DLO Desktop Agents:<br>• To push-install to a computer, you must enable certain items on the destination computer's Windows Firewall Exceptions list. You must enable the following items:<br>  ○ File and Printer Sharing<br>  ○ Windows Management Instrumentation (WMI)<br>  ○ Remote Service Management<br>  ○ Remote Registry Service |

| | |
|---|---|
| | For more information, refer to the Microsoft Windows documentation. https://docs.microsoft.com/en-us/windows/<br><br>• 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. |
| Other Considerations | • The latest service pack and windows updates should be installed, to be able to install the DLO components.<br><br>Note: The DLO 9.3.2 version onwards provides support for Transport Layer Security (TLS) 1.2. OS KB articles and SQL related prerequisites required to support TLS 1.2, should be updated manually. TechNote created for this, is also available from the First screen of installer.<br><br>• WMI service should be running on all machines where the DLO Server components are installed.<br><br>• .NET 4.0 or above versions should be installed.<br><br>http://www.microsoft.com/en-in/download/details.aspx?id=17718<br>Note: On Windows 2012/ 2012 R2 /2016 Server, it is not mandatory to install .NET 4.0 since .NET 4.5 is installed by default in Windows 2012/2012 R2 Server and .NET 4.6 is installed by default in Windows 2016 Server. |

# Installing Veritas DLO

The installation package is used to install a new DLO Administration Server and other required components of Veritas DLO 9.4. For instructions, refer to the *Veritas Desktop and Laptop Option Quick Reference Guide for Installation and Configuration* and *Veritas Desktop and Laptop Option Administrator's Guide* document available here.

## Upgrading to Veritas DLO 9.4

DLO supports upgrades from the following previous versions:

- Veritas DLO 9.3.3
- Veritas DLO 9.3.2
- Veritas DLO 9.3.1
- Veritas DLO 9.3
- Veritas DLO 9.2
- Veritas DLO 9.1
- Veritas DLO 9.0 SP1

For any existing customers with previous version of DLO (DLO 7.6 SP1, DLO 8.0, DLO 8.0 SP1, DLO 8.0 SP2, DLO 8.0 SP3, and DLO 8.0 SP4), it will be a stepped upgrade support. That is, customers should first upgrade from the existing version to DLO 9.3.2, and then upgrade to this latest version.

For the versions prior to 7.6 SP1, first upgrade to 7.6 SP1, followed by 9.3.2 and then to the latest version.

**Considerations before Upgrading:**

It is recommended to backup the DLO and Dedupe Database (.ldf and .mdf files) before the upgrade.

**To upgrade from a supported version of DLO to Veritas DLO 9.4, 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. Proceed with the installation.
6. When the installation is completed, click **Finish**.

# Installing the Desktop Agent on Mac

Users with administrator rights can install the Desktop Agent. After the Desktop Agent is installed on a Mac 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.

When the Mac Desktop Agent is installed on a computer that is not in a domain, and when you launch the Desktop Agent for the first time, you are prompted to enter the user name, password, and domain. Provide the domain user credentials.

### Prerequisites

Complete the following tasks before installing the Desktop Agent on a Mac machine.

1. Install and configure DLO Administration Server on a Windows server machine.
2. The DLO administrator must ensure that the TCP/IP protocol is enabled for the DB instance, and the port number is set.
3. Irrespective of the firewall state in the DB server (ON or OFF), the administrator must enter the DB port in **SQL Server Configuration Manager > SQL Server Network Configuration > "Protocols for <Instance name>" > TCP/IP Protocol Settings > TCP Port**.

   **Note:** The default DB port is **1433**.

   a. If the firewall is ON in the DB server, then this TCP port should also be included in the firewall exception list.
4. Restart the DLO DB service after providing the DB port number.
5. In case a customized TCP Port is provided, then do the following on DLO Mac Agent once it is installed:

   a. Open the `Agentconfiguration.plist` file located in users/<username>/.Applications/Veritas/DLO/.settings folder.

   b. Change the String value of the key `DBPort` from 1433 to the new value

   c. Launch the DLO Mac Agent

   **Note:** The default port to communicate with the DB Server is **1433**.

6. To verify the communication to DB server use Telnet. (Example, telnet <IP> <port>.)

### To Install the Desktop Agent on Mac:

1. From the desktop on which you want to install the Desktop Agent, go to the desktop menu options, select **Finder**.
2. Select **Go > Connect to Server**.
3. In the **Server Address** field, type the network address of DLO Server using one of the following formats.
   - **smb://IPaddress/**
   - **smb://DNSname/**
4. Click **Connect**.

   **Note:** You can also type the server address along with the share name. `smb://IPaddress/DLOMacAgent`.

5. From the list of shared folders, open **DLOMacAgent** folder, copy the **setup.ini** and the installer package for Mac to your local machine.
6. Copy the installer package for Mac to the same location where you copied the **setup.ini** file.
7. Double-click the file **Veritas_DLO_Agent.pkg**.
8. On the Welcome screen, click **Continue**.
9. Read the license agreement, and click **Continue**.
10. Click **Agree**.
11. The default installation path for Mac is: **/Applications**. To install the Desktop Agent in an alternate location, click the **Change Install Location** button, and do one of the following:
    - Select **Install for all users** to install Desktop Agent in the default location
    - Select **Install on a specific disk** to install in any other disk other than the default startup disk. This option is useful when you want to install the Desktop Agent on any additional hard disks or hard drive partitions that exist on the local Mac machine.
12. Click **Continue**.
13. Click **Install**.
14. Once the installation is completed, click **Close**.

For more information about launching and configuring the Agent on Mac, refer to the *Veritas Desktop and Laptop Mac Getting Started Guide* available here.

# Upgrading the Desktop Agent on Mac

To upgrade the Desktop Agent on Mac, refer to the section To install the Desktop Agent on Mac.

# Known Issues

This section describes the known issues in DLO 9.4. The issues are listed based on the ET number (software bug tracking number).

| ET Number | Description | Workaround |
|---|---|---|
| 3962843 | Email Notifications are not supported with SMTP server configured using SSL with GSSAPI authentication. | Not Applicable |
| 3947060 | Backup Summary fields like Backup Completion is reflecting value '0' for some computers in the Backup Status report, History tab and Restore tab. | Fields like Backup Completion are not supported for computers with Windows desktop agent versions prior to DLO 8.0 SP3 and Mac agent versions prior to DLO 9.1. Refer to Understanding the Backup Status Report for more details.<br><br>To resolve this issue, the agents need to be upgraded to the latest supported version. |
| 3942638 | Synchronization is not supported for configured PST files and configured Lotus Notes. | Not Applicable |
| 3946759 | Windows 10 Desktop Agent crashes while exiting when synchronized folders are configured for the user. | Not Applicable |
| 3941231 | Desktop Agents with Scheduled backups crash when frequency is updated from 'Run every' to 'Run once' and vice versa. | Not Applicable |
| 3941231 | With scheduled backups, when editing backup schedule, files in the queue are backed up immediately the first time. | Not Applicable |
| 3898325 | Edge Service gets deleted when upgrading from some Symantec DLO versions to Veritas DLO versions | Re-install the Edge Server component after upgrading to the latest Veritas DLO version. |
| 3901312 | After failover in a DLO cluster, the Startup Type of Mindtree StoreSmart Dedupe Service, SQL Service and DLO Administration Service are changing from Automatic to Manual. | Update the Startup Type for the services as Automatic. |
| 3903787 | On a Japanese OS, Notification Properties window is seen in Japanese even after changing the language to English with the Change Language option. | Not Applicable |
| 3901307 | Desktop Agent does not work in BOI mode if the DLO Server is configured in clustered environment. | Refer to the Technote https://www.veritas.com/support/en_US/article.100040945 |

| | | |
|---|---|---|
| 3763796 | Any new Certificate push from the Server does not get updated for the Desktop Agents working in BOI mode | Desktop Agents need to connect over LAN at least once for the settings to be updated automatically.<br><br>Alternatively, the Server certificates can be manually downloaded from the Web Restore page and copied to the Desktop Agent install location.<br><br>For more details, refer to the Pre-requisites for Web restore section of the Administrator's Guide. |
| 3921934 | Desktop Agents of Symantec versions are going to disabled state after the Server is upgraded to any Veritas version. | Manually upgrade the agents to the latest Server version. |

# Known Issues in Mac Agent

| ET Number | Description | Workaround |
|---|---|---|
| 3931685 | Rollback restore is not honored during Staging to an unregistered Mac machine. | Destination Mac machine should be registered for honoring Rollback restore while Staging. |
| 3923286 | Backup completion field in Backup Status report exceeds 100% value | This is observed when the maintenance cycle and the backups are running simultaneously. This will be auto corrected with the next maintenance cycle. |

# Resolved Issues

| ET Number | Description |
|---|---|
| 3985276 | Post upgrade, if large number of endpoints (> 2k) are connected in BOI mode, the endpoint backups are not working. |
| 3979576 | Data migration fails if temporary files like .vts, .vrts are part of NUDF. |
| 3989553 | Unable to update DSL credentials after password change, when some DSL shares are not accessible |
| 3989596 | Emergency restore is failing for user names having polish characters. |
| 3987318 | Could not generate ‘User Status by Profile’ report using Japanese characters |
| DLO-2320 | If a user is launching the client on a machine other than the one set in 'User-Machine' mapping, a dialog box should be displayed. |
| 3985047 | After upgrade to 9.3.2, email notifications were failing. |
| 3982120 | backup status % is not getting updated successfully |
| DLO-2939 | When a folder named DBBackup is created in the root of any drive, DLO Admin service is deleting it automatically |
| DLO-2902 | Restore from admin console for users not part of AD. |
| 3999145 | Error occurs if either 'Domain' or 'Group' fields are blank and try to configure AUA by selecting the second option i.e. 'Assign using Active Directory'. |
| 3997352 | Dedupe server label is reported as "I" instead of "Dedupe Server" in Dashboard of DLO Admin console. |
| 3988036 | Files and folders under /Users/<USERNAME>/Library/Application Support/ are not backed up on Mac. |
| DLO-3012 | Restart of dedupe service shouldn't update the 'cleanup_time' in potential garbage table to current system date. |
| 4006351 | The global exclude "Lengthy Files" should not allow clients to backup any file name having more than 200 characters. |
| 4001314 | Client logs should be enhanced incase if network throttling during backup doesn't work |
| 3995469 | Report generation fails when the system date format is changed |
| DLO-3090 | Updating DLO DR document for 9.4 |
| DLO-3117 | Modifying the content of "Importing Storage locations" in DLO admin guide |
| 4007467 | Description for the remote storage locations is incorrect in the DLO Admin Guide. |