Veritas™ Desktop and Laptop Option 9.2

BOI Setup and Configuration Details

VERITAS

11 May 2018

Veritas Desktop and Laptop Option: Updated BOI Setup and Configuration Details.

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.

Veritas Technologies LLC
500 East Middlefield Road
Mountain View, CA 94043
http://www.Veritas.com/

Contents

Introduction

Veritas DLO an endpoint backup and recovery product provides the Backup Over Internet (BOI) capability that focuses on protecting laptop user's data, by ensuring backup of files using the available internet connection. The BOI option is intended for organizations where the employees are mostly or always on the move and spend limited to no time in the corporate network respectively.

BOI capability ensures continuous backup of files over the internet through an automatic network selection mechanism with no manual effort required from the end user.

This document provides the details for an administrator to Install and Configure the Veritas Desktop and Laptop Option for the BOI capability.

Architecture Overview

Veritas DLO Server has the following components:

1. **DLO Administration Server**: The service responsible for the Administrative activities.
2. **DLO Administration Console**: A graphical user interface for the Administrator to configure, manage and monitor the endpoint backup environment.
3. **DLO Maintenance Server**: Component responsible for revision maintenance and file grooming operations in the storage locations.
4. **DLO Dedupe Server**: Application server that facilitates deduplication by maintaining the Global Hash Table, which helps in identifying unique and duplicate data on the desktop agents.
5. **DLO Storage**: Backup destination where the endpoint data will be stored. Comprises of the DLO Storage Location and Dedupe Storage Location.
6. **DLO Database**: Component that maintains the application information. Comprises of the DLO DB and Dedupe DB.

   The BOI capability has been implemented with the introduction of two Server components - **DLO Edge Server** and **DLO IO Server** component. Please note that these two components are optional and need to be configured only when opting for the BOI capability. Similar to the other Server components, the Edge Server and IO Server components can be installed as a Standalone setup in the same machine or can be installed in a Distributed setup, across different server machines as well.

7. **DLO IO Server:** Application server residing within the corporate network, making the DLO resources accessible over internet.
8. **DLO Edge Server**: Component exposed to internet for front-ending the Application Servers.

In the BOI mode, the DLO Desktop Agent deployed on the user's endpoints, contacts the DLO Edge Server, which in turn contacts the DLO IO Server and DLO Dedupe Server for backup and restore operations. The communication from the DLO Agents to the DLO Edge Server happens over port 443 by default and can be reconfigured if required.

Prerequisites

Following are the prerequisites for the BOI capability:

System Requirements

Following are the minimum system requirements for running the DLO Edge Server.

Item	Description
Operating System	• Microsoft Windows Server 2016 (Standard, Data Center) • Microsoft Windows Server 2012, 2012 R2 - Update 2919355 (Standard, Data Center) • Microsoft Windows 2008 Server R2 SP1 (Standard, Enterprise, Data Center) • Microsoft Windows 2008 Server SP2 (Standard, Enterprise and 32-bit, 64-bit) • Windows Storage Server 2016 (Standard) • Windows Storage Server 2012, 2012 R2 (Standard) • Windows Storage Server 2008, 2008 R2 (Standard)
CPU	Quad Core
Processor	Xeon compatible
Memory	Minimum required: 8 GB RAM
Disk Space	500 MB free space

Following are the minimum system requirements for running the DLO IO Server.

Item	Description
Operating System	• Microsoft Windows Server 2016 (Standard, Data Center) • Microsoft Windows Server 2012, 2012 R2-Update 2919355 (Standard, Data Center) • Microsoft Windows 2008 Server R2 SP1 (Standard, Enterprise, Data Center) • Microsoft Windows 2008 Server SP2 (Standard, Enterprise and 32-bit, 64-bit) • Windows Storage Server 2016 (Standard) • Windows Storage Server 2012, 2012 R2 (Standard) • Windows Storage Server 2008, 2008 R2 (Standard)
CPU	Quad Core
Processor	Xeon compatible
Memory	Minimum required: 8 GB RAM
Disk Space	50 GB free space

Hardware Requirements

The following table summarizes the Hardware requirements for the DLO components based on the number of users for a standalone setup and distributed setup. Please note that a single IO Server can handle upto 16,000 users. For supporting more than 16,000 users, multiple IO Servers will be required.

Hardware requirements for Standalone Setup for BOI

Total Users	Administration Server, Maintenance Server, Database, Dedupe Server, Edge Server, IO Server	
	CPU	RAM
<=1000	64 Bit Quad Core Xeon, or compatible	12 GB
<=4000	64 Bit 8 Core Xeon, or compatible	32 GB
<=8000	64 Bit 16 Core Xeon, or compatible	32 GB
<=16000	64 Bit 16 Core Xeon, or compatible	48 GB
<=32000	64 Bit 16 Core Xeon, or compatible	48 GB
<=64000	64 Bit 16 Core Xeon, or compatible	64 GB
~100000	64 Bit 16 Core Xeon, or compatible	96 GB

Hardware requirements for Distributed Setup for BOI

In the following table the users count for DLO IO Server and DLO Edge Server are the **expected** number of roaming users.

Users	Administration Server		Dedupe Server		Maintenance Server		Database Server		Edge Server		IO Server	
	CPU	RAM	CPU	RAM	CPU	RAM	CPU	RAM	CPU	RAM	CPU	RAM
<=1000	32/64 Bit Dual Core Xeon, or compatible	8 GB	64 Bit Dual Core Xeon, or compatible	4 GB	32/64 Bit Dual Core Xeon, or compatible	8 GB	64 Bit Dual Core Xeon, or compatible	4 GB	64 Bit Quad Core Xeon, or compatible	4 GB	64 Bit Quad Core Xeon, or compatible	4 GB
<=4000	32/64 Bit Dual Core Xeon, or compatible	8 GB	64 Bit Quad Core Xeon, or compatible	4 GB	32/64 Bit Dual Core Xeon, or compatible	8 GB	64 Bit Quad Core Xeon, or compatible	4 GB	64 Bit Quad Core Xeon, or compatible	4 GB	64 Bit Quad Core Xeon, or compatible	4 GB
<=8000	32/64 Bit Dual Core Xeon, or compatible	8 GB	64 Bit 8 Core Xeon, or compatible	8 GB	32/64 Bit Dual Core Xeon, or compatible	8 GB	64 Bit 8 Core Xeon, or compatible	4 GB	64 Bit Quad Core Xeon, or compatible	4 GB	64 Bit 8 Core Xeon, or compatible	8 GB
<=16000	32/64 Bit Dual Core Xeon, or compatible	8 GB	64 Bit 16 Core Xeon, or compatible	8 GB	32/64 Bit Dual Core Xeon, or compatible	8 GB	64 Bit 16 Core Xeon, or compatible	8 GB	64 Bit 8 core Xeon, or compatible	8 GB	64 Bit 16 Core Xeon, or compatible	12 GB
<=32000	32/64 Bit Dual Core Xeon, or compatible	12 GB	64 Bit 16 Core Xeon, or compatible	12 GB	32/64 Bit Dual Core Xeon, or compatible	12 GB	64 Bit 16 Core Xeon, or compatible	12 GB	64 Bit 16 Core Xeon, or compatible	8 GB	-	-
<=64000	32/64 Bit Dual Core Xeon, or compatible	16 GB	64 Bit 16 Core Xeon, or compatible	16 GB	32/64 Bit Dual Core Xeon, or compatible	16 GB	64 Bit 16 Core Xeon, or compatible	16 GB	64 Bit 16 Core Xeon, or compatible	8 GB	-	-
~100000	32/64 Bit Dual Core Xeon, or compatible	32 GB	64 Bit 16 Core Xeon, or compatible	16 GB	32/64 Bit Dual Core Xeon, or compatible	32 GB	64 Bit 16 Core Xeon, or compatible	16 GB	64 Bit 16 Core Xeon, or compatible	8 GB	-	-

Port Requirements

The table provides details of the Port configuration for the DLO Server components and DLO Clients in a firewall environment, for the following three deployment scenarios:

- **Non BOI Deployment**: For organizations having endpoints that are always within the organization premises and are connected over the corporate network.
- **Exclusive BOI Deployment**: For organizations having endpoints that are always outside the corporate network and connect only using internet connection.
- **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.

Port Configuration for DLO Server Components

Process	Port	Port Type	Non BOI Deployment	Exclusive BOI Deployment	Occasional BOI Deployment
DLO Administration Service	3999	TCP/UDP	**Source (Outbound)**: DLO Administration Console **Destination (Inbound):** DLO Administration Server	**Source (Outbound)**: DLO Administration Console **Destination (Inbound):** DLO Administration Server	**Source (Outbound)**: DLO Administration Console **Destination (Inbound):** DLO Administration Server
SQL Server Browser	1434	UDP	**Source (Outbound)**: DLO Administration Server DLO Administration Console DLO Dedupe Server **Destination (Inbound):** SQL Server	**Source (Outbound)**: DLO Administration Server DLO Administration Console DLO Dedupe Server DLO IO Server DLO Edge Server **Destination (Inbound):** SQL Server	**Source (Outbound)**: DLO Administration Server DLO Administration Console DLO Dedupe Server DLO IO Server DLO Edge Server **Destination (Inbound):** SQL Server
SQL Server	1433 or dynamic port	TCP	**Source (Outbound)**: DLO Administration Server DLO Administration Console DLO Dedupe Server **Destination (Inbound):** SQL Server	**Source (Outbound)**: DLO Administration Server DLO Administration Console DLO Dedupe Server DLO IO Server DLO Edge Server **Destination (Inbound):** SQL Server	**Source (Outbound)**: DLO Administration Server DLO Administration Console DLO Dedupe Server DLO IO Server DLO Edge Server **Destination (Inbound):** SQL Server

Process	Port	Port Type	Non BOI Deployment	Exclusive BOI Deployment	Occasional BOI Deployment
File Sharing/ Browsing	135-139, 445	TCP/UDP	**Source (Outbound):** DLO Administration Server DLO Administration Console DLO Dedupe Server DLO Maintenance Server **Destination (Inbound):** Storage Location Dedupe Storage Location SQL Server*	**Source (Outbound):** DLO Administration Server DLO Administration Console DLO Dedupe Server DLO Maintenance Server DLO IO Server DLO Edge Server **Destination (Inbound):** Storage Location Dedupe Storage Location SQL Server* DLO Administration Server	**Source (Outbound)**: DLO Administration Server DLO Administration Console DLO Dedupe Server DLO Maintenance Server DLO IO Server DLO Edge Server **Destination (Inbound):** Storage Location Dedupe Storage Location SQL Server* DLO Administration Server
			** If default named pipes are used for SQL Server communication.*		
Dedupe Port	8443	HTTPS	**Source (Outbound):** DLO Administration Console **Destination (Inbound):** DLO Dedupe Server	**Source (Outbound):** DLO Administration Console **Destination (Inbound):** DLO Dedupe Server	**Source (Outbound):** DLO Administration Console **Destination (Inbound):** DLO Dedupe Server
Dedupe Port	8080	HTTP	**Source (Outbound):** DLO Administration Console **Destination (Inbound):** DLO Dedupe Server	**Source (Outbound):** DLO Administration Console **Destination (Inbound):** DLO Dedupe Server	**Source (Outbound):** DLO Administration Console **Destination (Inbound):** DLO Dedupe Server
Dedupe Port	8009	AJP	NA	**Source (Outbound):** DLO Edge Server **Destination (Inbound):** DLO Dedupe Server	**Source (Outbound):** DLO Edge Server **Destination (Inbound):** DLO Dedupe Server
Edge Server Port	443	HTTPS	NA	**Source (Outbound):** DLO Administration Console **Destination (Inbound):** DLO Edge Server	**Source (Outbound):** DLO Administration Console **Destination (Inbound):** DLO Edge Server
Edge Server Port	90	HTTP	NA	**Source (Outbound):** DLO Administration Console **Destination (Inbound):** DLO Edge Server	**Source (Outbound):** DLO Administration Console **Destination (Inbound):** DLO Edge Server
IO Server Port	7080	HTTP	NA	**Source (Outbound):** DLO Administration Console **Destination (Inbound):** DLO IO Server	**Source (Outbound):** DLO Administration Console **Destination (Inbound):** DLO IO Server

Process	Port	Port Type	Non BOI Deployment	Exclusive BOI Deployment	Occasional BOI Deployment
IO Server Port	7009	AJP	NA	**Source (Outbound):** DLO Edge Server **Destination (Inbound):** DLO IO Server	**Source (Outbound):** DLO Edge Server **Destination (Inbound):** DLO IO Server
Additional Ports for Push Installation	135, 1037, 441,1125	TCP	**Source (Outbound)**: DLO Administration Server DLO Administration Console **Destination (Inbound):** DLO Clients	NA	**Source (Outbound):** DLO Administration Server DLO Administration Console **Destination (Inbound):** DLO Clients

Port Configuration for DLO Clients

Process	Port	Port Type	Non BOI Deployment	Exclusive BOI Deployment	Occasional BOI Deployment
Edge Server Port	443	HTTPS	NA	**Source (Outbound):** DLO Clients Web Restore Machine **Destination (Inbound):** DLO Edge Server	**Source (Outbound):** DLO Clients Web Restore Machine **Destination (Inbound):** DLO Edge Server
File Sharing/ Browsing	135-139, 445	TCP/UDP	**Source (Outbound)**: DLO Clients **Destination (Inbound):** Storage Location Dedupe Storage Location	NA	**Source (Outbound)**: DLO Clients **Destination (Inbound):** Storage Location Dedupe Storage Location
Dedupe Port	8443	HTTPS	**Source (Outbound):** DLO Clients **Destination (Inbound):** DLO Dedupe Server	NA	**Source (Outbound):** DLO Clients **Destination (Inbound):** DLO Dedupe Server
Dedupe Port	8080	HTTP	**Source (Outbound):** DLO Clients **Destination (Inbound):** DLO Dedupe Server	NA	**Source (Outbound):** DLO Clients **Destination (Inbound):** DLO Dedupe Server
SQL Server Browser	1434	UDP	**Source (Outbound)**: DLO Clients **Destination (Inbound):** SQL Server	NA	**Source (Outbound)**: DLO Clients **Destination (Inbound):** SQL Server
SQL Server	1433 or dynamic port	TCP	**Source (Outbound)**: DLO Clients **Destination (Inbound):** SQL Server	NA	**Source (Outbound)**: DLO Clients **Destination (Inbound):** SQL Server

Certificate Requirements

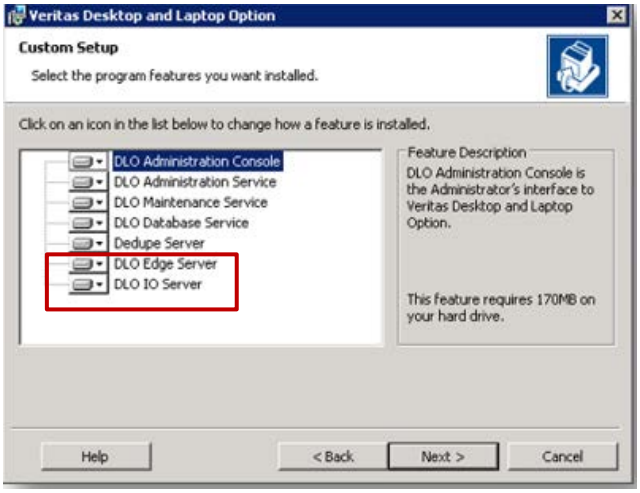
Ensure to have the SSL certificate (Issued to: zzz.domain.com) procured from a Trusted CA, for the Desktop Agents to communicate with the DLO Edge Server over a public URL.

***Note**: It is recommended to use an SSL certificate procured from a Trusted CA when deploying in production. By default, an inbuilt self-signed SSL certificate is also provided in the DLO installer package for customers wanting to evaluate the BOI capability.*

Installation of BOI Components

This section provides details on the installation of the BOI components.

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 components **DLO Edge Server** and **DLO IO Server** to be installed on the computer for the BOI capability.



***Note**: BOI Server components can be installed as a Standalone setup in the same machine or can be installed in a Distributed setup, across different server machines as well. It is recommended to install the DLO Edge Server on an independent Server machine.*

6. To install in a different directory, click **Change**.
7. Select the new directory and click **OK**.
8. Click **Next** and proceed to complete the installation.

Configuration of BOI Setup

An SSL certificate procured from a Trusted CA is a pre-requisite for configuring the BOI setup. This certificate is required for the Desktop Agents to communicate with the DLO Edge Server over a public URL. However, an inbuilt self-signed certificate is also provided in the DLO Installer package for customers wanting to evaluate the BOI capability.

Configuring the BOI setup has been categorized into two sections depending on the type of SSL certificate. It is recommended to opt for a trusted CA certificate when deploying in production and inbuilt self-signed certificate for customers wanting to evaluate the product before actual deployment.

Configure BOI using SSL certificate procured from a Trusted CA

This section elaborates on the steps to configure the BOI setup when using an SSL certificate procured from a Trusted CA. These steps can be followed when configuring the DLO BOI setup for a production environment.

1. Register a Public IP for the DLO Edge Server.
2. Map the SSL certificate to the Registered Public IP.
3. Map the DLO IO Server to the DLO Storage Location.
4. Update the DLO Desktop Agents with SSL Certificate.
5. Test Connectivity to the DLO Edge Server.
6. Enable the BOI option in a Profile.

Step 1 – Register a Public IP for the DLO Edge Server

Register a public IP for the DLO Edge Server, so that the desktop agents will be able to access the DLO Edge Server over internet.

***Note**: Once the administrator registers the public IP for the DLO Edge Server, the DLO Edge Server needs to be deployed. Below are listed few options on how the DLO Edge Server can be deployed:*

- *Through NAT (Dynamic or static) configured on the firewall.*
- *The DLO Edge Server can reside in Demilitarized zone (DMZ).*
- *Through a Reverse Proxy Server in Demilitarized zone (DMZ) which would redirect all the DLO Agent requests to the DLO Edge Server (residing in the corporate network).*

Step 2 – Map the SSL Certificate to the Registered Public IP

1. Bind the SSL certificate to the URL.
   E.g.: https://zzz.domain.com
   where **zzz.domain.com** is the **Issued to** field for the Server Certificate procured from the Trusted CA.
   ***Note**: In some cases, the SSL Server Certificate chain may need to be created manually. For more details on how to create the Server Certificate Chain for the SSL certificate, refer Creating the SSL Server Certificate Chain.*

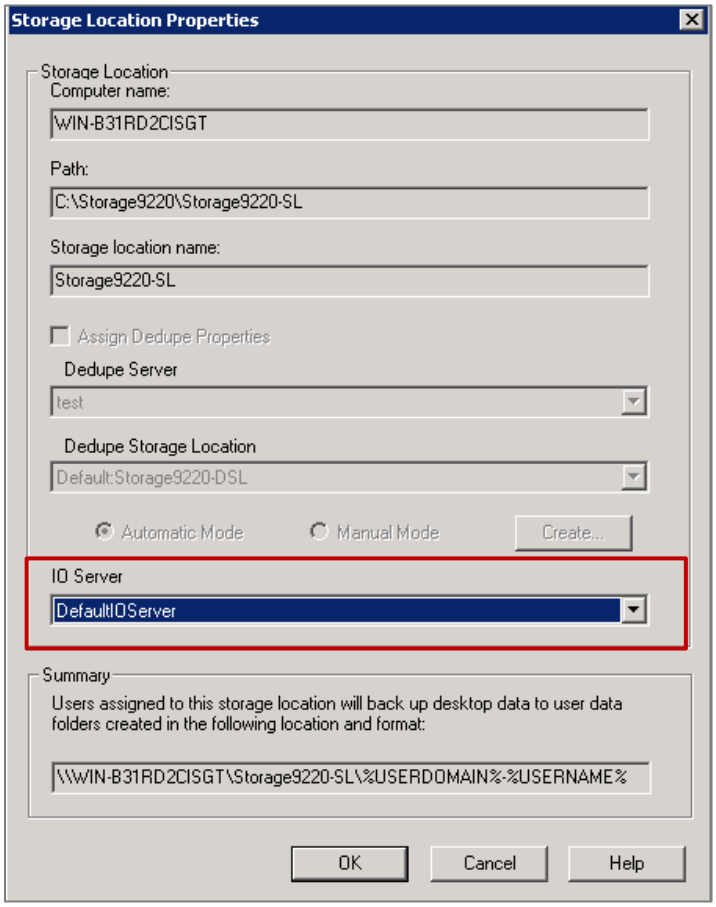
2. Map the SSL certificate (Issued to: zzz.domain.com) to the registered public IP (of DLO Edge Server) either:
   a. In the Domain Name Server (DNS)
      Or
   b. As a Host entry update in the DLO Edge Server machine.
      ***Note**: If this is a host entry update on the DLO Edge Server, additionally on the Desktop Agent machines, update the host file as below:*
      - *Map the **Certificate Name** to the **Public IP***
        - *where the **Certificate Name** is the **SERVERNAME** entry in the **EdgServer.ini** file present in the path <Install Path>\Veritas DLO\DLO*
        - *where the **Public IP** is the Public IP of the DLO Edge Server*

      E.g.: <Registered Public IP> zzz.domain.com

Step 3 – Map the DLO IO Server to the DLO Storage Location

The DLO IO Server can be mapped to the DLO Storage location either while creating a new storage location or by updating properties of an existing Storage location as below

- **Storage Locations Properties > IO Server**



Step 4 – Update the DLO Desktop Agents with SSL Certificate

The Desktop Agents can be updated with the SSL certificate by pushing the SSL certificate information to the desktop agents as follows:

1. For the SSL certificate issued by a trusted CA, place the chained Server certificate (*dloserver_new.crt - as created in* Creating the SSL Server Certificate Chain) and the Private key file for Server in a folder in the DLO Administration Server machine. Make sure no other .crt files are present in this location.
2. Backup and remove any existing .crt files from the location "*C:\Program Files\Apache Software Foundation\Apache24\Conf\SSL*" in the DLO Edge Server machine.
3. In the DLO Administration Console, on the DLO navigation bar, click **Setup**.
4. In the **Settings** pane, right-click **Edge Server**, and select **Edit Edge Server**.
5. Click **Browse** and select the chained Server Certificate (*dloserver_new.crt*) from the folder created in Step 1.
6. Click **Push Certificate**.
7. Click **OK**.

Please note that only the Desktop Agents that are online in the corporate network (Non-BOI mode) will be updated with the SSL certificate. In case of scenarios like Exclusive BOI deployments, where endpoints will not be connected to the corporate network, the following additional steps need to be performed from the desktop agent side for updating the web certificate information.

a. Login to Web Restore using the DLO Edge Server URL *https://<Edge_Server_URL>* on the Desktop Agent machine.
b. The '**Server Certificate'** option in the left pane provides the option to download the **Server certificate** and **EdgeServer.ini** file.
c. Download these files and move them to the Veritas DLO Install Path *<Install Path>\Veritas DLO\DLO.*

Step 5 – Test Connectivity to the DLO Edge Server

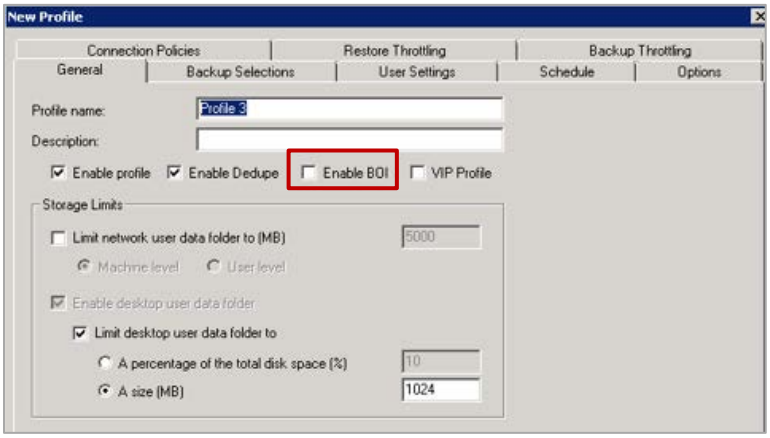
Test the connectivity to the DLO Edge Server by accessing the below URL from any machine with internet connection.

- https://<Edge_Server_URL>

Step 6 – Enable the BOI option in a Profile

The BOI option can be enabled either in an existing profile or while creating a new profile as follows

- **Profile > General** > **Enable BOI**



If this is a new profile, the BOI enabled profile can be assigned to the users either manually or using the automated user assignment.

Configure BOI using the Inbuilt Self-Signed Certificate

This section elaborates on the steps to configure the BOI setup when using the inbuilt self-signed certificate available with the DLO Installer package. These steps can be followed when configuring the DLO BOI setup for customers wanting to evaluate the product before actual deployment.

1. Register a Public IP for the DLO Edge Server.
2. Map the SSL certificate to the Registered Public IP.
3. Map the DLO IO Server to the DLO Storage Location.
4. Test Connectivity to the DLO Edge Server.
5. Enable the BOI option in a Profile.

Step 1 – Register a Public IP for the DLO Edge Server

Register a public IP for the DLO Edge Server, so that Desktop Agents will be able to access the DLO Edge Server over internet.

***Note**: Once the administrator registers the public IP for the DLO Edge Server, the DLO Edge Server needs to be deployed. Below are listed few options on how the DLO Edge Server can be deployed:*

- *Through NAT (Dynamic or static) configured on the firewall.*
- *The DLO Edge Server can reside in Demilitarized zone (DMZ).*
- *Through a Reverse Proxy Server in Demilitarized zone (DMZ) which would redirect all the DLO Agent requests to the DLO Edge Server (residing in the corporate network).*

Step 2 – Map the SSL certificate to the Registered Public IP

Map the SSL certificate (Issued to: dlo.veritas.com) to a registered public IP (of DLO Edge Server) either:

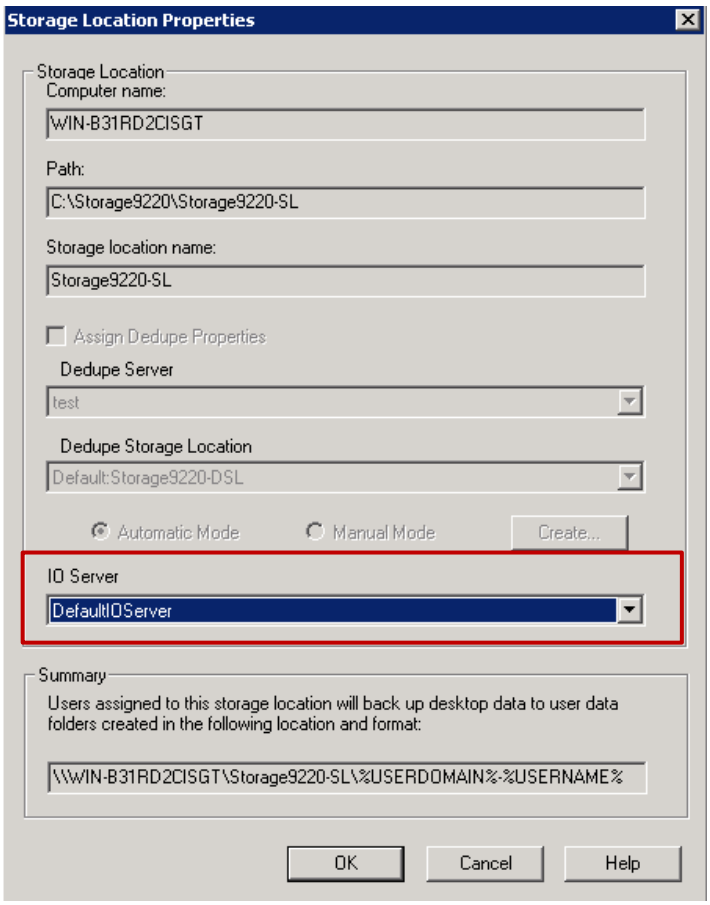
a. In the Domain Name Server (DNS)
   Or
b. As a Host entry update in the DLO Edge Server machine.
   ***Note**: If this is a host entry update on the DLO Edge Server, additionally on the Desktop Agents machine, update the host file as below:*
   - *Map the **Public IP** to the **Certificate Name***
     - *where the **Public IP** is as present in the **SERVERNAME** entry of the **EdgeServer.ini** file present in the path <Install Path>\Veritas DLO\DLO)*
     - *where the **Certificate Name** is for the DLO Edge Server. **(Issued to: dlo.veritas.com)***

     E.g.: <Registered Public IP> dlo.veritas.com

Step 3 – Map the DLO IO Server to the DLO Storage Location

The DLO IO Server can be mapped to the DLO Storage location either while creating a new storage location or by updating properties of an existing Storage location as below

- **Storage Locations Properties > IO Server**



Step 4 – Test Connectivity to the DLO Edge Server

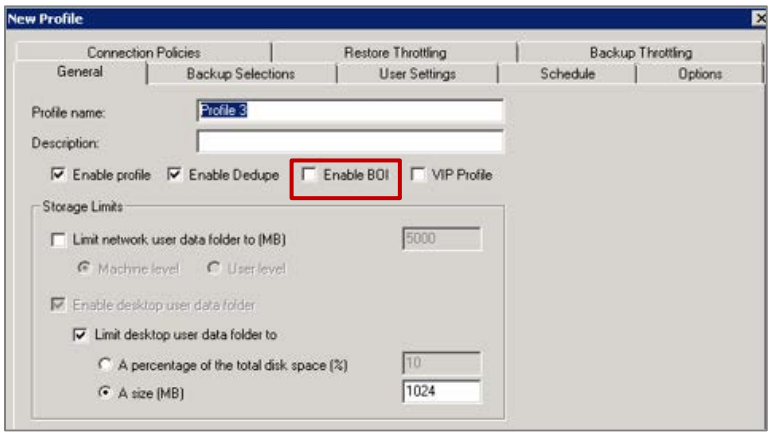
Test the connectivity to the DLO Edge Server by accessing the below URL from any machine with internet connection.

- https://<Public_Edge_Server_IP>

Step 5 – Enable the BOI option in a Profile

The BOI option can be enabled either in an existing profile or while creating a new profile as follows

- **Profile > General** > **Enable BOI**



If this is a new profile, the BOI enabled profile can be assigned to the users either manually or using the automated user assignment.

Supporting Section on SSL Server Certificate

Procuring the SSL Certificate from a Trusted CA

To procure the SSL certificate from a Trusted CA, a **Certificate Signing Request (CSR)** is required. In case the administrator is purchasing SSL certificate for a production server, please consult the Network team of the organization to understand the policies if any and get the relevant information for the CSR file.

The CSR includes information that is added to the SSL certificate. During the CSR creation, a **public private key pair** is also generated. This private key is added to a private key file (.key) and the public key is added to the CSR. The private key file should be kept secure.

The **Openssl command** as below can be used for generating the CSR and a private key file. In the following example the **sslCSR.csr** is the CSR and **privateKey.key** is the private key file.

openssl req -out sslCSR.csr -new -newkey rsa:2048 -nodes -keyout privateKey.key -days 365

Creating the SSL Server Certificate Chain

The list of SSL certificates, from the root certificate to the end-user certificate, represents the **SSL Certificate Chain.**

Note*: In this example the end user certificate is represented by the Server certificate file for the DLO Edge Server.*

Prerequisites

The files mentioned below are required to create the Server certificate chain (Components of CA issued certificate):

- Server certificate file (PEM-encoded X.509 with .crt extension).
- Intermediate chain certificates (if any) for the server certificate (PEM-encoded X.509 with .crt extension).
- Root certificate for the server certificate (PEM-encoded X.509 with .crt extension).

To create a .crt file that represents the SSL Server Certificate chain, place all the certificates in the following order - end-user certificate, followed by Intermediate chain certificates and then the Root certificate. In the following example, four certificates represent the SSL Server certificate chain:

Certificate Chain	Certificate Name	Issued to	Issued by	Certificate Content
Server Certificate (end user certificate)	dloserver.crt	zzz.domain.com	Intermediate Example-2 CA	-----BEGIN CERTIFICATE------ <Server Certificate Content> -----END CERTIFICATE-----
Intermediate certificate 2	dloint_2.crt	Intermediate Example-2 CA	Intermediate Example-1 CA	-----BEGIN CERTIFICATE----- <Intermediate Certificate 2 Content> -----END CERTIFICATE-----
Intermediate certificate 1	dloint_1.crt	Intermediate Example-1 CA	Chief Root CA	-----BEGIN CERTIFICATE----- <Intermediate Certificate 1 Content> -----END CERTIFICATE-----
Root Certificate	dloserverCA.crt	Chief Root CA	Chief Root CA	-----BEGIN CERTIFICATE----- <Root Certificate Content> -----END CERTIFICATE-----

The **dloserver_new.crt** file that represents the Server Certificate Chain should have the below content:

Content in dloserver_new.crt
-----BEGIN CERTIFICATE----- <Server Certificate Content> -----END CERTIFICATE------ -----BEGIN CERTIFICATE----- <Intermediate Certificate 2 Content> -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- <Intermediate Certificate 1 Content> -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- <Root Certificate Content> -----END CERTIFICATE-----

Troubleshooting BOI

This section includes the details for troubleshooting the issues observed in BOI setups.

In case any issues are observed in the BOI setup, the administrator needs to run the Veritas DLO Diagnostic Utility first on the DLO Server setup and resolve the issues using the available help.

If the issue still persists then

- For endpoints that are connected in a domain, run the diagnostic utility on the desktops agents and resolve the issues using the available help.
- For endpoints that are connected in a workgroup, check the **DLO Webclient.log** and **DLOClient.log** file present in the path ***<%localappdata%>\Veritas\DLO\.settings*** on the desktop agent machine.

Below is the list of possible issues observed in a BOI setup

Push Certificate from the DLO Administration Console fails

This issue occurs when the administrator does a **Push Certificate** (for a trusted CA certificate) to notify the desktop agents either while configuring the BOI Server components or post the BOI configuration when the administrator is switching from a default self-signed certificate to an SSL certificate (procured from a Trusted CA).

This issue occurs if the SSL certificate procured from a Trusted CA is generated using RSASSA-PSS algorithm with OpenSSL versions prior to Openssl v 1.1.0f. This issue is due to changes in Openssl v 1.1.0f. As the RSASSA-PSS algorithm is obsolete, the support for this algorithm is removed in this version of OpenSSL.

How to confirm the issue?

- Error Message seen in the DLO Administration Console during **Push Certificate** is *"Push Certificate failed"*.
- On the machine where DLO Edge Server is installed, the DLO Edge Server Service will be in the **Stopped** state.

Steps to resolve the issue:

If DLO Edge Server certificate is signed with RSASSA-PSS algorithm, the certificates need to be renewed with the latest algorithm. All intermediate certificates in the Server certificate chain should also be updated with the latest algorithm.

In case the administrator is able to update only the Server certificate and not the intermediate certificates in the Server certificate chain, as a workaround follow the below steps:

For Fresh Configuration:

1. Update the Server certificate with the latest algorithm on the DLO Administration Server machine.
2. Take a backup of the chained Server certificate file and the Private key files (.crt and .key) from the path "C:\Program Files\Apache Software Foundation\Apache24\Conf\SSL" in the DLO Edge Server machine.
3. Remove the chaining in the chained Server certificate file residing in the Install Path of the DLO Edge Server machine.
4. Start the **DLO Edge Server** service.
5. On the DLO Administration Server machine, verify the name of the existing .pem file in the path *<Install Path>\Veritas DLO\DLOAgent\Certificates.*
    - If there is a dloclient.pem file only, delete the dloclient.pem file and rename the backed up file(server.crt in Step 2) as dloclient.pem file.
    - If there is a dloclient.pem and servercert.pem file, delete the servercert.pem file, rename the backed up file(server.crt) in Step 2 as servercert.pem file.
6. The .pem file needs to be updated on the DLO Administration Console machine in the below paths:
    - *<Install Path>\Veritas DLO\DLOAgent\Certificates*
    - *<Install Path>\Veritas DLO\DLOAgent.zip\Certificates*
7. The .pem file needs to be updated on the DLO Desktop Agent machines either manually or using the Web Restore option in the below path:
    - *<Install Path>\Veritas DLO\DLO*

For Upgrade Scenarios:

1. Update the Server certificate with the latest algorithm.
2. Remove the chaining in the certificates.
3. Start the **DLO Edge Server** service.
4. Do not push the certificate.

Login failures observed on the Web Restore UI

This issue is observed when the user is not able to login to the web restore UI.

Error observed in the Web restore console: *Configuration failed*

Steps to resolve the issue:

1. On the DLO IO Server machine, browse to the path *<InstallPath>**IOServer**Tomcat**webapps**DLOServer**META-INF*, verify the **serverName** and **instanceName** entries in the *context.xml* file are correct where
    - **serverName** should be the SQL server name
    - **instanceName** should be the SQL server instance which is in use by DLO.
2. Restart the **Veritas DLO Web Server** service.
3. Refresh the Web restore page and login using the user credentials.

Desktop Agents in offline mode in BOI Setup

When the Desktop Agents are in the offline mode, the administrator as a first step should run the Veritas DLO Diagnostic Utility on the DLO Edge Server machine and check the Summary to understand the problems at hand. In case there are no issues reported as per the diagnostic utility, the administrator should check the **DLOWebClient.log** file present in DLO Desktop Agent machine for further troubleshooting.

Errors reported in the Veritas DLO Diagnostic Tool

Based on the results of the DLO Diagnostic tool, the administrator needs to resolve the issues using the available help (*Click Here option*). Below are listed few cases where the desktop agents are in offline mode and the troubleshooting steps for the same is covered in the ***Troubleshooting Section for Desktop Agents in offline mode***.

- SSL Server Certificate for the DLO Edge Server expired
- Incorrect Server Certificate Chain
- DLO Edge Server configured on a machine with dual network adapters

Error reported in the DLO WebClient.log

In case the DLO diagnostic utility reports no errors, proceed to check the **DLO WebClient.log** file present in the path ***%localappdata%\Veritas\DLO\.settings*** in the Desktop Agent machine.

Following is the error observed when the Desktop Agents are in offline mode and the troubleshooting steps for the same is covered in ***Troubleshooting Section for Desktop Agents in offline mode***.

[Error],"WebServerRequest::RunWebRequest: curl error code = 60; curl error message = SSL certificate problem: unable to get local issuer certificate"

Troubleshooting Section for Desktop Agents in offline mode

This section details out the troubleshooting steps for the different cases discussed earlier where the Desktop Agents go to the offline mode in BOI setup.

SSL Server Certificate for the DLO Edge Server expired

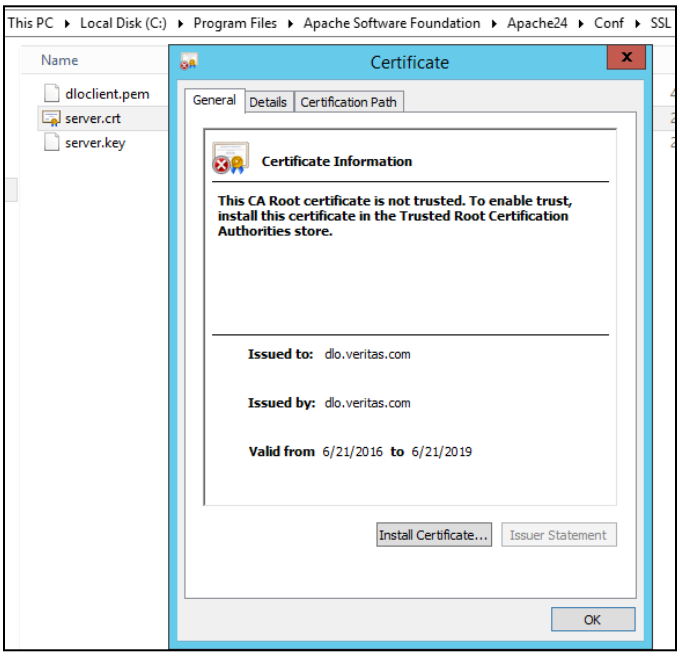
How to confirm the issue?

Error seen in the Diagnostic tool is: ***Edge Server not available***

Steps to resolve the issue:

1. Check if the SSL certificate used for DLO Edge Server has expired**.**

   Note*: To check the certificate validity, double click on the SSL certificate to check the validity.*



   Default DLO Edge Server SSL certificate validity

   - *Until 8.0 SP3, the default self-signed certificate comes with 1-year validity.*
   - *From 8.0 SP4 onwards the self-signed certificate comes with 3-year validity.*

2. Renew the expired SSL certificate.

   ***Note**: If this is a default self-signed SSL certificate that has expired, the administrator may choose to use the new default self-signed SSL certificate that is available with the upgraded DLO release package. In the upgraded setup, the self-signed SSL certificate will be present in the installer package. From the Installer package, extract the issued self-signed certificate from the **Edgeserver1.cab** file. In this cab file, search for "*server" to get **server.crt** and **server.Key** file.*

3. From the DLO Administration Console, push the updated SSL certificate to notify the Desktop Agents. For more details on the steps, refer Update the DLO Desktop Agents with SSL Certificate.

Incorrect Server Certificate Chain

How to confirm the issue?

Error seen in the diagnostic tool:

Edge Server not available: SSL certificate problem: Unable to get local issuer certificate

Steps to resolve this issue:

1. Check if SSL Server certificate chain for the DLO Edge Server has missing certificates, extra certificates or incorrect certificate order. For more details on how to create a Server certificate chain, refer Creating the SSL Server Certificate chain.

2. Once the SSL Server certificate chain issues are resolved, from the DLO Administration Console push the updated certificate to notify the desktop agents. For more details, refer Update the DLO Desktop Agents with SSL Certificate.

DLO Edge Server configured on a machine with dual network adapters

In case the DLO Edge Server is configured on a machine with dual network adapters (public IP and private IP) and the primary network adapter is allocated with the Private IP of the DLO Edge Server, the DLO Desktop Agent goes into the offline state.

How to confirm the issue?

On the DLO Edge Server machine, the **Edge server.ini** file contains private IP address of the DLO Edge server, though there is a public IP allocated to the DLO Edge Server.

Error seen in the diagnostic tool: ***Edge Server not available***

Steps to resolve this issue:

1. On the DLO Administration Server, browse to *<InstallPath>\Veritas\Veritas DLO\DLOAgent* and modify the "**SERVERNAME**" in **EdgeServer.ini** with Public IP of the DLO Edge Server.
2. On the DLO Administration Server, browse to *<InstallPath>\Veritas\Veritas DLO\DLOAgent\DLOAgent.zip\DLOAgent* and modify the **EdgeServer.ini** file with Public IP of the DLO Edge Server.
3. For this information to be updated on the DLO Desktop Agent machines:
    a. Take a backup of original **EdgeServer.ini** and **.pem** certificate file present in the DLO Desktop Agent Install path i.e. *<InstallPath>\Veritas\Veritas DLO\DLO*
    b. Access the Web restore page i.e. https://<EdgeServer name/IP>:443
    c. Download the **certificate (.pem)** and **EdgeServer.ini** file and copy them in the Agent install path.

[Error],"WebServerRequest::RunWebRequest: curl error code = 60; curl error message = SSL certificate problem: unable to get local issuer certificate"

The above error indicates that there is some issue with respect to the certificate.

How to confirm the issue?

1. To confirm that the issue is with the SSL certificate:
    a. View the SSL certificate by double clicking on it.
    b. Check the certificate's hierarchy levels of trust in the "**Certification Path**" tab in SSL cert. In practice, a typical SSL certificate hierarchy includes
        i. End user certificate (in this case Server certificate).
        ii. Intermediate CA
        iii. Root CA
    c. Once the hierarchy levels are confirmed, open the SSL certificate with any editor and check the number of "Begin" and "End Certificate" pairs in it. The number of "Begin", "End" pairs should match with the hierarchy level count as present in certification path of certificate.

For example, if the hierarchy level count in SSL certificate is 3 i.e. contains root CA, intermediate CA and the end user -server certificate, then the number of "Begin", "End" certificate pairs in the SSL certificate (can be viewed from an editor) should also be 3.
Usually the mismatch scenario would include one single "Begin", "End" pair in SSL certificate, which would be the DLO Edge server certificate whereas the certification path of certificate will contain multiple hierarchy levels.

Steps to resolve the issue:

1. Double click on the certificate
    - Go to **Certification Path**
    - Click on any intermediate CA certificate, which is just above the end user certificate.
2. **View Certificate** button will be highlighted at the bottom of the **Certification Path** section.
    - Click on **View Certificate**.
    - Go to the **Details** tab and click on **Copy to File...** button
3. In the certificate export wizard
    - Click **Next**
    - Select the **Export file format** as **Base_64 encoded X.509 (.CER)**
    - Click **Next**
4. Browse and select the destination where the file needs to be exported and click **Next >Finish**.
5. Repeat **Steps 1 to 4** till the root CA certificate (including the root CA).
6. Open the first **.CER** certificate that was exported; copy the content in it (from BEGIN to END).
7. Open the SSL certificate from an editor and copy the content of exported certificate (FROM Step 6) right after the "END CERTIFICATE" in SSL certificate. Repeat this for all other certificates that were exported till the root CA.
   ***Note**: The above steps will ensure that the SSL certificate has proper hierarchy levels chained together.*
8. Once the updated SSL certificate is ready, push this certificate from DLO Administrator console to update the new certificate across all the desktop agents.
9. Desktop Agents working out of the corporate network and connected to any private network should come online either by connecting to corporate network or by downloading the updated certificate from the web restore page. The same should be copied into the DLO Agent Install directory (copy both .ini file and .pem file).

Frequently asked questions (FAQs)

What is the maximum number of users that can be supported through BOI in a DLO deployment?

Every DLO IO Server can handle up to 16000 users. In case more than 16000 users need to be supported, it is recommended to configure multiple IO servers and have the required configuration as specified in the Hardware requirements.

How to identify the connectivity issues with BOI?

Following are few URL's to check the DLO Edge Server and DLO IO Server status:

1. https://<DLO Edge Server IP (or) hostname>
   Verifies if the DLO Edge Server and DLO IO Server machines are reachable. On successful access, the web restore page appears.

2. https://<DLO Edge Server IP (or) hostname>/DLOServer/rest1/DefaultIOServer/status/
   Verifies connectivity to DLO IO Server via the DLO Edge Server.

3. http://<Edge Server IP (or) hostname>:7080/DLOServer/rest1/operations/status
   Verifies connectivity to DLO IO Server (this is the direct connectivity check to the DLO IO Server)

4. https://<Edge Server IP (or hostname>/DedupeServer/rest/dedupeManager/checkServerStatus/
   Verifies the DLO Dedupe Server connectivity via DLO Edge Server.

In addition to this, the DLODiagnosticUtility.exe present in the DLO Server Install path can be used to identify the connectivity issues of the DLO Dedupe Server, DLO IO Server and DLO Edge Server. Also ensure the .PEM file present in DLO Agent install path and certificate chain on the DLO Edge Server are appropriate.

How to change Server certificates on the DLO Edge Server?

This can be done using the **Edit Edge Server** option in the DLO Console. Browse to the path with the updated files mentioned below and use the **Push certificate** option.

- PEM-encoded private key file for the Server (with .key extension)
- PEM-encoded X.509 certificate data file (with .crt extension)

***Note**: It is recommended to use the **Push certificate** option available in the DLO Administration Console and not to change the certificates manually.*

How to enable verbose logging for the DLOWebclient.log file?

To enable the verbose logging for the DLOWebclient.log file, following are the registry changes:

[HKEY_CURRENT_USER\SOFTWARE\Veritas\Veritas DLO\Logger]

"ThresholdLevel"="4"

"FileSize"="100"

"BackupFileCount"="50"

"LogCmpression"="1"

***Note**: ThresholdLevel can be set to 4 (Trace and Debug) or 5 (Debug).*

Can wild card certificates be pushed from the DLO Console?

No. They cannot be pushed directly. Some manual steps need to be performed. Please refer TechNote TECH3916560 for more details: https://www.veritas.com/support/en_US/article.000126987

Can DER format certificate be used as a Server Certificate?

No**.**

How to configure more than the default number of users (4000) for BOI deployment using a single IO Server?

The maximum number of users supported by a single IO Server is 16,000. By default, 4000 users are supported in the Exclusive BOI deployment.

In order to modify the default value to the maximum value, where maxUsers is 16000, the following configuration parameters of DLO Edge Server, DLO IO Server(s) and DLO Dedupe Server(s) needs to be updated.

1. **DLO IO Server changes**

   DLO supports multiple IO Servers. In case of more than 16,000 users, multiple IO Servers should be deployed for better performance. For each IO Server, execute below request in the browser where **maxUsers** is the maximum number of users the given IO Server will handle.

   maxUsers= 16000

   ```
   http://<IOServer_IP>:<http_port>/DLOServer/rest1/operations/configureRequestScale/{maxUsers}/
   ```

   ```
   Ex:
   http://172.28.16.10:7080/DLOServer/rest1/operations/configureRequestScale/16000/
   ```

   ***Note:** This request is restricted to work within LAN network over http port.*

2. **DLO Dedupe Server changes**

   For each DLO Dedupe Server, execute below request in the browser where **maxUsers** is the number of users given Dedupe Server will handle.

   ```
   http://<DedupeServer_IP>:<http_port>/DedupeServer/rest/dedupeMana
   ger/configureRequestScale/{maxUsers}/
   ```

   ```
   Eg:
   http://172.28.16.10:8080/DedupeServer/rest/dedupeManager/configur
   eRequestScale/16000/
   ```

   Note: *This request is restricted to work within LAN network over http port.*

3. **DLO Edge Server changes**
   a. Calculate the ThreadLimit as below.

      set ThreadLimit = **maxUsers***0.16

      if ThreadLimit is greater than 15,000 then set ThreadLimit = 15,000

   b. Update the below content in the file "C:\Program Files\Apache Software Foundation\Apache24\Conf\extra\httpd-mpm.conf" for parameters **ThreadLimit** and **ThreadsPerChild**.

      # WinNT MPM

      # ThreadsPerChild: constant number of worker threads in the server process

      # MaxConnectionsPerChild: maximum number of connections a server process serves

      <IfModule mpm_winnt_module>

        ThreadLimit 2000

        ThreadsPerChild 2000

        MaxConnectionsPerChild 0

        AcceptFilter http none

        AcceptFilter https none

      </IfModule>