Veritas™ Desktop and Laptop Option 9.3

Domain Trust Independent Solution- Installation and Configuration

VERITAS

Introduction

Veritas Desktop and Laptop Option can now be deployed as a Domain Trust Independent Solution.

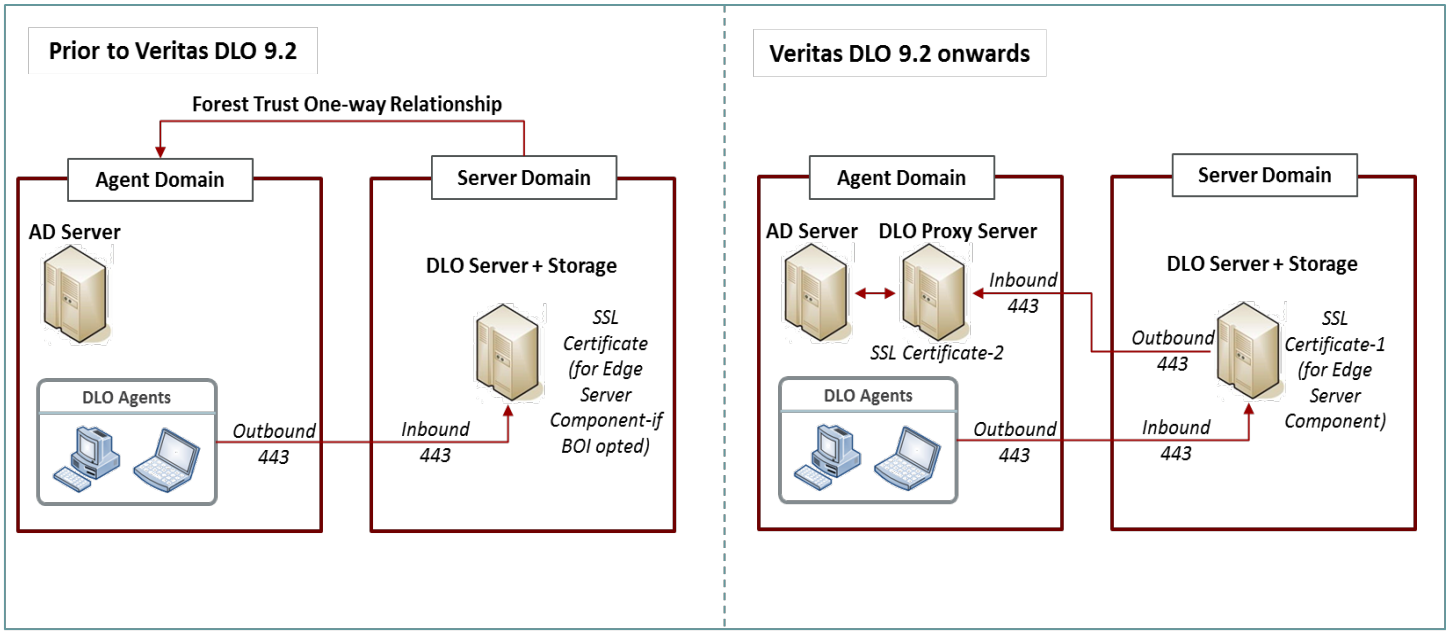
This document provides the details for an administrator to Install and Configure the Veritas Desktop and Laptop Option as a Domain Trust Independent Solution. This document is intended for organizations that want to deploy the Server and Agents across different domains with no trust relationship established between them.

Prior to the Veritas DLO 9.2 version, the DLO agents and DLO Server components had to be deployed on the same domain or if deployed on different domains, needed a one-way forest trust relationship to be established from the Server domain to the Agent domain.

With the Veritas DLO 9.2 version, this pre-requisite of domain trust is being overcome through the DLO Proxy Server component, which facilitates DLO operations even across domains that do not have a trust established between them.

Domain Trust Independent DLO is supported only in the Backup Over Internet (BOI) mode.

Architecture Overview



Domain Trust Independent Solution has been implemented with the introduction of a **DLO Proxy Server** component. DLO Proxy Server needs to be installed on the Agent Domain and acts as an intermediary between the DLO Server (Server Domain) and Active Directory (Agent Domain) to perform all necessary Active Directory calls. The communication between DLO Proxy Server and DLO Server happens over Port 443 by default, but can be reconfigured if required.

Prerequisites

Prerequisites for setting up the Domain Trust Independent DLO are:

- System Requirements
- Port Requirements
- Certificate Requirements

System Requirements

Following are the minimum system requirements for the DLO Proxy Server. Ensure that the Operating Systems are updated with the latest Service Packs. The DLO Proxy Server can be installed on a Server or Desktop class machine.

Item	Description
Operating System	■ Microsoft Windows Server 2016 (Standard, Enterprise, Data Center) ■ Microsoft Windows Server 2012, 2012 R2 - Update 2919355 (Standard, Enterprise, Data Center) ■ Microsoft Windows 2008 Server R2 SP1(Standard, Enterprise, Data Center)) ■ Microsoft Windows 2008 Server SP2 (Standard, Enterprise and 32-bit, 64-bit) ■ Microsoft Windows 10 with Version 1803, 1709, 1703, 1607, 1511 and 1507. ■ Microsoft Windows 8 and 8.1(with Update 1) ■ Microsoft Windows 7 SP1(32-bit and 64-bit)
CPU	Quad Core
Processor	Xeon compatible
Memory	Minimum required: 4 GB RAM
Disk Space	350 MB free space

Port Requirements

For a Domain Trust Independent DLO, in addition to the existing port configurations, port 443 needs to be opened between:

- DLO Administration Console and the DLO Proxy Server
- DLO IO Server and the DLO Proxy Server

Port 443 is the **Inbound port for the DLO Proxy Server** and **Outbound port for DLO Administration Console and DLO IO Server**.

Refer to following table for the Port Requirements for Domain Trust Independent DLO:

Port Requirements for Domain Trust Independent DLO			
Services or Process	**Default Ports**	**Port Type**	**Source(Outbound) And Destination(Inbound)**
Proxy Server	443	HTTPS	**Source**: IO Server, DLO Administration Console **Destination**: DLO Proxy Server
File sharing/Browsing	135-139	TCP/UDP	**Source**: IO Server, Maintenance Server, DLO Administration Server, DLO Administration Console and Dedupe Server. **Destination**: Storage Location and Dedupe Storage Location Machine.
File sharing/Browsing	445	TCP/UDP	**Source**: IO Server, Maintenance Server, DLO Administration Server, DLO Administration Console and Dedupe Server. **Destination**: Storage Location and Dedupe Storage Location Machine.
SQL	1434	TCP/UDP	**Source**: IO Server, Dedupe Server, DLO Administration Server, DLO Administration Console. **Destination**: SQL Server.
SQL Server	1433 or dynamic port	TCP	**Source:** IO Server, Dedupe Server, DLO Administration Server, DLO Administration Console. **Destination:** SQL Server
Dedupe Port	8443	HTTPS	**Source**: DLO Administration Console. **Destination**: Dedupe Server.
Dedupe Port	8080	HTTP	**Source**: DLO Administration Console. **Destination**: Dedupe Server
Dedupe Port	8009	AJP	**Source**: Edge Server **Destination**: Dedupe Server
Edge Server Port	443	HTTPS	**Source**: Clients and Web restore machine, DLO Administration Console. **Destination**: Edge Server
Edge Server Port	90	HTTP	**Source**: DLO Administration Console **Destination**: Edge Server
IO Server Port	7080	HTTP	**Source**: DLO Administration Console **Destination**: IO Server
IO Server Port	7009	AJP	**Source**: Edge Server **Destination**: IO Server
DLO Administration Service	3999	TCP/UDP	**Source**: DLO Administration Console **Destination**: DLO Administration Server

Certificate Requirements

1. Ensure the following components are exposed to public internet using SSL certificate.
    a. DLO Proxy Server in Agent Domain**.**
    b. DLO Edge Server in Server Domain.
2. A Client certificate, for communication from the DLO Server (Server Domain) to the DLO Proxy Server (Agent domain).

The administrator can choose to purchase the required SSL Certificates from a Trusted Certificate Authority (CA) or could generate Self-signed certificates. To generate Self-signed SSL certificates, refer to section Generation of Self-signed certificates. In case, the administrator procures the SSL certificate from a Trusted CA, ensure the SSL certificates are properly chained. For more details, refer to FAQs for Certificate Requirements.

Note:

- It is recommended to use the SSL certificate issued from a Trusted Certificate Authority.
- Veritas DLO 9.3 is bundled with a self-signed Server Certificate (server.crt).

Generation of Self-signed certificates

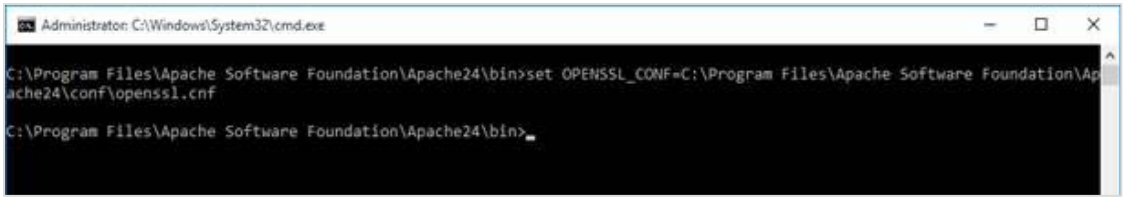
Generate a Self-signed Client certificate to be used for establishing communication between the DLO Server (Server Domain) and DLO Proxy Server (Agent Domain).The generated Client certificate should be in .**p12** format.

Prerequisites:

- Apache Service should be installed on the machine where the certificate will be generated.
- Commands should be run using an elevated command prompt from the openssl path (C:\Program Files\Apache Software Foundation\Apache24\bin)
  Note: Ensure to provide valid details while creating the certificate.

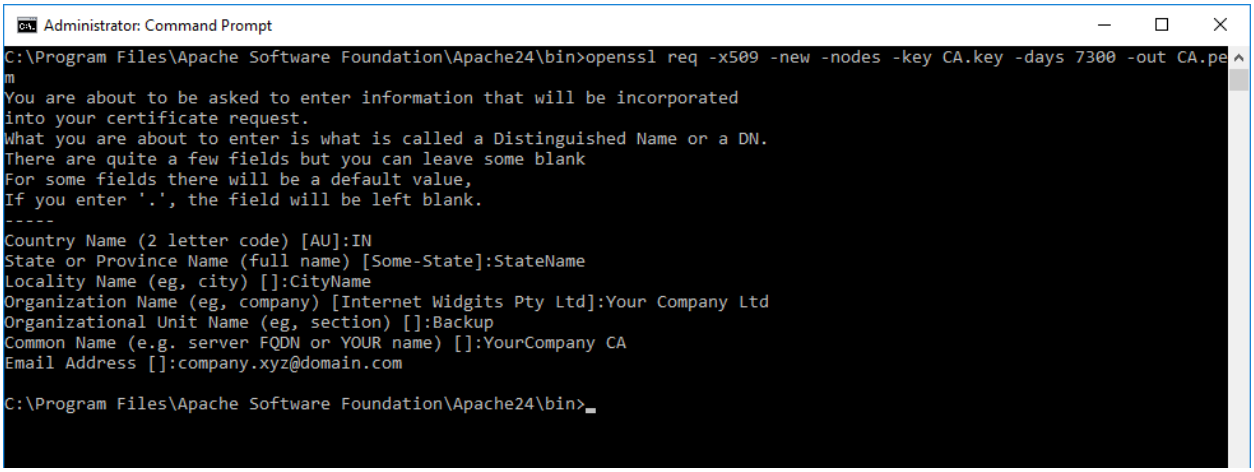
Commands:

a. set OPENSSL_CONF=C:\Program Files\Apache Software Foundation\Apache24\conf\openssl.cnf

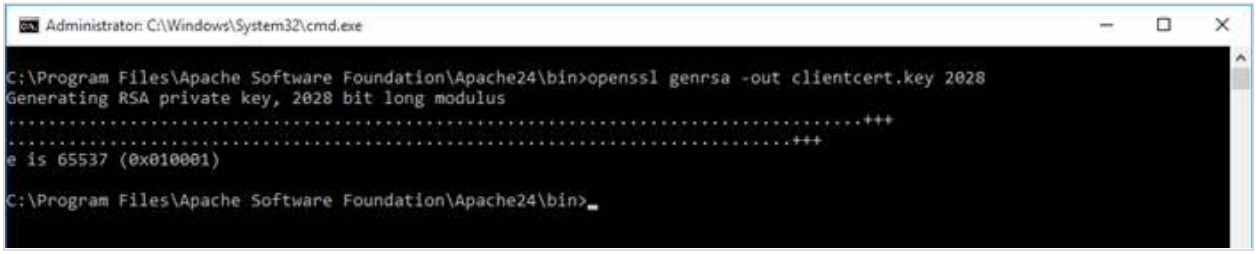


b. openssl genrsa -out CA.key 2048

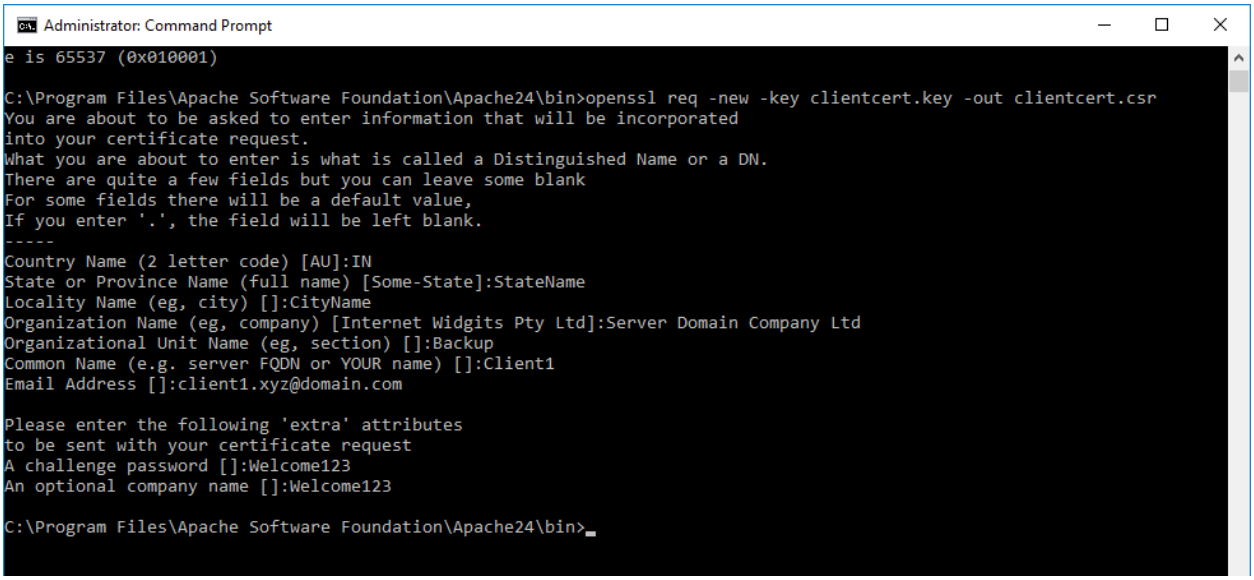
c. openssl req -x509 -new -nodes -key CA.key -days 7300 -out CA.pem



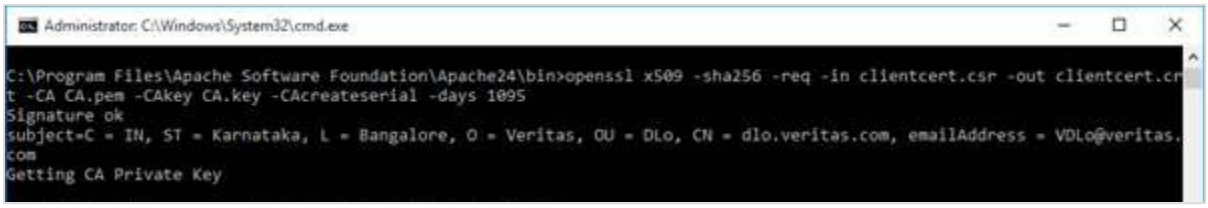
d. openssl genrsa -out clientcert.key 2028



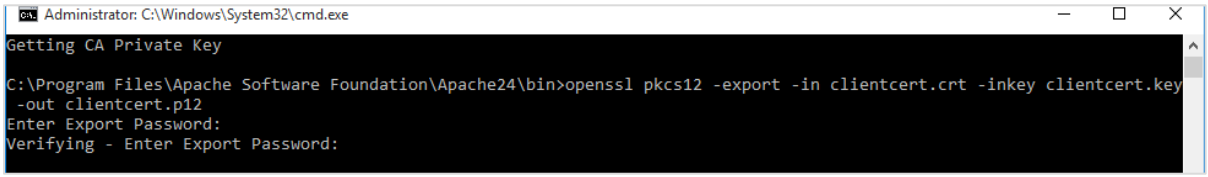
e. openssl req -new -key clientcert.key -out clientcert.csr



f. openssl x509 -sha256 -req -in clientcert.csr -out clientcert.crt -CA CA.pem -CAkey CA.key -CAcreateserial -days 1095



g. openssl pkcs12 -export -in clientcert.crt -inkey clientcert.key -out clientcert.p12



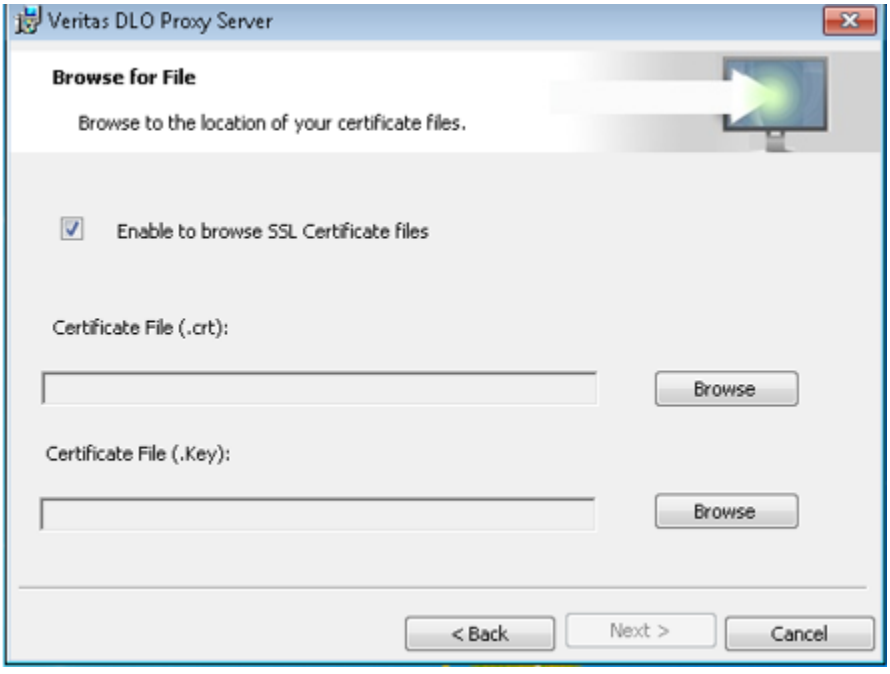
Deployment of Domain Trust Independent DLO

Following are the steps for deploying Domain Trust Independent DLO

1. Installing Veritas DLO 9.3
2. Configuring DLO Proxy Server in Agent Domain
3. Configuring DLO Server in Server Domain

Installing Veritas DLO 9.3

1. Install the **DLO Server components** in the **Server Domain** as follows**:**
    a. Download and Install the 32 bit or 64 bit package **Veritas_Desktop_and_Laptop_Option_xxxxxx_32-bit.zip or Veritas_Desktop_and_Laptop_Option_xxxxxx_64-bit.zip,** based on the bitness of the machine in the Server Domain where the DLO Server components will be installed.
2. Install the **DLO Proxy Server** setup on the machine in the **Agent Domain** as follows:
    a. Copy the **ProxyInstaller** folder from the Veritas DLO 9.3 package based on the bitness of the machine in the Agent Domain where the DLO Proxy Server will be installed.
    b. Click on **setup.exe** and continue with installation.
    c. In the DLO Proxy Server installation - **Browse for File** dialog



- Enabling the option **Enable to browse SSL Certificate Files**, allows the administrator to choose an alternate Server Certificate either procured from a Trusted CA or generated self-signed certificate and places this in the DLO Proxy Server's Apache path "*C:\Program Files\Apache Software Foundation\Apache24\conf\SSL*".
- By default this option is disabled and the Server Certificate **Server.crt** bundled with DLO package will be used.

Configuring DLO Proxy Server in Agent Domain

1. Place the Client certificate's CA, either procured from a trusted CA or generated self-signed CA certificate, in the Apache path of DLO Proxy Server (*C:\Program Files\Apache Software Foundation\Apache24\conf\SSL*).
2. Uncomment following lines in **httpd.conf** file (C*:\Program Files\Apache Software Foundation\Apache24\conf*).

   JkMount /DLOServer/web/ WebRestoreLoadBalancer*
   SSLCACertificateFile "conf\SSL\DLOCA.pem"
   <Location "/DLOServer/web/restore">
   SSLVerifyClient require
   SSLVerifyDepth 5
   </Location>
3. In the **httpd.conf** file (*C:\Program Files\Apache Software Foundation\Apache24\conf*), update the **DLOCA.pem** to the pem filename of the Client certificate's CA issued by a Trusted CA. In case this is a generated self-signed CA certificate, update the pem filename as in **Command (c)** of Generation of Self-signed certificates.

   SSLCACertificateFile "conf\SSL\DLOCA.pem"
4. Restart the **Veritas DLO Edge Server** service.

Configuring DLO Server in Server Domain

Configuring the DLO Server in the Server Domain includes:

- Establishing trust for the Server certificate used in DLO Proxy Server Setup
- Adding the Client Certificate to DLO IO Server
- Adding the DLO Proxy Server details in the DLO Administration Console

Establishing Trust for Server certificate used in DLO Proxy Server Setup

1. Copy the Server certificate (**server.crt, if self-signed)** file from the source path "*C:\Program Files\Apache Software Foundation\Apache24\conf\SSL*" from the DLO Proxy Server machine

(**Agent Domain**) to the destination path "*C:\Program Files\Veritas\Veritas DLO\IOServer\Jre\bin*" in the DLO Server machine (**Server Domain)**.

2. Open an elevated command prompt and browse to the path: "*C:\Program Files\Veritas\Veritas DLO\IOServer\Jre\bin"* on **Server Domain** machine. Run the following command
   keytool -import -file server.crt -alias veritaskeystore1 -keystore "C:\Program Files\Veritas\Veritas DLO\IOServer\Jre\lib\security\cacerts"
3. This prompts for the keysstore password. Enter password as **'changeit'**.
4. Select **'y'.**

```
C:\Program Files\Veritas\Veritas DLO\IOServer\Jre\bin>keytool -import -file serv
er.crt -alias veritaskeystore1 -keystore "C:\Program Files\Veritas\Veritas DLO\I
OServer\Jre\lib\security\cacerts"
Enter keystore password:
Owner: EMAILADDRESS="dlo.certs@mindtree.com ", CN=dlo.veritas.com, OU=DLO, O=Min
dtree Limited, L=Bangalore, ST=Karnataka, C=IN
Issuer: EMAILADDRESS="dlo.certs@mindtree.com ", CN=dlo.veritas.com, OU=DLO, O=Mi
ndtree Limited, L=Bangalore, ST=Karnataka, C=IN
Serial number: f5a57ef874979a86
Valid from: Tue Jun 21 05:50:16 PDT 2016 until: Fri Jun 21 05:50:16 PDT 2019
Certificate fingerprints:
         MD5:  CC:4D:F7:63:1A:66:53:70:B2:2F:BE:26:0F:7A:D1:2C
         SHA1: AB:D9:0B:AF:8E:03:98:B5:12:11:E7:5F:3D:8B:7E:B4:D1:98:35:2C
         SHA256: 38:E1:A4:B5:C5:7D:AB:CC:AB:92:31:0F:71:4F:B6:FE:2E:4E:38:04:72:
35:E3:F7:F1:90:FF:72:26:CB:B5:C4
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: C4 66 C8 33 7E 29 5E 9D   9C 1F 92 6C 4F B1 75 B4  .f.3.)^....lO.u.
0010: D5 40 9B 82                                        .@..
]
]

#2: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: C4 66 C8 33 7E 29 5E 9D   9C 1F 92 6C 4F B1 75 B4  .f.3.)^....lO.u.
0010: D5 40 9B 82                                        .@..
]
]

Trust this certificate? [no]:  y
Certificate was added to keystore
```

5. Restart the **Veritas DLO Web Server** service in the Server Domain**.**

Adding the Client Certificate to DLO IO Server

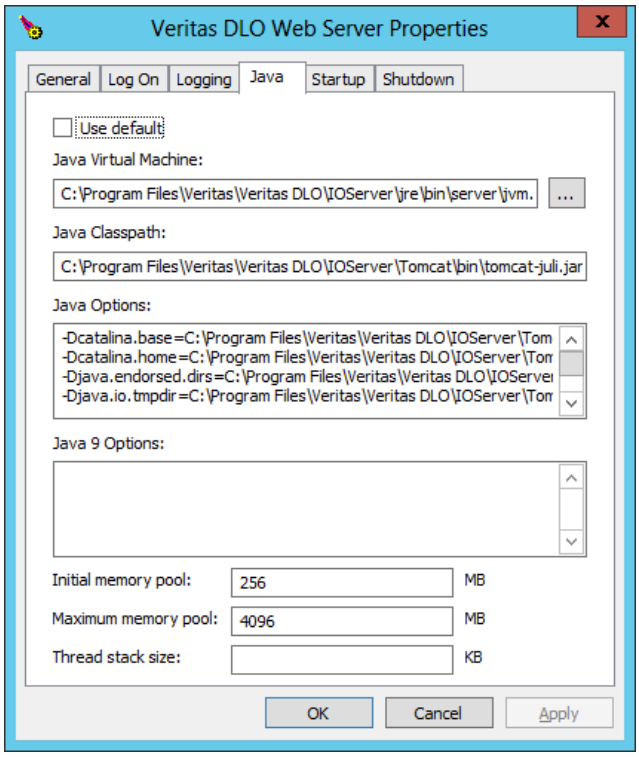
Following are the steps to add the Client certificate, either procured from a trusted CA or generated self-signed certificate to the DLO IO server.

1. Create a SSL folder in DLO IO Server install path in the Server Domain "*C:\Program Files\Veritas\Veritas DLO\IOServer\Tomcat\conf"*

2. Place the Client certificate(**clientcert.p12, if self-signed**) in the path "*C:\Program Files\Veritas\Veritas DLO\IOServer\Tomcat\conf\SSL"*

3. Open an elevated command prompt and run the following command from DLO IO Server install path *"C:\Program Files\Veritas\Veritas DLO\IOServer\Tomcat\Bin"*
   tomcat8w//ES//DLOWebserver

4. On the **Veritas DLO Web Server Properties** dialog, select **Java** tab



5. Add below parameters in **Java Options** in **Veritas DLO Web Server Properties** window:

   -Djavax.net.ssl.keyStoreType=pkcs12

   -Djavax.net.ssl.keyStore=C:\Program Files\Veritas\Veritas DLO\IOServer\Tomcat\conf\SSL\ClientCert.p12

   -Djavax.net.ssl.keyStorePassword=<Password>

   Note: *<Password>* entry should be updated with Client Certificate password. In case of self-signed client certificate, update as in **Command (g)** of Generation of Self-signed certificates.

6. Restart the **Veritas DLO Web Server** service.

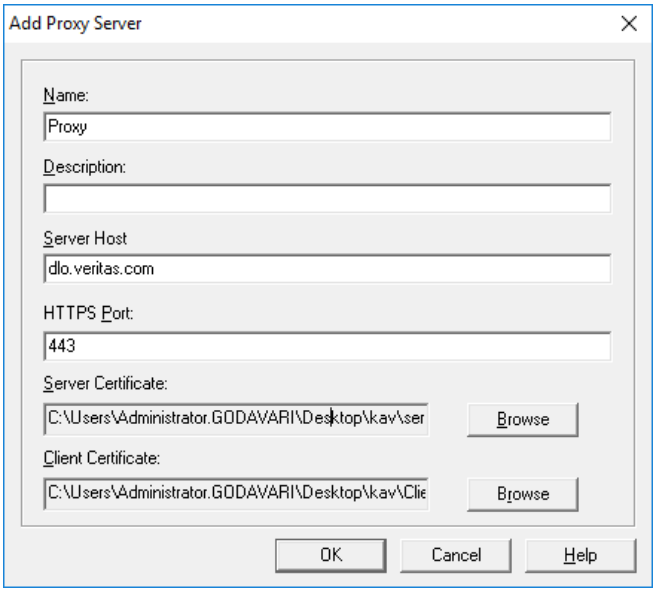
Adding the DLO Proxy Server details to DLO Administration Console

Before adding the DLO Proxy Server,

- Ensure the DLO Proxy Server is exposed to the public network and is accessible with certificate host name. If exposed with public IP, then add the host entry in DLO Server tagging public IP to certificate host name as mentioned in How to map the public IP to certificate hostname.
- The DLO IO Server is assigned to the appropriate Storage location.

Following are the steps to add the DLO Proxy Server details:

1. Launch the Veritas DLO Administration Console.
2. On the DLO navigation bar, click **Setup**.
3. In the **Settings** pane, click **Edge Server**.
4. Right-click the IO Server and select **New Proxy Server**.
5. The **Add Proxy Server** window appears.



6. Enter the following details:

    a. **Name:** Enter a name for the Proxy Server. This is just for identification purpose.

    b. **Description:** Enter a description to identify the Proxy Server.

    c. **Server Host:** Enter the certificate host name of the Proxy Server (Server Certificate).

    Note: By default this is **dlo.veritas.com**. In case an alternate Server Certificate has been used, update the details accordingly.

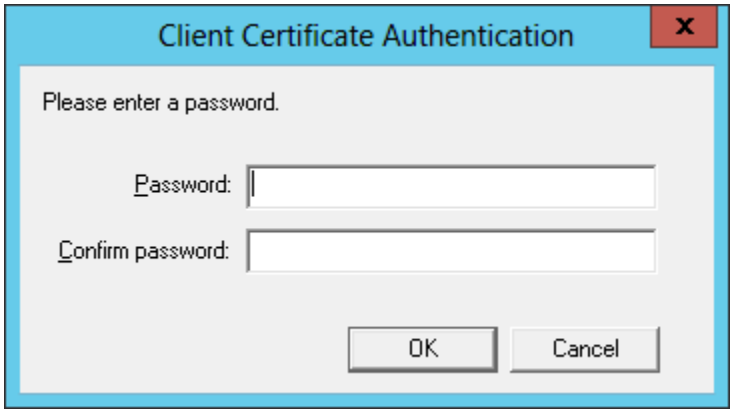
    d. **HTTPS Port:** Enter the port details, if you are using a customizable port and ensure this port is open. By default the port is 443.

    e. **Server Certificate**: Copy the Server Certificate used in DLO Proxy Server machine to DLO Server machine. Click **Browse** and select the Server Certificate.

    f. Client Certificate: Copy the Client Certificate (clientcert.p12, if self-signed) to DLO Server machine. Click **Browse** and select the Client Certificate**.**

7. Click **OK**.

8. Enter the credentials for the Client Certificate Authentication. In case of self-signed client certificate, update as in **Command (g)** of Generation of Self-signed certificates.



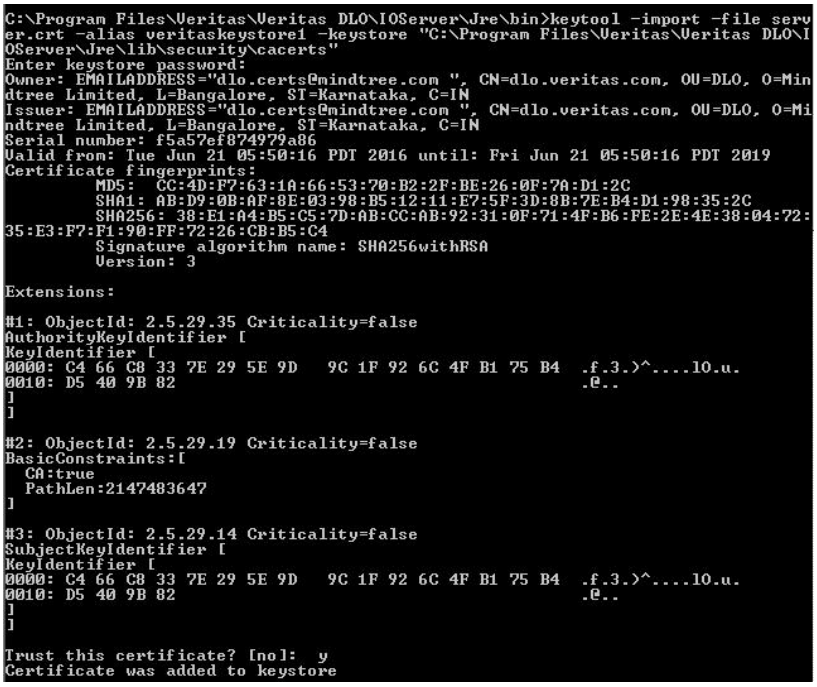
Note: The credentials will be cached in encrypted format for future authentication requests.

9. Click **OK**.

Considerations for Upgrade Scenarios

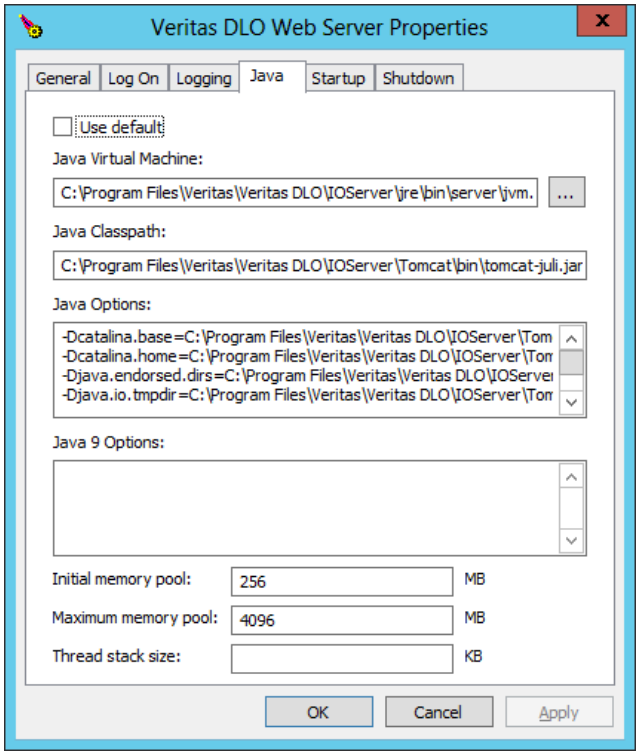
In case of upgrade scenarios for a DLO setup where the DLO Proxy Server is configured, the following steps need to be performed manually on the DLO Server machine in the Server Domain.

1. **Keystore Generation**
   - *a.* Open an elevated command prompt and browse to the path: *"C:\Program Files\Veritas\Veritas DLO\IOServer\Jre\bin"* on **Server Domain** machine. Run the following command :
     keytool -import -file server.crt -alias veritaskeystore1 -keystore "C:\Program Files\Veritas\Veritas DLO\IOServer\Jre\lib\security\cacerts"
   - b. This prompts for the keysstore password. Enter password as **'changeit'**.
   - **c.** Select **'y'.**



d. Restart the **Veritas DLO Web Server** service in the Server Domain**.**

2. **Update the Veritas DLO Web Server Properties**
    a. Open an elevated command prompt and run the following command from DLO IO Server install path *"C:\Program Files\Veritas\Veritas DLO\IOServer\Tomcat\Bin"*
        tomcat8w//ES//DLOWebserver
    b. On the **Veritas DLO Web Server Properties** dialog, select **Java** tab



c. Add below parameters in **Java Options** in **Veritas DLO Web Server Properties** window:

-Djavax.net.ssl.keyStoreType=pkcs12

-Djavax.net.ssl.keyStore=C:\Program Files\Veritas\Veritas DLO\IOServer\Tomcat\conf\SSL\ClientCert.p12

-Djavax.net.ssl.keyStorePassword=<Password>

Note: *<Password>* entry should be updated with Client Certificate password. In case of self-signed client certificate, update as in **Command (g)** of Generation of Self-signed certificates.

d. Restart the **Veritas DLO Web Server** service.

Limitations of Domain Trust Independent DLO

- Domain Trust Independent DLO is not supported for Mac agents, as they do not support BOI mode.
- For Adding Automated User Assignment (AUA), Adding Users and Staging operations, the Active Directory (AD) objects cannot be browsed and should be entered manually.
- Configuring AUA with Active Directory option is not supported.
- Configuring Connection policy using Active Directory is not supported.
- Restore to alternate computer option is not supported, if the alternate computer resides in the Agent Domain.

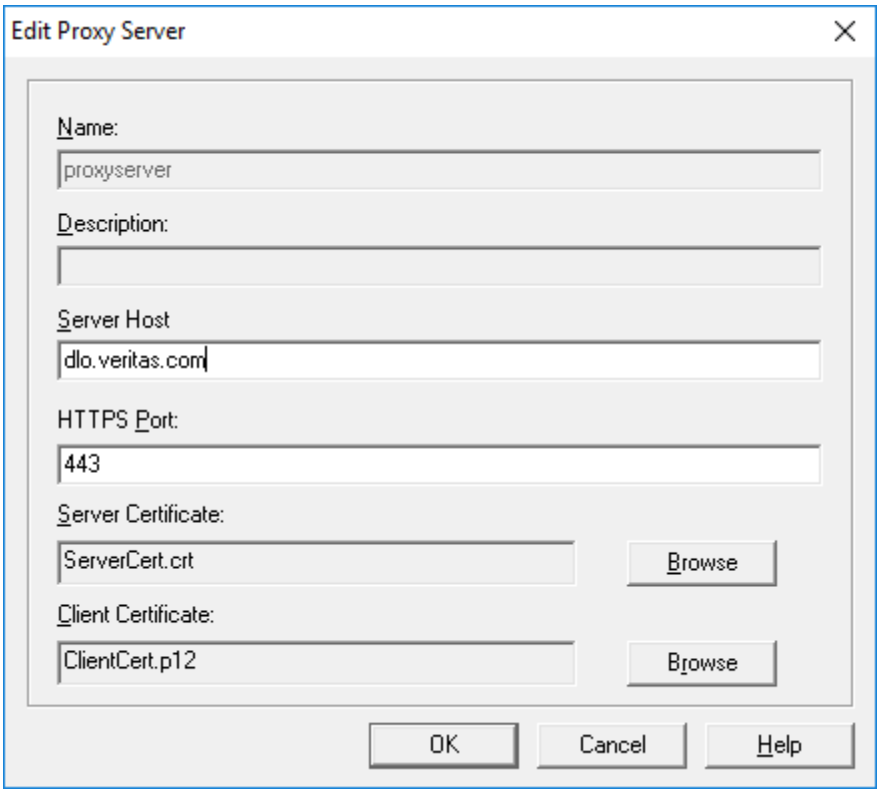
Post-Deployment: Maintenance

Once the DLO Proxy Server setup is configured, there could be possibilities where the SSL Certificates may expire or the administrator may choose to use a port other that the Default HTTPS Port.

The following section covers the steps for configuration changes, post deployment of the Domain Trust Independent DLO.

Editing the DLO Proxy Server Details in the DLO Administration Console

1. On the DLO navigation bar, click **Setup**.
2. In the **Settings** pane, double-click the **Edge Server**. The name of the Edge server is displayed.
3. Double-click the name of the Edge Server. The name of the IO Server will be displayed.
4. Double-click the name of the IO Server. The name of the Proxy Server will be displayed.
5. Right-click the Proxy Server name and select **Edit Proxy Server**.



6. Change the details as required.
7. Click **OK**.

Configuring DLO Proxy Server Setup to use new SSL Server Certificate

On the DLO Proxy Server Setup:

1. Stop the **Veritas DLO Edge Server** service.
2. Place newly generated **.crt, .key** files in "*C:\Program Files\Apache Software Foundation \Apache24\conf\ssl* "path.
3. Update **httpd.conf** files with new certificate name. Update below lines in **httpd.conf** file that is the hostname with new certificate name and the server.CRT, server.Key to new certificate file name.

   <VirtualHost hostname:443>
   ServerName hostname
   SSLCertificateFile "conf\SSL\SERVER.CRT"
   SSLCertificateKeyFile "conf\SSL\SERVER.KEY"
4. Update below lines in **httpd-ssl.conf** file with new certificate file name

   SSLCertificateFile "conf\SSL\SERVER.CRT"
   SSLCertificateKeyFile "conf\SSL\SERVER.KEY"
5. Start the **Veritas DLO Edge Server** service.

On DLO Server Setup:

1. Establish Trust for the new Server certificate in DLO Proxy Server setup, for more details refer Establishing Trust for Server certificate used in DLO Proxy Server Setup.
2. Edit the **Server Certificate** details in **Edit Proxy Server** dialog, for more details refer Editing the DLO Proxy Server Details in the DLO Administration Console.

Configuring DLO Proxy Server Setup to use updated (new) SSL Client certificate

Note: Ensure the new Client Certificate is in the **.p12** format.

Configuring DLO Proxy Server Setup to use updated (new) SSL Client certificate includes:

1. Adding the new Client certificate to the DLO IO Server, for more details refer Adding the Client Certificate to DLO IO Server.
2. Edit the **Client Certificate** details in the **Edit Proxy Server** dialog, for more information refer Editing the Proxy Server Details in the DLO Administration Console.

Configuring Proxy Server Setup to use updated (new) CA and Client Certificate

Note: Ensure the newly generated client certificate is in **.p12** format.

Configuring Proxy Server Setup to use updated (new) CA and Client Certificate includes:

1. Updating the new CA details in the DLO Proxy Server setup, for more information refer Configuring Proxy Server in Agent Domain.
2. Updating the new Client certificate details, for more information refer Configuring Proxy Server Setup to use updated (new) SSL Client certificate post configuration.

Configuring Proxy Setup to use a port other than default HTTPS port (443)

On DLO Proxy Server setup:

1. Stop the **Veritas DLO Edge Server** service.
2. Update below line in **httpd.conf** (*C:\Program Files\Apache Software Foundation\Apache24\Conf***)** file with new port details.

   <VirtualHost hostname:443>
3. Update below lines in **httpd-ssl.conf**(*C:\Program Files\Apache Software Foundation\Apache24\Conf\extra***)** file with new port details:

   Listen 443

   <VirtualHost _default_:443>
4. Start the **Veritas DLO Edge Server** service.

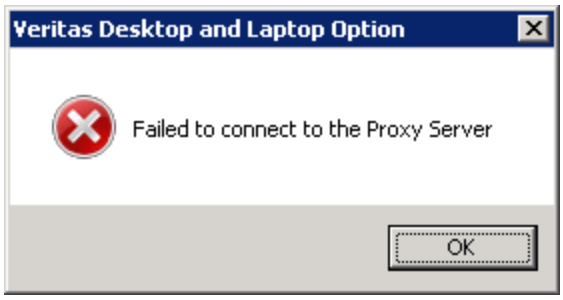
On DLO Server setup:

Edit the **HTTPS Port** details in the **Edit Proxy Server** dialog, for more information refer Editing the DLO Proxy Server Details in the DLO Administration Console

Troubleshooting Tips

For configuring DLO Proxy Server details in the DLO Administration Console

1. Failed to connect to the Proxy Server



- **On the DLO Proxy Server set up**
  - Check if the **Veritas DLO Edge Server** and **Veritas DLO IO Server** service are up and running. If not, restart the above services.
  - Check this URL to verify the DLO Proxy Server status
    - https://dlo.veritas.com/DLOServer/rest1/DefaultIOServer/status/

    This is a successful response

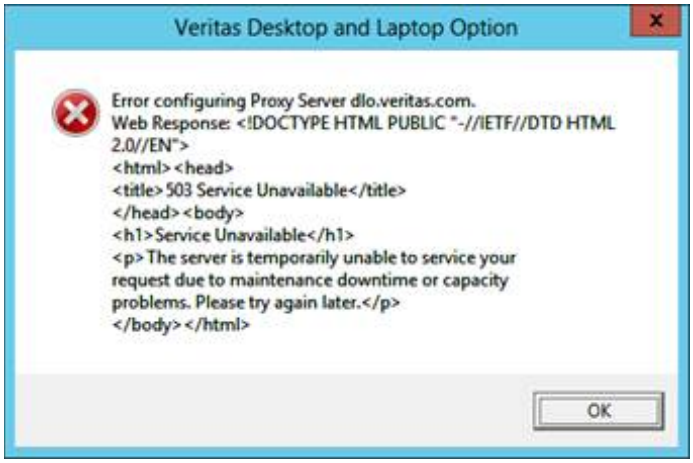
    IO Server is Reachable....!!!!!

    Status: Server not Initialized
  - Check if below entry in **httpd.conf** file Apache path "*C:\Program Files\Apache Software Foundation\Apache24\conf*" is uncommented
    - *JkMount /DLOServer/web/* WebRestoreLoadBalance*

    If this entry is commented, uncomment the same.

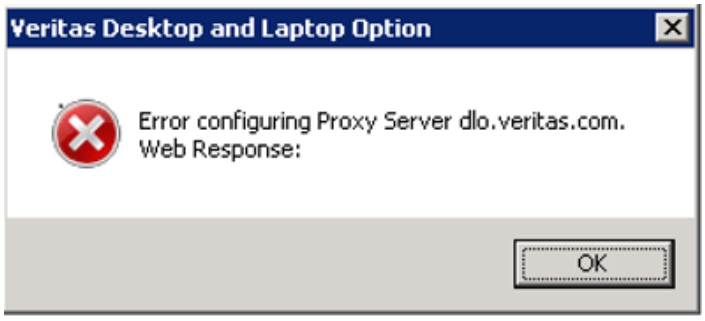
- **On the DLO Server set up**
  - If the DLO Proxy Server is exposed via public IP, check if the host entry mapping the public IP to the certificate host name is added. For more details refer How to map the public IP to the certificate hostname.
  - While adding the DLO Proxy Server details in the DLO Administration Console,
    - Ensure the Server certificate provided is the same as the one used in the DLO Proxy Server setup.
    - Ensure a valid Client certificate is provided.
    - Verify if the valid credentials are provided for Client Certificate authentication.
    - Ensure the HTTPS Port is open. If not, open the specified port.

2. **Error configuring Proxy Server: Web Response 503 Service Unavailable**



- **On the DLO Server setup**
  - Check if the **Veritas DLO IO Server** service is up and running. If not, restart this service.
  - Check if the DLO IO Server machine in the Server Domain is reachable. If not, ensure the machine is reachable and then try adding the DLO Proxy Server details in the DLO Administration Console.

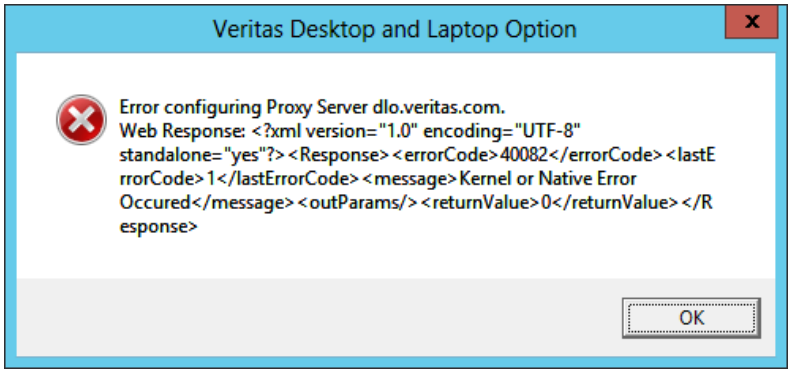
3. **Error Configuring Proxy Server**



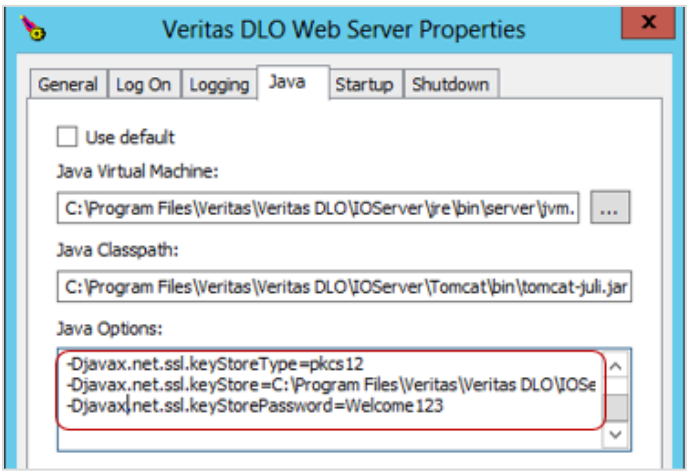
- **On the DLO Server setup**
  - Check if the **Veritas DLO Edge Server** service is up and running. If not, restart this service.

- Check if the DLO Edge Server machine in the Server Domain is reachable. If not, ensure the machine is reachable and try adding the DLO Proxy server details in the DLO Administration console.

4. Error Configuring Proxy Server :Kernel or Native error occurred

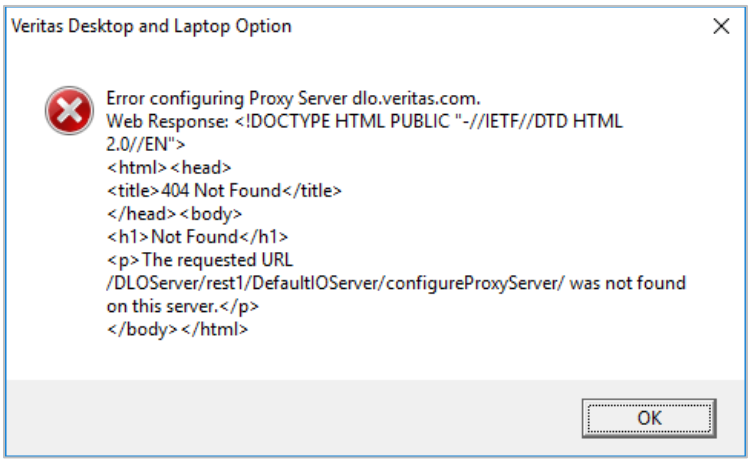


- **On the DLO Server setup**
  - Check if the Client Certificate is present in the Local DLO IO Server path: *"C:\Program Files\Veritas\Veritas DLO\IOServer\Tomcat\conf\SSL".* If not, copy the Client certificate (clientcert.p12 if self-signed) in this path.
  - Check whether trust is established for Server Certificate (used in Proxy Server setup) in the DLO IO Server machine. For more details, refer Establishing trust for Server certificate used in DLO Proxy Server Setup.
  - Open an elevated command prompt
    - Run the following command from DLO IO Server install path *"C:\Program Files\Veritas\Veritas DLO\IOServer\Tomcat\Bin"*
      tomcat8w//ES//DLOWebserver



- On the **Veritas DLO Web Server** Properties window, verify the Certificate Path, Certificate filename and Client Certificate password in the in **Java** options of the **Veritas DLO Web Server** Properties is valid. If not, update the path, Certificate filename and password appropriately.

5. **Error configuring Proxy Server: 404 Not Found**



- **On the DLO Server setup**
  - In the DLO Administration Console, check if the DLO IO Server is assigned to appropriate DLO Storage. If not, assign the appropriate DLO IO Server to the DLO Storage and try adding the DLO Proxy Server details.

If the above troubleshooting tips does not resolve the issue, contact the Veritas Technical Support at www.veritas.com/support.

FAQs for Certificate Requirements

What is a SSL certificate chain?

The list of SSL certificates, from the root certificate to the end-user certificate, represents the **SSL certificate chain.** In the following example the certificate chain is represented by four certificates.

1. End user certificate –issued to **yyy.domain.com** by Example Authority.
2. Intermediate certificate 1 - issued to Example Authority by Intermediate Example-1 CA.
3. Intermediate certificate 2 - issued to Intermediate Example-1 CA by Chief Root CA.
4. Root Certificate- issued to and by Chief Root CA.

What are the prerequisites for creating Server certificate chain?

The files mentioned below are needed to create the Server certificate chain

- Server SSL certificate file.
- Root certificate for the server certificate.
- Intermediate chain certificates (if any) for the server certificate. All are components of the CA issued certificate.

Note: All of the above files should be PEM-encoded X.509 with .crt extension.

- Private Key file for the Server (PEM-encoded with .key extension).

What are the steps to create the Server Certificate Chain ?

1. Create a .crt file and place all the certificates in the order - Server certificate, followed by Intermediate chain certificates and then the Root certificate

   E.g.: There is a Server certificate dlocert.crt which is issued by dloserverCA.crt (root certificate) and their certificates have below content respectively.

Content in dloserver.crt
-----BEGIN CERTIFICATE-----
<Content 1>
-----END CERTIFICATE-----

Content in dloserverCA.crt
-----BEGIN CERTIFICATE-----
<Content 2>
-----END CERTIFICATE-----

   The new .crt file should have below content

Content in new.crt
-----BEGIN CERTIFICATE-----
<Content 1>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Content 2>
-----END CERTIFICATE-----

2. Bind this URL to the Edge Server IP by registering it in the DNS.
3. Bind this certificate with a URL (EG: YYY.domain.com) that needs to be published over internet.
4. In case of self-signed certificate, add a DNS entry mapping the certificate name with the Edge server IP address OR add a local host entry in the Edge Server machine mapping the certificate name with the IP address.

How to map the public IP to the certificate hostname?

In the DLO Administration Console and the DLO IO Server machines, update the hosts file present in the

path “C:\Windows\System32\drivers\etc” with the entry as below

<Public IP> <Certificate hostname>

E.g.: 10.50.1.12 yyy.domain.com