Symantec™ Desktop and Laptop Option

BOI Setup and Configuration Details

Symantec

Disclaimer

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

Legal Notice

Copyright © 2016 Symantec Corporation. All rights reserved.

Symantec, Backup Exec, NetBackup, the Symantec Logo, and Desktop and Laptop Option are trademarks or registered trademarks of Symantec Software Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Symantec Software Corporation

350 Ellis Street
Mountain View, CA 94043
www.symantec.com

Third-Party Legal Notices

Certain third-party software may be distributed, embedded, or bundled with this Symantec product or recommended for use in connection with its installation and use. Such third-party software is separately licensed by its copyright holder. Licenses that govern the use of the third party software included in the Symantec product and proprietary notices of the copyright holders are listed in the Administrators Guide

Table of Contents

1 BOI - Setup and Configuration 4
1.1 Introduction 4
1.2 BOI Server Components 4
1.3 Client Communication with Edge Server which is Configured to use a SSL Certificate 4
1.4 About Server Certificates 4
1.5 Steps to Create Server Certificate Chain 5
1.6 Steps to Change the Certificate 5
1.7 Client Access through Public IP - Default Installation which comes with Self-signed Certificate 6
1.8 Test the Connectivity 6

1 BOI - Setup and Configuration

1.1 Introduction

Backup over Internet feature in DLO enables a user to back up his data over a public network. When Desktop Agent Computer goes outside of corporate network, the backups will continue using the available internet connection, thus allowing one to Write/Read data to/from network storage locations.

1.2 BOI Server Components

Following are the BOI Components:

1. Edge Server
2. IO Server

Note: Please refer DLO Administrator's Guide for all the Hardware requirements for installing the above Server components.

Pre-requisites:

1. Install and configure all DLO server components. Please refer DLO Administrator's Guide for installation and configuration of individual Server components.
2. Enable all the required firewall ports on all the DLO Server components. Please refer Symantec DLO Firewall Ports section in DLO Administrator's Guide.
3. Desktop Agent working in BOI mode communicates with the Edge Server over a public URL/IP. Make sure that you either publish this URL over internet or expose a Public IP through which requests are forwarded to Edge Server as mentioned below.

1.3 Client Communication with Edge Server which is Configured to use a SSL Certificate

1. Get a SSL certificate issued from a trusted CA.
2. Bind this certificate with a URL (EG: yyy.domain.com) that needs to be published over the internet.
3. Register this URL in the DNS.
4. Push the SSL cert. from DLO Administration Console.

1.4 About Server Certificates

The default installation of Edge Server comes with self-signed SSL certificate. It is recommended to use SSL certificate issued by a trusted Certificate Authority.

The files mentioned below will be needed while changing to a different certificate:

1. Server SSL certificate file.
2. Root certificate for the server certificate.
3. Intermediate chain certificates (if any) for the server certificate.

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

4. private key file for the Server (PEM-encoded with .key extension).

1.5 Steps to Create Server Certificate Chain

1. Create a `.crt` file and place all the certificates (Server certificate, intermediate chain certificates and root certificate) in this file.
2. The order is Server certificate followed by the intermediate and then the root certificate.
   Example: There is a Server certificate `dlocert.crt` which is issued by `dloserverCA.crt` and their certificates have below content respectively.
   Content in `dloserver.crt`
   -----BEGIN CERTIFICATE-----
   XXXXXXXXXXXXXXXXXXXXXXXXXXX
   -----END CERTIFICATE-----

   Content in dloserverCA.crt
   -----BEGIN CERTIFICATE-----
   YYYYYYYYYYYYYYYYYYYYYYYYYYY
   -----END CERTIFICATE-----

   Then the new .crt file should have below content
   -----BEGIN CERTIFICATE-----
   XXXXXXXXXXXXXXXXXXXXXXXXXXX
   -----END CERTIFICATE-----
   -----BEGIN CERTIFICATE-----
   YYYYYYYYYYYYYYYYYYYYYYYYYYY
   -----END CERTIFICATE-----

1.6 Steps to Change the Certificate

1. Create the Server certificate chain. Find the steps under heading "**Steps to create server certificate chain**" mentioned in section 1.5.
2. Place the Server certificate chain file (created in Step 1) and the private key file for Server in a folder. Make sure no other .crt files are present in this location.
3. Backup and remove any existing .crt files from the location "C:\Program Files\Apache Software Foundation\Apache24\Conf\SSL".
4. Launch the **Symantec DLO Administration Console**.
5. On the DLO navigation bar, click **Setup**.
6. In the **Settings** pane, right-click **Edge Server**, and select **Edit Edge Server**.
7. Click **Browse** and select the Server Certificate chain file from the folder created in Step 2.

8. Click **Push Certificate**.
9. Click **Ok**.

Once the certificate is pushed, publish the URL which is bound to the certificate over internet. This can be done through a Reverse Proxy Server setup by enabling SSL (port 443) access or any other mechanism which does the same.

The above is the recommended procedure to establish the client communication with DLO Servers.

1.7 Client Access through Public IP - Default Installation which comes with Self-signed Certificate

1. Have a registered public IP through which you will be able to access Internet.
2. Expose this public IP over internet and through Nat (Dynamic or static) configured on the firewall, port forward the requests (over port 443) that are being sent from DLO Clients to the Server (Edge Server) present in Corporate LAN network.
   You can even have a DMZ configured on the firewall/router which would forward all the client requests to the Static IP of the Edge server.

Note1: The above examples demonstrates how client requests from internet are routed to the corporate network. There could be other mechanisms through which one can achieve the same.

Note2: If the client communication is directly over a public IP, the Edge Server entry in **Edgserver.ini file** in the client install path typically "C:\Program Files (x86)\Symantec\Symantec DLO\DLO\ EdgeServer.ini" should be updated with its corresponding public IP.

1.8 Test the Connectivity

Once the deployment is done, you can test the connectivity to Edge Server by accessing the URL:

1. `https://<Edge_Server_URL>`

   Example: `https://zzz.domain.com`

NOTE: The URL must be published over internet.

---

2. `https://<Public_Edge_Server_IP>`

NOTE: Public IP must be exposed over internet.