Dell™ SMA 11.4 Global Traffic Optimizer
Deployment Guide
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Overview</td>
<td>4</td>
</tr>
<tr>
<td>Supported platforms</td>
<td>5</td>
</tr>
<tr>
<td>Limitations and unsupported features</td>
<td>5</td>
</tr>
<tr>
<td>Planning GTO Deployment</td>
<td>6</td>
</tr>
<tr>
<td>Choosing a deployment model</td>
<td>6</td>
</tr>
<tr>
<td>SMA appliances located in one data center</td>
<td>6</td>
</tr>
<tr>
<td>SMA appliances geo-distributed across multiple data center</td>
<td>6</td>
</tr>
<tr>
<td>Mixed mode</td>
<td>7</td>
</tr>
<tr>
<td>Minimizing configuration differences</td>
<td>7</td>
</tr>
<tr>
<td>Choosing a GTO service name and establishing DNS delegations</td>
<td>8</td>
</tr>
<tr>
<td>Choosing a GTO service name</td>
<td>8</td>
</tr>
<tr>
<td>Establishing the GTO service name delegations in DNS</td>
<td>8</td>
</tr>
<tr>
<td>Provisioning certificates</td>
<td>9</td>
</tr>
<tr>
<td>Setting up GTO</td>
<td>10</td>
</tr>
<tr>
<td>Setting up the CMS and SMA appliances</td>
<td>10</td>
</tr>
<tr>
<td>Setting up a basic GTO deployment</td>
<td>11</td>
</tr>
<tr>
<td>Registering an SMA appliance with the CMS</td>
<td>13</td>
</tr>
<tr>
<td>Defining the central policy</td>
<td>15</td>
</tr>
<tr>
<td>Extending GTO Deployment</td>
<td>17</td>
</tr>
<tr>
<td>Adding additional SMA appliances</td>
<td>17</td>
</tr>
<tr>
<td>Enabling cached credentials</td>
<td>17</td>
</tr>
<tr>
<td>Using distributed authentication servers</td>
<td>18</td>
</tr>
<tr>
<td>Varying tunnel address pools</td>
<td>19</td>
</tr>
<tr>
<td>Additional deployment notes</td>
<td>19</td>
</tr>
<tr>
<td>About Dell</td>
<td>20</td>
</tr>
<tr>
<td>Contacting Dell</td>
<td>20</td>
</tr>
<tr>
<td>Technical support resources</td>
<td>20</td>
</tr>
</tbody>
</table>
Introduction

Topics

- Overview
- Supported platforms
- Limitations and unsupported features

Overview

This deployment guide explains the Global Traffic Optimizer (GTO), a feature of SMA and CMS that presents a collection of SMA appliances to end users through a single GTO service name (for example access.example.com), which allows users to access their organization's network through an appropriate SMA appliance depending on their global location and other factors.

Dell Secure Mobile Access (SMA) appliances provide SSL VPN access to an organization's Intranet resources from virtually any endpoint on the Internet - including desktops, laptops, tablets, and smartphones. The Central Management Server (CMS) provides a single console for managing, maintaining, and monitoring a collection of similarly-configured SMA appliances that may be hosted in one data center or in multiple locations.
Previously, the benefits provided by GTO could only be achieved by deploying and coordinating an array of separate third-party appliances and services, such as content-distribution-network DNS redirectors, local traffic managers, and load balancers often under separate administrative control. GTO replaces this scenario with a single external DNS delegation, which manages all aspects of user traffic distribution automatically, including license provisioning and leveling.

Users have one consistent sign-on procedure with one GTO service name that connects them with the appropriate SMA appliance for their current location and circumstances, and gives them a similar experience every time they use the system anywhere in the world.

GTO makes intelligent routing decisions based on real-time data such as appliance availability, health, load, Internet and Intranet conditions. GTO redirects user connection requests to the most appropriate SMA appliance using the best possible route for the user at that moment.

This guide provides instructions on how to deploy CMS with GTO, including DNS configuration and certificate requirements.

**Supported platforms**

In the Dell SMA 11.4.0 release, GTO is supported on the following Dell SMA 1000 series appliances:

- EX9000
- EX7000
- EX6000
- SMA 6200
- SMA 7200
- SMA 8200v (ESX/Hyper-V)

**Limitations and unsupported features**

The following features are not supported with GTO in the SMA 11.4 release:

- ActiveSync clients
- Custom FQDNs
Planning GTO Deployment

This section describes how to make deploying GTO easier by some planning and adherence to a few guidelines as described in the topics below:

Topics
- Choosing a deployment model
- Minimizing configuration differences
- Choosing a GTO service name and establishing DNS delegations
- Provisioning certificates

Choosing a deployment model

Before you set up your equipment, you need to choose a deployment model that meets your organization's needs. There are several ways you can set up the network hierarchy of your GTO deployment:

- SMA appliances located in one data center
- SMA appliances geo-distributed across multiple data center
- Mixed mode

SMA appliances located in one data center

This model is typically employed by mid-sized organizations with major operations in a single location. All their SMA appliances are located in the organization's primary data center. Users have a single GTO service name (such as access.example.com) to access the network.

GTO eliminates the need for a load balancer in the data center for VPN traffic. User connections are automatically directed to an available appliance in the data center. The CMS and SMA appliances are all located in the data center. If any one of the appliances fails, the CMS detects the failure, and GTO automatically redirects the VPN connections to another appliance.

SMA appliances geo-distributed across multiple data center

This model is typically employed by mid-sized organizations with operations in more than one geographic location, and their SMA appliances are located in different geographic locations. For example, an organization deploys two SMA appliances, one located in their New York City data center and the second appliance located in their London branch office. The employees in the Americas connect to the appliance in New York City, while the employees in Europe connect to the appliance in London.

The CMS and one of their SMA appliances is located in New York City. The other SMA appliance is located in London and is also managed by the CMS. All the employees in the Americas and in Europe use a single service name: access.example.com, which directs all connections to an available and proximate appliance.
Mixed mode

This model is typically employed by larger sized organizations with a global workforce. Their SMA appliances are located in multiple geographic locations, and they may have more than one SMA appliance in the data center. For example, an organization has six SMA appliances: three in New York City, two in London, and one in Tokyo. Employees globally use the same service name: access.example.com.

GTO automatically directs connections from employees in the Americas to the SMA appliances in New York City, connections from employees in Europe to the SMA appliances in London, and connections from employees in Asia to the SMA appliance in Tokyo. GTO eliminates the need for a global traffic manager or load balancer in the data center.

Minimizing configuration differences

In a GTO service, users can get directed to different SMA appliances frequently, and users expect the same experience, regardless. You can minimize configuration differences between SMA appliances in a GTO service by observing the following guidelines:

- Maintain the same resource set and access rules on each SMA appliance in the GTO service. The best way to do this is to define one central policy on the CMS and synchronize it with all the managed SMA appliances.

- Use only DHCP tunnel address pools at each SMA deployment site. Other types of address pools can be used, but managing SMA appliances with different configurations is difficult. However, this can be done and is described in Varying tunnel address pools on page 19.

- Use a single authentication server configuration for all SMA appliances. If necessary, use transparently-distributed authentication services. CMS policy replication does include support for varying the authentication server configurations at each SMA appliance. You can do this by configuring locally-replicated authentication servers at the SMA appliance console. See Using distributed authentication servers on page 18.

- Use wildcard certificates for user access. GTO makes all of its SMA appliances available under a variety of names, each of which must match the certificate. It is possible to identify all such names each time the configuration changes and generate certificates without wildcards, but the process is tricky and error-prone. It is recommended that you use wildcard certificates.
Choosing a GTO service name and establishing DNS delegations

To establish a GTO service, you must choose a GTO service name and establish DNS delegations.

Topics
- Choosing a GTO service name
- Establishing the GTO service name delegations in DNS

Choosing a GTO service name

The GTO service name is a delegated DNS zone, which means you must control the parent zone and make a delegation from it to one or more SMA appliances under the GTO service.

If your organization controls the example.com DNS zone, the access.example.com or vpn.example.com could be appropriate GTO service names.

Establishing the GTO service name delegations in DNS

A GTO service name delegation is a DNS subzone delegation. It requires NS records that identify the authoritative server names for the subzone, and corresponding glue-A record that provides IP addresses for those authoritative server names.

The authoritative servers themselves are SMA appliances that are part of the GTO service and are identified by their public IP addresses and the NS record record names in the following format:

   DNSname dot ns dot GTOserviceName

For example, the following two DNS records in the zone configuration of example.com could establish a delegation for the GTO service and SMA appliance described above:

   access.example.com 86400 IN NS node1.ns.access.example.com.
   node1.ns.access.example.com 86400 IN A 123.231.55.77

In a typical GTO deployment with multiple SMA appliances, it is important to establish at least two such delegations. This ensures that the GTO service will remain available if any one the SMA appliances is brought down for maintenance (or a network outage).

At least one authoritative server (SMA appliance) must be running at any given moment. Otherwise, users will not be able to connect.

Additional authoritative servers can provide redundancy and improved performance for some users. You should limit GTO service delegations to about three. Ideally, they should be geographically distributed.
Provisioning certificates

You must provision certificates on the GTO-enabled SMA appliances to facilitate the GTO service. Certificates, which give connecting users proof of SMA authenticity before they submit credentials, must be configured on each individual SMA appliance. A single wildcard certificate naming both the GTO service name and all names underneath it (such as access.example.com and *.access.example.com) can be copied onto every SMA appliance.

The CMS console Dashboard provides convenient links to the management consoles of each SMA appliance, where certificates are uploaded under SSL Settings.

You can generate a CSR for a certificate that is appropriate for all the SMA appliances in the GTO service.

To generate a CSR for a certificate that is appropriate for all the SMA appliances in the GTO service:

1. Go to the Certificate Signing Requests page.
2. In the Fully Qualified Domain Name field, enter the GTO service name.
3. In the Alternate Names field, enter the corresponding wildcard name (such as *.access.example.com).
Setting up GTO

This section describes how to configure a basic GTO deployment, consisting of a CMS that manages at least one SMA appliance.

Topics
- Setting up the CMS and SMA appliances
- Setting up a basic GTO deployment
- Registering an SMA appliance with the CMS
- Defining the central policy

Setting up the CMS and SMA appliances

Before you can configure the Global Traffic Optimizer (GTO), you must first set up a CMS and at least one SMA appliance.

Set up a CMS by following the instructions in the Dell SMA Central Management Server Administration Guide for establishing a CMS virtual machine to control the GTO service and manage the configuration of its component SMA appliances.

Set up at least one SMA appliance by following the instructions in the Dell SMA Administration Guide. Follow the initial Setup Wizard configuration steps for cabling, administrator password, internal and external interface addresses, routing mode, and gateways, etc.

**NOTE:** Single-homed SMA appliances and SMA appliances configured in a high-availability cluster are not supported by GTO.
Setting up a basic GTO deployment

After you set up the Central Management Server (CMS) and at least one SMA appliance, you can set up a basic GTO deployment.

To set up a basic GTO deployment:

1. On the CMS, go to the Management Server > Configure page.

2. Select the Central Management Settings page. The Central Management Settings dialog appears.

3. Under Central User Licensing, select the checkbox for Enable managing appliance user licensing with one central license. The current license will support 500 concurrent user sessions across all appliances.

4. Under Global Traffic Optimizer Service, select the checkbox for Users connect to a service from anywhere in the world and are routed to the nearest managed appliance.
After you enable the **Global Traffic Optimizer Service**, the following message is displayed:

> The service name must be delegated in public DNS, see the admin guide for details.

5. In the **Service name** field, enter the name of your service. For example, `access.example.com`.

6. Under **Policy Synchronization**, select the checkbox for **Enable pushing policy configuration from this server to managed appliances**. This feature is recommended so that users will have a consistent experience on all GTO-enabled appliances.

7. Under **Authentication servers**, select **Nodes in the collection share centralized authentication servers**.

8. Go back to the **Management Server > Configure** page.

9. Select **Licensing**.
   The **Manage Licenses** page appears.

10. Click **Register**.

**NOTE:** The **Global Traffic Optimizer Service** checkbox is grayed out if **Central User Licensing** is not enabled. You must enable **Central User Licensing** before you can enable the **Global Traffic Optimizer Service**.
Registering an SMA appliance with the CMS

After you configure GTO on the CMS, you must register the SMA appliance with the CMS.

To register the SMA appliance with the CMS:

1. On the CMS, go to Managed Appliances > Add/Remove.
2. Click the New button. The Register new appliance dialog appears.
3. In the Name field, enter a name for the new appliance. For example, Seattle-01.
4. In the Internal IP or host field, enter the IP address for the new appliance.
5. In the One Time Password field, enter the one time password obtained from the Maintenance > Central Management page of the Dell SMA appliance.
6 Click **OK**. This registers the appliance with the CMS and adds it to the CMS list. The dialog changes with more options.

7 From the **Country** menu, select the country where the appliance is located.

8 In the **Location** field, enter the city, state, or province where the appliance is located.

9 Select the checkbox for **Enable Global Traffic Optimizer Service**.

10 In the **DNS name** field, enter a unique DNS-legal name for this appliance, for example `seattle01`.

11 In the **Public IP** field, enter the internet-visible, public IP address for this appliance. This should be the address by which remote users will access this appliance. The default IP address is the external IP address of the appliance. The public IP address may be different from its external IP address if the public WAN addresses are using NAT at the DMZ.

   **NOTE:** The client certificate warning, **DNS name** field, and **Public IP** field are only visible when CMS is enabled for GTO.

12 Select the checkbox for **Send user connections to this appliance**, so that users connecting to `access.example.com` may be routed to this appliance.

13 Click **Save**.
Defining the central policy

From the Central Management Console (CMS), you can define the central policy for a single-appliance SMA deployment. You can define the policies for your authentication servers and realms, resources and access rules, web and tunnel access methods, end-point control, and so on.

**NOTE:** The steps in this section are optional.

To define the central policy:

1. On the CMS, go to the Managed Appliances > Configure > Define policy page.

2. Define the policies you want. See the following sections for instructions on defining server certificates, authentication servers, and tunnel address pools:
   - **Enabling cached credentials** on page 17
   - **Using distributed authentication servers** on page 18
   - **Varying tunnel address pools** on page 19
3 When you have finished defining your policy, click **Apply Pending Changes** and follow the link in the results dialog to synchronize this new policy with the managed SMA appliance.

4 On the **Synchronize policy** page, select the checkbox for the SMA appliance you want to synchronize.

5 Click **Synchronize**.

   The message, “Synchronizing data, please wait…” appears as the policy is overwritten by the central policy.

6 When policy synchronization has completed, the screen displays the **Status** as **Synchronization finished**.

   You can now type the GTO service name into the address bar of any standard Internet Web browser, anywhere in the world, and sign in to securely access the configured resources.
Extending GTO Deployment

Topics
- Adding additional SMA appliances
- Enabling cached credentials
- Using distributed authentication servers
- Varying tunnel address pools
- Additional deployment notes

Adding additional SMA appliances

Additional SMA appliances can be added to the basic GTO configuration by following the steps in Setting up GTO on page 10. Each SMA appliance that is added automatically begins serving new requests for GTO user connections.

When a new SMA appliance is added to a different location than the existing appliances, it becomes available to GTO. When GTO evaluates a new user relative to the available SMA appliances, it includes the new appliance at the different location, and directs the new connection to the appropriate SMA appliance. This evaluation is repeated each time a user connects. GTO may connect users to different SMA appliances in different circumstances.

Enabling cached credentials

If your security settings allow cached credentials on end-user devices, you can assign nearly-seamless failover and high-availability capabilities to Connect Tunnel clients and Mobile Connect SSL VPN Tunnel clients. You can do this even if the SMA appliances are in different locations (and therefore do not share an internal network).

To enable cached credentials:
1. Go to the Managed Appliances > Configure page.
2. Go to Realms > Community > Access Methods > Tunnel.
3. Click the Configure button.
Using distributed authentication servers

The latency and reliability of authentication services can be improved in some situations by replicating authentication servers in widely-distributed locations, and configuring specific SMA appliances to use a nearby replicated authentication server instead of the central instance, which might be on another continent.

To accomplish this, first establish the authentication server settings in the central policy and then synchronize the central policy with all the managed SMA appliances. See Setting up a basic GTO deployment on page 11. Then, on the Management Server > Configure > Central Management Settings page, change the Policy synchronization settings so that the Each node has its own authentication server option is selected.

Click Save and Apply Pending Changes.

Now the central authentication server settings will only be pushed to appliances during policy synchronization if an authentication server of the same name does not already exist at the SMA managed appliance. Stated another way, if an SMA appliance already has an authentication server setting whose name matches a name configured at the CMS, that setting will not be touched during policy synchronization.

For each SMA appliance that needs local modifications to authentication server settings, log onto the management console at that appliance and adjust the configuration of the existing authentication server(s).

As long as each central policy authentication server has a corresponding SMA policy authentication server with the same name, your local changes will be preserved. Don’t create or delete authentication servers from the SMA policy as you cannot modify other parts of the local configuration that reference these servers. Those changes will be overwritten the next time CMS synchronizes the central policy with this SMA.
Varying tunnel address pools

The preferred tunnel address pool policy for GTO deployments is a single DHCP pool replicated to all SMA appliances, with no specific DHCP server mentioned in the policy. This is done using the **Routed address pool - dynamic** setting and not specifying a DHCP server (as shown below), so that appliances send broadcast requests to locate DHCP servers that can allocate addresses. This requires DHCP services to be available on the internal network that the appliances are on. Other policies are possible, but CMS does not help maintain them.

A tunnel address pool in the SMA policy will not be overwritten during policy synchronization if there is a corresponding tunnel address pool in the central policy with the same name. Be aware though, that the CMS will not synchronize with an SMA appliance at all if a tunnel address pool exists at the SMA appliance, but not in the CMS configuration. So the trick here is to create a tunnel address pool at the CMS, synchronize the central policy to all SMA appliances (to create the pool there), then adjust the configuration of that pool at each individual SMA appliance.

**NOTE:** You can adjust the parameters of pools (such as the address ranges in static pools or the NAT-from address in a NAT pool), but you cannot change the pool’s type.

Additional deployment notes

It is recommended that you configure a minimum of two SMA appliances, and that you delegate them in DNS as authoritative servers to minimize the likelihood that your users ever lose DNS resolution of the GTO service.

You must enable UDP 53 on your firewall for all traffic that is sent to CMS-managed appliances that are configured as authoritative servers.
Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.software.dell.com.

- Contacting Dell on page 20
- Technical support resources on page 20

Contacting Dell

Technical support:
Online support

Product questions and sales:
(800) 306-9329

Email:
info@software.dell.com

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to https://support.software.dell.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the portal provides direct access to product support engineers through an online Service Request system.

The site enables you to:
- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to Trial Downloads.
- View how-to videos
- Engage in community discussions
- Chat with a support engineer