IDGo 800 Minidriver for Windows
Integration Guide

Using IDGo 800 Minidriver for Windows for Blue Coat ProxySG
## Contents

- Third-Party Software Acknowledgement ........................................................................................................... 4
- Description ........................................................................................................................................................... 4
- Applicability .......................................................................................................................................................... 5
- Environment .......................................................................................................................................................... 5
- Audience .............................................................................................................................................................. 5
- CBA Flow using IDGo 800 ..................................................................................................................................... 5
- Prerequisites ........................................................................................................................................................ 6
- Supported Smart Cards in IDGo 800 Minidriver for Windows ........................................................................... 6
  - Smart Cards ....................................................................................................................................................... 6
- Configuring Blue Coat ProxySG .......................................................................................................................... 6
  - Configuring a CA Certificate List ..................................................................................................................... 7
  - Configuring a Certificate Realm ..................................................................................................................... 14
  - Configuring the HTTPS Reverse Proxy Service ............................................................................................. 18
  - Configuring an Authentication Policy ........................................................................................................... 19
- Running the Solution ........................................................................................................................................... 27
- Support Contacts .................................................................................................................................................. 29
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Blue Coat ProxySG.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

Customers today are looking to desktop virtualization to transform static desktops into dynamic mobile workspaces that can be centrally and securely managed from the datacenter, and accessed across a wide range of devices and locations. Deploying desktop virtualization without strong authentication is like putting your sensitive data in a vault (the datacenter), and leaving the key (user password) under the door mat. A robust user authentication solution is required to screen access and provide proof-positive assurance that only authorized users are allowed access.

IDGo 800 is a cryptographic middleware suite that enables enterprises to manage access to physical and network security systems through use of Gemalto IDPrime smart cards. IDGo 800 protects against unauthenticated network access and online identity theft. In addition, it supports certificate-based services for strong authentication, digital signature, data encryption, and secure remote access.

The IDGo 800 middleware suite consists of three components:

- **Minidriver**—This is a Gemalto-proprietary read/write minidriver that is compliant with the Microsoft Minidriver V7 specification.

  The IDGo 800 Minidriver supports both IDPrime MD (refer to the list in the IDGo release notes) and all IDPrime .NET smart cards.

- **PKCS#11 security module**—This is compliant with v2.20 of the PKCS#11 specification. It supports multiple PINs and elliptic curve algorithms.

- **Gemalto-proprietary Credential Provider (CP)**—This supports the loading and unblocking of multiple PINs and multiple PIN policies. It is available only for PCs running Windows 7 or later. If you do not require multiple PIN support, you can use the native Microsoft CP instead.

For information about the architecture of the IDGo 800 Minidriver, please refer to the *IDGo 800 Middleware Integration Guide*.

The Blue Coat ProxySG appliances provide complete control over all of your web traffic, delivering world-class threat protection. Robust features include user authentication, web filtering, data loss prevention, inspection, and visibility of SSL-encrypted traffic (including the ability to stream decrypted content to an external server with an Encrypted Tap license), content caching, bandwidth management, stream-splitting, and more.

The Blue Coat Secure Web Gateway Virtual Appliance (SWG VA) combines the market-leading security capabilities of Blue Coat ProxySG with the flexibility of virtualization to provide a cost-effective enterprise branch office solution. With the Blue Coat SWG VA, businesses can support web security and other critical remote office infrastructure on a common platform, reducing costs and IT resource requirements.

It is assumed that the Blue Coat ProxySG environment is already configured and working with static passwords prior to implementing Gemalto multi-factor authentication.

This document provides guidelines for deploying CBA for user authentication to Blue Coat ProxySG using Gemalto IDPrime MD smart cards.
**Applicability**

The information in this document applies to:

- **Gemalto IDGo 800 Minidriver**—A component of Gemalto’s IDGo 800 middleware that manages Gemalto’s smart cards
- **Blue Coat ProxySG**

**Environment**

The integration environment that was used in this document is based on the following software versions:

- **Gemalto IDGo 800 Minidriver**—Version 1.2.3.04
- **Gemalto PC USB-SL Reader**
- **Blue Coat ProxySG**—Version SGOS 6.5.6.4 SWG Edition
- **Blue Coat ProxySG (Virtual Appliance)**

**Audience**

This document is targeted to system administrators who are familiar with Blue Coat ProxySG, and are interested in adding certificate-based authentication capabilities using Gemalto smart cards.

**CBA Flow using IDGo 800**

The diagram below illustrates the flow of certificate-based authentication:

1. A user attempts to connect to the Blue Coat ProxySG server using the Blue Coat ProxySG client application. The user inserts the Gemalto IDPrime MD smart card (on which his/her certificate resides) into the smart card reader, and when prompted, enters the smart card PIN.
2. After successful authentication, the user is allowed access to internal resources.
Prerequisites

Before implementing certificate-based authentication for Blue Coat ProxySG using Gemalto smart cards, ensure the following:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. Note that any CA can be used. However, in this guide, integration is demonstrated using the Microsoft CA.
- Users must have a Gemalto IDPrime MD smart card enrolled with an appropriate certificate.
- IDGo 800 Minidriver for Windows should be installed on all client machines.
- Reverse proxy setup must be up and running.
- Client and Web Server Appliance certificates of type X.509 (issued from the same certificate authority) are required for testing purpose.

Supported Smart Cards in IDGo 800 Minidriver for Windows

IDGo 800 Minidriver supports the following smart cards that can be used as a second authentication factor for users who authenticate to Blue Coat ProxySG.

Smart Cards

- IDPrime MD 8840
- IDPrime MD 3840
- IDPrime MD 3810
- IDPrime MD 840
- IDPrime MD 830
- Optelio / Desineo D72
- Optelio R7
- IDPrime .NET
- Gemalto UICC in contact
- Card Emulation

Configuring Blue Coat ProxySG

Configuring Blue Coat ProxySG for CBA requires the following:

- Configuring a CA Certificate List, page 7
- Configuring a Certificate Realm, page 14
- Configuring the HTTPS Reverse Proxy Service, page 18
- Configuring an Authentication Policy, page 19
Configuring a CA Certificate List

Configuring a CA certificate list requires:
- Creating a Keyring, page 7
- Importing the Web Server Appliance Certificate, page 8
- Importing the Client CA Certificate, page 11
- Creating a CA Certificate List, page 13

Creating a Keyring

1. In a web browser, open the following URL, and then log in as an administrator:
   (\https://<ProxySG_IP_Address>:8082\)

   Where, <ProxySG_IP_Address> is the IP address of the ProxySG virtual appliance, and 8082 is the default management port.

2. On the Blue Coat ProxySG Management Console window, click the Configuration tab, and then in the left pane, click SSL > Keyrings.

3. In the right pane, on the Keyrings tab, click Create.
4. On the **Create Keyring** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Keyring name</th>
<th>Enter a name for the keyring (for example, <strong>Test</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private key visibility</td>
<td>Select <strong>Show key pair</strong>.</td>
</tr>
</tbody>
</table>

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

5. On the **Blue Coat ProxySG Management Console** window, in the right pane, the newly created keyring is listed. Click **Apply**.

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

**Importing the Web Server Appliance Certificate**

1. Copy the text of the Web Server Appliance certificate (including the **Begin Certificate** and **End Certificate** statements) to the system clipboard.
2. On the **Blue Coat ProxySG Management Console** window, click the **Configuration** tab, and then in the left pane, click **SSL > Keyrings**.

![Configuration tab](image1)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

3. In the right pane, on the **Keyrings** tab, select the keyring (for example, **Test**) that you created earlier in step 4 of “Creating a Keyring” on page 7, and then click **Edit**.

4. On the **Edit Keyring** window, under **Certificate**, click **Import**.

![Edit Keyring window](image2)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)
5. On the **Import Certificate** window, click **Paste From Clipboard**, and then click **OK**.

6. Click **Close**. 

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*
7. On the Blue Coat ProxySG Management Console window, click Apply.

8. A successful message is displayed. Click OK.

**Importing the Client CA Certificate**

A CA certificate verifies the identity of a Certificate Authority. It is used by Blue Coat ProxySG to verify the Web Server and Client certificates.

1. Copy the text of the CA certificate to the system Clipboard.
2. On the Blue Coat ProxySG Management Console window, click the Configuration tab, and then in the left pane, click SSL > CA Certificates.
3. In the right pane, on the CA Certificates tab, click Import.
4. On the **Import CA Certificate** window, perform the following steps:
   a. In the **CA Cert Name** field, enter the name of the CA certificate (for example, **ProxySGCA**).
   b. Click **Paste From Clipboard**.
   c. Click **OK**.

![Import CA Certificate window](image)

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*

5. On the **Blue Coat ProxySG Management Console** window, in the right pane, the CA certificate is listed. Click **Apply**.

![Blue Coat ProxySG Management Console](image)

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*

6. A successful message is displayed. Click **OK**.

![Changes Done Successfully](image)

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*
Creating a CA Certificate List

1. On the Blue Coat ProxySG Management Console window, click the Configuration tab, and then in the left pane, click SSL > CA Certificates.

2. In the right pane, on the CA Certificate Lists tab, click New.

3. On the Create CA Certificate List window, perform the following steps:
   a. In the CA Cert List Name field, enter a name for the certificate list (for example, ReverseProxyCCL).
   b. In the list box on the left, select the imported CA certificate (for example, ProxySGCA) that you imported earlier in step 4 of “Importing the Client CA Certificate” on page 11.
   c. Click Add >> to move the selected certificate to the list box on the right.
   d. Click OK.

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)
4. On the Blue Coat ProxySG Management Console window, in the right pane, the CA certificate list is listed. Click Apply.

5. A successful message is displayed. Click OK.

Configuring a Certificate Realm

Configuring a Certificate Realm requires:

- Creating a Certificate Realm, page 14
- Configuring the Certificate Realm Main Properties, page 16
- Configuring the Certificate Realm General Properties, page 17
Creating a Certificate Realm

1. On the Blue Coat ProxySG Management Console window, click the Configuration tab, and then in the left pane, click Authentication > Certificate.

2. In the right pane, on the Certificate Realms tab, click New.

3. On the Add Certificate Realm window, in the Realm name field, enter a name for certificate realm (for example, IDGo_CBA), and then click OK.

4. On the Blue Coat ProxySG Management Console window, in the right pane, the newly created certificate realm is listed. Click Apply.

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)
5. A successful message is displayed. Click OK.

![Changes Done Successfully](image)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

Configuring the Certificate Realm Main Properties

1. On the Blue Coat ProxySG Management Console window, click the Configuration tab, and then in the left pane, click Authentication > Certificate.

2. In the right pane, on the Certificate Main tab, in the Realm name field, select the certificate realm (for example IDGo_CBA) that you created earlier in step 3 of “Creating a Certificate Realm”, on page 15, and then click Add.

![Configuration Tab](image)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

3. On the Add OID window, enter the OID value, and then click OK.

![Add OID Window](image)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

NOTE: The OID value is available in the Enhanced Key Usage field of the client certificate.
4. On the Blue Coat ProxySG Management Console window, in the right pane, under Extended Key Usage, the OID value is listed. Click Apply.

![Extended Key Usage Screen](image)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

5. A successful message is displayed. Click OK.

![Successful Configuration](image)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

### Configuring the Certificate Realm General Properties

1. On the Blue Coat ProxySG Management Console window, click the Configuration tab, and then in the left pane, click Authentication > Certificate.

2. In the right pane, on the Certificate General tab, complete the following fields, and then click Apply.

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realm name</td>
<td>Select the certificate realm (for example IDGo_CBA) that you created earlier in step 3 of “Creating a Certificate Realm” on page 15.</td>
</tr>
<tr>
<td>Virtual URL</td>
<td>Enter the virtual URL configured for the reverse proxy setup.</td>
</tr>
</tbody>
</table>

![Certificate General Tab](image)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)
3. A successful message is displayed. Click OK.

![Changes Done Successfully](image1)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

**Configuring the HTTPS Reverse Proxy Service**

Ensure that your reverse proxy setup is up and running before configuring the HTTP reverse proxy service.

1. On the Blue Coat ProxySG Management Console window, click the Configuration tab, and then in the left pane, click Services > Proxy Services.

![Proxy Services](image2)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

2. In the right pane, on the Proxy Services tab, expand Reverse_proxy, select the HTTPS service (for example, HTTPS-Rev that you created at the time of creating the reverse proxy setup), and then click Edit Service.

![Edit Service](image3)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)
3. On the **Edit Service** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th><strong>Keyring</strong></th>
<th>Select the keyring (for example, Test) that you created earlier in step 4 “Creating a Keyring” of on page 7.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CCL</strong></td>
<td>Select the CA Certificate List (for example, ReverseProxyCCL) that you created earlier in step 3 of “Creating a CA Certificate List” on page 13.</td>
</tr>
<tr>
<td><strong>Verify Client</strong></td>
<td>Select this option.</td>
</tr>
</tbody>
</table>

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

## Configuring an Authentication Policy

With an authentication realm configured, now configure a policy on the ProxySG appliance to authenticate, log, and control user access to the web server.

The sections below explain about setting up rules to authenticate users, restrict access for specific users and groups, and deny all other access to the web server.
Creating the Web Authentication Layer

1. On the **Blue Coat ProxySG Management Console** window, click the **Configuration** tab, and then in the left pane, click **Policy > Visual Policy Manager**.

![Visual Policy Manager](image1)

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*

2. In the right pane, click **Launch**.

3. On the **Blue Coat Visual Policy Manager** window, click **Policy > Add Web Authentication Layer**.

![Web Authentication Layer](image2)

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*

4. On the **Add New Layer** window, enter a name for the web authentication layer, and then click **OK**.

![Add New Layer](image3)

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*
5. On the **Blue Coat Visual Policy Manager** window, on the newly created authentication layer (for example, **Web Authentication Layer**), right-click in the **Action** column of the default rule, and then click **Set**.

6. On the **Set Action Object** window, click **New > Authenticate**.

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*
7. On the **Add Authenticate Object** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the authenticate object (for example, <strong>Authenticate</strong>).</td>
</tr>
<tr>
<td>Realm</td>
<td>Select the certificate realm (for example, <strong>IDGo_CBA</strong>) that you created earlier in step 3 of “Creating a Certificate Realm” on page 15.</td>
</tr>
<tr>
<td>Mode</td>
<td>Select <strong>Auto</strong>.</td>
</tr>
</tbody>
</table>

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

8. On the **Set Action Object** window, click **OK**.

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)
Creating a Web Access Layer

Create a policy rule that enables the ProxySG appliance to grant users access to the network.

1. On the Blue Coat ProxySG Management Console window, click the Configuration tab, and then in the left pane, click Policy > Visual Policy Manager.

2. In the right pane, click Launch.


4. On the Add New Layer window, enter a name for the web access layer, and then click OK.
5. On the **Blue Coat Visual Policy Manager** window, on the newly created web access layer (for example, **Web Access Layer**), right-click in the **Source** column of the default rule, and then click **Set**.

![Image of Blue Coat Visual Policy Manager window](image)

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*

6. On the **Set Source Object** window, select **Authenticated User**, and then click **OK**.

![Image of Set Source Object window](image)

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*
7. On the **Blue Coat Visual Policy Manager** window, on the newly created web access layer (for example, **Web Access Layer**), right-click in the **Action** column of the default rule, and then click **Allow**.

![Image of Blue Coat Visual Policy Manager](image1.png)

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*

8. The icon in the **Action** column changes from red to green. Click **Install policy**.

![Image of Blue Coat Visual Policy Manager](image2.png)

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*
9. A successful message is displayed. Click OK.

![Policy Installed dialog box](image)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

Creating a CPL Layer

1. On the **Blue Coat ProxySG Management Console** window, click the **Configuration** tab, and then in the left pane, click **Policy > Visual Policy Manager**.

![Configuration tab](image)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

2. In the right pane, click **Launch**.

3. On the **Blue Coat Visual Policy Manager** window, click **Policy > Add CPL Layer**.

![Add New Layer window](image)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

4. On the **Add New Layer** window, enter a name for the CPL layer, and then click **OK**.

![Add New Layer dialog box](image)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)
5. On the Blue Coat Visual Policy Manager window, on the CP Layer tab, enter the following code:

```xml
<Proxy> ssl.proxy_mode = https-reverse-proxy authenticate(<certificate realm>)
```

Where, `<certificate realm>` is the certificate realm (for example IDGo_CBA) that you created earlier in step 3 of “Creating a Certificate Realm” on page 14.

6. Click Install policy.
7. Click OK.

---

Running the Solution

Ensure that the Blue Coat ProxySG virtual appliance is configured as a reverse proxy with HTTPS service. Also, a user certificate must be present in Gemalto IDPrime 800 cards.

This integration is tested with the following Gemalto cards:

- IDPrime MD 830
- IDPrime MD 840
- IDPrime MD 8310
- IDPrime MD 3840
1. In a web browser, open the following URL:

   https://<Virtual IP of Blue Coat>

   Where, <Virtual IP of Blue Coat> is an IP address that is configured on the Blue Coat ProxySG appliance.

2. The browser displays all the certificates available on the machine. Select the end user certificate that is added on the Gemalto IDGo 800 card.

3. You will be redirected to the Confirm Certificate window. Click OK.

   (The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

4. On the Microsoft Smart Card Provider window, enter the smart card PIN, and then click OK.

   (The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

After successful authentication, you are redirected to access the web page.
Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Gemalto, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td>Phone</td>
<td>United States</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td></td>
<td>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>