SafeNet Authentication Client
Integration Guide
Using SafeNet Authentication Client CBA for BIG-IP® ACCESS Policy Manager™ (APM)
Contents

Third-Party Software Acknowledgement........................................................................................................................................... 4
Description......................................................................................................................................................................................................................... 4
Applicability............................................................................................................................................................................................................... 5
Environment .............................................................................................................................................................................................................. 5
Audience.................................................................................................................................................................................................................... 5
CBA Flow using SafeNet Authentication Client.................................................................................................................................................................................. 5
Prerequisites........................................................................................................................................................................................................... 6
Supported Tokens in SafeNet Authentication Client.................................................................................................................................................................................. 6
Configuring F5 BIG-IP APM......................................................................................................................................................................................................... 7
Adding Root CA Certificates...................................................................................................................................................................................................... 8
Configuring Client SSL Profiles.................................................................................................................................................................................................. 10
Configuring Webtop...................................................................................................................................................................................................... 12
Configuring the Webtop Links................................................................................................................................................................................................... 13
Configuring the Access Profile................................................................................................................................................................................................... 14
Editing the Access Profile................................................................................................................................................................................................... 15
   Adding On-Demand Certificate Authentication.................................................................................................................................................................................. 17
   Assigning a Custom Variable.................................................................................................................................................................................................. 18
   Adding the Log Custom Message Variable.................................................................................................................................................................................. 21
   Adding AD Query..................................................................................................................................................................................................... 22
   Adding Message box.................................................................................................................................................................................................... 23
Adding a Webtop............................................................................................................................................................................................................ 25
Configuring the Virtual Server....................................................................................................................................................................................................... 26
Running the Solution....................................................................................................................................................................................................... 29
After Successful Authentication................................................................................................................................................................................................. 30
DNS and NTP Settings on the BIG-IP System................................................................................................................................................................................................. 32
   Configuring DNS.................................................................................................................................................................................................. 32
   Configuring NTP..................................................................................................................................................................................................... 32
   Configuring the Active Directory Server........................................................................................................................................................................ 33
How to find the primary group ID................................................................................................................................................................................................. 34
Support Contacts..................................................................................................................................................................................................................... 36
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as BIG-IP® ACCESS Policy Manager™ (APM).

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

Remote access poses both a security and a compliance challenge to IT organizations. The ability to positively identify users (often remote users) requesting access to resources is a critical consideration in achieving a secure remote access solution. Deploying remote access solution 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.

PKI is a strong effective authentication solution to the functional, security, and compliance requirements.

SafeNet Authentication Client (SAC) is a public key infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. SafeNet certificate-based tokens provide secure remote access, as well as other advanced functions, in a single token, including digital signing, password management, network logon, and combined physical/logical access.

The tokens come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are interfaced using a single middleware client, SafeNet Authentication Client (SAC). The SAC generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications, offering secure web access, secure network logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

BIG-IP Access Policy Manager (APM) is a flexible, high-performance access and security solution that provides unified global access to your applications and network. By converging and consolidating remote access, LAN access, and wireless connections within a single management interface, and providing easy-to-manage access policies, BIG-IP APM helps you free up valuable IT resources and scale cost-effectively.

BIG-IP APM protects your public-facing applications by providing policy-based, context-aware access to users while consolidating your access infrastructure. It also provides secure remote access to corporate resources, such as Microsoft Exchange, SharePoint, and VDI, from all networks and devices.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to F5 BIG IP APM using SafeNet tokens.

It is assumed that the F5 BIG IP APM environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

F5 BIG IP APM can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with SafeNet products.
Applicability

The information in this document applies to:

- SafeNet Authentication Client (SAC)—SafeNet Authentication Client is the middleware that manages SafeNet tokens.
- F5 BIG IP APM

**NOTE:** This guide is applicable to both BIG-IP VE and BIG-IP Hardware appliance.

Environment

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

- SafeNet Authentication Client (SAC)—10.2
- F5 BIG IP APM—12.0

Audience

This document is targeted to system administrators who are familiar with F5 BIG IP APM, and are interested in adding multi-factor authentication capabilities using SafeNet tokens.

CBA Flow using SafeNet Authentication Client

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

1. A user attempts to connect to the F5 BIG IP APM server using a browser. The user inserts the SafeNet token on which his certificate resides, and, when prompted, enters the token password.
2. After successful authentication, the user is allowed access to internal resources.
Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificate-based authentication for F5 BIG IP APM using SafeNet tokens:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. In general, any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.
- If SAM is used to manage the tokens, Token Policy Object (TPO) should be configured with MS CA Connector. For further details, refer to the section “Connector for Microsoft CA” in the SafeNet Authentication Manager Administrator Guide.
- Users must have a SafeNet token with an appropriate certificate enrolled on it.
- SafeNet Authentication Client 10.2 must be installed on all client machines.

Supported Tokens in SafeNet Authentication Client

SafeNet Authentication Client supports a number of tokens that can be used as a second authentication factor for users who authenticate to F5 BIG IP APM.

SafeNet Authentication Client 10.2 (GA) supports the following tokens:

**Certificate-based USB tokens**

- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID

**Smart Cards**

- SafeNet eToken 4100
- IDPrime MD 840
- IDPrime MD 840 B
- IDPrime MD 3840
- IDPrime MD 3840 B
- IDPrime MD 830-FIPS
- IDPrime MD 830-ICP
- IDPrime MD 830 B
- IDPrime MD 3810
- IDPrime MD 3811
- IDPrime .NET (only SAC PKCS#11 and IDGo 800 Minidriver interfaces)
Certificate-based Hybrid USB Tokens

- SafeNet eToken 7300
- SafeNet eToken 7300-HID
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)

Software Tokens

- SafeNet Virtual Token
- SafeNet Rescue Token

Configuring F5 BIG-IP APM

A virtual server is created on BIG-IP, on which an Access Policy is applied. To set up the virtual server, log in to the management portal of APM as a BIG-IP administrator. Configure the Access Policy, Webtop, and the virtual server.

**NOTE:** If the virtual server and Webtop are already configured on BIG-IP APM, skip the configuration steps for the virtual server and Webtop. Edit the Access Profile accordingly.

To access the management portal of F5 BIG-IP APM:

1. Browse to the public DNS/public IP of the BIG-IP APM Amazon instance.

   ![Management Portal](image)

   *(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)*

2. Enter administrator login credentials and then click **Log in**.

   On successful authentication, you are logged in as an administrator in the management portal.
Adding Root CA Certificates

1. Click System on the left side of the screen, then select File Management>SSL Certificate List>Import.

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

The SSL Certificate/Key Source window opens.

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
2. Complete the **SSL Certificate/Key Source** fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import Type</td>
<td>Select <strong>Certificate</strong> from the drop-down menu.</td>
</tr>
<tr>
<td>Certificate Name</td>
<td>Select <strong>Create New</strong> and enter a name in the Certificate Name field</td>
</tr>
<tr>
<td>Certificate Source</td>
<td>Select <strong>Upload File</strong> to upload the root CA (mentioned in the prerequisites).</td>
</tr>
</tbody>
</table>

3. Click **Import**.

4. To check the imported Root CA click **System>File Management>SSL Certificate List**. The list of imported certificates are displayed.

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
Configuring Client SSL Profiles

1. Click the **Main** tab, then click **Local Traffic>Profiles>SSL>Client**.

   ![Screen Image](image1)

   (The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

   The **Client Profile List** window opens.

2. Click **Create** on the top right of the screen.

   ![Screen Image](image2)

   (The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

   The **New Server SSL Profile** window opens.

3. Enter a unique profile name in the **Name** field.

4. Select **clientssl** in from the **Parent Profile** drop-down list.
5. Scroll down to the **Client Authentication** area and select the **Custom** check-box at the top right corner to enable the Client Authentication fields.

![Client Authentication](image)

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

6. Complete the **Client Authentication** fields as follows.

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Certificate</strong></td>
<td>Select <strong>Request</strong></td>
</tr>
<tr>
<td><strong>Trusted Certificate Authorities</strong></td>
<td>Select the root CA that was defined in Adding Root CA Certificates</td>
</tr>
</tbody>
</table>
Configuring Webtop

When a user is allowed access based on an Access Policy, that user is typically assigned a Webtop. A Webtop is the successful endpoint for a Web application or a network access connection.

To create a Webtop:

1. Go to **Access Policy>Webtops>Webtop List** and click the + icon.
2. Complete the **General Properties** fields as follows.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a Webtop name</td>
</tr>
<tr>
<td>Type</td>
<td>Select Full from the drop-down menu</td>
</tr>
</tbody>
</table>

3. Click **Finished**.

### Configuring the Webtop Links

Webtop links are the links to the resources, for example: Rupiwebtop, that are being added to the Webtop. After successful authentication, the links to the resources will be displayed on the assigned Webtop.

**To create the Webtop links:**

1. Go to **Access Policy>Webtops>Webtop Links** and click the + icon.

2. Complete the **New Webtop Link** fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the Webtop link. For example, Rupiwebtop.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Type a description for this link.</td>
</tr>
<tr>
<td>Link Type</td>
<td>Select either Application URL or Hosted Contents. For example: if your resource is an application, select Application URL.</td>
</tr>
<tr>
<td>Application URL</td>
<td>This field is available only when Application URL is selected as the Link Type. Specify the URL of the application.</td>
</tr>
<tr>
<td>Hosted File</td>
<td>This field is available only when Hosted Contents is selected as the Link Type. Specify the hosted file.</td>
</tr>
<tr>
<td>Caption</td>
<td>By default, the caption is the same as the Webtop link name; however, it may be changed to a unique value if desired.</td>
</tr>
</tbody>
</table>

3. Click **Finished**.
Configuring the Access Profile

The Access Profile module is used to define the criteria for granting access to the various servers, applications, and other resources on the network.

To create an Access Profile:

   The General Properties window opens.

2. Complete the General Properties fields as follows:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a profile name e.g. SAS_OWA_Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Type</td>
<td>Select All from the drop-down menu. Leave all fields with their default settings.</td>
</tr>
</tbody>
</table>

3. Under Language Settings, select a language in the Factory Builtin Languages list and then click << to move the selected language to the Accepted Languages list.

4. Click Finished.
Editing the Access Profile

Using an Access Policy, you can define a sequence of checks to enforce the required level of security on a user system before a user is granted access to servers, applications, and other resources on your network.

An Access Policy can also include authentication checks to authenticate a user before access is granted to the network resources. The Access Policy can be edited as per requirements.

A sample Access Policy looks like this:

```
To edit the Access Profile:

1. From the main screen, go to Access Policy>Access Profiles List.

2. In the Access Profiles List tab, find the Access Policy you want to edit and then click Edit in the Access Policy column. The Visual Policy editor opens in a new window or a new tab, depending on your browser settings. This is the new blank policy that you have just created.
```
To view the Authentication, Authorization, and Accounting servers (AAA) as well as the resources assigned to an Access Policy:

2. From the Access Profiles list, select Access Profile.
3. Click the Access Policy tab.

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
Adding On-Demand Certificate Authentication

The logon page requires entering a username and password.

**To add a logon page on the local traffic virtual server:**

1. In the Visual Policy editor, click the + symbol after Start.

2. Click the Authentication tab, select On-Demand Cert Auth and click Add Item.

3. A properties screen opens after clicking on Add item.

4. From the Auth Mode list, select one of the following and click on Save:
   - **Request** - This is the default mode.
   - **Required** - For an iPod or an iPhone, this is mandatory.

   (While testing we used request)

   **NOTE:** To pass a certificate check using Safari, the certificate must be selected multiple times.

   (The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
Assigning a Custom Variable

1. In the Visual Policy editor, click the + symbol after the On-Demand Cert Auth>Successful branch.

2. Click the Assignment tab, select Variable Assign and click ADD Item.

3. Under Variable Assign, click ADD new entry and click on change.
4. Under Custom Variable and Custom Expression enter the following expressions and click Finished.
   - Custom Variable (Unsecure): session.logon.last.domain
   - Custom Expression:
     ```
     set upn [mcget {session.logon.last.upn}];
     if {{string first "@" $upn} >= 0} {
       return [string range $upn [expr { [string first "@" $upn] + 1 }] end ];
     } else {
       return "";
     }
     ```

5. Repeat the above to add another two expressions and click Save.

Variable Assignment 2:
   - Custom Variable (Unsecure): session.logon.last.username
   - Custom Expression:
     ```
     set upn [mcget {session.logon.last.upn}];
     if {{string first "@" $upn} >= 0} {
       return [string range $upn 0 [expr { [string first "@" $upn] - 1 }] ];
     } else {
       return $upn;
     }
     ```
Variable Assignment 3:

- **Custom Variable (Unsecure):** session.logon.last.upn
- **Custom Expression:**

  ```plaintext
  set e_fields [split [mcget {session.ssl.cert.x509extension}] "\n"];

  foreach qq $e_fields {
    if {[string first "othername:UPN" $qq] >= 0} {
      return [string range $qq [expr { [string first "<" $qq] + 1 } ] [expr { [string first ">" $qq] - 1 } ]];
    }
  }

  return "";
  ```

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
Adding the Log Custom Message Variable

1. Click the + icon after Variable Assign.

2. Click the General Purpose tab, select logging and click Add item

3. In the Log Message field, enter After cert parsing and click Add new entry.

4. Under Session Variables, select Custom from the drop-down list and in the empty field next to that, enter session.logon.last.username.

5. Click Save.
Adding AD Query

See the Appendix on page Error! Bookmark not defined. for details on how to configure the AD Server.

1. Click the + icon after Logging.

2. Click the Authentication tab and select AD Query from the list then click Add Item.

3. From the Server drop-down menu, select AD Server.

4. From the Fetch Primary Group drop-down menu, select Enabled.
5. Click the Branch Rules tab and then click **change**.

![Branch Rules](image)

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

6. In the **User's Primary Group ID** field, enter the primary group ID of the user. (See the Appendix on page Error! Bookmark not defined. for details on how to locate the Primary Group ID.

![User's Primary Group ID](image)

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

7. Click **Finished** and then click **Save**.

**Adding Message box**

1. Click on the + icon after AD Query (user primary group id is 100) branch.

![Add Item](image)

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

2. Click the **General Purpose** tab, select **Message Box** and then click **Add Item**.

![Message Box](image)

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
3. In the message field enter **AD qry ok** and click **Save**.

![Message Box](image)

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

4. Click the + icon after the fallback>AD query.

![Message Tree](image)

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

5. Add another message box as performed above and write **AD Qry failed** under message and click **Save**.

![Message Box](image)

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
Adding a Webtop

When a user is successfully authenticated, they are presented with a Webtop containing customized resources.

To add a Webtop:

1. Click the + icon after `fallback>Message Box 3`.

2. Click the **Assignment** tab, select Advanced Resource Assign, and then click Add Item.

3. Under **Resource Assignment**, click **Add new entry**.

4. Under **Expression**, click **Add/Delete**.

5. Select the Webtop Links and Webtop tabs to define each item.

6. Click **Update** for the expression. The **Resource Assignment** window becomes active.
7. Click **Save**.

8. The final visual policy editor looks as follows:

```
<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the virtual server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Enter the virtual server host IP address.</td>
</tr>
<tr>
<td>Service Port</td>
<td>Select HTTPS.</td>
</tr>
</tbody>
</table>
```

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

**Configuring the Virtual Server**

When using BIG-IP APM, virtual servers are configured with specific settings for network access connections or web application access. The IP address assigned to a host virtual server is the one that is typically exposed to the Internet.

With the Access Policy Manager, you can configure a remote access connection to one or more internal web applications. Using web applications, you create an Access Policy and local traffic virtual server so that end users can access internal web applications through a single external virtual server.

**To create a virtual server for a secure connection:**

1. Click the **Main** tab on the navigation pane, select **Local Traffic>Virtual Servers>Virtual Server List** and click +.

2. Complete the **New Virtual Server** fields as follows:
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Profile</td>
<td>Select HTTP.</td>
</tr>
<tr>
<td>SSL Profile (Client)</td>
<td>From the <strong>Available</strong> list, select the name of the Client SSL profile you previously created, and using the Move button, move the name to the <strong>Selected</strong> list.</td>
</tr>
<tr>
<td>SSL Profile (Server)</td>
<td>If your web application server is using HTTPS services, select the server SSL profile to use with this virtual server.</td>
</tr>
<tr>
<td>Access Profile</td>
<td>Select the Access Profile to associate with this virtual server. You must create an Access Profile before you define the virtual server as there is no default Access Profile available.</td>
</tr>
<tr>
<td>Rewrite Profile</td>
<td>If you are creating a virtual server to use with web applications, select the rewrite profile.</td>
</tr>
</tbody>
</table>

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
<table>
<thead>
<tr>
<th>Content Rewrite</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rewrite Profile</td>
<td>None</td>
</tr>
<tr>
<td>HTML Profile</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access Policy</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Profile</td>
<td>None</td>
</tr>
<tr>
<td>Connectivity Profile</td>
<td>None</td>
</tr>
<tr>
<td>Per-Request Policy</td>
<td>None</td>
</tr>
<tr>
<td>VDI Profile</td>
<td>None</td>
</tr>
<tr>
<td>Application Tunnels (Java &amp; Per-App VPN)</td>
<td>Enabled</td>
</tr>
<tr>
<td>DDM Support</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acceleration</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Class</td>
<td>None</td>
</tr>
<tr>
<td>OneConnect Profile</td>
<td>None</td>
</tr>
<tr>
<td>NTLM Conn Pool</td>
<td>None</td>
</tr>
<tr>
<td>HTTP Compression Profile</td>
<td>None</td>
</tr>
<tr>
<td>Web Acceleration Profile</td>
<td>None</td>
</tr>
<tr>
<td>SPDY Profile</td>
<td>None</td>
</tr>
</tbody>
</table>

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
3. Click **Finished**.

Running the Solution

Once the BIG-IP local traffic virtual server is configured with an appropriate Access Policy, the administrator provides users with the address of BIG-IP local traffic virtual server.

1. Browse to the local traffic virtual server configured in APM, select the certificate from the certificate list and click **OK**.

The SafeNet Authentication Client Logon window opens.
2. Enter the Token/smart card Name and Password and click **OK**. The **AD qry ok** window opens.

3. Click **Click here to continue**.

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

**After Successful Authentication**

On successful authentication:

1. Click the **Click here to continue** link. The Webtop assigned in the Access Policy is displayed.

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

2. Click the Webtop link (for example, **safenet** in the screen above). The resource page is displayed for the user to provide credentials for the exchange server.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
DNS and NTP Settings on the BIG-IP System

For BIG-IP APM, you must have DNS and NTP settings configured. To configure these settings, use the following procedures.

Configuring DNS

Configure DNS on the BIG-IP system to point to the corporate DNS server.

DNS lookups go out over one of the interfaces configured on the BIG-IP system, not the management interface. The management interface has its own separate DNS configuration.

The BIG-IP system must have a route to the DNS server. The Route configuration is done on the Main tab. Expand Network and then click Routes. For specific instructions on configuring a route on the BIG-IP system, see the BIG-IP online help or documentation.

1. Select the Main tab and click System>Configuration.
2. From the Device menu, click DNS.
3. In the Address field, under the DNS Lookup Server List row, enter the IP address of the DNS server.
4. Click Add.
5. Click Update.

Configuring NTP

For authentication to work properly, you must configure NTP on the BIG-IP system.

1. Select the Main tab and click System>Configuration.
2. From the Device menu, click NTP.
3. In the Address field, enter the fully-qualified domain name (or the IP address) of the time server that you want to add to the Address List.
4. Click Add.
5. Click Update.
Configuring the Active Directory Server

1. Go to **Main>Access Policy>AAA Server>Active Directory** and then click the + icon in the right corner of the window.

![Diagram showing Access Policy options](image)

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

2. Under **General Properties**, complete the details, and then click **Finished**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the authentication server you are creating.</td>
</tr>
<tr>
<td><strong>Domain Name</strong></td>
<td>Enter the Windows Domain name. You must enter the FQDN.</td>
</tr>
<tr>
<td><strong>Domain Controller Pool Name</strong></td>
<td>Enter the Active Directory server configured with this role.</td>
</tr>
<tr>
<td><strong>Admin Name</strong></td>
<td>Enter an administrator name that has Active Directory administrative permissions.</td>
</tr>
<tr>
<td><strong>Admin Password</strong></td>
<td>Enter the administrative password for the server.</td>
</tr>
<tr>
<td><strong>Verify Admin Password</strong></td>
<td>Enter the administrative password for the server again.</td>
</tr>
</tbody>
</table>
How to find the primary group ID

1. Go to the CA server and click **Start>Administrative tools>Active directory users and computers.**
2. Expand the domain name and click **Users.**
3. Right-click the user name of the user and click **Properties**.

4. Click the Attribute Editor tab and scroll down to the primary group id of that user.
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 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 1-410-931-7520</td>
</tr>
<tr>
<td>Technical Support</td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td>Customer Portal</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>