SafeNet Authentication Client

Integration Guide

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

gemalto
security to be free

¬¬ All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Doc Number: 007-013678-001, Revision A
Release Date: December 2016

Contents

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:

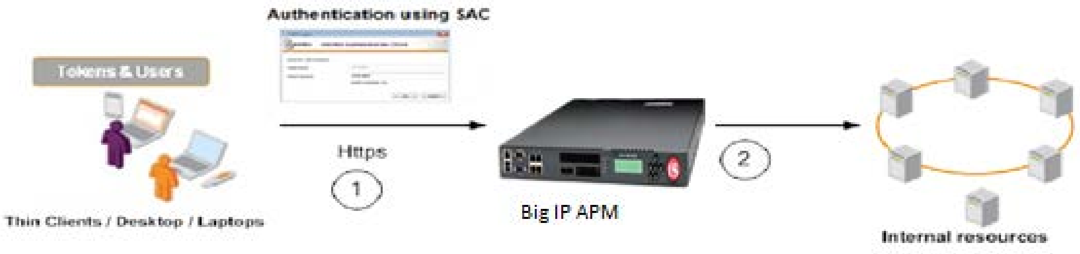
- SafeNet Authentication Client (SAC)—10.2
- F5 BIG IP APM—12.0

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

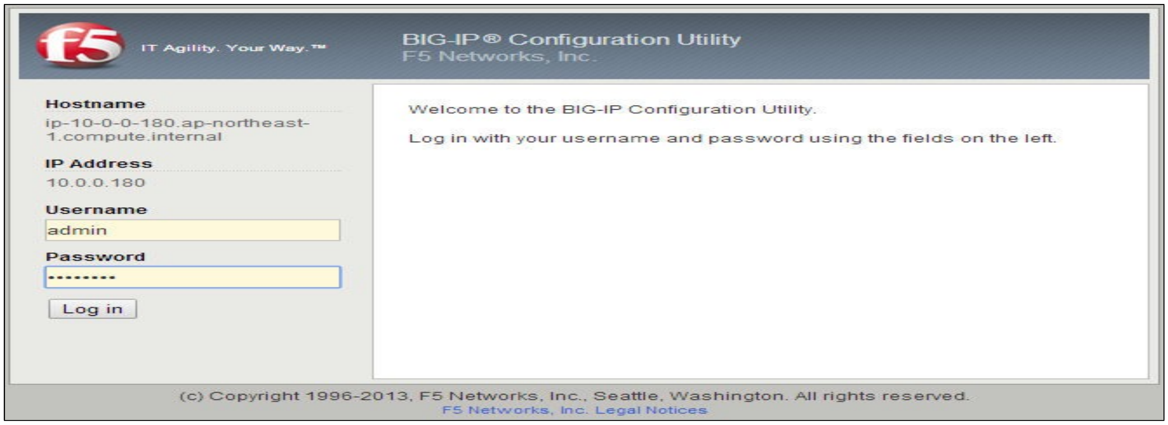
Configuring F5 BIG-IP APM

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.


f5
IT Agility. Your Way.™
BIG-IP® Configuration Utility
F5 Networks, Inc.
Log in
F5 Networks, Inc. Legal Notices

Hostname
ip-10-0-0-180.ap-northeast-1.compute.internal
IP Address
10.0.0.180
Username
admin
Password
•••••••••

Welcome to the BIG-IP Configuration Utility.

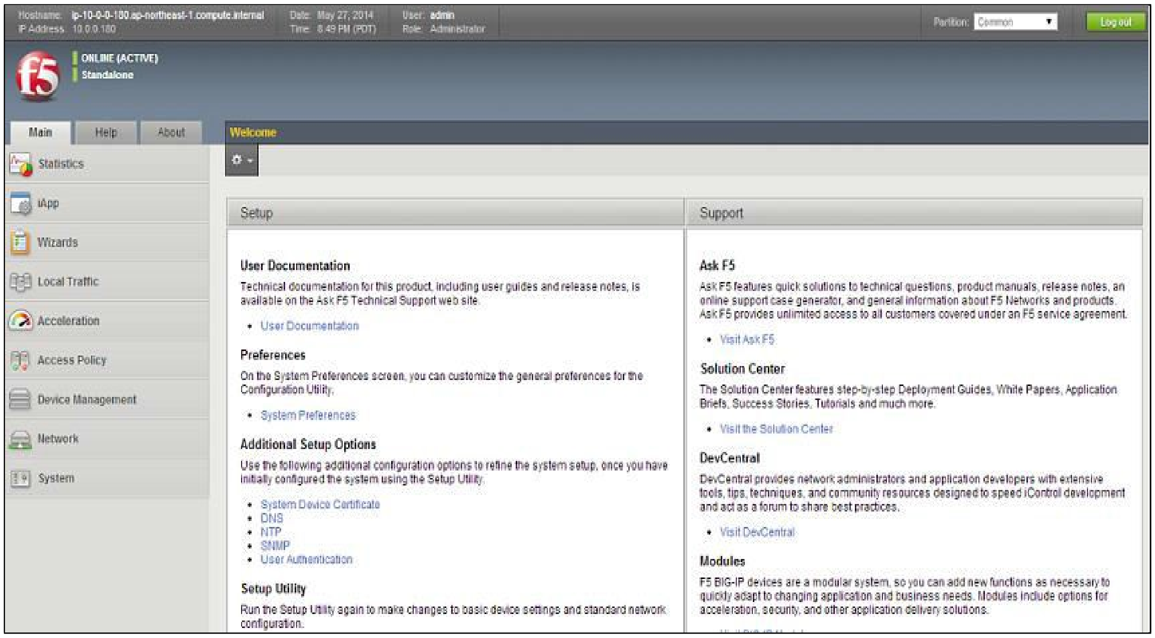
Log in with your username and password using the fields on the left.

(c) Copyright 1996-2013, F5 Networks, Inc., Seattle, Washington. All rights reserved.

(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.



Hostname: ip-10-0-0-180.ap-northeast-1.compute.internal
IP Address: 10.0.0.180
Date: May 27, 2014
Time: 8:49 PM (PDT)
User: admin
Role: Administrator
Partition: Common

ONLINE (ACTIVE)
Standalone

User Documentation

Technical documentation for this product, including user guides and release notes, is available on the Ask F5 Technical Support web site.

- User Documentation

Preferences

On the System Preferences screen, you can customize the general preferences for the Configuration Utility.

- System Preferences

Additional Setup Options

Use the following additional configuration options to refine the system setup, once you have initially configured the system using the Setup Utility.

- System Device Certificate
- DNS
- NTP
- SNMP
- User Authentication

Setup Utility

Run the Setup Utility again to make changes to basic device settings and standard network configuration.

Ask F5

Ask F5 features quick solutions to technical questions, product manuals, release notes, an online support case generator, and general information about F5 Networks and products. Ask F5 provides unlimited access to all customers covered under an F5 service agreement.

- Visit Ask F5

Solution Center

The Solution Center features step-by-step Deployment Guides, White Papers, Application Briefs, Success Stories, Tutorials and much more.

- Visit the Solution Center

DevCentral

DevCentral provides network administrators and application developers with extensive tools, tips, techniques, and community resources designed to speed iControl development and act as a forum to share best practices.

- Visit DevCentral

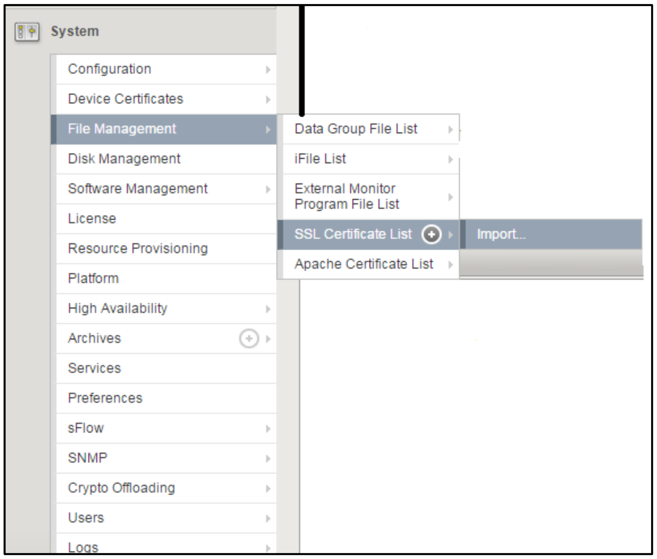
Modules

F5 BIG-IP devices are a modular system, so you can add new functions as necessary to quickly adapt to changing application and business needs. Modules include options for acceleration, security, and other application delivery solutions.

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

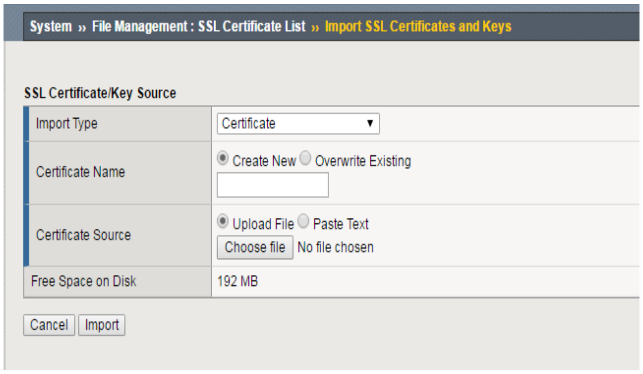
Adding Root CA Certificates

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.



System » File Management : SSL Certificate List » Import SSL Certificates and Keys

SSL Certificate/Key Source

Import Type	Certificate ▾
Certificate Name	● Create New ○ Overwrite Existing
Certificate Source	● Upload File ○ Paste Text Choose file No file chosen
Free Space on Disk	192 MB

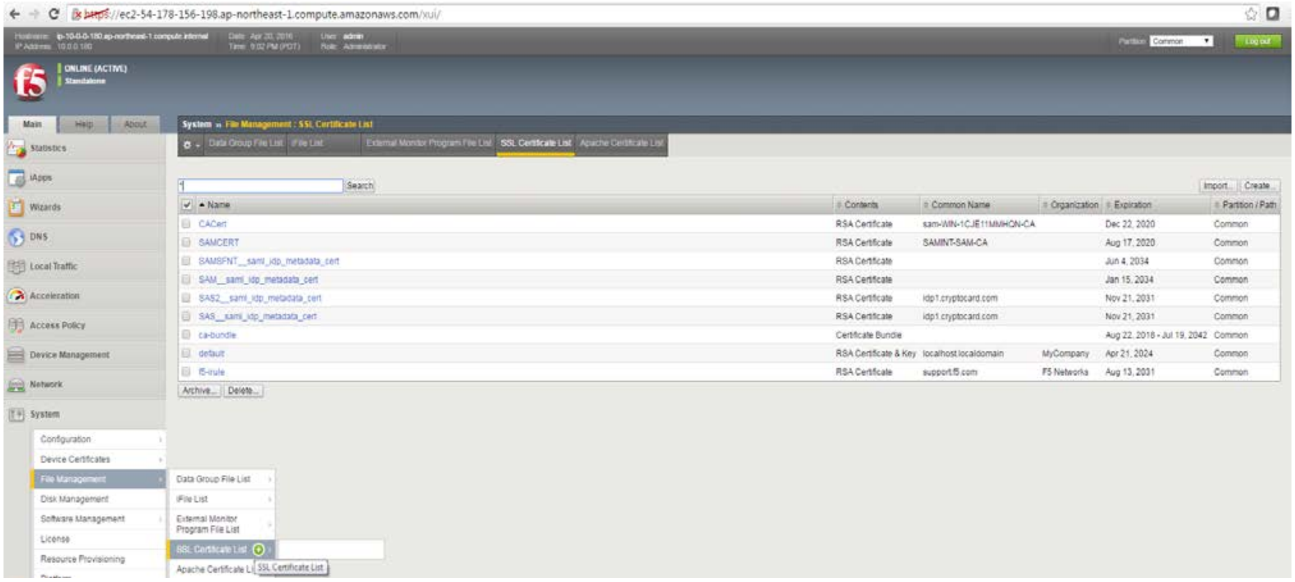
(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

2. Complete the **SSL Certificate/Key Source** fields as follows:

Import Type	Select **Certificate** from the drop-down menu.
Certificate Name	Select **Create New** and enter a name in the Certificate Name field
Certificate Source	Select **Upload File** to upload the root CA (mentioned in the prerequisites).

3. Click **Import**.

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



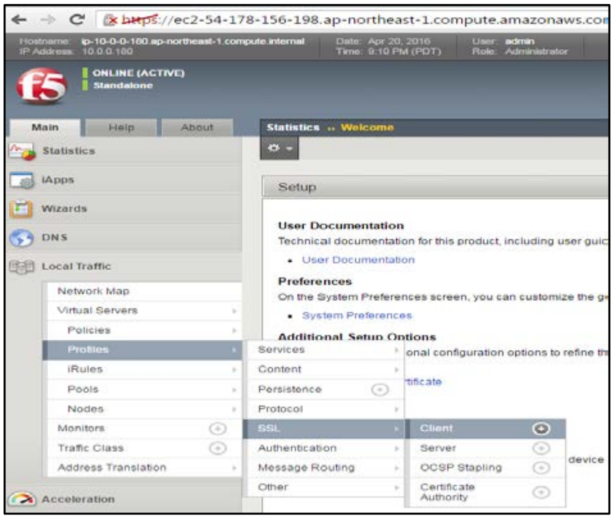
System » File Management : SSL Certificate List

Name	Contents	Common Name	Organization	Expiration	Partition / Path
CACert	RSA Certificate	sam-WIN-1CJE11MMHQN-CA		Dec 22, 2020	Common
SAMCERT	RSA Certificate	SAMINT-SAM-CA		Aug 17, 2020	Common
SAMSFNT__saml_idp_metadata_cert	RSA Certificate			Jun 4, 2034	Common
SAM__saml_idp_metadata_cert	RSA Certificate			Jan 15, 2034	Common
SAS2__saml_idp_metadata_cert	RSA Certificate	idp1.cryptocard.com		Nov 21, 2031	Common
SAS__saml_idp_metadata_cert	RSA Certificate	idp1.cryptocard.com		Nov 21, 2031	Common
ca-bundle	Certificate Bundle			Aug 22, 2018 - Jul 19, 2042	Common
default	RSA Certificate & Key	localhost.localdomain	MyCompany	Apr 21, 2024	Common
f5-irule	RSA Certificate	support.f5.com	F5 Networks	Aug 13, 2031	Common

(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**.



User Documentation

Technical documentation for this product, including user guic

- User Documentation

Preferences

On the System Preferences screen, you can customize the g

- System Preferences

Additional Setup Options

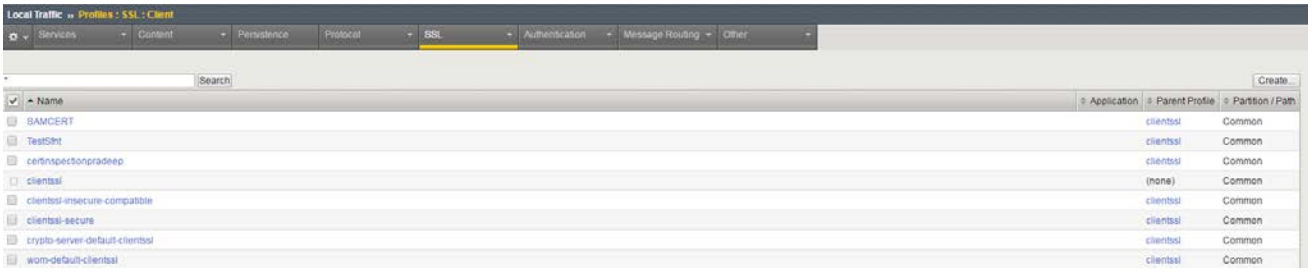
onal configuration options to refine th

tificate

device

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

The **Client Profile List** window opens.

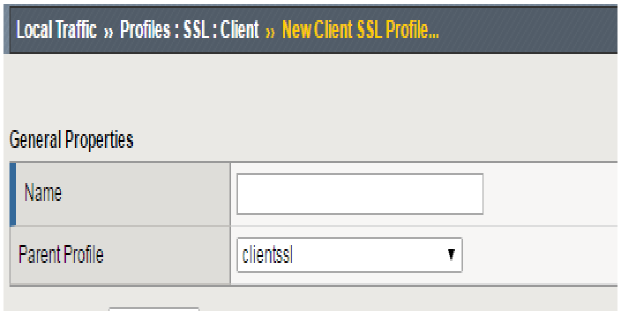


☑	Name	Application	Parent Profile	Partition / Path
□	SAMCERT		clientssl	Common
□	TestSfnt		clientssl	Common
□	certinspectionpradeep		clientssl	Common
□	clientssl		(none)	Common
□	clientssl-insecure-compatible		clientssl	Common
□	clientssl-secure		clientssl	Common
□	crypto-server-default-clientssl		clientssl	Common
□	wom-default-clientssl		clientssl	Common

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

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

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

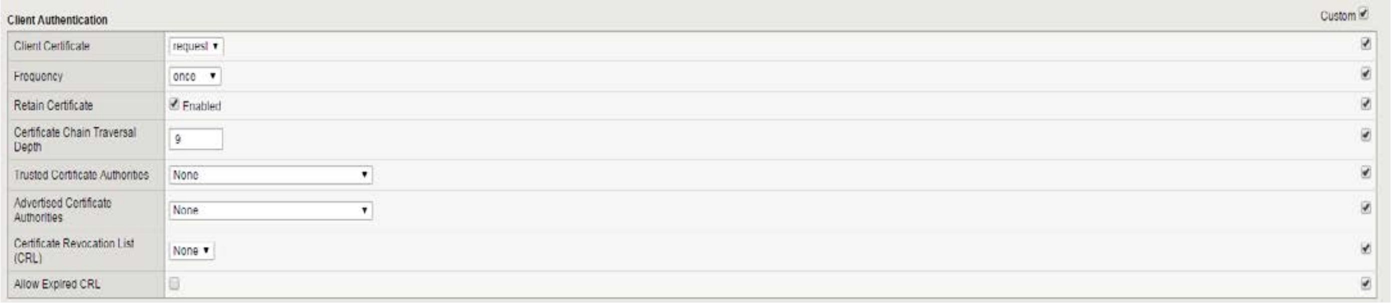

Local Traffic » Profiles : SSL : Client » New Client SSL Profile...
General Properties

Name	
Parent Profile	clientssl

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

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 — Custom ☑

Client Certificate	request ▾	☑
Frequency	once ▾	☑
Retain Certificate	☑ Enabled	☑
Certificate Chain Traversal Depth	9	☑
Trusted Certificate Authorities	None ▾	☑
Advertised Certificate Authorities	None ▾	☑
Certificate Revocation List (CRL)	None ▾	☑
Allow Expired CRL	□	☑

(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.

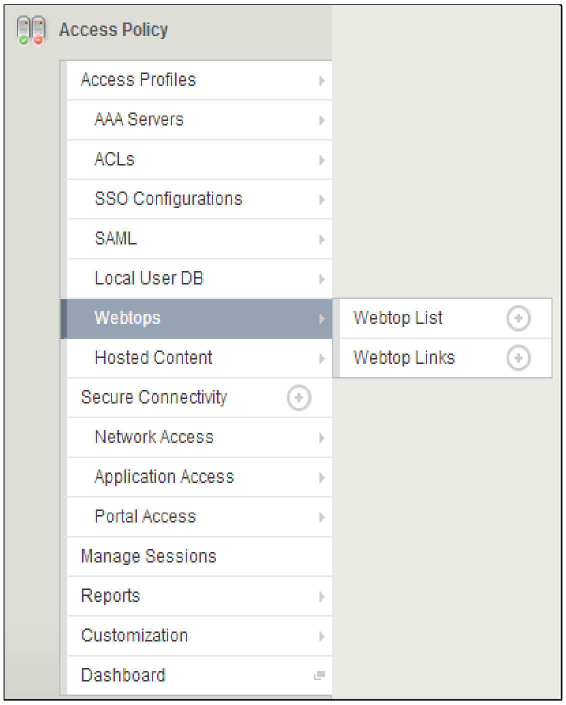
Client Certificate	Select **Request**
Trusted Certificate Authorities	Select the root CA that was defined in Adding Root CA Certificates

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.

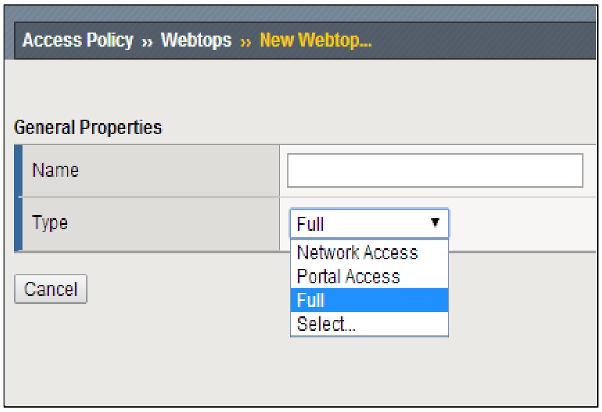
To create a Webtop:

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



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

The **New Webtop** window opens.



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

2. Complete the **General Properties** fields as follows.

Name	Enter a Webtop name
Type	Select Full from the drop-down menu

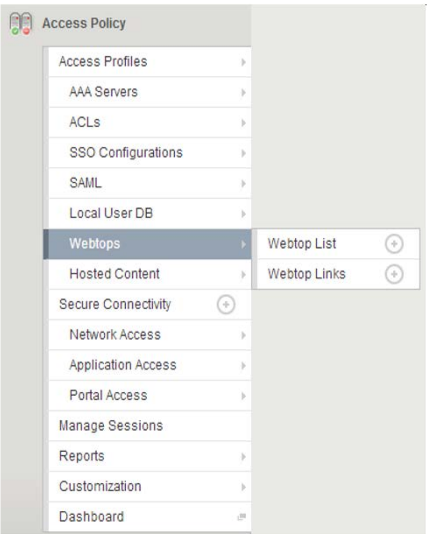
3. Click **Finished**.

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.



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

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

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

3. Click **Finished**.

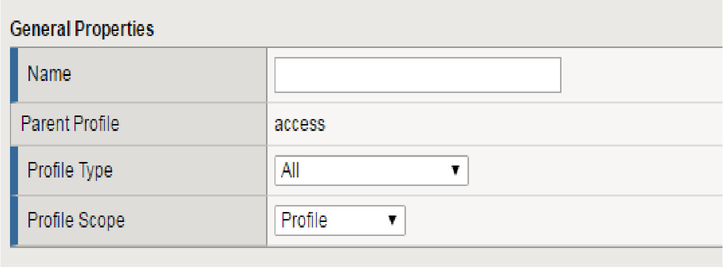
Configuring the Access Profile

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:

1. Click **Access Policy>Access Profiles**.

   The **General Properties** window opens.



General Properties

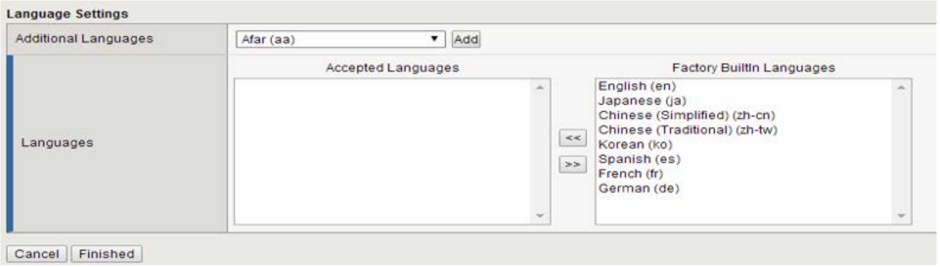
Name	
Parent Profile	access
Profile Type	All ▼
Profile Scope	Profile ▼

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

2. Complete the **General Properties** fields as follows:

Name	Enter a profile name e.g. SAS_OWA_Policy
Profile Type	Select **All** from the drop-down menu. Leave all fields with their default settings.

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.



Language Settings

Additional Languages: Afar (aa) ▼ Add

Languages

Accepted Languages

Factory Builtin Languages: English (en), Japanese (ja), Chinese (Simplified) (zh-cn), Chinese (Traditional) (zh-tw), Korean (ko), Spanish (es), French (fr), German (de)

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

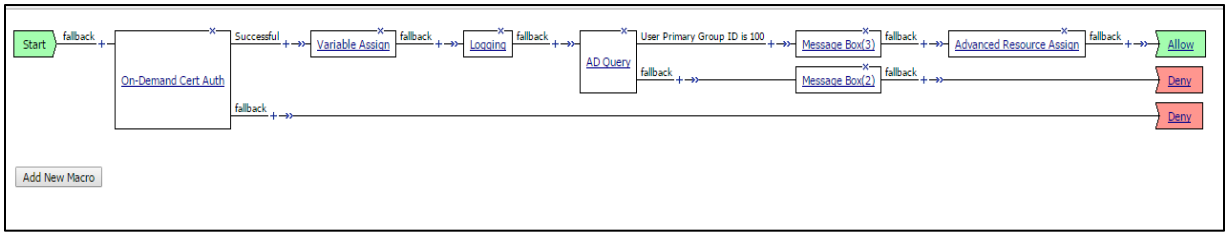
4. Click **Finished**.

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.

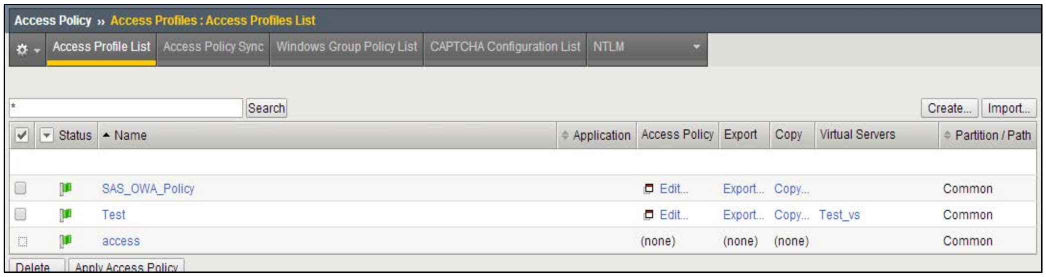
A sample Access Policy looks like this:



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

To edit the Access Profile:

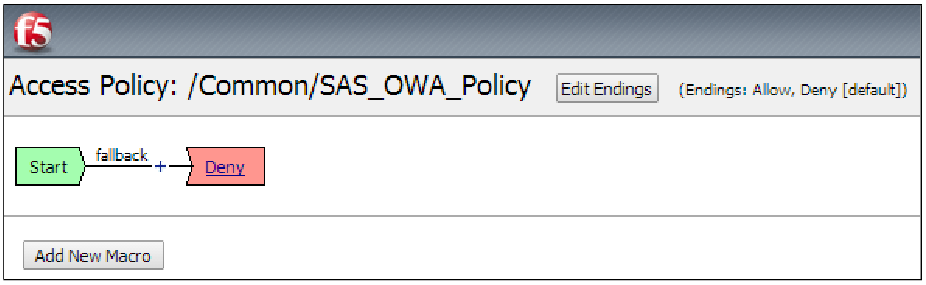
1. From the main screen, go to **Access Policy>Access Profiles List**.


Access Policy » Access Profiles : Access Profiles List
Access Profile List
Access Policy Sync
Windows Group Policy List
CAPTCHA Configuration List
NTLM
Search
Create...
Import...
Delete
Apply Access Policy

☑	Status	Name	Application	Access Policy	Export	Copy	Virtual Servers	Partition / Path
□		SAS_OWA_Policy		Edit...	Export...	Copy...		Common
□		Test		Edit...	Export...	Copy...	Test_vs	Common
□		access		(none)	(none)	(none)		Common

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

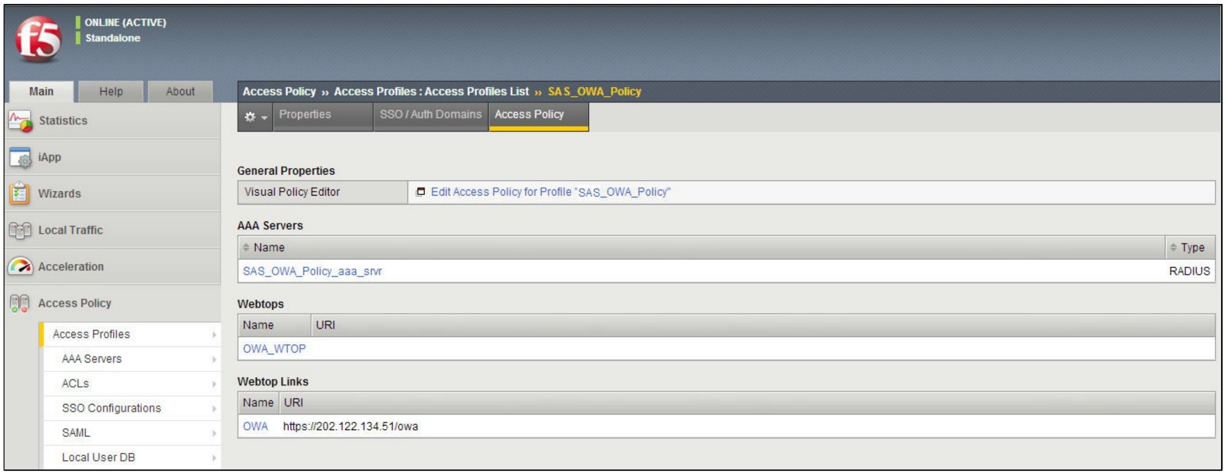
2. In the **Access Profiles List tab**, find the Access Policy you want to edit and then click **Edit** in the **Access Policy** column. The Visual Policy editor opens in a new window or a new tab, depending on your browser settings. This is the new blank policy that you have just created.


Access Policy: /Common/SAS_OWA_Policy
Edit Endings
(Endings: Allow, Deny [default])
Start
fallback
Deny
Add New Macro

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

To view the Authentication, Authorization, and Accounting servers (AAA) as well as the resources assigned to an Access Policy:

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



Access Policy » Access Profiles : Access Profiles List » SAS_OWA_Policy

General Properties

Visual Policy Editor	Edit Access Policy for Profile "SAS_OWA_Policy"

AAA Servers

Name	Type
SAS_OWA_Policy_aaa_srvr	RADIUS

Webtops

Name	URI
OWA_WTOP	

Webtop Links

Name	URI
OWA	https://202.122.134.51/owa

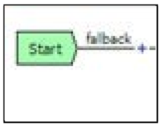
(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

Adding On-Demand Certificate Authentication

The logon page requires entering a username and password.

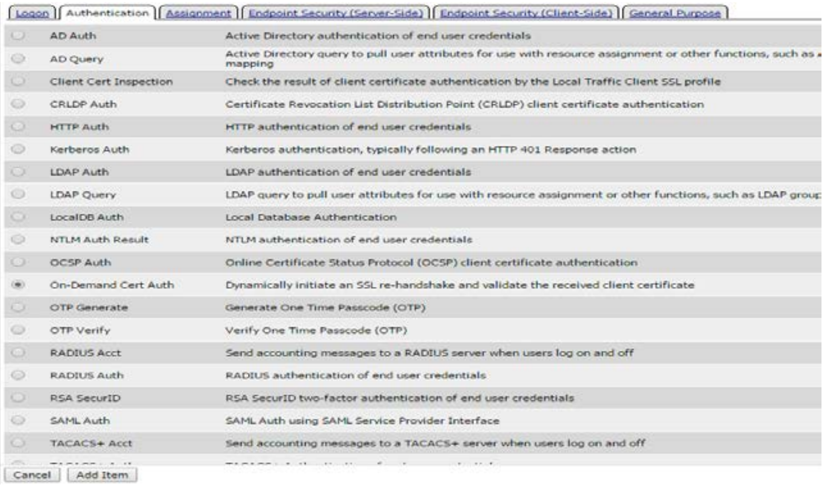
To add a logon page on the local traffic virtual server:

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



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

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


Logon
Authentication
Assignment
Endpoint Security (Server-Side)
Endpoint Security (Client-Side)
General Purpose
Cancel
Add Item

○	AD Auth	Active Directory authentication of end user credentials
○	AD Query	Active Directory query to pull user attributes for use with resource assignment or other functions, such as a mapping
○	Client Cert Inspection	Check the result of client certificate authentication by the Local Traffic Client SSL profile
○	CRLDP Auth	Certificate Revocation List Distribution Point (CRLDP) client certificate authentication
○	HTTP Auth	HTTP authentication of end user credentials
○	Kerberos Auth	Kerberos authentication, typically following an HTTP 401 Response action
○	LDAP Auth	LDAP authentication of end user credentials
○	LDAP Query	LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP grou
○	LocalDB Auth	Local Database Authentication
○	NTLM Auth Result	NTLM authentication of end user credentials
○	OCSP Auth	Online Certificate Status Protocol (OCSP) client certificate authentication
●	On-Demand Cert Auth	Dynamically initiate an SSL re-handshake and validate the received client certificate
○	OTP Generate	Generate One Time Passcode (OTP)
○	OTP Verify	Verify One Time Passcode (OTP)
○	RADIUS Acct	Send accounting messages to a RADIUS server when users log on and off
○	RADIUS Auth	RADIUS authentication of end user credentials
○	RSA SecurID	RSA SecurID two-factor authentication of end user credentials
○	SAML Auth	SAML Auth using SAML Service Provider Interface
○	TACACS+ Acct	Send accounting messages to a TACACS+ server when users log on and off

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

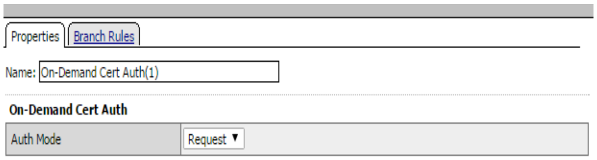
3. A properties screen opens after clicking on Add item.

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.



Name: On-Demand Cert Auth(1)

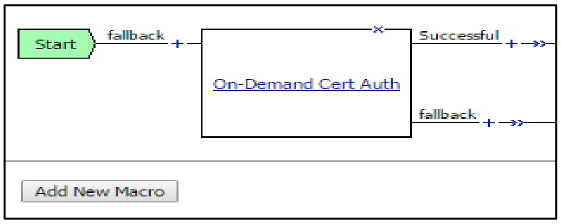
On-Demand Cert Auth

Auth Mode	Request ▼

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

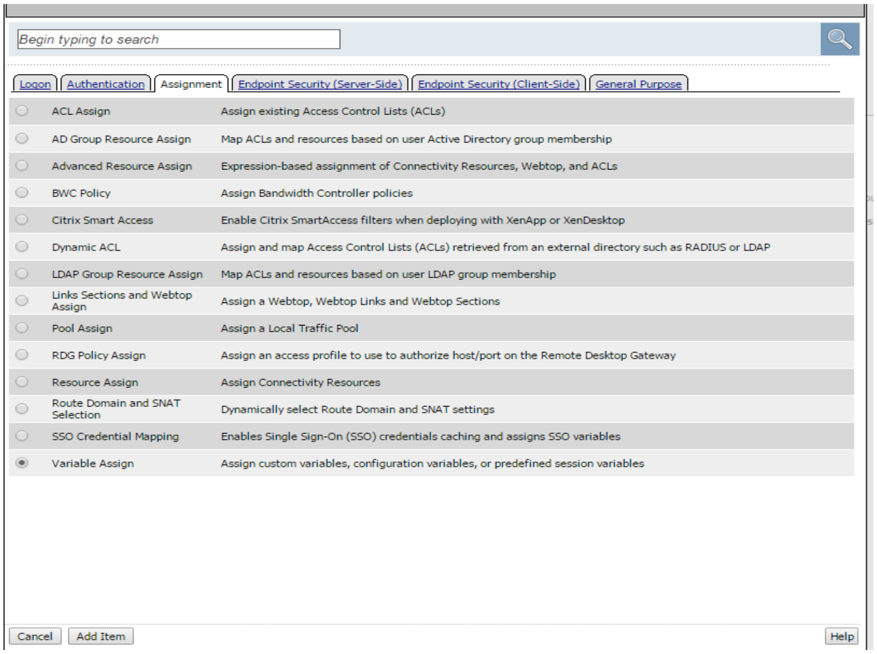
Assigning a Custom Variable

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



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

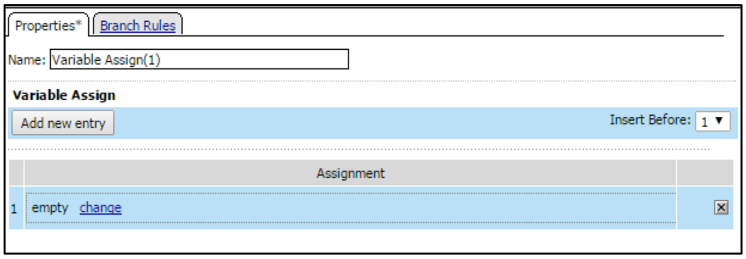
2. Click the **Assignment** tab, select **Variable Assign** and click **ADD** Item.



○	ACL Assign	Assign existing Access Control Lists (ACLs)
○	AD Group Resource Assign	Map ACLs and resources based on user Active Directory group membership
○	Advanced Resource Assign	Expression-based assignment of Connectivity Resources, Webtop, and ACLs
○	BWC Policy	Assign Bandwidth Controller policies
○	Citrix Smart Access	Enable Citrix SmartAccess filters when deploying with XenApp or XenDesktop
○	Dynamic ACL	Assign and map Access Control Lists (ACLs) retrieved from an external directory such as RADIUS or LDAP
○	LDAP Group Resource Assign	Map ACLs and resources based on user LDAP group membership
○	Links Sections and Webtop Assign	Assign a Webtop, Webtop Links and Webtop Sections
○	Pool Assign	Assign a Local Traffic Pool
○	RDG Policy Assign	Assign an access profile to use to authorize host/port on the Remote Desktop Gateway
○	Resource Assign	Assign Connectivity Resources
○	Route Domain and SNAT Selection	Dynamically select Route Domain and SNAT settings
○	SSO Credential Mapping	Enables Single Sign-On (SSO) credentials caching and assigns SSO variables
●	Variable Assign	Assign custom variables, configuration variables, or predefined session variables

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

3. Under **Variable Assign**, click **ADD new entry** and click on **change**.



Name: Variable Assign(1)

Variable Assign

Insert Before: 1

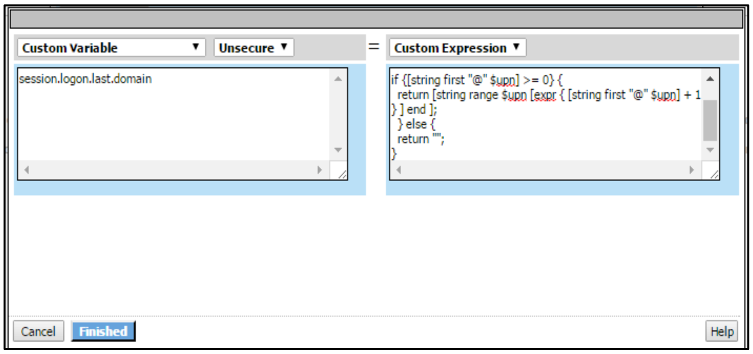
	Assignment
1	empty change

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

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 "";
}
```



```
session.logon.last.domain
```

```
if {[string first "@" $upn] >= 0} {
  return [string range $upn [expr { [string first "@" $upn] + 1
} ] end ];
  } else {
  return "";
}
```

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

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;
}
```

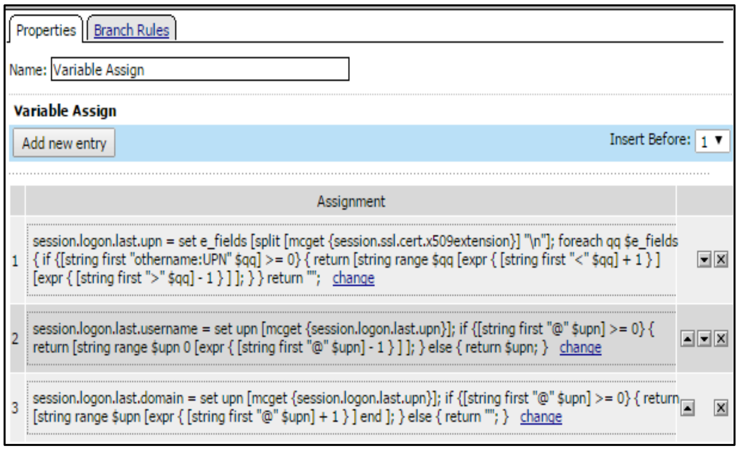
Variable Assignment 3:

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

```
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 "";
```



Name: Variable Assign

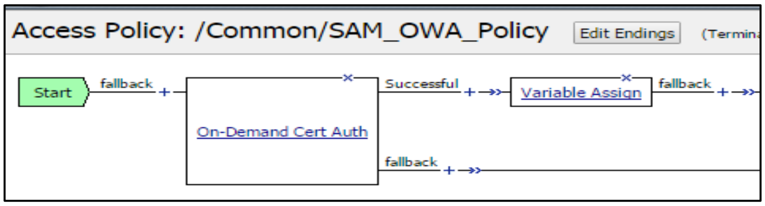
Variable Assign

	Assignment
1	session.logon.last.upn = 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 ""; change
2	session.logon.last.username = 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; } change
3	session.logon.last.domain = set upn [mcget {session.logon.last.upn}]; if {[string first "@" $upn] >= 0} { return [string range $upn [expr { [string first "@" $upn] + 1 }] end]; } else { return ""; } change

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

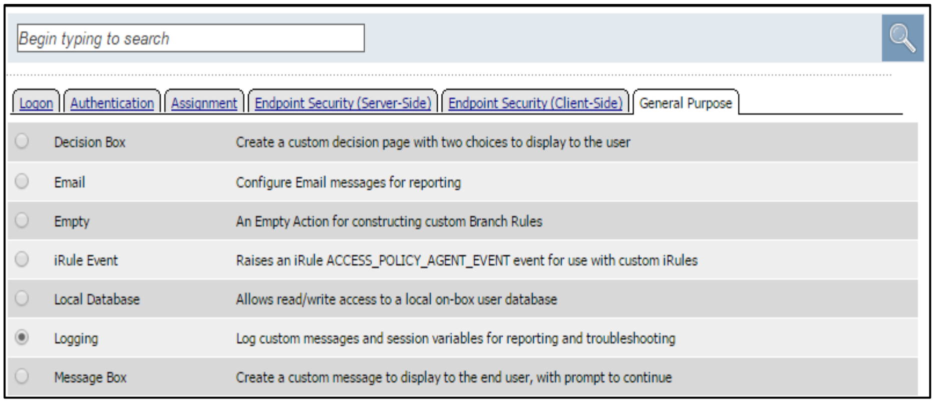
Adding the Log Custom Message Variable

1. Click the **+** icon after Variable Assign.



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

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

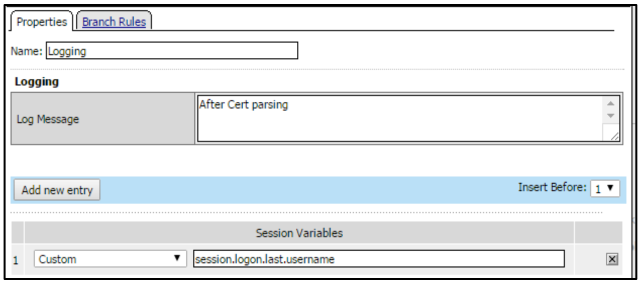


○	Decision Box	Create a custom decision page with two choices to display to the user
○	Email	Configure Email messages for reporting
○	Empty	An Empty Action for constructing custom Branch Rules
○	iRule Event	Raises an iRule ACCESS_POLICY_AGENT_EVENT event for use with custom iRules
○	Local Database	Allows read/write access to a local on-box user database
●	Logging	Log custom messages and session variables for reporting and troubleshooting
○	Message Box	Create a custom message to display to the end user, with prompt to continue

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

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.**



Name: Logging

Logging

Log Message: After Cert parsing

Insert Before: 1

	Session Variables		
1	Custom	session.logon.last.username	☒

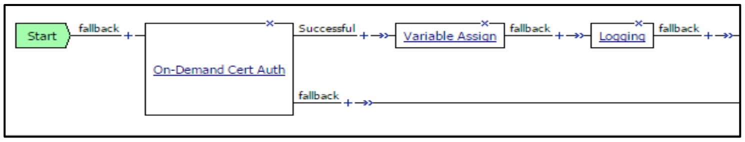
(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

5. Click **Save**.

Adding AD Query

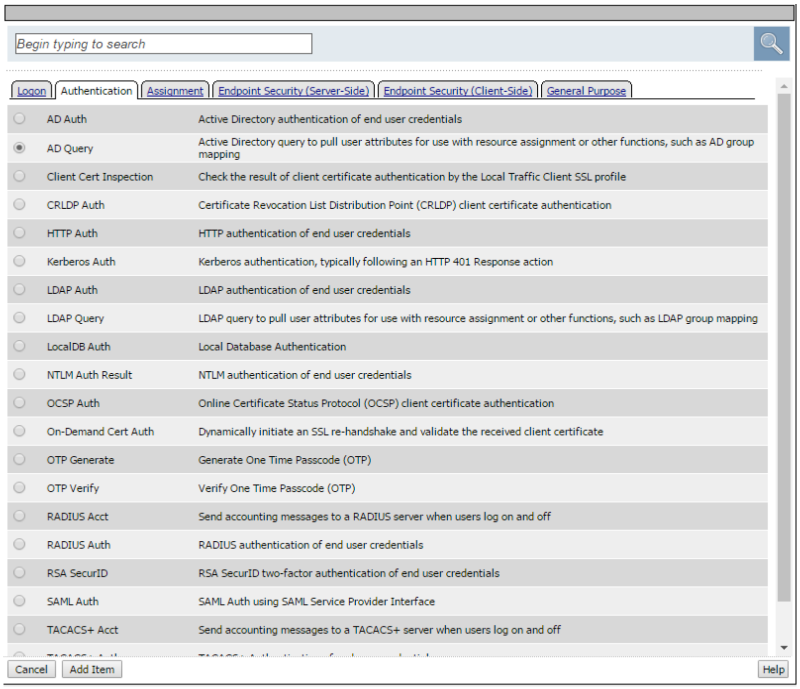
See the Appendix on page **Error! Bookmark not defined.** for details on how to configure the AD Server.

1. Click the **+** icon after Logging.



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

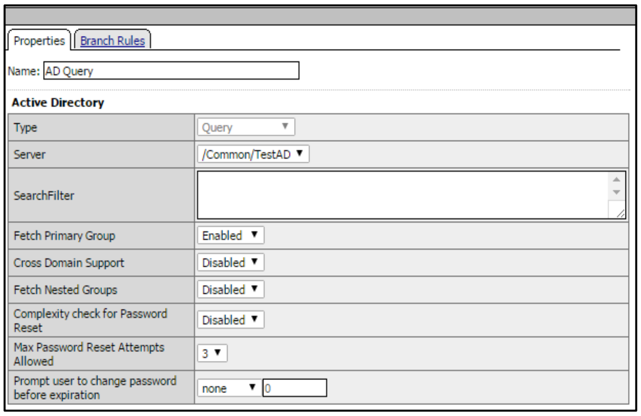
2. Click the **Authentication** tab and select **AD Query** from the list then click Add Item.



○	AD Auth	Active Directory authentication of end user credentials
●	AD Query	Active Directory query to pull user attributes for use with resource assignment or other functions, such as AD group mapping
○	Client Cert Inspection	Check the result of client certificate authentication by the Local Traffic Client SSL profile
○	CRLDP Auth	Certificate Revocation List Distribution Point (CRLDP) client certificate authentication
○	HTTP Auth	HTTP authentication of end user credentials
○	Kerberos Auth	Kerberos authentication, typically following an HTTP 401 Response action
○	LDAP Auth	LDAP authentication of end user credentials
○	LDAP Query	LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mapping
○	LocalDB Auth	Local Database Authentication
○	NTLM Auth Result	NTLM authentication of end user credentials
○	OCSP Auth	Online Certificate Status Protocol (OCSP) client certificate authentication
○	On-Demand Cert Auth	Dynamically initiate an SSL re-handshake and validate the received client certificate
○	OTP Generate	Generate One Time Passcode (OTP)
○	OTP Verify	Verify One Time Passcode (OTP)
○	RADIUS Acct	Send accounting messages to a RADIUS server when users log on and off
○	RADIUS Auth	RADIUS authentication of end user credentials
○	RSA SecurID	RSA SecurID two-factor authentication of end user credentials
○	SAML Auth	SAML Auth using SAML Service Provider Interface
○	TACACS+ Acct	Send accounting messages to a TACACS+ server when users log on and off

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

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



Name: AD Query

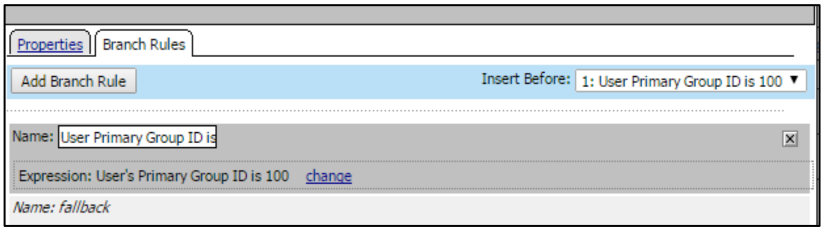
Active Directory

Type	Query ▼
Server	/Common/TestAD ▼
SearchFilter	
Fetch Primary Group	Enabled ▼
Cross Domain Support	Disabled ▼
Fetch Nested Groups	Disabled ▼
Complexity check for Password Reset	Disabled ▼
Max Password Reset Attempts Allowed	3 ▼
Prompt user to change password before expiration	none ▼ 0

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

4. From the Fetch Primary Group drop-down menu, select **Enabled**.

5. Click the Branch Rules tab and then click **change**.



Insert Before: 1: User Primary Group ID is 100

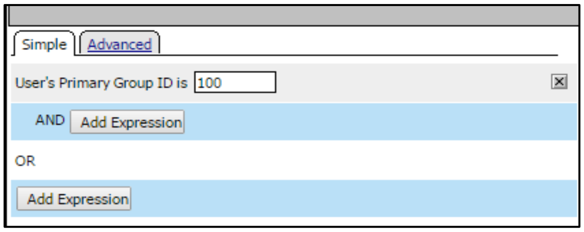
Name: User Primary Group ID is

Expression: User's Primary Group ID is 100 change

Name: fallback

(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.



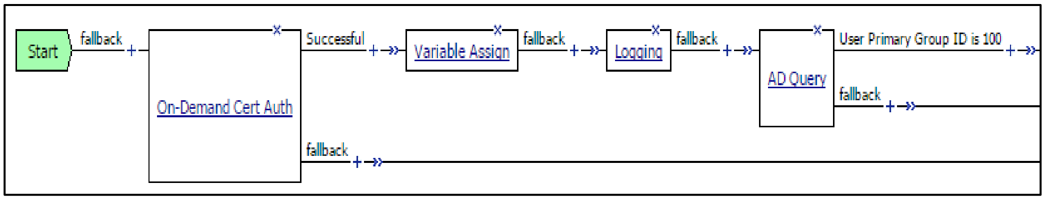
User's Primary Group ID is 100

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

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

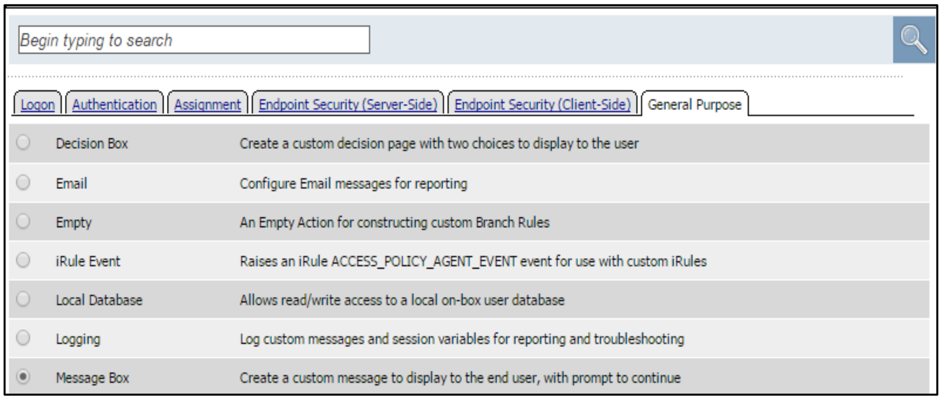
Adding Message box

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



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

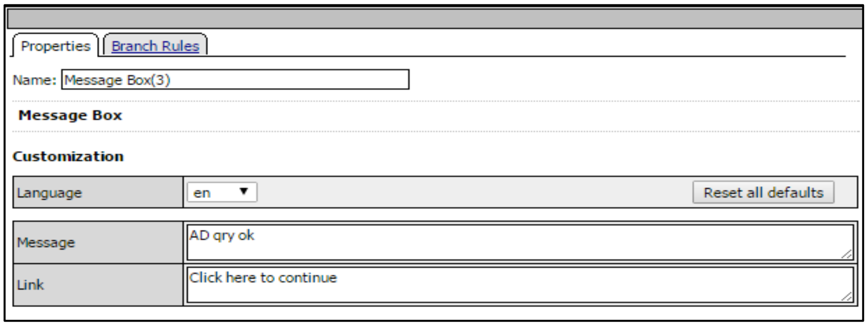
2. Click the **General Purpose** tab, select **Message Box** and then click **Add Item**.



○	Decision Box	Create a custom decision page with two choices to display to the user
○	Email	Configure Email messages for reporting
○	Empty	An Empty Action for constructing custom Branch Rules
○	iRule Event	Raises an iRule ACCESS_POLICY_AGENT_EVENT event for use with custom iRules
○	Local Database	Allows read/write access to a local on-box user database
○	Logging	Log custom messages and session variables for reporting and troubleshooting
●	Message Box	Create a custom message to display to the end user, with prompt to continue

(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**.



Name: Message Box(3)

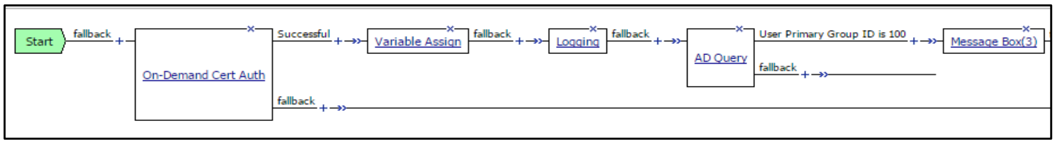
Message Box

Customization

Language	en
Message	AD qry ok
Link	Click here to continue

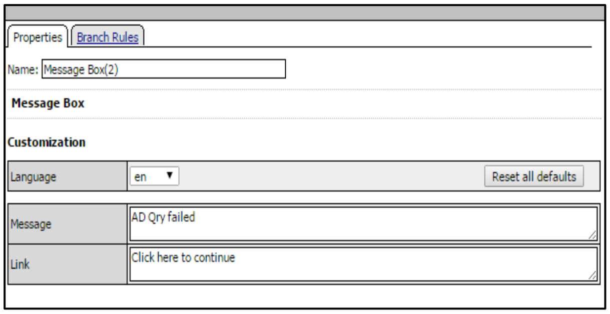
(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

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



(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.**



Name: Message Box(2)

Message Box

Customization

Language	en
Message	AD Qry failed
Link	Click here to continue

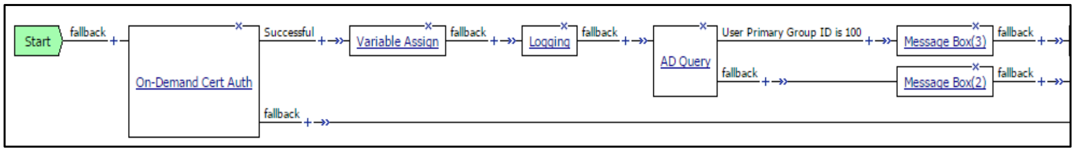
(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

Adding a Webtop

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

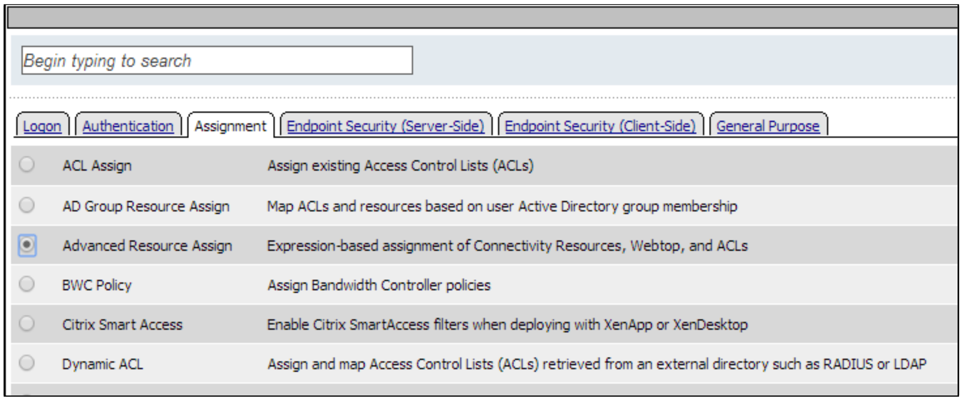
To add a Webtop:

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



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

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



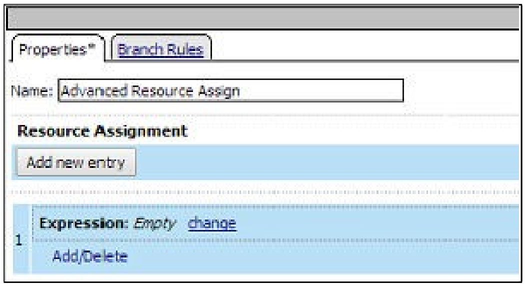
Begin typing to search

Logon | Authentication | Assignment | Endpoint Security (Server-Side) | Endpoint Security (Client-Side) | General Purpose

○	ACL Assign	Assign existing Access Control Lists (ACLs)
○	AD Group Resource Assign	Map ACLs and resources based on user Active Directory group membership
●	Advanced Resource Assign	Expression-based assignment of Connectivity Resources, Webtop, and ACLs
○	BWC Policy	Assign Bandwidth Controller policies
○	Citrix Smart Access	Enable Citrix SmartAccess filters when deploying with XenApp or XenDesktop
○	Dynamic ACL	Assign and map Access Control Lists (ACLs) retrieved from an external directory such as RADIUS or LDAP

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

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



Properties* | Branch Rules

Name: Advanced Resource Assign

Resource Assignment

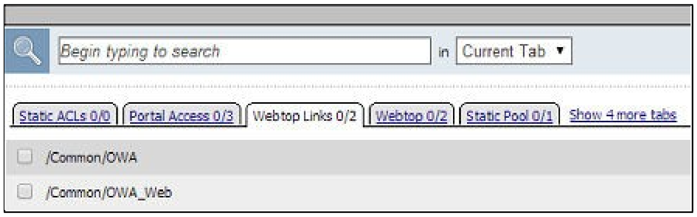
Add new entry

1 **Expression:** *Empty* change

Add/Delete

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

4. Under Expression, click **Add/Delete**.
5. Select the Webtop Links and Webtop tabs to define each item.



Begin typing to search in Current Tab ▼

Static ACLs 0/0 | Portal Access 0/3 | Webtop Links 0/2 | Webtop 0/2 | Static Pool 0/1 | Show 4 more tabs

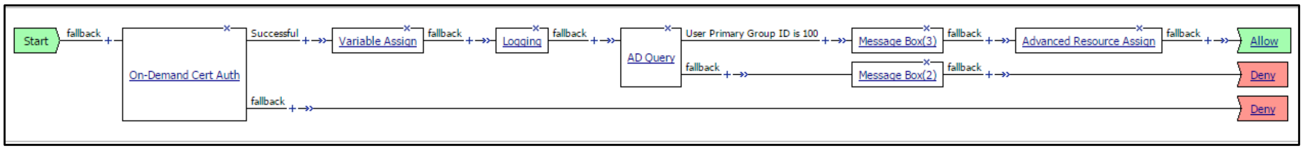
□ /Common/OWA

□ /Common/OWA_Web

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

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

7. Click **Save**.
8. The final visual policy editor looks as follows:



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

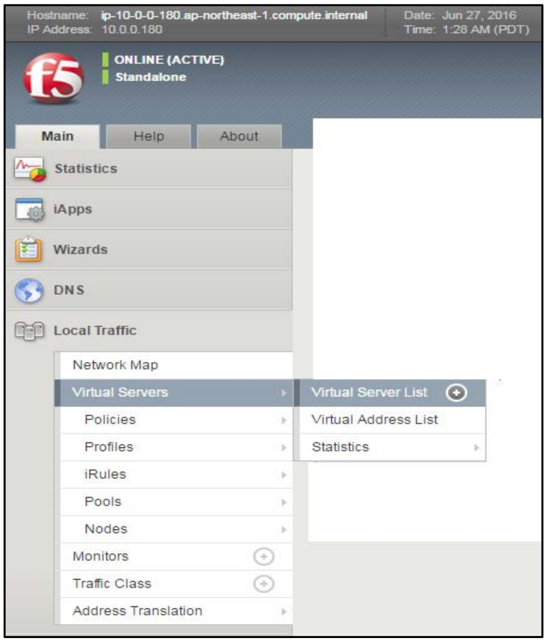
Configuring the Virtual Server

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 **+.**

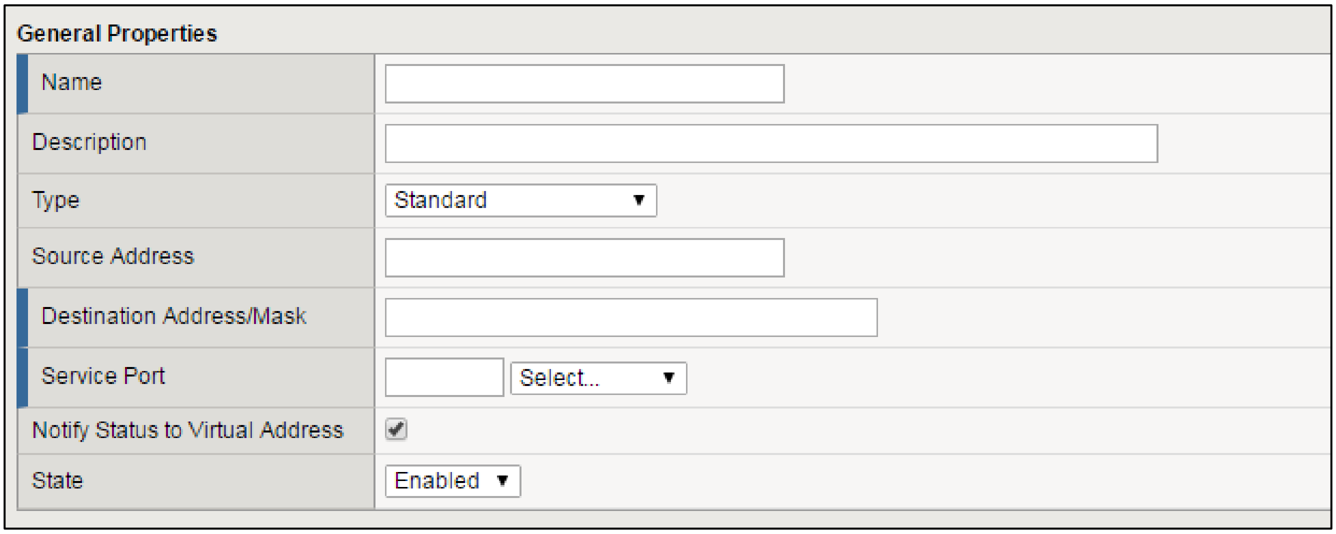

Hostname: ip-10-0-0-180.ap-northeast-1.compute.internal
IP Address: 10.0.0.180
Date: Jun 27, 2016
Time: 1:28 AM (PDT)
ONLINE (ACTIVE)
Standalone

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

2. Complete the **New Virtual Server** fields as follows:

Name	Enter a name for the virtual server.
Destination	Enter the virtual server host IP address.
Service Port	Select **HTTPS**.

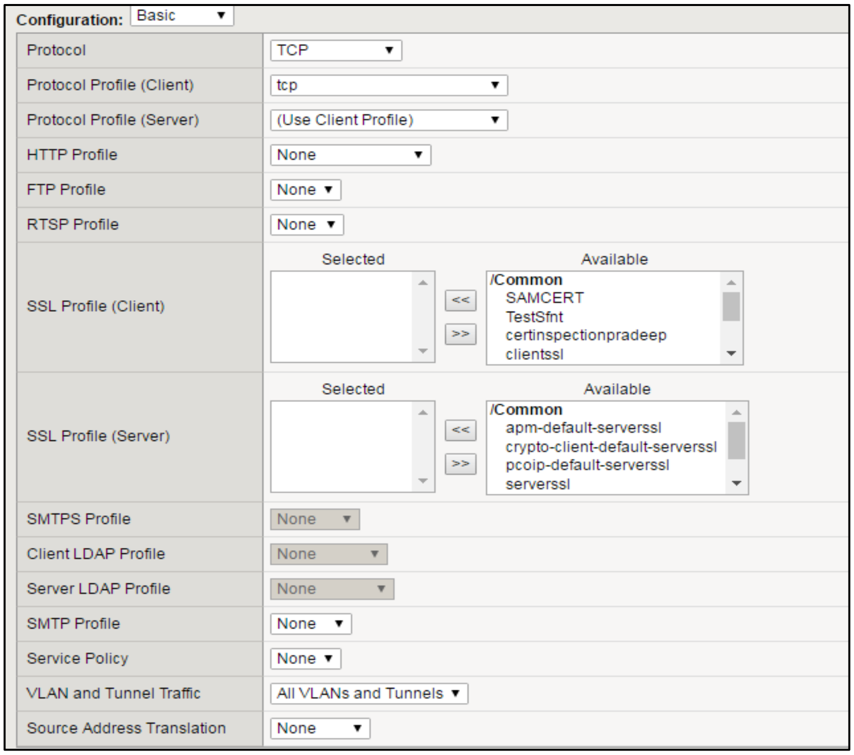
HTTP Profile	Select HTTP.
SSL Profile (Client)	From the **Available** list, select the name of the Client SSL profile you previously created, and using the Move button, move the name to the **Selected** list.
SSL Profile (Server)	If your web application server is using HTTPS services, select the server SSL profile to use with this virtual server.
Access Profile	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.
Rewrite Profile	If you are creating a virtual server to use with web applications, select the rewrite profile.



General Properties

Name	
Description	
Type	Standard ▼
Source Address	
Destination Address/Mask	
Service Port	Select... ▼
Notify Status to Virtual Address	☑
State	Enabled ▼

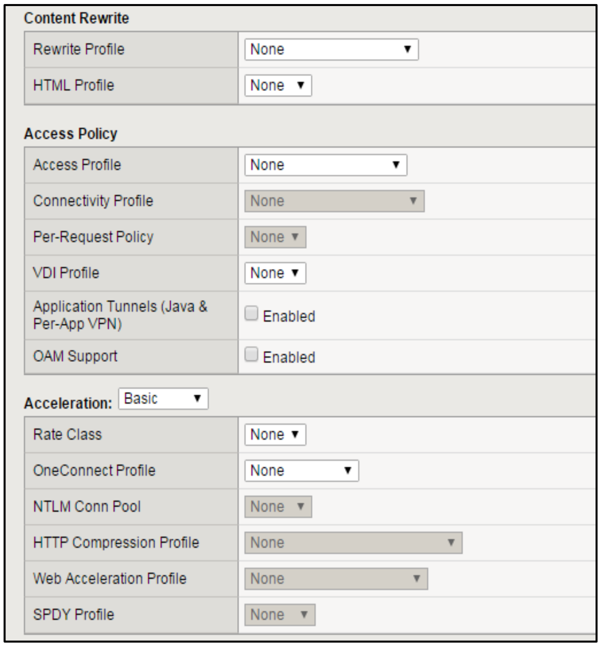
(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)



Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	None
FTP Profile	None
RTSP Profile	None
SSL Profile (Client)	Selected: Available: /Common SAMCERT TestSfnt certinspectionpradeep clientssl
SSL Profile (Server)	Selected: Available: /Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl
SMTPS Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
SMTP Profile	None
Service Policy	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	None

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



Content Rewrite

Rewrite Profile	None
HTML Profile	None

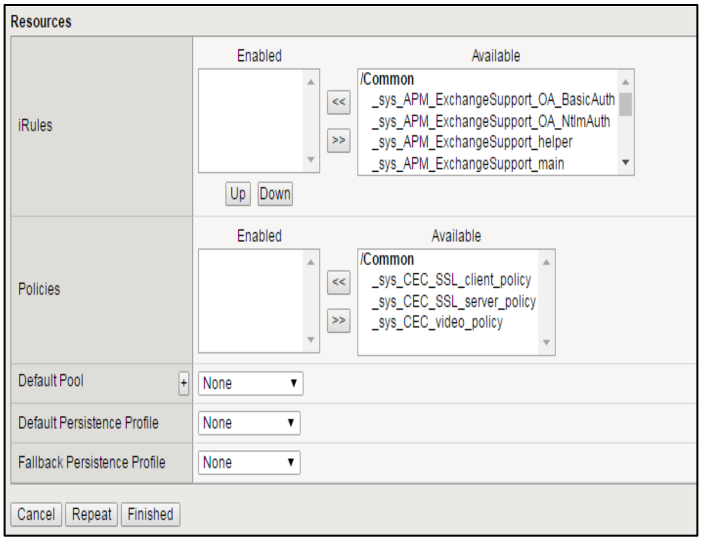
Access Policy

Access Profile	None
Connectivity Profile	None
Per-Request Policy	None
VDI Profile	None
Application Tunnels (Java & Per-App VPN)	□ Enabled
OAM Support	□ Enabled

Acceleration: Basic

Rate Class	None
OneConnect Profile	None
NTLM Conn Pool	None
HTTP Compression Profile	None
Web Acceleration Profile	None
SPDY Profile	None

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



Resources

iRules

Enabled

Available

/Common
_sys_APM_ExchangeSupport_OA_BasicAuth
_sys_APM_ExchangeSupport_OA_NtlmAuth
_sys_APM_ExchangeSupport_helper
_sys_APM_ExchangeSupport_main

Policies

Enabled

Available

/Common
_sys_CEC_SSL_client_policy
_sys_CEC_SSL_server_policy
_sys_CEC_video_policy

Default Pool	None
Default Persistence Profile	None
Fallback Persistence Profile	None

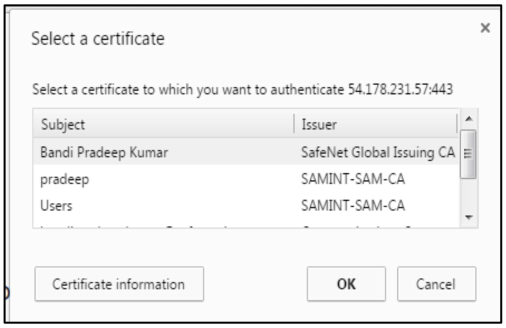
(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

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**.



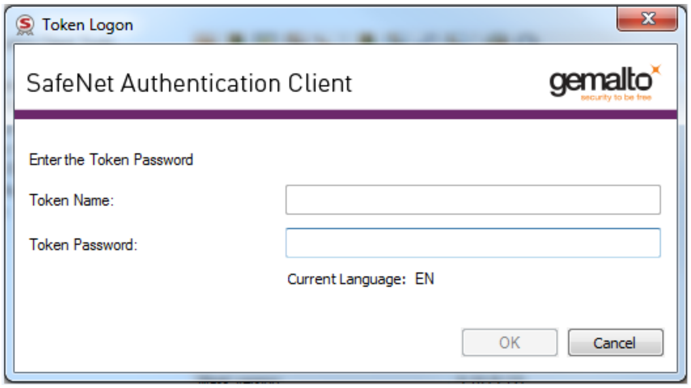
Select a certificate

Select a certificate to which you want to authenticate 54.178.231.57:443

Subject	Issuer
Bandi Pradeep Kumar	SafeNet Global Issuing CA
pradeep	SAMINT-SAM-CA
Users	SAMINT-SAM-CA

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

The SafeNet Authentication Client Logon window opens.



Token Logon

SafeNet Authentication Client

Enter the Token Password

Token Name:

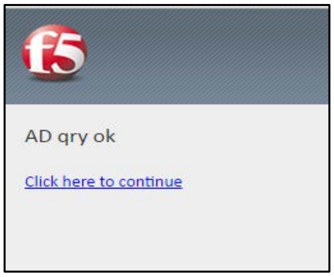
Token Password:

Current Language: EN

2. Enter the Token/smart card Name and Password and click **OK**.

   The **AD qry ok** window opens.

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



AD qry ok

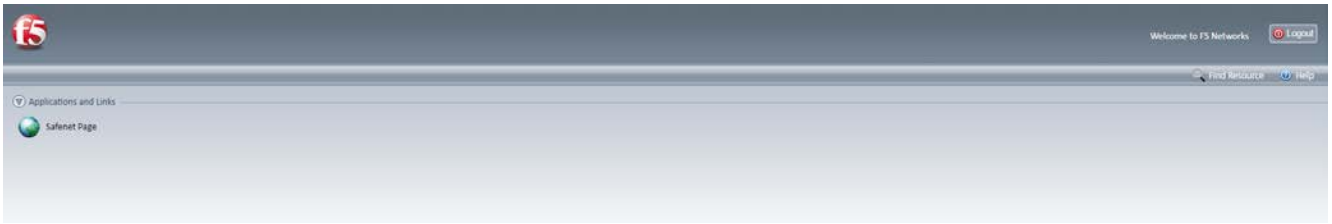
Click here to continue

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

After Successful Authentication

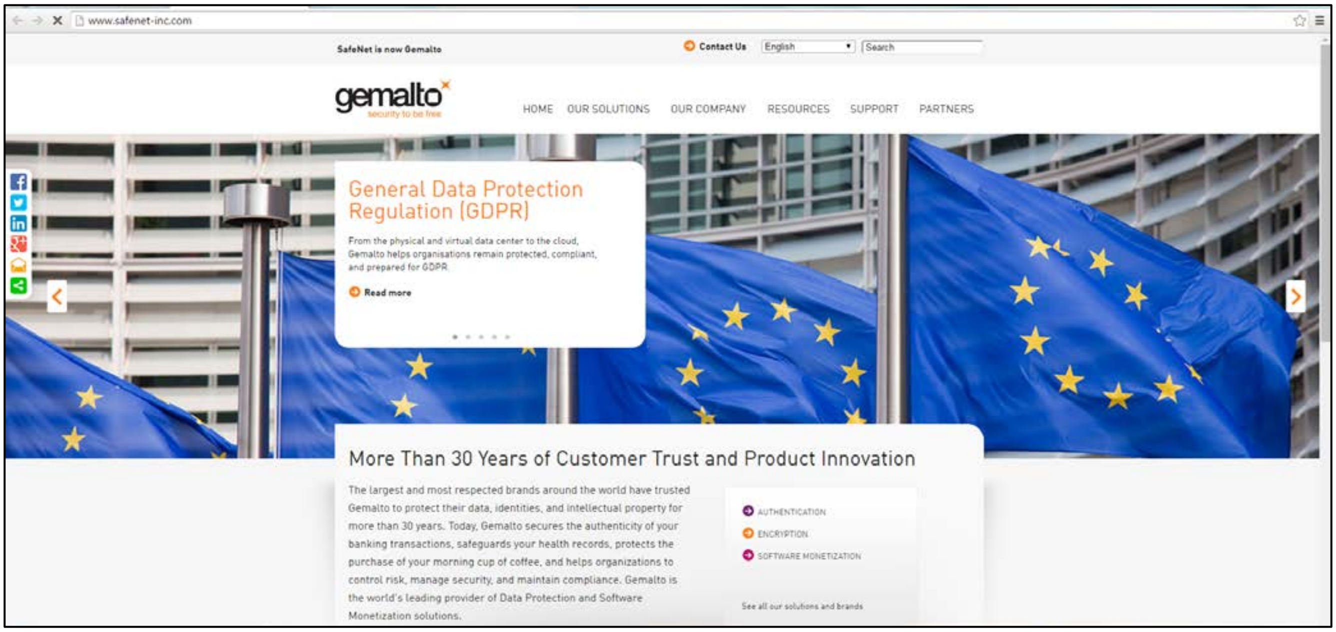
On successful authentication:

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.



General Data Protection Regulation (GDPR)

From the physical and virtual data center to the cloud, Gemalto helps organisations remain protected, compliant, and prepared for GDPR.

More Than 30 Years of Customer Trust and Product Innovation

The largest and most respected brands around the world have trusted Gemalto to protect their data, identities, and intellectual property for more than 30 years. Today, Gemalto secures the authenticity of your banking transactions, safeguards your health records, protects the purchase of your morning cup of coffee, and helps organizations to control risk, manage security, and maintain compliance. Gemalto is the world's leading provider of Data Protection and Software Monetization solutions.

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

APPENDIX

DNS and NTP Settings on the BIG-IP System

For BIG-IP APM, you must have DNS and NTP settings configured. To configure these setting, 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**.

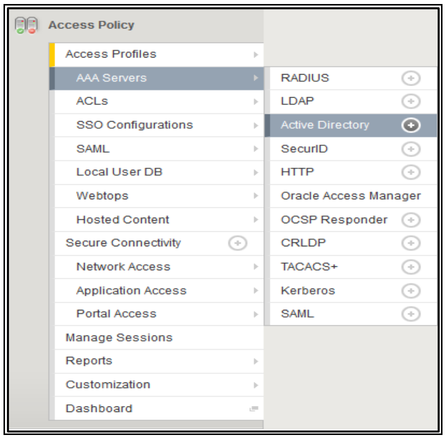
Configuring NTP

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

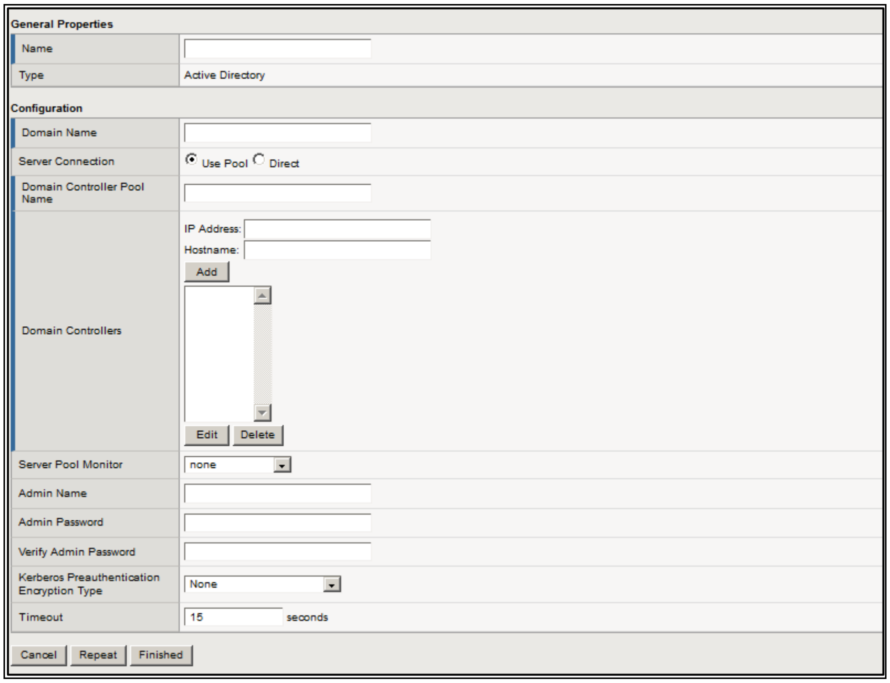
1. Go to **Main>Access Policy>AAA Server>Active Directory** and then click the **+** icon in the right corner of the window.



(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**.

Name	Enter a name for the authentication server you are creating.
Domain Name	Enter the Windows Domain name. You must enter the FQDN.
Domain Controller Pool Name	Enter the Active Directory server configured with this role.
Admin Name	Enter an administrator name that has Active Directory administrative permissions.
Admin Password	Enter the administrative password for the server.
Verify Admin Password	Enter the administrative password for the server again.



General Properties

Name	
Type	Active Directory

Configuration

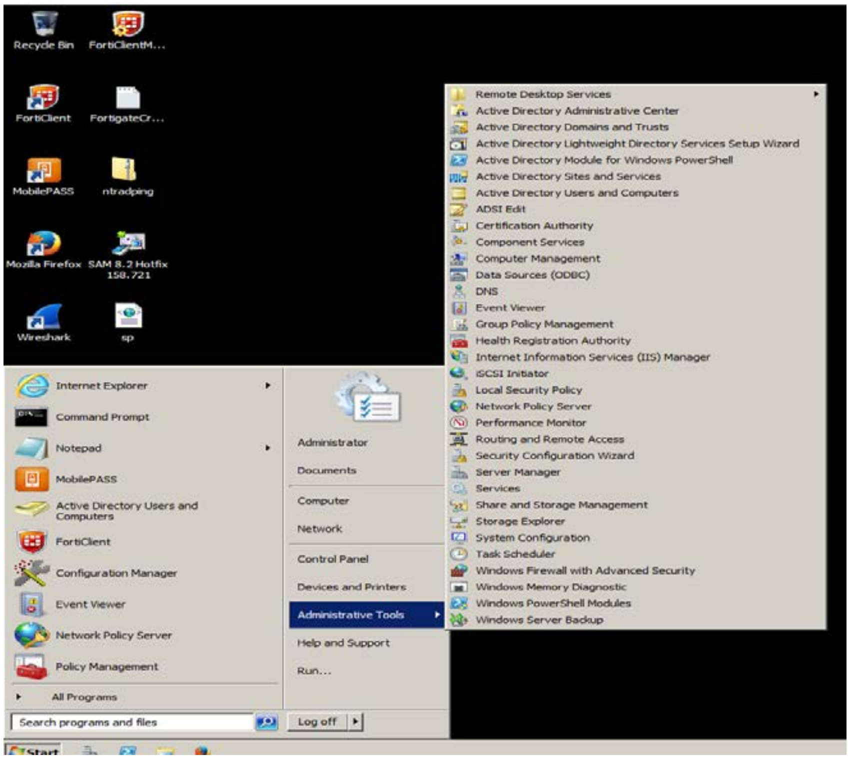
Domain Name	
Server Connection	● Use Pool ○ Direct
Domain Controller Pool Name	
Domain Controllers	IP Address: Hostname: Add Edit Delete
Server Pool Monitor	none
Admin Name	
Admin Password	
Verify Admin Password	
Kerberos Preauthentication Encryption Type	None
Timeout	15 seconds

Cancel Repeat Finished

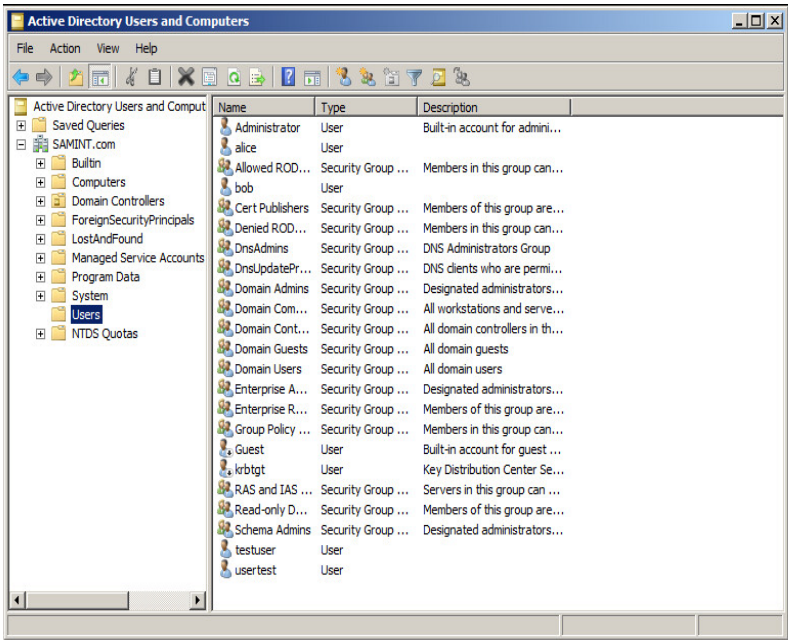
(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

How to find the primary group ID

1. Go to the CA server and click **Start>Administrative tools>Active directory users and computers.**

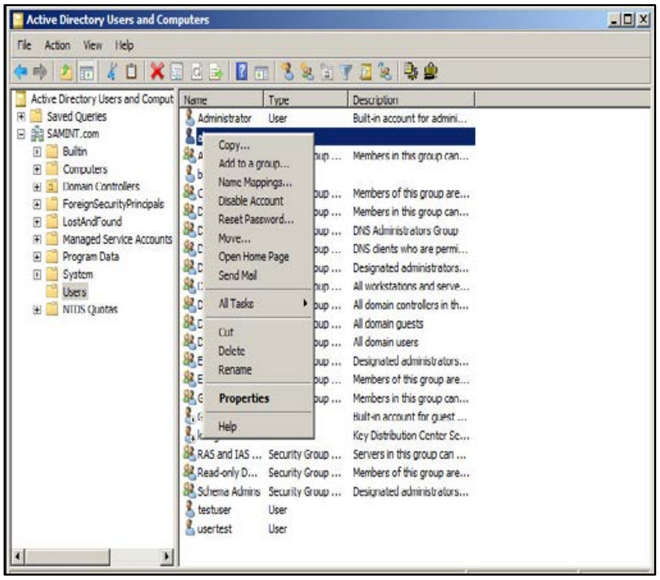


2. Expand the domain name and click **Users**.

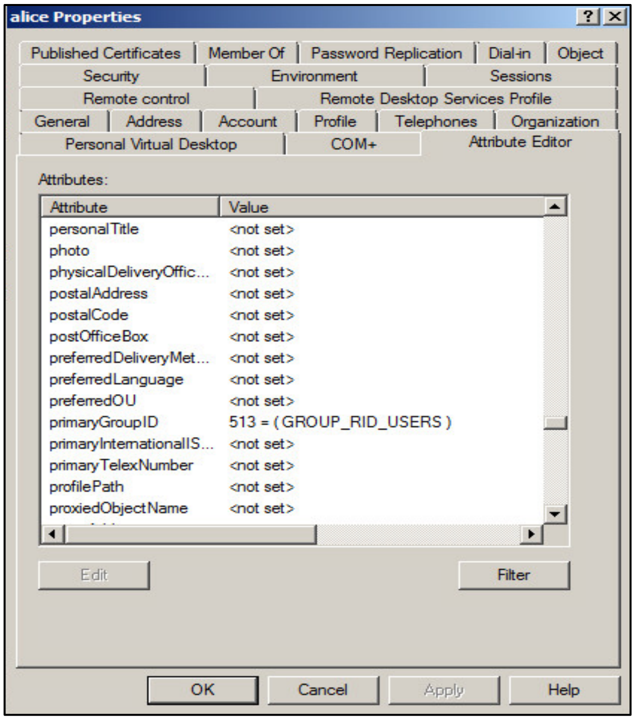


Name	Type	Description
Administrator	User	Built-in account for admini...
alice	User	
Allowed ROD...	Security Group ...	Members in this group can...
bob	User	
Cert Publishers	Security Group ...	Members of this group are...
Denied ROD...	Security Group ...	Members in this group can...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdatePr...	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Com...	Security Group ...	All workstations and serve...
Domain Cont...	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise A...	Security Group ...	Designated administrators...
Enterprise R...	Security Group ...	Members of this group are...
Group Policy ...	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
krbtgt	User	Key Distribution Center Se...
RAS and IAS ...	Security Group ...	Servers in this group can ...
Read-only D...	Security Group ...	Members of this group are...
Schema Admins	Security Group ...	Designated administrators...
testuser	User	
usertest	User	

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.



Attribute	Value
personalTitle	<not set>
photo	<not set>
physicalDeliveryOffic...	<not set>
postalAddress	<not set>
postalCode	<not set>
postOfficeBox	<not set>
preferredDeliveryMet...	<not set>
preferredLanguage	<not set>
preferredOU	<not set>
primaryGroupID	513 = (GROUP_RID_USERS)
primaryInternationalIS...	<not set>
primaryTelexNumber	<not set>
profilePath	<not set>
proxiedObjectName	<not set>

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.

Contact Method	Contact Information	
Address	Gemalto, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com 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.	