BIG-IP® Access Policy Manager®: Third-Party Integration Implementations

Version 11.5

Table of Contents

Legal Notices

Publication Date

This document was published on January 27, 2014.

Publication Number

MAN-0505-00

Copyright

Copyright © 2013-2014, F5 Networks, Inc. All rights reserved.

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, APM, Application Acceleration Manager, Application Security Manager, ARX, AskF5, ASM, BIG-IP, BIG-IQ, Cloud Extender, CloudFucious, Cloud Manager, Clustered Multiprocessing, CMP, COHESION, Data Manager, DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Portal, ELEVATE, EM, Enterprise Manager, ENGAGE, F5, F5 [DESIGN], F5 Certified [DESIGN], F5 Networks, F5 SalesXchange [DESIGN], F5 Synthesis, f5 Synthesis, F5 Synthesis [DESIGN], F5 TechXchange [DESIGN], Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, iApps, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, LineRate, LineRate Systems [DESIGN], LROS, LTM, Message Security Manager, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Real Traffic Policy Builder, SalesXchange, ScaleN, Signalling Delivery Controller, SDC, SSL Acceleration, software designed applications services, SDAC (except in Japan), StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TechXchange, TMOS, TotALL, Traffic Management Operating System, Traffix Systems, Traffix Systems (DESIGN), Transparent Data Reduction, UNITY, VAULT, vCMP, VE F5 [DESIGN], Versafe, Versafe [DESIGN], VIPRION, Virtual Clustered Multiprocessing, WebSafe, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents indicated at:
http://www.f5.com/about/guidelines-policies/patents

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the Swedish Institute of Computer Science and its contributors.

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at the Lawrence Berkeley Laboratory.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

This product includes software developed by Jochen Pohl for the NetBSD Project.

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

This product includes software developed by SigmaSoft, Th. Lockert.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed by Jason R. Thorpe for And Communications, http://www.and.com.

This product includes software developed for the NetBSD Project by Frank Van der Linden.

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed by Christos Zoulas.

This product includes software developed by the University of Vermont and State Agricultural College and Garrett A. Wollman.

This product includes software developed by Balazs Scheidler (bazsi@balabit.hu), which is protected under the GNU Public License.

This product includes software developed by Niels Mueller (nisse@lysator.liu.se), which is protected under the GNU Public License.

In the following statement, *This software* refers to the Mitsumi CD-ROM driver: This software was developed by Holger Veit and Brian Moore for use with 386BSD and similar operating systems. *Similar operating systems* includes mainly non-profit oriented systems for research and education, including but not restricted to NetBSD, FreeBSD, Mach (by CMU).

This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).

This product includes software licensed from Richard H. Porter under the GNU Library General Public License (© 1998, Red Hat Software), www.gnu.org/copyleft/lgpl.html.

This product includes the standard version of Perl software licensed under the Perl Artistic License (© 1997, 1998 Tom Christiansen and Nathan Torkington). All rights reserved. You may find the most current standard version of Perl at http://www.perl.com.

This product includes software developed by Jared Minch.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product contains software based on oprofile, which is protected under the GNU Public License.

This product includes RRDtool software developed by Tobi Oetiker (http://www.rrdtool.com/index.html) and licensed under the GNU General Public License.

This product contains software licensed from Dr. Brian Gladman under the GNU General Public License (GPL).

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes Hypersonic SQL.

This product contains software developed by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and others.

This product includes software developed by the Internet Software Consortium.

This product includes software developed by Nominum, Inc. (http://www.nominum.com).

This product contains software developed by Broadcom Corporation, which is protected under the GNU Public License.

This product contains software developed by MaxMind LLC, and is protected under the GNU Lesser General Public License, as published by the Free Software Foundation.

This product includes Intel QuickAssist kernel module, library, and headers software licensed under the GNU General Public License (GPL).

This product includes software licensed from Gerald Combs (gerald@wireshark.org) under the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or any later version. Copyright ©1998 Gerald Combs.

This product includes software developed by Daniel Stenberg. Copyright ©1996 - 2012, Daniel Stenberg, (daniel@haxx.se). All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

This product includes software developed by Thomas Williams and Colin Kelley. Copyright ©1986 - 1993, 1998, 2004, 2007

Permission to use, copy, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Permission to modify the software is granted, but not the right to distribute the complete modified source code. Modifications are to be distributed as patches to the released version. Permission to distribute binaries produced by compiling modified sources is granted, provided you

1. distribute the corresponding source modifications from the released version in the form of a patch file along with the binaries,
2. add special version identification to distinguish your version in addition to the base release version number,
3. provide your name and address as the primary contact for the support of your modified version, and
4. retain our contact information in regard to use of the base software.

Permission to distribute the released version of the source code along with corresponding source modifications in the form of a patch file is granted with same provisions 2 through 4 for binary distributions. This software is provided "as is" without express or implied warranty to the extent permitted by applicable law.

This product contains software developed by Google, Inc. Copyright ©2011 Google, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This product includes software developed by Jeremy Ashkenas and DocumentCloud, and distributed under the MIT license. Copyright © 2010-2013 Jeremy Ashkenas, DocumentCloud.

This product includes gson software, distributed under the Apache License version 2.0. Copyright © 2008-2011 Google Inc.

This product includes Boost libraries, which are distributed under the Boost license (http://www.boost.org/LICENSE_1_0.txt).

Chapter 1

Citrix Requirements for Integration with APM

About Access Policy Manager and Citrix integration types

When integrated with Citrix, Access Policy Manager® (APM™) performs authentication (and, optionally uses SmartAccess filters) to control access to Citrix published applications. APM supports these types of integration with Citrix:

Integration with Web Interface sites

In this deployment, APM load-balances and authenticates access to Web Interface sites, providing SmartAccess conditions based on endpoint inspection of clients. Web Interface sites communicate with XML Brokers, render the user interface, and display the applications to the client.

Integration with XML Brokers

In this deployment, APM does not need a Web Interface site. APM load-balances and authenticates access to XML Brokers, providing SmartAccess conditions based on endpoint inspection of clients. APM communicates with XML Brokers, renders the user interface, and displays the applications to the client.

About Citrix required settings

To integrate Access Policy Manager® with Citrix, you must meet specific configuration requirements for Citrix as described here.

Trust XML Requests

To support communication with APM®, make sure that the Trust XML requests option is enabled in the XenApp AppCenter management console.

Web Interface site authentication settings

If you want to integrate APM with a Citrix Web Interface site, make sure that the Web Interface site is configured with these settings:

- Authentication point set to **At Access Gateway**.
- Authentication method set to **Explicit**.
- Authentication service URL points to a virtual server on the BIG-IP® system; the URL must be one of these:
  - `http://address of the virtual server/CitrixAuth`
  - `https://address of the virtual server/CitrixAuth` (if traffic is encrypted between APM and the Citrix Web Interface site).

    The address can be the IP address or the FQDN. If you use HTTPS, make sure to use the FQDN that you use in the SSL certificate on the BIG-IP system.

Application access control (SmartAccess)

If you want to control application access with SmartAccess filters through Access Policy Manager, make sure that the settings in the XenApp AppCenter management console for each of the applications you want to control, match these:

Citrix setting	Value
Allow connections made through Access Gateway	enabled

Citrix setting	Value
Access Gateway Farm	`APM`
Access Gateway Filter	The value must match the literal string that Access Policy Manager sets during access policy operation (through the Citrix SmartAccess action item)

Note: *The navigation path for application access control is* `AppCenter > Citrix Resources > XenApp > farm_name > Applications > application_name > Application Properties > Advanced Access Control`.

User access policies (SmartAccess)

You can control access to certain features, such as Client Drive or Printer Mapping, so that they are permitted only when a certain SmartAccess string is sent to XenApp server. If you want to control access to such features with SmartAccess filters through Access Policy Manager, you need to create a Citrix User Policy with Access Control Filter in the XenApp AppCenter management console for each feature that you want to control. Make sure that the Access Control Filter settings of the Citrix User Policy match these:

Citrix setting	Value
Connection Type	With Access Gateway
Access Gateway Farm	`APM`
Access Gateway Filter	The value must match the literal string that Access Policy Manager sets during access policy execution (through the Citrix SmartAccess action item)

Note: *The navigation path for user access policies is* `AppCenter > Citrix Resources > XenApp > farm_name > Policies > Users > Citrix User Policies > new_policy_name`. *Choose the feature from Categories and, if creating a new filter, select New Filter Element from Access Control.*

About Citrix Receiver requirements for Mac, iOS, and Android clients

To support Citrix Receivers for Mac, iOS, and Android, you must meet specific configuration requirements for the Citrix Receiver client.

Address field for standard Citrix service site (`/Citrix/PNAgent/`)

`https://<APM-external-virtual-server-FQDN>`

Address field for custom Citrix service site

`https://<APM-external-virtual-server-FQDN/custom_site/config.xml`, where *`custom_site`* is the name of the custom service site

Access Gateway

Select the Access Gateway check box and select Enterprise Edition.

Authentication

Choose either: Domain-only or RSA+Domain authentication

About Citrix Receiver requirements for Windows and Linux clients

To support Citrix Receiver for Windows and Linux clients, you must meet specific configuration requirements for the Citrix Receiver client, as described here.

Address field for standard Citrix service site (`/Citrix/PNAgent/`)

`https://<APM-external-virtual-server-FQDN>`

Address field for custom Citrix service site

`https://<APM-external-virtual-server-FQDN/custom_site/config.xml`, where *`custom_site`* is the name of the custom service site.

About Citrix requirements for SmartCard support

Access Policy Manager supports auto logon for XenApp and XenDesktop clients that connect through an APM dynamic webtop. APM supports auto logon using these methods:

- Password-based APM takes the user password from a Citrix remote desktop resource, and performs single sign-on (SSO) into XenApp or XenDesktop.
- Kerberos Citrix supports APM takes the user name and domain from an SSO configuration, and uses them to obtain a Kerberos ticket and perform SSO into XenApp.
- SmartCard (two-PIN prompt) A logon page that you configure requests the SmartCard PIN, APM takes the user name from a Citrix remote desktop resource and peforms SSO into XenApp or XenDesktop. When the user launches the Citrix application, the Windows login prompt displays an option to enter the SmartCard PIN. Thus, the user enters the PIN twice: once when logging in to APM and once on the Windows login screen when launching an application.

To use Kerberos or SmartCard auto logon options from APM, you must meet specific configuration requirements for Citrix as described here:

- Kerberos: Configure Kerberos Delegation in Active Directory as described in Citrix knowledge article CTX124603.
- SmartCard: Enable SID Enumeration on XenApp and XenDesktop as described in these Citrix knowledge articles: CTX117489 and CTX129968.

Note: *Requirements specified in the knowledge articles are applicable.*

About Citrix product terminology

XenApp server

Refers to the XML Broker in the farm where Citrix SmartAccess filters are configured and from which applications and features are delivered.

XenApp AppCenter

Refers to the management console for a XenApp farm.

Note: *The names of the Citrix products and components that provide similar services might be different in your configuration. Refer to AskF5™ (`support.f5.com`) to identify the supported version of Citrix in the compatibility matrix for the Access Policy Manager® version that you have. Then refer to version-specific Citrix product documentation for Citrix product names and features.*

Chapter 2

Integrating APM with a Citrix Web Interface Site

Overview: Integrating APM with Citrix Web Interface sites

In this implementation, Access Policy Manager® performs authentication while integrating with a Citrix Web Interface site. The Web Interface site communicates with the XenApp server, renders the user interface, and displays the applications to the client.

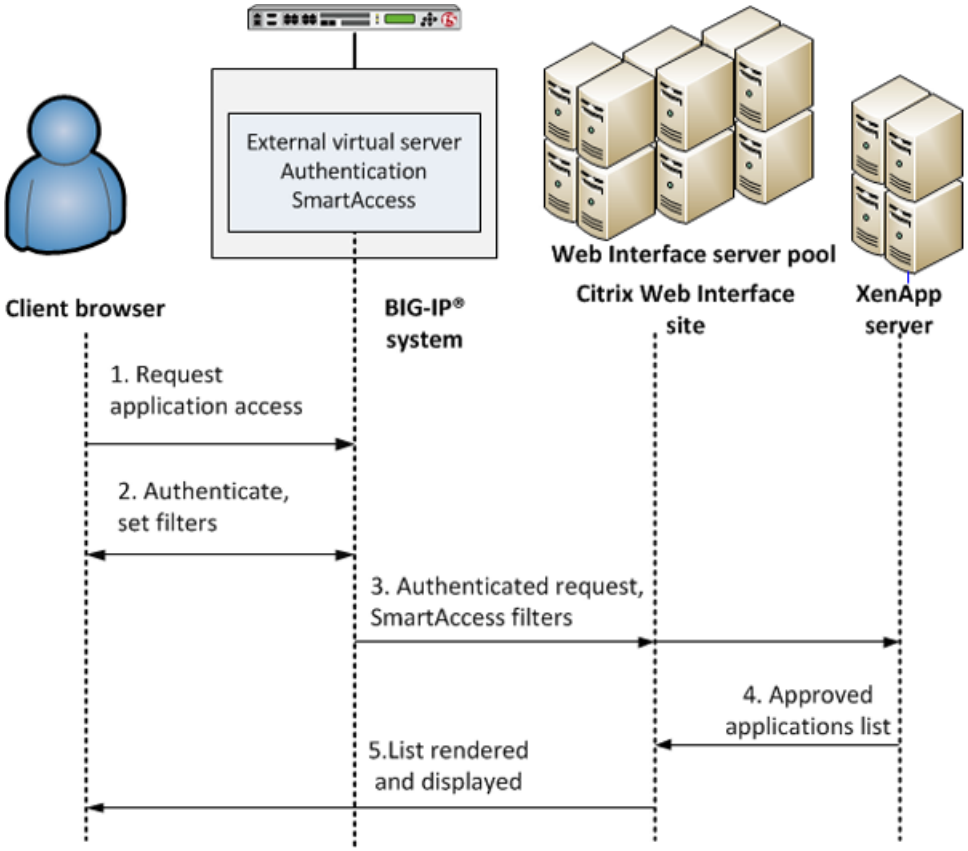


Figure 1: APM Citrix Web Interface integration with SmartAccess support

The preceding figure shows a configuration with one virtual server that communicates with clients and the Web Interface site.

1. A user (client browser or Citrix Receiver) requests access to applications or features.
2. The external virtual server starts an access policy that performs authentication and sets SmartAccess filters.
3. The external virtual server sends the authenticated request and filters to the Citrix Web Interface site. The Citrix Web Interface site, in turn, forwards the information to the XML broker (XenApp server).
4. The XML Broker returns a list of allowed applications to the Citrix Web Interface site.
5. The Citrix Web Interface site renders and displays the UI to the user.

In cases where the Web Interface site cannot communicate with an external virtual server, you must configure an additional, internal, virtual server to manage requests from the Citrix Web Interface as part of Smart Access and SSO. You need an internal virtual server, for example, when the Web Interface site is behind a firewall, uses HTTP in the Authentication URL, or uses a different SSL CA certificate for establishing trust with APM than the one used by client devices.

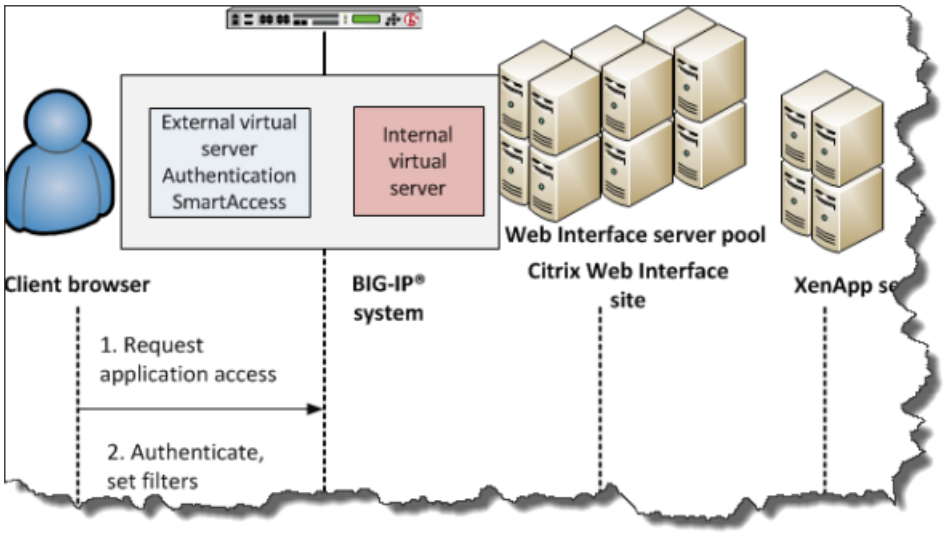


Figure 2: Internal virtual server for requests from Web Interface site

Supported clients

This implementation supports web clients and Citrix Receiver (iOS, Android, Mac, Windows, and Linux) clients.

Supported authentication

For Citrix Receiver Windows and Linux clients: only Active Directory authentication is supported.

For Citrix Receiver clients for iOS, Android, and Mac: Active Directory, or both RSA and Active Directory authentication is supported.

For web clients, you are not restricted in the type of authentication you use.

Task summary for APM integration with Citrix Web Interface sites

Ensure that you configure the Citrix components in the Citrix environment, in addition to configuring the BIG-IP® system to integrate with Citrix Web Interface sites.

Perform these tasks on the BIG-IP system to integrate Access Policy Manager® with a Citrix Web Interface site.

Task list

Creating an access policy for Citrix SSO
Adding Citrix Smart Access actions to an access policy
Creating a pool of Citrix Web Interface servers
Adding a connectivity profile
Creating a custom HTTP profile
Configuring the external virtual server
Creating a data group to support a nonstandard Citrix service site
Configuring an internal virtual server

Creating an access policy for Citrix SSO

Before you can create an access policy for Citrix single sign-on (SSO), you must meet these requirements:

- Configure the appropriate AAA servers to use for authentication.

  Note: *An Active Directory AAA server must include the IP address of the domain controller and the FQDN of the Windows domain name. If anonymous binding to Active Directory is not allowed in your environment, you must provide the admin name and password for the Active Directory AAA server.*

- Create an access profile using default settings.

Configure an access policy to authenticate a user and enable single sign-on (SSO) to Citrix published resources.

Note: *APM supports different types of authentication depending on the client type. This access policy shows how to use both RSA SecurID and AD Auth authentication (supported for Citrix Receiver for iOS, Mac, and Android) or AD Auth only (supported for Citrix Receiver for Windows and Linux). Use the type of authentication for the client that you need to support.*

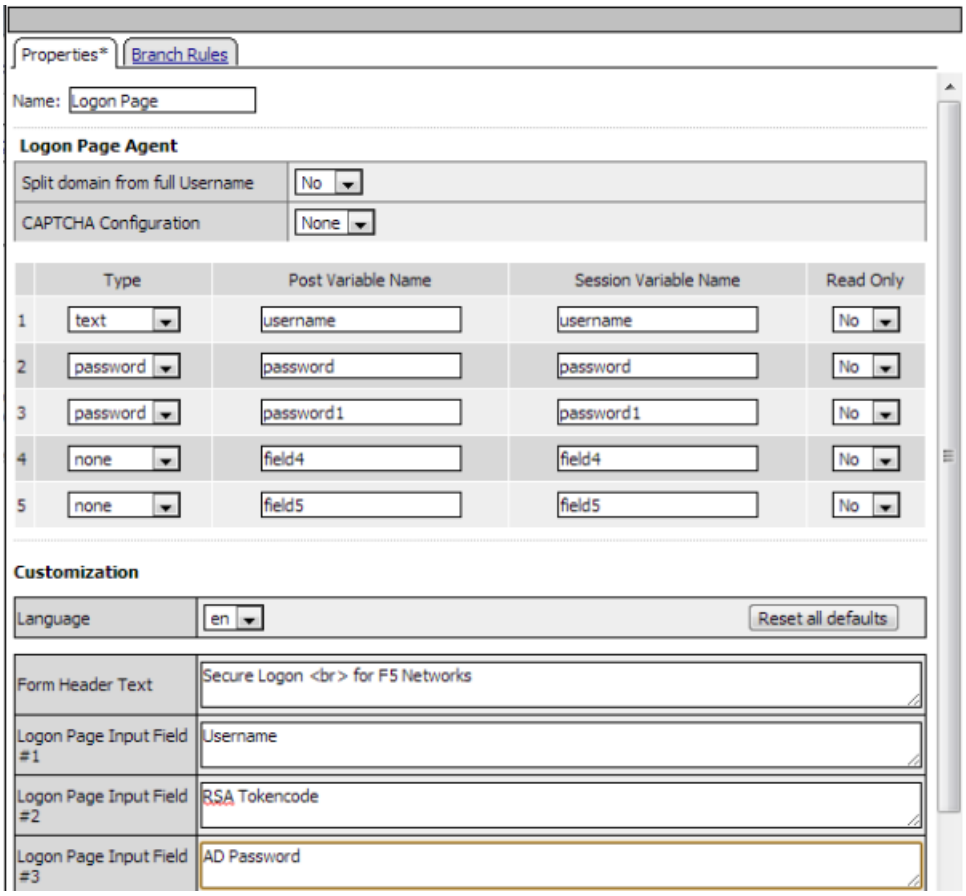
1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new action item.
   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
4. From the Logon Page tab, select **Logon Page**, and click **Add Item**.

   A properties screen displays.
5. Configure the Logon Page properties:

   - To support Active Directory authentication only, click **Save**.
   - To support both Active Directory and RSA SecurID authentication, configure the Logon Page to accept an RSA token and an AD password and click **Save**.

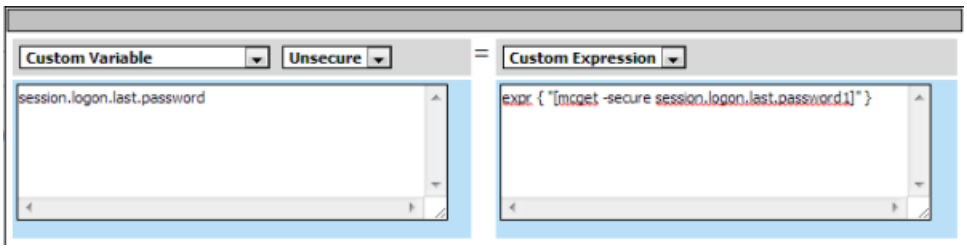
   In this example, Logon Page Input Field #2 accepts the RSA Token code into the `session.logon.last.password` variable (from which authentication agents read it). Logging Page

Input Field #3 saves the AD password into the *session.logon.last.password1* variable.



The properties screen closes.

6. (Optional) To add RSA SecurID authentication, click the plus (+) icon between **Logon Page** and **Deny**:
   a) From the **Authentication** tab, select **RSA SecurID**, and click **Add Item**.
   b) In the properties screen from the **Server** list, select the AAA server that you created previously and click **Save**.
      The properties screen closes.
   c) After the RSA SecurID action, add a Variable Assign action.
      Use the Variable Assign action to move the AD password into the *session.logon.last.password* variable.
   d) Click **Add new entry**.
      An **empty** entry appears in the Assignment table.
   e) Click the **change** link next to the empty entry.
      A dialog box appears, where you can enter a variable and an expression.
   f) From the left-side list, select **Custom Variable** (the default), and type `session.logon.last.password`.
   g) From the right-side list, select **Custom Expression** (the default), and type `expr { "[mcget -secure session.logon.last.password1] }"`.



The AD password is now available for use in Active Directory authentication.

h) Click **Finished** to save the variable and expression, and return to the Variable Assign action screen.

7. Add the AD Auth action after one of these actions:

- Variable Assign - This action is present only if you added RSA SecurID authentication.
- Logon Page - Add here if you did not add RSA SecurID authentication.

A properties screen for the AD Auth action opens.

8. Configure the properties for the AD Auth action:

a) From the **AAA Server** list, select the AAA server that you created previously.
b) To support Citrix Receiver clients, you must set **Max Logon Attempts** to 1.
c) Configure the rest of the properties as applicable to your configuration and click **Save**.

9. Click the Add Item (+) icon between **AD Auth** and **Deny**.

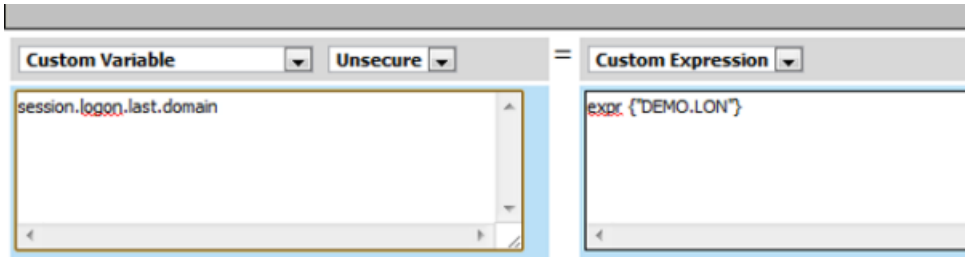
a) From the Assignment tab, select **SSO Credential Mapping**, and click **Add Item**.
b) Click **Save**.

The SSO Credential Mapping makes the information from the `session.logon.last.password` variable available (for Citrix SSO).

10. Add a Variable Assign action after the SSO Credential Mapping action.

Use the Variable Assign action to pass the domain name for the Citrix Web Interface site so that a user is not repeatedly queried for it.

a) Click **Add new entry**.
An **empty** entry appears in the Assignment table.
b) Click the **change** link next to the empty entry.
A dialog box appears, where you can enter a variable and an expression.
c) From the left-side list, select **Custom Variable** (the default), and type `session.logon.last.domain`.
d) From the right-side list, select **Custom Expression** (the default), and type an expression `expr {"DEMO.LON"}`, to assign the domain name for the Citrix Web Interface site (where DEMO.LON is the domain name of the Citrix Web Interface site).



e) Click **Finished** to save the variable and expression, and return to the Variable Assign action screen.

11. On the fallback path between the last action and **Deny**, click **Deny**, and then click **Allow** and **Save**.

12. Click **Close**.

You should have an access policy that resembles either of these examples:

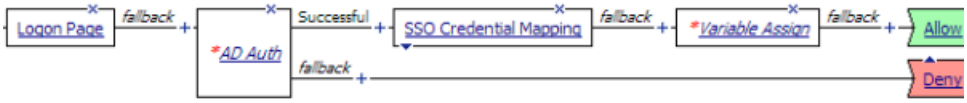


Figure 3: Example access policy with AD authentication, credential mapping, and Web Interface site domain assignment

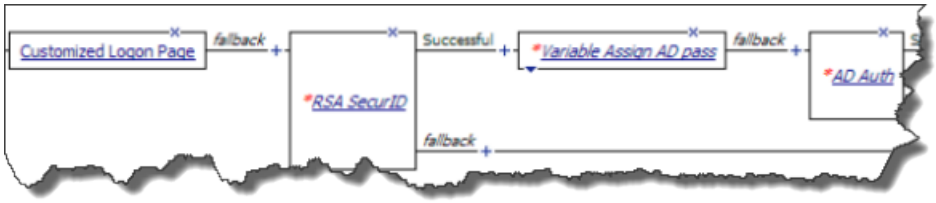


Figure 4: Configuring RSA SecurID authentication before AD authentication

Adding Citrix Smart Access actions to an access policy

To perform this task, first select the access profile you created previously, and open the associated access policy for edit.

You can set one or more filters per Citrix Smart Access action. If you include multiple Citrix Smart Access actions in an access policy, Access Policy Manager accumulates the SmartAccess filters that are set throughout the access policy operation.

1. Click the(+) icon anywhere in your access profile to which you want to add the Citrix Smart Access action item.
   The Add Item screen opens.
2. From **General Purpose**, select **Citrix Smart Access** and click **Add Item**.
   The Variable Assign: Citrix Smart Access properties screen opens.
3. Type the name of a Citrix SmartAccess filter in the open row under Assignment.

   A filter can be any string. Filters are not hardcoded, but must match filters that are configured in the XenApp™ server for application access control or a user policy.

   Note: *In the XenApp server, you must specify* `APM` *as the Access Gateway farm when you configure filters.*
4. To add another filter, click **Add entry** and type the name of a Citrix filter in the open row under Assignment.
5. When you are done adding filters, click **Save** to return to the Access Policy.

You now need to save the access policy and assign it to a virtual server.

Example access policy with Citrix SmartAccess filters

Here is a typical example access policy that uses Citrix SmartAccess filters to restrict access to published applications based on the result of client inspection. Client inspection can be as simple as IP Geolocation

Match or Antivirus. The figure shows an access policy being configured with a Citrix Smart Access action to set a filter to `antivirus` after an antivirus check is successful.

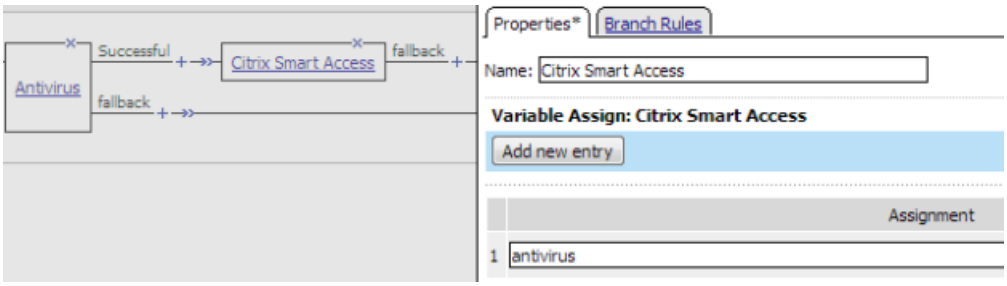


Figure 5: Example access policy with Citrix SmartAccess action and an antivirus check

Creating a pool of Citrix Web Interface servers

Create a pool of Citrix Web Interface servers for high availability.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. In the Resources area, using the **New Members** setting, add each resource that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select **Node List** and select an address from the list of available addresses.
   b) If access to the Web Interface site is through SSL, in the **Service Port** field type `443`; otherwise, type `80`.
   c) Click **Add**.
5. Click **Finished**.

The new pool appears in the Pools list.

Adding a connectivity profile

Create a connectivity profile to configure client connections for Citrix remote access.

Note: *A Citrix client bundle provides an installable Citrix Receiver client. The default parent connectivity profile includes a default Citrix client bundle.*

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Click **Add**.
   The Create New Connectivity Profile popup screen opens and displays General Settings.
3. Type a **Profile Name** for the connectivity profile.
4. From the **Parent Profile** list, select the default profile, **connectivity**.
5. To use a Citrix bundle that you have configured, select **Citrix Client Settings** from the left pane and select the bundle from the **Citrix Client Bundle** list in the right pane.

The default Citrix client bundle is included if you do not perform this step.

6. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

The connectivity profile appears in the Connectivity Profile List.

Creating a custom HTTP profile

An HTTP profile defines the way that you want the BIG-IP® system to manage HTTP traffic.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Services** > **HTTP**.
   The HTTP profile list screen opens.
2. Click **Create**.
   The New HTTP Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Parent Profile** list, select **http**.
5. Select the **Custom** check box.
6. From the **Redirect Rewrite** list, select **All**.
7. Click **Finished**.

The custom HTTP profile now appears in the HTTP profile list screen.

Configuring the external virtual server

Create a virtual server to support Citrix traffic and respond to client requests.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, select **Host** and in the **Address** field, type the **IP address** for the virtual server.

   If you plan to configure only one virtual server to integrate with Citrix Web Interface sites, then the authentication URL of the Web Interface site must match the IP address of this virtual server.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **Configuration** list, select **Advanced**.
7. (Optional) For the **SSL Profile (Client)** setting, select an SSL profile with an SSL certificate that is trusted by clients.
8. If you use SSL to access the Web Interface site, add an SSL profile to the **SSL Profile (Server)** field.
9. From the **HTTP Profile** list, select the custom http profile that you created previously.

   The HTTP profile must have **Redirect Rewrite** set to **All**.
10. From the **Source Address Translation** list, select **Auto Map**.
11. In the Access Policy area, from the **Access Profile** list, select the access profile.
12. In the Access Policy area, from the **Connectivity Profile** list, select the connectivity profile.
13. Select the **VDI & Java Support** check box.

14. In the Resources area, from the **Default Pool** list, select the name of the pool that you created previously.
15. Click **Finished**.

The access policy is now associated with the virtual server.

Creating a data group to support a nonstandard Citrix service site

By default, APM recognizes `/Citrix/PNAgent/config.xml` as the default URL that Citrix Receiver clients request. If your Citrix Receiver clients use a value that is different from /Citrix/PNAgent/config.xml, you must configure a data group so that APM® can recognize it.

1. On the Main tab, click **Local Traffic** > **iRules** > **Data Group List**.
   The Data Group List screen opens, displaying a list of data groups on the system.
2. Click **Create**.
   The New Data Group screen opens.
3. In the **Name** field, type `APM_Citrix_ConfigXML`.
   Type the name exactly as shown.
4. From the **Type** list, select **String**.
5. In the Records area, create a string record.
   a) In the **String** field, type the FQDN of the external virtual server (using lowercase characters only).
   For example, type `apps.mycompany.com`.
   b) In the **Value** field, type the value that you use instead of Citrix/PNAgent/config.xml. For example, type `/Connect/config.xml`.
   c) Click **Add**.
6. Click **Finished**.
   The new data group appears in the list of data groups.

Configuring an internal virtual server

Before you start this task, configure an access profile with default settings.

Configure an internal virtual server to handle requests from the Citrix Web Interface site when it is behind a firewall, using HTTP, or otherwise unable to communicate with an external virtual server.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, select **Host** and in the **Address** field, type the IP address for the virtual server.
   When you configure an internal virtual server, the authentication URL of the Web Interface site must match the IP address of this virtual server.
5. For the **Service Port** setting, select **HTTP** or **HTTPS**.
   The protocol you select must match the protocol you used to configure the authentication service URL on the Web Interface site.

6. If you are encrypting traffic between the APM and the Citrix Web Interface, for the **SSL Profile (Client)** setting, select an SSL profile that has an SSL certificate trusted by the Citrix Web Interface.
7. From the **HTTP Profile** list, select **http**.
8. In the Access Policy area, from the **Access Profile** list, select the access profile.
9. In the Access Policy area, from the **Connectivity Profile** list, select the connectivity profile.
10. Select the **VDI & Java Support** check box.
11. Click **Finished**.

The access policy is now associated with the virtual server.

Chapter 3

Integrating APM with Citrix XML Brokers

Overview: Integrating APM with Citrix XML Brokers with SmartAccess support

In this implementation, you integrate Access Policy Manager® (APM®) with Citrix XML Brokers and present Citrix published applications on an APM dynamic webtop.

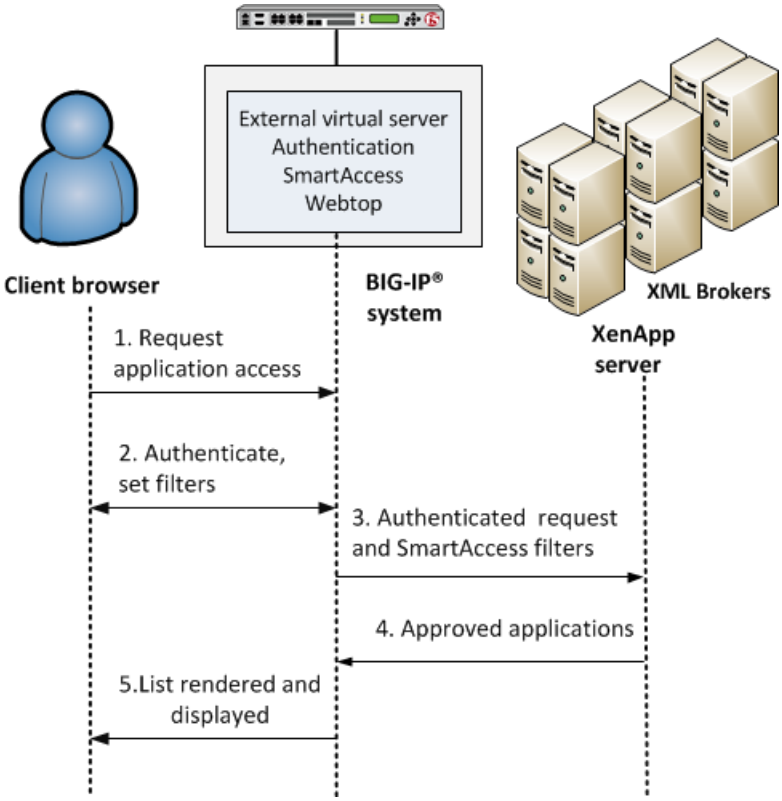


Figure 6: APM integration with Citrix XML Brokers

1. A user (client browser or Citrix Receiver) requests access to applications.
2. The virtual server starts an access policy that performs authentication and sets SmartAccess filters.
3. The virtual server sends the authenticated request and filters to a Citrix XML Broker.
4. An XML Broker returns a list of allowed applications to the external virtual server.
5. The virtual server renders and displays the user interface to the client on an Access Policy Manager webtop.

Supported authentication

For Citrix Receiver Windows and Linux clients: only Active Directory authentication is supported.

For Citrix Receiver clients for iOS, Android, and Mac: Active Directory, or both RSA and Active Directory authentication is supported.

For web clients, you are not restricted in the type of authentication you use.

About APM dynamic webtop for Citrix XML Brokers

A dynamic webtop enables Access Policy Manager® (APM®) to act as a presentation layer for Citrix published resources. APM communicates directly with Citrix XML Brokers, retrieves a list of published resources, and displays them to the user on a dynamic webtop.

The addresses of XML Brokers are configured in pools on APM. A pool includes addresses from one Citrix farm. You specify a pool as a destination in a Citrix remote desktop resource. Each resource logically represents a Citrix farm. You can assign multiple resources to a user, enabling the user to access Citrix applications from multiple Citrix farms.

How to specify different actions for different clients

The Client Type action determines whether the client is using a full browser, the BIG-IP® Edge Client, or another client to access the Access Policy Manager®. (APM®) This action makes it possible for you to specify different actions for different client types in one access policy. As a result, when you add such an access policy to a virtual server, you can then use one virtual server for traffic from different client types. This figure shows the Client Type action as it looks when first added to an access policy.

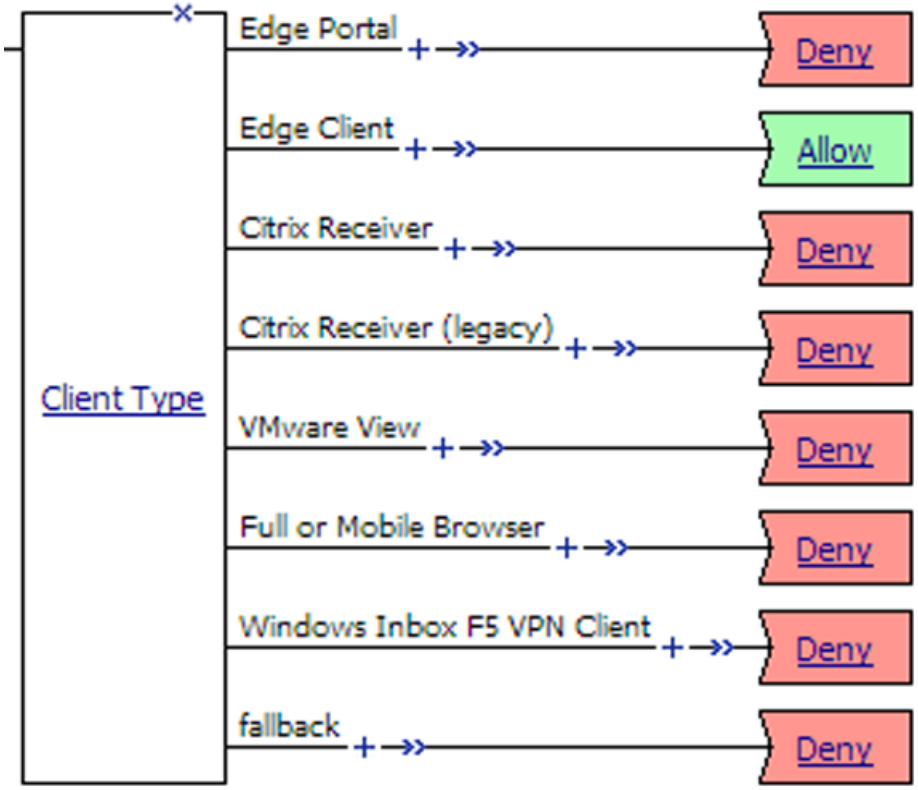


Figure 7: Client Type action

By default, the Client Type action includes these branches:

Edge Portal

Indicates that the user is connecting with the BIG-IP® Edge Portal® mobile app.

Edge Client
Indicates that the user is connecting with the BIG-IP® Edge Client® or BIG-IP Edge Client app, supported on multiple devices and operating systems.

Citrix Receiver
Indicates that the user is connecting using a later Citrix Receiver client.

Citrix Receiver (legacy)
Indicates that the user is connecting using an earlier Citrix Receiver client (identified with PN Agent).

VMware View
Indicates that the user is connecting using a VMware Horizon View client.

Full or Mobile Browser
Indicates the user is connecting with a Windows web browser or a mobile browser.

Windows Inbox F5 VPN Client
Indicates the user is connecting using the Windows Inbox F5 VPN client.

fallback
Indicates the user is connecting with another method.

APM supports the client types on multiple operating systems. Refer to AskF5™ (`support.f5.com`) to look up the supported operating systems and versions in the compatibility matrix for your version of APM.

Note: *To create additional branching for a client type based on operating system, you can add a client operating system (Client OS) action on the client type branch.*

About Citrix client bundles in APM

A Citrix client bundle enables delivery of a Citrix Receiver client to a user's Windows computer when a client is not currently installed, or when a newer client is available. Access Policy Manager® (APM®) detects whether the Citrix Receiver client is present and redirects users to a download URL, or downloads a Citrix Receiver client that you have uploaded.

In Access Policy Manager, you specify the Citrix client bundle in a connectivity profile. By default, a connectivity profile includes the default Citrix bundle, `/Common/default-citrix-client-bundle`, which contains a download URL, `receiver.citrix.com`.

Note: *You can upload Citrix Receiver clients from the Application Access area of Access Policy Manager.*

About auto logon from APM dynamic webtop and authentication

Access Policy Manager® supports two auto logon options for Citrix that provide password-less authentication:

- Kerberos - Supports any kind of password-less authentication on APM®: SmartCard, RSA PIN, client SSL certificate, and so on. Citrix supports Kerberos only for XenApp.
- SmartCard - Citrix supports SmartCard for XenDesktop. Citrix also supports SmartCard for XenApp.

  Note: *When using SmartCard with XenApp, a user is prompted for a SmartCard PIN twice: once when logging in to APM and again when starting a Citrix application.*

These options work in APM only when:

- Citrix is configured to support SmartCard SSO (with Kerberos) or SmartCard.
- Citrix requirements for using SmartCard SSO or SmartCard are met.

Task summary for XML Broker integration with APM

Ensure that you configure the Citrix components in the Citrix environment, in addition to configuring the BIG-IP® system to integrate with Citrix XML Brokers.

Perform these tasks on the BIG-IP system so that Access Policy Manager® can present Citrix published resources on a dynamic webtop.

Task list

Creating a pool of Citrix XML Brokers

Create one pool of XML Brokers for each Citrix farm that you want to support.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. In the Resources area, using the **New Members** setting, add each resource that you want to include in the pool:
   a) Either type an IP address in the **Address** field, or select a preexisting node address from the **Node List**.
   b) If access to the XML Broker is through SSL, in the **Service Port** field, type `443` or select **HTTPS** from the list; otherwise, type `80` or select **HTTP** from the list.
   c) Click **Add**.
5. Click **Finished**.

The new pool appears in the Pools list.

Configuring a Citrix remote desktop resource

Create one Citrix remote desktop resource for each Citrix farm that you want to support.

1. On the Main tab, click **Access Policy** > **Application Access** > **Remote Desktops**.
   The Remote Desktops list opens.
2. Click **Create**.
   The New Resource screen opens.
3. Type a name for the remote desktop resource.
4. For the **Type** setting, retain the default **Citrix**.
5. For the **Destination** setting, select **Pool** and select the pool that you created previously.
6. In the Auto Logon area, select the **Enable** check box to automatically log on to a Citrix XML Broker.
   a) From the **Broker Authentication** list, select the type of authentication to use, either Password-based, Kerberos, or SmartCard.

      The Kerberos and SmartCard options enable password-less authentication. You cannot use either of them successfully unless Citrix is configured for SmartCard SSO (Kerberos) or SmartCard.

      The fields that are displayed vary based on this selection.
   b) In the **Username Source** field, accept the default or type the session variable to use as the source for the auto logon user name.
   c) In the **Password Source** field, accept the default or type the session variable to use as the source for the auto logon user password.
   d) In the **Domain Source** field, accept the default or type the session variable to use as the source for the auto logon user domain.
   e) From the **Kerberos SSO** list, select a Kerberos SSO configuration that has already been configured.
7. In the Customization Settings for *language_name* area, type a **Caption**.
   The caption is the display name of the Citrix resource on the APM webtop.
8. Click **Finished**.
   All other parameters are optional.

This creates the Citrix remote desktop resource.

Configuring a dynamic webtop

A dynamic webtop allows you to see a variety of resources protected by Access Policy Manager®, including Citrix Published Applications.

1. On the Main tab, click **Access Policy** > **Webtops**.
2. Click **Create**.
3. Type a name for the webtop.
4. From the **Type** list, select **Full**.
5. Click **Finished**.

The webtop is now configured, and appears in the webtop list.

Creating an access policy for Citrix SSO (APM dynamic webtop)

Before you can create an access policy for Citrix single sign-on (SSO), you must meet these requirements:

- Configure the appropriate AAA servers to use for authentication.

Note: *An Active Directory AAA server must include the IP address of the domain controller and the FQDN of the Windows domain name. If anonymous binding to Active Directory is not allowed in your environment, you must provide the admin name and password for the Active Directory AAA server.*

- Create an access profile using default settings.

Configure an access policy to authenticate a user and enable single sign-on (SSO) to Citrix published resources.

Note: *APM® supports different types of authentication depending on the client type. This access policy shows how to use the Client Type action to configure authentication for legacy Citrix Receiver clients (Windows and Linux) and later Citrix Receiver clients (iOS, Mac, and Android) in the same access policy.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new action item.
   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
4. Type `client` in the search field and select **Client Type** from the results.
   A properties screen displays.
5. Click **Save**.
   The properties screen closes and the Client Type action displays in the visual policy editor.
6. To configure actions for Citrix Receiver for Windows and Linux clients, perform these substeps.

   Note: *Citrix Receiver for Windows and Citrix Reciver for Linux support Active Directory authentication only.*

   a) Click the (+) icon on the Citrix Receiver (legacy) branch after the Client Type action.
   b) On the Logon tab, select **Logon Page**, and click **Add Item**.

      A properties screen displays. The default logon page settings are acceptable.

   c) Click **Save**.
   d) After the Logon Page action, add an SSO Credential Mapping action with default settings.
   e) After the SSO Credential Mapping action, click the (+) icon.
   f) Type **var** into the search field, select **Variable Assign** from the results, and click **Add Item**.

      Use the Variable Assign action to pass the domain name for the Citrix remote desktop resource so that a user is not repeatedly queried for it.

      A properties screen opens.

   g) Click **Add new entry**.
      An **empty** entry appears in the Assignment table.
   h) Click the **change** link next to the empty entry.
      A dialog box appears, where you can enter a variable and an expression.
   i) From the left-side list, retain the **Custom Variable** setting, and type `session.logon.last.domain`.
   j) From the right-side list, retain the **Custom Expression** setting and type `expr { "[example.com] }"` to assign the domain name for the Citrix remote desktop resource (where `example.com` is the domain name of the resource).

      The Citrix remote destop resource equates to an XML Broker that is selected from a pool.

   k) Click **Finished**.
   l) Click **Save**.
   m) After the previous action, click the **Deny** ending and select the **Allow** ending.

The access policy branch for legacy Citrix Receiver clients is complete.

7. To configure actions for Citrix Receiver for iOS, Android, and Mac, complete the remaining steps.

   Citrix Receiver for iOS, Android, and Mac, support both RSA SecurID and AD Auth authentication. This example shows how to use both.

8. After the Client Type action, on the Citrix Receiver branch, click the (+) icon.
9. On the Logon tab, select **Logon Page**, and click **Add Item**.
10. Customize the Logon Page to accept an RSA token and an Active Directory password:
    a) In row 3: From the **Type** list, select **password**; In the **Post Variable Name** field, type `password1`; In the **Session Variable Name** field, type `password1`.

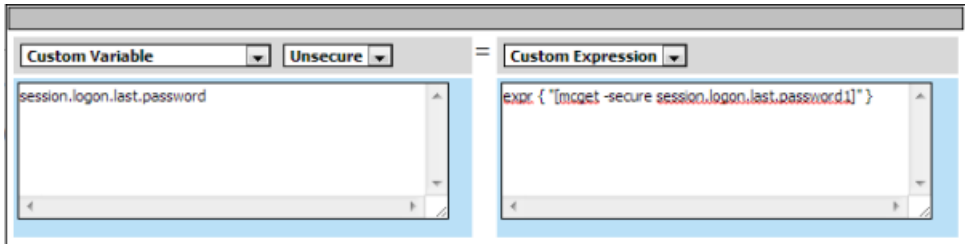
       APM stores the text that a user types into this field in the *`session.logon.last.password1`* session variable.

       You have added another password field to the logon page.
    b) In **Login Page Input Field #2**, type `RSA Token`.
       You replaced the existing prompt for the first password field.
    c) In **Login Page Input Field #3**, type `AD Password`.
       You provided a prompt for the second password field.

11. To add RSA SecurID authentication, click the plus (+) icon between **Logon Page** and **Deny**:
    a) Type `rsa` in the search field, select **RSA SecurID** from the results, and click **Add Item**.
    b) From the **Server** list, select the AAA RSA SecurID server that you created previously and click **Save**.
       The properties screen closes.
    c) After the RSA SecurID action, add a Variable Assign action.

       Use the Variable Assign action to move the AD password into the *`session.logon.last.password`* session variable; the authentication agent requires this.

       A Variable Assign properties page opens.
    d) Click **Add new entry**.
       An **empty** entry appears in the Assignment table.
    e) Click the **change** link next to the empty entry.
       A dialog box appears, where you can enter a variable and an expression.
    f) From the left-side list, retain the **Custom Variable** setting, and type `session.logon.last.password`.
    g) From the right-side list, retain the **Custom Expression** setting, and type `expr { "[mcget -secure session.logon.last.password1] }"`.



    h) Click **Finished** to save the variable and expression, and return to the Variable Assign action screen.
    i) Click **Save**.

12. After the previous action, add an AD Auth action and configure properties for it:
    a) From the **AAA Server** list, select the AAA server that you created previously.
    b) To support Citrix Receiver clients, you must set **Max Logon Attempts** to 1.
    c) Configure the rest of the properties as applicable to your configuration and click **Save**.

13. Click the Add Item (+) icon between **AD Auth** and **Deny**.
    a) On the Assignment tab, select **SSO Credential Mapping**, and click **Add Item**.
    b) Click **Save**.

    The SSO Credential Mapping makes the information from the `session.logon.last.password` variable available for Citrix SSO.
14. Add a Variable Assign action after the SSO Credential Mapping action.

    Use the Variable Assign action to pass the domain name for an XML Broker so that a user is not repeatedly queried for it.
    a) Click **Add new entry**.
    An **empty** entry appears in the Assignment table.
    b) Click the **change** link next to the empty entry.
    A dialog box appears, where you can enter a variable and an expression.
    c) From the left-side list, select **Custom Variable** (the default), and type `session.logon.last.domain`.
    d) From the right-side list, select **Custom Expression** (the default), and type an expression `expr {"example.com"}`.
    e) Click **Finished** to save the variable and expression, and return to the Variable Assign action screen.
15. On the fallback path between the last action and **Deny**, click **Deny**, and then click **Allow** and **Save**.
    The access policy branch for the Citrix Receiver client type is complete.
16. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.
17. Click **Close**.

You should have an access policy that contains actions for both Citrix Receiver client types.

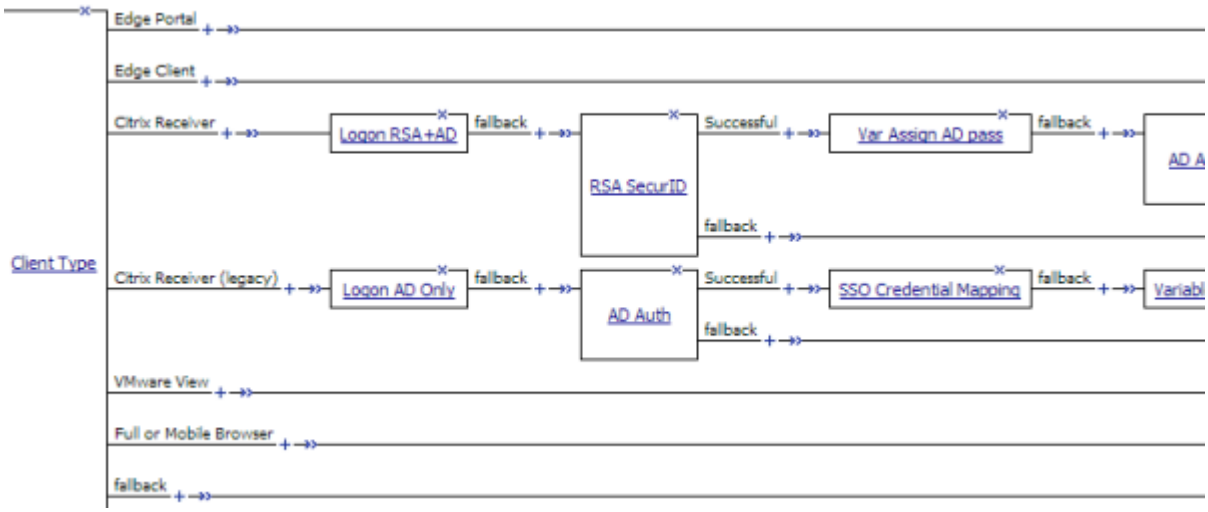


Figure 8: Example access policy for legacy Citrix Receiver clients and later Citrix Receiver clients

Assigning Citrix resources to an access policy for Citrix integration

Before you start, create or select an access profile and open the associated access policy for edit.

Assign the webtop and Citrix remote desktop resources that you configured to a session so that XML Brokers associated with the resources can return the appropriate published resources for display on the webtop.

Note: *This access policy shows how to use the Advanced Resource Assign action item to assign the resources. Alternatively, you can use the Resource Assign and Webtop and Links Assign action items.*

1. Click the **(+)** icon anywhere in the access policy to add a new action item.
   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
2. On the Assignment tab, select **Advanced Resource Assign** and click **Add Item**.
   The properties screen opens.
3. Click **Add new entry**.
   An **Empty** entry displays.
4. Click the **Add/Delete** link below the entry.
   The screen changes to display resources that you can add and delete.
5. Select the Remote Desktop tab.
   A list of remote desktop resources is displayed.
6. Select Citrix remote desktop resources and click **Update**.
   You are returned to the properties screen where Remote Desktop and the names of the selected resources are displayed.
7. Click **Add new entry**.
   An **Empty** entry displays.
8. Click the **Add/Delete** link below the entry.
   The screen changes to display resources that you can add and delete.
9. Select the Webtop tab.
   A list of webtops is displayed.
10. Select a webtop and click **Update**.
    The screen changes to display properties and the name of the selected webtop is displayed.
11. Select **Save** to save any changes and return to the access policy.

Citrix remote desktop resource and an Access Policy Manager® (APM®) dynamic webtop, are now assigned to the session.

Adding Citrix Smart Access actions to an access policy

To perform this task, first select the access profile you created previously, and open the associated access policy for edit.

You can set one or more filters per Citrix Smart Access action. If you include multiple Citrix Smart Access actions in an access policy, Access Policy Manager accumulates the SmartAccess filters that are set throughout the access policy operation.

1. Click the(+) icon anywhere in your access profile to which you want to add the Citrix Smart Access action item.
   The Add Item screen opens.
2. From **General Purpose**, select **Citrix Smart Access** and click **Add Item**.
   The Variable Assign: Citrix Smart Access properties screen opens.
3. Type the name of a Citrix SmartAccess filter in the open row under Assignment.
   A filter can be any string. Filters are not hardcoded, but must match filters that are configured in the XenApp™ server for application access control or a user policy.

Note: *In the XenApp server, you must specify* `APM` *as the Access Gateway farm when you configure filters.*

4. To add another filter, click **Add entry** and type the name of a Citrix filter in the open row under Assignment.
5. When you are done adding filters, click **Save** to return to the Access Policy.

You now need to save the access policy and assign it to a virtual server.

Example access policy with Citrix SmartAccess filters

Here is a typical example access policy that uses Citrix SmartAccess filters to restrict access to published applications based on the result of client inspection. Client inspection can be as simple as IP Geolocation Match or Antivirus. The figure shows an access policy being configured with a Citrix Smart Access action to set a filter to `antivirus` after an antivirus check is successful.

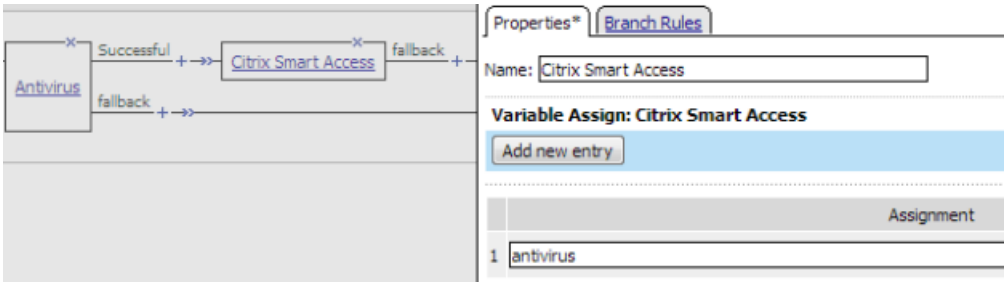


Figure 9: Example access policy with Citrix SmartAccess action and an antivirus check

Adding a connectivity profile

Create a connectivity profile to configure client connections for Citrix remote access.

Note: *A Citrix client bundle provides an installable Citrix Receiver client. The default parent connectivity profile includes a default Citrix client bundle.*

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Click **Add**.
   The Create New Connectivity Profile popup screen opens and displays General Settings.
3. Type a **Profile Name** for the connectivity profile.
4. From the **Parent Profile** list, select the default profile, **connectivity**.
5. To use a Citrix bundle that you have configured, select **Citrix Client Settings** from the left pane and select the bundle from the **Citrix Client Bundle** list in the right pane.
   The default Citrix client bundle is included if you do not perform this step.
6. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

The connectivity profile appears in the Connectivity Profile List.

Adding Citrix Receiver for HTML5 to a connectivity profile

Download the Citrix Receiver for HTML5 from the Citrix website.

You add Citrix Receiver for HTML5 to a Citrix bundle and add the bundle to a connectivity profile so that APM® can deliver Citrix Receiver for HTML5 to clients.

1. From the command line, type `msiexec /a filepath to MSI file /qb TARGETDIR=filepath to target folder`.
2. On the Main tab, click **Access Policy** > **Application Access** > **Remote Desktops** > **Citrix Client Bundles**.
   a) In the **Name** field, type a name that includes `html5`.
   b) From the **Source** list, select **Windows Package File**.
   c) Click **Choose File** and upload the file `./Citrix/HTML5 Management/HTML5Client.zip`.
3. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   a) Click the **Connectivity Profile List** tab.
   b) Select the connectivity profile you want to update.
   c) Click **Edit Profile**.
   A popup screen opens.
   d) Click **Citrix Client Settings**.
   e) From the **Citrix Client Bundle** list, select the bundle with `html5` in its name.

The Citrix Receiver for HTML5 is included in a bundle with a particular connectivity profile.

For a connectivity profile to go into effect, you must add it to a virtual server.

Creating a virtual server to support Citrix web and mobile clients

This virtual server supports Citrix traffic and responds to web and mobile client requests.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, select **Host** and in the **Address** field, type the IP address for the virtual server.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **Configuration** list, select **Advanced**.
7. For the **SSL Profile (Client)** setting, from the **Available** list, select an SSL profile with an SSL certificate that the clients trust, and use the Move button to move the name to the **Selected** list.
8. If access to XML Brokers requires SSL, then for the SSL Profile (Server) setting, select an SSL profile.
9. From the **Source Address Translation** list, select **Auto Map**.
10. In the Access Policy area, from the **Access Profile** list, select the access profile.
11. In the Access Policy area, from the **Connectivity Profile** list, select the connectivity profile.
12. Select the **VDI & Java Support** check box.
13. Click **Finished**.

The access policy is now associated with the virtual server.

Chapter 4

Shaping Citrix Client MultiStream ICA Traffic

Overview: Shaping traffic for Citrix clients that support MultiStream ICA

Access Policy Manager® (APM®) can perform traffic shaping for Citrix clients that support MultiStream ICA. You can add the configuration required for traffic shaping to an existing integration of APM by adding a BWC Policy action to an existing access policy.

Consult Citrix documentation for the clients and client platforms that support MultiStream ICA.

About Citrix XenApp server requirements for shaping traffic with APM

To support traffic shaping for Citrix MultiStream ICA clients with Access Policy Manager® (APM®), you must meet specific configuration requirements on the Citrix XenApp server as described here.

- Citrix MultiStream ICA must be enabled.
- A Citrix Multi-Port Policy must be configured with four MultiStream ICA ports, one for each priority (high, very high, medium, and low). This example uses ports `2598-2601`.
  - CGP default port: Default port; CGP default port priority: High

    Note: *CGP default port is usually `2598`.*

  - CGP port1: 2799 CGP port1 priority: Very High
  - CGP port2: 2800 CGP port2 priority: Medium
  - CGP port3: 2801 CGP port3 priority: Low

When a XenApp server is configured correctly, you can use a network monitoring utility, such as `netstat`, and see that an XTE.exe process is listening on the configured ports as shown in this example.

```
C:\> netstat –abno

Active Connections

Proto  Local Address          Foreign Address        State           PID
…
TCP    0.0.0.0:2598           0.0.0.0:0              LISTENING       6416
[XTE.exe]
TCP    0.0.0.0:2799           0.0.0.0:0              LISTENING       6416
[XTE.exe]
TCP    0.0.0.0:2800           0.0.0.0:0              LISTENING       6416
[XTE.exe]
TCP    0.0.0.0:2801           0.0.0.0:0              LISTENING       6416
[XTE.exe]
```

Note: *When you change or configure a policy, it takes effect on the XenApp server after a system restart.*

Task summary

Task list

Creating a dynamic bandwidth control policy for Citrix MultiStream ICA traffic
Adding support for Citrix traffic shaping to an access policy

Creating a dynamic bandwidth control policy for Citrix MultiStream ICA traffic

You create a dynamic bandwidth control policy to support traffic shaping for Citrix MultiStream ICA traffic on the BIG-IP® system.

1. On the Main tab, click **Acceleration** > **Bandwidth Controllers**.
2. Click **Create**.
3. In the **Name** field, type a name for the bandwidth control policy.
4. In the **Maximum Rate** field, type a number and select the unit of measure to indicate the total throughput allowed for the resource you are managing.

   The number must be in the range from `1 Mbps` to `320 Gbps`. This value is the amount of bandwidth available to all the connections going through this static policy.
5. From the **Dynamic** list, select **Enabled**.
   The screen displays additional settings.
6. In the **Maximum Rate Per User** field, type a number and select the unit of measure to indicate the most bandwidth that each user or session associated with the bandwidth control policy can use.

   The number must be in the range from `1 Mbps` to `2 Gbps`.
7. In the **Categories** field, add four categories of traffic that this bandwidth control policy manages for Citrix: very high, high, medium, and low.

   All the categories share the specified bandwidth, in accordance with the rate specified for each category.

   The category names you specify here display in the visual policy editor when you add a bandwidth control (BWC) policy action to an access policy.
   a) In the **Category Name** field, type a descriptive name for the category.
   b) In the **Max Category Rate** field, type a value to indicate the most bandwidth that this category of traffic can use, and select **%** from the list and type a percentage from `1` to `100`.
   c) Click **Add** to add the category to the **Categories** list.
   d) Repeat these steps to add the additional categories until you have defined all four required categories.
8. Click **Finished**.

The system creates a dynamic bandwidth control policy.

You might create a policy with a maximum rate of 20 Mbps and a maximum rate per user of 10 Mbps with categories named like this: bwcVH, bwcH, bwcM, and bwcL and with maximum category rate in percent, such as 40, 30, 20, 10 accordingly.

For the bandwidth control policy to take effect, you must apply the policy to traffic, using the BWC policy action in an access policy.

Adding support for Citrix traffic shaping to an access policy

Add actions to an existing access policy to provide traffic shaping for Citrix MultiStream ICA clients.

Note: *You need to determine where to add these actions in the access policy. You might need to precede these actions with a Client Type action to determine whether these actions are appropriate to the client.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. On an access policy branch, click the **(+)** icon to add an item to the access policy.
   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
4. Add a BWC Policy action:
   a) Type BWC into the search field.

      Search is not case-sensitive.

      Results are listed.
   b) Select **BWC Policy** from the results and click **Add Item**.

      A properties screen opens.
   c) From the **Dynamic Policy** list, select the dynamic bandwidth policy that you configured previously for Citrix MultiStream ICA clients.
      Lists for these properties: **Very High Citrix BWC Category**,**High Citrix BWC Category**, **Medium Citrix BWC Category**, and **Low Citrix BWC Category** include the categories configured in the selected dynamic bandwidth policy.
   d) From the **Very High Citrix BWC Category** list, select the category that corresponds to the very high setting.
   e) For each of the remaining properties: **High Citrix BWC Category**, **Medium Citrix BWC Category**, and **Low Citrix BWC Category**, select a category that corresponds to the setting.
   f) Click **Save**.
5. On an access policy branch, click the **(+)** icon to add an item to the access policy.
   A popup screen displays actions on tabs, such as General Purpose and Authentication, and provides a search field.
6. Type `Var` in the search field, select **Variable Assign** from the results, and click **Add Item**.

   In this Variable Assign action, you create one entry for each of the four ports that are configured in the Citrix Multi-Port Policy on the Citrix XenApp server.

   A properties screen opens.
7. Assign a variable for the CGP port that is configured with very high priority in the Multi-Port Policy on the Citrix XenApp server.
   a) Click **Add new entry**.
      An **empty** entry displays in the Assignment table.
   b) Click the **change** link next to the empty entry.
      A dialog box, where you can enter a variable and an expression, displays.
   c) In the **Custom Variable** field, type `citrix.msi_port.very_high`.
   d) In the **Custom Expression** field, type `expr {"2599"}`.

      Replace `2599` with the port number defined for the CGP port with very high priority on the Citrix XenApp server.

e) Click **Finished**.
The popup screen closes.

8. Assign a variable for the CGP port that is configured with high priority in the Multi-Port Policy on the Citrix XenApp server.

a) Click **Add new entry** and click the **change** link next to the new empty entry that displays.
b) In the **Custom Variable** field, type `citrix.msi_port.high`.
c) In the **Custom Expression** field, type `expr {"2598"}`.

Replace `2598` with the port number defined for the CGP port with high priority on the Citrix XenApp server.

d) Click **Finished**.
The popup screen closes.

9. Assign a variable for the CGP port that is configured with medium priority in the Multi-Port Policy on the Citrix XenApp server.

a) Click **Add new entry** and then click the **change** link next to the new empty entry that displays.
b) In the **Custom Variable** field, type `citrix.msi_port.mid`.
c) In the **Custom Expression** field, type `expr {"2600"}`.

Replace `2600` with the port number defined for the CGP port with medium priority on the on the Citrix XenApp server.

d) Click **Finished**.
The popup screen closes.

10. Assign a variable for the CGP port that is configured with low priority in the Multi-Port Policy on the Citrix XenApp server.

a) Click **Add new entry** and click the **change** link next to the new empty entry that displays.
b) In the **Custom Variable** field, type `citrix.msi_port.low`.
c) In the **Custom Expression** field, type `expr {"2601"}`.

Replace `2601` with the port number defined for the CGP port with low priority on the Citrix XenApp server.

d) Click **Finished**.
The popup screen closes.
e) Click **Save**.
The properties screen closes and the visual policy editor is displayed.

11. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.

Chapter 5

APM Integration with Oracle Access Manager

About integration with supported Oracle Access Manager versions

Access Policy Manager® can provide the same functionality as an Oracle 10g WebGate. Access Policy Manager native OAM integration is built on top of Oracle® 10g's latest Access Manager SDK. When you deploy Access Policy Manager with an OAM 10g or 11g server and OAM 10g WebGates, you no longer need to deploy a WebGate proxy or WebGate agent for each OAM-protected web application.

Access Policy Manager supports multiple WebGates and can function as an Authentication WebGate (when deployed with Oracle 10g server) as well as a Resource WebGate (when deployed with either Oracle 10g or 11g server).

Authentication WebGate (AWG)
The front-end agent of the OAM server that provides the interface of authentication and authorization for the user's access request to specific web resources.

Resource WebGate (RWG)
The front-end agent of protected web servers; the RWG validates the OAM session cookie (ObSSOCookie) to determine whether the user has been authenticated and can be authorized to access the requested web resources.

Although the Oracle 11g server is backward compatible with Oracle 10g WebGates, with Oracle 11g, Access Policy Manager acts in place of OAM 10g resource webgates, but cannot act as a authentication webgate. This is because a new architecture was introduced with OAM 11g in which the OAM 11g server becomes the central management point for everything including authentication, that is, the role of AWG. Refer to *Oracle® Fusion Middleware Administrator's Guide for Oracle Access Manager 11g* for a comparison of OAM 10g and 11g architectures.

Because the Oracle 11g server handles all user authentication requests, you should take steps to prevent and mitigate Layer 7 Denial of Server (DoS) and brute force attacks by installing a Web Application Firewall in front of the Oracle 11g server. BIG-IP® Application Security Manager® can provide you with intelligent Layer 7 protection in this case. For more information, refer to *Configuration Guide for BIG-IP® Application Security Manager®*.

How does native integration with OAM work?

You can achieve SSO functionality with OAM for HTTP/HTTPS requests passing through a virtual server to the web application. With OAM support enabled on a Local Traffic Manager® (LTM) virtual server, Access Policy Manager® will be the OAM policy enforcement point (PEP) on the BIG-IP® system, while the OAM server is still the policy decision point (PDP) in the overall system architecture. When a user requests access to a protected web resource, Access Policy Manager® communicates with the OAM server to determine whether the user can be authenticated/authorized for the request, and enforces the policy evaluation decision (made by OAM server) on the BIG-IP® device.

The figures that follow show a typical configuration before and after OAM native integration is enabled.

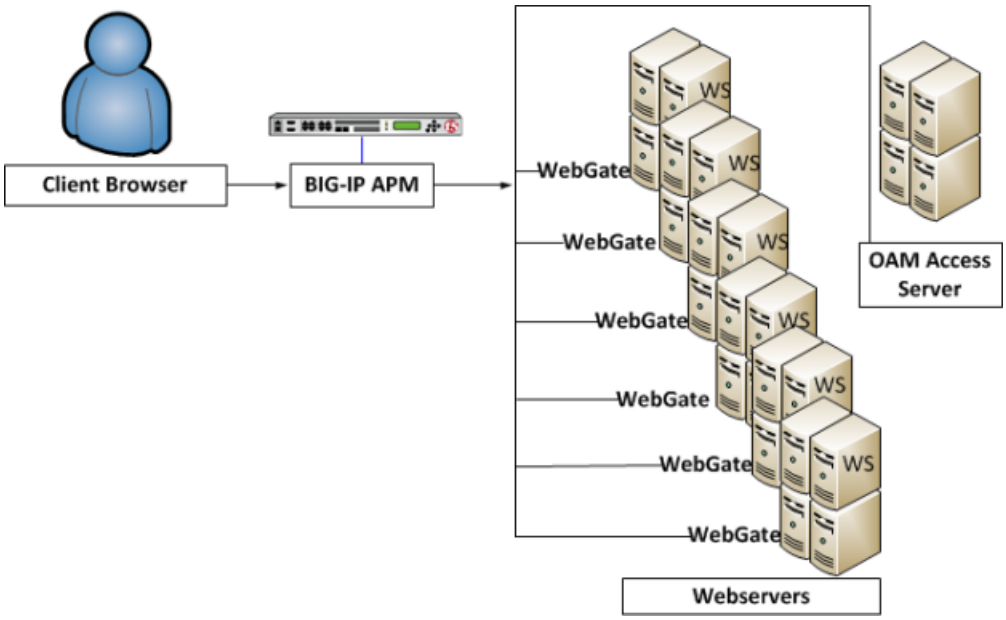


Figure 10: Typical configuration before OAM native integration is enabled on the BIG-IP system

In this figure individual WebGates, installed on each webserver, interact with the OAM Access Server.

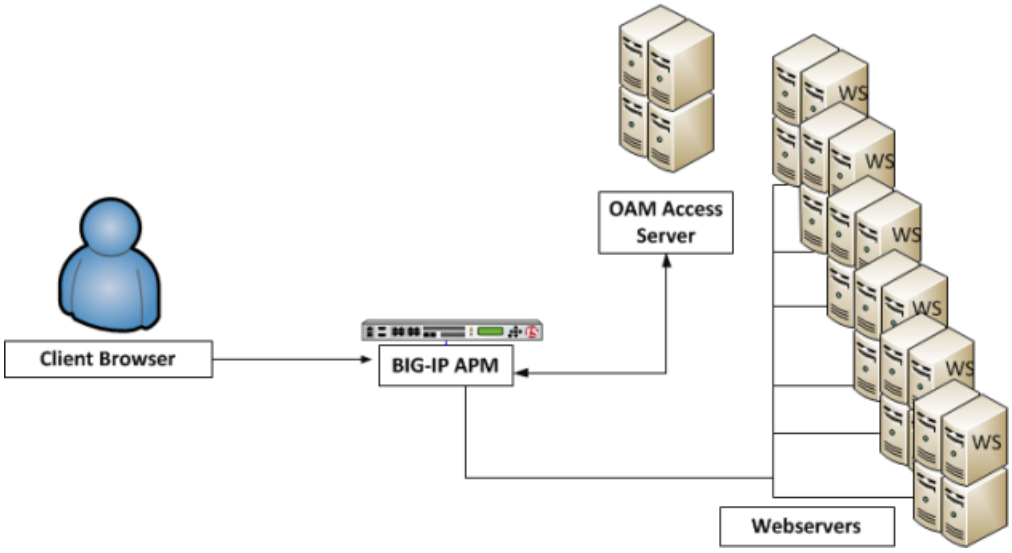


Figure 11: Typical configuration after OAM native integration is enabled on the BIG-IP system

In this figure WebGates are no longer required on the webservers, and, even if they are installed, they are not used. Access Policy Manager acts in place of the WebGates, contacting the OAM Access Server for policy information, and enforcing the policies.

OAM 11g SSO integration example

Let's walk through an example deployment with Oracle 11g. You can integrate Access Policy Manager® with a Oracle 11g server whether it is configured for single sign on (SSO) single domain or SSO multi-domain. To keep this example simple, we will assume that Oracle 11g server is configured for SSO

single domain. The Oracle 11g server performs all authentication. A single Resource WebGate is configured in OAM.

In Access Policy Manager on the BIG-IP® system, a AAA OAM server has been configured and includes the details of the OAM Access Server and one AccessGate. One virtual server has been configured with OAM native integration enabled. BIG-IP® Application Security Manager® (ASM) is installed in another virtual server as a web application firewall configured to prevent DoS and mitigate brute force attacks.

This figure depicts the traffic flow for the example.

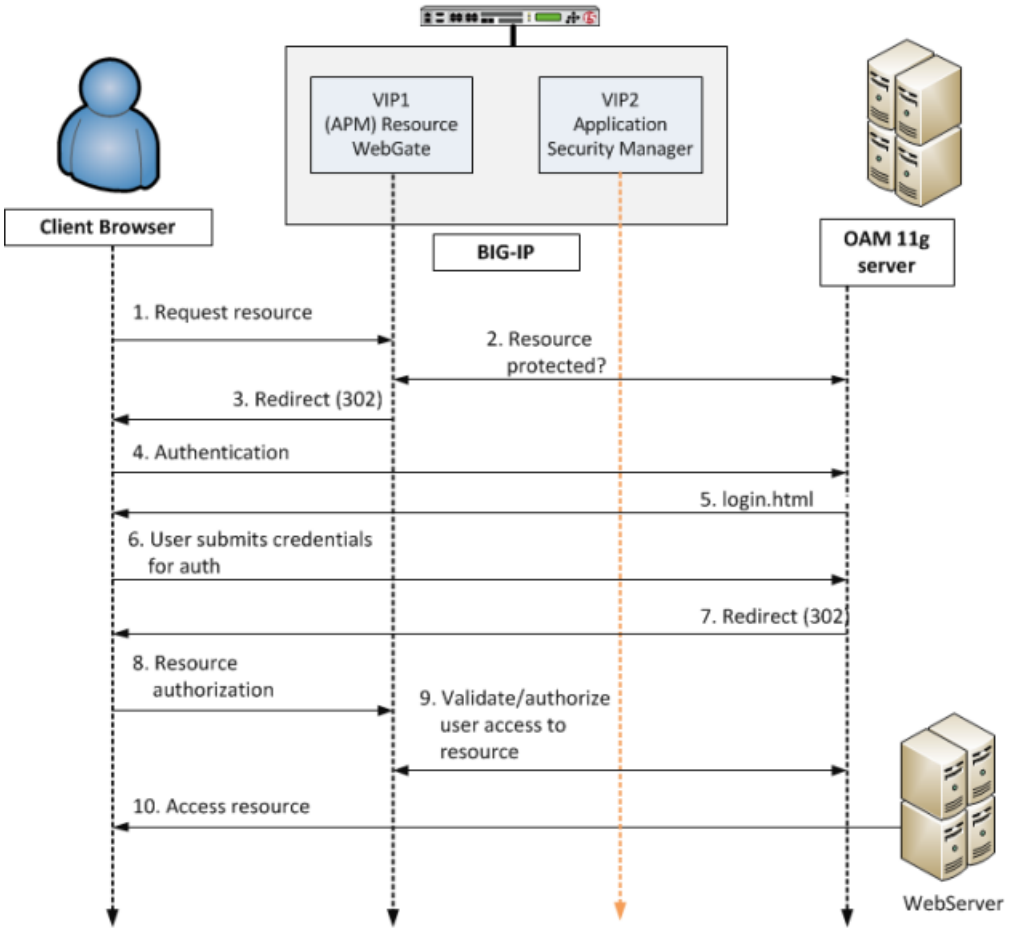


Figure 12: Accessing a protected resource using Access Policy Manager deployed with OAM 11g

1. Client requests access to a resource. The request comes to the Resource Webgate (RWG).
2. RWG checks whether the resource is protected per OAM. The resource is protected and the user has not yet authenticated.
3. RWG sends a 302 redirect to the client so that the client will be redirected to the OAM 11g server for authentication.
4. User will follow the redirect to OAM 11g server for authentication. In this example, the user has never been authenticated and form-based authentication is the authentication scheme of the OAM policy protecting the original user-requested resource.

Note: *Before going to OAM, traffic is checked against security policies that are configured with anomaly protection on ASM, provided that the ASM module is enabled to protect the OAM 11g server on the BIG-IP system.*

---

5. OAM sends a login page to the client.

6. User submits credentials which come to OAM server where the user's credentials will be validated. In this example, it is assumed that the user submitted valid credentials.
7. After user credentials are successfully validated on the OAM 11g server, the server will send another 302 redirect, so that the user will be redirected back to the original RWG.
8. Resource request comes to RWG.
9. RWG verifies the user's original request again using the `ObSSOCookie` passed from the OAM 11g server. Upon successful authorization, the user will be allowed to access the resource.
10. The protected resource behind VIP1 will be sent back to the user.

OAM 10g SSO integration example

Let's walk through an example deployment. An Oracle 10g server is configured for SSO multi-domain; an Authentication WebGate is configured and, in another domain, a Resource WebGate is configured.

In Access Policy Manager®, an AAA OAM server has been configured and includes the details of the OAM Access Server and the two AccessGates. Two virtual servers have been configured with OAM native integration enabled.

This figure depicts the traffic flow for the example.

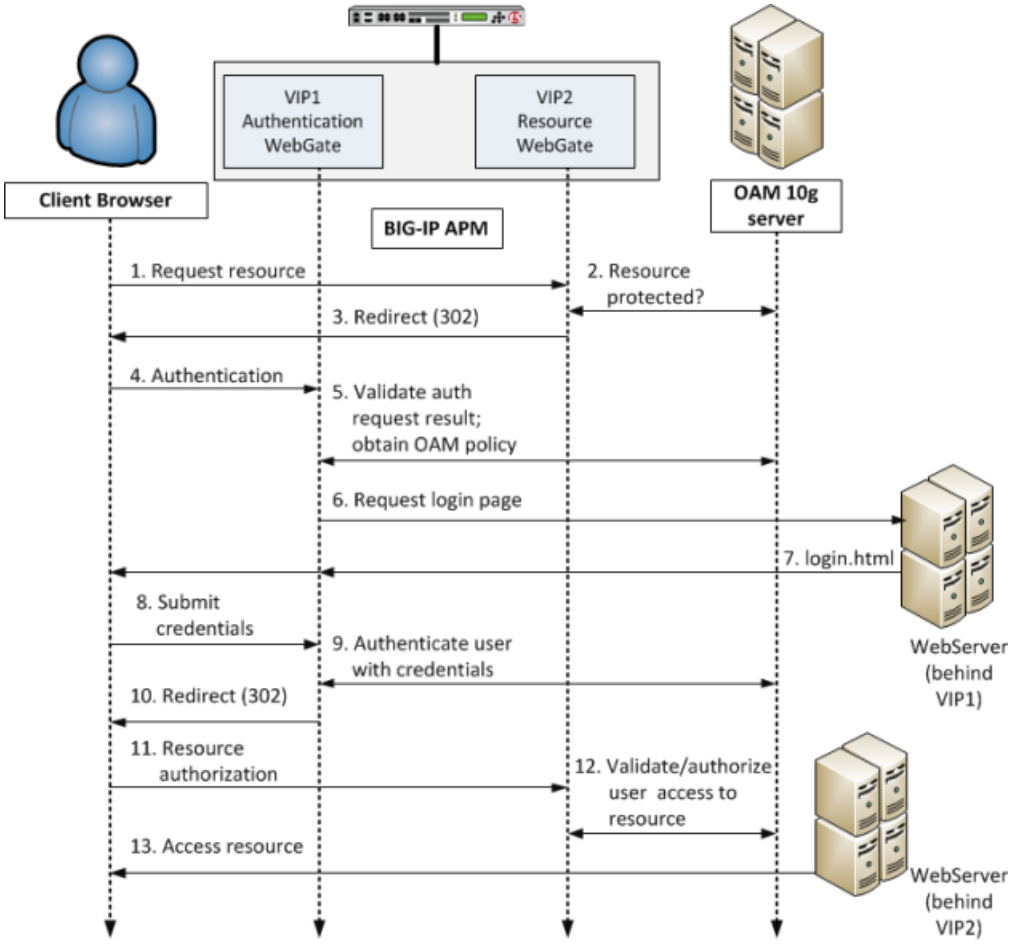


Figure 13: Accessing a protected resource via Access Policy Manager native integration with OAM 10g

1. Client requests access to a resource. The request comes to the RWG (Access Policy Manager AccessGate at VIP2).
2. RWG checks whether the resource is protected per OAM. The resource is protected and the user has not yet authenticated.
3. RWG sends a 302 redirect to the client so that the client will be redirected to the AWG for authentication.
4. Authentication request comes to the AWG (Access Policy Manager AccessGate at VIP1).
5. AWG validates user authentication status with OAM and obtains policy. In this case, the policy calls for form-based authentication and gives the location of the form.
6. For the form-based authentication scheme, AWG allows the user to access the login page hosted on a webserver behind the AWG.
7. The webserver returns the login.html file to the AWG, which sends it to the client.
8. Via login.html, the user submits credentials.
9. The AWG uses the credentials to authenticate the user with the OAM 10g server.
10. With user authentication successful, the AWG sends a 302 redirect to the client so that the client will be redirected to the original RWG.
11. Request for resource comes to the RWG again.
12. The RWG validates user access to the resource with OAM.
13. The protected resource behind VIP2 will be sent back to the user.

Chapter 6

Integrating APM with Oracle Access Manager

About AAA OAM server configuration

You can configure only one AAA OAM server, but it can support multiple AccessGates from the same access server. When you create a AAA OAM server, its transport security mode must match the setting in the OAM access server.

Task summary for integrating Access Policy Manager with OAM

Before you begin

Before you start to integrate Access Policy Manager® with OAM, configure the Access Server and AccessGates through the Oracle Access administrative user interface. Refer to *Oracle® Access Manager Access Administration Guide* for steps.

Task list

Follow these steps to integrate Access Policy Manager with a supported OAM server.

Importing AccessGate files when transport security is set to cert
Creating an AAA OAM server
Adding AccessGates to the OAM AAA server
Creating a virtual server

Importing AccessGate files when transport security is set to cert

Check the transport security mode that is configured on the OAM access server. If transport security mode is configured to cert, copy the certificate,certificate chain, and key files (by default, `aaa_cert.pem`, `aaa_chain.pem`, and `aaa_key.pem` respectively) for each AccessGate from the OAM access server to the BIG-IP system.

Note: *If Transport Security Mode is set to open or simple, you can skip this procedure.*

You must import the certificate, certificate chain, and key files for each AccessGate into the BIG-IP system. Repeat this procedure for each AccessGate. Import certificate and certificate chain files before importing the corresponding private key file.

Note: *If a signing chain certificate (CA) is the subordinate of another Certificate Authority, both certificates, in PEM format, must be included in the file with the subordinate signer CA first, followed by the root CA, including " -----BEGIN/END CERTIFICATE-----".*

---

1. On the Main tab, click **Local Traffic** > **SSL Certificate List**.
   The SSL Certificate List screen opens.
2. From the **Import Type** list, select **Certificate**.
3. For the **Certificate Name** setting, select the **Create New** option, and type a unique name that enables you to identify the file as belonging to this particular AccessGate.
4. For the **Certificate Source** setting, select the **Upload File** option, and browse to the location of the certificate or the certificate chain file.

If you kept the default filenames when you copied the files to the BIG-IP system, look for `aaa_cert.pem` or `aaa_chain.pem`.

5. Click **Import**.
   A certificate or certificate chain file has been imported for the AccessGate. To import the other (certificate or certificate chain) file for this AccessGate, repeat the steps that you have just completed before you continue.
6. On the Main tab, click **Local Traffic** > **SSL Certificate List**.
   The SSL Certificate List screen opens.
7. From the **Import Type** list, select **Key**.
8. For the **Key Name** setting, select the **Create New** option, and type a unique name that enables you to identify the file as belonging to this particular AccessGate.

   When you import the key file, you are importing the private key that corresponds to the already imported certificate and certificate chain while renaming the file from its default name `aaa_key.pem`.
9. For the **Key Source** setting, do one of the following:
   - Select the **Upload File** option, and browse to the location of the key file.
   - Select the **Paste Text** option, and paste the key text copied from another source.
10. Click **Import**.
    The key file is imported.

Certificate, certificate chain, and key files have been imported for an AccessGate.

Repeat the procedure to import these files for any other AccessGate.

Creating an AAA OAM server

If transport security mode is configured to cert on the access server, import the certificates, keys, and CA certificate for the AccessGates into the BIG-IP system.

Create a AAA server for OAM to deploy Access Policy Manager® in place of OAM 10g WebGates.

Note: *Only one OAM server per BIG-IP system is supported. Multiple OAM 10g webgates from the same OAM server are supported.*

---

1. In the navigation pane, click **Access Policy** > **AAA Servers** > **Oracle Access Manager**.
   The Oracle Access Manager Server screen opens.
2. Click **Create** if no Oracle Access Manager server is defined yet,.
   The New OAM Server screen opens.
3. Type a name for the AAA OAM server.
4. For **Access Server Name**, type the name that was configured in Oracle Access System for the access server.

   For the access server name, open the OAM Access System Console and select **Access system configuration** > **Access Server Configuration**.
5. For **Access Server Hostname**, type the fully qualified DNS host name for the access server system.
6. For **Access Server Port**, accept the default 6021, or type the port number.
7. For **Admin Id**, type the admin ID.

   Admin Id and Admin Password are the credentials that are used to retrieve host identifier information from OAM. Usually, these are the credentials for the administrator account of both Oracle Access Manager and Oracle Identity Manager.

8. For **Admin Password**, type the admin password.
9. For **Retry Count**, accept the default 0, or enter the number of times an AccessGate should attempt to contact the access server.
10. For **Transport Security Mode**, select the mode (open, simple, or cert) that is configured for the access server in Oracle Access System.
11. If Transport Security Mode is set to simple, type and re-type a **Global Access Protocol Passphrase**; it must match the global passphrase that is configured for the access server in OAM.
12. For **AccessGate Name**, type the name of an AccessGate; it must match the name of an AccessGate that is configured on the OAM access server.
13. For **AccessGate Password** and **Verify Password**, type the password; it must match the password that is configured for it on the OAM access server.
14. If transport security mode is set to cert, select the **Certificate**, **Key**, and **CA Certificate** that you imported for this particular AccessGate.
15. If transport security mode is set to cert and if a sign key passphrase is needed, type a **Sign Key Passphrase** and re-type it to verify it.
16. Click the **Finished** button.
    This adds the new AAA server to the AAA Servers list.

Add any other AccessGates that are configured for the OAM access server to this Oracle Access Manager AAA server. Then, for each AccessGate, configure a virtual server and enable OAM support on it for native integration with OAM.

Adding AccessGates to the OAM AAA server

You must create an Oracle Access Manager AAA server with one AccessGate before you can add other AccessGates.

Access Policy Manager can support multiple AccessGates from the same OAM access server. To enable the support, add the AccessGates to the Oracle Access Manager AAA server.

1. In the navigation pane, click **Access Policy** > **AAA Servers** > **Oracle Access Manager**.
   The Oracle Access Manager Server screen opens.
2. Click the name of the Oracle Access Manager AAA server.
   The Properties page opens.
3. Scroll down to the **AccessGate List** and click **Add**.
   The New AccessGate page opens.
4. For **AccessGate Name**, type the name of an AccessGate; it must match the name of an AccessGate that is configured on the OAM access server.
5. For **AccessGate Password** and **Verify Password**, type the password; it must match the password that is configured for it on the OAM access server.
6. If transport security mode is set to cert for the access server, select the **Certificate**,**Key**, and **CA Certificate** that you imported for this particular AccessGate.
7. If transport security mode is set to cert for the access server, and if a sign key passphrase is needed, type a **Sign Key Passphrase** and re-type it to verify it.
8. Click the **Finished** button.

The AccessGate is added.

Creating a virtual server

Configure an AAA OAM server and add AccessGates to it before you perform this task.

A virtual server represents a destination IP address for application traffic. Configure one virtual server for each AccessGate that is included on the AAA OAM server AccessGates list.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. For the **Destination** setting, in the **Address** field, type the IP address you want to use for the virtual server.

   The IP address you type must be available and not in the loopback network.
4. In the **Service Port** field, type a port number or select a service name from the **Service Port** list.
5. In the Resources area of the screen, from the **Default Pool** list, select a pool name.
6. Scroll down to the Access Policy section and check the **Enabled** box for OAM Support.
7. Select an AccessGate from the list.

   If you select `Default`, Access Policy Manager reads Oracle configuration information to determine which AccessGate to associate with this virtual server.
8. Click **Finished**.

A destination IP address on the Access Policy Manager® system is now available for application traffic.

Troubleshooting tips

You might run into problems with the integration of Access Policy Manager® and OAM in some instances. Follow these tips to try to resolve any issues you might encounter.

Troubleshooting tips for initial configuration

You should	Steps to take
Check network connectivity	Ping the OAM Access Server from the BIG-IP system.
Test without OAM support enabled first	Before you test with OAM support enabled, make sure that the BIG-IP system has basic connectivity to protected applications. • Disable the OAM Support property on the virtual server. • Verify that you can reach the pool and the application. After succeeding, reenable OAM support on the virtual server.
Check the configuration for accuracy	• Confirm that the AAA server object is correct, particularly the OAM server section. • Confirm that the AccessGates configured on the BIG-IP system within the AAA server are correct.

Additional troubleshooting tips

You should	Steps to take
Verify access	OAM provides tools for the administrator to test how access policies respond to various requests. Use the Access Tester to test access policies with given identities and for given users. This tool can be helpful in determining whether the access provided by BIG-IP system is consistent with the policies configured under OAM.
Resolve sudden problems	Changes that have been made on the OAM server can cause mismatches on the BIG-IP system due to a configuration cache that is kept on the BIG-IP system. To resolve this problem, delete the cache configuration file of the corresponding AccessGate configuration. • Delete the config.cache file located in config/aaa/oam/<filepath>, e.g. /config/aaa/oam/Common/oamaaa1/AccessGate1/config.cache. • At the command line, restart the EAM service by typing `bigstart restart eam`.
Check logs	Enable and review the log files on the BIG-IP system. • Most relevant log items are kept in the /var/log/apm log file. This /var/log/apm log file is the primary location for messages related to the operation of OAM. • Additional logging is done in /var/log/oblog.log. This file contains AccessGate logging which might be helpful in certain circumstances.

Using OAM authentication in an access policy

Before you start this procedure, Access Server and AccessGates must be configured through the Oracle Access administrative user interface. An Access Policy Manager® AAA OAM server and a virtual server must be configured on the BIG-IP® system.

Configure OAM authentication in an access policy only if you need to provide a client with SSL VPN access, authenticating with an Oracle server that is configured for single sign on single domain use. This approach does not work for Oracle single sign on multi-domain configurations.

Note: *You do not need an access policy to use Access Policy Manager as an OAM 10g Webgate.*

Tip: *In this procedure, you create a new access profile as part of the configuration. Alternatively, you can edit an existing access profile and add OAM authentication to the access policy.*

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click **Create**.
   The New Profile screen opens.
3. In the **Name** field, type a name for the access profile.
4. Click **Finished**.
5. Click the name of the access profile for which you want to edit the access policy.
   The properties screen opens for the profile you want to edit.
6. Click **Edit Access Policy for Profile *profile_name***.
   The visual policy editor opens the access policy in a separate screen.

7. Click the **(+)** icon anywhere in the access policy to add a new action item.
   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
8. Select **OAM**, and click **Add item**.
9. For Server, select the AAA OAM server from the list.
10. For URL, type in a URL resource.
11. For Agent Action, select either Authentication and Authorization or Authentication Only.
12. Click **Save**.
    You will return to the visual policy editor.
13. Click **Apply Access Policy** to save your configuration.

The access policy associated with the AAA OAM server uses OAM authentication.

Chapter 7

VMware Horizon View Requirements for APM Integration

About VMware Horizon View server required settings

To integrate Access Policy Manager® with VMware Horizon View, you must meet specific configuration requirements for VMware, as described here.

SecureTunnel and PCoIP Secure Gateway disabled

Ensure that Secure Tunnel and PCoIP Secure Gateway are disabled on the VMware Horizon View server.

Advanced authentication disabled

Ensure that RSA authentication and other advanced authentication types are disabled on the VMware Horizon View server.

About VMware Horizon View server settings and SSL offloading

If you want to use Access Policy Manager® (APM®) to offload SSL from VMware View Horizon servers, you must configure your VMware View Horizon servers for SSL offloading. For more information, refer to the administration guide for your VMware Horizon View server and search for Off-load SSL Connections.

Note: *APM supports SSL offloading. However, it is not a requirement for integrating APM with VMware.*

Chapter 8

Authenticating Standalone View Clients with APM

Overview: Authenticating View Clients with APM

Access Policy Manager® can present VMware View logon pages on a View Client, perform authentication, and load-balance VMware View Connection Servers. APM™ supports the PCoIP (PC over IP) display protocol for the virtual desktop.

A View Client makes connections to support different types of traffic between it and a View Connection Server. APM supports these connections with two virtual servers that share the same destination IP address. You must configure one virtual server to serve each of these purposes:

- View Client authentication and View Connection Server load-balancing
- Handle PCoIP traffic

Task summary

Creating a pool of View Connection Servers
Configuring a VMware View remote desktop resource
Configuring a full webtop
Creating an access profile
Creating an access policy for View Client authentication
Creating a connectivity profile
Creating a custom server SSL profile
Verifying the certificate on a View Connection Server
Configuring an HTTPS virtual server for View Client authentication
Configuring a UDP virtual server for PCoIP traffic
Configuring virtual servers that use a private IP address

Creating a pool of View Connection Servers

You create a pool of View Connection Servers to provide load-balancing and high-availability functions.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. In the Resources area, using the **New Members** setting, add each View Connection Server that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
   b) In the **Service Port** field, type `443` (if your View Connection Servers use HTTPS), or type `80` (if your View Connection Servers use HTTP).
      By default, View Connection Servers use HTTPS. However, if you configure your View Connection Servers for SSL offloading, they use HTTP.
   c) Click **Add**.
5. Click **Finished**.

The new pool appears in the Pools list.

Configuring a VMware View remote desktop resource

Configure a VMware View remote desktop resource so that you can log on to a View Connection Server and gain access to a standalone View Client, or launch a View desktop from an APM® webtop, depending on the access policy.

1. On the Main tab, click **Access Policy** > **Application Access** > **Remote Desktops**.
   The Remote Desktops list opens.
2. Click **Create**.
   The New Resource screen opens.
3. For the **Type** setting, select **VMware View**.
4. For the **Destination** setting, select **Pool** and from the **Pool Name** list, select a pool of View Connection Servers that you configured previously.
5. For the **Server Side SSL** setting:
   - Select the **Enable** check box if your View Connection Servers use HTTPS (default).
   - Clear the **Enable** check box if your View Connection Servers use HTTP; that is, they are configured for SSL offloading.
6. In the Auto Logon area, select the **Enable** check box, so that a user can automatically log on to a View Connection Server after logging in to APM®.
   If you enable auto logon, you must also configure credential sources.
   a) In the **Username Source** field, accept the default or type the session variable to use as the source for the auto logon user name.
   b) In the **Password Source** field, accept the default or type the session variable to use as the source for the auto logon user password.
   c) In the **Domain Source** field, accept the default or type the session variable to use as the source for the auto logon user domain.
7. In the Customization Settings for *language_name* area, type a **Caption**.
   The caption is the display name of the VMware View resource on the APM full webtop.
8. Click **Finished**.
   All other parameters are optional.

This creates the VMware View remote desktop resource. To use it, you must assign it along with a full webtop in an access policy.

Configuring a full webtop

You can use a full webtop to provide web-based access to VMware View and other resources.

1. On the Main tab, click **Access Policy** > **Webtops**.
   The Webtops screen opens.
2. Click **Create**.
   The New Webtop screen opens.
3. Type a name for the webtop.
4. From the **Type** list, select **Full**.
   The Configuration area displays with additional settings configured at default values.
5. Click **Finished**.

The webtop is now configured and appears in the webtop list.

Creating an access profile

You create an access profile to provide the access policy configuration for a virtual server that establishes a secured session.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click **Create**.
   The New Profile screen opens.
3. Type a name for the access profile.
4. From the **Profile Type** list, select one:
   - **APM-LTM** - Select for a web access management configuration.
   - **SSO** - Select only when you do not need to configure an access policy.
   - **SWG - Explicit** - Select to configure access using Secure Web Gateway explicit forward proxy.
   - **SWG - Transparent** - Select to configure access using Secure Web Gateway transparent forward proxy.
   - **SSL-VPN** - Select for other types of access, such as network access, portal access, application access. (Most access policy items are available for this type.)
   - **ALL** - Select for any type of access.

   Additional settings display.
5. In the Language Settings area, add and remove accepted languages, and set the default language.
   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
6. Click **Finished**.

This creates an access profile with a default access policy.

Creating an access policy for View Client authentication

Before you can create this access policy, configure the AAA server (or servers) to use for authentication.

Note: *The View Client supports authentication with Active Directory domain credentials (required) and with an RSA SecureID PIN (optional). To use both types of authentication, place the Active Directory logon and authentication actions after the RSA logon and authentication actions.*

Create an access policy so that a View Client can use a View desktop after logging on and authenticating with Access Policy Manager® (APM®).

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new action item.
   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
4. Type `client` in the search field, select **Client Type** from the results list, and click **Add Item**.

The Client Type action identifies clients and enables branching based on the client type.

A properties screen opens.

5. Click **Save**.
   The properties screen closes. The visual policy editor displays the Client Type action. A VMware View branch follows it. Add the remaining actions on the VMware View branch.
6. Configure logon and authentication actions for Active Directory:

   Active Directory authentication is required.

   a) Click the (+) sign on the VMware View branch. An Add Item screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on
   b) On the Logon tab, select **VMware View Logon Page**, and click **Add Item**.

      A properties screen displays.

   c) From the **VMware View Logon Screen Type** list, retain the default setting **Windows Password**.
   d) In the **VMware View Windows Domains** field, type domain names separated by spaces to use for Active Directory authentication.

      Type at least one domain name. These domains names are displayed on the View Client.

   e) Click **Save**.
      The properties screen closes and the visual policy editor is displayed.
   f) Click the plus (+) icon after the previous VMware View Logon Page action.
      A popup screen opens.
   g) On the **Authentication** tab, select **AD Auth**, and click **Add Item**.
   h) From the **Server** list, select an AAA server and click **Save**.
      The properties screen closes.

7. Assign a full webtop and the VMware View remote desktop resource that you configured previously.

   a) Click the (+) sign after the previous action.
   b) Type **adv** in the search field, select **Advanced Resource Assignment** from the results, and click **Add Item**.

      A properties screen displays.

   c) Click **Add new entry**
      A new line is added to the list of entries.
   d) Click the **Add/Delete** link below the entry.
      The screen changes to display resources on multiple tabs.
   e) On the Remote Desktop tab, select the VMware View remote desktop resource that you configured previously.
   f) On the Webtop tab, select a full webtop and click **Update**.
      The properties screen closes and the resources you selected are displayed.
   g) Click **Save**.
      The properties screen closes and the visual policy editor is displayed.

8. To use RSA SecurID authentication in addition to Active Directory authentication, insert logon and authentication actions for RSA SecurID ahead of those for Active Directory:

   a) Click the (+) sign before the previous VMware View Logon Page action.
      A popup screen opens.
   b) On the Logon tab, select **VMware View Logon Page**, and click **Add Item**.

      A properties screen displays.

   c) From the **VMware View Logon Screen Type** list, select **RSA SecurID**.
   d) In the **VMware View Windows Domains** field, type the domain names to use for logon.
   e) Click **Save**.
      The properties screen closes and the visual policy editor is displayed.

f) Click the plus (+) icon after the previous VMware View Logon Page action.
A popup screen opens.
g) On the **Authentication** tab, select **RSA SecurID**, and click **Add Item**.
h) From the **Server** list, select the AAA server that you created previously and click **Save**.
The properties screen closes.

9. (Optional) If you want to display a message to the user inside of the View Client (for example, a disclaimer or acceptable terms of use), this is how you do it:
a) Click the **(+)** icon anywhere in your access profile to add a new action item.
An popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
b) On the Logon tab, select **VMware View Logon Page**, and click **Add Item**.
A properties screen displays.
c) From **VMware View Logon Screen Type**, select **Disclaimer**
d) In the Customization area from the **Language** list, select the language for the message.
e) In the **Disclaimer message** field, type the message to display on the logon page.
f) Click **Save**.
The properties screen closes and the visual policy editor is displayed.

You have configured a logon page that displays a logon page with a message on a View Client.

10. On the fallback branch between the last action and **Deny**, select the **Deny** check box, click **Allow**, and click **Save**.

11. Click **Apply Access Policy**.

You have an access policy that displays at least one logon page, and authenticates a View Client against Active Directory before assigning resources to the session; and at most, displays three logon pages and performs two-factor authentication before assigning resources to the session.

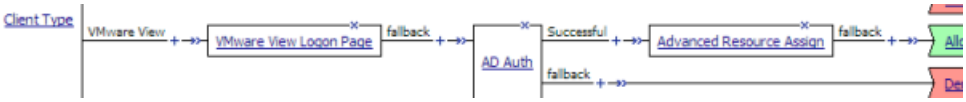


Figure 14: Example access policy with single-factor authentication for View Client

Figure 15: Example access policy with two-factor authentication for View Client

For the access policy to take effect, you must add it to a virtual server.

Creating a connectivity profile

You create a connectivity profile to configure client connections.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
A list of connectivity profiles displays.

2. Click **Add**.
The Create New Connectivity Profile popup screen opens and displays General Settings.

3. Type a **Profile Name** for the connectivity profile.
4. Select a **Parent Profile** from the list.
   APM® provides a default profile, **connectivity**.
5. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

The connectivity profile appears in the list.

To provide functionality with a connectivity profile, you must add the connectivity profile to a virtual server.

Creating a custom server SSL profile

With a server SSL profile, the BIG-IP® system can perform decryption and encryption for server-side SSL traffic.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Server**.
   The SSL Server profile list screen opens.
2. Click **Create**.
   The New Server SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the Parent Profile list, select **serverssl**.
5. In the Configuration area, select **Advanced** and select the **Custom** check box.
   Additional settings display. All settings in the Configuration area become available.
6. Scroll down to the **Server Name** field and type `pcoip-default-sni`.
7. Click **Finished**.

The custom server SSL profile is listed in the SSL Server list.

Verifying the certificate on a View Connection Server

Before you start, obtain the CA certificate that was used to sign the SSL certificate on View Connection Servers and obtain a Certificate Revocation List (CRL).

You install the CA certificate and CRL, then update the server SSL profile to use them only if you want the BIG-IP system to check the validity of the certificate on the View Connection Server.

1. On the Main tab, click **System** > **File Management** > **SSL Certificate List**.
   The SSL Certificate List screen opens.
2. Click **Import**.
3. From the **Import Type** list, select **Certificate**.
4. For the **Certificate Name** setting, do one of the following:
   - Select the **Create New** option, and type a unique name in the field.
   - Select the **Overwrite Existing** option, and select a certificate name from the list.
5. For the **Certificate Source** setting, select **Upload File** and browse to select the certificate signed by the CA server.
6. Click **Import**.
   The SSL Certificate List screen displays. The certificate is installed.
7. Click **Import**.

8. From **Import Type** list, select **Certificate Revocation List**.
9. For **Certificate Revocation List Name**, type a name.
10. For **Certificate Revocation List Source**, select **Upload File** and browse to select the CRL you obtained earlier.
11. Click **Import**.
    The SSL Certificate List screen displays. The CRL is installed.
12. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Server**.
    The SSL Server profile list screen opens.
13. Click the name of the server SSL profile you created previously.
    The Properties screen displays.
14. Scroll down to the Server Authentication area.
15. From the **Server Certificate** list, select **require**.
16. From the **Trusted Certificate Authorities** list, select the name of the certificate you installed previously.
17. From the **Certificate Revocation List (CRL)** list, select the name of the CRL you installed previously.
18. Click **Update**.

The BIG-IP system is configured to check the validity of the certificate on the View Connection Server.

Overview: Accessing a View Desktop from an APM webtop
Creating a custom server SSL profile
Configuring an HTTPS virtual server for a dynamic webtop

Configuring an HTTPS virtual server for View Client authentication

Before you start this task, create a connectivity profile in Access Policy Manager®. (Default settings are acceptable.)

Create this virtual server to support View Client authentication. This is the virtual server that users will specify in the View Client.

Note: *This is one of two virtual servers that you must configure for View Client connections. Use the same destination IP address for each one.*

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, select **Host** and in the **Address** field, type the IP address for the virtual server.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **HTTP Profile** list, select **http**.
7. For the **SSL Profile (Client)** setting, in the **Available** box, select a profile name, and using the Move button, move the name to the **Selected** box.
8. For the **SSL Profile (Server)** setting, from the **Available** list, select the name of the Server SSL profile you previously created, and using the Move button, move the name to the **Selected** list.
9. From the **Source Address Translation** list, select **Auto Map**.
10. In the Access Policy area, from the **Access Profile** list, select the access profile.
11. From the **Connectivity Profile** list, select the connectivity profile.

12. Select the **VDI & Java Support** check box.
13. Locate the Resources area of the screen and from the **Default Persistence Profile** list, select one of these profiles:
    - **cookie** - This is the default cookie persistence profile. Cookie persistence is recommended.
    - **source_addr** - This is the default source address translation persistence profile. Select it only when the cookie persistence type is not available.
14. Click **Finished**.

A virtual server handles View Client access and handles XML protocol data.

Configuring a UDP virtual server for PCoIP traffic

Create this virtual server to support a PC over IP (PCoIP) data channel for View Client traffic.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, select **Host** and in the **Address** field, type the IP address for the virtual server.

   Type the same IP address as the one for the View Client authentication virtual server.
5. In the **Service Port** field, type `4172`.
6. From the **Protocol** list, select **UDP**.
7. From the **Source Address Translation** list, select **Auto Map**.
8. From the Access Policy area, select the **VDI & Java Support** check box.
9. Click **Finished**.

This virtual server is configured to support PCoIP transport protocol traffic for VMware View Clients.

Configuring virtual servers that use a private IP address

If you configured the HTTPS and UDP virtual servers with a private IP address that is not reachable from the Internet, but instead a publicly available device (typically a firewall or a router) performs NAT for it, you need to perform these steps.

You update the access policy by assigning the variable *`view.proxy_addr`* to the IP address that the client uses to reach the virtual server. Otherwise, a View Client cannot connect when the virtual servers have a private IP address.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new action item.
   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
4. Type `var` in the search field, select **Variable Assign** from the results list, and click **Add Item**.

The Variable Assign properties screen opens.

5. Click the **change** link next to the empty entry.
   A popup screen displays two panes, with Custom Variable selected on the left and Custom Expression selected on the right.
6. In the Custom Variable field, type `view.proxy_addr`.
7. In the Custom Expression field, type `expr {"proxy address"}` where proxy address is the IP address that the client uses to reach the virtual server.
8. Click **Finished** to save the variable and expression and return to the Variable Assign action popup screen.
9. Click **Save**.
   The properties screen closes and the visual policy editor displays.
10. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.

Chapter 9

Presenting a View Desktop on an APM Webtop

Overview: Accessing a View Desktop from an APM webtop

In this implementation, you integrate Access Policy Manager® (APM®) with View Connection Servers and present View Desktops on an APM dynamic webtop. APM authenticates to a View Connection Server and renders the View Desktops. APM load balances the View Connection Servers for high availability.

APM supports the necessary connections with two virtual servers that share the same destination IP address.

Task summary

Creating a pool of View Connection Servers
Configuring a VMware View remote desktop resource
Configuring a full webtop
Creating an access profile
Creating an access policy for a dynamic webtop
Assigning resources to the access policy
Creating a connectivity profile
Creating a custom server SSL profile
Verifying the certificate on a View Connection Server
Configuring an HTTPS virtual server for a dynamic webtop
Configuring a UDP virtual server for PCoIP traffic
Configuring virtual servers that use a private IP address

About client requirements to launch View Client from a webtop

If you want to use Access Policy Manager® (APM®) to launch a View Client from an APM webtop, you must install the standalone View Client on your client. The standalone View Client is available from VMware.

Creating a pool of View Connection Servers

You create a pool of View Connection Servers to provide load-balancing and high-availability functions.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. In the Resources area, using the **New Members** setting, add each View Connection Server that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
   b) In the **Service Port** field, type `443` (if your View Connection Servers use HTTPS), or type `80` (if your View Connection Servers use HTTP).
      By default, View Connection Servers use HTTPS. However, if you configure your View Connection Servers for SSL offloading, they use HTTP.
   c) Click **Add**.
5. Click **Finished**.

The new pool appears in the Pools list.

Configuring a VMware View remote desktop resource

Configure a VMware View remote desktop resource so that you can log on to a View Connection Server and gain access to a standalone View Client, or launch a View desktop from an APM® webtop, depending on the access policy.

1. On the Main tab, click **Access Policy** > **Application Access** > **Remote Desktops**.
   The Remote Desktops list opens.
2. Click **Create**.
   The New Resource screen opens.
3. For the **Type** setting, select **VMware View**.
4. For the **Destination** setting, select **Pool** and from the **Pool Name** list, select a pool of View Connection Servers that you configured previously.
5. For the **Server Side SSL** setting:
   - Select the **Enable** check box if your View Connection Servers use HTTPS (default).
   - Clear the **Enable** check box if your View Connection Servers use HTTP; that is, they are configured for SSL offloading.
6. In the Auto Logon area, select the **Enable** check box, so that a user can automatically log on to a View Connection Server after logging in to APM®.

   If you enable auto logon, you must also configure credential sources.
   a) In the **Username Source** field, accept the default or type the session variable to use as the source for the auto logon user name.
   b) In the **Password Source** field, accept the default or type the session variable to use as the source for the auto logon user password.
   c) In the **Domain Source** field, accept the default or type the session variable to use as the source for the auto logon user domain.
7. In the Customization Settings for *language_name* area, type a **Caption**.

   The caption is the display name of the VMware View resource on the APM full webtop.
8. Click **Finished**.

   All other parameters are optional.

This creates the VMware View remote desktop resource. To use it, you must assign it along with a full webtop in an access policy.

Configuring a full webtop

You can use a full webtop to provide web-based access to VMware View and other resources.

1. On the Main tab, click **Access Policy** > **Webtops**.
   The Webtops screen opens.
2. Click **Create**.
   The New Webtop screen opens.
3. Type a name for the webtop.
4. From the **Type** list, select **Full**.

The Configuration area displays with additional settings configured at default values.

5. Click **Finished**.

The webtop is now configured and appears in the webtop list.

Creating an access profile

You create an access profile to provide the access policy configuration for a virtual server that establishes a secured session.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click **Create**.
   The New Profile screen opens.
3. Type a name for the access profile.
4. From the **Profile Type** list, select one:
   - **APM-LTM** - Select for a web access management configuration.
   - **SSO** - Select only when you do not need to configure an access policy.
   - **SWG - Explicit** - Select to configure access using Secure Web Gateway explicit forward proxy.
   - **SWG - Transparent** - Select to configure access using Secure Web Gateway transparent forward proxy.
   - **SSL-VPN** - Select for other types of access, such as network access, portal access, application access. (Most access policy items are available for this type.)
   - **ALL** - Select for any type of access.

   Additional settings display.
5. In the Language Settings area, add and remove accepted languages, and set the default language.
   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
6. Click **Finished**.

This creates an access profile with a default access policy.

Creating an access policy for a dynamic webtop

Before you can create an access policy for an Access Policy Manager® (APM®) dynamic webtop, you must configure AAA server objects in APM to use for authentication. (You can use any type of authentication.)

Note: *An Active Directory AAA server must include the IP address of the domain controller and the FQDN of the Windows domain name. If anonymous binding to Active Directory is not allowed in your environment, you must provide the admin name and password for the Active Directory AAA server.*

Configure an access policy to authenticate a user and enable APM dynamic webtop.

Note: *This example access policy shows how to use RSA SecurID and Active Directory authentication. However, you can use any type of authentication.*

---

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.

2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new action item.
   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
4. From the Logon Page tab, select **Logon Page**, and click **Add Item**.

   A properties screen displays.
5. Configure the Logon Page properties.

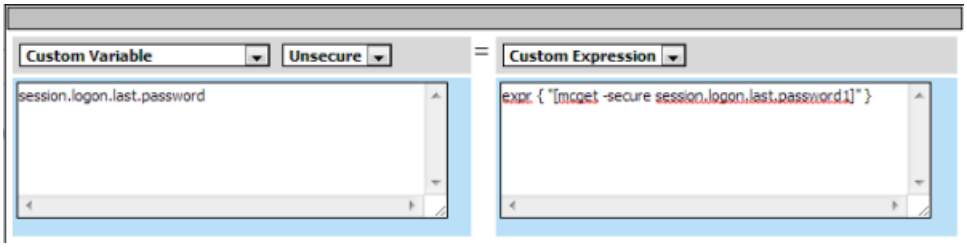
   To support Active Directory authentication only, no changes are required. To support both Active Directory and RSA SecurID authentication, an additional password field is required and the labels for the password fields require change.
   a) In the Logon Page Agent table row 3, for **Type**, select **password**.
   b) In the **Post Variable Name** field, type `password1`.
   c) In the **Session Variable Name** field, type `password1`.
   d) In the Customization Area in **Logon Page Input Field #2**, type `RSA Tokencode`.

      RSA Tokencode replaces the default label, Password.
   e) In the Customization Area in **Logon Page Input Field #3**, type `AD Password`.
   f) Click **Save**.

   The properties screen closes.

   The Logon Page is configured to display Username, RSA Tokencode, and AD Password. **Logon Page Input Field #2** accepts the RSA Tokencode into the *`session.logon.last.password`* variable (from which authentication agents read it). **Logon Page Input Field #3** saves the AD password into the *`session.logon.last.password1`* variable.
6. (Optional) To add RSA SecurID authentication, click the plus (+) icon between **Logon Page** and **Deny**:
   a) From the **Authentication** tab, select **RSA SecurID**, and click **Add Item**.
   b) In the properties screen from the **Server** list, select the AAA server that you created previously and click **Save**.
      The properties screen closes.
   c) After the RSA SecurID action, add a Variable Assign action.

      Use the Variable Assign action to move the AD password into the *`session.logon.last.password`* variable.
   d) Click **Add new entry**.
      An **empty** entry appears in the Assignment table.
   e) Click the `change` link next to the **empty** entry.
      A popup screen displays, where you can enter a variable and an expression.
   f) From the left-side list, select **Custom Variable** (the default), and type `session.logon.last.password`.
   g) From the right-side list, select **Custom Expression** (the default), and type `expr { "[mcget -secure session.logon.last.password1]" }`.

   The AD password is now available for use in Active Directory authentication.

h) Click **Finished** to save the variable and expression, and return to the Variable Assign action screen.

7. Add the AD Auth action after one of these actions:
   - **Variable Assign** - This action is present only if you added RSA SecurID authentication.
   - **Logon Page** - Add here if you did not add RSA SecurID authentication.

   A properties screen for the AD Auth action opens.
8. Configure the properties for the AD Auth action:
   a) From the **AAA Server** list, select the AAA server that you created previously.
   b) Configure the rest of the properties as applicable to your configuration and click **Save**.
9. On the fallback path between the last action and **Deny**, click the **Deny** link, and then click **Allow** and **Save**.
10. Click **Close**.

You have an access policy that is configured to enable APM dynamic webtop after the appropriate authentication checks.

Assigning resources to the access policy

Before you start, open the existing access policy for edit.

Assign the full webtop and VMware View remote desktop resource that you configured previously to a session so that users can log into View Connection Servers and launch a View Desktop from the webtop.

Note: *This access policy shows how to use the Advanced Resource Assign action item to assign the resources. Alternatively, you can use the Resource Assign and Webtop and Links Assign action items.*

---

1. Click the **(+)** icon anywhere in the access policy to add a new action item.
   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
2. On the Assignment tab, select **Advanced Resource Assign** and click **Add Item**.
   The properties screen opens.
3. Click **Add new entry**.
   An **Empty** entry displays.
4. Click the **Add/Delete** link below the entry.
   The screen changes to display resources that you can add and delete.
5. Select the Remote Desktop tab.

   A list of remote desktop resources is displayed.
6. Select VMware View remote desktop resources and click **Update**.
   You are returned to the properties screen where Remote Desktop and the names of the selected resources are displayed.
7. Click **Add new entry**.
   An **Empty** entry displays.
8. Click the **Add/Delete** link below the entry.
   The screen changes to display resources that you can add and delete.
9. Select the Webtop tab.

   A list of webtops is displayed.
10. Select a webtop and click **Update**.
    The screen changes to display properties and the name of the selected webtop is displayed.

11. Select **Save** to save any changes and return to the access policy.

A VMware View remote desktop resource and an Access Policy Manager® dynamic webtop are assigned to the session when the access policy runs.

Creating a connectivity profile

You create a connectivity profile to configure client connections.

1. On the Main tab, click **Access Policy** > **Secure Connectivity**.
   A list of connectivity profiles displays.
2. Click **Add**.
   The Create New Connectivity Profile popup screen opens and displays General Settings.
3. Type a **Profile Name** for the connectivity profile.
4. Select a **Parent Profile** from the list.
   APM® provides a default profile, **connectivity**.
5. Click **OK**.
   The popup screen closes, and the Connectivity Profile List displays.

The connectivity profile appears in the list.

To provide functionality with a connectivity profile, you must add the connectivity profile to a virtual server.

Creating a custom server SSL profile

With a server SSL profile, the BIG-IP® system can perform decryption and encryption for server-side SSL traffic.

1. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Server**.
   The SSL Server profile list screen opens.
2. Click **Create**.
   The New Server SSL Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the Parent Profile list, select **serverssl**.
5. In the Configuration area, select **Advanced** and select the **Custom** check box.
   Additional settings display. All settings in the Configuration area become available.
6. Scroll down to the **Server Name** field and type `pcoip-default-sni`.
7. Click **Finished**.

The custom server SSL profile is listed in the SSL Server list.

Verifying the certificate on a View Connection Server

Before you start, obtain the CA certificate that was used to sign the SSL certificate on View Connection Servers and obtain a Certificate Revocation List (CRL).

You install the CA certificate and CRL, then update the server SSL profile to use them only if you want the BIG-IP system to check the validity of the certificate on the View Connection Server.

1. On the Main tab, click **System** > **File Management** > **SSL Certificate List**.
   The SSL Certificate List screen opens.
2. Click **Import**.
3. From the **Import Type** list, select **Certificate**.
4. For the **Certificate Name** setting, do one of the following:
   - Select the **Create New** option, and type a unique name in the field.
   - Select the **Overwrite Existing** option, and select a certificate name from the list.
5. For the **Certificate Source** setting, select **Upload File** and browse to select the certificate signed by the CA server.
6. Click **Import**.
   The SSL Certificate List screen displays. The certificate is installed.
7. Click **Import**.
8. From **Import Type** list, select **Certificate Revocation List**.
9. For **Certificate Revocation List Name**, type a name.
10. For **Certificate Revocation List Source**, select **Upload File** and browse to select the CRL you obtained earlier.
11. Click **Import**.
    The SSL Certificate List screen displays. The CRL is installed.
12. On the Main tab, click **Local Traffic** > **Profiles** > **SSL** > **Server**.
    The SSL Server profile list screen opens.
13. Click the name of the server SSL profile you created previously.
    The Properties screen displays.
14. Scroll down to the Server Authentication area.
15. From the **Server Certificate** list, select **require**.
16. From the **Trusted Certificate Authorities** list, select the name of the certificate you installed previously.
17. From the **Certificate Revocation List (CRL)** list, select the name of the CRL you installed previously.
18. Click **Update**.

The BIG-IP system is configured to check the validity of the certificate on the View Connection Server.

Overview: Accessing a View Desktop from an APM webtop

Creating a custom server SSL profile

Configuring an HTTPS virtual server for a dynamic webtop

Configuring an HTTPS virtual server for a dynamic webtop

Before you start this task, create a connectivity profile in Access Policy Manager®. (Default settings are acceptable.)

Create this virtual server to support launching a View Desktop from an APM® dynamic webtop. This is the virtual server that users will specify in the browser.

Note: *This is one of two virtual servers that you must configure. Use the same destination IP address for each one.*

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.

3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, select **Host** and in the **Address** field, type the IP address for the virtual server.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **HTTP Profile** list, select **http**.
7. For the **SSL Profile (Client)** setting, in the **Available** box, select a profile name, and using the Move button, move the name to the **Selected** box.
8. For the **SSL Profile (Server)** setting, from the **Available** list, select the name of the Server SSL profile you previously created, and using the Move button, move the name to the **Selected** list.
9. From the **Source Address Translation** list, select **Auto Map**.
10. In the Access Policy area, from the **Access Profile** list, select the access profile.
11. From the **Connectivity Profile** list, select the connectivity profile.
12. Select the **VDI & Java Support** check box.
13. Locate the Resources area of the screen and from the **Default Persistence Profile** list, select one of these profiles:
    - **cookie** - This is the default cookie persistence profile. Cookie persistence is recommended.
    - **source_addr** - This is the default source address translation persistence profile. Select it only when the cookie persistence type is not available.
14. Click **Finished**.

This virtual server handles access and handles XML protocol data.

Configuring a UDP virtual server for PCoIP traffic

Create this virtual server to support a PC over IP (PCoIP) data channel for View Client traffic.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, select **Host** and in the **Address** field, type the IP address for the virtual server.

   Type the same IP address as the one for the View Client authentication virtual server.
5. In the **Service Port** field, type `4172`.
6. From the **Protocol** list, select **UDP**.
7. From the **Source Address Translation** list, select **Auto Map**.
8. From the Access Policy area, select the **VDI & Java Support** check box.
9. Click **Finished**.

This virtual server is configured to support PCoIP transport protocol traffic for VMware View Clients.

Configuring virtual servers that use a private IP address

If you configured the HTTPS and UDP virtual servers with a private IP address that is not reachable from the Internet, but instead a publicly available device (typically a firewall or a router) performs NAT for it, you need to perform these steps.

You update the access policy by assigning the variable *view.proxy_addr* to the IP address that the client uses to reach the virtual server. Otherwise, a View Client cannot connect when the virtual servers have a private IP address.

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** icon anywhere in the access policy to add a new action item.
   A popup screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.
4. Type `var` in the search field, select **Variable Assign** from the results list, and click **Add Item**.
   The Variable Assign properties screen opens.
5. Click the **change** link next to the empty entry.
   A popup screen displays two panes, with Custom Variable selected on the left and Custom Expression selected on the right.
6. In the Custom Variable field, type `view.proxy_addr`.
7. In the Custom Expression field, type `expr {"`*proxy address*`"}` where proxy address is the IP address that the client uses to reach the virtual server.
8. Click **Finished** to save the variable and expression and return to the Variable Assign action popup screen.
9. Click **Save**.
   The properties screen closes and the visual policy editor displays.
10. Click the **Apply Access Policy** link to apply and activate the changes to the access policy.

Chapter 10

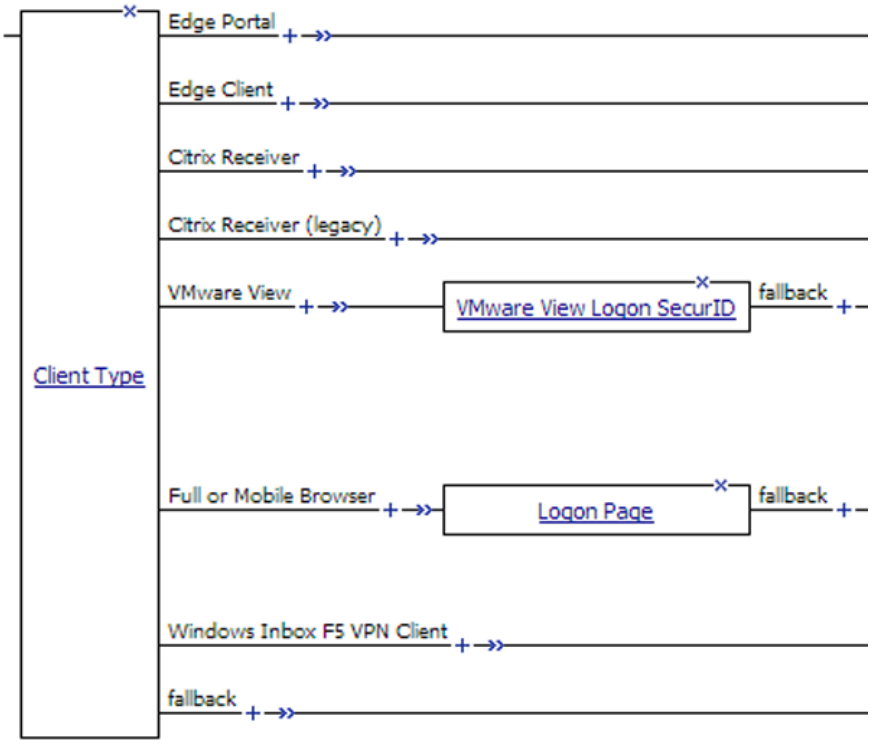
Tips for Standalone View Client and Dynamic Webtop Integration

Example access policy for standalone View Client and View on webtop

You can configure one access policy that can provide access to a standalone View Client and can launch View from a webtop depending on the client type.

Client Type action branch rules

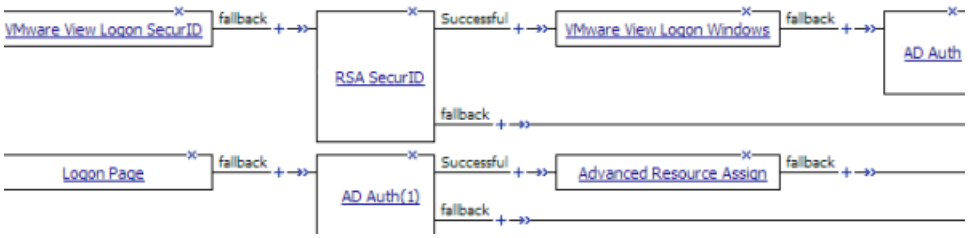
Place actions for the standalone View Client on the VMware View branch, and place actions for launching View from a dynamic webtop on the Full or Mobile Browser branch.



Example access policy continued: Logon and authentication

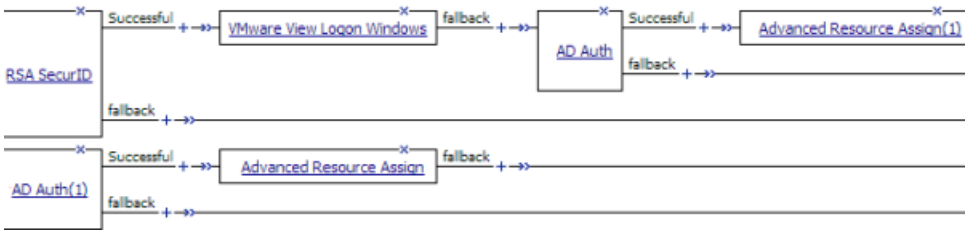
To support a standalone View Client, you must provide a VMware View Logon page and Active Directory authentication. This example shows RSA SecurID authentication followed by Active Directory (AD) authentication. (SecurID authentication is optional for a standalone View Client; if used, it must precede AD Auth.)

To support launching View from a webtop, you can provide a Logon Page and any authentication type. This example includes AD Auth.



Example access policy completed: Resource assignment

After successful authentication, assign resources to the session.



Note: *You might choose to configure your access policy differently. For example, you might not use SecurID authentication for a standalone View Client at all, and you might choose a different type of authentication, or multiple types of authentication, before launching View from a webtop.*

About a configuration for standalone View Client and View on webtop

When you configure Access Policy Manager® (APM®) to support standalone View Client authentication and to support launching View from a dynamic webtop, the instructions specify the same type of configuration objects for either case. You can use the same objects for both cases if you begin the access policy with the Client Type action. Then configure actions for View Client authentication on the VMware View branch and configure actions for the webtop on the Full or Mobile Browser branch.

Chapter 11

Configuring AAA Servers in APM

About VMware View and APM authentication types

You can authenticate View Clients in Access Policy Manager® (APM®) using the types of authentication that View Clients support: Active Directory authentication (required) and RSA SecurID authentication (optional). APM supports these authentication types with AAA servers that you configure in APM.

For more information, refer to the *BIG-IP® Access Policy Manager®: Authentication Configuration Guide* at `http://support.f5.com`.

Task summary

You need at least one AAA Active Directory server object in APM to support AD authentication for VMware View. If you also want to collect RSA PINs, you need at least one AAA SecurID server object in APM.

Configuring an Active Directory AAA server
Configuring a SecurID AAA server in APM

Configuring an Active Directory AAA server

You configure an Active Directory AAA server in Access Policy Manager® (APM) to specify domain controllers and credentials for APM® to use for authenticating users.

1. On the Main tab, click **Access Policy** > **AAA Servers** > **Active Directory**.
   The Active Directory Servers list screen opens.
2. Click **Create**.
   The New Server properties screen opens.
3. In the **Name** field, type a unique name for the authentication server.
4. In the **Domain Name** field, type the name of the Windows domain.
5. For the **Server Connection** setting, select one of these options:
   - Select **Use Pool** to set up high availability for the AAA server.
   - Select **Direct** to set up the AAA server for standalone functionality.
6. If you selected **Direct**, type a name in the **Domain Controller** field.
7. If you selected **Use Pool**, configure the pool:
   a) Type a name in the **Domain Controller Pool Name** field.
   b) Specify the **Domain Controllers** in the pool by typing the IP address and host name for each, and clicking the **Add** button.
   c) To monitor the health of the AAA server, you have the option of selecting a health monitor: only the **gateway_icmp** monitor is appropriate in this case; you can select it from the **Server Pool Monitor** list.
8. In the **Admin Name** field, type a is case-sensitive name for an administrator who has Active Directory administrative permissions.
   APM uses the information in the **Admin Name** and **Admin Password** fields for AD Query. If Active Directory is configured for anonymous queries, you do not need to provide an Admin Name. Otherwise, APM needs an account with sufficient privilege to bind to an Active Directory server, fetch user group

information, and fetch Active Directory password policies to support password-related functionality. (APM must fetch password policies, for example, if you select the Prompt user to change password before expiration option in an AD Query action.) If you do not provide Admin account information in this configuration, APM uses the user account to fetch information. This works if the user account has sufficient privilege.

9. In the **Admin Password** field, type the administrator password associated with the Domain Name.
10. In the **Verify Admin Password** field, retype the administrator password associated with the **Domain Name** setting.
11. In the **Group Cache Lifetime** field, type the number of days.
    The default lifetime is 30 days.
12. In the **Password Security Object Cache Lifetime** field, type the number of days.
    The default lifetime is 30 days.
13. From the **Kerberos Preauthentication Encryption Type** list, select an encryption type.
    The default is **None**. If you specify an encryption type, the BIG-IP® system includes Kerberos preauthentication data within the first authentication service request (AS-REQ) packet.
14. In the **Timeout** field, type a timeout interval (in seconds) for the AAA server. (This setting is optional.)
15. Click **Finished**.
    The new server displays on the list.

This adds the new Active Directory server to the Active Directory Servers list.

Configuring a SecurID AAA server in APM

Configure a SecurID AAA server for Access Policy Manager® (APM®) to request RSA SecurID authentication from an RSA Manager authentication server.

1. On the Main tab, click **Access Policy** > **AAA Servers**.
   The AAA Servers list screen opens.
2. On the menu bar, click **AAA Servers By Type**, and select **SecurID**.
   The SecurID screen opens and displays the servers list.
3. Click **Create**.
   The New Server properties screen opens.
4. In the **Name** field, type a unique name for the authentication server.
5. In the Configuration area, for the **Agent Host IP Address (must match the IP address in SecurID Configuration File)** setting, select an option as appropriate:
   - **Select from Self IP List**: Choose this when there is no NAT device between APM and the RSA Authentication Manager. Select an IP from the list of those configured on the BIG-IP® system (in the Network area of the Configuration utility).
   - **Other**: Choose this when there is a NAT device in the network path between Access Policy Manager and the RSA Authentication Manager server. If selected, type the address as translated by the NAT device.
6. For the **SecurID Configuration File** setting, browse to upload the `sdconf.rec` file.
   Consult your RSA Authentication Manager administrator to generate this file for you.
7. Click **Finished**.
   The new server displays on the list.

This adds a new RSA SecurID server to the AAA Servers list.

Index

W

X