BIG-IP® Access Policy Manager®: Citrix Integration

Version 11.4

Table of Contents

Legal Notices.....5
Acknowledgments.....7

Chapter 1: Citrix Requirements for Integration with APM.....11
About Access Policy Manager and Citrix integration types.....12
About Citrix required settings.....12
About Citrix Receiver requirements for Mac, iOS, and Android clients.....13
About Citrix Receiver requirements for Windows and Linux clients.....14
About Citrix requirements for SmartCard support.....14
About Citrix product terminology.....14

Chapter 2: Integrating APM with a Citrix Web Interface Site.....17
Overview: Integrating APM with Citrix Web Interface sites.....18
Task summary for APM integration with Citrix Web Interface sites.....19
Creating an access policy for Citrix SSO.....20
Adding Citrix Smart Access actions to an access policy.....23
Creating a pool of Citrix Web Interface servers.....24
Adding a connectivity profile 24
Creating a custom HTTP profile.....25
Configuring the external virtual server.....25
Creating a data group to support a nonstandard Citrix service site.....26
Configuring an internal virtual server 26

Chapter 3: Integrating APM with Citrix XML Brokers.....29
Overview: Integrating APM with Citrix XML Brokers with SmartAccess support.....30
About APM dynamic webtop for Citrix XML Brokers.....31
About the Client Type action.....31
About Citrix client bundles in APM.....32
About auto logon from APM dynamic webtop and authentication.....32
Task summary for XML Broker integration with APM.....32
Creating a pool of Citrix XML Brokers.....33
Configuring a Citrix remote desktop resource.....33
Configuring a dynamic webtop.....34
Creating an access policy for Citrix SSO (APM dynamic webtop).....34
Assigning Citrix resources to an access policy for Citrix integration.....37
Adding Citrix Smart Access actions to an access policy.....38
Adding a connectivity profile 39
Adding Citrix Receiver for HTML5 to a connectivity profile.....39
Creating a virtual server to support Citrix web and mobile clients.....40

Chapter 4: Shaping Client Traffic.....41
Overview: Shaping traffic for Citrix clients that support MultiStream ICA.....42
About Citrix XenApp server requirements for shaping traffic with APM.....42
Task summary.....43
Creating a dynamic bandwidth control policy for Citrix MultiStream ICA traffic.....43
Adding support for Citrix traffic shaping to an access policy.....44

Legal Notices

Publication Date

This document was published on May 15, 2013.

Publication Number

MAN-0403-01

Copyright

Trademarks

Access Policy Manager, Advanced Client Authentication, Advanced Routing, APM, 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 Management Pack, F5 Networks, F5 World, Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iApps, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, Message Security Manager, MSM, OneConnect, OpenBloX, OpenBloX [DESIGN], Packet Velocity, Policy Enforcement Manager, PEM, Protocol Security Manager, PSM, Real Traffic Policy Builder, Rosetta Diameter Gateway, Scale^{N}, Signaling Delivery Controller, SDC, SSL Acceleration, StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TMOS, Traffic Management Operating System, Traffix Diameter Load Balancer, Traffix Systems, Traffix Systems (DESIGN), Transparent Data Reduction, UNITY, VAULT, VIPRION, vCMP, virtual Clustered Multiprocessing, WA, WAN Optimization Manager, WebAccelerator, WOM, 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 U.S. Patent 7,114,180; 8,301,837. This list is believed to be current as of May 15, 2013.

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.

Chapter 1

Citrix Requirements for Integration with APM

- *About Access Policy Manager and Citrix integration types*
- *About Citrix required settings*
- *About Citrix Receiver requirements for Mac, iOS, and Android clients*
- *About Citrix Receiver requirements for Windows and Linux clients*
- *About Citrix requirements for SmartCard support*
- *About Citrix product terminology*

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*
- *Task summary for APM integration with Citrix Web Interface sites*

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.

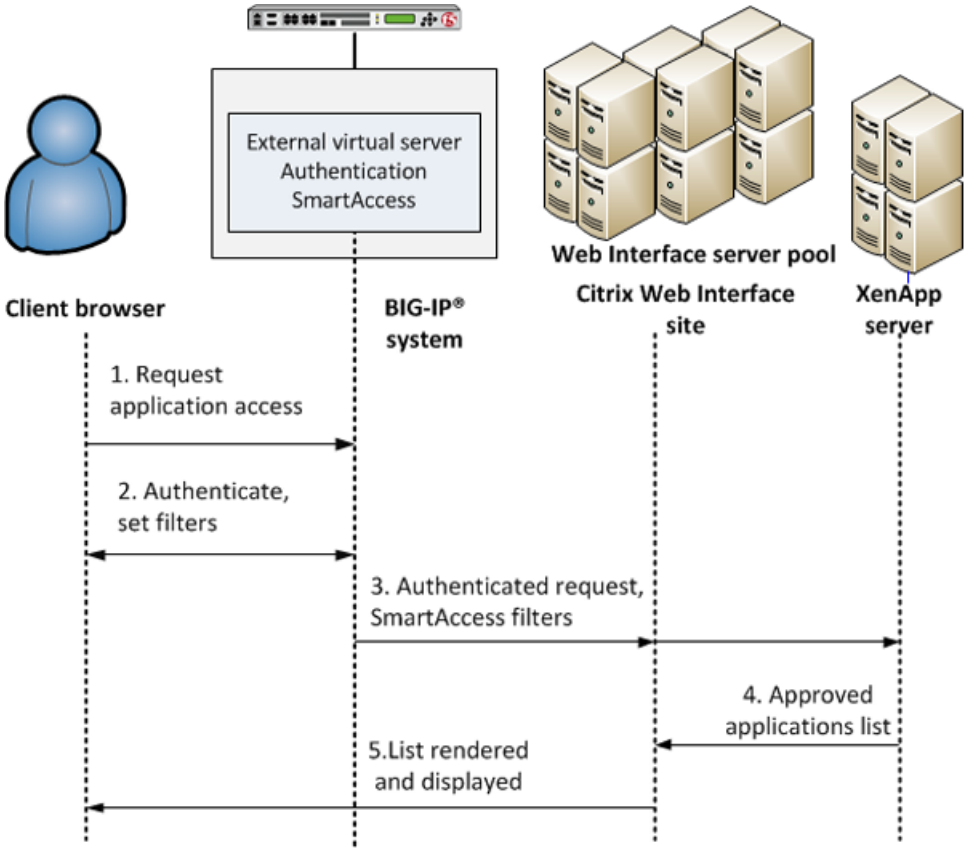


Figure 1: APM Citrix Web Interface integration with SmartAccess support

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.

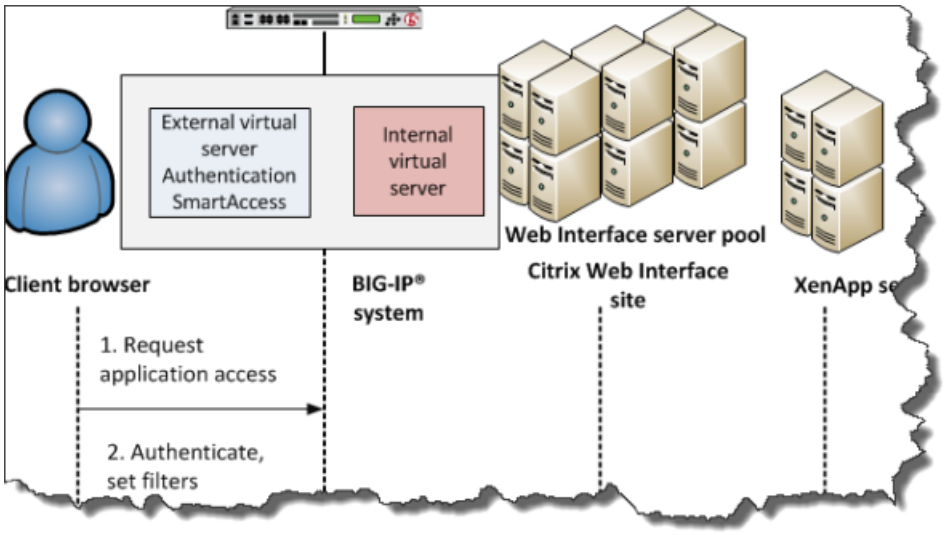


Figure 2: Internal virtual server for requests from Web Interface site

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.*

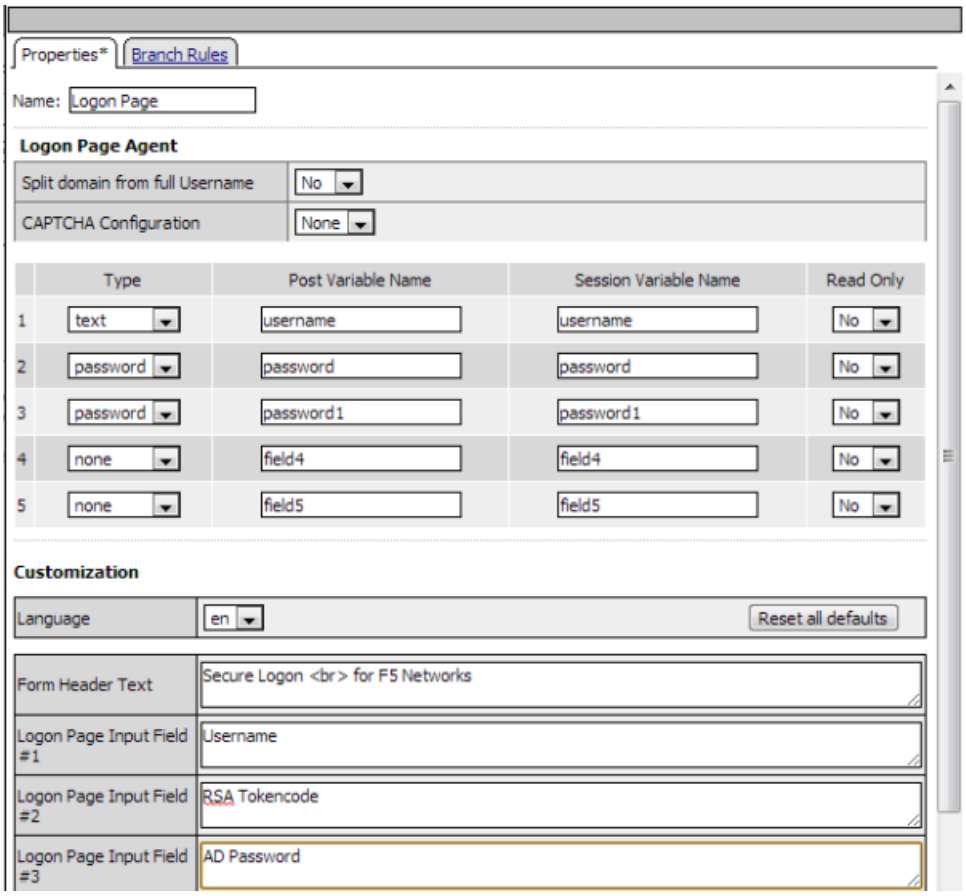
1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure to launch the visual policy editor.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** sign anywhere in the access policy to add a new action item.
   An Add Item 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**.

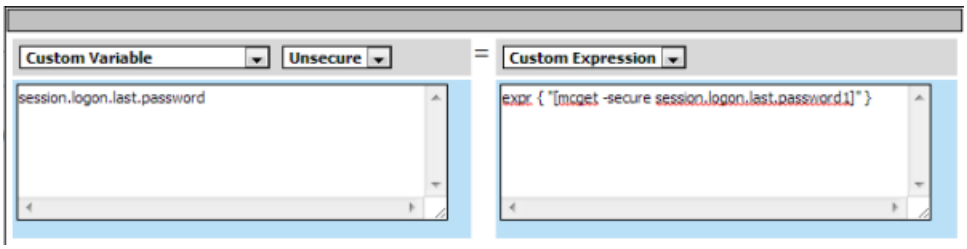
   In this example, Logon Page Input Field #2 accepts the RSA Token code into the `session.logon.last.password` variable (from which authentication agents read it). Logging Page

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**.

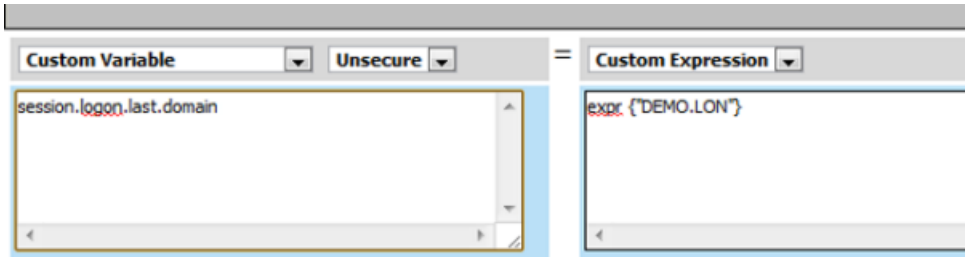
a) From the Assignment tab, select **SSO Credential Mapping**, and click **Add Item**.
b) Click **Save**.

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:

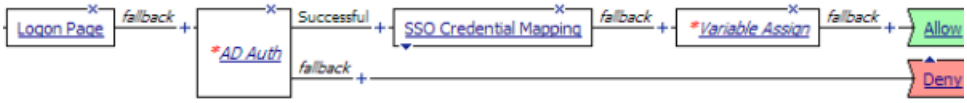


Figure 3: Example access policy with AD authentication, credential mapping, and Web Interface site domain assignment

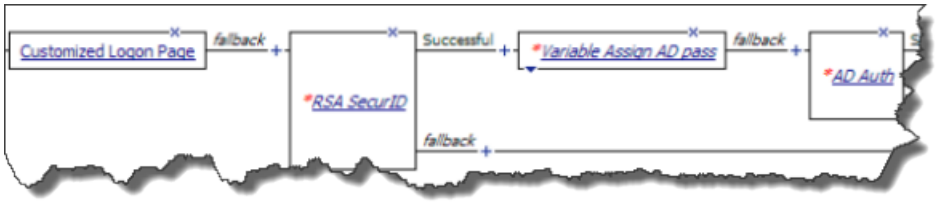


Figure 4: Configuring RSA SecurID authentication before AD authentication

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.

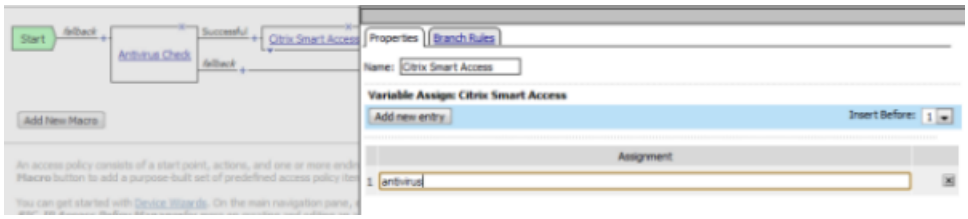


Figure 5: Example access policy with Citrix SmartAccess action and an antivirus check

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. 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*
- *Task summary for XML Broker integration with APM*

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.

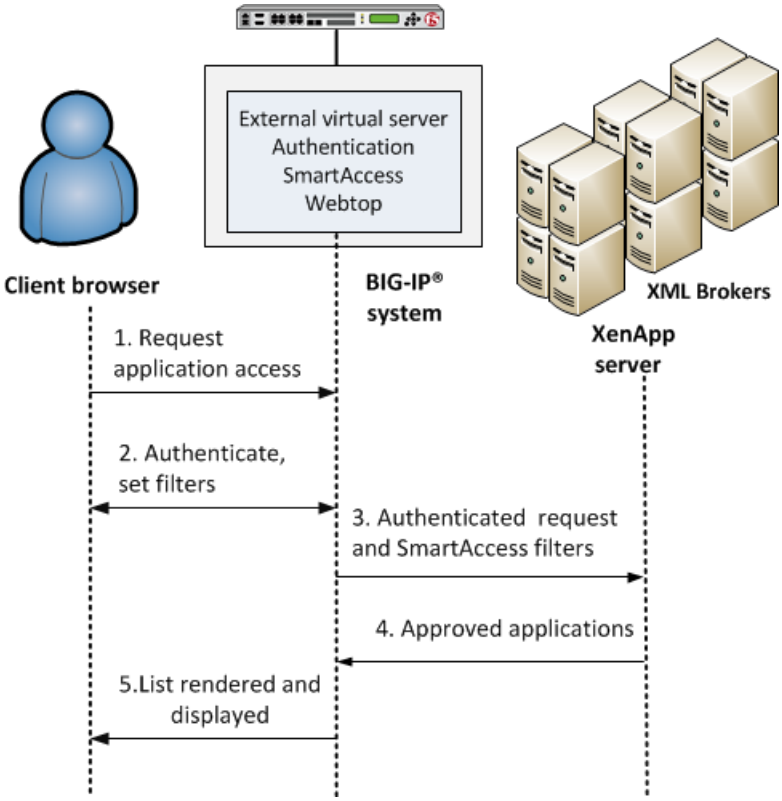


Figure 6: APM integration with Citrix XML Brokers

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.

About the Client Type action

The Client Type action identifies various client types and provides branches for them. This action makes it possible for you to specify different actions for different clients types in one access policy. As a result you can then use one virtual server for traffic from different client types. An example of adding a Client Type action to an access policy is shown in this figure.

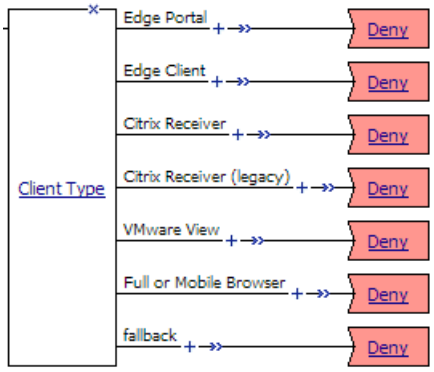


Figure 7: Client Type action

The client types include:

Edge Portal
BIG-IP® Edge Portal® clients

Edge Client
BIG-IP® Edge Client®

Citrix Receiver
Later Citrix Receiver clients

Citrix Receiver (legacy)
Earlier Citrix Receiver clients (identified with PN Agent)

VMware View
View Clients

Full or Mobile Browser
Web access from desktops and mobile apps

Access Policy Manager® 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 Access Policy Manager.

Note: *To create additional branching for a client type based on operating system, you can add a Client operating system (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
Configuring a Citrix remote desktop resource
Configuring a dynamic webtop
Creating an access policy for Citrix SSO (APM dynamic webtop)

Assigning Citrix resources to an access policy for Citrix integration
Adding Citrix Smart Access actions to an access policy
Adding a connectivity profile
Adding Citrix Receiver for HTML5 to a connectivity profile
Creating a virtual server to support Citrix web and mobile clients

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 to launch the visual policy editor.
   The visual policy editor opens the access policy in a separate screen.
3. Click the **(+)** sign anywhere in the access policy to add a new action item.

An Add Item 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.

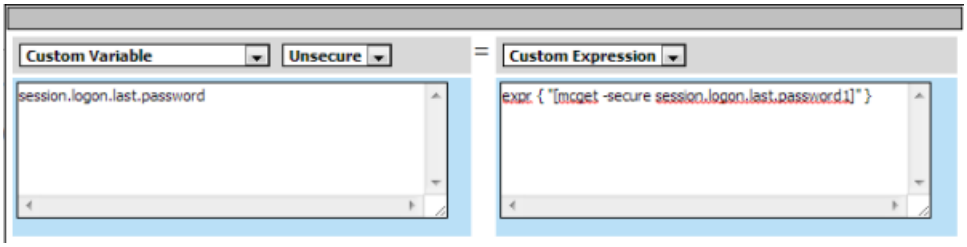
A Variable Assign properties page opens.

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.

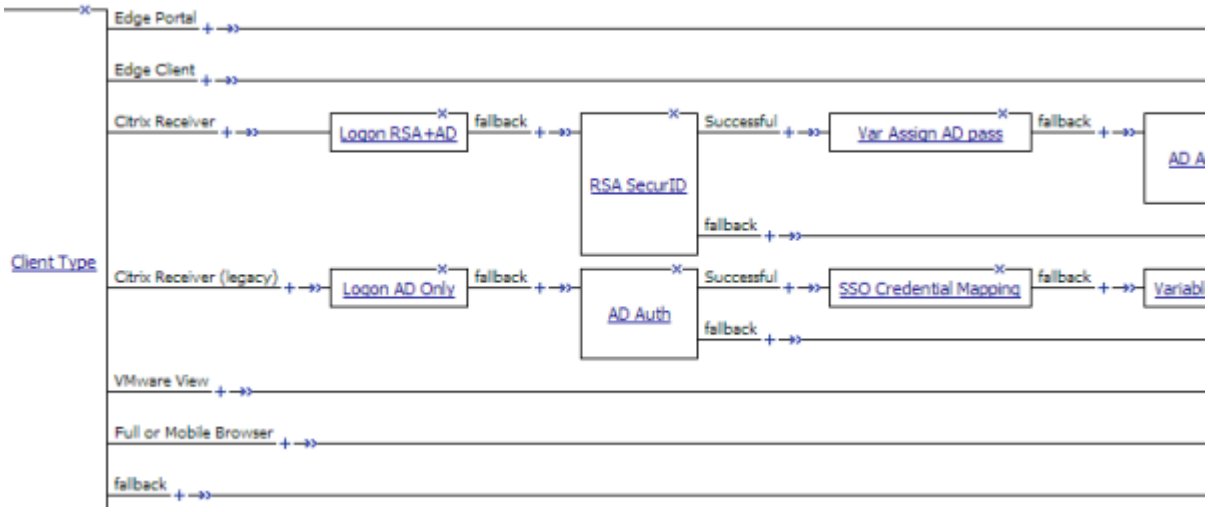


Figure 8: Example access policy for legacy Citrix Receiver clients and later Citrix Reciever clients

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 **(+)** sign anywhere in the access policy to add a new action item.
An Add Item 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.

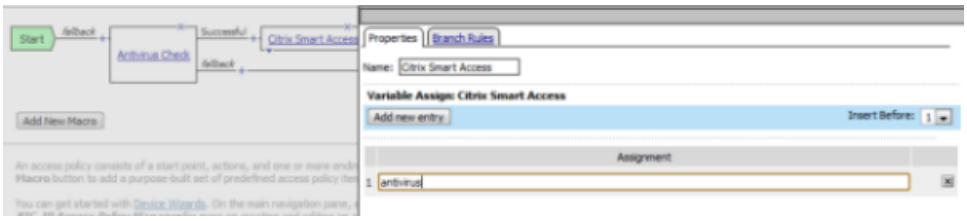


Figure 9: Example access policy with Citrix SmartAccess action and an antivirus check

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 Client Traffic

- *Overview: Shaping traffic for Citrix clients that support MultiStream ICA*
- *Task summary*

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 to launch the visual policy editor.
   The visual policy editor opens the access policy in a separate screen.
3. On an access policy branch, click the plus symbol (+) 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 plus symbol (+) 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.

Index

A

access policy
  adding authentication actions *34*
  authentication actions, adding *20*
  Citrix SSO, supporting *20*
  Smart Access action item *23*, *38*
  supporting Citrix SSO *34*
APM integration with Citrix
  about *12*
authentication
  AAA servers, creating for *20*, *34*
  AD Auth *20*, *34*
  AD Auth and RSA Auth *20*, *34*
  logon page, customizing *20*, *34*

B

bandwidth control policies
  dynamic, creating *43*
BIG-IP system tasks
  integration with Citrix XML Brokers *32*

C

Citrix client bundle *32*
Citrix farm
  31
  XML Brokers in *33*
Citrix Multi-Port Policy *42*
Citrix MultiStream ICA
  42
  traffic shaping *44*
Citrix Receiver client
  Citrix service site *26*
Citrix remote desktop resource
  assigning to a session *37*
  Citrix farm, relationship to *31*
  configuring *33*
Citrix SmartCard SSO *32*
Client Type action
  compared with Client OS action *31*
  in an access policy *31*
  traffic types, supporting *31*
connectivity profile
  configuring *24*, *39*

D

data group
  APM_Citrix_ConfigXML *26*

F

full webtop
  assigning to a session *37*
  configuring *34*

H

HTML5
  Citrix client bundle, configuring *39*
  configuring *39*
HTTP profiles
  creating *25*

L

logon
  Citrix Receiver for Android client *13*
  Citrix Receiver for iOS client *13*
  Citrix Receiver for Linux client *14*
  Citrix Receiver for Mac client *13*
  Citrix Receiver for Windows client *14*

P

passwordless authentication *32*
pool
  Web Interface servers *24*
  XML Brokers *33*
profiles
  creating for HTTP *25*

R

remote desktop
  configuring a resource *33*
resource item
  configuring for a remote desktop *33*

S

Smart Access
  action item, about *23*, *38*
SmartAccess string
  Citrix settings *12*

T

Trust XML Requests
  Citrix setting *12*

V

virtual server
  and Web Interface site URL *25*
  creating for traffic behind the firewall *26*
  enabling Citrix support *25*, *40*
  Web Interface pool *25*

W

Web Interface server
    pool *24*
Web Interface site
    Citrix settings *12*
    firewall, behind *26*
    HTTP, using *26*
    URL *26*
Web Interface site integration
    authentication types, supported *18*
    clients, supported *18*
    configuration visualized *19*
webtop
    configuring full *34*

X

XenApp AppCenter *14*
XenApp server *14*
XML Brokers
    from a Citrix farm *33*
XML Brokers integration
    about *30*, *42*
    authentication types, supported *30*, *42*