BIG-IP® Access Policy Manager®: Citrix Integration Guide

Version 11.3

IT agility. Your way.

Table of Contents

Table of Contents

Legal Notices

Publication Date

This document was published on February 14, 2013.

Publication Number

MAN-0361-01

Copyright

Trademarks

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 February 14, 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,

Acknowledgments

Chapter 1

Citrix Requirements for Integration with APM

Topics:

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 the Access Gateway 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
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.

For the address field for the standard Citrix service site, `/Citrix/PNAgent/`, use the format `https://<APM-external-virtual-server-FQDN>`.

For the address field for a custom Citrix service site, use the format `https://<APM-external-virtual-server-FQDN/custom_site/config.xml`, where *custom_site* is the name of the custom service site.

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

Topics:

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.

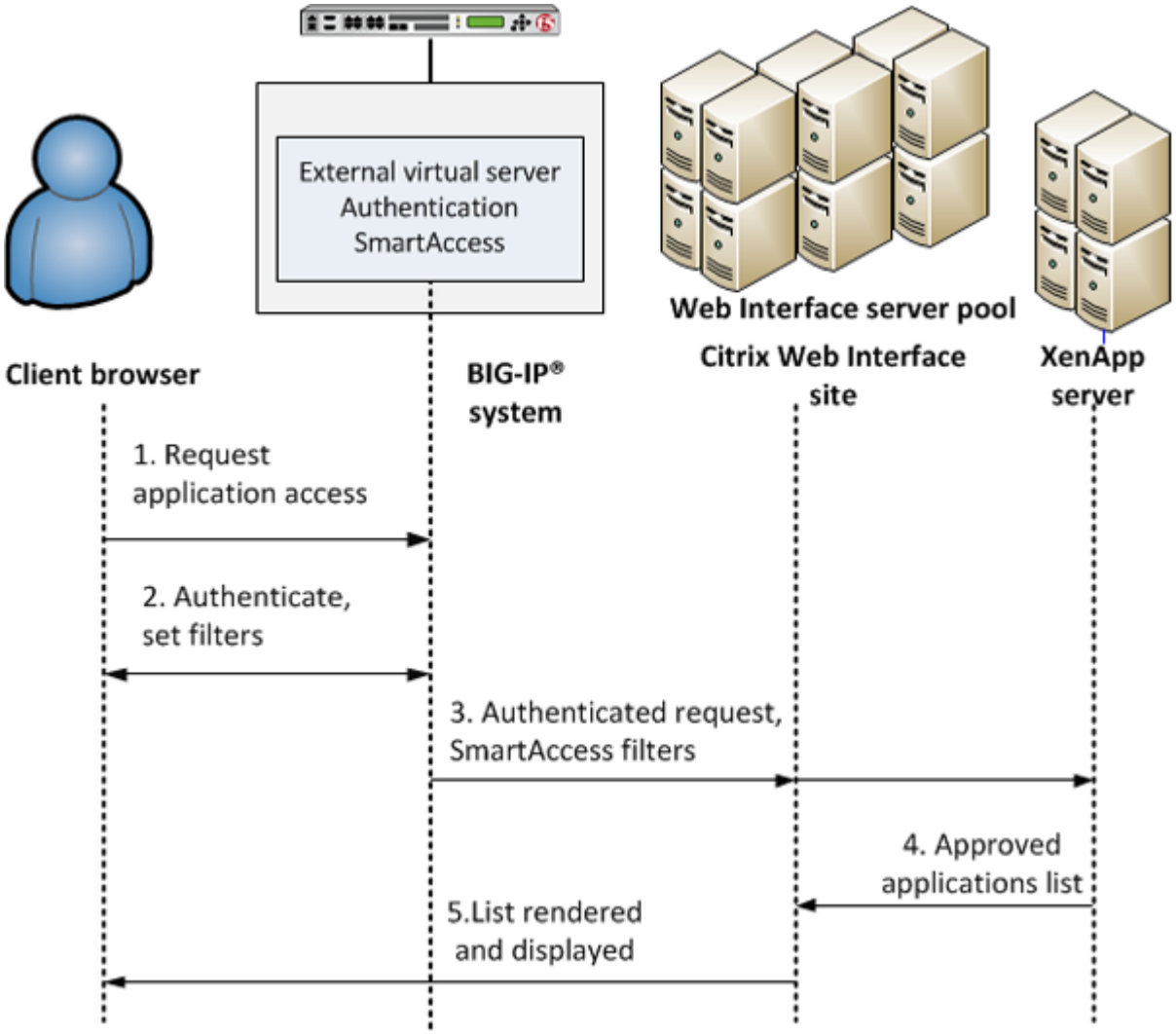


Figure 1: APM Citrix Web Interface integration with SmartAccess support

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 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 special certificates.

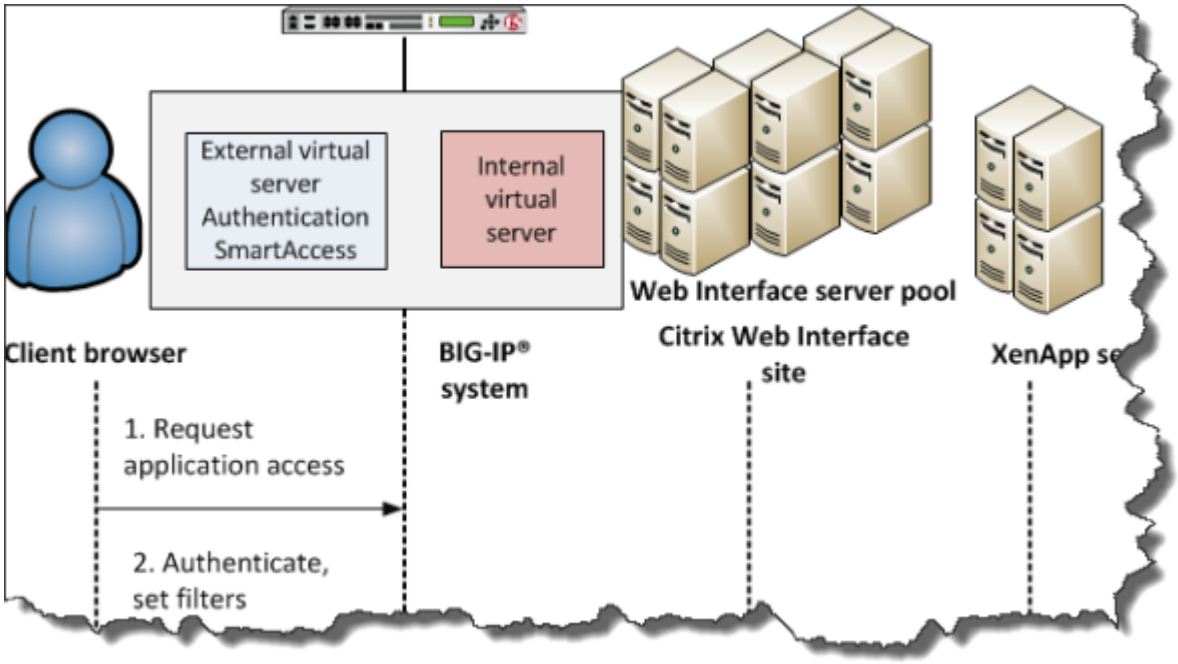


Figure 2: Internal virtual server for requests from Web Interface site

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

Before you can create an access policy for Citrix Web Interface 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.*

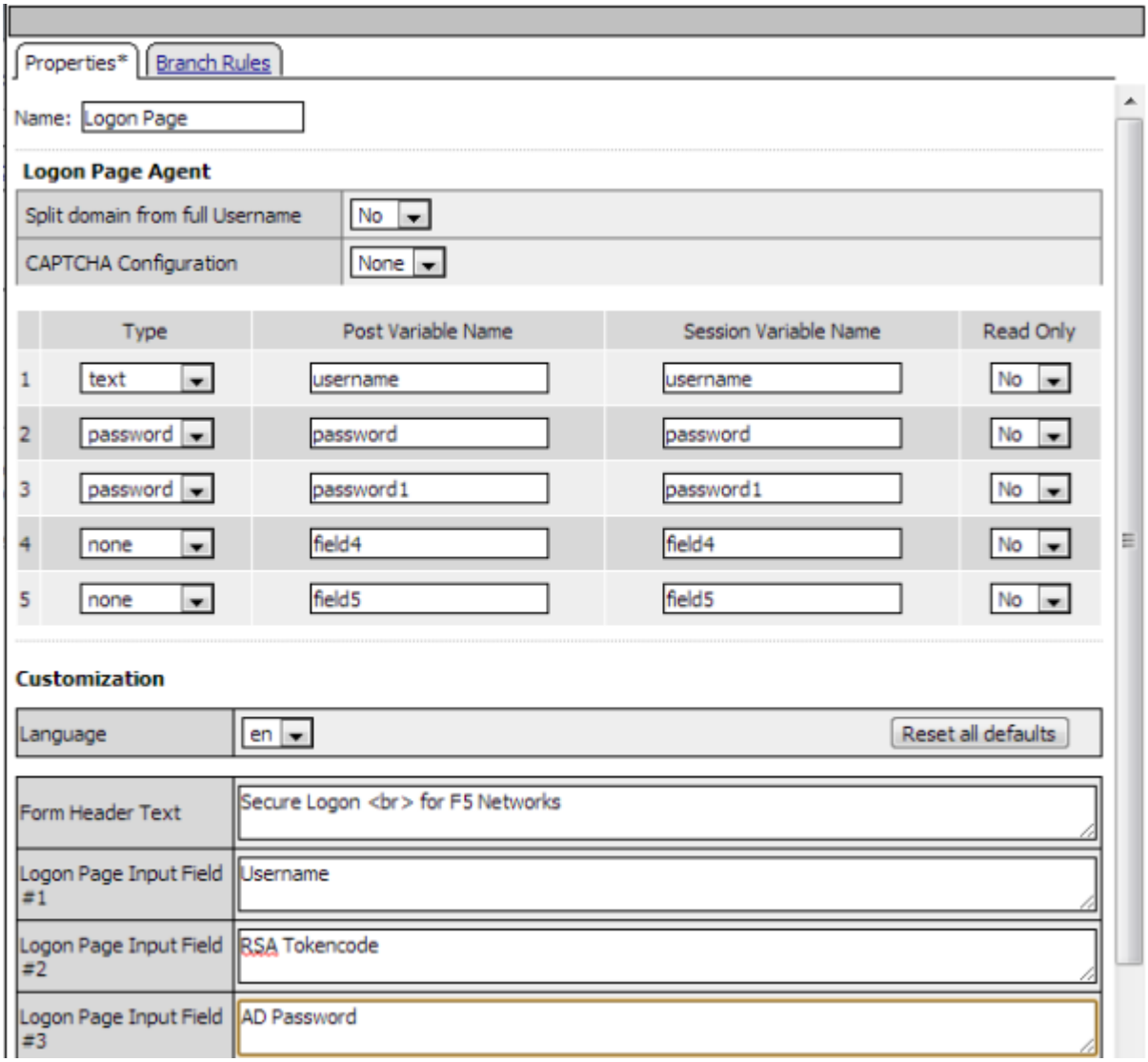
1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure to launch the visual policy editor.
   The visual policy editor opens the access policy in 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 that are grouped by General Purpose, Authentication, and so on.
4. In the General Purpose area, 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**.

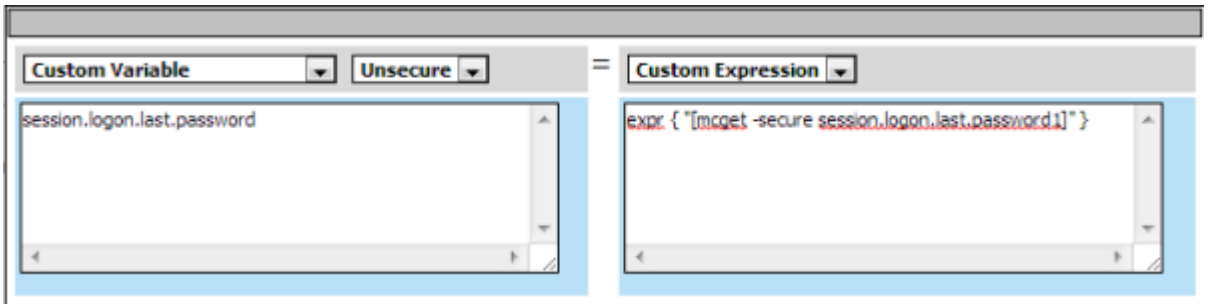
   In this example, Login Page Input Field #2 accepts the RSA Token code into the *session.logon.last.password* variable (from which authentication agents read it). Logging Page Input Field #3 saves the AD password

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 General Purpose area, 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.

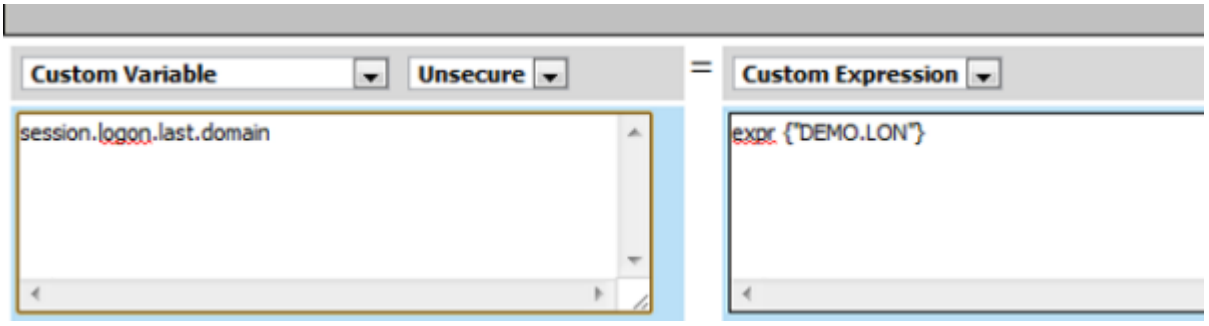
Use the Variable Assign action to pass the domain name for the Citrix Web Interface site so that a user is not repeatedly queried for it.

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 the **Deny** box, and then click **Allow** and **Save**.
12. Click **Close**.

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

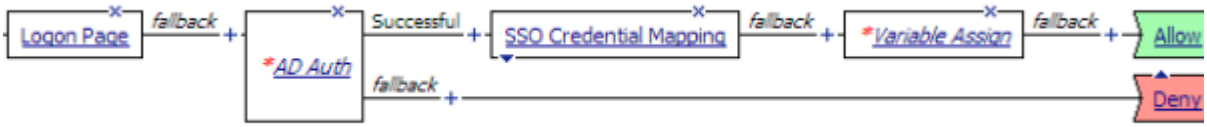


Figure 3: Example access policy with AD authentication, credential mapping, and Web Interface site domain assignment

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 Add Item (+) 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 Citrix XenApp server for application access control or a user policy.

   Note: *You must specify APM as the Access Gateway farm when you configure filters on the XenApp server.*

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.

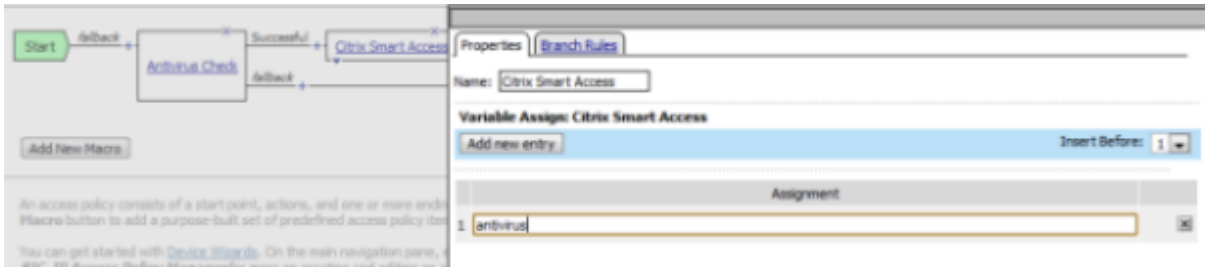


Figure 5: Example access policy with Citrix SmartAccess action and an antivirus check

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.

Creating a connectivity profile

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

1. On the Main tab, click **Access Policy** > **Secure Connectivity** > **Connectivity Profiles**.
2. Click **Create**.
   The New Profile screen opens.
3. Type a **Name** for the connectivity profile.
4. Leave the **Parent Profile** setting at the default option, **connectivity**.

5. Click **Finished**.

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 profile must have **Redirect Rewrite** set to **All**.
10. Depending on the APM version that you have, do one of the following:

    - From the **SNAT Pool** list, select **Auto Map**.
    - 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. Depending on the APM version that you have, select the **Citrix Support** or the **Citrix & 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. In the Configuration area, 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. Depending on the APM version that you have, select the **Citrix Support** or the **Citrix & 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

Topics:

Overview: Integrating APM with Citrix XML Brokers with SmartAccess support

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

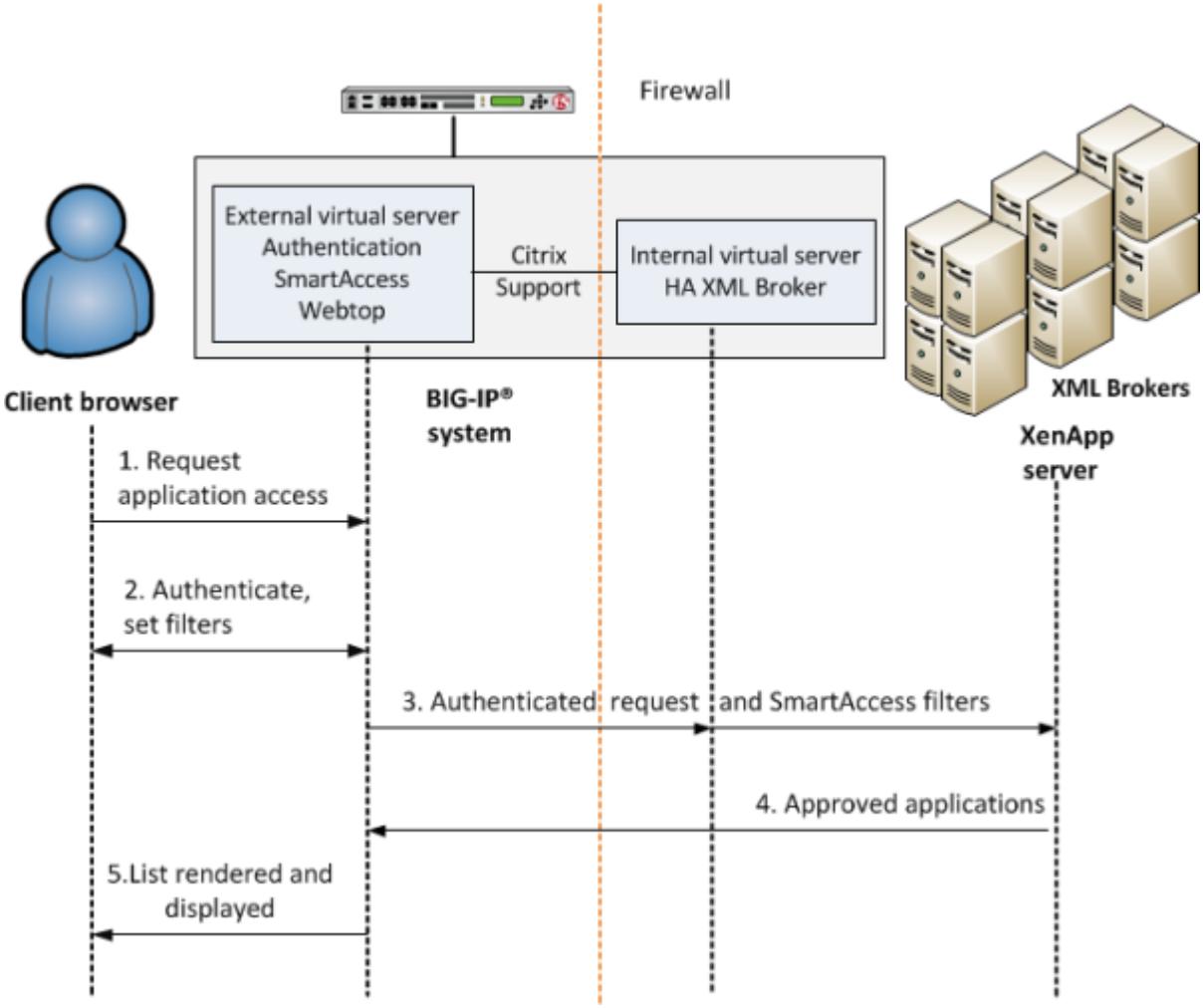


Figure 6: APM integration with Citrix XML Brokers

1. A user (client browser or Citrix Receiver) requests access to applications.
2. The 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 a Citrix XML Broker. A separate, internal virtual server load balances multiple XML Brokers.
4. An XML Broker returns a list of allowed applications to the external virtual server.
5. The external 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® 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 address of an XML Broker is configured on APM through a Citrix remote desktop resource. Each of these resources 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 remote desktop resource support for Citrix Receiver clients

APM supports multiple Citrix remote desktop resources for web clients. However, support for Citrix Receiver (iOS, Android, Mac, Windows, and Linux) clients is limited to one Citrix remote desktop resource.

Important: *APM uses the first Citrix remote desktop resource in alphabetical order. For example, if you have two resources with names /Common/Alpha and /Common/Beta, APM serves only /Common/Alpha to Citrix Receiver clients.*

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
Creating an internal virtual server for Citrix XML Broker HA
Configuring a Citrix remote desktop resource
Configuring a Citrix client bundle
Configuring a dynamic webtop
Creating an access policy for Citrix SSO
Assigning connectivity resources to an access policy for Citrix integration
Adding Citrix Smart Access actions to an access policy
Creating a connectivity profile
Creating an external virtual server to support Citrix web and mobile clients
Creating a data group for Citrix Receiver (Windows and Linux) clients

Creating a pool of Citrix XML Brokers

You can create a pool of Citrix XML Brokers to provide high availability functions. 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 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.

Creating an internal virtual server for Citrix XML Broker HA

This virtual server enables high availability for a pool of Citrix XML Brokers. Create one internal virtual server for each Citrix farm that you want to support.

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 Configuration area, from the **HTTP Profile** list, select **http**.
6. In the **Service Port** field, type `80`, or select **HTTP** from the list.
7. If you use SSL to access the XML Brokers, select an SSL Profile for the **SSL Profile (Server)** field.
8. In the Resources area, locate the **Default Pool** setting.
9. From the **Default Pool** list, select the name of the pool that you created previously.
10. Click **Finished**.

Configuring a Citrix remote desktop resource

This Citrix remote desktop resource uses a pool of XML Brokers that are load-balanced by an internal virtual server. 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, ensure that **Citrix** is selected.
   The default is `Citrix`.
5. For the **Destination** setting, specify the IP address for the internal virtual server that you created.
6. Accept or change the **Port**.
   The port must match the port configured on the internal virtual server.
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 Citrix client bundle

You configure a Citrix client bundle to enable delivery of a Citrix Receiver client to a user's computer when a client is not currently installed, or when a newer client is available. Access Policy Manager® detects whether the Citrix Receiver client is present, and detects the operating system that is running. APM™ redirects users to a download URL. Or, in the case of Windows systems, downloads the Citrix Receiver client that you have uploaded.

Note: *Creating a Citrix client bundle is optional, but you still need a Citrix Receiver client on client systems. If you do not create a Citrix client bundle, you must download the Citrix Receiver client from the Citrix web site and install it on client systems.*

1. On the Main tab, click **Access Policy** > **Application Access** > **Remote Desktops** > **Citrix Client Bundles**.
   The Citrix Client Bundles list screen opens.
2. Click **Create**.
   The New Citrix Client Bundle screen opens.
3. In the **Name** field, type a name for the Citrix client bundle.
4. In the **Download URL** field, accept the default location or type the location from which the user can download a Citrix Receiver client.
   If Access Policy Manager detects that the user's computer is running Windows Citrix Receiver at or above the minimum version that you specify, instead of redirecting the user to this URL, APM performs an action based on the **Source** setting.
5. For **Source**, select one of these options.
   - To redirect the user to download a Windows version of a Citrix Receiver client, select **Windows Download URL**.
   - To enable Access Policy Manager to push a Windows version of a Citrix Receiver client to the user's computer, select **Windows Package File**.
6. Provide additional information, depending on the **Source** option that you selected.
   - For **Windows Download URL**, type the URL to which the Windows user is redirected to download the Citrix Receiver client.
   - For **Windows Package File**, click **Browse** to upload a Windows Citrix Receiver installation package.

7. For the **Windows Minimum Version** setting, type the minimum version of Windows Citrix Receiver.
8. Click **Finished**.

This creates the Citrix client bundle.

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

Before you can create an access policy for Citrix Web Interface 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.

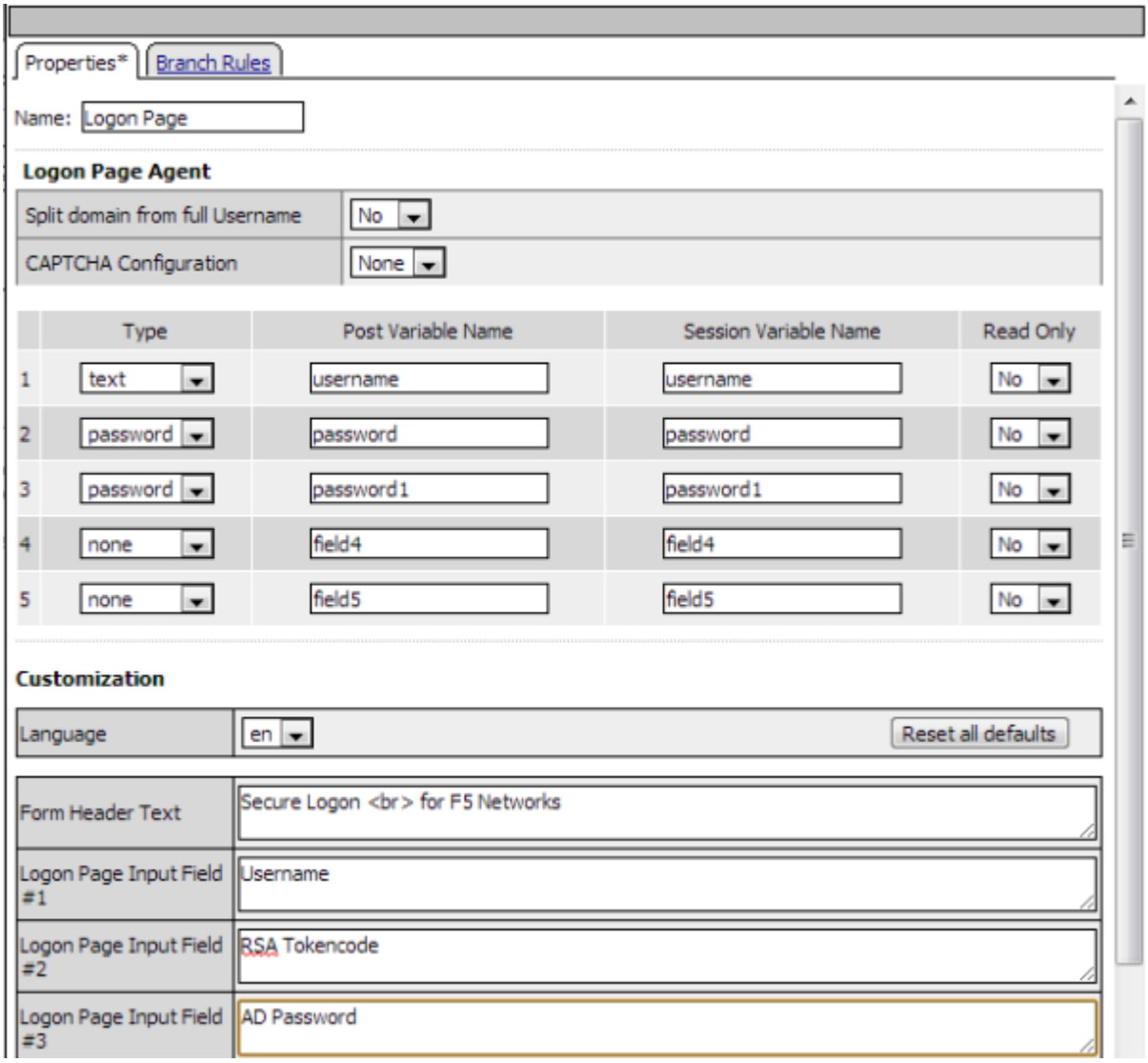
Note: *APM supports different types of authentication depending on the client type. This access policy shows how to use both RSA SecurID and AD Auth authentication (supported for Citrix Receiver for iOS, Mac, and Android) or AD Auth only (supported for Citrix Receiver for Windows and Linux). Use the 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 that are grouped by General Purpose, Authentication, and so on.
4. In the General Purpose area, 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, Login 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.



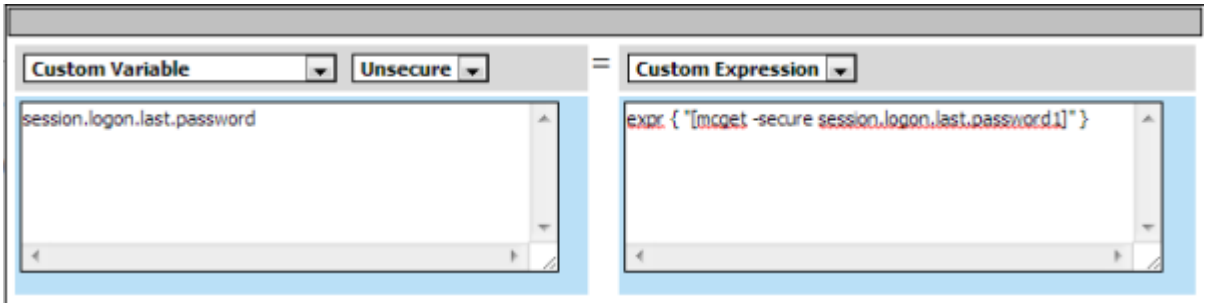
The properties screen closes.

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 General Purpose area, 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.

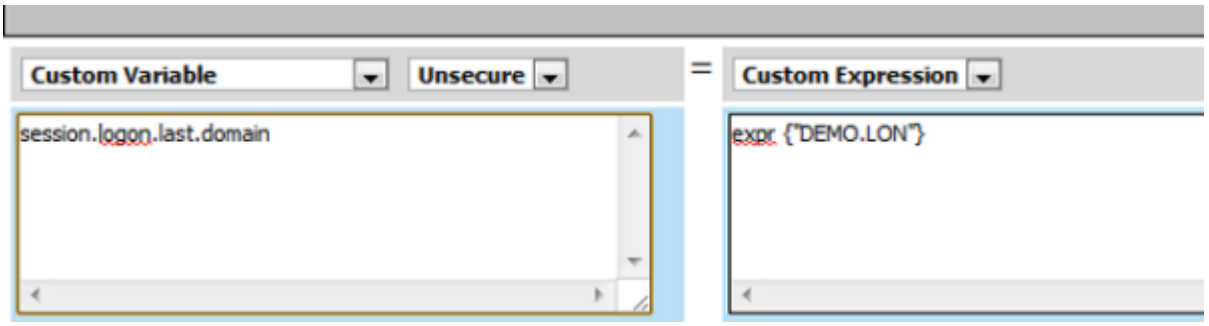
Use the Variable Assign action to pass the domain name for the Citrix Web Interface site so that a user is not repeatedly queried for it.

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 the **Deny** box, and then click **Allow** and **Save**.

12. Click **Close**.

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

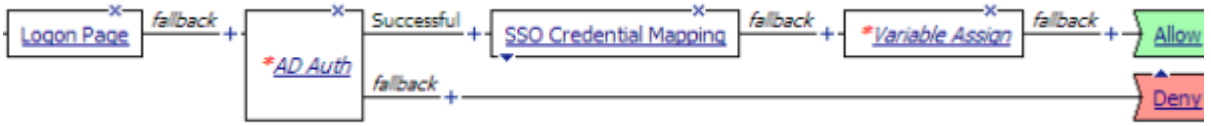


Figure 7: Example access policy with AD authentication, credential mapping, and Web Interface site domain assignment

Figure 8: Configuring RSA SecurID authentication before AD authentication

Assigning connectivity 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 Full 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 that are grouped by General Purpose, Authentication, and so on.

2. From **General Purpose**, select **Full Resource Assign** and click **Add Item**.
   The Properties screen opens.
3. Click **Add new entry**.
   An **Empty** entry appears.
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 Resources** 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 appears.
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 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 Add Item (+) 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 Citrix XenApp server for application access control or a user policy.

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

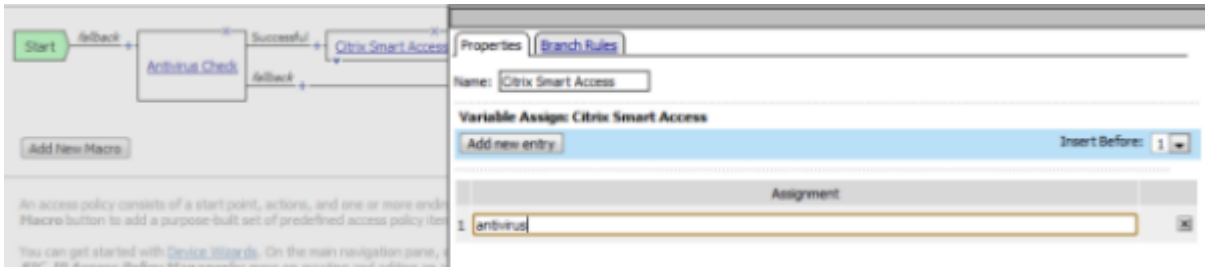


Figure 9: Example access policy with Citrix SmartAccess action and an antivirus check

Creating a connectivity profile

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

1. On the Main tab, click **Access Policy** > **Secure Connectivity** > **Connectivity Profiles**.
2. Click **Create**.
   The New Profile screen opens.
3. Type a **Name** for the connectivity profile.
4. Leave the **Parent Profile** setting at the default option, **connectivity**.
5. Click **Finished**.

The connectivity profile appears in the Connectivity Profile List.

Creating an external 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. In the Configuration area, from the **HTTP Profile** list, select **http**.
8. For the **Stream Profile** setting, retain the default profile, **stream**.

9. 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.
10. Depending on the APM version that you have, do one of the following:
    - From the **SNAT Pool** list, select **Auto Map**.
    - 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. Depending on the APM version that you have, select the **Citrix Support** or the **Citrix & Java Support** check box.
14. To support Citrix Receiver (for Windows and Linux) clients, from the **Default Pool** list, select the name of the pool that you created previously.

    If you include multiple Citrix remote desktop resources in your configuration, select the pool that is associated with the first Citrix remote desktop resource (when listed alphabetically by Citrix remote desktop resource name).
15. Click **Finished**.

The access policy is now associated with the virtual server.

Creating a data group for Citrix Receiver (Windows and Linux) clients

Perform this task only when you need to support Citrix Receiver Windows and Linux clients on Access Policy Manager® and you are integrating APM™ with Citrix XML Brokers. This task creates a data group that associates the external virtual server with an iRule to accomplish the support.

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_PNAgentProtocol`.

   Type the name exactly as shown.
4. From the **Type** list, select **String**.
5. In the **Records** area, create this string record.
   a) In the **String** field, type the FQDN of the APM of the external virtual server (using lowercase characters only).
   b) In the **Value** field, type the number `1`.
   c) Click **Add**.
6. Click **Finished**.
   The new data group appears in the list of data groups.

Index

W

X