BIG-IP® Access Policy Manager®: VMware Horizon View Integration Implementations

Version 11.4

Table of Contents

Legal Notices

Publication Date

This document was published on July 29, 2013.

Publication Number

MAN-0464-00

Copyright

Copyright © 2012-2013, F5 Networks, Inc. All rights reserved.

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

Trademarks

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, Alive With F5, APM, Application Acceleration Manager, Application Security Manager, ARX, AskF5, ASM, BIG-IP, BIG-IQ, Cloud Extender, CloudFucious, Cloud Manager, Clustered Multiprocessing, CMP, COHESION, Data Manager, DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Portal, ELEVATE, EM, Enterprise Manager, ENGAGE, F5, F5 [DESIGN], F5 Certified [DESIGN], F5 Networks, Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, iApps, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, LineRate, LineRate Systems [DESIGN], LROS, Message Security Manager, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Real Traffic Policy Builder, Scale^{N}, Signalling Delivery Controller, SDC, SSL Acceleration, StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TMOS, Traffic Management Operating System, Traffix Systems, Traffix Systems (DESIGN), Transparent Data Reduction, UNITY, VAULT, VIPRION, vCMP, VE F5 [DESIGN], 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 July 29, 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.

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

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

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

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

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

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

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

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

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

Chapter 1

VMware Horizon View Requirements for APM Integration

About VMware Horizon View server required settings

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

SecureTunnel and PCoIP Secure Gateway disabled

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

Advanced authentication disabled

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

About VMware Horizon View server settings and SSL offloading

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

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

Chapter 2

Authenticating Standalone View Clients with APM

Overview: Authenticating View Client with APM

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

A View Client makes connections to support different types of traffic between it and a View Connection Server. APM supports these connections with two virtual servers that share the same destination IP address.

Task summary

Creating a pool of View Connection Servers

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

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

The new pool appears in the Pools list.

Configuring a VMware View remote desktop resource

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

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

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

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

   All other parameters are optional.

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

Configuring a full webtop

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

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

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

Creating an access profile

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

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click **Create**.
   The New Profile screen opens.
3. Type a name for the access profile.
4. In the Language Settings area, add and remove accepted languages, and set the default language.

   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
5. Click **Finished**.

This creates an access profile with a default access policy.

Creating an access policy for View Client authentication

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

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

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

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure 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, select **Client Type** from the results list, and click **Add Item**.

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

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

   Active Directory authentication is required.

   a) Click the (+) sign on the VMware View branch. An Add Item screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on

b) On the Logon tab, select **VMware View Logon Page**, and click **Add Item**.

A properties screen displays.

c) From the **VMware View Logon Screen Type** list, retain the default setting **Windows Password**.

d) In the **VMware View Windows Domains** field, type domain names separated by spaces to use for Active Directory authentication.

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

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

f) Click the plus (+) icon after the previous VMware View Logon Page action.
A popup screen opens.

g) On the Authentication tab, select **AD Auth** and click **Add Item**.

h) From the **Server** list, select an AAA server and click **Save**.
The properties screen closes.

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

a) Click the (+) sign after the previous action.

b) Type `adv` in the search field, select **Advanced Resource Assignment** from the results, and click **Add Item**.

A properties screen displays.

c) Click **Add new entry**
A new line is added to the list of entries.

d) Click the **Add/Delete** link below the entry.
The screen changes to display resources on multiple tabs.

e) On the Remote Desktop tab, select the VMware View remote desktop resource that you configured previously.

f) On the Webtop tab, select a full webtop and click **Update**.
The properties screen closes and the resources you selected are displayed.

g) Click **Save**.
The properties screen closes and the visual policy editor is displayed.

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

a) Click the (+) sign before the previous VMware View Logon Page action.
A popup screen opens.

b) On the Logon tab, select **VMware View Logon Page**, and click **Add Item**.

A properties screen displays.

c) From the **VMware View Logon Screen Type** list, select **RSA SecurID**.

d) In the **VMware View Windows Domains** field, type the domain names to use for logon.

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

f) Click the plus (+) icon after the previous VMware View Logon Page action.
A popup screen opens.

g) On the Authentication tab, select **RSA SecurID**, and click **Add Item**.

h) From the **Server** list, select the AAA server that you created previously and click **Save**.
The properties screen closes.

9. (Optional) If you want to display a message to the user inside of the View Client (for example, a disclaimer or acceptable terms of use), this is how you do it:

a) Click the **(+)** sign anywhere in your access profile to add a new action item.

An Add Item screen opens, listing predefined actions on tabs such as General Purpose, Authentication, and so on.

b) On the Logon tab, select **VMware View Logon Page**, and click **Add Item**.
A properties screen displays.

c) From **VMware View Logon Screen Type**, select **Disclaimer**

d) In the Customization area from the **Language** list, select the language for the message.

e) In the **Disclaimer message** field, type the message to display on the logon page.

f) Click **Save**.
The properties screen closes and the visual policy editor is displayed.

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

10. On the fallback branch between the last action and **Deny**, select the **Deny** check box, click **Allow** and click **Save**.
11. Click **Apply Access Policy**.

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

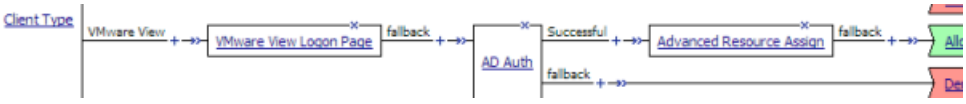


Figure 1: Example access policy with single-factor authentication for View Client

Figure 2: Example access policy with two-factor authentication for View Client

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

Creating a connectivity profile

You create a connectivity profile to configure client connections.

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

The connectivity profile appears in the list.

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

Creating a custom server SSL profile

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

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

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

Configuring an HTTPS virtual server for View Client authentication

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

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

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

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, select **Host** and in the **Address** field, type the IP address for the virtual server.
5. In the **Service Port** field, type `443` or select **HTTPS** from the list.
6. From the **HTTP Profile** list, select **http**.
7. For the **SSL Profile (Client)** setting, select a client SSL profile.
8. For the **SSL Profile (Server)** setting, from the **Available** list, select the name of the Server SSL profile you previously created and move the name to the **Selected** list.
9. From the **Source Address Translation** list, select **Auto Map**.
10. In the Access Policy area, from the **Access Profile** list, select the access profile.
11. From the **Connectivity Profile** list, select the connectivity profile.
12. Select the **VDI & Java Support** check box.
13. Locate the Resources area of the screen and from the **Default Persistence Profile** list, select one of these profiles:
    - **cookie** - This is the default cookie persistence profile. Cookie persistence is recommended.

- **source_addr** - This is the default source address translation persistence profile. Select it only when the cookie persistence type is not available.

14. Click **Finished**.

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

Configuring a UDP virtual server for PCoIP traffic

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

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

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

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

Configuring for virtual servers that use a private IP address

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

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

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. In the Access Policy column, click the **Edit** link for the access profile you want to configure 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 `var` in the search field, select **Variable Assign** from the results list, and click **Add Item**.
   The Variable Assign properties screen opens.
5. Click the **change** link next to the empty entry.
   A popup screen displays two panes, with Custom Variable selected on the left and Custom Expression selected on the right.

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

Chapter 3

Presenting a View Desktop on an APM Webtop

Overview: Accessing a View Desktop from an APM webtop

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

Note:

Access Policy Manager supports this implementation in APM version 11.4.0 (with hotfix 3) and later.

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

Task summary

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

About client requirements to launch View Client from a webtop

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

Note:

Access Policy Manager supports launching View Client from a dynamic webtop in APM version 11.4.0 (with hotfix 3) and later.

Creating a pool of View Connection Servers

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

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. In the Resources area, using the **New Members** setting, add each View Connection Server that you want to include in the pool:

a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
b) In the **Service Port** field, type `443` (if your View Connection Servers use HTTPS), or type `80` (if your View Connection Servers use HTTP).

   By default, View Connection Servers use HTTPS. However, if you configure your View Connection Servers for SSL offloading, they use HTTP.
c) Click **Add**.

5. Click **Finished**.

The new pool appears in the Pools list.

Configuring a VMware View remote desktop resource

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

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

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

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

   All other parameters are optional.

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

Configuring a full webtop

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

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

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

Creating an access profile

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

1. On the Main tab, click **Access Policy** > **Access Profiles**.
   The Access Profiles List screen opens.
2. Click **Create**.
   The New Profile screen opens.
3. Type a name for the access profile.
4. In the Language Settings area, add and remove accepted languages, and set the default language.

   A browser uses the highest priority accepted language. If no browser language matches the accepted languages list, the browser uses the default language.
5. Click **Finished**.

This creates an access profile with a default access policy.

Creating an access policy for a dynamic webtop

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

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

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

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

---

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

2. In the Access Policy column, click the **Edit** link for the access profile you want to configure 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.

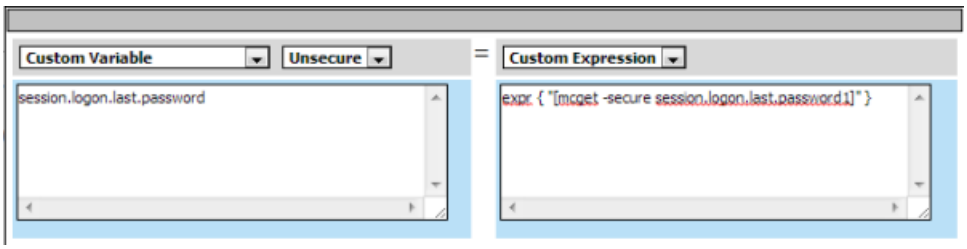
   To support Active Directory authentication only, no changes are required. To support both Active Directory and RSA SecurID authentication, an additional password field is required and the labels for the password fields require change.
   a) In the Logon Page Agent table row 3, for **Type**, select **password**.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

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

   The properties screen closes.

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

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



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

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

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

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

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

Assigning resources to the access policy

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

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

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

---

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

   A list of webtops is displayed.

10. Select a webtop and click **Update**.
    The screen changes to display properties and the name of the selected webtop is displayed.
11. Select **Save** to save any changes and return to the access policy.

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

Creating a connectivity profile

You create a connectivity profile to configure client connections.

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

The connectivity profile appears in the list.

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

Creating a custom server SSL profile

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

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

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

Configuring an HTTPS virtual server for a dynamic webtop

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

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

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

---

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

This virtual server handles access and handles XML protocol data.

Configuring a UDP virtual server for PCoIP traffic

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

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

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

9. Click **Finished**.

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

Configuring for virtual servers that use a private IP address

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

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

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

Chapter 4

Tips for Standalone View Client and Dynamic Webtop Integration

Example access policy for standalone View Client and View on webtop

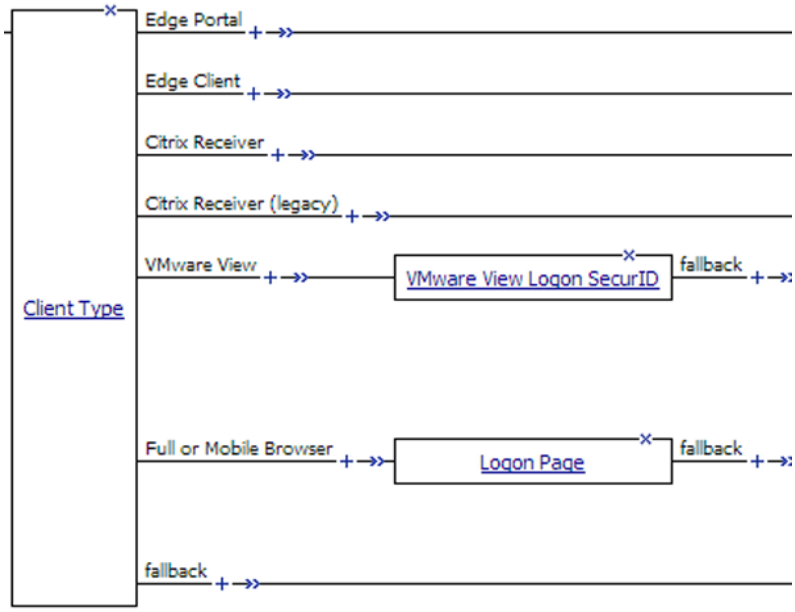
You can configure one access policy for access to standalone View Client and for launching View from a webtop by using the Client Type action in the access policy.

Note:

Access Policy Manager® (APM®) supports launching View from a webtop in APM version 11.4.0 (with hotfix 3) and later.

Client Type action branch rules

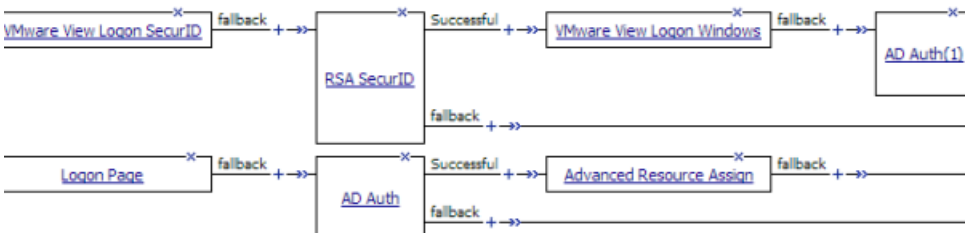
Place actions for the standalone View Client on the VMware View branch, and place actions for launching View from a dynamic webtop on the Full or Mobile Browser branch.



Example access policy continued: Logon and authentication

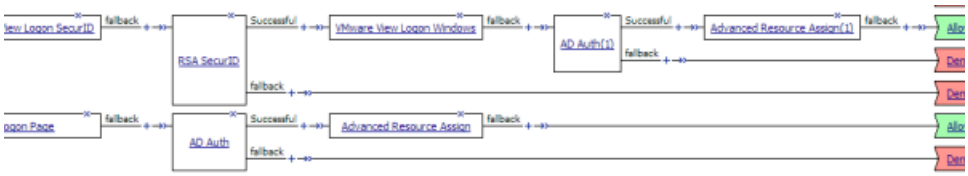
To support a standalone View Client, you must provide a VMware View Logon page and Active Directory authentication. (SecurID authentication is optional for a standalone View Client; if used, it must precede AD Auth.)

To support launching View from a webtop, you can provide a Logon Page and any authentication type.



Example access policy completed: Resource assignment

After successful authentication, you can assign resources to the session.



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

About a configuration for standalone View Client and View on webtop

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

Note:

Access Policy Manager supports starting View Client from a dynamic webtop in APM version 11.4.0 (with hotfix 3) and later.

Chapter 5

Configuring AAA Servers in APM

About VMware View and APM authentication types

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

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

Task summary

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

Configuring an Active Directory AAA server

Configuring a SecurID AAA server in APM

Configuring an Active Directory AAA server

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

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

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

Note: *The administrator name is case-sensitive.*

9. In the **Admin Password** field, type the administrator password associated with the Domain Name.
10. From the **Kerberos Preauthentication Encryption Type** list, select an encryption type.
    The default is **None**. If you specify an encryption type, the BIG-IP® system includes Kerberos preauthentication data within the first authentication service request (AS-REQ) packet.
11. In the **Timeout** field, type a timeout interval (in seconds) for the AAA server. (This setting is optional.)
12. Click **Finished** to add the new server to the configuration, and return to the main screen.

This adds the new Active Directory server to the AAA Server List.

Configuring a SecurID AAA server in APM

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

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

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

Index