Advanced Authentication 6.3

Virtual Desktop Authentication Agent Installation Guide

December 2019

Legal Notices

Contents

About this Book

This guide provides information about system requirements and how to install and configure the Virtual Desktop Authentication Agent on Windows.

Intended Audience

This guide is intended for the Advanced Authentication domain administrators.

About Virtual Desktop Authentication Agent

The Advanced Authentication Virtual Desktop Authentication Agent facilitates you to enable multi-factor authentication for the following desktop virtualization clients software:

- VMware Horizon (formerly known as VMware View)
- Microsoft Remote Desktop
- Citrix XenApp or XenDesktop

The Administrator can create profiles to access the different supported virtualization platforms and a user needs to choose a required profile and perform a pre-session multi-factor authentication. After authentication, the shared desktop or application starts automatically. Also, VDA supports a kiosk mode that can be used on workstations or thin clients where the user does not need to interact with local desktop to connect to remote resources.

For example, Sussane, who is an end-user uses the VMware Horizon client to access the office computer from home. She must perform multi-factor authentication using the Virtual Desktop Authentication agent to get secured access to the office computer.

1 System Requirements

For system requirements of Virtual Desktop Authentication agent, see Virtual Desktop Authentication Agent.

You must have the administrator privileges to install and uninstall the Virtual Desktop Authentication agent.

2 Configuring Preliminary Settings

This chapter contains sections about the pre-configuration settings for Virtual Desktop Authentication Agent.

Configuring the Mandatory Settings

The following are the mandatory settings for irtual Desktop Authentication Agent.

Setting a DNS for Advanced Authentication Server Discovery

You can configure a DNS to allow the Virtual Desktop Authentication agents to connect to the Advanced Authentication server through the DNS.

To configure the DNS for server discovery, perform the following tasks:

Adding a Host to DNS

1 Click **Start > Administrative Tools > DNS**.

2 In the DNS Manager, perform the following steps to add the A or AAAA host record and a PTR record:

2a Right-click your domain name, then click **New Host (A or AAAA)** under **Forward Lookup Zone** in the console tree.

2b Specify a DNS name for the Advanced Authentication Server in **Name**.

2c Specify the IP address for the Advanced Authentication Server in **IP address**.

You can specify the address in IP version 4 (IPv4) format (to add a host (A) resource record) or IP version 6 (IPv6) format (to add a host (AAAA) resource record).

2d Select **Create associated pointer (PTR) record** to create an additional pointer (PTR) resource record in a reverse zone for this host, based on the information that you have provided in **Name** and **IP address**.

Adding an SRV Record

For better load balancing, it is recommended to perform the following actions only for Advanced Authentication web servers.You need not create the records for Global Master, DB Master, and DB servers.

- Adding an SRV Record from a Primary Advanced Authentication Site
- Adding an SRV Record from Other Advanced Authentication Sites

---

NOTE: Ensure that the LDAP SRV record exists at the DNS server. If the record is not available, you must add it manually.

Adding an SRV Record from a Primary Advanced Authentication Site

To add an SRV record for the Advanced Authentication servers from a primary Advanced Authentication site (a site with the Global Master server), perform the following steps:

1. Right-click on a node with the domain name and click **Other New Records** in the **Forward Lookup Zones** of the console tree.
2. Select **Service Location (SRV)** from **Select a resource record type**.
3. Click **Create Record.**
4. Specify **_aav6** in **Service** of the **New Resource Record** window.
5. Specify **_tcp** in **Protocol**.
6. Specify **443** in **Port Number**.
7. Specify the Fully Qualified Domain Name (FQDN) of the server that is added in **Host offering this service**. For example, `authsrv.mycompany.com.service`.
8. Click **OK**.

Adding an SRV Record from Other Advanced Authentication Sites

1. Expand the preferred domain name node and select **_sites** in the **Forward Lookup Zones** of the console tree.
2. Right-click on the preferred site name and click **Other New Records**.
3. Select **Service Location (SRV)** from **Select a resource record type**.
4. Click **Create Record**.
5. Specify **_aav6** in **Service** of **New Resource Record** window.
6. Specify **_tcp** in **Protocol**.
7. Specify **443** in **Port Number**.
8. Specify the FQDN of the server that is added in **Host offering this service.** For example, `authsrv.mycompany.com`.
9. Click **OK**.

You must add a host and SRV records in DNS for all the authentication servers. The Priority and Weight values for different servers may vary. For a better load balancing, you must have records only for the Advanced Authentication web servers instead of records for Global Master, DB Master, and DB servers.

DNS Server Entries

The following table defines these elements available in an SRV record:

Element	Description
Domain	Domain name for which this record is valid. It ends with a dot.
Service	Symbolic name of an applicable service.
Protocol	Transport protocol of an applicable service. Typically, TCP or UDP.
Priority	Priority of the target host. The lower the value, the higher the priority.
Weight	A relative weight for records with the same priority. The higher the value, the higher the priority.
Port number	TCP or UDP port on which the service is located.
Target (Host offering this service)	Canonical hostname of the machine providing the service. It ends with a dot.

Configuring Authentication Server Discovery in Virtual Desktop Authentication Agent

You can configure server discovery in the Virtual Desktop Authentication agent by using the following parameters in the `config.properties` file:

Parameter	Description
`discovery.Domain`	DNS name of the domain.
`discovery.port`	Option to specify the port number for the client-server interaction.
`discovery.host`	Option to specify the DNS name or the IP address of an Advanced Authentication server.
`discovery.subDomains`	Lists additional sub domains separated by a semicolon.
`discovery.useOwnSite`	Set the value to `True` to use the local site (Windows Client only).
`discovery.dnsTimeout`	Set time out for the DNS queries. The default value is 3 seconds.
`discovery.connectTimeout`	Time out for the Advanced Authentication server response. The default value is 2 seconds.
`discovery.resolveAddr`	Set the value to `False` to skip resolving the DNS. By default, the value is set to `False` for Windows Client.
`discovery.wakeupTimeout`	Timeout after the operating system starts or resumes from sleep. The default value is 10 seconds.

Using a Specific Advanced Authentication Server in a Non-DNS Mode

You can achieve the following requirements with this setting:

- Enforce a connection to a specific workstation where the DNS is not available.
- Override a DNS based entry for a specific workstation and use the settings specified in the `config.properties` file.

In the `C:\ProgramData\NetIQ\VDA\config.properties` file, configure `discovery.host: <IP_address|domain_name>`.

For example, `discovery.host: 192.168.20.40` or `discovery.host: auth2.mycompany.local.`

You can specify multiple Advanced Authentication servers separated by a semicolon (;):

`discovery.hosts: aaf-1.domain.com;aaf-2.domain.com;....;aaf-n.domain.com`

You can specify a port number (optional parameter) for the client-server interaction: `discovery.port: <portnumber>`.

Configuring Optional Settings

The following table describes the optional settings that you can do for Virtual Desktop Authentication Agent.

Setting	Description
vmware.singleAutoConnect:False	To disable direct launching of single entitled desktop. For more informations, see"Disabling the Direct Launching of Single Entitlement." on page 12

Disabling the Direct Launching of Single Entitlement.

If user is entitled for only one VDI machine in VM Horizon, we skip the entitled desktop selection screen by default.

To disable the behavior and show the entitled desktop selection screen even if only one VDI machine is entitled for user, perform the following actions:

1. Open the file `C:\ProgramData\NetIQ\VDA\config.properties`.
2. Set the parameter `vmware.singleAutoConnect` to `False` (By default, the parameter is set to `True`).
3. Save the configuration file.

3 Installing and Uninstalling the Virtual Desktop Authentication Agent

This chapter contains the following sections:

- Installing the Virtual Desktop Authentication Agent
- Uninstalling the Virtual Desktop Authentication Agent

Installing the Virtual Desktop Authentication Agent

1. Run the file `naaf-vda-x86-release-<version>.msi` for a 32-bit operating system or `naaf-vda-x64-release-<version>.msi` for a 64-bit operating system.
2. Read and accept the **License Agreement** and click **Next**.
3. Click **Install**.
4. Click **Finish**.
5. Restart your machine.

Uninstalling the Virtual Desktop Authentication Agent

You can uninstall the Virtual Desktop Authentication agent in one of the following ways:

- Using Setup Wizard
- Using Control Panel

Using the Setup Wizard

1. Run the file `naaf-vda-x86-release-<version>.msi` for a 32-bit operating system or `naaf-vda-x64-release-<version>.msi` for a 64-bit operating system.
2. Click **Next**.
3. Select **Remove**.
4. Click **Remove** to confirm.

Using Control Panel

1. Click **Start > Control Panel > Programs and Features**.
2. Right click **NetIQ Virtual Desktop Authentication** and select **Uninstall**.
3. Click **OK**.

4 Configuring VDA Agent

You must complete the following tasks before using the Virtual Desktop Authentication agent for multi-factor authentication:

Configuring the Advanced Authentication Server

Before configuring the Virtual Desktop Authentication agent, you must configure **VDA** event to enable the multi-factor authentication for the virtual desktop client software.

1. Log in to the Advanced Authentication Administration portal.
2. Create a chain with the preferred authentication methods.
3. Create an event and set **Event type** as **OS Logon (domain)**.

   By default, the event name is **VDA**. If you need to customize the event name, specify the new name in the `event_name: <CustomEventName>` parameter in the configuration file. To open the configuration file, navigate to the following path:

   `C:\ProgramData\NetIQ\VDA\config.properties`
4. Assign the preferred chain from the **Available** list to the event.
5. Click **Save**.

Configuring VDA Profile Editor

You can configure the Virtual Desktop Authentication agent with the desktop virtualization client and server details to implement multi-factor authentication for the supported desktop virtualization software.

NOTE: The domain users can run `AAA.VDA.Shell.exe` on a domain or non domain-joined machine. The Profile Editor works only on a domain-joined machine.

General Settings

In the **General** tab, select the required desktop virtualization software from **Launcher**. The following are the available options:

- Citrix

- Microsoft RDP
- VMware View

IMPORTANT: While configuring the latest version of Citrix StoreFront that uses API 3.0, it is required to enable the **HTTP Basic** authentication in Citrix Studio - Citrix StoreFront - **Stores > Manage Authentication Methods** in the Actions pane. After configuring, wait for few minutes.

Kiosk Mode Settings

The Kiosk mode allows one application to run. In Kiosk mode, the remote session opens in a full-screen mode and it is not possible to switch outside the remote session. Kiosk mode settings are enabled by default. When Kiosk mode is enabled the VDA launches on a separate desktop. As a result, the VDA Shell and remote sessions are isolated from the operating system

You can configure the following settings in the **Kiosk Mode** tab:

Field	Description
VDA admins group	Members of VDA admins group can close the VDA shell. **NOTE:** Users who are not associated to admins group does not have the privilege to quit from VDA shell.
Quit hot-key	The Quit hot-key is a combination using which VDA admin can close the VDA shell. The default hot key is Control + Alt + Q. To set the quit hot-key as per your requirement, click the ... icon and then press preferred keys simultaneously. The minimum key combination that you can set as quit hot-key is two and the maximum key combination is three. For example, Control + A or Control + Shift + A.
Enable app filtering	Enable this option to prevent use of any applications except the whitelisted app when VDA shell is active. Specify the full path of the exe file of an application that you want to prevent users from using it. For example, `C:\Windows\System32\calc.exe`
Background image	Click the ... icon and select the image that you want to set as the background of the VDA agent login screen and click **Open**. The supported formats are BMP, JPG, JPEG, and PNG. It is recommended to place the image in the network path and save the path in profile or ensure the file is placed locally in the same folder on all clients. **NOTE:** Ensure the resolution of background image fits your desktop screen resolution.

Creating a VDA Profile

You can configure the Virtual Desktop Authentication agent with the desktop virtualization client and server details then create profile to implement multi-factor authentication for the supported desktop virtualization software.

You can create profile for the following desktop virtualization softwares:

- VMware View
- Citrix
- Microsoft RDP

Creating a Profile for VMware View

1. Launch the VDA.`Profile.Editor.exe` from the path `C:\Program Files\NetIQ\Virtual Desktop Authentication`.
2. In the **General** tab, select **VMware View** from **Launcher**.
3. In the **VMware View** tab, specify the following details:
   - **Server Name**: IP address or host name of VMware Horizon server.
   - **Startup Desktop**: Display name of the virtual machine that you want to launch after authenticating to VMware View client. This is optional.
4. Click **File > Save As** and select the preferred local directory to save the VMware view related details as a profile.
5. Specify **File name** and click **Save**.

   The file saves in the `.profile` format.
6. Close the **VDA Profile Editor**.

Creating a Profile for Citrix

1. Launch the VDA.`Profile.Editor.exe` from the path `C:\Program Files\NetIQ\Virtual Desktop Authentication`.
2. In the **General** tab, select **Citrix** from **Launcher**.
3. In the **Citrix** tab, perform one of the following:
   - Use StoreFront server

     The **Use StoreFront server** check box is selected by default to enable the following settings where you can manually specify the details:

     1. Specify the Store Front server URL in the http://<ip address or host name>/Citrix/StoreWeb/ format in **URL**.
     2. Retain the default version 2.5 in **API Version**.
     3. Select **Use Gateway** option to enable the use of gateway. This option is to be selected only when StoreFront is secured by Citrix NetScaler.
     4. Specify **Username** and **Password** required to log in to the Store Front and access the list of applicable resources.
     5. Click **Load** to view the resources applicable for specified user.

6. Select the preferred resource and click **Select**.

   The resource that you select appears under **Loaded resource**.

- Load ICA templates directly

  If you want to load the ICA template of Citrix StoreFront, select **Load ICA templates directly**. To upload the ICA template, click **Load**, select the `.ica` file and then click **Open**.

  To download and verify the configuration, click **Export**.

4 Click **File > Save As** and select the preferred local directory to save the Citrix StoreFront related details as a profile.

5 Specify **File name** and click **Save**.

  The file saves in the `.profile` format.

6 Close the **VDA Profile Editor**.

Creating a Profile for Microsoft RDP

Before you create a profile for Microsoft RDP, ensure to have the RDP file that contains connection setting of the remote computer. In case you do not have the RDP file, perform the following steps:

1 Launch mstsc from the **Run** dialog.

  The **Remote Desktop Connection** window is displayed.

2 Specify the IP address of remote computer in **Computer**.

3 Specify **User name** required to access the remote computer.

4 Click **Show Options**.

5 Click **Save As** in **Connection Settings**.

6 Select location and specify name to save the RDP file with all connection settings.

  For example: Win1

7 Click **Save**.

  The file is saved in the `.rdp` format.

To create a profile for Microsoft RDP in VDA agent, perform the following steps:

1 Launch the VDA`.Profile.Editor.exe` from the path `C:\Program Files\NetIQ\Virtual Desktop Authentication`.

2 In the **General** tab, select **RDP** from **Launcher**.

3 In the RDP tab, click **Load** and select the .rdp file that contains all connection settings to the remote computer.

4 Click **Open**.

  To download and verify the configuration, click **Export**.

5 Click **File > Save As** and select the preferred local directory to save Microsoft RDP related details as a profile.

6 Specify **File name** and click **Save**.

  The file saves in the `.profile` format.

7 Close the **VDA Profile Editor**.

Managing VDA Profiles

You can add a profile to **VDA Profiles list** and set one of the profile as default.

1. In the command prompt, run the following commands to launch the **VDA Profiles List** window:

   ```
   cd C:\Program Files\NetIQ\Virtual Desktop Authentication
   AAA.VDA.Shell.exe /manageProfiles
   ```

2. In the **VDA Profiles List** window, click **Add** and select the profile that you saved.
3. (Conditional) If you want to allow users to launch default profile without a prompt for selection, select the profile and click **Set as default**.
4. Close the **VDA Profiles List** window.

5 Troubleshooting

This chapter contains the following section on troubleshooting:

Debugging Logs for Advanced Authentication

With the Diagnostic Tool, you can check the network problems on a workstation, issues in connection between a workstation and DNS Server, and to get a list of the Advanced Authentication servers that can be discovered. To identify Advanced Authentication server, perform the following steps:

NOTE: As a prerequisite, ensure that `DiagTool.exe` file is available with the following files in the same directory:

- `DiagTool.exe.config`
- `Ionic.Zip.dll`
- `JHSoftware.DNSClient.dll`

---

1. Run `DiagTool.exe` (the tool must have Microsoft .NET Framework 3.5 installed).
2. Click **Servers**.
3. In the **Search settings**, specify the domain name in **Domain** to find a list of Advanced Authentication servers in the specified domain.

   If you want to find particular server then clear **Use system DNS server** and specify the IP address of the DNS server in **DNS server**.
4. Select **Use v6 DNS lookup** to allow the Diagnostic tool to find the Advanced Authentication server using `_aav6` records.

   If you want to find the Advanced Authentication server using `_aaa` records, clear **Use v6 DNS lookup**.
5. Click **Search**.

NOTE: If you configure the IP address of the Advanced Authentication server in the DNS service record, the Diagnostic tool cannot find and retrieve the respective record. Ensure that you configure the DNS service record with the Fully Qualified Domain Name (FQDN) to enable the Diagnostic tool to find and retrieve the respective record.

You can collect the logs for Advanced Authentication in the following ways:

- Using a Diagnostic Tool
- Manual

Using a Diagnostic Tool

1. Run `DiagTool.exe`. The tool must have Microsoft .NET Framework 3.5 installed.
2. Click **Clear All** (if applicable) in the **Debug logs** tab.
3. Click **Enable**.
4. Restart the Windows operating system.
5. Reproduce your problem.
6. Run `DiagTool.exe`.
7. Click **Save logs** in the **Debug logs** tab.
8. Specify a file name and path.
9. Click **Save** to save the logs.
10. Click **Disable** to disable the logging.
11. Click **Clear All**.

Manual

1. Create a text file `C:\ProgramData\NetIQ\Logging\config.properties.`
2. Add a string to the file: `logEnabled=True` that ends by a line break.
3. Create a directory: `C:\ProgramData\NetIQ\Logging\Logs\`.
4. Restart the machine.
5. Reproduce your problem.
6. Pack the logs located in `C:\ProgramData\NetIQ\Logging\Logs\` into a zip file.
7. Change `logEnabled=True` to `logEnabled=False` in the folder, `C:\ProgramData\NetIQ\Logging\config.properties`.