



NetIQ Advanced Authentication
Framework - Virtual Desktop
Authentication (VDA) Shell

User's Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	3
About This Document	3
Managing NetIQ Advanced Authentication Framework Virtual Desktop	
Authentication Shell	4
Pre-Session Authentication	5
Card Authentication	6
FIDO U2F Authentication	7
Fingerprint Authentication	8
OATH TOTP Authentication	10
In-Session Authentication	12
Card Authentication	13
Fingerprint Authentication	14
OATH TOTP Authentication	16
Index	18

Introduction

About This Document


Purpose of the Document


This Virtual Desktop Authentication Shell User's Guide is intended for all user categories and describes how to use NetIQ Advanced Authentication Framework VDA Shell.

For more information about NetIQ Advanced Authentication Framework software, see NetIQ Advanced Authentication Framework Administrative Tools - Administrator's Guide.


Document Conventions

This document uses the following conventions:

 **Warning.** This sign indicates requirements or restrictions that should be observed to prevent undesirable effects.


 **Important notes.** This sign indicates important information you need to know to use the product successfully.


 **Notes.** This sign indicates supplementary information you may need in some cases.

 **Tips.** This sign indicates recommendations.

- Terms are italicized, e.g.: ***Authenticator***.
- Names of GUI elements such as dialogs, menu items, and buttons are put in bold type, e.g.: the **Logon** window.

Managing NetIQ Advanced Authentication Framework Virtual Desktop Authentication Shell

 To change profile for VDA Shell on the thin client, to display the profile selection dialog and to save changes in the registry, execute NAAF VDA Shell (which is located in C:\Program Files\NetIQ\NetIQ Advanced Authentication Framework\) with **/manageProfiles** parameter. This action requires **Local Admins** privileges.

 To open the profile selection dialog for one session only, execute NAAF VDA Shell with **/showProfiles** parameter.


NetIQ VDA Shell allows using 2 methods of authentication:

- [pre-session authentication](#)
- [in-session authentication](#)

Pre-Session Authentication

Pre-session authentication starts before the remote session is started. NetIQ VDA Shell application on the thin client does the authentication using NetIQ Advanced Authentication Framework – Web Service and then starts the remote session. VDI environment has a Broker that decides what to do with a request.

It is required to check if there is already a disconnected session and then reconnect the user to it. This works with pre-session method of authentication because the session is actually started with the user credentials and the broker knows which user it is.

To start the pre-session authentication, run the **NAAF.VDA.Shell** application that is marked with the following icon  and appears in NetIQ distributive kit after the installation of the VDA Shell on the Client. The NetIQ VDA Profile List window will be displayed. Click **Load** to start using it.

The authentication window will be displayed.

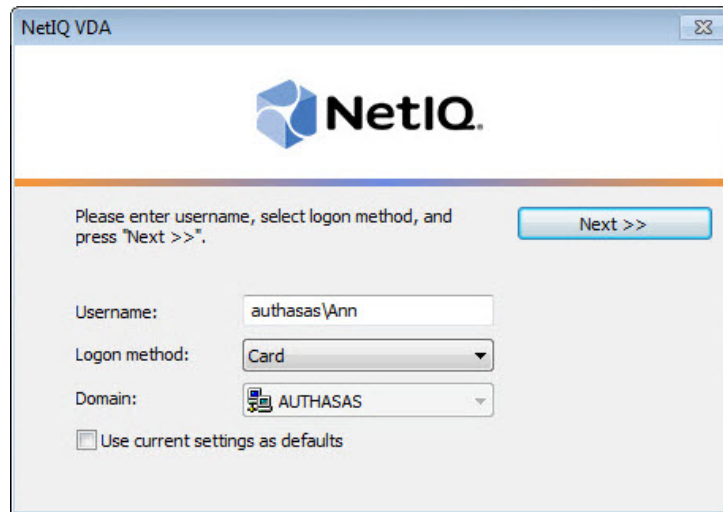
Pre-session authentication supports the following logon methods:

- [Card authentication](#)
- [FIDO U2F authentication](#)
- [Fingerprint authentication](#)
- [OATH OTP authentication](#)

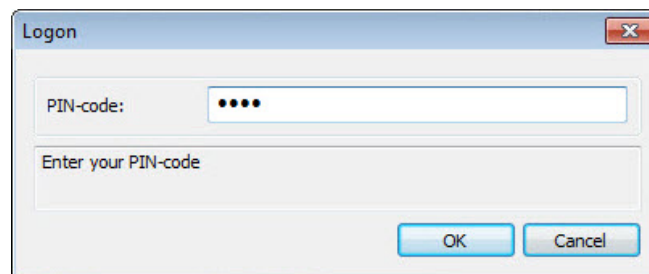
In the **Username** field it is required to enter the **Domain** name before the username. The user is not located in the domain during the pre-session authentication.

Card Authentication

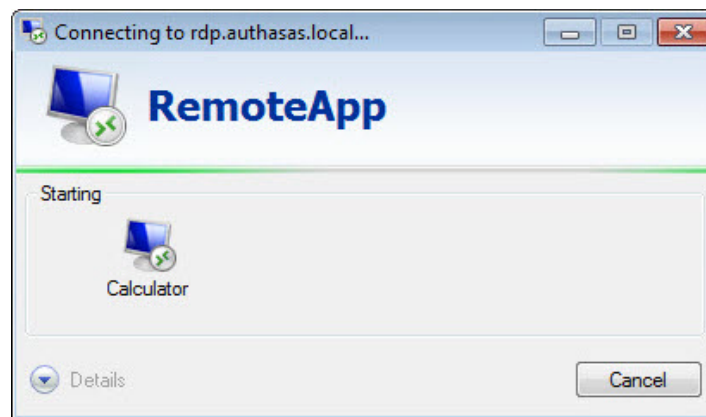
1. Select **Card** as the **Logon method** in the authentication window.



2. After tapping a card, enter the PIN-code in the **Logon** window.

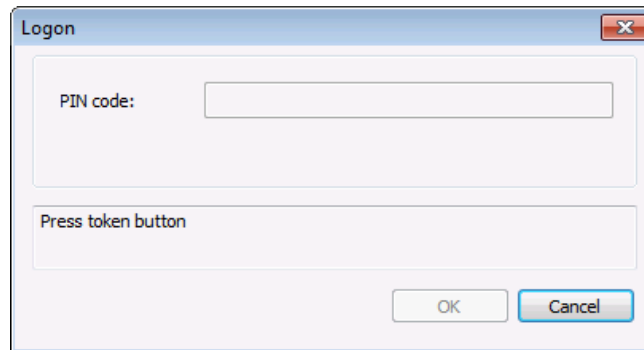


3. The remote session starts.

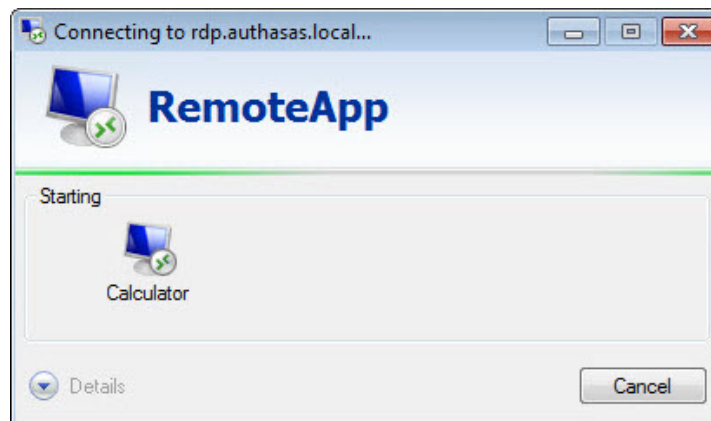


FIDO U2F Authentication

1. Select **FIDO U2F** as the **Logon method** in the authentication window.
2. Enter the PIN code in the **Logon** window and press the token button.

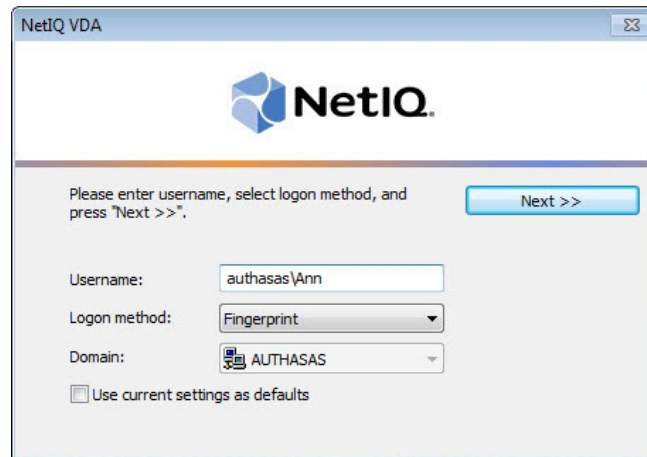


3. The remote session starts.

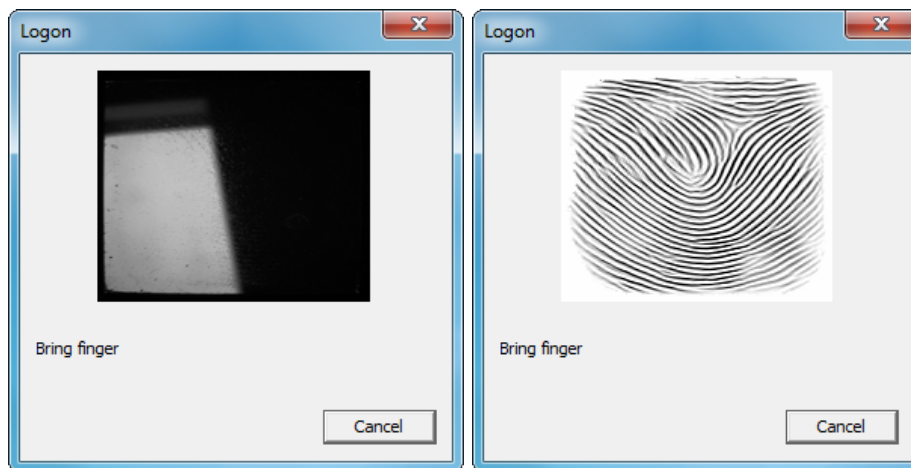


Fingerprint Authentication

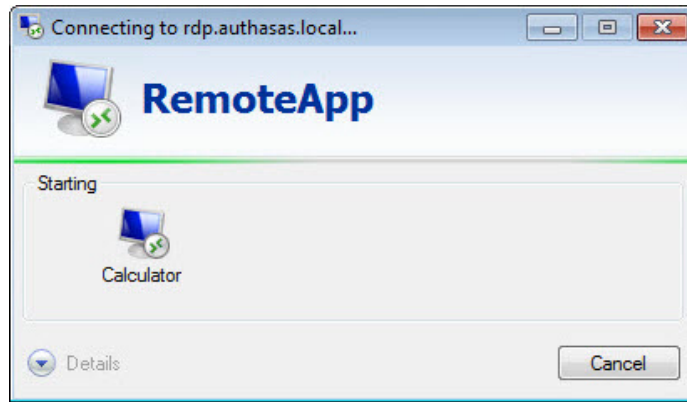
1. Select **Fingerprint** as the **Logon method** in the authentication window.



2. Place the finger on the reader until the wizard gives you confirmation.

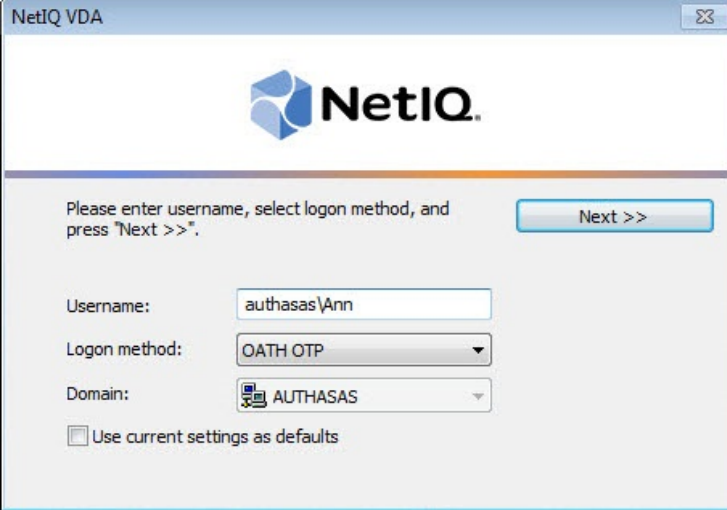


3. The remote session starts.



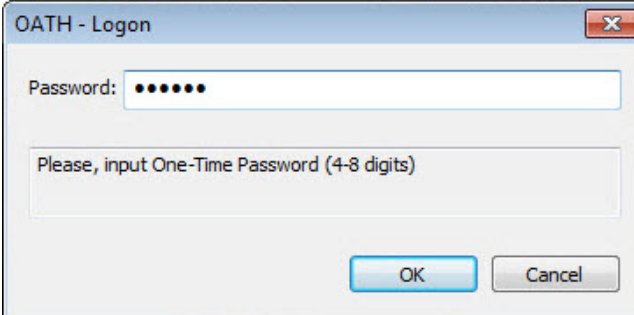
OATH TOTP Authentication

1. Select **OATH OTP** as the **Logon method** in the authentication window.



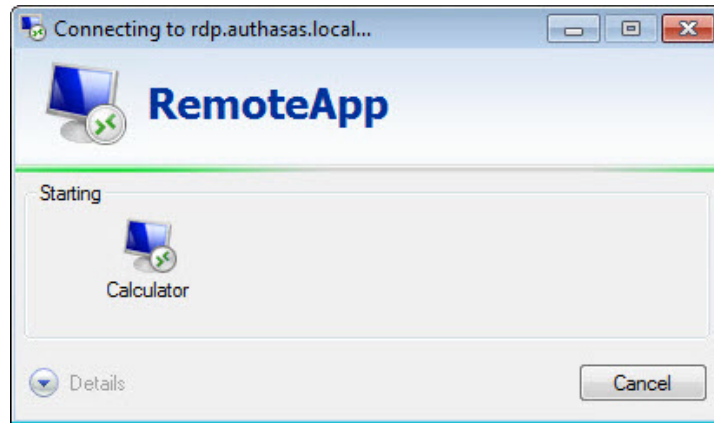
The screenshot shows the NetIQ VDA authentication window. At the top, it displays the NetIQ logo. Below the logo, there is a prompt: "Please enter username, select logon method, and press 'Next >>'." To the right of this prompt is a "Next >>" button. Below the prompt, there are three input fields: "Username:" with the value "authasas\Ann", "Logon method:" with a dropdown menu set to "OATH OTP", and "Domain:" with a dropdown menu set to "AUTHASAS". At the bottom left, there is a checkbox labeled "Use current settings as defaults" which is currently unchecked.

2. Enter the password in the **OATH - Logon** window.



The screenshot shows the "OATH - Logon" window. It has a title bar with a close button. The main area contains a "Password:" label followed by a text box filled with seven black dots. Below this is a larger text box with the prompt "Please, input One-Time Password (4-8 digits)". At the bottom right, there are two buttons: "OK" and "Cancel".

3. The remote session starts.



In-Session Authentication

In-session method of authentication is used to authenticate after the start of the remote session in VMware View, Citrix XenApp or Microsoft RDP. With in-session authentication the session is already setup.

If the session is hard-coded to a specific remote server, then inside the session the user will do authentication to the windows logon. The credentials will be sent to the NetIQ Advanced Authentication Framework - Client or RTE inside the session. The user will be authenticated successfully.

After the start of the remote session in VMware View, Citrix XenApp or Microsoft RDP, the in-session authentication will be started. The authentication window will be displayed.

In-session authentication supports the following logon methods:

- [Card authentication](#)
- [Fingerprint authentication](#)
- [OATH OTP authentication](#)

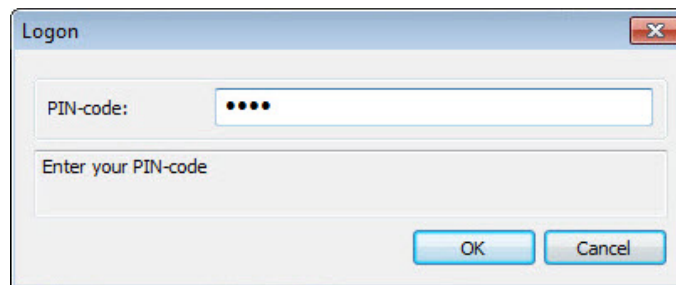
Enter the **Username** in the **Username** field. The user is located in the domain during the in-session authentication.

Card Authentication

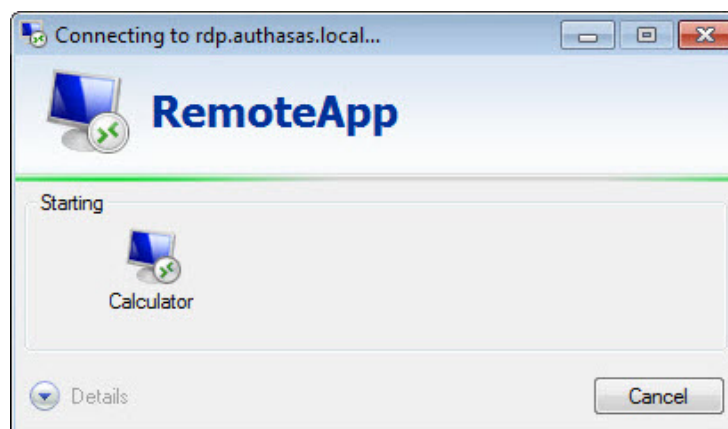
1. Select **Card** as the **Logon method** in the authentication window.



2. After tapping a card, enter the PIN-code in the **Logon** window.

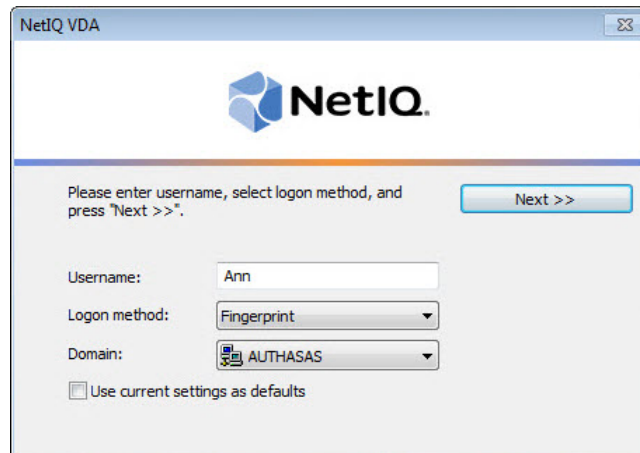


3. The remote session starts.

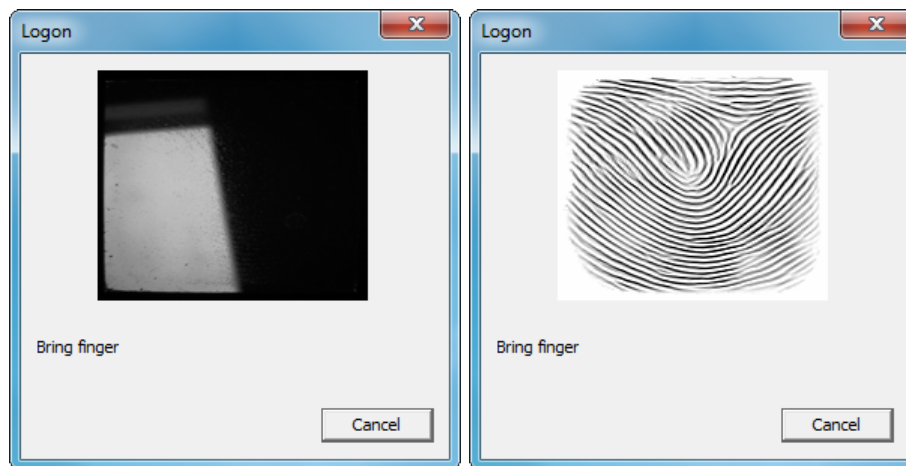


Fingerprint Authentication

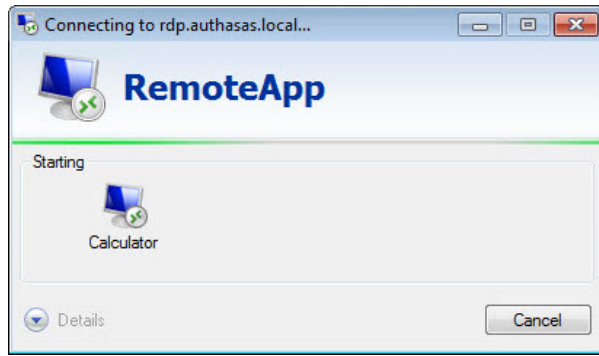
1. Select **Fingerprint** as the **Logon method** in the authentication window.



2. Place the finger on the reader until the wizard gives you confirmation.



3. The remote session starts.



OATH TOTP Authentication

1. Select **OATH OTP** as the **Logon method** in the authentication window.

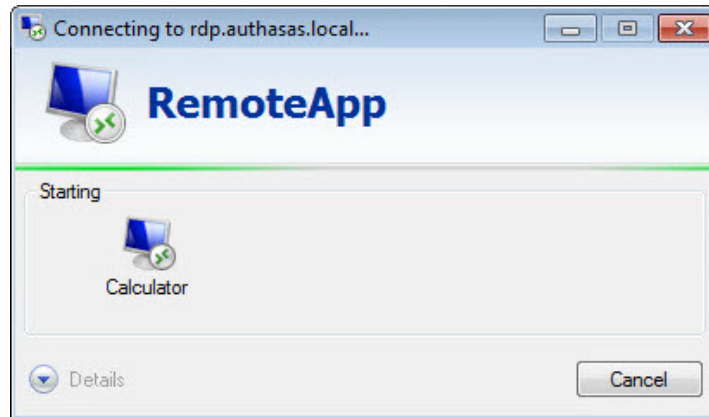
The image shows two screenshots of authentication windows. The top window is titled "Authasas VDA" and features the Authasas logo with the tagline "WE MAKE AUTHENTICATION WORK". Below the logo, it prompts the user to "Please enter username, select logon method, and press 'Next >>'". The "Username" field contains "Ann". The "Logon method" dropdown menu is set to "OATH OTP". The "Domain" dropdown menu is set to "AUTHASAS". There is a checkbox for "Use current settings as defaults" which is unchecked. A "Next >>" button is located to the right of the instructions.

The bottom window is titled "NetIQ VDA" and features the NetIQ logo. It has the same layout and content as the Authasas VDA window, including the "Username" field with "Ann", "Logon method" set to "OATH OTP", "Domain" set to "AUTHASAS", and the "Use current settings as defaults" checkbox.

2. Enter the password in the **OATH - Logon** window.

The image shows a screenshot of the "OATH - Logon" window. It has a title bar with a close button. The window contains a "Password:" label followed by a text input field with six dots. Below this is a larger text input field with the prompt "Please, input One-Time Password (4-8 digits)". At the bottom of the window, there are two buttons: "OK" and "Cancel".

3. The remote session starts.



Index

A

Administrator 3
Authentication 1, 3-5, 7, 12
Authenticator 3

C

Card 5-6, 12-13
Client 5, 12

D

Desktop 1, 3-4
Domain 5

F

Fingerprint 5, 8, 12, 14

L

List 5
Local 4
Logon 3, 6-8, 10, 13-14, 16

O

OATH 5, 10, 12, 16
OTP 10, 16

P

PIN 7
PIN-code 6, 13

U

User 1
Username 5, 12