# 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

Fingerprint Authentication ..... 7

OATH TOTP Authentication ..... 9

In-Session Authentication ..... 11

Card Authentication ..... 12

Fingerprint Authentication ..... 13

OATH TOTP Authentication ..... 15

**Index** ..... **17**

**Contacts and Further Help** ..... **18**




© NetIQ

# 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.



© NetIQ

# Managing NetIQ Advanced Authentication Framework Virtual Desktop Authentication Shell

To change profile for VDA Shell on the thin client, execute NAAF VDA Shell (which is located in C:\Program Files\NetIQ\NetIQ Advanced Authentication Framework\) with **/manageprofiles** parameter.

NetIQ VDA Shell allows using 2 methods of authentication:

- pre-session authentication
- in-session authentication

These methods of authentication are used for the following terminal server connections on thin clients:

- Microsoft RDP 7.1/8.0;
- Citrix XenApp 6.5;
- VMware View 5.0.



© NetIQ

## 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
- Fingerprint authentication
- OATH OTP authentication

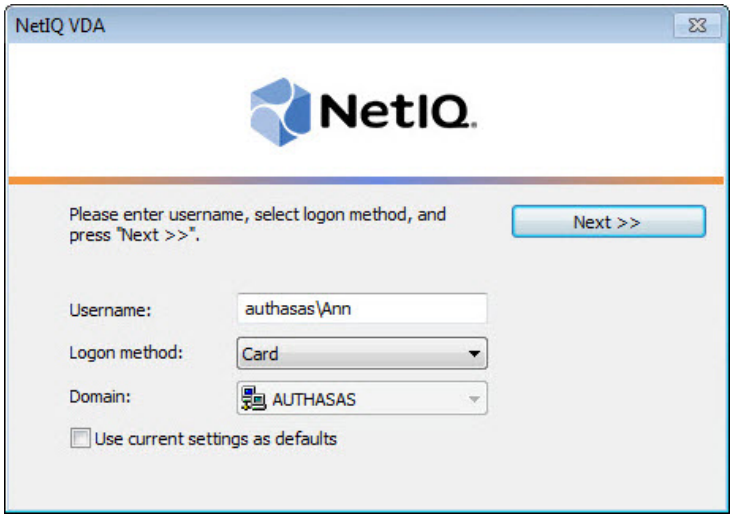
In the **Username** field it is required to enter the **Domain** name before the username. The user is not located in the domain during the pre-session authentication.



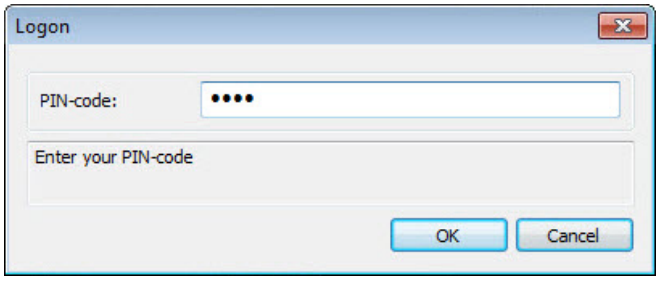
© NetIQ

## Card Authentication

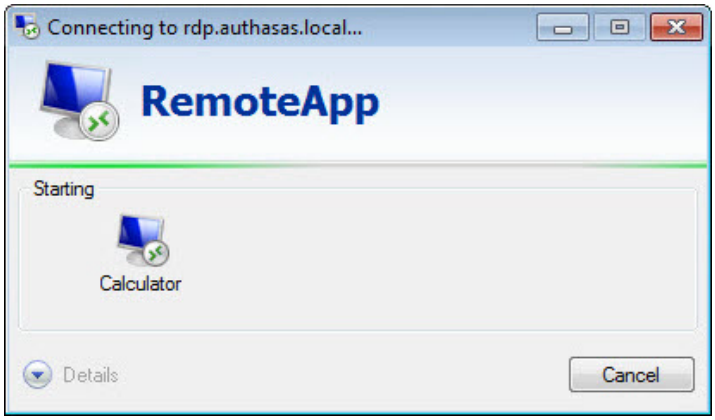
1. Select the required **Logon method** in the authentication window:




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




3. The remote session starts:



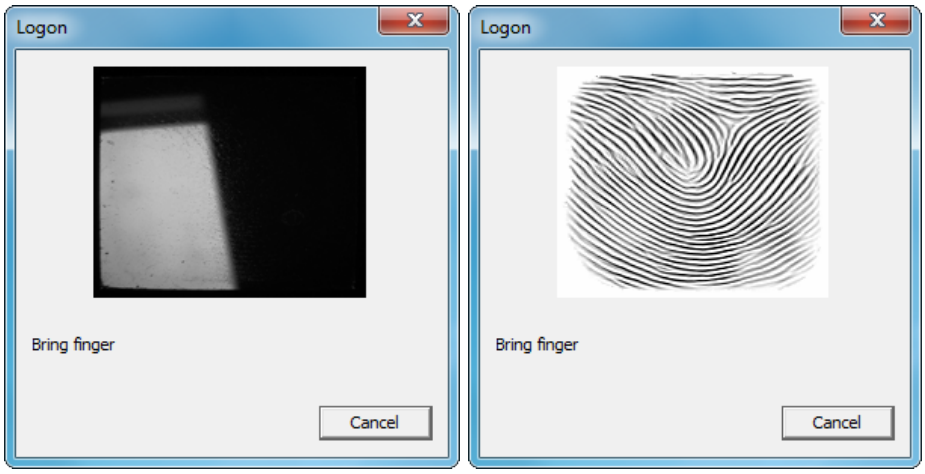



© NetIQ

## Fingerprint Authentication

1. Select the required **Logon method** in the authentication window:

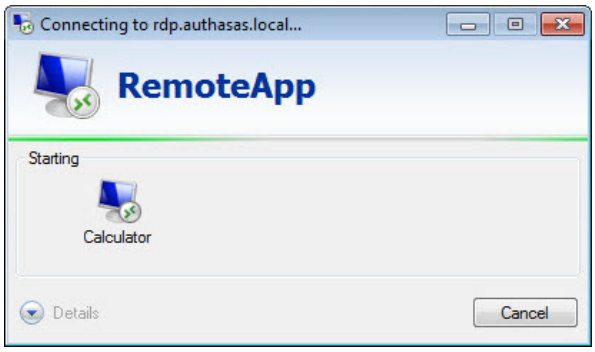
2. Place the finger on the reader until the wizard gives you confirmation.




3. The remote session starts:



© NetIQ

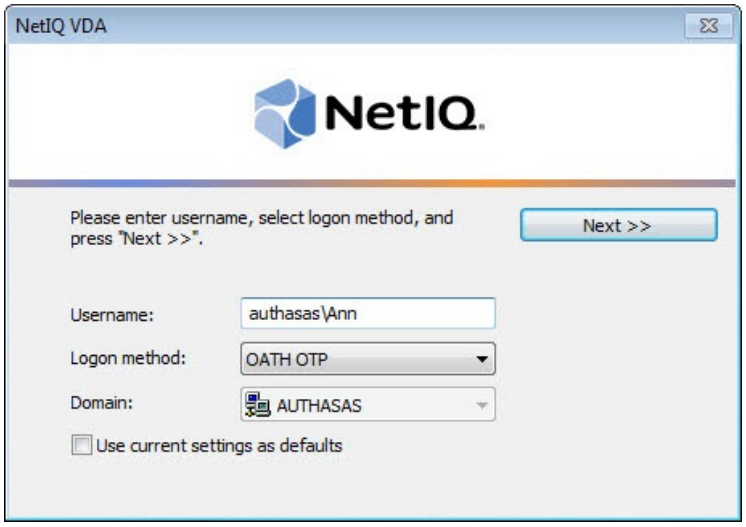

Connecting to rdp.authasas.local...
RemoteApp
Starting
Calculator
Details
Cancel



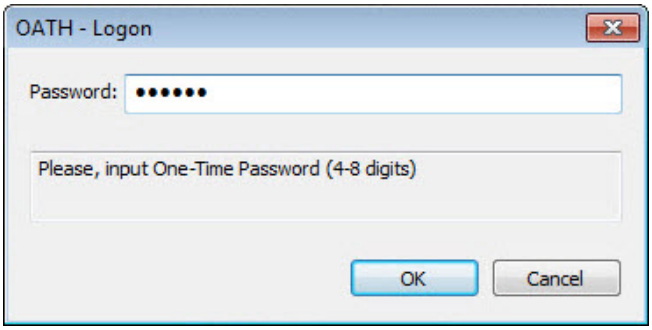
© NetIQ

## OATH TOTP Authentication

1. Select the required **Logon method** in the authentication window:



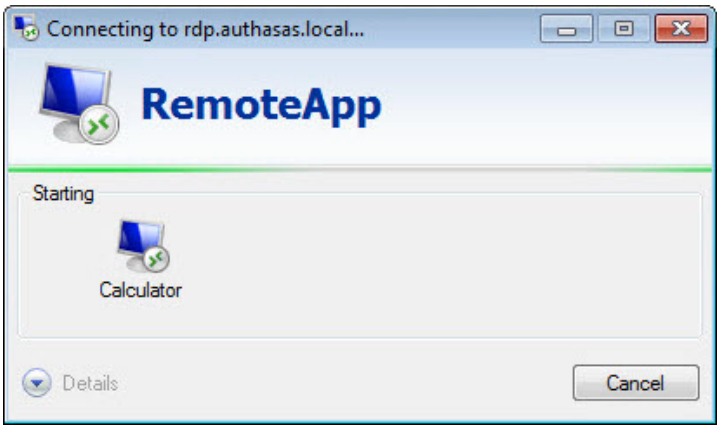

2. Enter the password in the **OATH - Logon** window:




3. The remote session starts:



© NetIQ


Connecting to rdp.authasas.local...
RemoteApp
Starting
Calculator
Details
Cancel



© NetIQ

## 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.

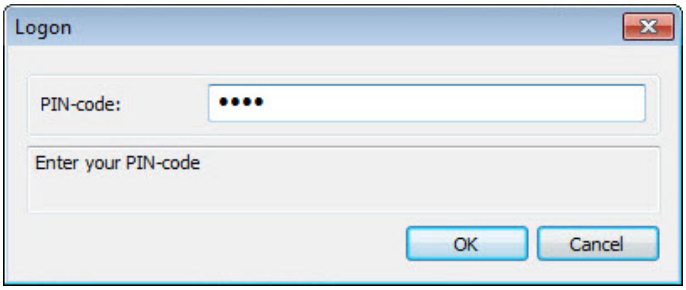


© NetIQ

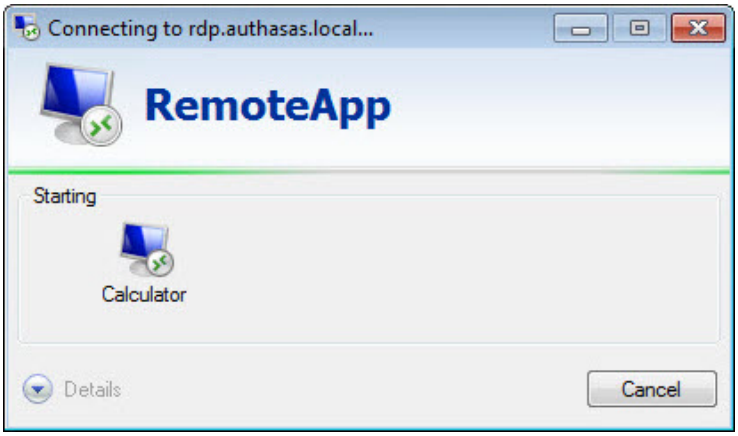
## Card Authentication

1. Select the required **Logon method** in the authentication window:

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




3. The remote session starts:

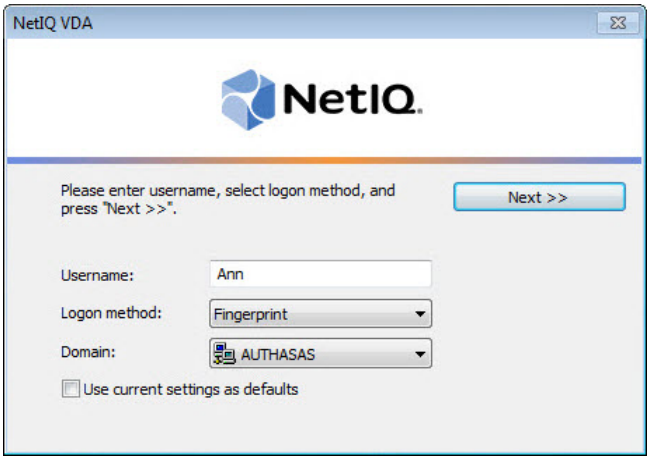




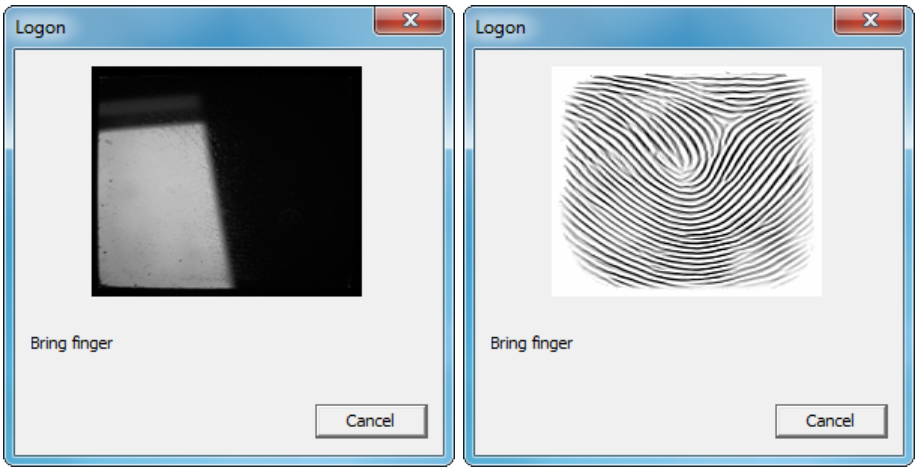

© NetIQ

## Fingerprint Authentication

1. Select the required **Logon method** in the authentication window:



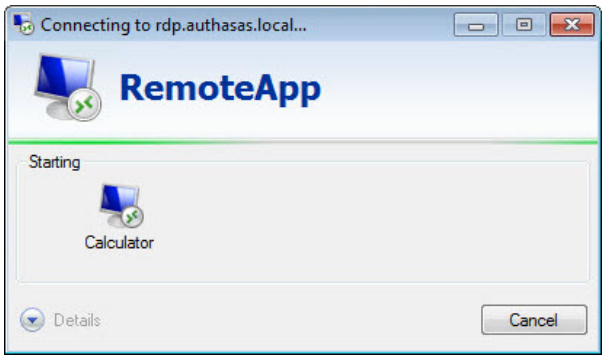

2. Place the finger on the reader until the wizard gives you confirmation.




3. The remote session starts:



© NetIQ

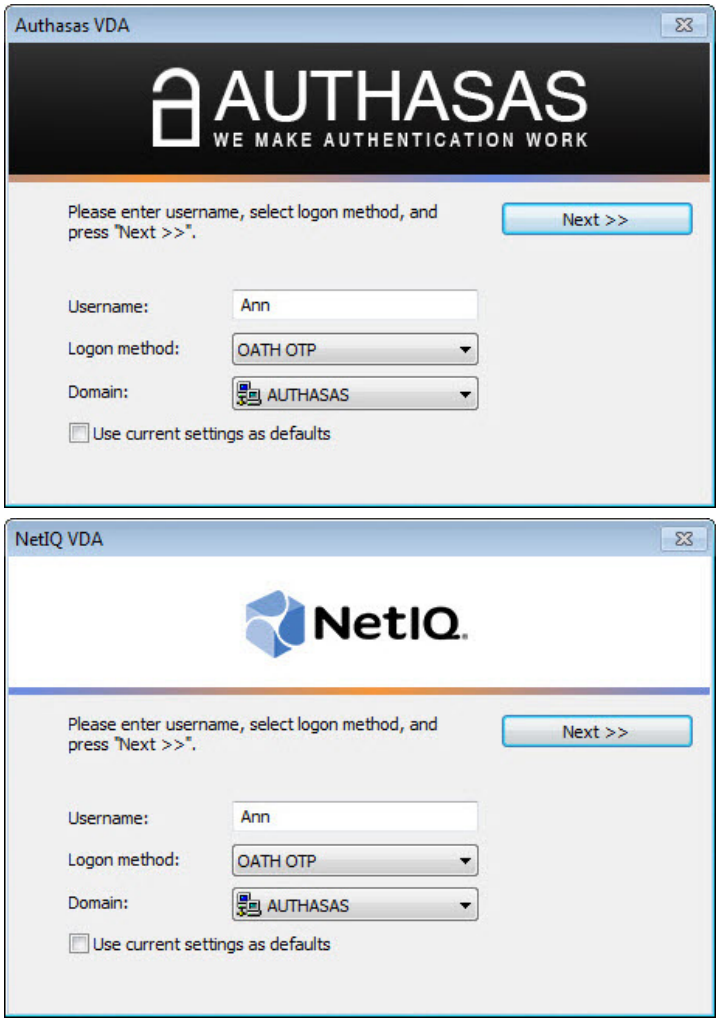

Connecting to rdp.authasas.local...
RemoteApp
Starting
Calculator
Details
Cancel



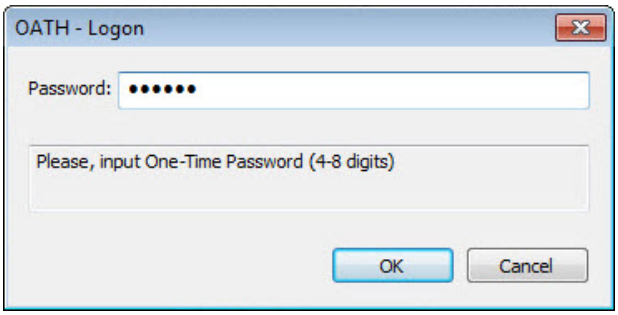
© NetIQ

## OATH TOTP Authentication

1. Select the required **Logon method** in the authentication window:



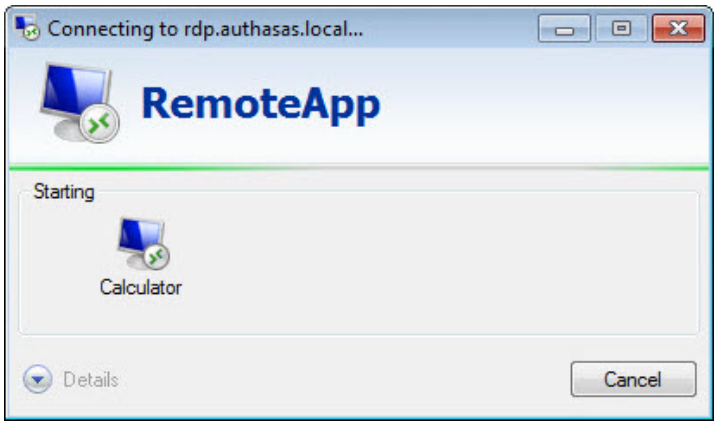

2. Enter the Password in the **OATH - Logon** window:






© NetIQ

3. The remote session starts:






© *NetIQ*

# Index


**A**

Administrator 3
Authentication 1, 3-5, 11
Authenticator 3

**C**

Card 5-6, 11-12
Client 5, 11

**D**

Desktop 1, 3-4
Domain 5

**F**

Fingerprint 5, 7, 11, 13

**L**

List 5
Logon 3, 6-7, 9, 12-13, 15

**O**

OATH 5, 9, 11, 15

**P**

Password 15
PIN-code 6, 12

**U**

User 1
Username 5, 11




© *NetIQ*

# Contacts and Further Help



© NetIQ