Authlogics Remote Desktop Agent Integration Guide

With PINgrid, PINphrase & PINpass Technology

Product Version: 3.0.6231.0

Publication date: January 2017

Authlogics, 12th Floor, Ocean House, The Ring, Bracknell, Berkshire, RG12 1AX, United Kingdom
UK Tel: +44 1344 568 900 US Tel: +1 857 214 2174 email: info@authlogics.com web: http://authlogics.com/

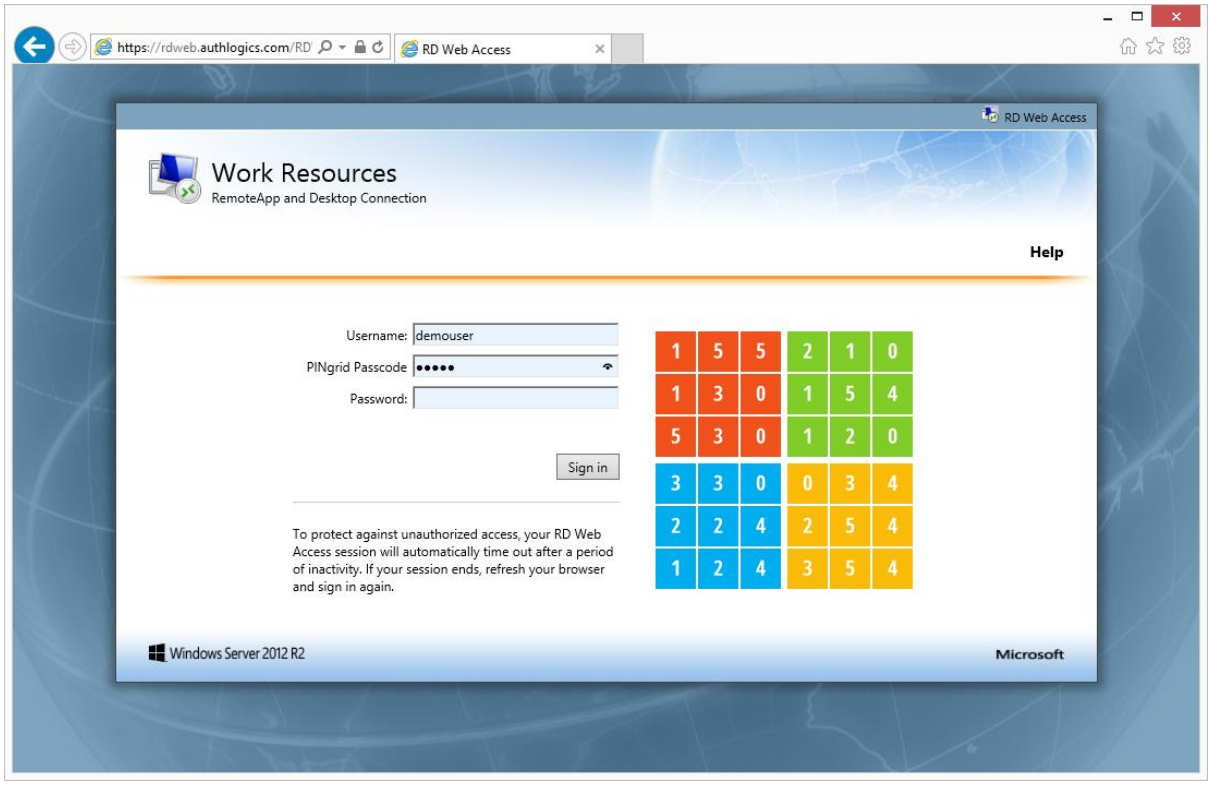
Table of Contents

Introduction

Authlogics Authentication Server is a multi-factor authentication system which provides:

- Token and token-less multi-factor authentication.
- Award winning transaction signing / verification technology.
- Self-service password reset and unlocking.
- Web Service API and RADIUS interfaces for connectivity.
- Authentication technologies:
    - PINgrid Pattern Based Authentication.
    - PINphrase Random Character Authentication
    - PINpass OATH (TOTP) Compliant Authentication

This guide includes details for integrating Authlogics with Windows Remote Desktop Services via the Remote Desktop web interface. Integrating Authlogics with Remote Desktop Services is an ideal way to add strong authentication to the Remote Services access method.



Licensing

Authlogics Remote Desktop Agent is licensed on a per server basis with each Server requiring a licence. A licence must be purchased for each server the agent is installed onto.

> **Note**
> For detailed information on the licence types please refer to the licence agreement document embedded within the installation package.

Design and Deployment Scenarios

The Authlogics Remote Desktop Agent has been designed to be installed directly onto the Remote Desktop Gateway server hosting the web based logon page.

The installation will update the existing web logon pages with modified versions to add support for Authlogics strong authentication.

Deployment

The following deployment overview walks through the installation process for deploying the Authlogics Remote Desktop Agent.

Overview

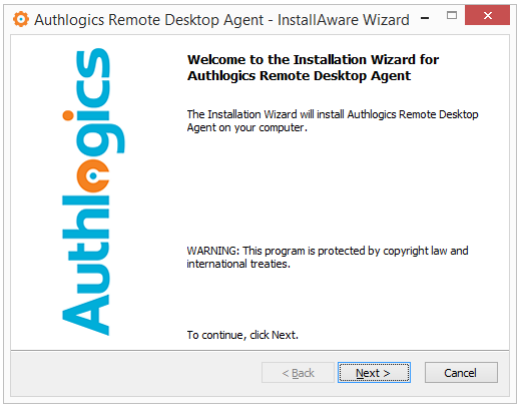
This deployment section assumes that at least one Authlogics Authentication Server has already been installed and is functional. See the Authlogics Authentication Server Installation and Configuration guide for further information on setting up the Authlogics Authentication Server. In addition, Authlogics user accounts should already be configured for users.

Installing/Removing the Authlogics Remote Desktop Agent

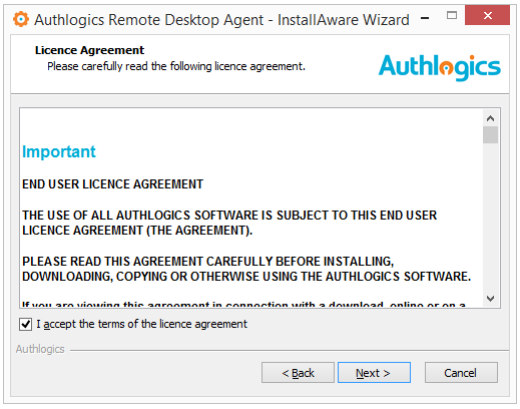
The installation should be performed on the server running the Remote Desktop Web Access role.

Running an installation

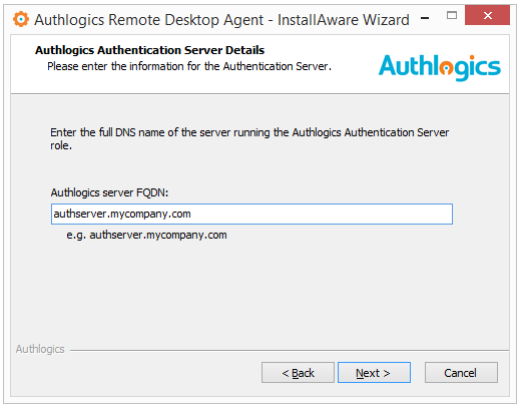
(1) To start the Authlogics Windows Desktop Logon Agent installation, run the *Authlogics Remote Desktop Agent xxxxx.exe* installer with **elevated privileges**.



(2) Click *Next* to begin the install or *Cancel* to quit.

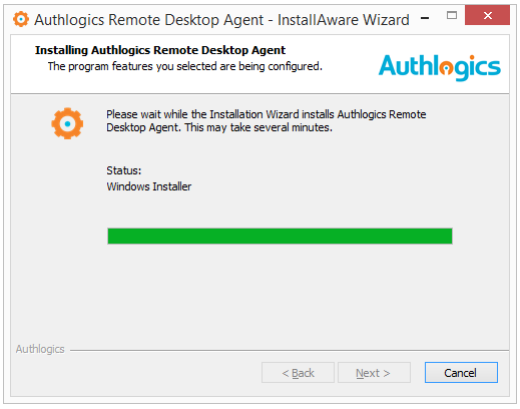


(3) Review the Authlogics Licence Agreement, check the *I accept the terms of the licence agreement* box and click *Next*.

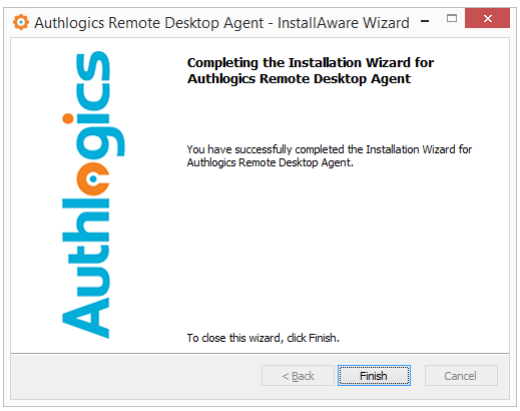


(4) Enter the FQDN of the Authlogics Authentication Server, click *Next*.

(5) Click *Next* to begin the install or *Cancel* to quit.



The installation is being performed.



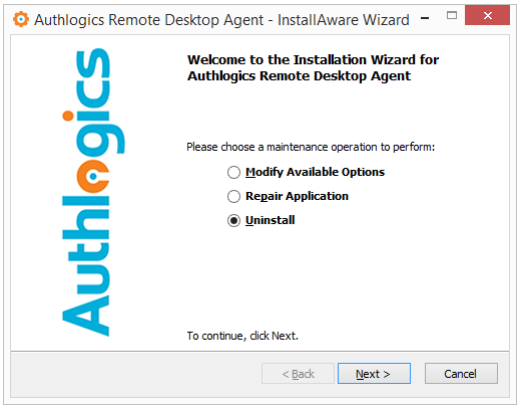
(6) All necessary Authlogics Remote Desktop Agent files have been installed. Click *Finish* to complete the installation process.

Running a removal

Uninstalling the Authlogics Remote Desktop Agent does NOT remove the metadata from user accounts in the Active Directory.

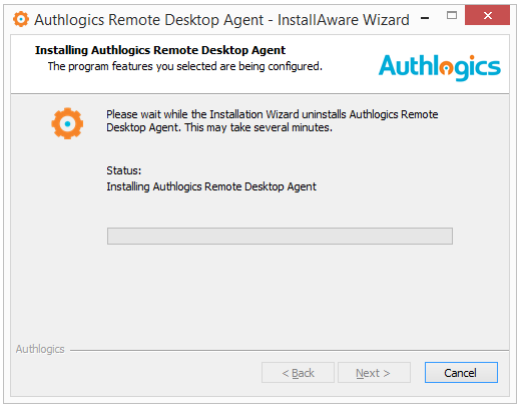
If you no longer require Authlogics Remote Desktop Agent on a server, you can remove it by performing an uninstall as follows:

(1) To start the Authlogics Remote Desktop Agent un-installation, execute the *Authlogics Remote Desktop Agent xxxxx.exe* installer or use the *Uninstall or change a program* option in Control Panel and click *Remove*.

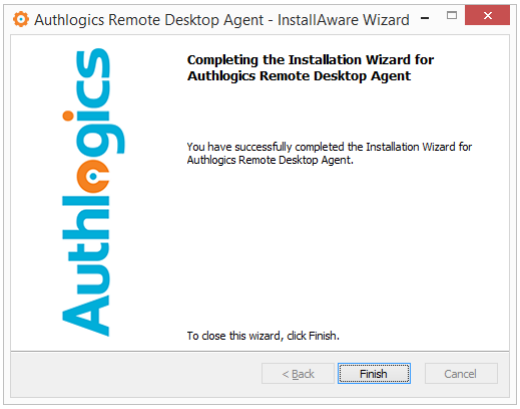


(2) Select *Uninstall.* Click *Next* to continue.

(3) Click *Next* to continue.



(4) The Authlogics uninstall will remove configured components.



(5) Click *Finish* to complete the uninstall process.

Configuring the Authlogics Remote Desktop Agent

Once the agent has been installed, there are a few settings that can be modified to change the configuration of the agent. These reside in a web.config file located in the following directory.

```
C:\Windows\Web\RDWeb\Pages\en-US
```

The default web.config settings are as follows:

```
<?xml version="1.0"?>
<configuration>
  <appSettings>

    <!-- Sets whether or not RDWeb will use Private Mode or not. Set to true or false.
         Default: true -->
    <add key="PrivateMode" value="false"/>

    <!-- Fill in the default domain name to enable users to login with just their username
         Default: blank -->
    <add key="DomainName" value=""/>

    <!-- Default ports: HTTP = 14000, HTTPS = 14443. -->
    <add key="AuthenticationServerPort" value="14000"/>

    <!-- Valid values for PinTechnology are "PINgrid", "PINphrase", "PINpass" -->
    <add key="AuthenticationType" value="PINgrid"/>

    <!-- Use SSL encryption when connecting to the Authlogics Authentication Server. NB: Ensure to set the correct
           "AuthenticationServerPort" value. -->
    <add key="EnableSSL" value="false"/>
    <!-- When using SSL use a DNS name that matches the Common Name of the SSL certificate. -->

    <!-- Enable the display of a 1.5 factor challenge on the logon page. -->
    <add key="WebBasedChallengeEnabled" value="true"/>

    <!-- The DNS FQDN of the Authlogics Authentication Server -->
    <!-- This key is added dynamically by the Installer -->
    <add key="AuthenticationServer" value="server.mycompany.com"/>
  </appSettings>
</configuration>
```