Authlogics

Authlogics Remote Desktop Agent Integration Guide

With PINgrid, PINphrase & PINpass Technology

Product Version: 4.1.3000.0

Publication date: June 2022

Call us on: +44 1344 568 900 (UK/EMEA)
+1 408 706 2866 (US)

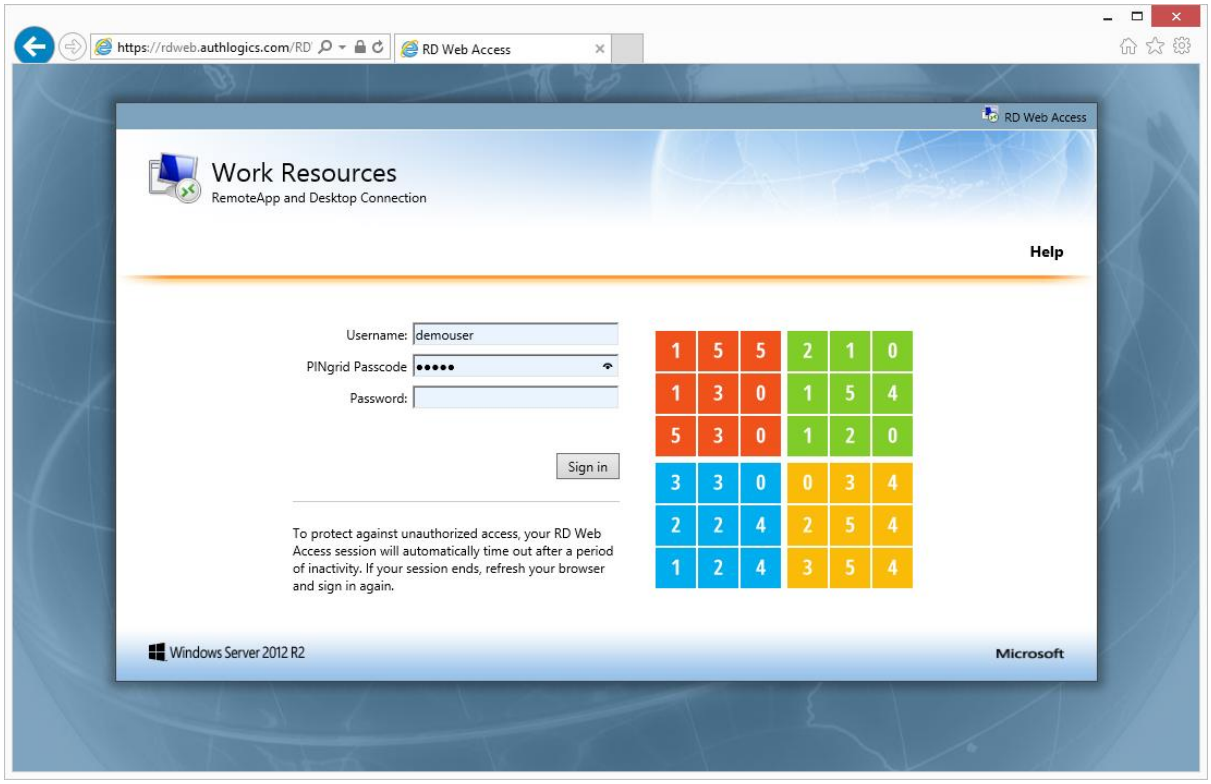
Email us: sales@authlogics.com

Table of Contents

Introduction

This guide includes details for integrating Authlogics Multi-Factor Authentication with Windows Remote Desktop Services via the Remote Desktop web interface using the Authlogics Remote Desktop Agent.

The Authlogics Remote Desktop Agent also simplifies the customisation of the Remote Desktop login pages for removing the requirement to enter the domain name, removing the public/private option and displaying the company name for branding purposes.



Considerations

System Requirements

The supported operating systems for Authlogics Remote Desktop Agent are:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

The Remote Desktop Web Access Windows Role must be installed and configured on the sever before installing the Authlogics Remote Desktop Agent.

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

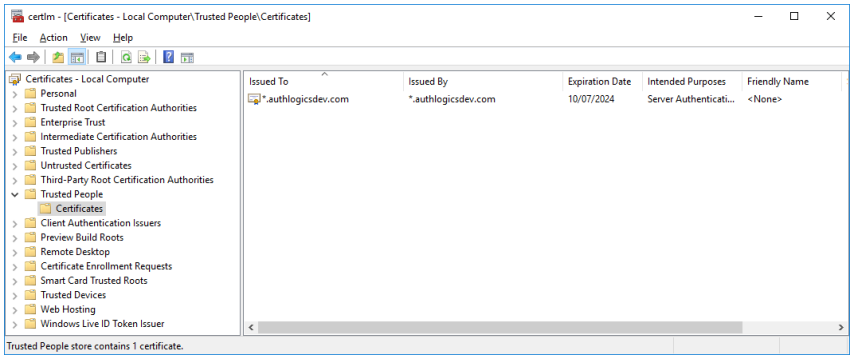
This deployment section assumes that at least one Authlogics Authentication Server has already been installed and is functional. See the Authlogics Authentication Server Installation and Configuration guide for further information on setting up the Authlogics Authentication Server. In addition, Authlogics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

SSL Certificates

The Authlogics Remote Desktop Agent connects to the Authlogics Authentication Server over SSL. The SSL certificate used in IIS on the Authlogics Authentication Server must be trusted by the Authlogics Remote Desktop Agent and must match the configured DNS name.

By default, the Authlogics Authentication Server uses a self signed certificate which will NOT be trusted by the Authlogics Remote Desktop Agent. To allow the Authlogics Remote Desktop Agent to trust the self signed certificate on the Authlogics Authentication Server:

(1) Export the certificate (without the private key) in Base64 format from the Authlogics Authentication Server.
(2) Import the certificate into the Local Computer “Trusted People” certificate store.



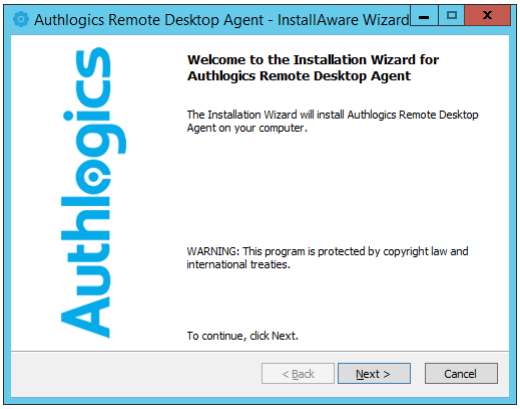
Installing/Removing the Authlogics Remote Desktop Agent

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

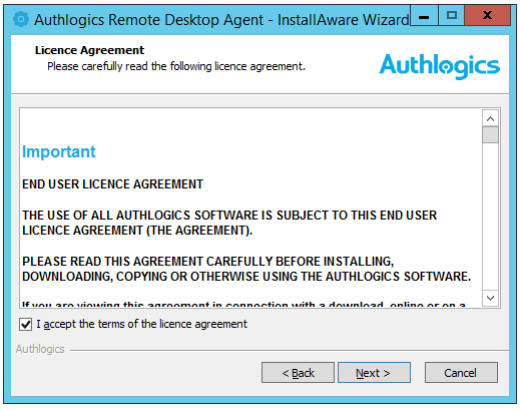
Running an installation

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

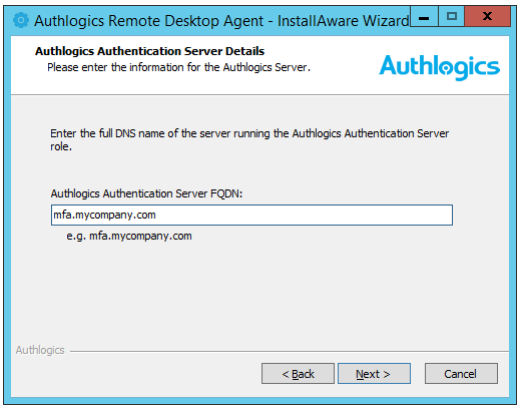
(2) Click *Next* to begin the install or *Cancel* to quit.



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

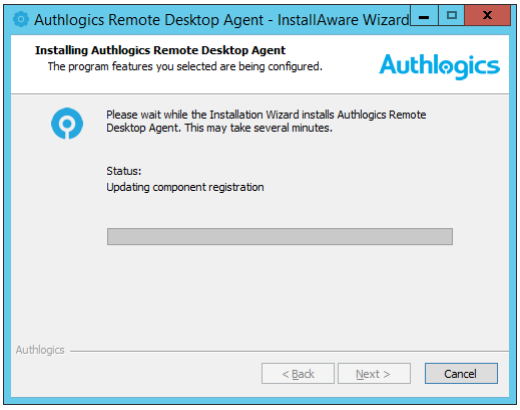


(4) Enter the FQDN of the Authlogics Authentication Server, click *Next*.

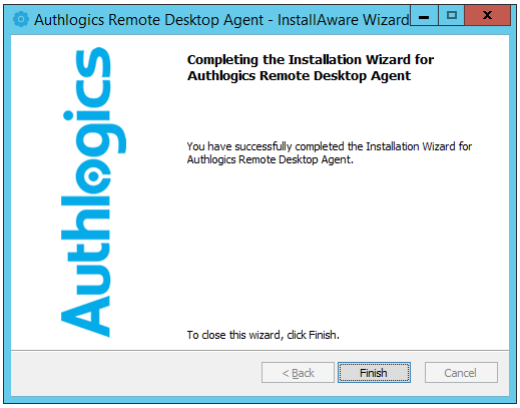


(5) Click *Next* to begin the install or *Cancel* to quit.

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 Authentication Server on a server, you can remove it by performing an uninstall from Control Panel > Programs > Programs and Features.

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 a custom Company Name. Default: "Work Resources" -->
    <add key="CompanyName" value="Work Resources"/>

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

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

    <!-- Enable the display of a Deviceless OTP challenge on the logon page. Default: true -->
    <add key="DevicelessOTPEnabled" value="true"/>

    <!-- Enable the use of self signed certificates on the Authlogics Authentication Server. Default: true -->
    <add key="EnableSelfSignedCerts" value="true"/>

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

    <!-- Default ports: HTTPS = 14443. -->
    <add key=" AuthlogicsServerPort" value="14443"/>


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