

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



Authlogics, 329, Doncastle Road, Bracknell, Berkshire, RG12 8PE, UK www.authlogics.com | sales@authlogics.com | +44 1344 568 900 | +1 408 706 2866

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organisations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organisation, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

Authlogics may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written licence agreement from Authlogics, the furnishing of this document does not give you any licence to these patents, trademarks, copyrights, or other intellectual property.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

The information contained in this document represents the current view of Authlogics on the issues discussed as of the date of publication. Because Authlogics must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Authlogics, and Authlogics cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. AUTHLOGICS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS Document.

Copyright © 2022 Authlogics. All rights reserved.



UK/EMEA: +44 1344 568 900 | sales@authlogics.com | US: +1 408 706 2866

Table of Contents

Introduction	1
Considerations	
System Requirements	
Design and Deployment Scenarios4	
Deployment4	
Overview4	
SSL Certificates4	
Installing/Removing the Authlogics Remote Desktop Agent5	
Running an installation5	
Running a removal6	,
Configuring the Authlogics Remote Desktop Agent7	,





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.

EN I	Work Resources			17	5				RD Web Access
	RemoteApp and Desktop Connecti	ion							
1									Help
<u> </u>	Username:	demouser							
	PINgrid Passcode		1	5	5	2	1	0	
	Password:		1	3	0	1	5	4	
		······································	5	3	0	1	2	0	
		Sign in	3	3	0	0	3	4	
-	To protect against u	nauthorized access, your RD Web	2	2	4	2	5	4	
	Access session will a	utomatically time out after a period ession ends, refresh your browser	1	2	4	3	5	4	
1 June - Law	vs Server 2012 R2								Microsoft

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.

🚟 certIm - [Certificates - Local Computer\Trusted Pe	eople\Certificates]				-	×
Eile Action View Help						
🗢 🏟 🖄 📰 📋 🙆 💀 🛛 🖬						
Certificates - Local Computer Person Person Trusted Root Certification Authonities Intermediate Certification Authonities Tutted Publishers Untrusted Certification Tinted Publishers Tusted People Tusted People Certification	Issued To ^	Issued By *.authlogicsdev.com	Expiration Date 10/07/2024	Intended Purposes Server Authenticati	Friendly <none></none>	
> Client Authentication Issuers > Preview Build Roots > Renete Desktop > Centificate Enrollment Requests > Smart Card Tuxted Roots > Tuxted Devices > Web Hooting > Windows Live ID Token Issuer	¢					>
Trusted People store contains 1 certificate.						





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 <u>elevated privileges</u>.
- (2) Click *Next* to begin the install or *Cancel* to quit.

Authlogics Remote E	Desktop Agent - InstallAware Wizard 💻 🗖 🗙
ogics	Welcome to the Installation Wizard for Authlogics Remote Desktop Agent The Installation Wizard will install Authlogics Remote Desktop Agent on your computer.
Authl	WARNING: This program is protected by copyright law and international treaties.
	< Badk Next > Cancel
	Control Berry Control

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

Authlogics Remote Desktop Agent - InstallAware Wizard -	
Licence Agreement Please carefully read the following licence agreement.	5
Important END USER LICENCE AGREEMENT THE USE OF ALL AUTHLOGICS SOFTWARE IS SUBJECT TO THIS END USER LICENCE AGREEMENT (THE AGREEMENT). PLEASE READ THIS AGREEMENT CAREFULLY BEFORE INSTALLING, DOWNLOADING, COPYING OR OTHERWISE USING THE AUTHLOGICS SOFTWARE. I wave accounted to a greement Authlogics	
< Back Next > Cancel	

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

O Authlogics Remote Desktop Agent - InstallAware Wizard	- 🗆 X
Authlogics Authentication Server Details Please enter the information for the Authlogics Server.	hlogics
Enter the full DNS name of the server running the Authlogics Authentication S role.	erver
Authlogics Authentication Server FQDN:	
mfa.mycompany.com	
e.g. mfa.mycompany.com	
Authlogics	
< <u>B</u> ack <u>N</u> ext >	Cancel



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

Authlogics Remote	e Desktop Agent - InstallAware Wizard 🗕 😐 🗙
S	Completing the Installation Wizard for Authlogics Remote Desktop Agent
S	The Installation Wizard is now ready to configure Authlogics Remote Desktop Agent on this computer.
	- Click Next to begin configuration
	- Click Back to change settings
	- Click Cancel to exit
Auth	
	< <u>B</u> ack <u>N</u> ext > Cancel

The installation is being performed.

Authlogi	cs Remote Desktop Agent - InstallAware Wizard 🗕 📮 🗙
	Authlogics Remote Desktop Agent am features you selected are being configured.
Ø	Please wait while the Installation Wizard installs Authlogics Remote Desktop Agent. This may take several minutes.
	Status: Updating component registration
Authlogics	
ria a no gita	< <u>B</u> ack Next > Cancel

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

Authlogics Remote Desktop Agent - InstallAware Wizard -				
S	Completing the Installation Wizard for Authlogics Remote Desktop Agent			
S	You have successfully completed the Installation Wizard for Authlogics Remote Desktop Agent.			
Nuth				
Ā	To close this wizard, click Finish.			
	< Back Finish Cancel			

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="14443"/>
</add key="AuthlogicsServerPort" value="14443"/>
</add

<!-- 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>

