Authlogics Remote Desktop Agent

Bridging the security gap between Remote Desktop and your Security Policy

Whitepaper
Introduction

Microsoft’s Remote Desktop Services provides a convenient way for users to access published applications remotely. Users are able to access remote apps and full desktop sessions from any PC with an Internet connection and is delivered through a Web-based portal (the RDWeb website).

Out of the box, the portal uses standard forms based authentication which requires users to enter their Active Directory username and password to gain access. While the Remote Desktop functionality provides many business benefits, many IT security departments face the issue that it does not include any built in Two Factor Authentication (2FA), and therefore doesn’t meet the security requirements defined by their company’s policy, especially when being accessed remotely.

Organisations requiring strong authentication with Remote Desktop typically had to resort to larger, more expensive solutions, such as Citrix, to benefit from built in 2FA. The Authlogics Remote Desktop Agent bridges the gap by providing the missing strong authentication layer.
Integrating RDS with Strong Authentication

Adding a security layer should not be a difficult or complex process, and it shouldn’t be cumbersome for users either. The Authlogics Remote Desktop Agent (RDA) is quick and easy to install on a Remote Desktop gateway server. The logon process for the user remains familiar too with just the extra requirement of entering a One Time Code (OTC) at the login screen.

The Authlogics Remote Desktop Agent is able to deliver PINgrid, PINphrase or PINpass authentication options to the Remote Desktop services web portal logon screen for complete flexibility. In addition, PINgrid and PINphrase can be deployed as 1.5 Factor for OTC logins without any token requirement.

![Sample PINgrid 1.5 FA integration](image)

To protect against unauthorized access, your RD Web Access session will automatically time out after a period of inactivity. If your session ends, refresh your browser and sign in again.

**Why AuthCentral?**

Unlike some other Remote Desktop Services 2FA solutions, the Authlogics Desktop Logon Agent is quick and easy to deploy via a setup wizard, with no code changes for administrators to implement. The agent will seamlessly work with an existing Authlogics server and users for immediate access. The non-obtrusive style of the agent only slightly modifies the look and feel of the portal logon page, keeping the feel completely consistent for users, while enabling all the normal customisable text changes that RDWeb provides.

Users can benefit from the convenience of 1.5 Factor and administrators can require 2 Factor for some/all users through software based token, email or TEXT messaging, to create a truly flexible solution that fits with the business needs.
About Authlogics

Authlogics provides IT security professionals with a fresh alternative to legacy authentication and transaction verification methods. We help companies remove the reliance on password-based authentication and hardware tokens, and encourage the use of self service capabilities. We eliminate costs and administration surrounding card readers and keyring tokens, and innovate without the need to implement expensive biometrics.

Whether you want to authenticate to a Web portal, VPN, firewall, or to a multitude of different Cloud providers, Authlogics offers a range of authentication methods to suit your business. Our solution provides 1.5, 2 and 3 Factor Authentication options, via three authentication technologies (PINpass, PINphrase & PINgrid) and can be delivered via the Web, Mobile App, Email or SMS/TEXT. Additionally, we have several integration agents for various 3rd party systems should you need them.

PINgrid

PINgrid is an award-winning and patented multi-factor authentication and transaction signing solution that is being used in the public and private sector today to transform any mobile device into a soft-token, via a simple offline application, replacing passwords with a memorable pattern that automatically generates a One Time Code (OTC).

PINphrase

PINphrase is a memorable word technology where users are asked for random letters from answers they already know to log in, instead of providing a full password. PINphrase is the only off-the-shelf solution that delivers this type of technology used by many banking web sites.

PINpass

PINpass is a 2 and 3 Factor OATH compliant 6 - 8 digit random code solution. This standard is widely adopted by many vendors and is well trusted. PINpass turns a mobile device into a token via an App or by sending an OTP via SMS or e-mail. Like most OATH solutions, PINpass works with a fixed PIN code which must be remembered, however it can also be used with an AD password or work in PIN-less mode.