AGTRAX™

Building Multi-Factor Authentication

10 South Main, STE A
Hutchinson, KS 67501
(866) 360-0016
traxview@agtrax.com

WHITE PAPER

TABLE OF CONTENTS

WHAT IS MFA?

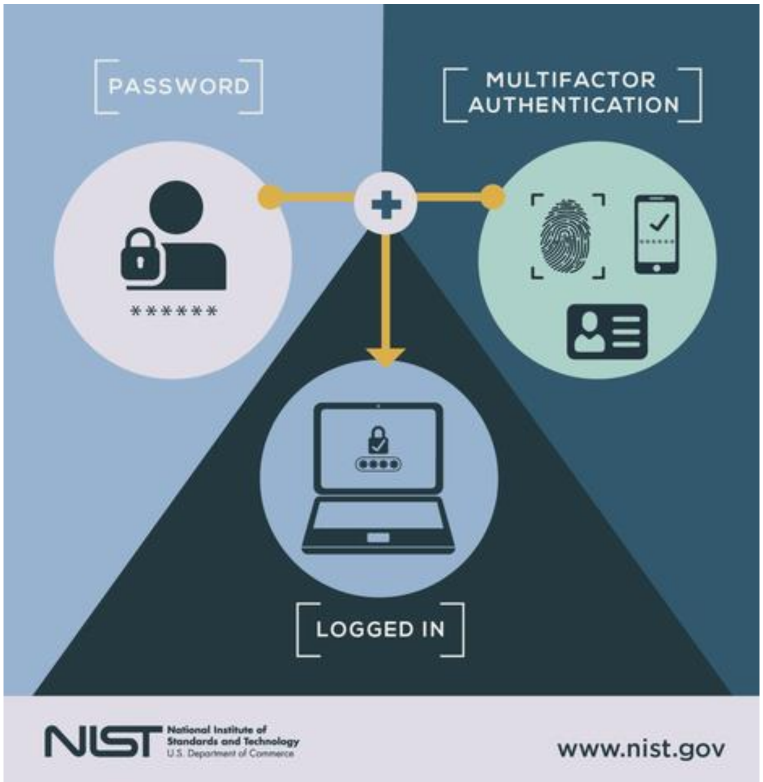
Multi-factor authentication (MFA) may sound complex but really is simple to understand, and you are more than likely already using it in some form.
For example, if you've: logged into a website that texted a code to your phone, and you then use that code to gain access to your online account or swiped a bank card and then entered your PIN number at an ATM, then you've used MFA.

MFA, sometimes referred to as two-factor authentication or 2FA, is a security strategy that allows you to present two pieces of evidence or factors when logging in to an account.

Those factors fall into three categories:

1. something you know - like your password or PIN
2. something you have - like a smart device or card
3. something you are - like your fingerprint or retina scan

You must use two different categories to enhance security – so entering a PIN and a password would not be considered multi-factor.


PASSWORD
******
MULTIFACTOR AUTHENTICATION
LOGGED IN
NIST National Institute of Standards and Technology U.S. Department of Commerce
www.nist.gov

To make things easier than that though often a site will remember your device, so if you come back using the same phone or computer, the site remembers your device as the second factor.

WHY IT’S IMPORTANT

With the increase in remote work and the rise in identity-based data attacks the need for multi-factor authentication (MFA) has never been greater.

AgSupport connections

All AgTrax Support connections thru traxview go through

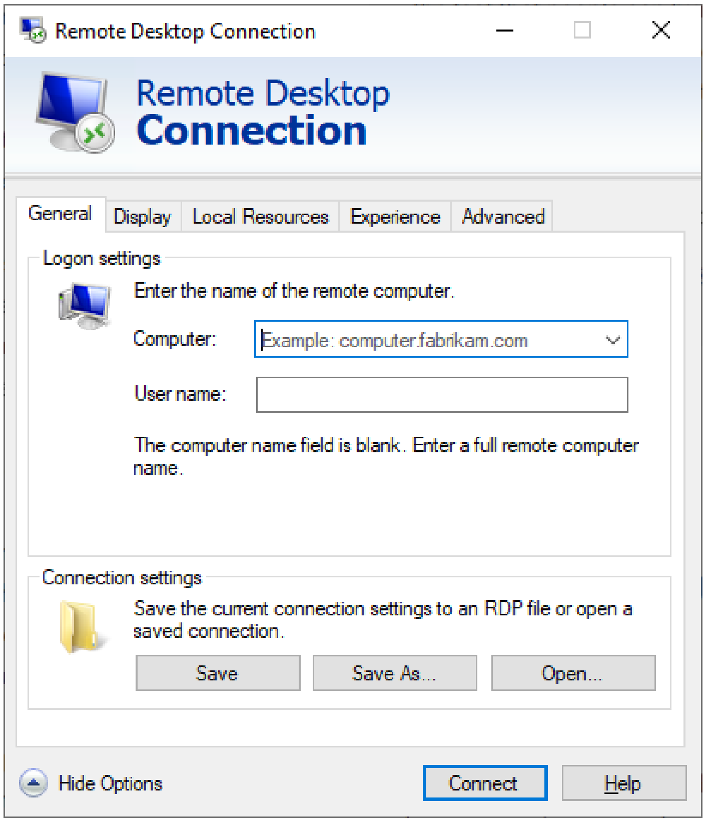
SSH with an Encryption Key…

Traxview connections

All Traxview desktop applications should be set up to connect through a Remote Desktop connection or through a VPN.

Plus

We will use SSH with an Encryption Key…



Logon settings

Enter the name of the remote computer.

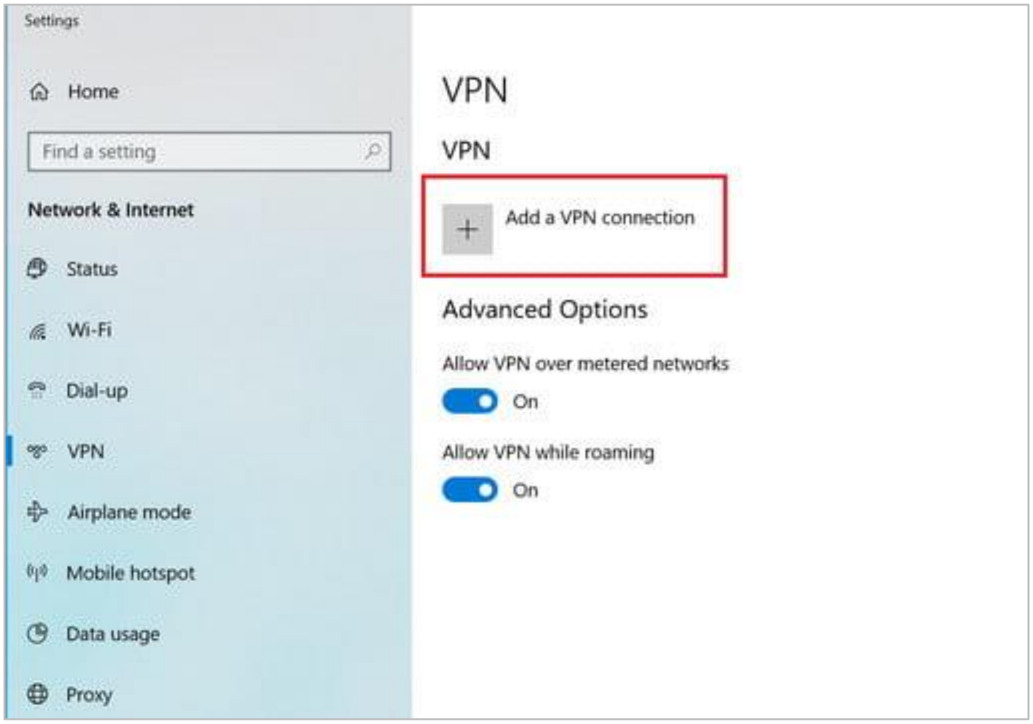
Computer: Example: computer.fabrikam.com

User name:

The computer name field is blank. Enter a full remote computer name.

Connection settings

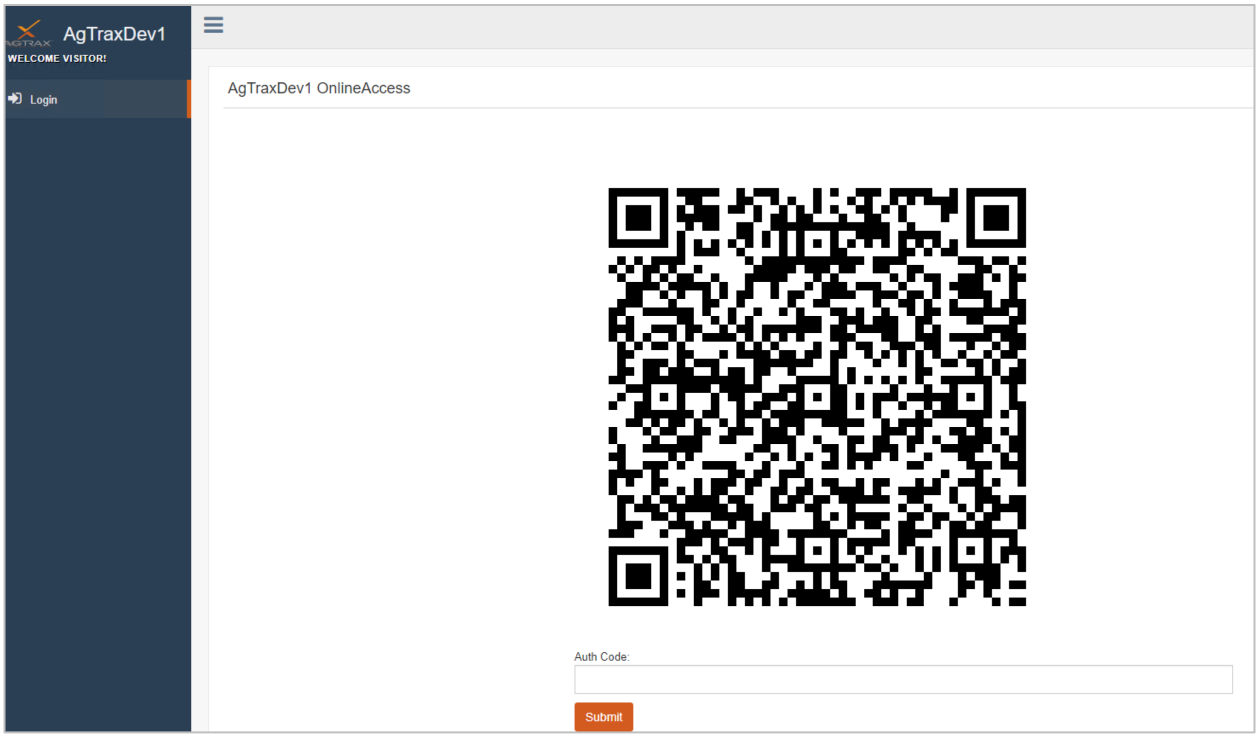
Save the current connection settings to an RDP file or open a saved connection.

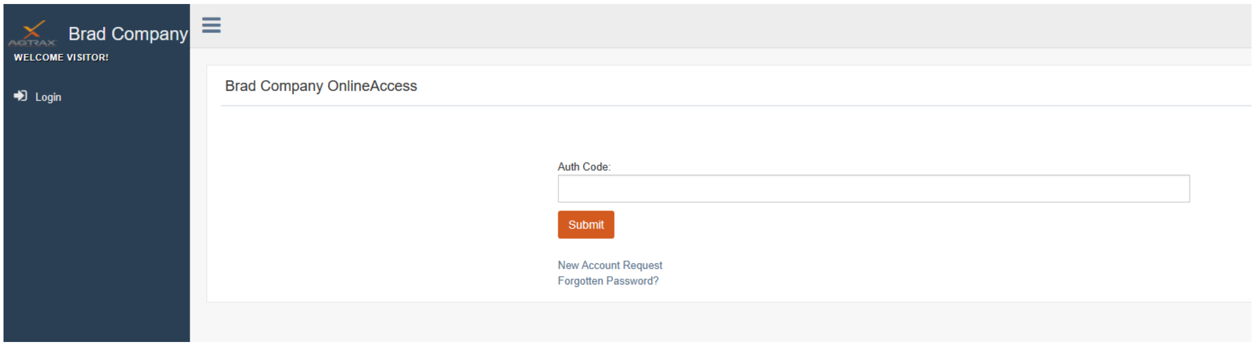


Allow VPN over metered networks: On

Allow VPN while roaming: On

Online Access connections





Research and argument

Google Authentication

Research and argument

CONCLUSION

is clear that enterprises must continue to evolve and improve their authentication of users, moving beyond the limitations of passwords and

traditional 2FA. MFA is better, but using contextual data to dynamically step-up authentication is the right approach for enterprises.

Today, contextual authentication is seen as complementary to active and explicit authentication factors. But in the future, Ping Identity expects

contextual authentication to become the norm and explicit authentication to be used less frequently. A risk-based authentication architecture

combines step-up MFA with passive contextual authentication for the optimal combination of cost-effectiveness, usability and security.

Ping Identity recommends these five high-level best practices for step-up MFA:

• Step-up MFA should be supplemented with passive contextual authentication.

• A risk-based approach, based on operation requests and contextual indicators, should be used to determine when to request step-up MFA.

• Step-up MFA should be optional for the majority of customer scenarios. Customers should be encouraged to opt into step-up MFA by

educating them on its advantages and by creating optin incentives. Risks of customers opting out of step-up MFA should be mitigated

through other mechanisms.

• Employees should be given a choice of and options for their authentication mechanisms. If employees opt out of enhanced active modes of

authentication, companies should supplement their practices with passive modes.

• A variety of MFA options should be supported to address the needs of different user constituencies—for example, users with disabilities or users who are less tech savvy.