NETWORK BOX
managed security services

Setting up Multi-Factor Authentication

Introduction

Multi-Factor Authentication (or MFA) is a simple best practice that adds an extra layer of protection on top of your user name and password. We have implemented a RFC 6238 TOTP compliant authentication server in our NBRS-5 platform. that we can leverage this for access to the Admin Portal access and/or Dual-Factor Authentication for SSLVPN clients w/ specific entity user which is stored locally on the NWB.

What is Time-based One-time Password (TOTP)?

RFC 6238 standardizes a time-based one-time password algorithm, allowing a multitude of servers and clients to inter-operate according to the standard. The algorithm relies on a shared secret between the client and the server. To generate a 6-digit PIN code, each side can independently (a) take the current time divide by 30, (b) add that to the shared secret, (c) get an SHA1 HMAC of that, (d) normalize the result, and (e) modulo 1,000,000. In such an arrangement, a unique 6-digit PIN is created every 30 seconds, and both the server and client can independently know that PIN (remember that it changes every 30 seconds), and auto-refresh a replacement PIN as necessary.

Typical Use Case

The usual approach is that the client is asked to authenticate to the server (admin portal, vpn). He/she needs to provide his/her username and his/her password along with the current PIN (the PIN is either provided in a separate field, or merely concatenated onto the end of the password). The user runs the TOTP app to get the current PIN, then switches back to the authentication screen to enter it (along with password and username) and send to the server.

Upon receiving the authentication credits, the server requires **username+password+6-digit passcode** authentication as usual. If it finds the user account is configured to require TOTP authentication, it performs the extra step of generating the current PIN (based on the shared secret) and compares that to the PIN provided by the user. Authentication only succeeds if the username matches, the password matches, and the PIN matches.

Typical Use Case (cont.)

To allow for a delay from the user looking up the PIN, to entering it, most implementations will permit authentication against all the PINs from a configurable one or two time periods before and after the current time. For example, allowing

one time period either way (30 seconds ago, now, and 30 seconds time) will allow for some reasonable clock drift, plus some time for the user to switch apps and enter the six digit PIN.

Applications for Multi-Factor Authentication

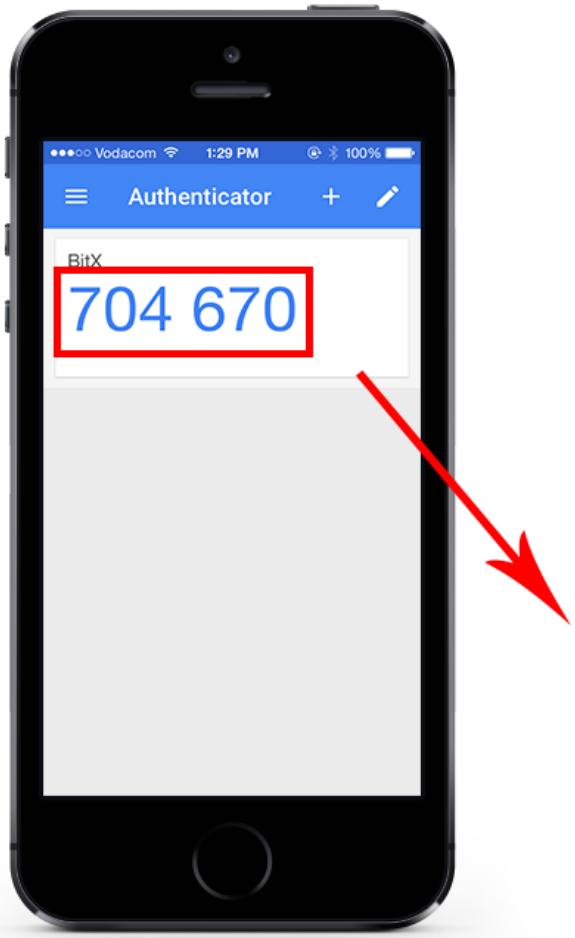
There are several free/downloadable RFC 6238 compliant applications available for all popular smart phone/device platforms. The most popular is the **Google Authenticator** (supported on various platforms) is an MFA application can be found for download via the play store or apple store and/or via google. https://support.google.com/accounts/answer/1066447?hl=en

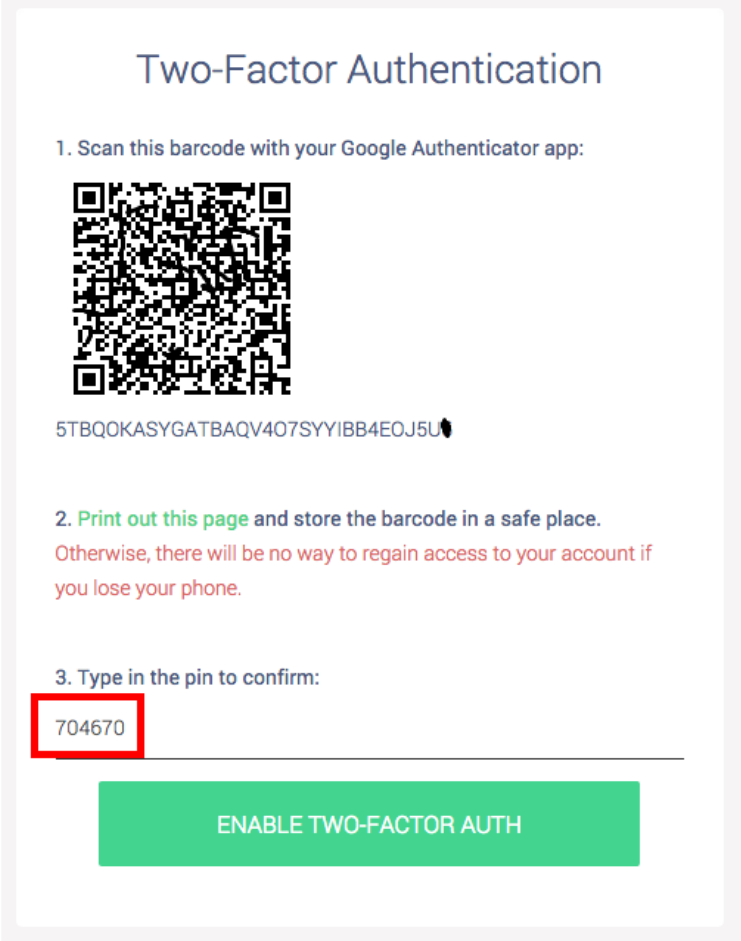
NOTE: Please refer to their site for instruction on how to install and setup the app for the first time.

Setup for Multi-Factor Authentication using TOTP

In order for NWB to leverage MFA via Google Authenticator, we will need a box office ticket opened requesting to add an entity user and a creating a random password along with TOTP enabling so we can provide you a URL to the QR code so you can scan with your mobile device. This will be provided upon creation via box office. Below are some screenshots of the Google Authenticator in action with QR code that you will receive from NWB

NETWORK BOX
managed security services





WARNING!!! WARNING !!! A unique QR Code URL will be issued for each entity user!!!
PLEASE DO NOT LOSE OR SHARE THIS WITH ANYONE ELSE!!!!