EN_BMS AuthAnvil Authenticator

January 10, 2018

Copyright Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Contents

Introduction

This guide is intended to document and explain how to setup and use the AuthAnvil authenticator in BMS as a validation mechanism to authorize access to BMS system.

With this option users will be validating their login in AuthAnvil login screen with Two-Factor Authentication if enabled, and if successful, they will be authorized automatically in BMS.

AA - Creating an AAOD Web Auth Agent

In order to set up a push window, we first must create a web auth agent in AAOD.

1. Log onto AAOD with an administrative account
2. Go to Auth Manager
3. Click the Plus(+) sign on the bottom right to create a new agent
4. Select 'Embedded Web Auth'
5. Give it a name and click 'Add Agent'

AA - Creating the policy for the agent

1. In AAOD, go to Policy Manager.
2. Click the plus(+) sign at the bottom right to create a new policy
3. Give the policy a name, We will use "2FA Test Policy" for this example
4. Set 'Select policy element' to 'User' from the dropdown choices
5. Set "Select Criteria' to 'is signing in'
6. In the 'then' area, pick "Set Allowed Methods' and uncheck 'require password authentication'
7. Add and 'AND' (By clicking the green plus icon) and pick 'require 2FA' ,leave all criteria checked on.
8. Create another 'AND' condition of 'Set Session Lifetimes" and uncheck "Sign out when all browser windows have been closed' and set access token lifetime to 1 minute and refresh token lifetimes' to zero.

Set Agent Policy

1. Go back to Auth Manager and find the agent created above and click on it.
2. Select 'edit' and set the authentication Policy to the policy created in Part 2.
3. Save Changes.

NOTE: please copy the ID and Key of the agent and save along with your homerealm to a text file for easy reference. Your home realm value is the base url of your AAOD page

IE: if your sign page was this:

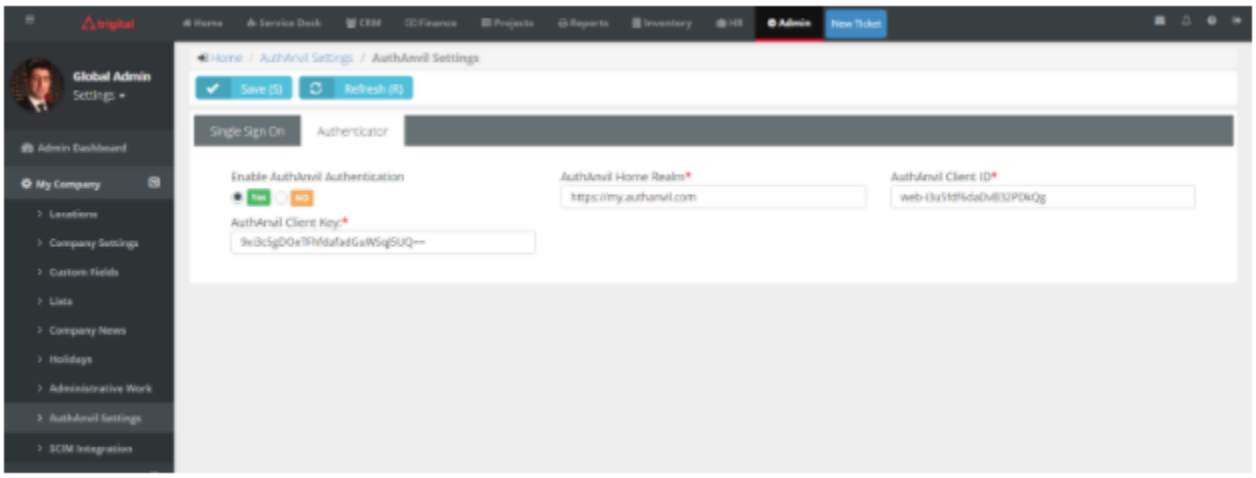
https://braindead.staging.orangemesa.com/signin

Your home realm is this **'braindead.staging.orangemesa.com'**

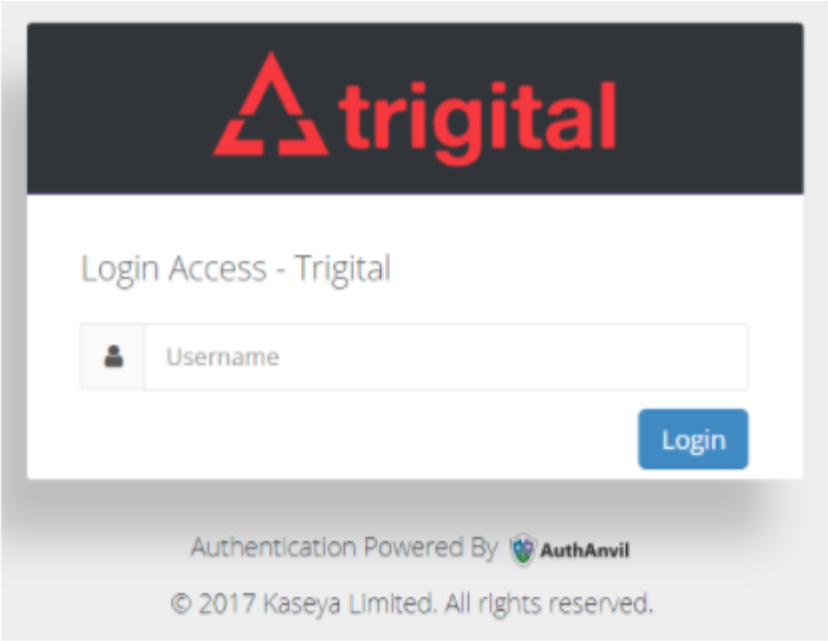
Enable AuthAnvil Authentication in BMS

Following the setup on AuthAnvil part, to enable the Authenticator in BMS, we have to navigate to the Administration Module > My Company > AuthAnvil Settings.

Under this section you will find a new tab called “Authenticator” where we will enable the authenticator.

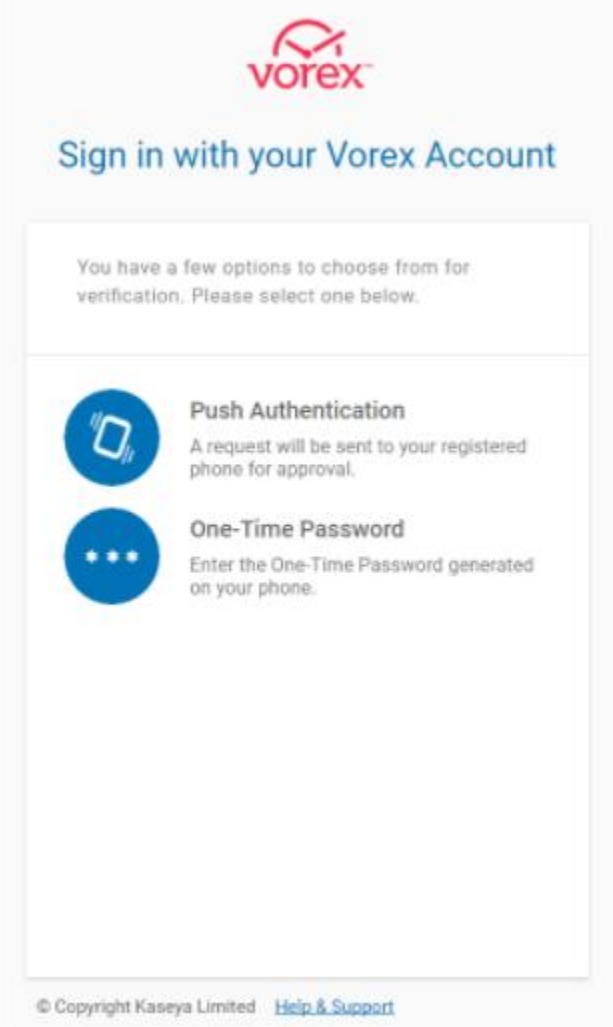


1. Three fields have to be filled based on what was copied from Part 3 above (**Set Agent Policy**):
    a. AuthAnvil Home Realm
    b. AuthAnvil Client ID
    c. AuthAnvil Client Key
2. Once AuthAnvil Authentication is enabled, logout from BMS.
3. You will be redirected to the login page with the tenant name above . You are only required to submit the username without the password to login to BMS.
    a. Note that the username MUST exist in both Authanvil and BMS.
4. Upon logging in , you will be redirected to a page displaying options to login wia two options : **Push Authentication** or via a **One Time Password.**



BMS - Gateway Screen when AuthAnvil Authenticator

Please note that the Username to use when logging in has to be available in AuthAnvil for the validation to work.



Authentication and Verification with AuthAnvil