

Authentication 2FA

Natively, the web-based access supports 2-factor authentication using a variety of technologies including TOTP Applications such as Google Auth, as well as Yubikey.

Google Authentication Instructions

Google Auth is easy to use and setup within the UMS:

The screenshot displays the 'Settings' page of a web-based application. On the left is a dark sidebar with icons for Compose, Mail, Contacts, Cloud, Notes, Help, Calendar, Tasks, Settings (highlighted), Dark mode, About, and Logout. The main content area is titled 'Settings' and lists various options: Preferences, Folders, Identities, Responses, User info, Vacation, Junk, Cloud View, and 2-Factor Authentication (selected). A modal window is open for the '2-Factor Authentication' settings. It shows a 'Code OK' confirmation from 'n2.mstcdun.com' with an 'OK' button. The 'Activate' checkbox is checked. The 'Secret' field contains 'RH7EGGIUGEL5BMEM' with 'Hide secret' and 'Generate New Secret' buttons. The 'Recovery codes' section shows five codes: 'SNQJV', 'DQDJJ', 'DRSWC', 'NFEXU', and a 'Hide recovery codes' button. A large QR code is displayed for scanning. Below the QR code, text instructs the user to scan the code with a TOTP app like 'google-authenticator'. A 'Save' button is present. At the bottom, a section for testing the PIN shows the server time as '11 Oct 2022 7:59:53' and a current PIN of '281759' with a 'Check code' button.

Once setup within the UMS, the user can scan the QR Code with their phone using the mobile Google Authenticator app and a new rotating code is automatically setup for the user account.

Upon next login to the UMS, the user is presented with two factor challenge screen after they enter their username and password.



2-Factor Authentication Code:

☐ Don't ask me codes again on this computer for 7 days

PROCEED

Revision #2

Created 11 October 2022 19:14:12 by Stephen D

Updated 11 October 2022 20:11:15 by RackCorp