eRAD RIS

RELEASE ANNOUNCEMENT

Build 4.2025.065

UPDATED DECEMBER 19, 2025

TABLE OF CONTENTS

PUBLICATION HISTORY

Revision	Author	Description
December 19, 2025	Kevin Brooks	▪ Commercial release.

SUMMARY

Release Announcement

This release of eRAD RIS 4.2025.065 introduces an option to enable Multi-Factor Authentication (MFA) login for the Referring Portal, enhancing security of patient data.

New Features

This release introduces the following features and enhancements:

Category	Redmine #	Subject	Description
Security	36931	Support MFA on Provider Portal	This enhancement to Security introduces an option to enable Multi-Factor Authentication (MFA) login for the Referring Portal, enhancing security of patient data.

SORTED BY CATEGORY AND REDMINE

Refer to the FEATURE DETAILS section below for configuration and usage information.

FEATURE DETAILS

Security

Feature #36931 - Support MFA on Provider Portal

Summary

This enhancement to Security introduces an option to enable Multi-Factor Authentication (MFA) login for the Referring Portal, enhancing security of patient data.

Background

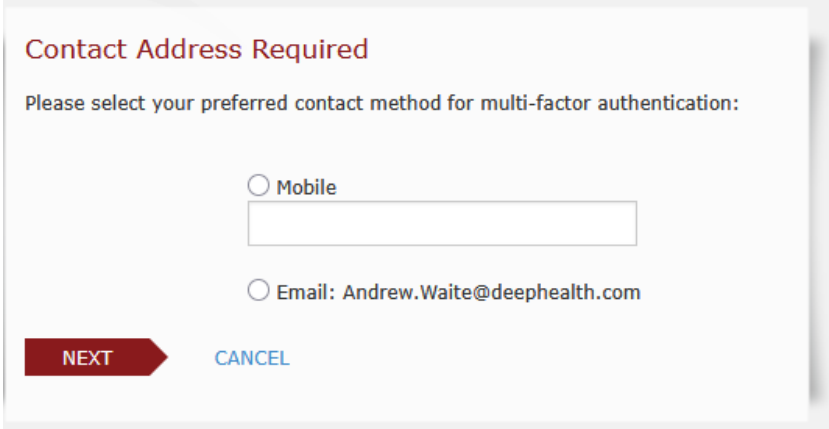
Previously, the Provider Portal used simple authentication. With the addition of digital forms and increased patient interaction, the portal can provide access to a great deal of private data. Additionally, referring practices sometimes fail to notify administrators of staff changes, resulting in the potential for former employees to retain their credentials and continue to access data.

Feature Description

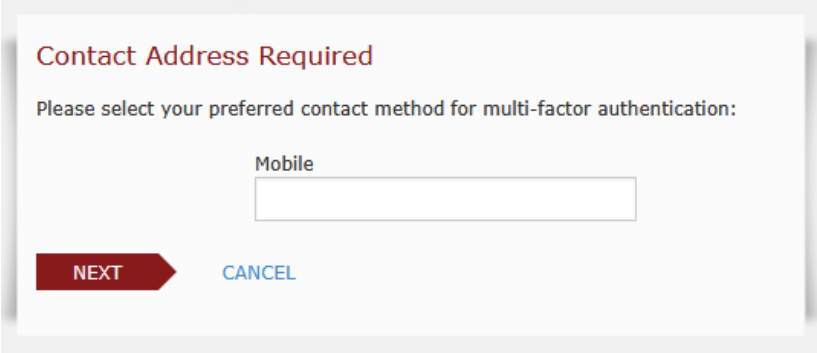
Multi-Factor or Two-Factor Authentication enhances login security by challenging users to enter a verification code when logging in. This code is sent to them via email or SMS (or both).

With this change, a new `MFAEnabled` configuration setting enables Multi-Factor Authentication for users of the Provider and Provider Admin Portals. This setting is overridable per Site Group, meaning that if configured for a particular site, a users would not be presented with MFA when logging in under a different site group.

Based on new `MFAContactType` and `MFAAdminContactType` configuration settings, users may be prompted to provide an Email, Mobile, or both as their MFA notification address:

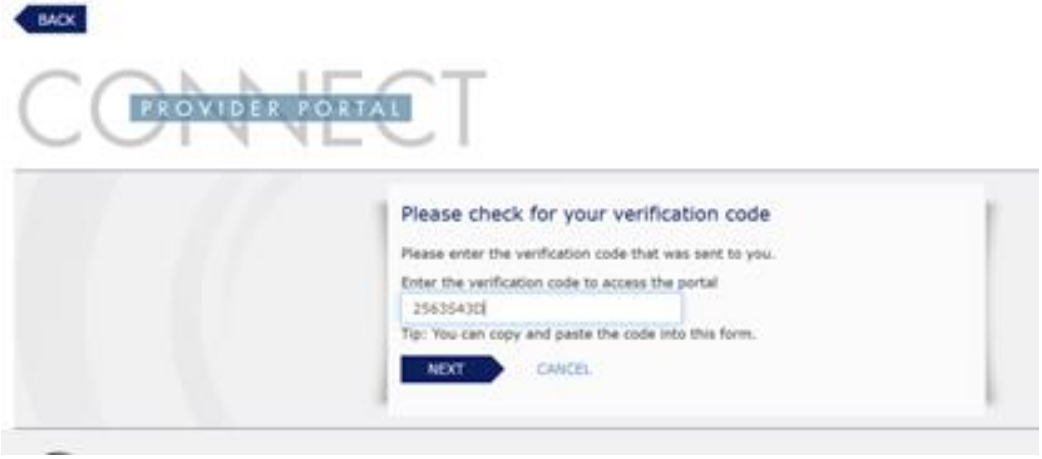


CONFIGURATION ALLOWS USERS TO RECEIVE THEIR VERIFICATION CODE BY MOBILE AND/OR EMAIL.



ALTERNATIVELY, CONFIGURATION CAN LIMIT VERIFICATION TO ONLY MOBILE OR EMAIL.

When logging in, users are prompted to enter the verification code:



Service Team Upgrade Instructions

The Service Team must complete the following actions to deploy this feature:

Provider Portal

See also CHANGES TO PARAGRAPHCONFIG LOOKUP TABLE.

Changes to applicationsettings.config

The following settings were added or updated with this release:

Setting	Default	Purpose
MFAEnabled	False	When True, multi-factor authentication is enabled. Overridable at the Practice Level in the Organization lookup.
MFACodeExpiration	30	Number of minutes for which the MFA verification code is valid.
MFACodeLength	8	Number of characters for the generated MFA verification code.
MFAContactType	default: single [email,mobile,single,both]	MFA communication options for Portal users.
MFAAdminContactType	default: single [email,mobile,single,both]	MFA communication options for Admin Portal users.

Examples as it would be entered in the applicationsettings.config file

```
<ADD KEY="MFAENABLED" VALUE="FALSE"/>

<ADD KEY="MFACODEEXPIRATION" VALUE="3"/>

<ADD KEY="MFACODELENGTH" VALUE="4"/>

<ADD KEY="MFACONTACTTYPE" VALUE="BOTH"/>

<ADD KEY="MFAADMINCONTACTTYPE" VALUE="BOTH"/>
```

Configuration Instructions

Service Team assistance is required to enable this feature.

Optional configuration is available:

Changes to ParagraphConfig Lookup Table

The following settings were added:

Setting	Default	Purpose
PortalInvalidMFAError	Invalid verification code entered, please try again.	Message presented to the user when MFA verification code is entered incorrectly.
PortalTwoFactorAuthMessage	Your verification code is {0}. This code is valid for the next {1} minutes.	Message sent to the user containing {0} for MFA verification code, and {1} for the time in minutes.
PortalTwoFactorAuthSMS	Your one-time portal verification code is {0}	SMS message text sent to the user with MFA verification code.
PortalTwoFactorAuthSubject	Multi-Factor Authentication Code	Email Subject text sent as part of the MFA verification message.
RPMFACheckForCode	Please check for your verification code	Message displayed to the user after the MFA verification code is sent.
RPMFAContactAddress	Your organization requires you to set up multi-factor authentication. Please select your preferred contact method for multi-factor authentication.	Message displayed to the user after MFA has been enabled for Provider Portal, requesting the user to provide a contact address.
RPMFAContactAddressAdmin	Your organization requires you to set up multi-factor authentication. Please select your preferred contact method for multi-factor authentication.	Message displayed to the user after MFA has been enabled for Provider Admin Portal, requesting the user to provide a contact address.
RPMFAContactRequired	Keep Your Account Secure	Message title displayed to the user after MFA has been enabled.
RPPleaseEnterTheVerificationCodeAdmin	Please enter the verification code that was sent to you.	Message displayed to the user prompting them to enter a MFA verification code.

VERSION DETAILS

Code Stream

The following source code branches have been merged into this release: