Exa® PACS RIS

Feature Summary

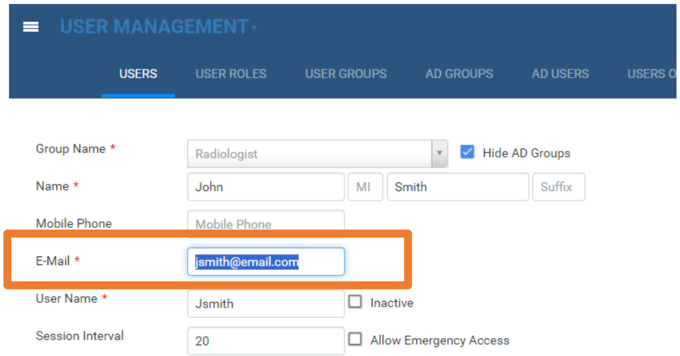
2FA User Configuration

Two-factor authentication (2FA) adds an extra layer of security by requiring not only a password but also a second form of verification, such as a code sent by email. This helps protect your account even if your password is compromised.

User configuration

Every user of Exa PACS/RIS must have an email address configured to use 2FA.

SETUP → USER MANAGEMENT → USER



Group Name * Radiologist ☑ Hide AD Groups

Name * John MI Smith Suffix

Mobile Phone Mobile Phone

E-Mail * jsmith@email.com

User Name * Jsmith □ Inactive

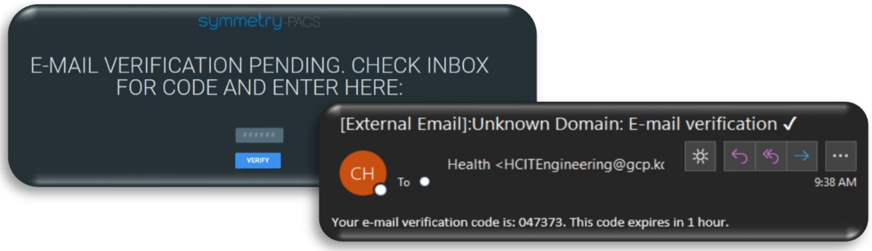
Session Interval 20 □ Allow Emergency Access

When using 2FA, the **user name is case-sensitive**.

Sign in

The first time a user signs in, their email address is verified.

1. Sign in.
   The system sends a code by email.
2. Enter the code.



E-MAIL VERIFICATION PENDING. CHECK INBOX FOR CODE AND ENTER HERE:

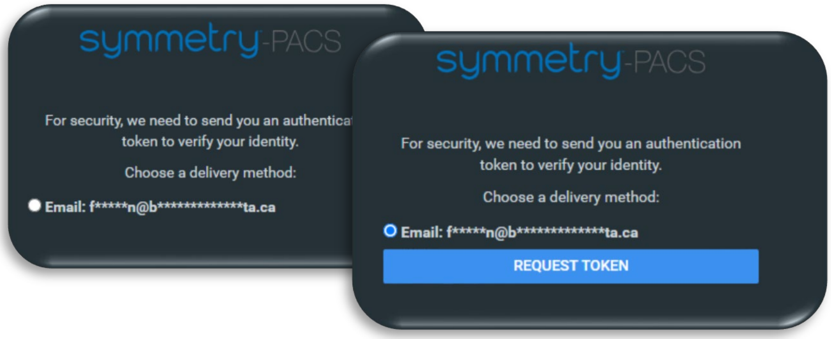
[External Email]:Unknown Domain: E-mail verification ✓

CH Health <HCITEngineering@gcp.kc To 9:38 AM

Your e-mail verification code is: 047373. This code expires in 1 hour.

For the second and subsequent sign-ins, the verified email address is used for two-factor authentication.

1. Sign in.
2. Choose your email.
3. Request a token.
   The system sends a token by email.
4. Enter the Authentication code.



For security, we need to send you an authentica token to verify your identity.

Choose a delivery method:

○ Email: f*****n@b**************ta.ca

For security, we need to send you an authentication token to verify your identity.

Choose a delivery method:

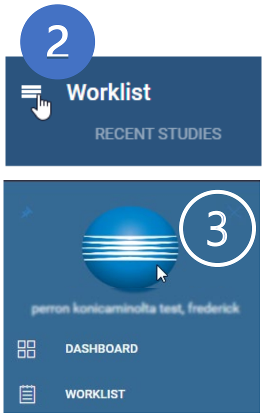
● Email: f*****n@b**************ta.ca

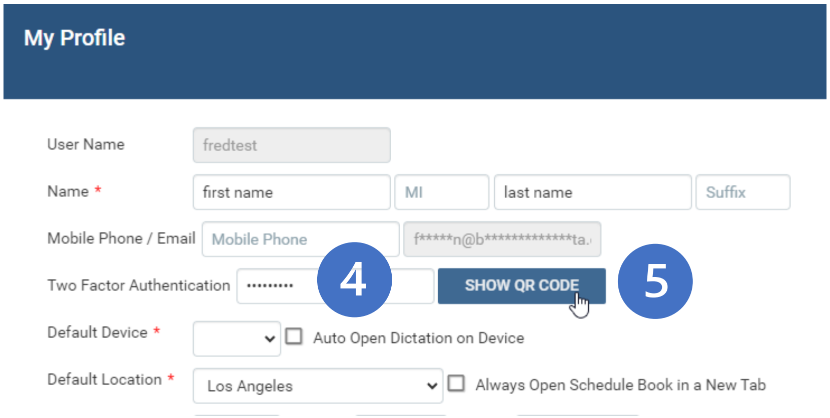
5. Sign in.

Authenticator application

After completing the initial email verification, you can set up an authenticator application on your phone. You can use the authenticator app as an alternative to email tokens for verifying sign-in attempts.

1. Sign in to Exa PACS/RIS using email Authentication.
2. Select the burger menu.
3. Select the blue Konica Minolta Logo.
4. Type your Exa password in the **Two Factor Authentication** field.
5. Select **SHOW QR CODE.**
6. Add your secret key (QR code or text) in your Authenticator app.
7. Type your time-base one-time passcode displaying in your app and then select **Verify**.
8. Close the **MY PROFILE** window.





My Profile

User Name: fredtest

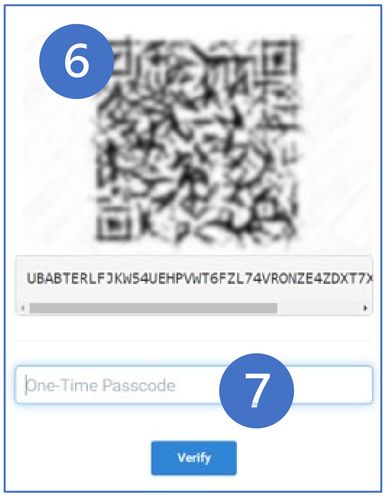
Name *: first name | MI | last name | Suffix

Mobile Phone / Email: Mobile Phone | f*****n@b**************ta.

Two Factor Authentication: ········· SHOW QR CODE

Default Device *: □ Auto Open Dictation on Device

Default Location *: Los Angeles □ Always Open Schedule Book in a New Tab

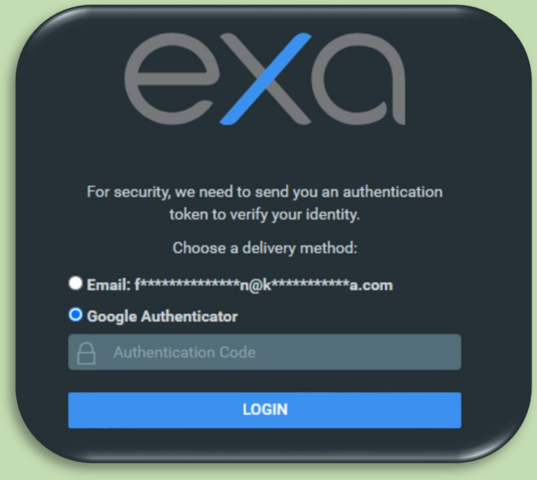


UBABTERLFJKW54UEHPVWT6FZL74VRONZE4ZDXT7X

One-Time Passcode

Verify

After adding the authenticator app, you can choose it the next time you sign in for authentication



For security, we need to send you an authentication token to verify your identity.

Choose a delivery method:

○ Email: f**************n@k***********a.com

● Google Authenticator

Authentication Code

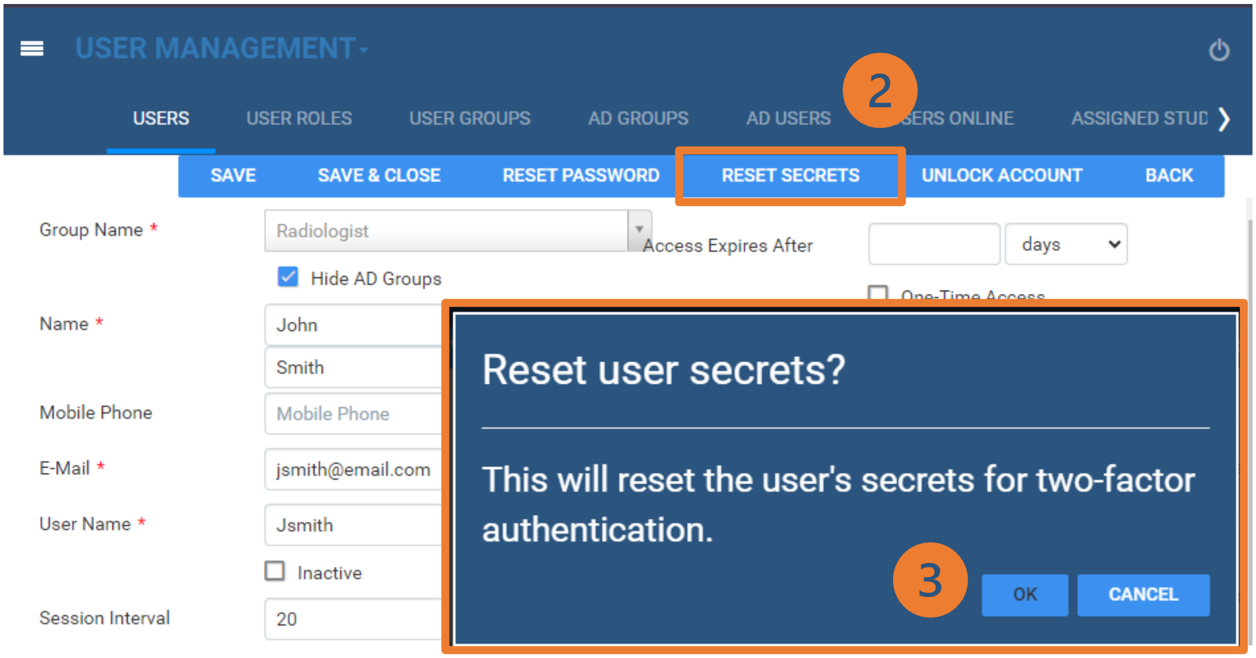
LOGIN

Reset secret

If you need to replace or reconfigure the authenticator app, an administrator must reset the secret key. This allows you to reconfigure the authenticator application with a new key.

SETUP → USER MANAGEMENT → USER

1. Open the user.
2. Select **RESET SECRETS.**
3. Select **OK.**



Group Name * Radiologist

Access Expires After days

☑ Hide AD Groups

□ One-Time Access

Name * John

Smith

Mobile Phone Mobile Phone

E-Mail * jsmith@email.com

User Name * Jsmith

□ Inactive

Session Interval 20

Reset user secrets?

This will reset the user's secrets for two-factor authentication.