ACCURO®

USER GUIDE

ACCURO CLOUD USER ONBOARDING GUIDE

Getting to the Cloud: A Step-by-Step Guide for Accuro Users

☎ 1.866.729.8889

🔗 www.AccuroEMR.com

TABLE OF CONTENTS

WELCOME TO ACCURO CLOUD

We're transitioning our clients to Accuro Cloud to stay at the forefront of digital technology, and to ensure your user experience is everything it should be.

GET STARTED

You will receive communication letting you know it is time to create your Accuro ONE ID. Once you create your new log-in, your account will move to Accuro Cloud. Once you're ready to begin, please follow the below steps.

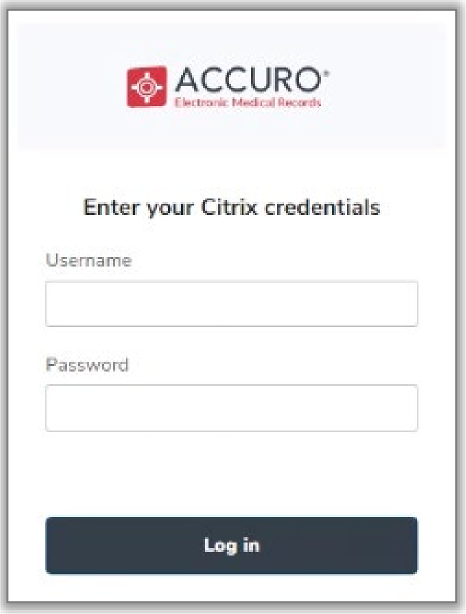
User Account: Accuro ONE ID

Accuro ONE ID is your new log in. This will help you gain access not only to Accuro, but also to our other products going forward.

To get started:

1. Navigate to **accuro.cloud/upgrade.**
2. Log in with your current Username and Password.
3. Create a new Password for Accuro ONE ID. Make sure it fits all the listed requirements.
4. Set up your preferred Multi-Factor Authentication (MFA). Please review the Multi-Factor Authentication section of this document for more information and assistance in setting up MFA.
5. When prompted, enter your unique work email address if you have one.

You are now ready to log in to Accuro using your new Accuro ONE ID at Accuro.Cloud! Make sure to bookmark this new link on your computer's web browser.



Note: If you are using ACCUROgo, your ACCUROgo login is your Accuro ONE ID. You can now log in to Accuro Cloud using those credentials.

Why Should I Add My Email Address?

Adding your email address to your ONE ID account ensures the best security for your office and your patient's data. You will be notified by email if there is any new device login activity on your account.

This also allows us to contact you in the event of any issues with Accuro, and send you more information about other products, upcoming events, and education included in your subscription.

The following are the different types of emails you can expect from Accuro:

Required Emails (Accuro ONE ID System Emails)

- Welcome (**account activation**) emails.
- Password resets.
- Account lockout help.
- New device login detected.
- Multi-factor enrollment and reset.

Optional Emails

For optional emails, you will be able to manage your **opt-out preferences** using a link in the email:

- Information about new features and products.
- AccuroEMR issues or interruptions.
- Details about programs included in your subscription.
- CONNECT AccuroEMR newsletter.
- Event announcements.

Note: It is important to watch for phishing attempts through email. If you receive an email from us that you're not expecting, do not click on any links or attachments included in it. We will **never** ask you to provide your **password** or user **credentials** by email.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication is a security technology that requires more than one method of authentication. Entering your password is the first required method while your next method is selected by you. Speak to your IT professional to see what options might be best for you.

Note: Multi-Factor Authentication is required as part of the transition to Accuro Cloud. However, more than one additional Authentication method may be used for your account if desired. The first time you set up MFA, you will be prompted to prove your identity. While subsequent logins may not prompt you, certain conditions (location, change of device, etc.) will require you to prove your identity as an additional security measure.

Phone

If you are comfortable using your smart phone for authentication, here are some options that might be right for you:

Okta Verify App

To prove your identity with Okta Verify, you can either **approve a push notification** or **enter a one-time code** the first time you sign in to Accuro Cloud.

Select **iPhone** or **Android** as your device type, then tap the link to **Download** Okta Verify or Google Authenticator onto your mobile device. You can also download your MFA app using the links below:

Okta Verify: Android / Apple iOS

1. Download the application with the above links.
2. Open the application and select Add Account > Organization > Scan a QR Code.
3. At the Setup Okta Verify screen, scan the QR Code with your smart phone.
4. After completing this step, you will see the account added in your Okta Verify app.
5. Whenever prompted for your Okta Verify code, select Push Notification and approve on your smart phone OR select enter code, open your Okta Verify app and copy the code in the field.

Note: Okta Verify codes are only valid for a limited time. If you get an error when entering your verification code, you may need to return to your MFA app to get a new 6 digit code.

Google Authenticator: Android / Apple iOS

1. Download the application with the above links.
2. Open the application and select Scan a QR Code or Enter a Setup Key.
3. Scan the QR with your smart phone or select **Can't scan?** to enter your secret key.
    a. After scanning your QR code, enter the Code shown on your device.
    b. After selecting **Can't scan?** enter your setup code into the Secret Key Field.
4. After completing either of these steps, you will see the account added in your Google Authenticator app.
5. Whenever prompted for your Google Authenticator passcode, open your Google Authenticator app and copy the code into the field.

Note: Google Authenticator codes are only valid for 30 seconds. If you get an error when entering your verification code, you may need to return to your MFA app to get a new 6 digit code.

Computer

The Security Key or Biometric Authenticator gives you the ability to pick computer authentication options that you might already be using in your clinic. Some common options are:

Windows Hello

This authentication method uses a biometric (fingerprint, iris scan, or facial recognition) or PIN. It is enabled for all Windows 10 users. Please see Windows Hello Setup for more information.

Touch ID (Apple Devices Only)

Much like Windows Hello, Touch ID utilizes a fingerprint as a biometric to authenticate your account. Touch ID is only set up for iPhone, iPad, and MacBook Pro. Please see Touch ID Setup for more information.

YubiKey

This is a physical hardware device (very similar to a USB Stick) and is used as a security token that allows users to add a second authentication factor. Please see yubico.com for more information.

Authy

Authy will allow you to use either your computer or mobile device to set up MFA. It can work offline and is a great option for those wishing to use multiple ways to authorize accounts. Please see authy.com for more information.

Logging in with your Accuro ONE ID

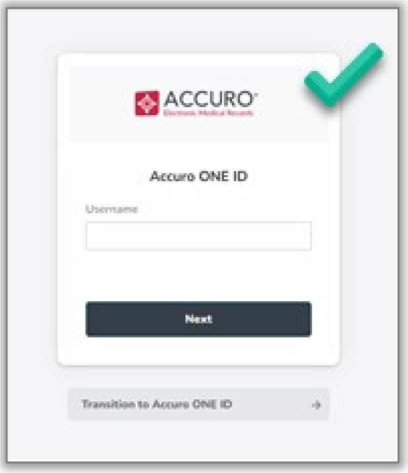
Now that you've transitioned to Accuro Cloud by creating your Accuro ONE ID, it is important to log in at https://accuro.cloud to benefit from using MFA and to keep your patient records protected. **Your previously used login will expire soon, so be sure to bookmark Accuro Cloud on all devices you use to access Accuro**:

- Different exam rooms at your clinic.
- Laptop or remote devices.
- Your home computer.

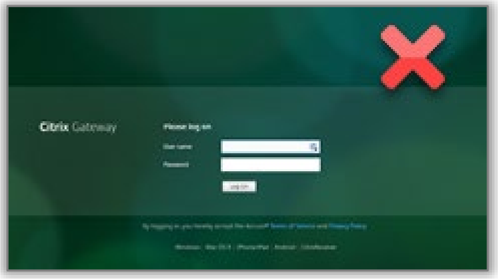
We have provided a checklist for fully transitioning to Accuro ONE ID below:

1. Create Accuro ONE ID.
2. Bookmark https://accuro.cloud on your favorite browser (we recommend Google Chrome).
3. Create a desktop shortcut to get to your Accuro login quickly.
4. Delete old bookmarks and shortcuts from all devices where you use Accuro.

Going forward, you will see the screen to the right when logging in. You can also create a desktop shortcut using the link https://accuro.cloud.



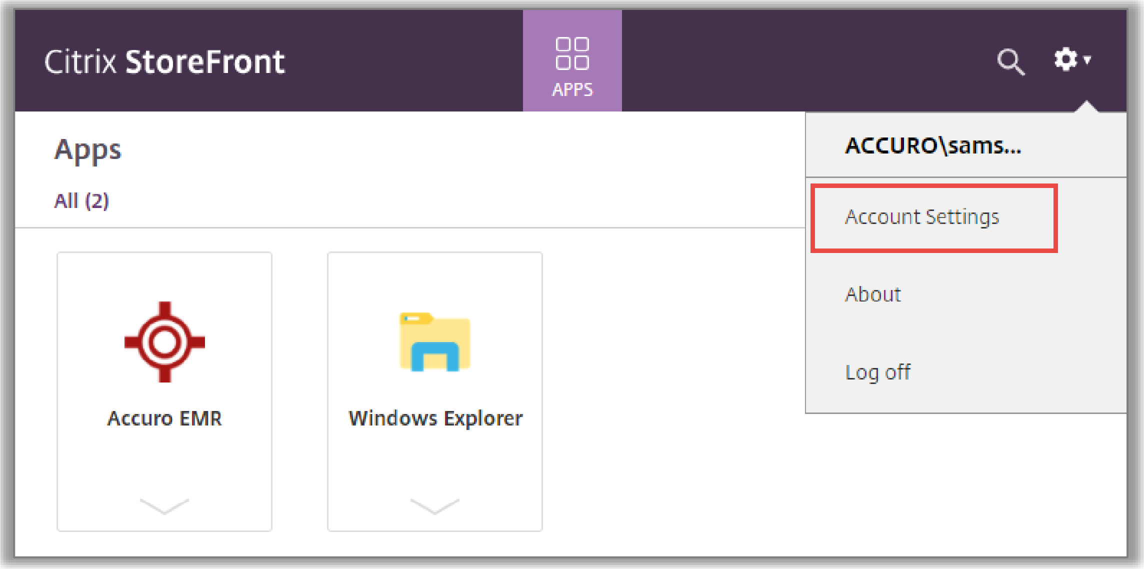
The Citrix Gateway will no longer be displayed (as seen on the right). Navigate to https://accuro.cloud to log in instead. We recommend deleting your existing shortcuts and bookmarks to ensure you don't log in using the previous method.



What's New?

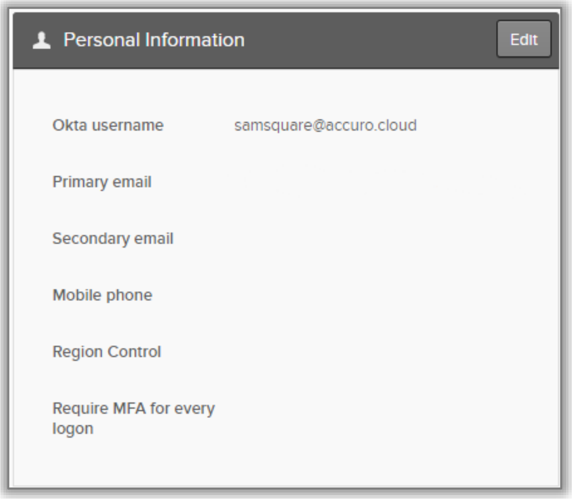
Once you are logged in with your new Accuro ONE ID, you will have some new options available to you on your Citrix StoreFront. With the move to the Cloud, your StoreFront and Accuro will not change and this move will not affect your experience once you are logged into Accuro.

1. Click on the Configure button in the top right of the site > Account Settings



2. In Account Settings you can:

- Update your personal information such as your email address and region

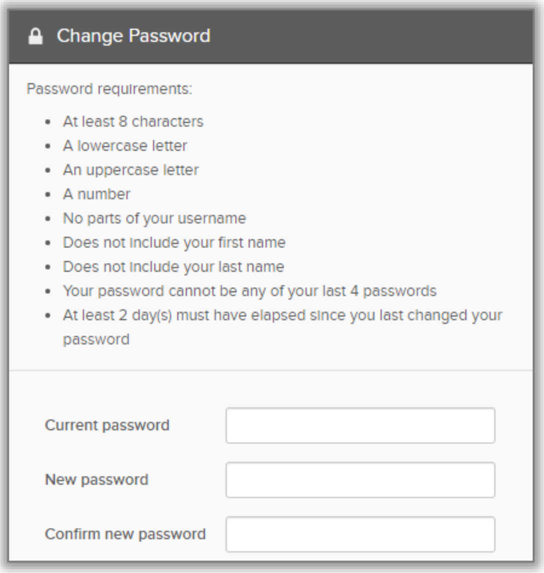


Personal Information

Edit

Okta username	samsquare@accuro.cloud
Primary email	
Secondary email	
Mobile phone	
Region Control	
Require MFA for every logon	

- Change your password



Change Password

Password requirements:

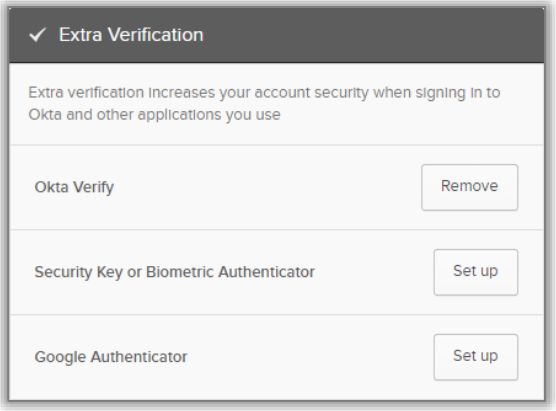
- At least 8 characters
- A lowercase letter
- An uppercase letter
- A number
- No parts of your username
- Does not include your first name
- Does not include your last name
- Your password cannot be any of your last 4 passwords
- At least 2 day(s) must have elapsed since you last changed your password

Current password

New password

Confirm new password

- Update your Multi-Factor Authentication



✓ Extra Verification

Extra verification increases your account security when signing in to Okta and other applications you use

Okta Verify	Remove
Security Key or Biometric Authenticator	Set up
Google Authenticator	Set up

SUPPORT

Clinic Support

QHR Technologies Inc. Client Services
Phone: 866.729.8889
Email: accuro@QHRTech.com

Content Disclaimer

All content in this User Guide is valid and deemed correct as of the date of publishing. The images and content are subject to change as the product develops and evolves. To view the most current version, please refer to the Accuro User Guide accessed from within Accuro (Accuro Start Menu > Help > Accuro User Guide).