



USER GUIDE

ACCURO CLOUD SYSTEM ADMINISTRATOR ONBOARDING GUIDE

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



 1.866.729.8889

 www.AccuroEMR.com

TABLE OF CONTENTS

WELCOME TO ACCURO CLOUD	3
GET STARTED	3
Accuro	3
User Account: Accuro ONE ID	5
Multi-Factor Authentication (MFA)	5
What's New?	8
FAQs and Key Information	10
SUPPORT	11
Clinic Support	11

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.

As an Accuro System Administrator, you are in control of deciding when your clinic is ready to move to Accuro Cloud. An Accuro System Administrator may be an Office Manager, Provider, or IT Specialist (please see [the FAQ and Key Information](#) section for more information).

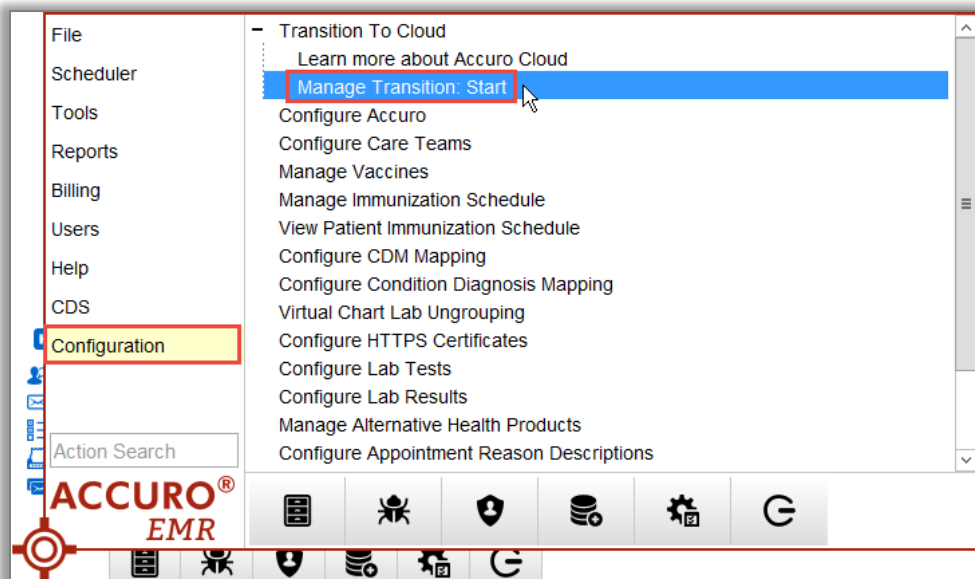
This guide is designed to walk you through the set-up steps as you move to Accuro Cloud. This transition to the Cloud will eventually be necessary for all clients.

GET STARTED

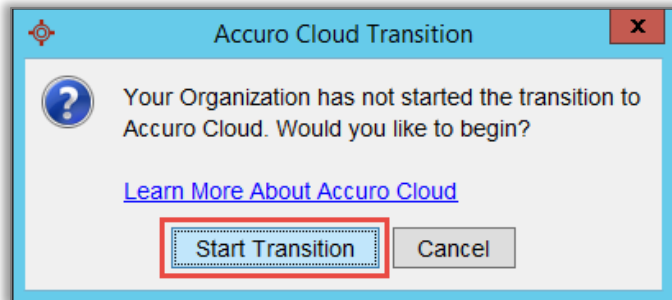
You will receive communication from QHR Technologies letting you know when your clinic is eligible to move to Accuro Cloud. Once you are ready to begin the transition, please follow the below steps.

Accuro

1. Log in to Accuro and navigate to the Accuro start menu.
2. Accuro Start Menu > Configuration > **Transition to the Cloud** OR Search: Accuro Cloud, Transition to Cloud, or ONE ID.
3. Select **Manage Transitions: Start**



4. The Accuro Cloud Transition pop-up will appear. Select **Start Transition** to begin.



Your clinic is now ready to have users sign up for their new Accuro ONE ID! Follow the [User Account: Accuro ONE ID](#) instructions to create your own Accuro ONE ID, then communicate to all the users in your clinic and encourage them to follow the user steps for their new login.

Note: If you are unable to complete the above workflow, you might not be an Accuro System Administrator.

User Account: Accuro ONE ID

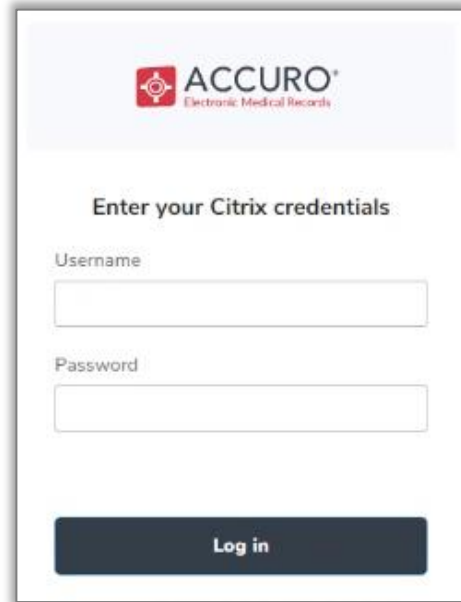
Accuro ONE ID is your new log in. This will help you gain access not only to Accuro, but also to our other products going forward.

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!](https://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.



The screenshot shows a web browser window displaying the Accuro login interface. At the top, the Accuro logo and 'Electronic Medical Records' are visible. Below the logo, the heading 'Enter your Citrix credentials' is centered. There are two input fields: 'Username' and 'Password'. At the bottom of the form is a dark blue button labeled 'Log in'.

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. Or, 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.

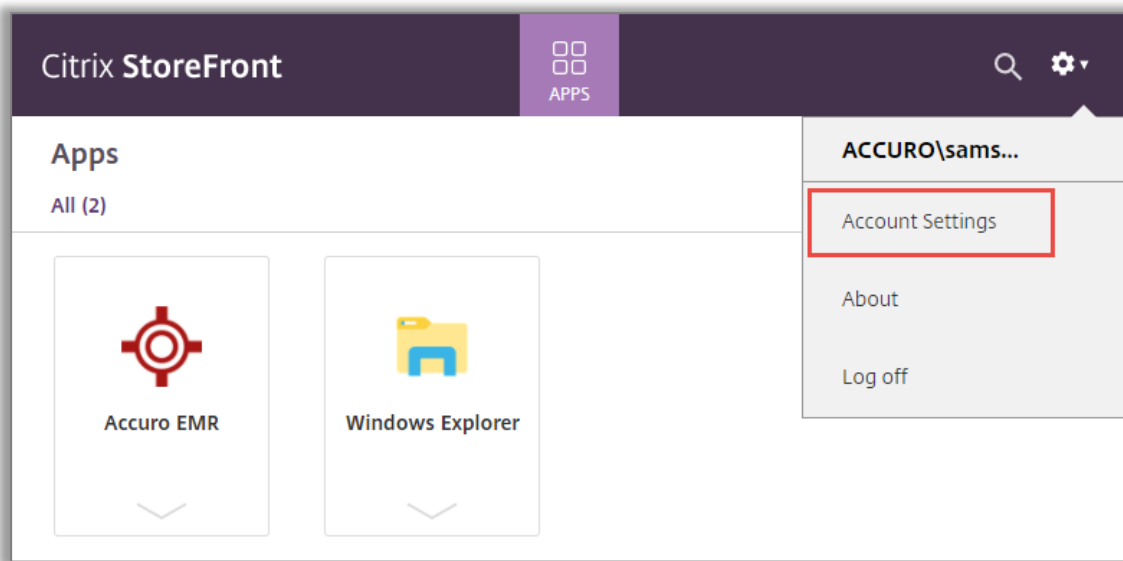
Authy

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.

What's New?

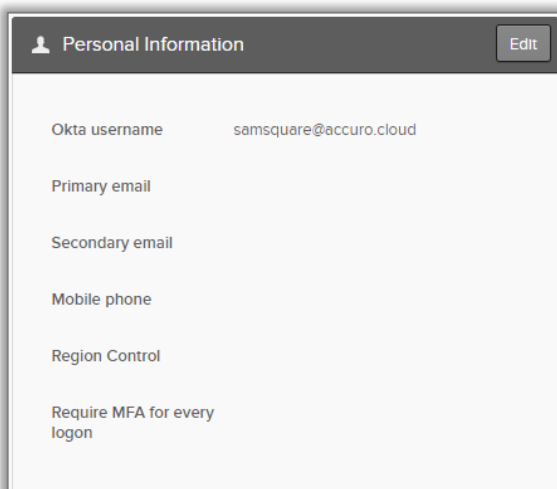
Once you're logged in with your new Accuro ONE ID, you will have some new options available to you on your Citrix StoreFront. With the move to the Cloud, your StoreFront and Accuro will not change and this move will not affect your experience once you are logged into Accuro.

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



2. In Account settings you can:

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



- 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	<input type="button" value="Remove"/>
Security Key or Biometric Authenticator	<input type="button" value="Set up"/>
Google Authenticator	<input type="button" value="Set up"/>

FAQs and Key Information

Question	Answer
How do I know if I am an Accuro System Administrator?	You can add and remove users in Accuro. Think you might be an Administrator? Try to search Transition, ONE ID, or Cloud in the Accuro Start Menu.
Why does a System Administrator need to initiate the process?	We want the control to remain within your clinic. We understand that this change might cause some questions and you might want to enable users at certain times. Please see our Accuro System Administrator information page or Clinic Support for more information.
Is everyone doing this?	Yes! Transitioning to the Cloud will happen in waves, but all Accuro users will eventually be on Accuro Cloud and using Accuro ONE ID.
My clinic has its own Single Sign-On Provider.	Please contact us at 1-866-454-4681 for federation options.
We don't have the ability to switch to Accuro Cloud.	Your clinic might be hosted on Local servers. That means your data is housed in your own clinic rather than our data centres. Local clinics will be contacted to transition in later 2021.
Will my Accuro ONE ID work for everything right away?	Unfortunately, Accuro ONE ID will not work for Accuro Web and Accuro Mobile. Please use your previous credentials to continue using these platforms.

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).