FREQUENTLY ASKED QUESTIONS

Moving from Accuro ASP to Accuro Cloud

OVERVIEW

What is different? What has changed?

Initially, the only change will be to the new URL and login to access Accuro; your data hosting will remain the same. Accuro Cloud is a more modern, more secure offering than Accuro ASP. It is built on Microsoft Server 2019 while Accuro ASP is built on Microsoft Server 2012, and it has a web-application-firewall front-end to help detect and mitigate certain types of malicious activity. It employs a best-in-class identity management solution that provides strong multi-factor authentication and other access controls to significantly improve security. It also contains improvements like faultdomains to provide increased reliability.

What are the benefits of moving to Accuro Cloud?

With Accuro Cloud, you'll get:

- Multi-factor authentication (MFA) for user logins
- World-class security services that provide stronger defenses to our already-secure solutions
- The option to take full user management control with your own federated, single sign-on provider

When must we make the transition to Accuro Cloud?

To get the enhanced security features mentioned above, you should make the transition as soon as you can.

I'm a locally hosted customer. Can I move to Accuro Cloud?

Yes. You first need to move to our ASP hosted solution and then we can move you to Accuro Cloud.

Where will our data be stored?

Your data will always be stored in Canada in a professionally managed co-location data center. Active data is stored in a data center in Toronto, Ontario, and backups of that data are stored in the same Toronto data center with another set stored in our Kelowna, British Columbia data center. In the not-too-distant future, and with your consent, some or all of your data will be stored in Azure Canada Central and Azure Canada East.

Is this a 'big bang' transition (in other words, a hard cut over from current to new)?

No, you can make the change gradually. Your users can, for a period of time, log in to either Accuro ASP or Accuro Cloud. This allows you to move a few users at a time. It also allows a user who is having difficulty with MFA to immediately, but temporarily, go back to using their existing ASP login until the issue is resolved, either through education or by changing how that user does multi-factor authentication.

How can we test this before we commit?

Initially, the only change will be the new URL and login to access Accuro; your data hosting will remain the same. The transition has been designed so that the vast majority of users will be able to complete their own account activation without impacting their current ASP login. This means that for a period of time, users can revert to the login process they use now.

Are there any additional costs?

No, the cost of Accuro Cloud is the same as Accuro ASP. There is, however, additional cost for using Federation. See the Identity Management section below for more detail.

Is there any downtime or outage associated with this transition?

No, as soon as the administrator enables the transition, users can immediately begin activating their Accuro One ID and logging into Accuro via the new Cloud URL.

This sounds too easy. Why isn't it going to be painful?

There are several reasons why this transition will be painless:

- QHR has dedicated significant time and resources to making the experience easy and allowing clinics to manage the process themselves
- There is no data transfer or data transformation associated with moving from Accuro ASP to Accuro Cloud
- Because users can access their data from either Accuro ASP or Accuro Cloud for a period of time, there is no risk to users as they will be able to fall back to a known functional state if they stumble in their early use of MFA

MULTI-FACTOR AUTHENTICATION (MFA)

Is MFA mandatory?

If you use QHR's included identity management solution, your users do have to use MFA to log in to Accuro Cloud. MFA is an important security feature for protecting your data. If your company uses federated identity management, however, you can set your own rules for identity management.

ACCURO

What types of MFA do you support or not support, and why?

We support a wide variety of MFA options, including one-time passwords (OTP), physical tokens such as Yubikey, MS Authenticator, Google Authenticator, or similar apps available for smartphones. We encourage your users to use a password manager, such as 1Password or similar, and many password managers have OTP and/or authenticators built in. We do not support MFA via SMS (text message on phones) or via email because they are not as secure as the methods we do support. Of course, if you use your own identity and access management system and federate it with our system, you can use whatever type of authentication you choose.

Tell me more about your support for multi-factor authentication

QHR's included identity management solution, known as Accuro ONE ID, supports 3 types of second factor authentication: Okta Verify, FIDO2, and Time Based One Time Passwords (TOTP). More information for each is given below.

- Okta Verify - A user-friendly mobile app provided by Okta that facilitates push notifications or fallback to one-time passwords. This is a recommended option when users reliably have access to mobile devices.
- FIDO2 - Labeled as Security Key and Biometrics, this is the technology that powers biometric authentication such as Windows Hello (fingerprint and facial recognition), Mac OS fingerprint recognition, as well as hardware security keys (e.g. YubiKey, Google Titan).
- Time Based One Time Passwords (TOTP) - Often referred to as Google Authenticator, this is the common technology of 6-digit passwords with limited validity. Despite being labeled as Google Authenticator, TOTP codes can be configured in a nearly infinite number of apps, including most password managers. This method is often the best starting point when a password manager is already in use.

Recommended Option

If you are comfortable using your smart phone for authentication, **OKTA VERIFY** is the choice we recommend for you.

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 onto your mobile device.

OKTA VERIFY: Android / Apple iOS

- Download the application with the above links.
- Open the application and select Add Account > Organization > Scan a QR Code.
- At the Setup Okta Verify screen, scan the QR Code with your smart phone.
- After completing this step, you will see the account added in your Okta Verify app.
- 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.

Other options for Multi-Factor Authentication without a smartphone

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 and 11 users. Please see Windows Hello Setup for more information.

TOUCH ID (APPLE DEVICES ONLY)

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

YUBIKEY

This is a physical hardware device, 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.

What if I want more options for my users' MFA?

If your users already have an identity provider, we can federate it through our Enterprise Premium offering. Contact us to find out more about this option. This is known as Enterprise Premium and you can contact us for more details.

IDENTITY MANAGEMENT

What are the possibilities for identity management?

You have two choices for identity management:

- Use QHR's identity management system
  - Offers strong MFA
- Use your own identity system and federate it with QHR's system
  - You can provide a seamless single sign-on experience
  - You can use strong, weak or even no MFA if you wish
  - You have complete control of the rules and experience for authenticating your users

What do we have control over with federation?

With federation, you have complete control. You can set security as high or low as you wish to achieve a balance between ease of use and protecting your system and data.

What do you recommend for identity federation?

Although there are many good identity management systems, including Okta, Microsoft Azure Active Directory, and many others, we opt not to recommend a specific solution. If you already have an identity management system, we can most likely federate with it using established (standardized) methods. We will federate with virtually any modern solution (Oauth 2.0, OpenID connect (OIDC), SAML 2.0).

Can we start with QHR doing identity management and then transition to federated later?

Yes, definitely. You can choose federated identity management either at the time you transition to Accuro Cloud or anytime after.

USER EXPERIENCE

Will my new login work with Accuro Web or Mobile?

Not at this time, though we have some exciting alternatives: the ability to launch Accuro in the browser (currently in preview and available to all cloud users); and ACCUROgo, a mobile Accuro companion application.

I already use ACCUROgo. Will my login change?

No. ACCUROgo already uses the same identity management system as Accuro Cloud.

All my users have been set up with Accuro ONE ID. How can I make sure they're not logging in through the old method?

You can request that QHR disable the old method, or you can do this using self-serve tools that will soon be available to you. If a user goes 60 days without signing in to their old login, it will automatically be disabled.

Will my clinic continue to use the Citrix Receiver?

Yes. We typically recommend that you continue using the receiver wherever it was used prior. With Accuro Cloud, however, we have a new Preview option available that allows users to select 'Launch Accuro in Browser' using a web browser such as Google Chrome, Safari, or Microsoft Edge.