Advanced Security for Acumatica

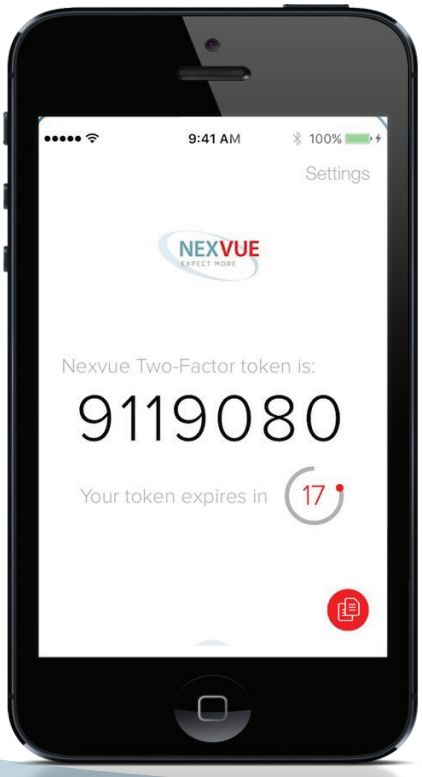
(Two-Factor Authentication)

Your Acumatica installation contains some of your company's most valuable information as well as some of its most sensitive information. Password protection is simply not enough to protect your company against hackers and breaches. Organizations that need the next level of protection are turning to two-factor authentication, or 2FA, to secure their information from unwanted intruders. Now NexVue makes 2FA available for Acumatica.

BENEFITS OF TWO-FACTOR AUTHENTICATION

Two-factor authentication is a two-step process of identifying a user before allowing access to a computer system. 2FA requires two different kinds of authentication factors—usually something you know and something you have. NexVue's two-factor authentication for Acumatica requires a password and a code that is delivered to your cell phone or email if you are trying to access the system from an unknown IP address. By entering the code, you are demonstrating that you not only know the password, but that you are also in possession of your phone, i.e., something you know plus something you have.

With 2FA, it is no longer necessary to ensure anyone who accesses your data is within the walls of your organization. Remote access becomes a viable option and in today's world of home offices, outsourcing, business travel, and field operations; secure, remote access is a must. 2FA also fills most compliance requirements.



Advanced Security sends a code to via email or text or to the Advanced Security app.

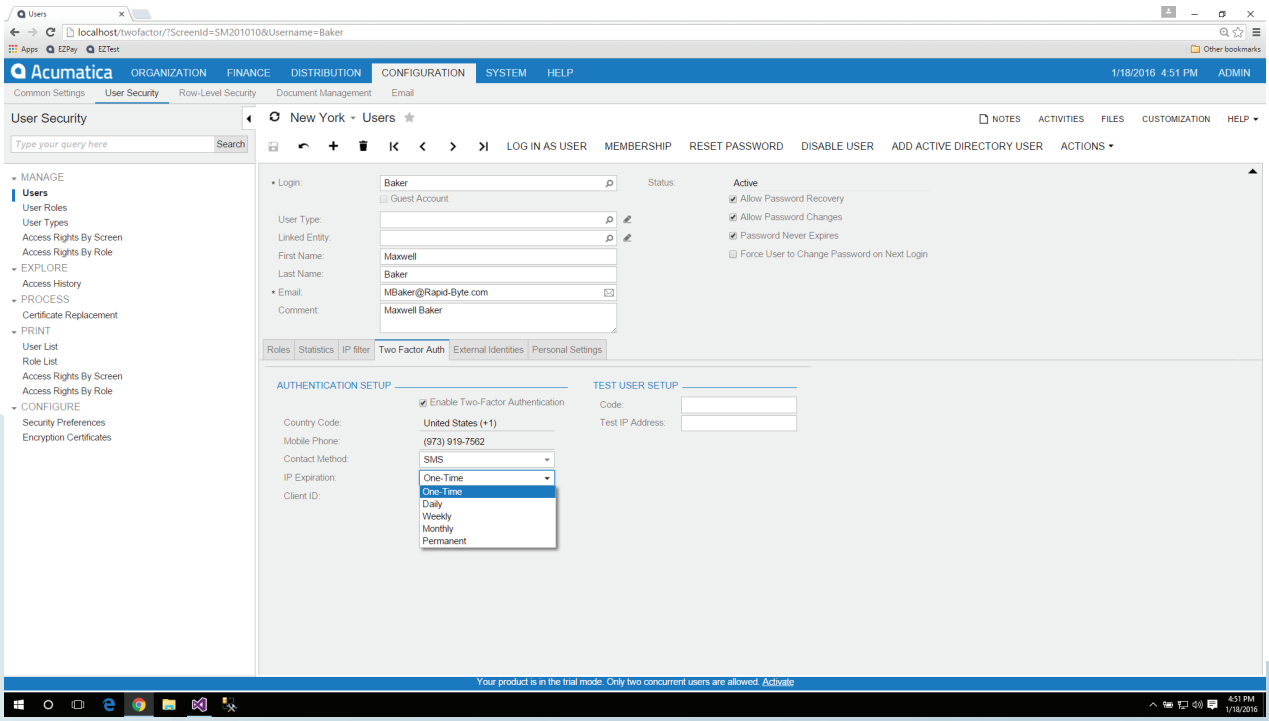
NEXVUE
EXPECT MORE

NEXVUE'S ADVANCED SECURITY

Advanced Security detects the user's current IP address. If the user is trying to access from an approved location, a password is sufficient to gain access. If Advanced Security does not recognize the location, it immediately sends a numeric code to the user's mobile phone or other device via text or email. The user can also obtain the code from the Advanced Security app, which generates a new code every 30 seconds. The user must enter the code into the Acumatica login screen to proceed. At that point, based in the user's profile, he may be able to save this location for a specified period of time-perhaps indefinitely if accessing Acumatica from a home office or for a just a week if accessing the system from a hotel.

Advanced Security provides secure, two-factor authentication for Acumatica, whether your installation is deployed on premises or in the Cloud.

Advanced Security is maintained at the admin level to add and delete users, define which level of security applies to individual users, and manage authentication devices. A complete report of all access is generated, giving the admin the information needed to trace any breach attempt.



Advanced Security allows you to determine if access from a particular IP address should be one-time access or permanent or something in-between.

Advanced Security makes your Acumatica implementation more secure, allowing a greater range of freedom for users.