

Password Requirements?

[Home](#) > [eICS](#) > [Community Resources - FAQs](#) > Password Requirements?



Question

Are there specific conventions for creating a password?

Answer

Yes. eICS was built according to the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act, both of which are based on the [National Institute of Standards and Technology](#) (NIST) security protocols. Additional security measures were implemented to meet or exceed industry best practices.

Helpful Links

[Juvare.com](#)

[Juvare Training Center](#)

[Announcements](#)

[Community Resources](#)

Conventions

Your eICS password must be formatted using the following conventions:

Length: Passwords must be a minimum of eight characters long.

Complexity: Passwords must use characters from three of the following four character sets:

- Lowercase letters
- Uppercase letters
- Numbers 0 - 9
- Any of the following special characters: - ! @ # \$ % ^ & * () { } []

Expiration: Passwords automatically expire in 90 days.

History: Passwords cannot duplicate the last five passwords in your account history.

Reset Delay: Passwords cannot be changed more than once in a 24 hour period.

Note: Depending on your system configuration, you may be locked out of your account after a preset number of unsuccessful login attempts. If this occurs, contact your eICS system administrator or **Juvare Support** at **1-877-771-0911**.

Guidelines

We recommend that you follow these guidelines.

- Change your password every 90 days.
- Use a unique password for eICS; pick a password that is different from the password you use to access other software applications.
- Do not store written documentation of your password near your computer or where it might be visible to others.
- Do not reveal your password on questionnaires or security forms.
- Do not reveal your username, login ID, or password to anyone, including your co-workers, supervisor, or family members.

Other Password FAQs

Q: If I use multiple products (such as eICS, EMResource, and EMTrack) and I change the password for one, will it change it for the others?

A: Yes, if you have linked your accounts to a single username and password.

Q: Is the password requirement a minimum of eight characters or exactly eight characters?

A: The password requirement is for a minimum of eight characters. The requirement also includes using at least three out of four character sets: a lowercase character, an uppercase character, a special character, or a number.

Q: How many characters must I change when I change my password?

A: One.

Q: When a user tries to log in after their password expires, are they forced to change it or are they locked out?

A: The user is forced to change their password upon logging into the application.

Q: Are Domain and Facility Administrators still be able to reset passwords for users?

A: Yes.

Q: Is there an alternative method for handling a forgotten password for eICS users who may not have access to email during an incident?

A: Users can still use the phone number validation on both web and mobile. Users can also call the Support Desk 24/7.

Q: What happens if the user has no security question set up?

A: That user is required to call their System Administrator or Juvare Support to reset their password.

Q: What happens if the security question is set up?

A: When the user selects the **forgot password?** link on the login screen, the application sends an email to the user's email address. This message includes a link to reset the password. This link can only be used for one password reset, and expires after one hour.

Q: Can the system administrator ask the security question and then provide the password to the user?

A: No, this is not secure and actual passwords should never be visible to anyone other than the user.

Q: Has Juvare explored the use of finger image technology?

A: Juvare is currently exploring the use of this technology for mobile apps, but has not explored using it for Web applications yet.

Need More Help?

For security and verification reasons, local application administrators have the ability to unlock your account. When necessary, Juvare Support can help administrators and users reset passwords and unlock accounts. Contact the Support Desk by sending an email to support@juvare.com or calling 1-877-771-0911.