



Two-Factor Authentication Enrollment Instructions

By December 31, 2017, all Alion employees must move to two-factor authentication when accessing company machines or information to remain compliant with new DFARS regulations from the U.S. Government.

While there are a variety of ways to approach two-factor authentication, we have elected to use a password and PIN combination, in line with industry best practices. The password will be your standard Alion password, and the PIN will be generated using an Entrust Identity Guard token (shown right) that we are in the process of distributing to all employees. This token will display a continually changing set of numbers that you will add to your password to authenticate and allow access to Alion systems and Internet-accessible Alion sites, like PeopleSoft, IETIME, IEMAIL, and KMS.



Figure 1-1: Entrust Token

STEP-BY-STEP INSTRUCTIONS

The instructions that follow outline the steps for self-registration and use of the token. If you have questions, email noc-security-team@alionscience.com.

1. After you receive a hardware token, and after your account is populated in the self-registration portal on November 20, the first step is to register your account and activate your token at: <https://auth.alionscience.com/>

2. Login Page – Enter your Alion credentials (username / password) at the prompt, leaving the 'Group' field empty. See figure 1-2 for the login portal.

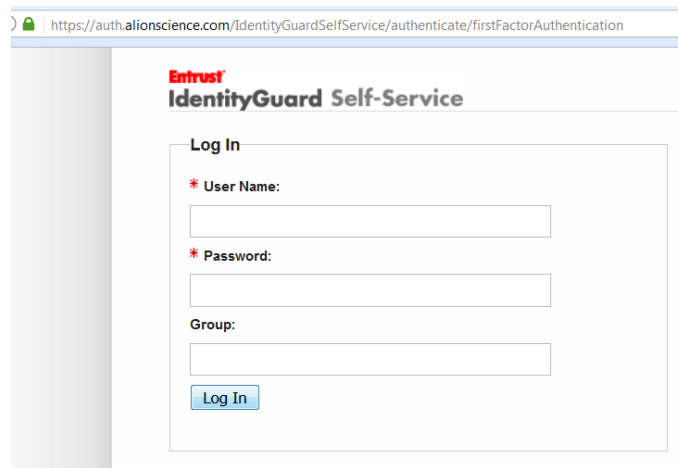


Figure 1-2 Login Portal

3. Personal Information – On the first page, please enter or confirm your full name and click the 'Next' button. See figure 1-3 for Personal Information.

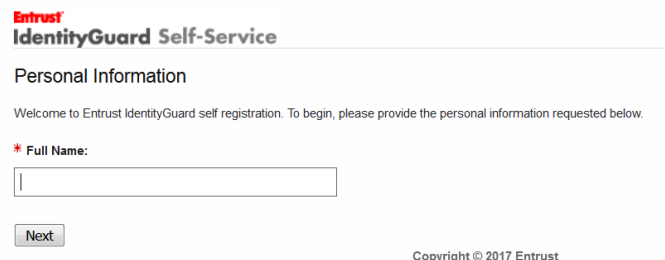


Figure 1-3 Personal Information

4. Question & Answer Pairs – On the next page, you are required to enter five question-and-answer pairs that the system can use as an alternate method of authentication in case your hardware token is unavailable. Four of these will be selected from a list, while the fifth is user-generated. These Q&A pairs form one alternate method of authentication if you lose access to your token. See Figure 1-4 for Questions and Answer Pairs.

**** Responses are CASE SENSITIVE, so take care when answering. ****

Entrust
IdentityGuard Self-Service

✓ Your personal information has been successfully saved!

Questions & Answers

You must answer 4 predefined questions and one question of your own choosing.

Predefined Questions

Predefined Question 1:
Please choose a question...
Answer:

Predefined Question 2:
Please choose a question...
Answer:

Figure 1-4 for Questions and Answer Pairs

5. Self-Administration – Once you have finished the initial portion of the registration, you will be taken to the Self-Administration section of the site. For the first time you access it, you will be prompted for a challenge using the Q&A pairs that you just entered. On subsequent visits, it will prompt you for a response from your registered token. You may also use your Q&A pairs or a Temporary PIN at a later date if your token is unavailable. See Figure 1-5 Self-Administration.

If you made a mistake during the initial Q&A registration process and cannot progress due to an incorrect answer, please contact your site administrator or the Helpdesk for assistance.

Entrust
IdentityGuard Self-Service

✓ You've successfully completed your registration with Entrust IdentityGuard

Self-Administration

Challenge

Please answer the following questions.

What was the name of your first girlfriend/boyfriend?

What is your favorite drink?

What is your best friend's first name?

OK Cancel

Figure 1-5 Self-Administration

6. Self-Administration Actions – Select “I’d like to activate my hardware token so I can start using it” link to begin registering your token. You will then be asked to confirm your choice; select “Yes” at this point. See Figure 1-6 Self-Administration Actions.

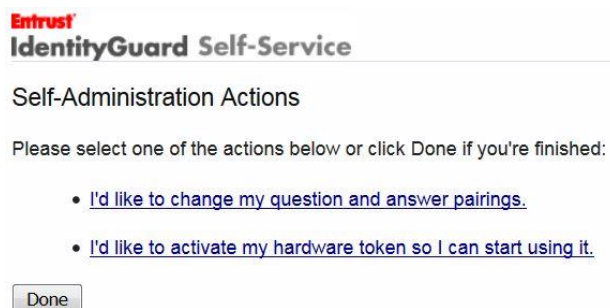


Figure 1-6 Self-Administration Actions

- 6.1 Confirm choice, see Figure 1-7 Confirm Choice

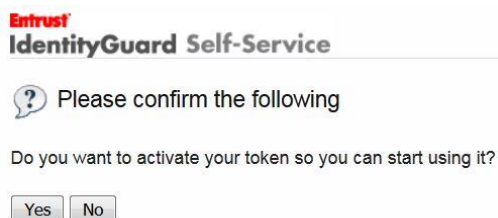


Figure 1-7 Confirm Choice

7. Token Activation – The reverse side of your token displays the 10-digit serial number. Enter that number as shown in the first box. On the next page of these instructions, see Figure 1-8 Token Activation.

- 7.1 Skip over the section regarding the Token Name.

- 7.2 For the final box, first generate a response by pressing the button on your token, and then enter the 8-digit number as shown and click “Ok”. If you receive an error as to an incorrect response or serial number, please double-check the values supplied and try again.

Token Activation

* Enter your token's serial number:

Token Name

Enter a name for your token:

If you don't provide a new name for your token above, then the existing name chosen below will be used.

Choose an existing name for your token:

 ▼

* Enter your token's response:

OK

Cancel

Figure 1-8 Token Activation

8. Completing Registration - Once your token has been registered, you will be brought back to the Self-Administration Actions screen. Click "Done" to log out.

The Entrust IdentityGuard Desktop Client

On 11/13/2017 the desktop client will be pushed to all Alion enterprise desktops. Until your token has been registered you will not be prompted to enter a response from your hardware token.

There are three use cases for which the client will prompt for a second-factor authentication when using your Alion credentials; Local computer accounts will not be required to use the Two Factor Authentication:

1. During Windows login
 2. Changing your domain password
 3. Elevated credential prompts
9. Desktop Login Screen – The initial first-factor login process should be unchanged; continue to enter your Alion username / password at the prompts. See Figure 1-9 Desktop Login Screen.



Figure 1-9 Desktop Login Screen

10. Online Challenge Response Screen – Once you have registered on the Self-Service portal, you will be prompted for a second-factor challenge. See Figure 1-10 Online Challenge Response.



Figure 1-10 Online Challenge Response

Information:

- Token Serial# - This should match the token you have registered, and is found on the reverse side of the device.
- Token Answer – Press the button on your token to generate a one-time-password (OTP), then enter the 8-digit response in the box and hit the arrow to continue. The OTP generated by your token will change every 30 seconds, and each response may only be used once.
- Use Temporary Pin – If you have forgotten, lost, or otherwise misplaced your token, please contact your local site administrator or the Helpdesk for a temporary PIN that you may use. This PIN is good for 24 hours, or until you authenticate with your old token or a replacement, whichever comes first. Click this link to enter your PIN.
- Configure Offline Q&A – The first time that you log in after completing IdentityGuard registration, this box is automatically checked. Proceeding with this enabled allows you to answer a subset of the questions you previously registered, and will securely cache the responses to provide one way of authenticating if this machine is offline or away from the Alion network. *Answers that you provide during this initial setup are CASE SENSITIVE, so please be sure that they are correct.* If you ever update your Q&A pairs through the Self Service portal, you may manually check this box to update the locally stored cached values.
- Download Offline Tokens – As an additional method of authenticating while offline or away from the Alion network, the client will download and encrypt a number of token challenges, allowing you to respond with your token. *Be aware that this offline refresh occurs only during the login to the Windows desktop.* By default, the allotted time period is 3 days to provide for after-hours or weekend usage if a laptop is removed from the network. By checking this box prior to answering

the second-factor prompt, additional challenges will be downloaded to extend that time period to 14 days. If further access beyond this time period is required, you may authenticate using the Offline Q&A option, or an Offline Temporary PIN that you may receive by contacting your site administrator or the Helpdesk.

11. Offline Challenge Response Screen – If your computer is not on the Alion network or the IdentityGuard server is unavailable, the desktop client will go into offline mode. In this mode, if you have cached token challenges available, you may continue to use your token to respond as normal. You also have the choice to use your Q&A responses if you successfully answered a previous challenge using them, or an Offline Temporary PIN that you receive from your site administrator or the Helpdesk. Please note that any Offline PIN that you receive will only remain valid until you answer a successful online challenge through your desktop login. Click on the links as shown to switch between the various options. Additional instructions may be found by clicking the 'What is my offline temporary PIN?' and 'How do I use Q&A?' links. See Figure 1-11 and Figure 1-12 Offline Challenge Response Screens.



Figure 1-11 Offline Challenge Response Screens



Figure 1-12 Offline Challenge Response Screens