NaviNet® Security Officers

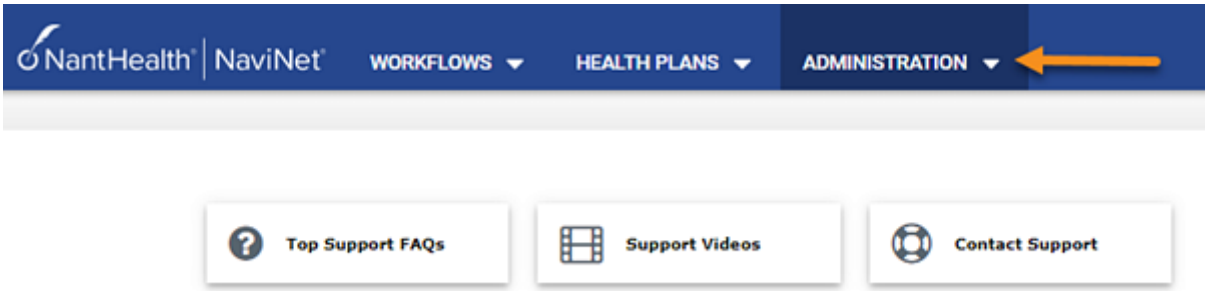
Contents

NaviNet security officer tasks

As a NaviNet security officer, you must ensure compliance by managing user access to NaviNet. The Licensee Designated Security Officer Agreement outlines your responsibilities. Watch: Security officer training.

Note *Your NaviNet-enabled office must have at least one NaviNet security officer. Consider having two security officers, especially if you're in a larger office. To update your office's security officer assignments, see Change or add a security officer.*

To complete security officer tasks in NaviNet, click the **Administration** menu at the top of the screen.



Compliance rules

Follow these rules to avoid compliance violations:

- Every month, review the NaviNet user accounts associated with your office.
- Terminate user accounts that are no longer in use.
- Implement or take training on how to identify and report phishing, social engineering, and spoofing attempts.
- Verify the identity of every person who you create a NaviNet account for.
- If you provide sign-in credentials through phone, web, or email, ensure that you send the information to the authorized user only.
- If you receive suspicious or unusual emails related to a NaviNet user account, such as multiple denied password recovery attempts or password resets, contact the user directly to investigate or terminate the user account.
- If a NaviNet user account is compromised—for example, more than one user used the same sign-in credentials, or an unauthorized user accessed the account—terminate the account immediately and contact NantHealth Support.

Create new users in NaviNet

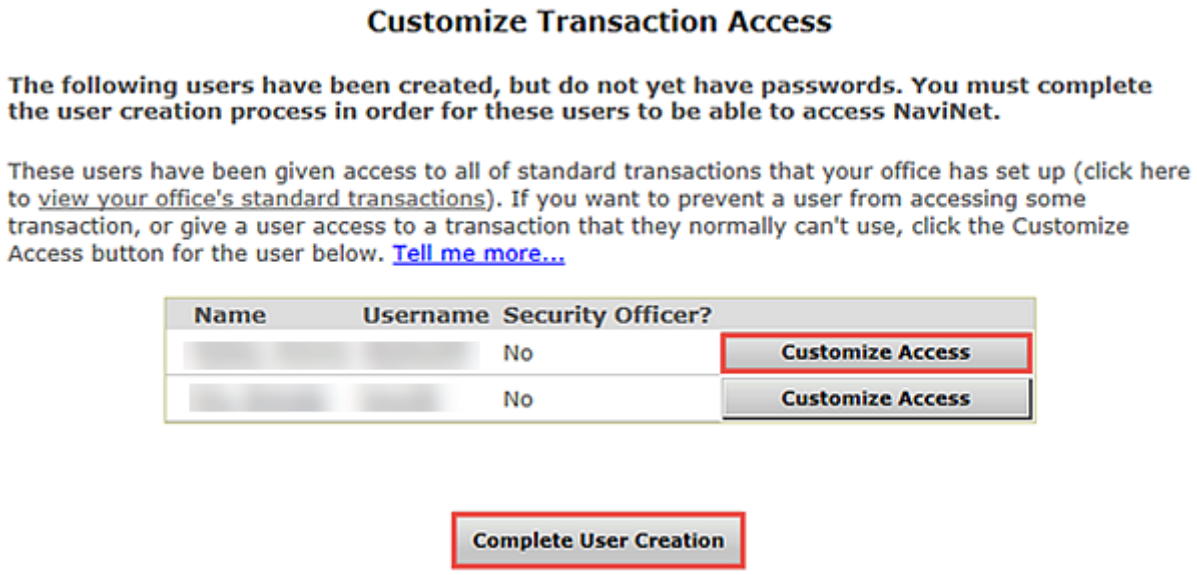
Only a NaviNet security officer can add a new user to NaviNet. This new user can be a physician, a clinician, or any user in your office who benefits from using NaviNet.

Do not add users from third parties that you contract with, such as billing or credentialing agencies. Third parties must create their own NaviNet office and user accounts.

If you're not a security officer, you don't see the **Administration** menu and can't perform these steps. To find your NaviNet security officer, see Find your NaviNet security officer.

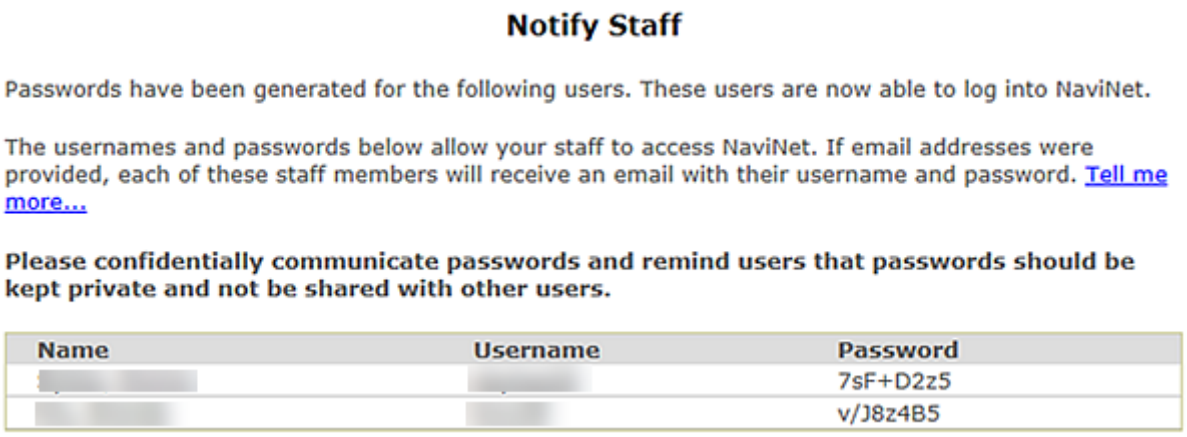
1. On the NaviNet toolbar, select **Administration > Create New User**.
2. On the User Creation screen, follow these steps for each new user. You can add up to three new users at a time.
   a) Type the user's first name, last name, and contact number. Type the name *specific to that user*. Do not type a generic name, such as Team, Billing.
   b) If available, type the new user's email address so we can send them their username and temporary password.
   c) Choose whether to grant the new user NaviNet security officer privileges. If you do, that user must review and accept the NaviNet Security Officer Agreement when they sign into NaviNet.
   d) Click **Add User to List**. The new user information appears in the lower part of the screen.
3. After you add up to three users, click **Continue User Creation**.

   The Customize Transaction Access screen appears. By default, the system gives new users access to all transactions, as determined by each health plan. We also generate a unique username for the user based on their first name initial and last name.



4. To review or edit user access privileges, click **Customize Access** next to a user's name. Enable or disable transactions for the user as needed, and then click **Complete User Creation** at the end of the screen to return to the Customize Transaction Access screen.
5. After you finish editing access for all the users, click **Complete User Creation**.

   The Notify Staff screen appears.


Notify Staff

Passwords have been generated for the following users. These users are now able to log into NaviNet.

The usernames and passwords below allow your staff to access NaviNet. If email addresses were provided, each of these staff members will receive an email with their username and password. Tell me more...

Please confidentially communicate passwords and remind users that passwords should be kept private and not be shared with other users.

Name	Username	Password
		7sF+D2z5
		v/J8z4B5

6. View the new users' usernames and passwords.
   - If you provided email addresses for the users, click **Continue**. We'll send them their username and temporary password in two separate emails.
   - If you did *not* provide email addresses, you must note the passwords in this screen, and confidentially communicate them to each user. Then, click **Continue** to exit the screen.

When the user signs in for the first time, they must change their password and verify their email address.

If you create a new user and then realize that you entered a portion of the user's information incorrectly, you can fix it by terminating and then recreating the user. To terminate a user, see Terminate user accounts.

Manage user permissions

The transactions available in NaviNet vary across health plans. To view the transactions for each health plan, go to **Health Plans**, click the health plan name, and then view the items under Workflows for This Plan. NaviNet comes with a default set of permissions that each health plan determined for their own transactions. You may need to enable or disable user permissions to specific transactions.

Additionally, before a user can view patient documents or practice documents that a health plan sends, you must enable permissions for each user.

1. On the NaviNet toolbar, select **Administration > Manage User Permissions**.
2. On the User Search screen, search for and select a user and then click **Edit Access**.

   The Transaction Management for User screen appears.

   After you click **Edit Access**, you may see a blank screen for up to 45 seconds, depending on your office size. Please wait.
3. In the **All Plans** and **All Groups** drop-down lists, choose values to narrow the list, if necessary. For the user to view patient documents and practice documents, you must choose a health plan and then choose **DocumentExchangeCategories** in the **All Groups** drop-down list to view and enable the options. For more details, see Enable user permissions to documents.

4. Click **Enable** next to a transaction to enable it for that user, or click **Disable** to disable it. If you don't see an **Enable** or **Disable** button, you can't change the permission for the transaction.

   Click **Enable All** or **Disable All** to enable or disable all of the transactions in the list for the user.

It may take up to 24 hours for your changes to take effect. The user must sign out and sign back in to use their new permissions.

Note *To add or remove security officer privileges for an existing user, an existing security officer must create a new user with the correct privileges and terminate the previous user account. To identify your NaviNet security officer, see Find your NaviNet security officer.*

Change or add a security officer

If you're a NaviNet security officer, you can create a new user and make them a security officer. However, if you must add or remove security officer privileges for an *existing* user, you must create a new user with the correct privileges and terminate the previous user account.

If your office has no security officer, an authorized individual must register as a security officer.

Review the NaviNet users in your office

To avoid compliance violations, review the NaviNet users in your office monthly. Review the active NaviNet users, determine which users *should* be active on NaviNet but aren't, and check for users who should be terminated.

For each user, you can view their username, status, last sign-in date, and whether the user is a security officer or a new user. (A new user is one who has a NaviNet account but has not yet signed in.) You can also see when a user's password will expire, and when the system will disable a user's account based on inactivity.

Use the **User Status** and **Combined User Status** menus to find users by status. See User account statuses for a description of each status.

1. On the NaviNet toolbar, select **Administration > Manage Users**.
2. On the User Search screen, provide the search criteria and click **Search**. For example:
   - To view all active NaviNet users in your office (users who created their own password and signed into NaviNet), select **Active** in the **User Status** menu. The **User Status** menu has nine statuses to choose from. See User account statuses for a description of each status.
   - Use the **Combined User Status** menu for a broader view. For example, select **Able to Access NaviNet** to view active users as well as those who *can* access NaviNet but they must perform an action first, such as create a new password. Select **Unable to Access NaviNet** to find users who cannot access NaviNet without intervention from a NaviNet security officer.

3. Determine the action to take, if necessary. From this screen, you can terminate a user who should no longer access NaviNet, or you can generate a new password to reactivate a user's account. If you notice a user whose password expires soon, or whose account will be soon be disabled due to inactivity, reach out to the user to remind them to take action.

Note *Security officers cannot reset their own passwords. If you're a security officer that needs your password reset, ask another security officer at your site or contact NantHealth Support.*

Review this list monthly to see who from your office is using NaviNet, who needs help getting access, and who should be terminated. To add or remove security officer privileges for an existing user, you must create a new user with the correct privileges and terminate the previous user account.

User account statuses

In **Administration > Manage Users**, view the status of every NaviNet user in your office.

User statuses

Each NaviNet user account has one of the following statuses.

Active	Users created their own password and signed into NaviNet.
Generate Initial Password	Users have a NaviNet username but cannot sign in. A NaviNet security officer has not yet generated a temporary password for them.
Password Generated/ No Initial Login	Users have a temporary password, but never signed in.
Change Password	Users signed into NaviNet at least once, but a security officer or NantHealth Support generated a new temporary password for them. The users must create their own password.
Disabled/No Initial Login	New users who never signed into NaviNet with their temporary passwords within 60 days. The system automatically terminates a user account when the status is Disabled/No Initial Login for more than 30 days.
Disabled	• Users signed into NaviNet but didn't change their temporary password within 60 days. • Users signed into NaviNet, and their permanent password expired 90 days ago. • Users tried to reset their password, but failed the challenge and response questions three times.

	The system automatically terminates a user account if the status is Disabled for more than 30 days.
Expired Password	Users signed in at least once, created a permanent password, and it has since expired. These users have 90 days to reset their own password.
Deactivated	Users who tried to sign in, but used an incorrect username and password combination three times. These deactivated users can still try to reset their password by clicking **Forgot Password** on the NaviNet sign-in screen.
Terminated	Users who the security officer or NantHealth Support terminated, or users whose status is Disabled or Disabled/ No Initial Login for more than 30 days. Terminated accounts cannot be reactivated.

Combined user statuses

The **Combined User Status** menu lets you search by a broader status category.

Able to Access NaviNet	All users with a status of Active, Deactivated, Expired Password, Password Generated/No Initial Login, or Change Password. These are active users as well as those who *can* access NaviNet but they must perform an action first, such as create a new password.
Unable to Access NaviNet	All users with a status of Disabled, Disabled/No Initial Log In, and Generate Initial Password. Terminated users are not included. These users cannot access NaviNet without NaviNet security officer intervention.
Disabled and Terminated	All users with a status of Disabled, Disabled/No Initial Login, or Terminated. These users cannot access NaviNet without NaviNet security officer intervention.
All Statuses (Except Terminated)	All users in the office except those with a Terminated status.
All Statuses (Including Terminated)	All users in the office.

Reactivate a user's account

Users can click **Forgot password** on the sign-in page to reset their own passwords unless their account is disabled or terminated. Security officers can reset and generate passwords for users whose accounts are disabled to reactivate their accounts. Terminated accounts cannot be reactivated.

Note *Security officers cannot reset their own passwords. If you're a security officer who needs your password reset, ask another security officer at your site or contact NantHealth Support.*

1. On the NaviNet toolbar, select **Administration > Manage Users**.
2. On the User Search screen, type search criteria to find the users, and then click **Search**.
3. In the list of matching users, do the following:
   a) Select each user or click **Check All** to select all users.
   b) Click **Generate Password** to generate new passwords for the selected users.

   In the user search results, the New User column indicates that a user is new and has not yet signed into NaviNet.

   The Notify Staff screen displays the users and their new temporary passwords. Note the passwords in this screen, and confidentially communicate them to each user.

Click **Continue** to return to the User Search screen.

Terminate user accounts

To ensure compliance, if a member of your staff no longer works in your office, you must terminate their access to NaviNet. The system automatically terminates a NaviNet user account when the status is Disabled or Disabled/No Initial Login for more than 30 days.

1. On the NaviNet toolbar, select **Administration > Manage Users**.
2. On the User Search screen, provide the search criteria to find users whose accounts you want to terminate.
3. Click **Search**.
4. Select the check box next to each user who must no longer access NaviNet, and then click **Terminate**.

The users that you select can no longer sign into NaviNet. Terminated accounts cannot be reactivated.

Change your office's timeout period

NaviNet security officers can change the amount of time before NaviNet automatically signs out users due to session inactivity.

The default and minimum timeout period is 30 minutes. You can choose a timeout period up to 120 minutes (two hours). The timeout period affects all users in your office.

To identify your NaviNet security officer, see Find your NaviNet security officer.

Note *This setting does not impact sessions that a user closes on their own. A user's NaviNet session always ends immediately when they close all browser windows or tabs that they are signed into.*

1. On the NaviNet toolbar, select **Administration > NaviNet Timeout Duration**.
2. On the NaviNet Timeout screen, choose a timeout option from the **New Timeout** drop-down menu.
3. Click **Submit**.

The change is immediate, but users must log out and sign in again to experience the changed timeout period. You can change the timeout settings at any time.

Passwords

Users must change their passwords periodically in accordance with HIPAA security standards.

Protect NaviNet passwords as you would passwords to the EMR system or other systems containing PHI.

Temporary passwords

- After you generate a temporary password for a user, they have 60 days to sign in and select a permanent password.
- If they don't reset their password within 60 days, their account is automatically disabled and they can't sign in. They must contact a NaviNet security officer to reset their password.

Permanent passwords

- After a user creates a permanent password, they can use that password for 120 days.
- Two weeks before the 120-day period ends, when the user signs into NaviNet, we notify them that their password will expire soon, and remind them to change it. After the 120 days, they cannot sign in with their old password. They have 90 days to reset it by clicking **Forgot Password** on the sign-in page.
- If they don't reset their password within 90 days, we disable their account, and they can't sign in. They must contact a NaviNet security officer to reset their password.

Password requirements

Your new password must meet the following requirements:

- Be at least eight characters long
- Be different from the last six passwords you've used
- Contain at least three of the following types of characters: uppercase letters, lowercase letters, numbers, and symbols (`! @ # $ % ^ & * ( ) _ + } { " : ; ? \ /`)
- Not contain your NaviNet username or your first or last name
- Not contain three or more repeated or sequential characters, such as `aaa`, `abc`, or `123`

Password guidelines

A good password is critical to protecting the confidential information available through your NaviNet account. Choose a password that is unique and difficult for others to guess.

- Use a combination of letters and numbers, but avoid simply placing numbers at the beginning or end of a word.

- Use a word you can remember, but replace some of the letters with numbers, for example, use s3cr3t for secret.
- Use the first letters of a memorable phrase, for example, mdSi12yo for "my daughter Sally is 12 years old."
- Use the longest password that you can remember. NaviNet passwords can be up to 30 characters. Consider using a passphrase, which is a string of unrelated words.
- *Do not* use personal information such as family names, anniversaries, birthdays, or social security numbers.

Licensee Designated Security Officer Agreement

ROLE OF LICENSEE DESIGNATED SECURITY OFFICER

Licensee is required to designate one Licensee Authorized User as a security officer (the "Licensee Designated Security Officer") and to ensure that the Licensee Designated Security Officer complies with his or her obligations under this Agreement. The Licensee Designated Security Officer serves as Licensee's primary contact with Company regarding security issues. Company's Security Officer oversees Company's information security program and serves as the primary contact for requests pertaining to Service security from Licensee Designated Security Officers.

Licensee represents and warrants that its Licensee Designated Security Officer is knowledgeable concerning the statutory and regulatory requirements applicable to Licensee and the electronic storage and transmission of patient information within and from Licensee, including HIPAA and any state medical privacy mandates. Licensee Designated Security Officer is responsible for remaining actively informed of developments concerning these legal requirements and will identify security services, products and solutions to ensure Licensee adheres to legal requirements related to information privacy and security.

Licensee Designated Security Officer responsibilities include the following:

- Ensuring that every Licensee Authorized User will have his or her own unique password.
- Ensuring that these unique passwords are not shared with anyone, even among Licensee Authorized Users.
- Regenerating a user password, if a Licensee Authorized User forgets his or her password and challenge and response answers and needs it to be regenerated.
- Regenerating a user password, if a Licensee Authorized User's username or password has been shared or otherwise compromised.
- Adding or terminating the access of any Licensee Authorized Users to the Services.
- Managing the access of any Licensee Authorized Users to the Services by granting or denying access to specific functions of the Services.
- Maintaining tax IDs and provider IDs within the Services, if authorized by Licensee to do so.
- Ensuring that information accessed via the Services is only used for legitimate business purposes.
- Setting the amount of time before the Services automatically log off inactive sessions.

If you have any questions regarding this Agreement, please call NaviNet Customer Support at 1-888-482-8057.

This text is part of the NaviNet Use Agreement.