BioSense Platform Quick Start Guide to Using the Access & Management Center
April 2019

NSSP
National Syndromic Surveillance Program
BioSense Platform
Quick Start Guide to Using the Access & Management Center

CONTENTS

1 Overview, 1

2 Access, 2
   Obtaining Log-in Credentials, 2
   Logging In to AMC, 2
   Accepting Code of Conduct, 2
   Changing Password and Activating Account, 3

3 Home Page, 4
   User Home Page, 4
   Site Administrator Home Page, 5

4 Navigation, 6
   Use Home Tab, 6
   Manage User Profile, 6
   Manage Users, 10
   Access and Share Data, 11
   Create a New Data Access Rule, 11
   Edit a Rule, 17
   Translate AMC Data Access Rules to ESSENCE, 18
   User Groups, 19
   Create a New User Group, 20
   Edit a User Group, 21
   Master Facility Table, 22
   View Reports, 22

5 Commonly Performed AMC Activities, 23

Technical Assistance: support.syndromicsurveillance.org

The National Syndromic Surveillance Program (NSSP) promotes and advances development of the cloud-based BioSense Platform, a secure integrated electronic health information system that hosts standardized analytic tools and facilitates collaborative processes. The BioSense Platform is a product of the Centers for Disease Control and Prevention (CDC).
Quick Start Guide to Using the Access & Management Center

1. Overview

The Access & Management Center (AMC) supports the BioSense Platform’s administrative functions for implementing tools and applications.

The AMC provides the following functionality:

- Obtains user acceptance to the BioSense Platform Code of Conduct.
- Allows users to change passwords.
- Allows site administrators to create user accounts.
- Allows site administrators to control who can access ESSENCE and view site data.
- Allows site administrators to control site-level access to the DataMart for everyone who uses the Adminer, RStudio Pro, and SAS Studio applications.

This quick start guide will help you access and navigate the AMC’s main features. The guide will be updated as functionality is added.

The username and password you use for the AMC are the same credentials you will use to log in to ESSENCE, Adminer, RStudio Pro, and SAS Studio (if applicable).

What happens when I create an account through the AMC?

- You will receive a username and password. This username will work for all applications on the BioSense Platform to which you have access, including AMC, ESSENCE, Adminer, RStudio Pro, and SAS Studio. Not all users have access to all applications on the BioSense Platform.
- You must log in to the AMC to accept the Code of Conduct and set a new password before logging in to ESSENCE or other applications.

What is a site?

NSSP organizes facilities (e.g., hospitals, emergency departments, urgent care centers) under a single administrative authority called a site. A site may oversee any number of facilities, all of which share the same site administrator and Master Facility Table (facility metadata).

What is a site administrator?

- A site administrator creates user accounts and controls access to data on the BioSense Platform.
- Your site will assign one or more people to serve as site administrator.

If you’re a site administrator who needs access to the AMC, please submit a ticket to the NSSP Service Desk at support.syndromicsurveillance.org.
2. Access

Obtaining Log-in Credentials

You will receive emails with your log-in information for the BioSense Platform AMC. To request AMC access, contact the site administrator(s) for your site. Sites are responsible for creating policies to manage user accounts and provide access to data in ESSENCE.

Logging In to AMC

2. Enter the username and temporary password sent to you via separate emails (figure 1).
3. Click Submit.

![Figure 1. AMC Log-in Screen](image)

If you forget your password or username, you can use the links on this log-in page to retrieve them. If you have trouble logging in to the AMC, contact the NSSP Service Desk at http://support.syndromicsurveillance.org.

Accepting Code of Conduct

The first time you log in to the system, you are required to review and accept the BioSense Platform Code of Conduct (figure 2). The Code of Conduct outlines proper practices and responsibilities (data-sharing etiquette) for the BioSense Platform user community.

Users must accept the Code of Conduct under the following conditions:

- First time logging in.
- Every 90 days when password expires.
- User resets password.
- Changes are made to user’s authorized access (e.g., if a user account becomes a site administrator account).

![Figure 2. BioSense Platform Code of Conduct](image)
Changing Password and Activating Account

You must change your password the first time you log in to the AMC (figure 3). You will not be able to access the AMC or other tools until you have changed your password and accepted the Code of Conduct.

Click “Save” to make sure your password is successfully changed.

Password requirements:

- Passwords must meet all of the following four criteria:
  - Contain both upper and lowercase letters
  - Contain numbers
  - Contain special characters
  - Contain exactly 12 characters
- Passwords must not contain a sequence of three or more characters from any part of the following:
  - First name
  - Last name
  - Email
  - The word “password”
- Passwords must be more than 75% different from your previous password on a character-by-character basis (e.g., ABCD is original password, AEFG or ADBC are valid changes, but AECD or ABCE are invalid changes)
- Passwords must not match your previous 24 passwords

You may change your password at any time.

What if I forget my password?

Navigate to the AMC log-in page, and click the “Forgot Password” link.

Provide the requested information to receive an email with your new password.

The same username and password combination is used for AMC, ESSENCE, Adminer, RStudio Pro, and SAS Studio. You cannot log in to any NSSP applications until you have accepted the Code of Conduct and set your password in the AMC.
3. Home Page

User Home Page

The AMC home page (figure 4) enables access to applications and links to useful resources:

![AMC User Home Page](image)

Figure 4. AMC User Home Page

My Info

Users and site administrators can follow links to change passwords, update profiles, and view the Code of Conduct for using the BioSense Platform’s AMC tool.

NSSP Applications

Users and site administrators can gain quick access to tools and applications for viewing data submitted to the BioSense Platform:

- **ESSENCE** — Capture, analyze, store, and share data.
- **Adminer** — View MS SQL data and do basic queries.
- **RStudio Pro** — Perform advanced data analysis.
- **SAS Studio** — Perform advanced data analysis.

Resources

- **NSSP Service Desk** — You will be asked to set up a password. Once you have a password, you may submit general or technical questions about NSSP. Your question will be routed to a specialist.
- **NSSP Resource Center** — This is a go-to place for NSSP publications, forms, standards and guidance, message mapping guides, fact sheets, onboarding guidance, and quick start guides for BioSense Platform applications.
- **Syndromic Surveillance Community of Practice Portal** — The portal links to forums, work groups, training, knowledge repository, and more. It is for anyone interested in syndromic surveillance who wants to collaborate, share ideas, and learn from or contribute to the community.
**Site Administrator Home Page**

Site administrators can perform additional functions in the AMC. The home page for site administrators (figure 5) includes the following tabs:

- **Home**—Change password, update profile, and navigate to other BioSense Platform tools.
- **Manage Users**—Add, modify, or remove user accounts for your site.
- **Data Access**—Add, modify, or remove data access permissions for ESSENCE accounts.
- **User Groups**—Add, modify, or remove group members.
- **Master Facility Table (MFT)**—Add, modify, or view facilities for your site.
- **Reports**—View users who can access your data.

![Figure 5. Site Administrator Home Page](image)

Both the user and site administrator have a section on the home page that allows them to see data they can access via ESSENCE (figure 6).

![Figure 6. Data Viewable in ESSENCE](image)
4. Navigation

The AMC home page is organized by tabs across the top. A list and description of each tab follows.

*Use Home Tab*

The Home tab allows users and site administrators to
- View My Info;
- Navigate to NSSP Applications;
- Navigate to Resources; and
- View data accessible via ESSENCE.

*My Info*

You may update your profile, change your password, and view the Code of Conduct for users. As a site administrator, the functionality is similar, but you will be able to see the Code of Conduct for both users and site administrators.

*NSSP Applications*

Users and site administrators can gain quick access to tools and applications (ESSENCE, Adminer, RStudio Pro, and SAS Studio).

*Resources*

This section links to resources available to all users: Service Desk for technical and general support; Resource Center for NSSP-specific onboarding materials, quick start guides, and guidance documents; Syndromic Surveillance Community of Practice Portal for connecting with thought leaders and experts in the field; and Data Dictionary and Data Flow Requirements.

*Manage User Profile*

The User Profile page (figure 7) displays a user’s contact information as well as account information and details. These sections are described below.
User Profile
This section of the user profile contains contact information and background.

- **User Name**—The user name required when logging into all BioSense Platform applications. The user name is automatically generated by AMC and cannot be changed once a user’s account has been created.
- **First Name**—The user’s first name. This field is editable by the user and site administrators.
- **Last Name**—The user’s last name. This field is editable by the user and site administrators.
- **Email Address**—The user’s email address. Password expiration emails will be sent to this email address. This field is editable by the user and site administrators. Federal users are required to use their government email address.
- **Office Phone**—The user’s contact phone number. This field is editable by the user and site administrators.
- **Organization**—The user’s organization affiliation. This field is editable by the user and site administrators.
- **Epidemiologist**—This check box is checked if the user is an epidemiologist. This field is editable by site administrators but NOT by individual users.
- **Site**—The site affiliation assigned to a user during account creation. If a user requires multiple site affiliations, multiple user accounts must be created. A user’s site affiliation cannot be changed once a user’s account has been created. Site administrators should contact the NSSP Service Desk if a change of site affiliation is required.
- **Privilege Level**—The level of access a user is granted for the BioSense Platform tools and applications. This field is only editable by NSSP staff. Site administrators may contact the NSSP Service Desk if a change of privilege level is required.
- **PIV Required**—This check box is checked if the user has a PIV card and requires a PIN code for logging in to both AMC and ESSENCE. Once checked, the U.S. Department of Health and Human Services (HHS) ID field and PIV Exception Status field become visible. These fields are only editable by NSSP staff.
- **HHS ID**—The user’s HHS ID found on the back of the PIV card. This number is required if the “PIV Required” check box is selected.
- **PIV Exception Status**—“Active” indicates that PIV user may log in with a user name, password, and PIN code. To activate field, the site administrator must select the “Grant PIV Exception” button.
- **Foreign National**—“Yes” indicates that the user is a foreign national, whereas “No” indicates that the user is not. This is required for security purposes but does not alter permission. This field is editable by site administrators but NOT by individual users. (A Foreign National is anyone who is not a U.S. citizen, U.S. national, or immigrant who has been granted the right to permanently reside and work in the United States.)
- **Contractor**—“Yes” indicates that the user is a contractor. “No” indicates that the user is not a contractor. This information is required for security purposes but does not alter permissions. The field is editable by site administrators but NOT by individual users.

Figure 7. User Profile Page
Account Information

This section of the user’s profile details information about the account and password status. To implement the BioSense Platform’s single sign-on functionality, the AMC synchronizes passwords across the Active Directory, AMC, and ESSENCE. If any of the three password statuses show “Password Locked,” a site administrator can select the “Unlock ALL Accounts” button to unlock accounts and change the password status to “Active.” If any password statuses show “Password Expired,” or if the user has forgotten the password, the site administrator can click “Reset User Password” to email the user a password reset link and temporary password.

- **Account Status**—When “active,” indicates the user’s account is enabled. When “inactive,” the user’s account is disabled. A site administrator can activate or inactivate a user’s account by selecting the corresponding radio button and saving. When a user’s account status is “inactive,” he or she will be unable to log in to any of the applications on the BioSense Platform.

- **AMC Password Status**—The status of the user’s AMC account password.

- **Active Directory Password Status**—The status of the user’s Active Directory account password.

- **ESSENCE Password Status**—The status of the user’s ESSENCE account password.

- **AMC Password Expiration Date**—The expiration date of the user’s current password.

**ESSENCE National View Controls**—Site administrators are able to control which accounts can view the National View and Chief Complaint Query Validation data sources within ESSENCE. By default, accounts do not have access to these data sources.

- **National View Aggregate Only**—Select this option to view the ESSENCE data sources “Patient Location (Limited Details by HHS Region)” and “Facility Location (Limited Details by HHS Region)” at an aggregate level (i.e., the user may view charts, graphs, and maps with no access to line-level data).

- **National View Aggregate and Details**—Select this option to view the full details for the ESSENCE data sources “Patient Location (Limited Details by HHS Region)” and “Facility Location (Limited Details by HHS Region)” (i.e., the user may view charts, graphs, and maps as well as the line-level data).

- **Chief Complaint Query Validation Tool**—Select this option to view the ESSENCE data source “Chief Complaint Query Validation.”

The National View data sources contain limited fields aggregated to the HHS Region level. The intent is to provide a high-level national picture of syndromic surveillance data. Every site that sends data to the BioSense Platform is contributing to National View data sources.

The Chief Complaint Query Validation data source contains Chief Complaint and Discharge Diagnosis text to allow users to refine queries. No identifying information—such as age, region, facility, or sex—is available in this data source. Sites may choose NOT to include their data in the Chief Complaint Query Validation data source.
**Database Access**—Site administrators may control which user accounts can access their site’s data within the DataMart. **By default, user accounts do not have access to this data source.**

- **DataMart (Site-level Access)**—Select this option to allow users to access and run queries against their site’s MS SQL tables. If this option is selected, access to Adminer is automatically assigned, enabling a user access to the full set of site data. This option does not grant access to any custom SQL views for counties, facilities, or other data subsets developed by request. To grant user access to custom SQL views, site administrators need to submit a Service Desk request.

**Application Access**—Site administrators may control which accounts have access to the Adminer, RStudio Pro, and SAS Studio applications. **By default, new user accounts do not have access to these tools.**

- **Adminer**—Adminer access is automatically assigned when DataMart access is selected. To revoke a user’s access to Adminer, deselect access to the DataMart. If the Adminer check box is selected, the user will be granted access to all data available within his or her site.
- **RStudio Pro**—Select this option to allow users to visualize site-level SQL data via RStudio. You must also grant access to the DataMart.
- **SAS Studio**—Select this option to allow viewers to visualize site-level SQL data via SAS Studio. You must also grant access to the DataMart.

**Site-specific Communications**—Site administrators may control which user accounts receive site-specific communications. There are two categories of site-specific communications:

1. **Data Quality and Processing Communications**—Select this option to allow a user to receive site-specific communications related to data quality and data processing, including
   - Daily BioSense Platform Site Processing Summary
   - Quarterly Executive Data Quality Summary
   - Monthly Data Quality Report emails (completeness, timeliness, validity)
   - Miscellaneous data quality issue information

2. **Onboarding Communications**—Select this option to allow a user to receive site-specific communications related to onboarding, including information about
   - Data validation and facility management emails (i.e., day-to-day onboarding operations)
   - Connectivity and technical assistance emails (e.g., feed setup)
   - Strategic onboarding initiatives emails (e.g., baseline cleanups)

*Note.* NSSP sends system updates and announcements to all account users.

**Account Details**
The Account Details section of the user profile provides information about creation and subsequent modification of the user account.

- **Created By**—The site administrator who created the displayed user account.
- **Created Date**—The date the user account was created.
- **Last Modified By**—The last user to have modified the displayed user account. This could be a site administrator or the user.
- **Last Modified Date**—The date the user account was last modified.
Manage Users

The Manage Users tab (figure 8) is available only to site administrators. This tab allows site administrators to create new accounts or to view and modify user accounts within their site. The site administrator can also use this page to download a CSV or Excel list of users within their site. Site administrators are responsible for creating and managing the user accounts for their site.

Create Users

To create a new user account, click “Add New User.” Provide the requested information and click “Save.” Once you successfully save a new user, an email containing log-in credentials will be sent to the user.

Things to remember when creating a new user:

- First Name, Last Name, and Email Address are required.
- You can only add users to your site.
- Users within your site must have unique email addresses.

Modify User Accounts

To review or modify a user account, select a row in the user table and click “View/Edit.” You will be able to see and update the user profile.

If you need to remove a user account, select the account, click “View/Edit,” and change the Account Status radio button selection to “Inactive.” If you deactivate a user in the AMC, that user will no longer be able to use the AMC or other BioSense Platform tools.
**Access and Share Data**

The Data Access tab (figure 9) is only available to site administrators. This tab allows site administrators to create, review, and edit system rules that control access to their site data. These system rules, called Data Access Rules, are applied to user accounts in the ESSENCE application.

![Figure 9. Data Access Page](image)

**Create a New Data Access Rule**

**Step 1: Describe Rule**

First, name your rule (figure 10) and enter a description. This will help you find your rule later.

![Figure 10. Data Access Page (Rule Characteristics)](image)
Step 2: Select Users

Who should be included in the Data Access Rule? Keep in mind that any user selected here (figure 11) will receive access to the data you specify in the next step.

- Individual users
- User groups (two types)
  1. NSSP user groups
  2. Site-defined user groups (public or private)

*Note: Site-defined user groups must be created before adding to a data access rule.*

---

Figure 11. Data Access Page (Select Users)

**Select All Users**—To select all site users and epidemiologists (figure 12), expand the top section of the Select Users page and click “Select a User Group.” Always select at least one user to include in your Data Access Rule. You may change the user(s) at any time.

---

Figure 12. Data Access Page (Select a User Group)
What should I keep in mind when sharing data with the NSSP Team?

Occasionally you might want to share your site’s data with one or more members of the NSSP Team to provide analytic support.

- To share data with the entire NSSP Team, select the “All NSSP Site Users” group through the User Group option as part of a data sharing rule.
- To share with one or more individuals, select the “Individual User” option. We suggest you filter by site = “NSSP,” and then select the user name(s) with whom you want to share data.

Why would I select users not in my site?

You might want to share your site’s data with users in other sites, particularly adjoining sites that could experience fallout from the same hazardous event or get ill from the same contaminated food. If you select a user account from another site, the data you share with that user will add to any other data that user’s account can access. To ensure queries run as anticipated, users must understand what data they have access to within ESSENCE.
Step 3: Select Data

Next, select the data you want included in the Data Access Rule (figure 13). If you’re a site administrator, be mindful that you can only control access to your site’s data. As a site administrator, you may grant user access to multiple data sources and restrict user(s) from accessing your site data by

- Facility
- State and county

You must select one or more ESSENCE data sources to include. These data sets map directly to the data source names within the ESSENCE application.

Available Data Sources:

- **Patient Location (Full Details) Visit**—Provides access to data based on where the patient lives. A user granted access to this data source may view a complete list of patient details for all patients residing in the corresponding site. Any restrictions made after selecting the data set (e.g., by facility, state, or county) will be applied based on the location of the patient.

- **Facility Location (Full Details) Visit**—Provides access to data based on the hospital location where a patient sought treatment. A user granted access to this data source may view a complete list of patient details for all facilities located in the corresponding site. Any restrictions made after selecting the data set will be applied based on the location of the facility.

- **Facility/Syndrome Alert**—Provides access to public health event alerts by facility or syndrome for the corresponding site. A site administrator may control the alerts based on the location of the facility.
- **Time of Arrival Alert**—Provides access to public health event alerts by time of arrival for the corresponding site. A site administrator may control the alerts based on the location of the facility.

- **Data Quality**—Provides access to multiple data quality metrics, including completeness of data (by variable, by location, etc.), whether data are mapped to known values, and status of data processing by facility.

Use caution when applying the optional restrictions by facility, state, or county. Such restrictions might limit data visibility, especially for the Patient Location data source.

As part of your Data Access Rule, you **must select data**. Users assigned to the rule can view the selected data when they use the ESSENCE application.

---

**How do the data sets on the Select Data screen correspond to access in ESSENCE?**

Data sources in the drop-down menu mirror those available in the ESSENCE Query Portal data source drop-down list. For example, selecting aggregate or data details for the “Patient Location (Full Details) and Visit” data source will allow an ESSENCE user to run a query against the “Patient Location (Full Details)” and “Patient Location & Visit (Full Details)” data sources in ESSENCE.

If you apply any of the optional filters, the available data source will be a subset of your site’s data based on those parameters. For example, by selecting state = “GA” for the By Patient Location data source, you will restrict those data available for queries against the “Patient Location (Full Details)” to data from your site where the patient lives in GA.

**What is the difference between “Aggregate Only” and “Data Details”?**

In ESSENCE, the aggregate-only selection will allow users to view high-level data via charts, graphs, and maps. However, the user will not have access to line-level data. For example, when running a query against a data source with aggregate-only permissions, a user can view the time series graph. However, that user cannot click on that graph to view data details or patient information.

**Note to site administrators**—If you grant a user access to the data details, you must also grant the user access to the aggregate data set.
Step 4: Review and Save the Rule

Do’s and Don’ts of Data Sharing Rules in the AMC

1. You can share data with other users in your site and restrict by a patient’s location using the “By Patient Location” data sources.
2. When sharing data with users outside your site, we recommend you do not share by patient location because ESSENCE will consolidate that rule with other patient location access controls, and you might share more than intended (for details, see section titled “Translate AMC Data Access Rules to ESSENCE”).

Once you name your rule and select users and data, you’re ready to save and implement your Data Access Rule (figure 14).

First, confirm that your selections are as expected. Use the edit buttons to modify the information displayed. Next, select the appropriate status for your rule (note that the default status value is “draft”):

- Active = rule will be saved and applied.
- Draft = rule will be saved but not applied.
- Suspend = rule will be saved but not applied.

When you’re done, click “Submit.” You’ll be returned to the Data Access tab.

Figure 14. Data Access Page (Review & Save)
**Edit a Rule**

**Step 1: Select a Rule**

On the Data Access tab under View/Edit, click the View/Edit button beside the rule you want to edit (figure 15).

![Figure 15. Data Access Page (Editing Rules)](image)

**Step 2: Modify Rule Characteristics and Save**

After you click View/Edit, you'll be directed to the Review & Save page (figure 16). Use the “Edit” buttons to change rule information, users, or data. You can also use the status drop-down menu to change a rule’s status. When you're done modifying your Data Access Rule, click “Submit.”

**How do I deactivate a rule?**

Follow these steps to remove or deactivate a rule:

1. Select the rule from the Data Access tab, and click “Edit.”
2. In the Status drop-down menu, change the value to “Suspend.”
3. Click “Submit.”

Permissions for the rule will be removed from user accounts in ESSENCE. However, the AMC will preserve the Data Access Rule with a status of “Suspend.” You may reactivate this rule again later.

![Figure 16. Editing Rules (Review & Save)](image)
Translate AMC Data Access Rules to ESSENCE

The AMC uses rules to control access to ESSENCE data sources. Most ESSENCE data sources have two access controls: patient location and facility location.

Suppose you want to share the “Patient Location (Full Details)” data source for your site. You can use the AMC to create a Data Access Rule to share all of your site’s data for the “Patient Location (Full Details)” data source.

The AMC will translate these selections into ESSENCE as demonstrated in the table below.

<table>
<thead>
<tr>
<th>I want to…</th>
<th>Site</th>
<th>State</th>
<th>County</th>
<th>Data source (ESSENCE Variable Name)</th>
<th>Facility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share all of the data from my site</td>
<td>;SiteID;</td>
<td>*</td>
<td>*</td>
<td>;va_er_hosp;</td>
<td>*</td>
</tr>
<tr>
<td>For patients that live anywhere (but were seen in my site)</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>;va_er;</td>
<td>*</td>
</tr>
</tbody>
</table>

ESSENCE manages data access for each user account by consolidating all data selected in rules that include that user and assigns the highest level of access for any given data source.

Suppose you want to share data from your site, Site X (where the patient lives in Alaska), with another user, John Doe. John already has access to all data by patient location for a different site, Site Y.

His current data access would be as follows:

<table>
<thead>
<tr>
<th>John Doe can access…</th>
<th>Site</th>
<th>State</th>
<th>County</th>
<th>Data source (ESSENCE Variable Name)</th>
<th>Facility</th>
</tr>
</thead>
<tbody>
<tr>
<td>All data from site Y</td>
<td>;SiteY ID;</td>
<td>All</td>
<td>All</td>
<td>;va_er_hosp;</td>
<td>All</td>
</tr>
<tr>
<td>For patients that live anywhere (but were seen in site Y)</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>;va_er;</td>
<td>All</td>
</tr>
</tbody>
</table>

Your rule in the AMC to share your site’s data by patient location of Alaska would be as demonstrated below:

<table>
<thead>
<tr>
<th>Your rule grants access to…</th>
<th>Site</th>
<th>State</th>
<th>County</th>
<th>Data source (ESSENCE Variable Name)</th>
<th>Facility</th>
</tr>
</thead>
<tbody>
<tr>
<td>All data from site X</td>
<td>;SiteX ID;</td>
<td>All</td>
<td>All</td>
<td>;va_er_hosp;</td>
<td>All</td>
</tr>
<tr>
<td>For patients that live in Alaska (but were seen in site X)</td>
<td>All</td>
<td>Alaska</td>
<td>All</td>
<td>;va_er;</td>
<td>All</td>
</tr>
</tbody>
</table>
If you include John in your rule, he will be able to access *all of your site’s data* because *ESSENCE combines data access and defaults to the highest permission available* for the “Patient Location (Full Details)” data source.

John’s combined data access would be:

<table>
<thead>
<tr>
<th>John’s access after the rule...</th>
<th>Site</th>
<th>State</th>
<th>County</th>
<th>Data source (ESSENCE Variable Name)</th>
<th>Facility</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>All data from these sites</em></td>
<td>;SiteX ID; SiteY ID;</td>
<td>All</td>
<td>All</td>
<td>;va_er_hosp;</td>
<td>All</td>
</tr>
<tr>
<td><em>For patients that live in Alaska</em></td>
<td>All</td>
<td>All</td>
<td>Alaska</td>
<td>;va_er;</td>
<td>All</td>
</tr>
</tbody>
</table>

**User Groups**

The User Groups tab is only available to site administrators (figure 17). User groups are a convenient way to add multiple users to data access rules instead of adding individual users one-by-one. Site administrators may create any number of public or private user groups. Public user groups are viewable and usable by other site’s administrators to add to their data access rules. Private user groups are only viewable and usable by that site’s administrators. Once a user group is created, that user group will be assignable to data access rules.

![Figure 17. User Groups Page](image-url)
Create a New User Group

Step 1: Select User Group Characteristics
Click the “Add New User Group” button on the main User Groups page. Enter the user group’s characteristics (figure 18). Create a unique name for the user group, add a description, and select a group (public or private). Provide enough detail so that you can quickly distinguish user groups from each other. Note that the site will be associated with the logged-in user’s site and cannot be changed.

Group Types: There are currently two types of groups:

- **Public**—All users (site administrators) who are authorized to manage user groups can see the group. This will be listed in the All Public Groups table on the main User Groups page.
- **Private**—Only users (site administrators) who are associated with the site that owns and controls the group will see the user group.

![Figure 18. User Group Description and Information](image-url)
Step 2: Select Users
Click the “Add/Edit User” button to add users to the group (figure 19). At least one user is required to submit the group. Remember that any users selected here will receive access to the data you specify when you create your data access rules. Use the filters to locate users to add to the group. Adding users is simplified with one click of the “Add” button next to the user’s name. When you’ve completed adding users, click the “Submit” button to save the group. Now, your group is active.

![Figure 19. User Groups Page (View & Select Users)](image)

**Edit a User Group**
Site administrators may edit the site-specific user groups they create. Examples include changing the group name, changing the group to public or private, and adding or removing group members. The site administrator may also delete a group that is no longer needed.

Once a user group is associated with a data access rule, the site administrator may delete or add users without affecting other members of the group. The remaining members of the user group will always maintain their association with the user group’s previously assigned data rules.

Members of the user group cannot view ESSENCE syndromic surveillance data UNLESS they have an associated data access rule.
**Master Facility Table**

The Master Facility Table (MFT) resides within the AMC, and this module provides a streamlined user experience for site administrators and the NSSP onboarding team throughout the multistage onboarding process. The *BioSense Platform Quick Start Guide to Using the Master Facility Table* can be accessed by clicking the button in the upper right-hand corner of the MFT tab (figure 20).

![Figure 20. Master Facility Table (MFT) Page](image)

**View Reports**

The Reports tab (figure 21) is only available to site administrators. They may use this tab to view a report listing the users who have access to their site’s data within ESSENCE.

![Figure 21. Data Reports Page](image)
5. Commonly Performed AMC Activities

These are common examples of activities that can be performed to check and view your data. This is not an exhaustive list of activities.

*Site Administrators can:*

1. Log in with provided credentials.
   a. Accept the Site Administrator Code of Conduct.
   b. Change user password.
2. View and edit user profile information.
3. Create a user in their site.
4. Create a user group for their site.
5. View existing users within their site.
6. Edit users within their site.
7. Create Data Access Rules for user(s) in their site. (Confirm with user that Data Access Rule results in the desired permissions in ESSENCE.)
8. Create Data Access Rules for user(s) not in their site (optional). (Confirm with user that Data Access Rule results in the desired permissions in ESSENCE.)

*Users can:*

1. Log in with provided credentials.
2. Accept the Code of Conduct.
3. Change their passwords.
4. View and edit their profile information.