Quick Start Guide to Using the Access & Management Center

Release 1.5.4 Enhancements

June 2021

NSSP
National Syndromic Surveillance Program
BioSense Platform

Centers for Disease Control and Prevention
Center for Surveillance, Epidemiology, and Laboratory Services

Division of Health Informatics and Surveillance

CS324706-A

CONTENTS

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 CDC.

Quick Start Guide to Using the Access & Management Center Release 1.5.4 Enhancements

1. Overview

This Quick Start Guide describes enhancements introduced in the Access and Management Center (AMC) release 1.5.4.3 on March 18, 2021. Please refer to the *BioSense Platform User Manual for the Access & Management Center* for additional information about the AMC and features provided by this application.

2. AMC 1.5.4 Functionality

Here is the functionality added in this release. Each feature will be described in detail below.

3. Data Access Timeframe Restriction

This enhancement lets a site administrator restrict access to data collected or recorded within a specified timeframe. Because this restricts which data a user can see, it differs from the limitation described in section 4 (below), which restricts when the user can access data. The Data Access Time Limitation (Section 4) can be combined with the Data Access Timeframe Restrictions described here to further constrain access.

These restrictions are applied to data sources, so, for example, a Timeframe Restriction applied to the Patient Location and View data source does not affect access to the Facility Location and View data.

There are three scenarios that describe how this enhancement can be used.

Scenarios:

1. Administrator specifies a start (**From**) date but no end (**To**) date.
2. Administrator does not specify a start (**From**) date but specifies an end (**To**) date.
3. Administrator specifies both a start (**From**) date and an end (**To**) date.

In scenario 1, the administrator intends to grant access to all data collected or recorded beginning with the From date and into the future until the rule is deleted or suspended.

In scenario 2, the administrator plans to grant access to all data collected or recorded in the past and up to the To date, which could be in the future.

Finally, **in scenario 3,** the administrator wants to grant access to all data collected or recorded between the From and To dates. Any data collected or recorded from the From (start) date up to and including the To (end) date will be made available to the user(s).

Here is an example of how to apply scenario 1:

The user to whom data access is granted will have access only to the data collected starting from the specified date. The user will have no access to any data collected before that date but will be able to access all data collected or recorded after that date for that data source. Figure 1 shows the setup.

- The administrator creates a new rule and specifies which users and user groups are to be granted access.
- The administrator selects a data source, e.g., Patient Location and Visit (Full Details).
- After choosing Data details or No data details, the administrator selects "Timeframe–From Date" for the first clause and places a date in the From field.

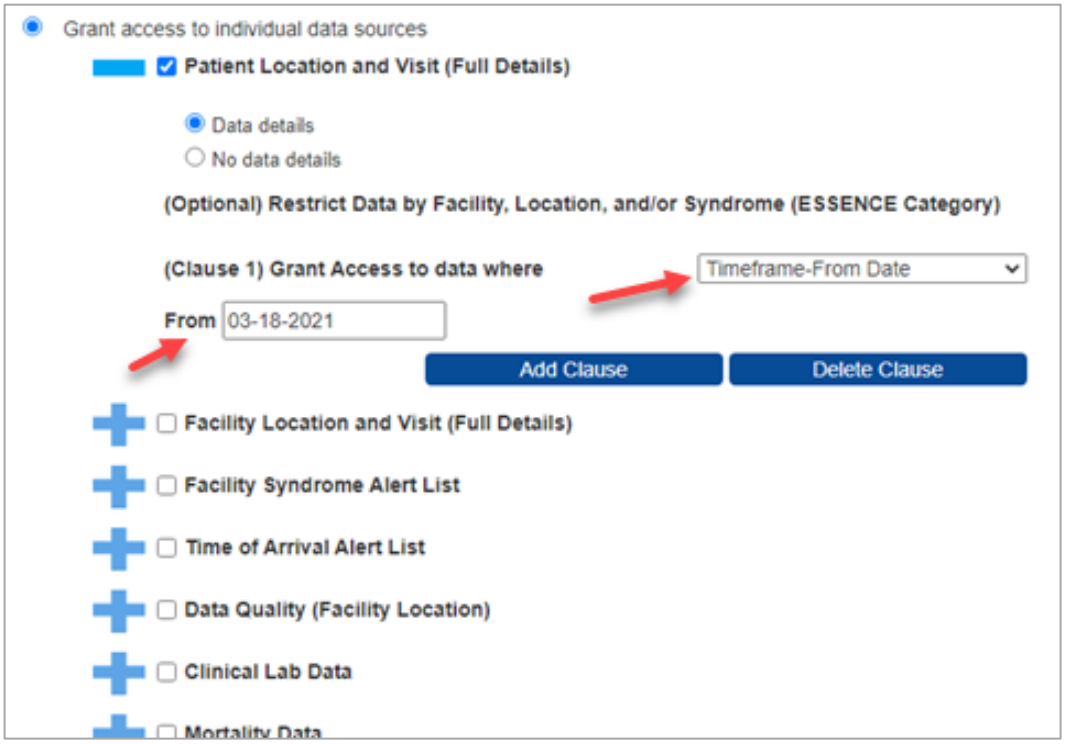

Figure 1. Create a Timeframe Restriction Clause.

- Clauses are now available for Timeframe–From Date and the Timeframe–To Date criteria. Other familiar constraints, such as counties or facilities, can also be placed on the data access.

4. Data Access Time Limitation

The Data Access Time Limitation functionality lets the site administrator specify a period during which a data access rule will be active. Because the rule specifies when and for how long users may access data, it will often be used in combination with a rule controlling which data they can access.

For example, on May 1, 2021, a site administrator could decide that data access should be active for 6 months starting on June 1, 2021, and ending on November 30, 2021. In this example the rule would stay in the Suspended status until June 1, at which time it would automatically become Active. Then, on December 1, 2021, it would reset to the Suspend status.

Figure 2 is a screenshot of what this example might look like as we set it up. (Note that we opened the pick list for the Predetermined Range feature as additional information only.)

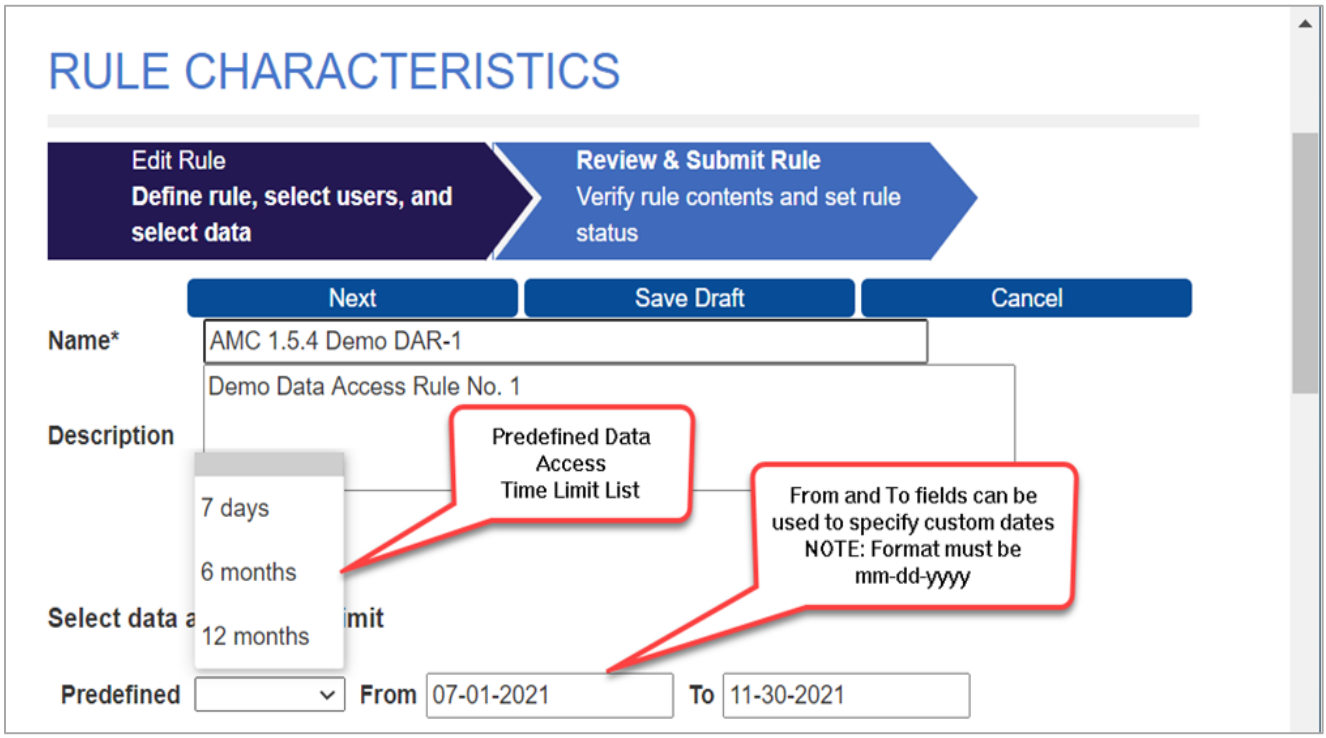

Figure 2. Data Access Rule setup shows both predefined and custom data range alternatives.

After we click on the **Next** button shown in Figure 2, the rule is placed in Suspend status because (in our example) June 1, 2021, is in the future (Figure 3).

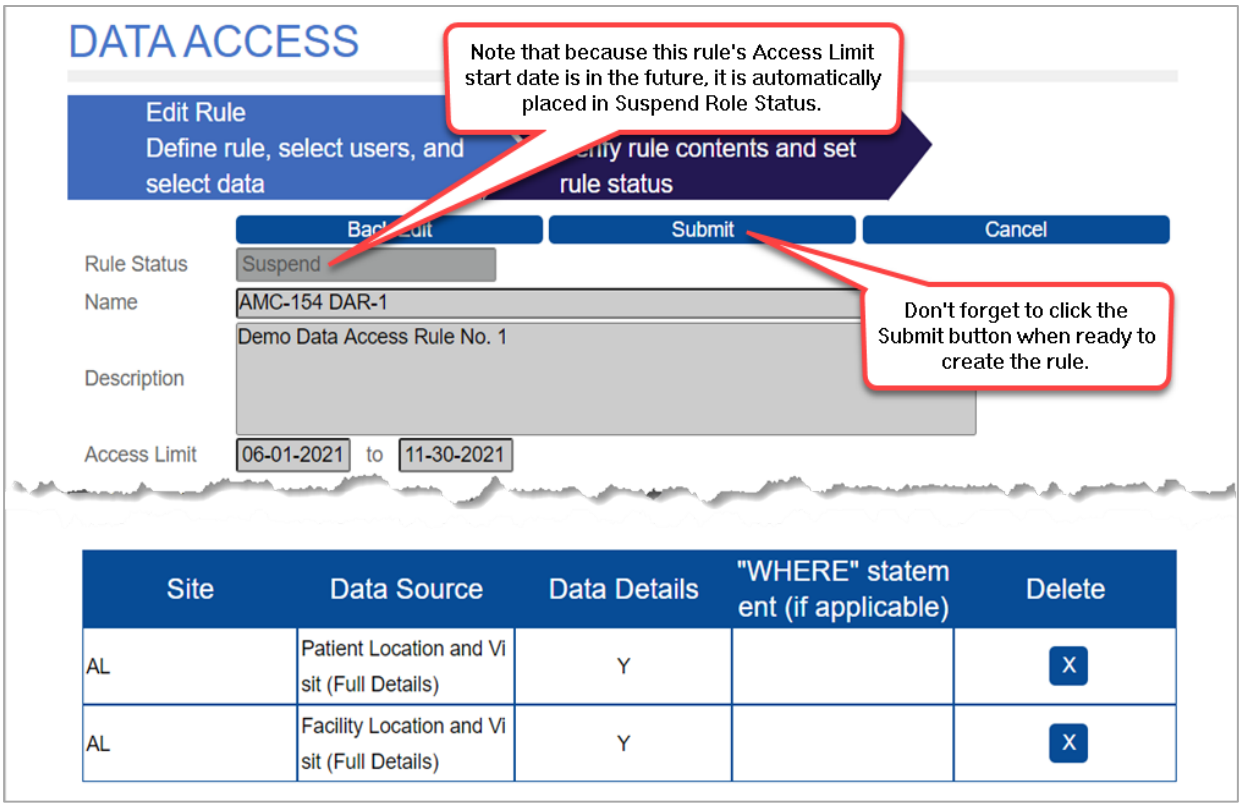

Figure 3. When Access Limit start date is in the future, the rule is automatically placed in Suspend status.

5. Date/Time Stamp for Data Access Rules

This functionality captures the date and time when a data access rule was created or last edited and displays it in the Data Access Rules table. The site administrator can elect to display Data Access Rules in ascending or descending order based on date and time (Figure 4). This feature allows Data Access Rules to be located more easily.

Clicking on the Date/Time column header toggles between ascending and descending order of display.

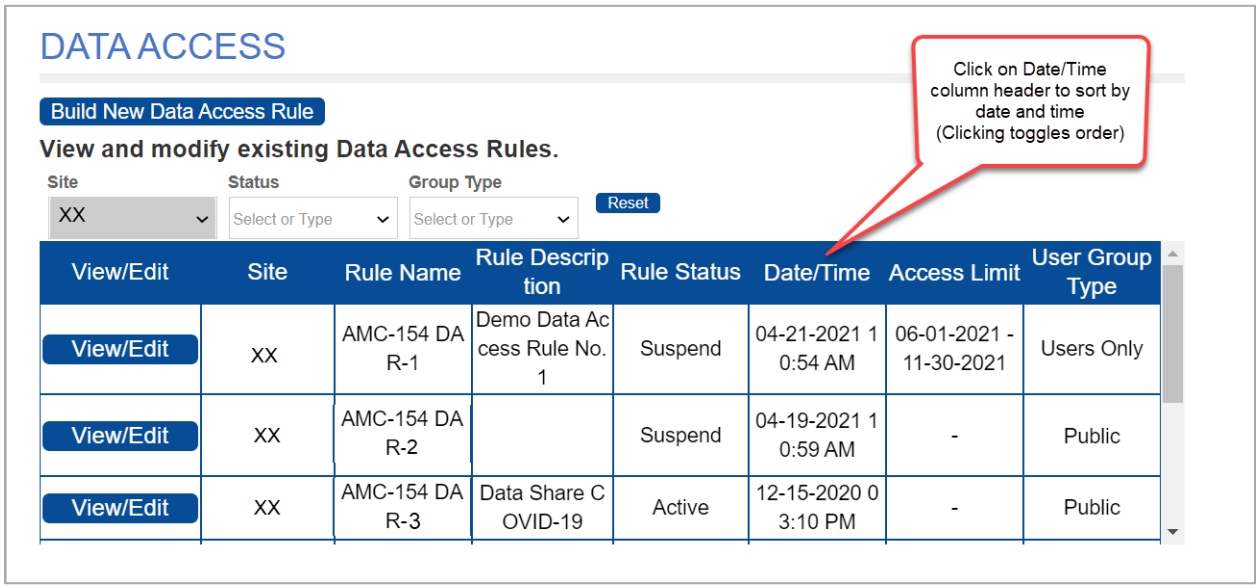

Figure 4. Date/Time column can be sorted by clicking on the header.

6. Manage Users—Organization Filter

On the Manage Users tab, you can now filter by Organization. Simply click in the Organization field in the Filters at the top of the table (Figure 5) and start typing the name or any part of the name of the organization you are searching for. The filter is dynamic in that it uses what you are typing to continually regenerate the results and refresh the Manage Users table.

Site administrators can search for a user in the Manage Users table by searching on the user's assigned organization. Note, in this example, there were no other organizations with "AM" in their name, so when the "A" and "M" of AMC were typed, the dynamic search located the user (Figure 5).

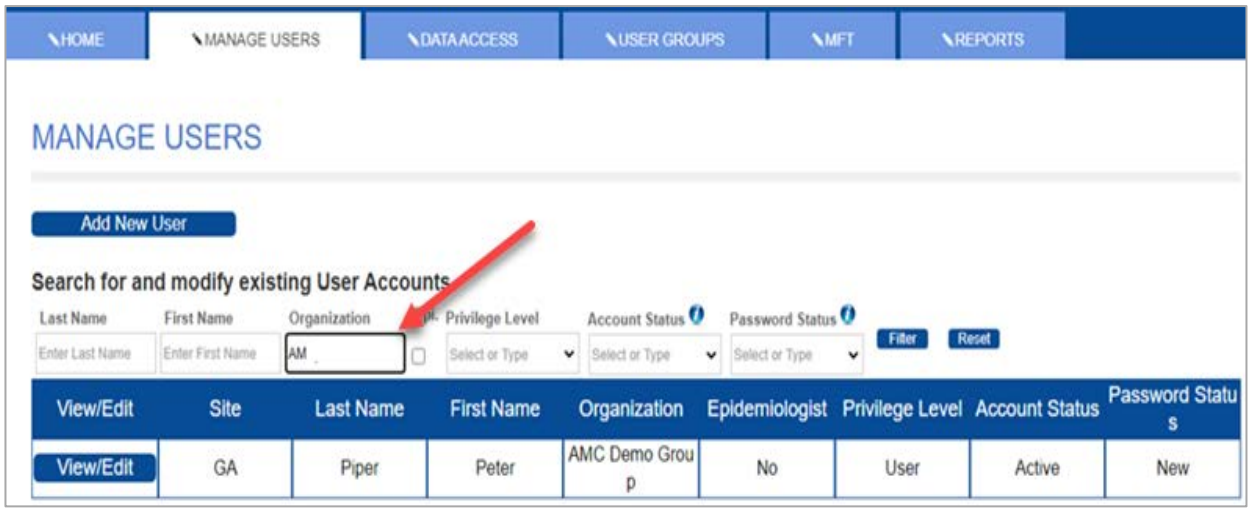

Figure 5. Dynamic search locates records as you type the search string.

7. Password Requirement Messaging

Enhanced password requirement messaging provides feedback on whether password criteria are being met when creating a new password or changing an old password. This dynamic verification "checks off" each criterion as it is met, e.g., if you type a lower-case letter as part of your new password, the red **X** beside the "Lower-case letter" requirement will change to a green checkmark (Figure 6).

All red **X**s must be changed to green checkmarks for the new password to be accepted.

Figure 6. This is an example of the Dynamic Password Validation.