SONICU™

MONITORING. MEASURED.

SoniCloud Users, Groups, Permissions, and SSO

SoniCloud implements a fine-grained, flexible permission structure to ensure that users can only see what they need to see and access what they need to access.

This ensures your SoniCloud system stays in a regulatory compliant setup with no upkeep.

It’s important to understand how this system is implemented as you consider the SoniCloud system.

SoniCloud Users

SoniCloud users have the ability to view one (or more) sites, depending upon the size of their organization and what their permissions include

SoniCloud users login via their *email address* and are able to have site-specific:

- **Alarm Notification Methods**: These determine how a user can be notified about an alarm.
    - SoniCloud supports email, SoniCloud Mobile push notifications, SMS, and phone calls.
    - Alarm notification methods are set up by Manager and Admin permission level users for other users without those permissions, ensuring tiered alarming across an organization
    - The only exception is SoniCloud Mobile push notifications:limitations of iOS and Android means each individual user must opt into push notifications when logging into the SoniCloud mobile app.

- **Alarm Escalation Settings**: Escalation settings allow alarm escalation to occur in a flexible manner, ensuring that the right people get alarm notifications at the right time.
    - For example, maybe facilities teammates should receive immediate alarms, while department management is notified if alarms haven’t been acted upon within 12 hours
    - This is how alarm escalation adds an extra layer of asset protection

- **Alarm Repeating Settings**: Ensure an alarm is never missed by enabling repeating alarm notifications
    - ll All alarms that haven't been resolved or snoozed can continue to send alarm notifications to users.
- **Alarm Notification Schedule**: Set up flexible notification schedules and only get notified outside of work hours
- **Groups**: Discussed below
- **Permission Level:** Discussed below

Password Restrictions

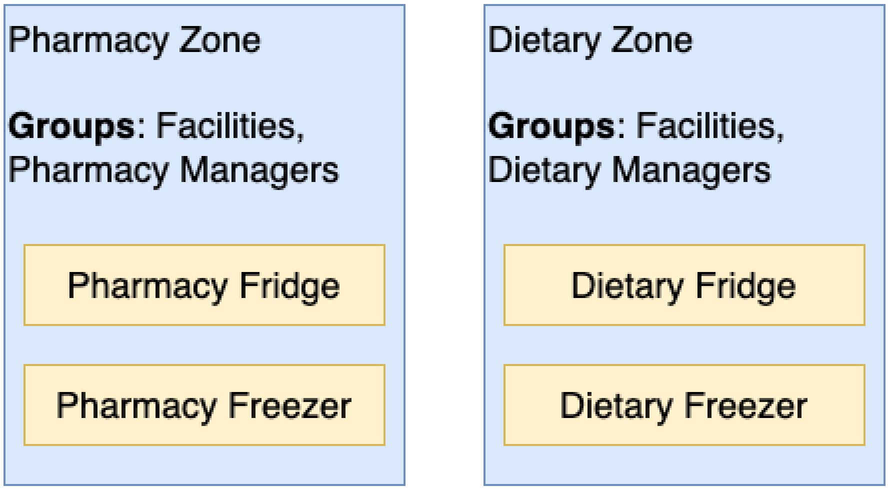
SoniCloud provides the option for customers to use the following password restrictions:

- **Password Requirement Options**
    - **Minimum Password Length**
    - **Password Reuse**
    - **Require 1 or More Upper-Case Letters**
    - **Require 1 or More Lower-Case Letters**
    - **Require 1 or More Numbers**
    - **Require 1 or More Symbols**
    - **Password Expiration**
- **Account Lockout Options**
    - **Account Locking**
    - **Lockout Window**
    - **Lockout Duration**
- **Login Statement**

SoniCloud Groups

Each SoniCloud user can belong to one or more *groups*.

These groups are assigned to a Zone, which gives users the ability to view points in that zone.



In the example above, there are two zones:

- Pharmacy Zone, consisting of
    - Pharmacy Fridge Pharmacy Freezer
    -
- Dietary Zone: consisting of
    - Dietary Fridge
    - Dietary Freezer
-
- There are also three groups:
    - *Facilities*,
    - *Pharmacy Managers*
    - *Dietary Managers*

A user that belongs to the *Pharmacy Managers* group would only be able to see the points in the *Pharmacy Zone*.

A user that belongs to the *Dietary Managers* group would only be able to see the points in the *Dietary Zone*.

A User that belongs to the *Facilities* group, however, would be able to see both the *Pharmacy Zone* and the *Dietary Zone*.

This ensures each user only sees information relevant to them.

SoniCloud Permission Levels

SoniCloud permission levels allow for fine-grained capabilities on a per-site basis.

If a user has access to multiple sites, they can have different permissions levels for each site – for instance, a user may need to have *Admin* permissions at a central location, but only *View* permissions at satellite locations.

Sonicu recommends limiting *Manager* and *Admin* permission levels to only critical teammates to ensure that changes aren't made that unintentionally affect others in the system.

- **Basic****: User who has the capacity to view points, run reports, and view (but not take action on!) alarms.
- **View**: User who can view points, run reports, and take action on alarms.
- **Manager****: View User permissions, plus the ability to edit View Users and control alarm notifications.
- **Admin**: User who can manage alarms, reports, points, users, and general configuration of the site.

- **** These permissions levels are not enabled by default – contact Sonicu Support to determine if these permissions levels would be a benefit to your organization**

SoniCloud Single Sign-On (SSO) Support

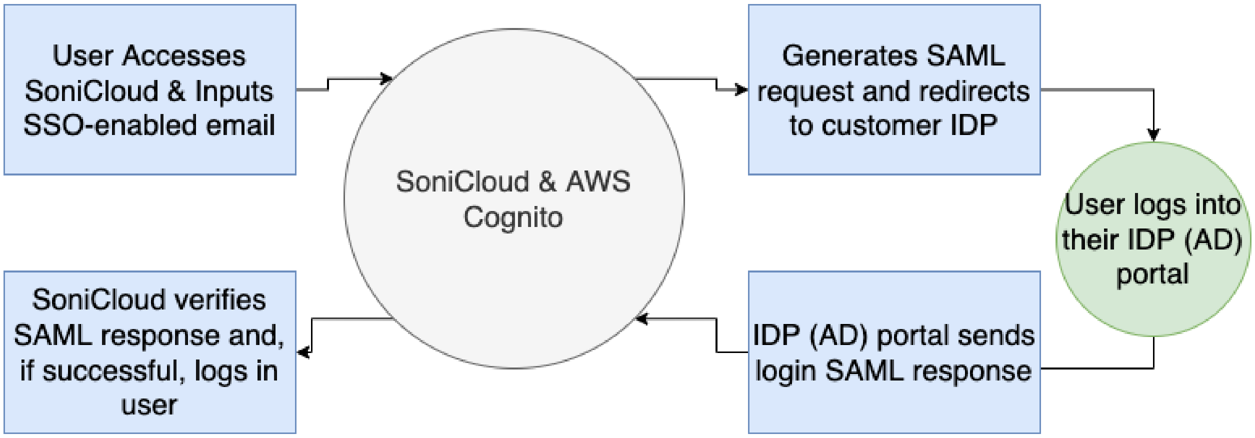
SoniCloud offers Single Sign-On (SSO) support via the Security Markup Language (SAML), the industry standard for logging in users to multiple applications via a single authentication method.

SoniCloud leverages AWS Cognito as the SAML federation provider.

This allows a customer to pair with SoniCloud and leverage SAML and their internal Active Directory (AD) implementation to provide SSO for SoniCloud.

Sonicu recommends SSO be enabled for all customers, as this allows customer IT to enforce desired security settings, including

- Multi-factor authentication
- password complexity requirements
- password rotation requirements


User Accesses SoniCloud & Inputs SSO-enabled email
SoniCloud & AWS Cognito
Generates SAML request and redirects to customer IDP
User logs into their IDP (AD) portal
IDP (AD) portal sends login SAML response
SoniCloud verifies SAML response and, if successful, logs in user

Technical Setup Requirements

Enabling SSO starts with an exchange of technical contact information between Sonicu and the customer.

The customer will be asked to provide the following information:

- SAML2.0 Metadata file
- Enable email address of the user to be sent via the `email` attribute
- A list of domains that users will be registering with (ex. Any subsidiary domains)
- Is IdP Signout flow (SLO) desired?

Sonicu will provide the following information:

- ACS URL
- Entity ID
- Signed Responses: Not required
- Name ID format: persistent

After this information is exchanged, a 30 minute meeting will be scheduled between Sonicu IT and customer IT to enable SSO and validate the SSO connection.

After this, all existing user accounts for the customer will be swapped to SSO.

What else changes with SSO?

- Sonicu technical support will no longer be able to send password reset emails – this must be done via the customer’s IT processes.
- Customers must ensure that all users who may need SoniCloud access are added to the correct AD groups prior to having the users log in.
- To leverage the SoniCloud Mobile app, users will be required to follow the SSO flow on their mobile devices.

- If a user decides to use a personal mobile device (PMD), they must abide by their IT policy on PMDs.

Authentication vs Authorization

SoniCloud's SSO implementation is limited to *authentication* – that is, SSO is utilized to determine if a user has met the requirements to be logged in.

SoniCloud does not utilize SSO for *authorization* – that is, to determine which groups a user should be in (and, therefore, which points of monitoring they have access to).

User authorization will still be handled by the permission levels and groups described earlier in this document.

SONICU™

MONITORING. MEASURED.