

Contents


- ProcessUnity Help Center Information
- Getting Started
 - Application Instances
 - System Access
 - Logging into ProcessUnity**
 - Changing Your Password
 - User Interface
 - Subject Areas
 - Index & Personal Dashboard
 - Application Administration
 - User Management
 - Reporting
 - Properties
 - Expressions & Functions
 - Collaboration and Workflow
 - Importing Data

Getting Started > System Access > Logging into ProcessUnity

Logging into ProcessUnity

To log into ProcessUnity you must have an active user account, which must be set up in the system by an Application Administrator. The user account specifies your user name, which may be your email address, or an alternate username as configured by your Application Administrator

A password is also required to gain access to the application. The initial password (or a new password that results from a password reset request) is system-generated and emailed to the user, either along with their user name or in a separate email (depending upon the application settings). The user is automatically required to change their password when they log into the system using the initial password.

 **Important:** You must log into ProcessUnity each time you use the system. If you are logged in, but the session remains inactive, the system will automatically log you out after 20 minutes, which requires you to log in again. The system does not automatically save your work before timing out, so it is important to save your work before leaving the application idle for any length of time.

To Log Into the ProcessUnity Application:

1. Open the Login page by using a web browser to open the direct URL link to your ProcessUnity instance.

Contents

- ProcessUnity Help Center Information
- Getting Started
- Application Administration
- User Management
 - Administering User Accounts
 - Managing User Access
 - Configuring Single Sign-On
 - Single Sign-On Overview
 - SAML 2.0 Overview and Workflow
 - SAML 2.0 Requirements and Setup
 - Digest Token Authentication Overview and Workflow**
 - Digest Token Authentication Setup
 - Digest Token Authentication Redirect
 - Digest Token Authentication Token Expir

User Management > Configuring Single Sign-On > Digest Token Authentication Overview and Workflow

Digest Token Authentication Overview and Workflow

Digest Token Authentication is similar to HTTP Basic Authentication, except that the Identity Provider (IdP) sends user credentials with a digest token, which is a cryptographic hash of the password and a timestamp.

Digest Token Authentication provides a customized Single Sign-On (SSO) method in that it enables customers to use custom business logic and internal entitlement systems (Active Directory, SiteMinder, etc.) for authentication.

Digest Token Authentication Workflow

Digest Token Authentication requires the customer to have an authentication server for pre-authenticating users on their network. The customer's authentication server sends the user credentials along with a digest token to the ProcessUnity web server for authentication against a ProcessUnity user account. The digest token is created using a secret key that is shared between the customer's authentication server and the ProcessUnity web server.