Password Authenticator Plugin

The Password Authenticator plugin manages passwords for CO People. *(experimental)*

⚠️ This plugin is considered Experimental.

- Installation
- Password Source Mode
  - Autogenerate
  - External
  - Self Select
- Password Policies
- Password Hashing Formats
- Supported Provisioners
- Self Service Reset (Registry v4.1.0 and later)
- Self Service Reset (Registry v4.0.x)
- See Also

Installation

1. This is a non-core plugin, see Installing and Enabling Registry Plugins for more information.
2. This plugin requires PHP 7 or later (for random_bytes).

Password Source Mode

Beginning with Registry v3.3.0, each instantiated PasswordAuthenticator is configured with a *Password Source* mode, indicating how the Passwords associated with the Authenticator are created. Supported modes are

- **Autogenerate**: The Password is autogenerated on demand, and displayed once.
- **External**: The Password is managed by an external component via the REST API.
- **Self Select**: The Password is self selected by the individual. This is the mode for all PasswordAuthenticators instantiated prior to v3.3.0.

Autogenerate

Autogenerated Passwords are established by visiting the *Manage* link for the appropriate Authenticator. The autogenerated Password will be displayed once when it is generated, afterwards the Password cannot be recovered through the Registry interface and a new Password must be generated. Autogenerated Passwords are suitable for use as Service Tokens.

The maximum length of the Password can be specified, though note that generated passwords may occasionally be 1 or 2 characters shorter. Dashes will be inserted in the generated password after every fourth character to increase readability, but do not count towards the maximum Password length.

External

External Passwords are expected to be entirely managed by another component via the REST API. The use of Unprivileged API Users may be supported in a future release (CO-1874).

Self Select

Self Selected Passwords are managed directly by the individual, in accordance with the configured Password Policies (below).

Password Policies

Much angst has been generated over the years as security experts try to decide what the appropriate password policies should be. How long should a password be? How many character classes should be required? How often should the password be changed? What types of questions are good for resetting the password?

The Password Authenticator Plugin supports the NIST 800-63B Digital Identity Guidelines. In summary:

- Passwords must be at least 8 characters in length (§5.1.1.1). The minimum and maximum length of the password is configurable.
- Password hints are not supported (§5.1.1.2).
- Password character composition checks are not supported (§5.1.1.1).
- Passwords do not expire on a scheduled basis (§5.1.1.2). That is, there is no ability to require a password change after (eg) 90 days. (A password can be manually expired or reset.)
- Passwords may not be reset using knowledge based pre-stored secrets (ie: password reset questions or "backup memorized secrets", §6.1.2.3).

Checking against commonly used or compromised passwords (CO-1501) and password strength meters (CO-1502) are not currently supported.

These policies only apply to Self Selected Passwords.

Password Hashing Formats

The following hashing formats are currently supported:

1. **Crypt**, as implemented by the PHP password_hash function using PASSWORD_DEFAULT. This is the strongest hashing option, but is only suitable for use in PHP based applications that implement password_verify. This format is enabled by default and cannot be disabled since it is used internally by the plugin.
2. **SSHA**, or Salted SHA-1. This option is suitable for writing to LDAP servers. Available as of Registry v3.2.0.
3. **Plaintext**, or unhashed. This option is normally not recommended, but may be suitable for select scenarios where a password must be provisioned in plaintext to a legacy downstream system.
4. **External**. This option indicates hashing of the Password is handled by an external component, for use with the External Password Source Mode, and can only be set via the REST API. Available as of Registry v3.3.0.

Additional formats are likely to be supported in future releases.

Multiple hashing formats may be enabled concurrently. When a Password is set or changed, the password will be hashed in each enabled format.

Supported Provisioners

The LDAP Provisioning Plugin supports writing the hashed password to the `userPassword` attribute. As of Registry v3.2.0, the plugin will only write SSHA hashed values to the LDAP record.

Self Service Reset (Registry v4.1.0 and later)

Self Service Credential Reset is managed by the Recovery Dashboard Widget, working with the Password Authenticator Plugin. The Recovery Widget handles user identity lookup before handing off the reset operation the the Password Authenticator.



Self Service Reset currently only supports Self Select Password Source Mode.

Self Service Reset (Registry v4.0.x)

Registry v4.0.0 introduces the ability for users to reset their own password. This feature is disabled by default.

Self Service Reset works by exposing an unauthenticated page where users may enter an Identifier or verified Email Address. If the value matches an active CO Person record, a reset notification message will be sent to all verified Email Addresses associated with the record. The message notification will include a single use token (embedded in a URL) that will allow the bearer to select a new password.

To enable Self Service Reset, first define a Message Template with a context of *Authenticator*. This is the message that will be sent to the verified email address(es), and should minimally include the `(@RESET_URL)` substitution. Next, enable Self Service Reset for the desired Password Authenticator configuration. Configure it with the appropriate Reset Message Template.

A Redirect URL may be specified on successful reset to send the user to an appropriate page, such as documentation, an application, or an account management page. Otherwise, the user will be sent to the Password Authenticator's password management page.

Once enabled, the Password Authenticator configuration will render the *Self Service Reset Initiation URL*, which is the path to the unauthenticated page used to start the reset process.



Self Service Reset currently only supports Self Select Password Source Mode.



Locked Authenticators cannot be reset. Similarly, Authenticators cannot be reset for CO People not in Active or Grace Period status.

The search interface may still send a reset token in these circumstances, however on validation the request will be rejected.

See Also

- Authenticator Notification on Change
- Recovery Dashboard Widget
- Password Dashboard Widget