Service Tokens

Service Tokens Using the Password Authenticator Plugin

As of Registry v3.3.0, Service Tokens can be implemented via Authenticator Plugins. As a result, Service Tokens need not be Passwords. To use Service Tokens, first set up an appropriate Authenticator. (In particular, the Password Authenticator Plugin may be useful.) Then edit (or create) the desired Registry Service and select the Authenticator in the configuration.

The LDAP Provisioner supports using PasswordAuthenticators to populate the `voPersonApplicationPassword` attribute.

Service Tokens in Registry v3.2.x and Earlier

As of Registry v3.3.0, Service Tokens as described in this documentation have been removed. Similar functionality is available via the Password Authenticator Plugin as described above. This documentation applies to Registry v2.0.0 through v3.2.x.

Service Tokens are currently implemented as an optional plugin, and must be enabled. Once enabled, Service Tokens will be available for all COs on the platform that have CO Services defined.

Background

CO Service Tokens are an implementation of *application specific passwords*. CO Service Tokens are based on Registry Services. CO Service Tokens are available as of v2.0.0.

Configuration

1. Define a CO Service for each application that Tokens will be enabled for.
2. Enable Tokens for each CO Service via *Configuration >> Service Token Settings*. Set an appropriate token type.
3. Each CO Person who wants to set a Token can access token generation via their identity drop down menu (from their name in the top menu bar), via *Service Tokens >> CO*.
    a. After clicking *Generate* for the desired service, the Service Token will be displayed once, and should be immediately copied to the desired application client. Subsequently, a new Token may be generated, but it is not possible to view the current token.

Restrictions

There are various restrictions with the current implementation:

1. Only plaintext tokens of 8 or 15 characters are supported.
2. Once set, a token cannot be revoked completely, though it can be changed.
3. Although provisioning is initiated when a Service Token is set, provisioners do not currently have access to the Service Token records via the normal mechanism for accessing provisioning data. In other words, there is no out of the box mechanism for accessing Service Tokens. A custom provisioner must be written.
    a. An experimental Provisioner Plugin, *LdapServiceTokenProvisioner* is available to write a service token to the `userPassword` attribute. It is an optional plugin, and must be enabled. Once enabled, it is configured by associating with an existing LDAP Provisioning Target and a single CO Service, for which it will write associated service tokens to the CO Person LDAP record. Be sure to order the Service Token Provisioner to run *after* the primary LDAP provisioner. This Plugin is likely to be replaced or removed in a future release.
4. Although administrators can technically assign tokens on behalf of a user, there is no link from the CO Person canvas page to do so.

See Also

- cm_co_service_token_settings
- cm_co_service_tokens

- cm_co_services