AuthTool Documentation

Release 1.0.0

Lucid Operations

January 05, 2016

Contents

Contents:

CHAPTER 1

AuthTool

AuthTool is a self-service password reset and SSH public key management application for OpenLDAP directories.

Features include:

- Forgotten passwords can be reset using a token sent by email.
- Forgotten username reminders can be sent by email.
- Passwords can be changed using the current password.
- SSH public keys can be validated and added or deleted.

1.1 Prerequisites

This application makes many assumptions about your LDAP server's configuration and schema.

1.1.1 LDAP Schema

- The sshPublicKey schema from the openssh-ldap-publickey project.
- The `posixUser` objectClass
- The `sambaSamAccount` objectClass

1.1.2 LDAP Configuration

This application assumes anonymous binds are permitted for obtaining limited user information. A service account is used for administrative operations such as setting passwords.

1.2 Running AuthTool

You can run AuthTool in two supported ways: Docker and locally. Both use the same interface, so it comes down to personal preference.

1.2.1 Docker

A Dockerfile is included to build and run the application.

1.2.2 Local

This application is meant to use the internal CherryPy server. Therefore, it can simply be run using the provided module:

python serve.py

CHAPTER 2

Configuration

AuthTool uses the standard CherryPy configuration mechanism. In keeping with the standard, there are two configuration files included: server.cfg and app.cfg.

2.1 Server Configuration

Nothing special here. Refer to the docs for what we do here.

2.2 Application Configuration

The application config consists of a few sections, each pertaining to a plugin or area of functionality within the application.

2.2.1 Branding

```
[branding]
appname: "Password & Key Utility"
domain: "example.com"
```

`appname`

The human readable name for the application. This overrides "AuthTool" as the name displayed in the web UI.

`domain`

When provided, adds functionality for input-group addons in the login forms. Also sets the default email domain so users aren't required to enter full email addresses for password resets or username reminders.

2.2.2 LDAP

```
[ldap]
uri: "ldaps://ldap.example.com/"
tls: True
no_verify: False
bind_dn: "cn=admin"
bind_pw: "admin"
base_dn: "ou=people,dc=example,dc=com"
```

`uri`

A valid LDAP url for the server.

`tls`

Negotiate TLS with the server.

`no_verify`

Don't perform certificate validation on TLS connections. Sets `OPT_X_TLS_REQUIRE_CERT` and `OPT_X_TLS_NEVER` on the ldap library.

`bind_dn`

The administrative dn to bind as. This dn should have permissions to write password attributes.

`bind_pw`

The password for the above dn.

`base_dn`

The dn where users will be found. All searches are performed with a scope of `ONE_LEVEL`, so be sure to set this accurately.

2.2.3 E-Mail

```
[email]
html_template: "email.html"
txt_template: "email.txt"
```

Note: The templates will be passed the user object as its input. The `cn`, `reset_url`, `uid`, and `login_url` attributes will be relvant to the templates.

`html_template`

A jinja templated html email template to be used in multi-part messaging for password resets and username reminders.

`txt_template`

A jinja templated plaintext email template to be used in multi-part messaging for password resets and username reminders.

2.2.4 SMTP

```
[smtp]
server: "localhost.com"
port: 25
user: "user"
password: "password"
from: "noreply@example.com"
```

`server`

The SMTP server to use to send email.

`port`

The port to connect to to send mail.

`user`

The optional user to authenticate as with the smtp server. If omitted, authentication is not used.

`password`

The password for the optional user. If user is supplied, this is required.

`from`

The "from" address to send mail from.

2.2.5 Token

```
[token]
secret: "s3kuR1ty"
expiry: 86400
```

`secret`

The secret to use to hash password reset tokens.

> **Warning:** Changing this invalidates all previously generated tokens.

`expiry`

The time, in seconds, to allow a token to exist. Default is 86400 (24 hours).

CHAPTER 3

Models

CHAPTER 4

Plugins

CHAPTER 5

Tools

CHAPTER 6

Indices and tables

- genindex
- modindex
- search