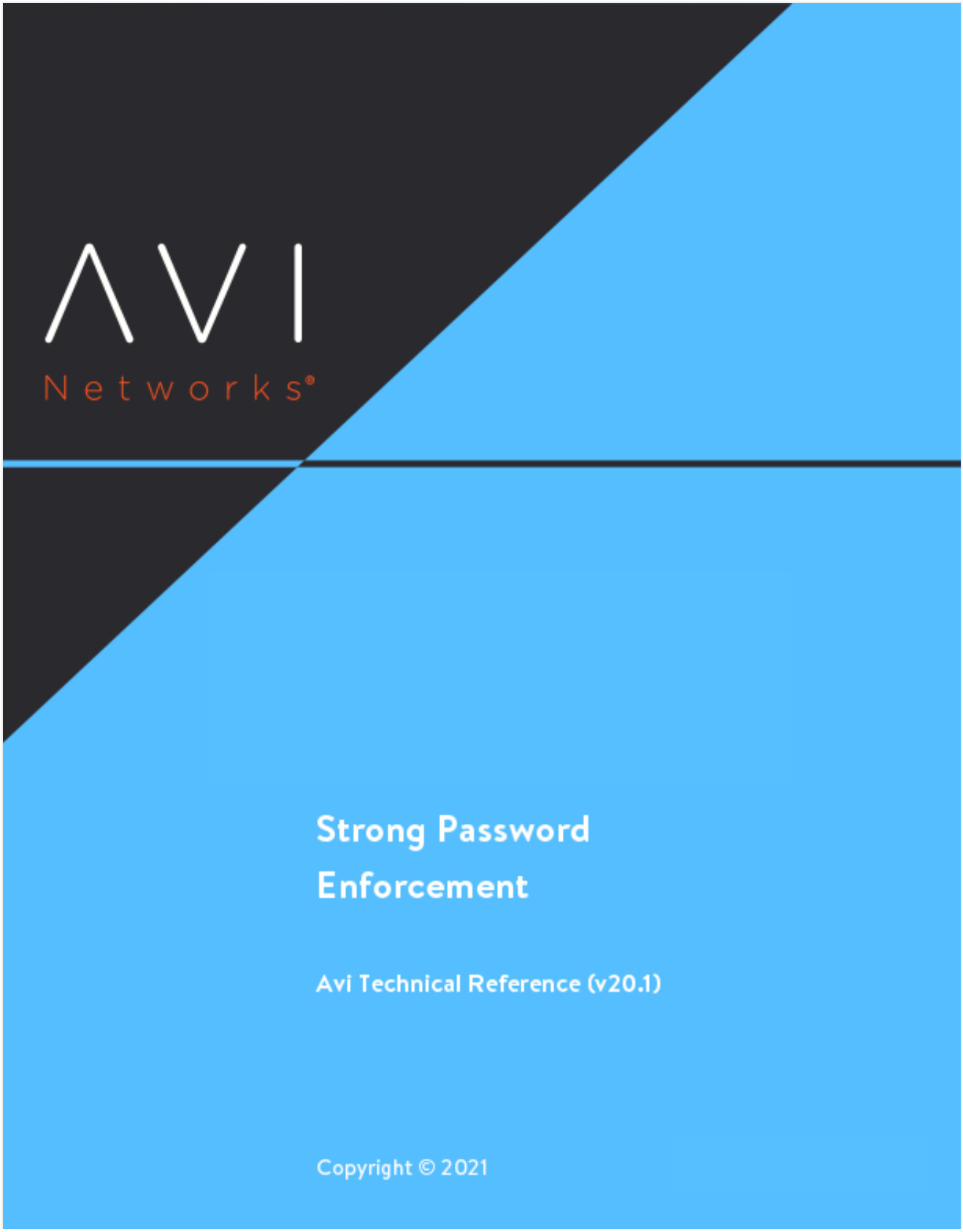

Strong Password Enforcement

Avi Technical Reference (v20.1)

Strong Password Enforcement

view online

The default deployment of Avi Vantage creates an admin account for access to the system. This initial account does not mandate any specific password requirements. Additional user accounts can be created, either local username/password, or remote accounts, which are tied into an external auth system such as LDAP.

For local accounts, it is possible to enable strong password enforcement. Enabling this option does not impact the passwords of existing accounts. It only impacts newly created accounts, or existing accounts that are attempting to change their password. The strong password enforcement feature does not affect remotely authenticated accounts. It also does not affect the password requirements for Avi Vantage's underlying Linux operating system.

Password Requirements (Strong Enforcement Enabled)

The following are the list of password requirements:

- Minimum of 8 characters
- Contains at least one character in each of 3 of the 4 following categories:
  - Uppercase letters
  - Lowercase letters
  - Digits
  - Special characters

Starting with Avi Vantage version 20.1.3, you can specify the minimum permissible password length when password complexity is enforced. The configurable minimum password length can be between 6 and 32 characters with the default as 8 characters.

You can configure minimum password length using the following CLI command:

```
[admin]: > configure systemconfiguration
[admin]: systemconfiguration > portal_configuration
[admin]: systemconfiguration:portal_configuration > minimum_password_length <value>
```

Strong password enforcement is enabled by default. However, you can disable it if required.

Note: Only an account that has the System Administrator role may change this setting.

Enabling Strong Password Enforcement

Strong password enforcement may be enabled using the CLI commands shown below.

```
bash# <b><i>shell</i></b>
: > <b><i>configure systemconfiguration</i></b>
: systemconfiguration> <b><i>portal_configuration</i></b>
: systemconfiguration:portal_configuration> <b><i>password_strength_check</i></b>
Overwriting the previously entered value for password_strength_check
: systemconfiguration:portal_configuration> <b><i>exit</i></b>
: systemconfiguration> <b><i>exit</i></b>
```

Truncated view of the results:

```
+-----------------------------------+---------------------------------+
| Field                             | Value                           |
+-----------------------------------+---------------------------------+
| uuid                              | default                         |
| portal_configuration              |                                 |
|   enable_https                    | True                            |
|   redirect_to_https               | True                            |
|   enable_http                     | True                            |
|   enable_clickjacking_protection  | True                            |
|   allow_basic_authentication      | False                           |
|   password_strength_check         | True                            |
+-----------------------------------+---------------------------------+
```

Disabling Strong Password Enforcement

```
bash# <b><i>shell</i></b>
: > <b><i>configure systemconfiguration</i></b>
: systemconfiguration> <b><i>portal_configuration</i></b>
: systemconfiguration:portal_configuration> <b><i>no password_strength_check</i></b>
Overwriting the previously entered value for password_strength_check
: systemconfiguration:portal_configuration> <b><i>exit</i></b>
: systemconfiguration> <b><i>exit</i></b>
```