Password Expiration Notification

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	5G-UPF
Applicable Platform(s)	VPC-SI
Feature Default Setting	Disabled – Configuration Required
Related Changes in This Release:	Not Applicable
Related Documentation	*UCC 5G UPF Configuration and Administration Guide*

Revision History

Table 2: Revision History

Revision Details	Release
First introduced.	2022.01.0

Feature Description

If the password isn't reset before the expiration date, you get locked from the UPF. You're allowed to log in back only when the password is reset by the administrators manually.

UPF provides password expiration notification to Context/AAA/Radius users. UPF supports configuration and expiration of passwords for Administrators, Config Administrators, Inspectors, and Operators. Following provisions are supported:

- Specify the password warning interval. It warns you about password expiry.
- Specify the password grace interval. During this grace interval, you can change the password by yourself rather than approaching the Administrator every time.
- Warning interval and Grace interval have a global configuration under a context. If the user level configuration doesn't specify either of these values, global values under the context take effect.

The default values of the parameters are according to the Security Guidelines.

- Expiry Interval—Maximum age of the password (default: 90 days)
- Warn Interval—Warning period before password expiry (default: 30 days). You get a warning about approaching password expiry. You can continue without changing the password.
- Grace Interval—Days after password expiry you can use the old password. Beyond the grace period, you may not be able to log in with the old password. Admin has to reset the password for you.

For example:

```
login: xxx
password: xxx

Case 1: [Normal]
# {you are logged in}

Case 2: [When in warning period]
Warning: Your password is about to expire in 0 days.
We recommend you to change password after login.
Logins are not allowed without acknowleding this.
Do you wish to continue [y/n] (times out in 30 seconds) :

Case 3: [when in grace period]
Your password has expired
Current password:
New password:
Repeat new password:

Case 4: [after the grace period]
Password Expired (even beyond grace period, if configured). Contact Security Administrator
to reset password
```

Upgrade and Downgrade Enhancement for Password Expiration Notification

Password Expiry Notification feature has introduced many new keywords in Subscriber configuration such as **max-age**, **exp-grace-interval**, and **exp-warn-interval**. These new parameters are configured at the Context Global level. Context Global level parameters are used when per user level configuration isn't configured with a default value. For example, for the **max-age** of the password, the default value is 90 days.

For the user profiles with no "expiry-date" at per user level, startup config takes an expiry date of 90 days for that user. This problem can be solved by manually editing the startup configuration file, but this solution leads to issues when users are distributed across locations.

In case if downgrade is needed, user profiles are lost as new keywords aren't valid for older releases.

With the password expiration notification enhancement, the upgrade procedure is updated, and the downgrade process is changed with the help of new **save config** CLI option, **legacy-password-expiry**.

Upgrading and Downgrading Procedures using Save Configuration Command

Use the following upgrade process:

- Before upgrade, add **no password max-age** command at context level, in all contexts where users are configured, in the startup configuration.
- When reloading with image using the updated startup config, all users that are configured without an expiry date pick up the context level configuration by default and set the user level **no-max-age** keyword automatically.

Use the following downgrade process:

Use the new CLI option, **legacy-password-expiry** in the save config command, based on which new keywords aren't saved. Configuration is stored in a format which the previous release recognizes.

The following prompt is displayed in the Exec mode:

```
configure
   context host_name
      save configuration url [ confd | ignore-locks | obsolete-encryption
| showsecrets | verbose ] [ -redundant ] [ -noconfirm ] [
legacy-password-expiry ]
```

Notes:

- **save configuration** *config-file-path* **legacy-password-expiry**:

  Generates a backward compatible file by removing new Expiry Notification keywords. The **save config** CLI option makes the configuration compatible with older UPF versions.