Password Expiration Notification

Feature Summary and Revision History

Summary Data

Applicable Product or Functional Area	All
Applicable Platforms	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	• *ASR 5500 System Administration Guide* • *VPC-DI System Administration Guide* • *VPC-SI System Administration Guide* • *Command Line Interface Reference*

Revision History

Revision Details	Release
The PasswordExpiryNotification SNMP trap is supported during warning interval before the password expiry.	21.28.m10
P-GW supports no-lockout password feature after the expiry of user account passwords.	21.26

Revision Details	Release
This feature is enhanced with a new option to the **save config** command. The enhancement supports downgrade and ensures that the user profiles do not get lost after downgrade.	• 21.26 • 21.25.3
First Introduced.	21.23

Feature Description

In StarOS, if the password is not reset before the expiration date, you get locked from the configured GWs. You are allowed to log on back only when the password is reset by the administrators manually.

StarOS is enhanced to provide password expiration notification to Context, AAA, and RADIUS users. The configured GWs such as P-GW, S-GW and so on supports configuration and expiration of passwords for Administrators, Config Administrators, Inspectors, and Operators. The following provisions are supported:

- Specify the password warning interval - It gives a warning to the user about password expiry.
- Specify the password grace interval - During this grace interval the user can change the password by themself rather than approaching the Administrator every time.
- Warning interval and Grace interval have a global configuration under a context. If the user level configuration does not specify either of these values, the global values under the context take effect.

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

- Expiry Interval – Maximum age of the password (90 days default).
- Warn Interval – Warning period before password expiry (30 days default). You get a warning about approaching password expiry. You can continue without changing the password.

Note During the warning interval, a PasswordExpiryNotification SNMP trap also gets generated daily for every 24 hrs.

- Grace Interval – Days after password expiry, you can use the old password. Beyond the grace period, you are not 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 Process for Password Expiration Notification

The Password Expiry Notification feature keywords in Subscriber configuration supports the **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 the per user level configuration is not 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.

If downgrade is needed, user profiles are lost as new keywords are not valid for older releases.

Upgrading and Downgrading Procedures Using Save Configuration Command

Use the following upgrade process:

- Before upgrade, add the **[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 will pickup the context level configuration by default and set the user level **no-max-age** keyword automatically.

Use the following downgrade process:

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

Use the following configuration under context configuration:

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

NOTES:

- **save configuration** *url* **legacy-password-expiry**: Generates a backward compatible file by removing the expiry notification keywords. The **save config** command makes the configuration compatible with older versions.