Enhanced Password Security

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All
Applicable Platform(s)	• 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* • *Command Line Interface Reference* • *VPC-DI System Administration Guide* • *VPC-SI System Administration Guide*

Revision History

Important Revision history details are not provided for features introduced before releases 21.2 and N5.1.

Revision Details	Release
With this release, the password security is enhanced with parameters like the maximum life of a password, password expiry warning interval, and password expiry grace period for local users at user, group, and system levels. Also, instead of specifying intervals, administrators can selectively suspend a user either immediately or at a specific date, which is the suspend date.	21.14
First introduced.	Pre 21.2

Feature Changes

As a security measure for Cisco ASR 5500 and VPC products, the local login password is enhanced to secure the products. It is now possible to configure parameters like the maximum life of a password, password expiry warning interval, and password expiry grace period for local users at user, group, and system levels.. By default, these parameters are enabled to secure the product. Administrators of the system can use the default values, change the values as per their need, or disable the parameters (though this is not recommended).

Previous Behavior: In releases earlier to 21.14, for local users, there was no option to configure the maximum life of a password, password expiry warning interval, and password expiry grace period for user and group levels.

New Behavior: In this release, for local users, it is possible to configure the maximum life of a password, password expiry warning interval, and password expiry grace period. These parameters are enabled by default. The Administrator can use the default values or change the values that are based on their requirement.

The parameters are configurable at the global level, user group level (operators, inspectors, administrators, and security administrators), and user level.

Also, instead of specifying intervals, administrators can selectively suspend a user either immediately or at a specific date, which is the suspend date.

The following keywords support the enhanced password functionality:

- The new **exp-grace-interval** and **[security-admin | administrator | inspector |operator]** keywords are added to the **local-user password** CLI command in Global Configuration Mode.
- The new **max-age**, **exp-grace-interval**, and **[security-admin | administrator | inspector |operator]** keywords are added to the **local-user username** CLI command in Global Configuration Mode.

Customer Impact:

The local user is notified with password expiry warnings and provided with password expired information.

Command Changes

local-user password

Use the following configuration to configure maximum life of a password, password expiry warning interval, and password expiry grace period for local users at user group levels.

```
configure
  [ no | default ] local-user password { max-age days | exp-warn-interval
 days | exp-grace-interval days} { security-admin | administrator | inspector
 | operator }
  end
```

NOTES:

- **no** : Disables the specified parameter.
- **max-age** *days*: Specifies the maximum age for a password. Users logging in with a password older than the specified limit are locked out. After the lockout period expires, at their next login attempt, they are prompted to change their password before accessing the CLI. The default is 90 days.

  

  Important Local-user accounts can be configured to either enforce or reject a lockout due to a password's maximum age being reached. Refer to the **local-user username** command for more information.

  days is the number of days that passwords remain valid entered as an integer from 1 through 365.
- **exp-warn-interval** *days*: Specifies the password expiry warning interval in days.

  days is the number of days before which password expiry warning is issued. The valid values range from 7 to 90 days. The default is 30 days.
- **exp-grace-interval** *days*: Specifies the password expiry grace interval in days.

  days is the number of days beyond password expiry date at which the account is locked. The valid values range from 1 to 7 days. The default is 3 days.
- **[security-admin | administrator | inspector | operator]**: Configures as follows:

  security-admin: Configures all local users with security administrator rights.

  administrator: Configures all local users with administrator rights.

  inspector: Configures all local users with inspector rights.

  operator: Configures all local users with operator rights.
- **default**: Sets or resets the corresponding parameter to its default value.

local-user username

Use the following configuration to selectively suspend a user either immediately or on the configured suspend date.

```
configure
  [ no | default ] local-user usernamename [ suspend-date YYYY:MM:DD:HH:MM:SS
 [ warn-date YYYY:MM:DD:HH:MM:SS ] ] [ max-age days [ exp-warn-interval days ]
 | [ exp-grace-interval  days ] ]
  end
```

NOTES:

- **no** : Disables the specified parameter.

- **suspend-date** *YYYY:MM:DD:HH:MM:SS*: Specifies the date and time when the local-user account should be suspended.

  YYYY:MM:DD:HH:MM:SS is the clock in format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss.

- **no warn-date** : Disables impending password expiry warnings.
- **warn-date** *YYYY:MM:DD:HH:MM:SS*: Specifies the date and time when the local-user account suspension warning notification starts.

  YYYY:MM:DD:HH:MM:SS is the clock in format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss.

- **max-age** *days*: Specifies the maximum age for a password. Users logging in with a password older than the specified limit are locked out. After the lockout period expires, at their next login attempt, they are prompted to change their password before accessing the CLI.

  

  Important Local-user accounts can be configured to either enforce or reject a lockout due to a password's maximum age being reached. Refer to the **local-user username** command for more information.

  days is the number of days that passwords remain valid entered as an integer from 1 to 365. The global or user group value is considered as the default value.

- **no exp-warn-interval** : Disables impending password expiry warnings.
- **exp-warn-interval** *days*: Specifies the password expiry warning interval in days.

  days is the number of days before which password expiry warning is issued. The valid values range from 7 to 90 days. The global or user group value is considered as the default value.

- **no exp-grace-interval** : Disables grace period of expired password.
- **exp-grace-interval** *days*: Specifies the password expiry grace interval in days.

  days is the number of days beyond password expiry date at which the account is locked. The valid values range from 1 to 7 days. The global or user group value is considered as the default value.