D

Password Aging

Password aging is a concept where a user's password is only valid for a specific period of time. When this time has expired, the user will be forced to change their password the next time they log in to the system. Enlighten**DSM** supports password aging for user accounts.

Password aging implementation generally has two time periods associated with it: how long the password is valid and a minimum time period where the user is not allowed to change their password. Both of these times are relative to the last time the password was changed. Consequently, every time the user changes their password, the expiration timer is reset.

Different operating systems may use different formats to implement password aging. The methods of storing information may differ along with the granularity of keeping time. The following sections describe two common types of password aging implementation.

Berkeley UNIX and pre-System V.4

This password implementation uses *n* weeks as the unit of time. If a user changes his or her password on two consecutive days, unless these days happened to fall on two different "weeks," the date of the last password change would be the same as the first password change. A password can be valid for a maximum of 64 weeks.

If your system supports this type of password aging, you cannot expire a user's password without first turning password aging on for that user.

System V.4

With the advent of UNIX Release 5.4, a secondary method of storing passwords was created — the shadow password file. This file also includes fields for password aging. The granularity of time for a shadow password is one day. This file is updated as a function of Enlighten**DSM**'s user account management.