

# Lookup Password

The “**Password**” class of Lookup settings allows the definition of what comprises a valid user password. A number of password rules can be configured to match the local policies. These rules will be used to validate the password users can set on their *local* NetYCE account. They have no bearing on the password used when the accounts are managed by Ldap or Active Directory.

The password settings are available for 'manager' level NetYCE users using the [Admin - Lookup](#) menu under the 'Password' class.

## Consec

<= 2

no more than 2 identical consecutive characters

## Default\_age

60

The default password expiry age

## Grace\_logins

2

The number of logins allowed when password is expired

## History

12

Check new password against history for repetitions. Set history to 12

## Lower

>= 1

at least 1 lowercase character

## MaxChars

$\leq 20$

no more than 20 chars

## MinChars

$\geq 8$

at least 8 characters

## MonthEnd

$\leq 12$

no trailing month numbers allowed ([0]1-12)

## MonthStart

$\leq 12$

no leading month numbers allowed ([0]1-12)

## Numbers

$\geq 1$

at least 1 digit

## Realm

CRC

The Realm value is used in calculating the MD5. If a change is desired, it should be done before creating the users. Calculates MD5 from: <user-id>:<realm>:<new-passwd>

## Spaces

$\leq 3$

no spaces allowed

## Special

$\geq 0$

at least 1 special char

## Unique

$\geq 5$

at least 5 unique characters

## Upper

$\geq 1$

at least 1 uppercase character

## Warn\_age

7

The number of days to warn before the password will expire

From:

<https://wiki.netyce.com/> - **Technical documentation**

Permanent link:

[https://wiki.netyce.com/doku.php?id=guides:reference:lookup\\_password](https://wiki.netyce.com/doku.php?id=guides:reference:lookup_password)

Last update: **2024/07/03 12:31**

