MyCena Desk Center Console User Guide

How to get started

Introduction

Warning: Cyber breaches are the number one threat to organisations' survival. Over 80% of those breaches start with passwords.

Problems:

1. Centralised cyberdefences are powerless against a guerilla cyber-army of hackers.
2. The human brain cannot remember strong passwords

Solution: MyCena is a 2-part credentials security solution that decentralises all accesses without remembering any password:

- A management console to distribute strong password rules and policies for every system, network, application, database, device... to all their users
- A decentralised credentials fortress for users to manage strong unique passwords without remembering any. Only the owner can access three-level of security (Bronze, Silver, Gold) of their fortress with a combination of PIN, lock pattern and passphrase (MDC version).

CONVENIENT
Distribute strong passwords rules for every system, application, database, network, device...

SECURE
No master password, no central point of failure

PRIVATE
Only user can access own credentials

MyCena credentials technology

A 2-in-1 solution to decentralise all accesses without having to remember any password

For company

Decentralised accesses

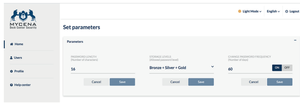
- ✓ **Use strong and unique passwords for every system, network, account, database, WiFi ...**
- ✓ No central point of failure for user or company
- ✓ Distribute password policies, control credentials strength and monitor usage without seeing users' passwords.
- ✓ Fast deployment using MyCena console: no modernisation of system or infrastructure needed
- ✓ Save 50% of your IT calls linked to password resets!

For users

No password to remember

- ✓ **No more passwords to create, type or remember - no master password!**
- ✓ Improved productivity: Passwords always available like keys, even without internet connection
- ✓ More security: Passwords encrypted locally. Only the owner can access with a combination of fingerprint, face ID, PIN, lock pattern and voice passphrase
- ✓ Three levels of security (bronze, silver or gold) to store credentials depending on their sensitivity.

1. Set general password rules



Go to Home > Set parameters, choose the default password length for your company, decide storage password levels and change password frequency (optional).

2. Preload passwords for users (WiFis, printers...)

A. Add passwords in bulk

1 Go to Home > Preload passwords> Upload Systems List and **download template**

2 Fill template, set passwords or specific password rules*, decide if password is shareable, choose security level, fill attributes and click **Save**

3 **Upload template**

4 Check entries and Click **Confirm**

Notes:
1. Fill Attributes with users/user groups to receive preloaded password. If Attributes field is empty, all registered users will receive preloaded password.
2. For urls, type full url address like mycena.co to get logo uploaded on users' password fortress

B. Add passwords one by one

1 Go to Home > Preload passwords> Preload Password and click **+ Add Password**

2 Fill pop-in, set specific password rules*, generate password, decide if password is shareable, choose security level, enter attributes (All or selected) and click **Save**

* Set specific password length and rules, for example excluding lowercase letters, uppercase letter, numbers, special characters, and click **Save**

3. Preload systems for users (user accounts, devices ...)

A. Add systems in bulk

1 Go to Home > Preload policies> Upload Systems List and **download template**

2 Fill system name (url, system, device, set specific password rules*, decide if password is shareable, choose security level, fill attributes) and click **Save**

3 **Upload template**

4 Check entries and Click **Confirm**

Notes:
1. Fill Attributes with users/user groups to receive preloaded system. If Attributes field is empty, all registered users will receive preloaded system
2. For urls, type full url address like mycena.co to get logo uploaded on users' password fortress

B. Add systems one by one

1 Go to Home > Preload policies> Preload Url and click **+ Add Url**

2 Fill pop-in, set specific password length and rules (for example excluding lowercase letters, uppercase letter, numbers, special characters), decide if password is shareable, choose security level, select or enter attributes (All or selected) and click **Save**

4. Set roles and permissions

1 Go to Users> User management> Roles and Permissions and choose role to edit

2 Change role permissions (access to console, manager users, manage settings, manage preloaded passwords, manage preloaded urls, create passwords) and click **Save**

Notes:
1. There are three preset role levels, with level 1 being the highest. Any role level can only manage levels under its own.

5. Add users

A. Add users in bulk using template

1 Go to Users> User management> Upload user list and **download template**

2 Fill template and click **Save**

3 **Upload template**

4 Check entries and Click **Confirm**

Notes:
1. Fill Attributes with users/user groups to receive the preloaded passwords and systems.

B. Add users in bulk using Active Directory

1 Go to Users> User management> Upload user list and click **AD Settings**

2 Fill pop-in and click **Save**

3 Click **Import from AD**

4 Check entries and Click **Confirm**

Notes:
1. Attributes is pre-filled with AD's location and department fields. Edit accordingly.
2. Role is pre-filled to Operator. Edit accordingly.

C. Add users one by one

1 Go to Users> User management> User list and click **Add user**

2 Fill pop-in and click **Save**

support@mycena.co
www.mycena.co