

Introduction

Congratulations for choosing MyCena to secure your organisation credentials!

Cyber breaches are the number one threat to organisations' survival. Over 80% of those breaches start with passwords. By solving your credentials security once and for all, you mitigate your biggest source of cyber breaches.

Problem 1: Centralised cyberdefences impotent against guerilla hackers

Problem 2: Human brain cannot remember strong passwords

MyCena solves both problems by decentralising all accesses without remembering any password. It comes in two parts:

- A management console to distribute strong password rules and policies for every system, network, application, database, device... to all users
- A decentralised credentials fortress only the user can access.

This is the MyCena console user guide for both MyCena Desk Center (MDC) and MyCena Business Fortress (MBF), except for Section 4 which only applies to MDC.



CONVENIENT

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



SECURE

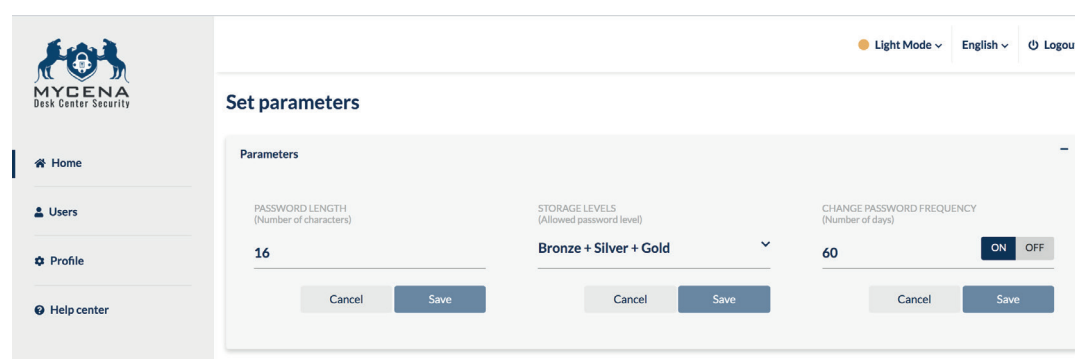
No master password, no central point of failure



PRIVATE

Only user can access own credentials

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

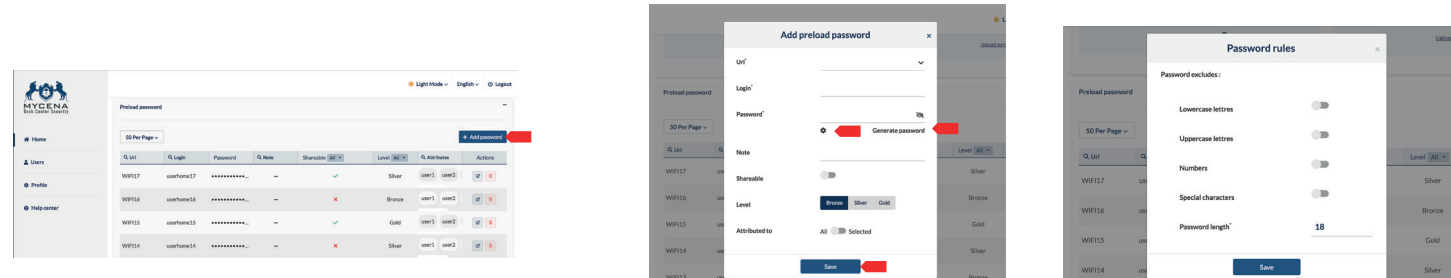


- Go to Home > Preload passwords> Upload Systems List and **download template**
- Fill template, set passwords* or specific password rules*, decide if password is shareable, choose security level, fill attributes and click **Save**
- Upload template**
- Check entries and Click **Confirm**

Notes:

- Fill Attributes with users/user groups to receive preloaded password.
- For urls, type full url address like mycena.co to get logo uploaded on users' password fortress

B. Add passwords one by one



- Go to Home > Preload passwords> Preload Password and click **+ Add Password**
- 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 lowercase letters, uppercase letter, numbers, special characters, and click **Save**

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

A. Add systems in bulk

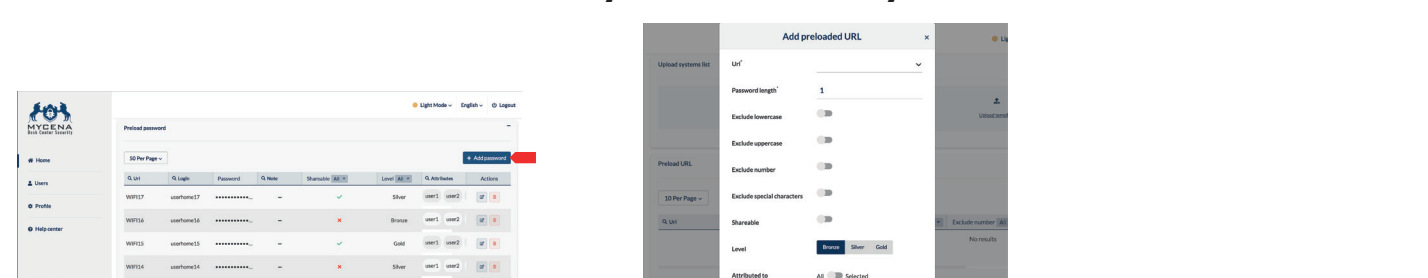


- Go to Home > Preload policies> Upload Systems List and **download template**
- Fill system name (url, system, device), set specific password rules*, decide if password is shareable, choose security level, fill attributes and click **Save**
- Upload template**
- Check entries and Click **Confirm**

Notes:

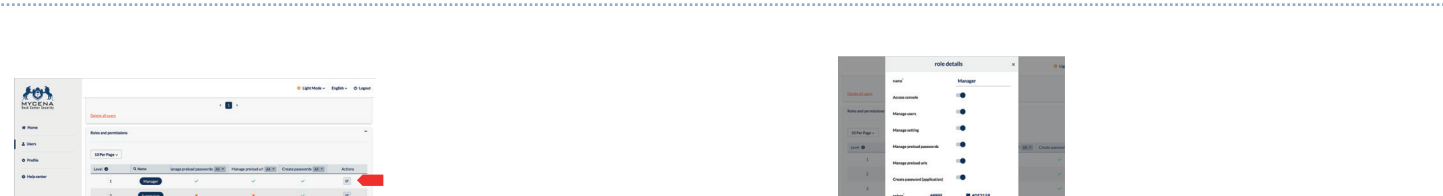
- Fill Attributes with users/user groups to receive preloaded system.
- For urls, type full url address like mycena.co to get logo uploaded on users' password fortress

B. Add systems one by one



- Go to Home > Preload policies> Preload Url and click **+ Add Url**
- 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 (only MDC)



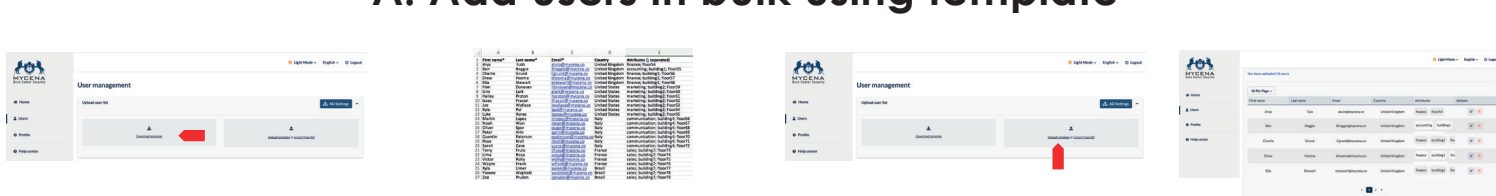
- Go to Users> User management> Roles and Permissions and choose role to edit
- Change role permissions (access to console, manager users, manage settings, manage preloaded passwords, manage preloaded urls, create passwords) and click **Save**

Notes:

- 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



- Go to Users> User management> Upload user list and **download template**
- Fill template and click **Save**
- Upload template**
- Check entries and Click **Confirm**

Notes:

- Fill Attributes with users/user groups to receive the preloaded passwords and systems.

B. Add users in bulk using Active Directory



- Go to Users> User management> Upload user list and click **AD Settings**
- Fill pop-in and click **Save**
- Click **Import from AD**
- Check entries and Click **Confirm**

Notes:

- Attributes is pre-filled with AD's location and department fields. Edit accordingly.
- Role is pre-filled to Operator. Edit accordingly. (Only MDC)

C. Add users one by one



- Go to Users> User management> User list and click **Add user**
- Fill pop-in and click **Save**