WebLAPS Documentation

weblaps.pro

May 13, 2019

Contents:

1 Working with LAPS Portal **3**
- 1.1 LAPS Passwords access . . . 3
- 1.2 Quick launch buttons . . . 4
- 1.3 LAPS security log . . . 5

2 Installation in Unix **7**

3 Installation in Windows **9**

4 LAPS Portal administration **11**
- 4.1 Accessing admin console . . . 11
- 4.2 Active Directory integration . . . 12
- 4.3 Certificates . . . 14
- 4.4 Access rights management . . . 14
- 4.5 Authentication setup . . . 15
- 4.6 LAPS passwords expiration . . . 17
- 4.7 LAPS Portal API and tokens . . . 18
- 4.8 LAPS Portal and SIEM integration . . . 19
- 4.9 LAPS Portal mobile app settings . . . 20
- 4.10 LAPS Portal high availability mode . . . 21
- 4.11 Extra settings . . . 22

5 LAPS Portal maintenance **25**
- 5.1 LAPS Portal restarting . . . 25
- 5.2 Log files . . . 25
- 5.3 engine.conf file . . . 26
- 5.4 LAPS Portal backup . . . 26
- 5.5 Admin password reset . . . 27
- 5.6 Errors . . . 27
  - 5.6.1 AcceptSecurityContext . . . 27
  - 5.6.2 SSLHandshakeException . . . 27

6 LAPS Portal mobile application **29**
- 6.1 LAPS mobile application enrollment . . . 29
- 6.2 LAPS mobile application usage . . . 31

LAPS Portal is a web application which helps to secure windows environment with MS LAPS solution implemented. MS LAPS is effective mechanism to perform automatic password rotation of built-in Administrator password. **In case of compromising one of user account which is used for LAPS passwords access (like account of help desk user) all computers could be compromised!** To eliminate security risks and provide convenient way for LAPS password accessing LAPS Portal was created.

LAPS Portal has mobile clients which works under Android and iOS devices which in a secure way delivers passwords to mobile device. Mobile client also allows to login to LAPS Portal with help of confirmation of authentication request which is delivered by push notification.

LAPS Portal is written in Java, and could be used on any operation systems which support Java 1.8. LAPS Portal includes all necessary components and does not require additional software like web server or database engine. It is possible to join several LAPS Portal to cluster to operatin in a high availability mode in such case you will need a load balancer and an external database engine.

LAPS Portal uses Active Directory user accounts and groups to perform access control. To increase security of passwords managed by LAPS authentication with one time passwords was added to the portal. Currently following 2fa connectors implemented:

- RADIUS
- LinOTP
- FortiAuthenticator
- Built-in TOTP provider which does not require any external system

Security controls implemented in LAPS Portal

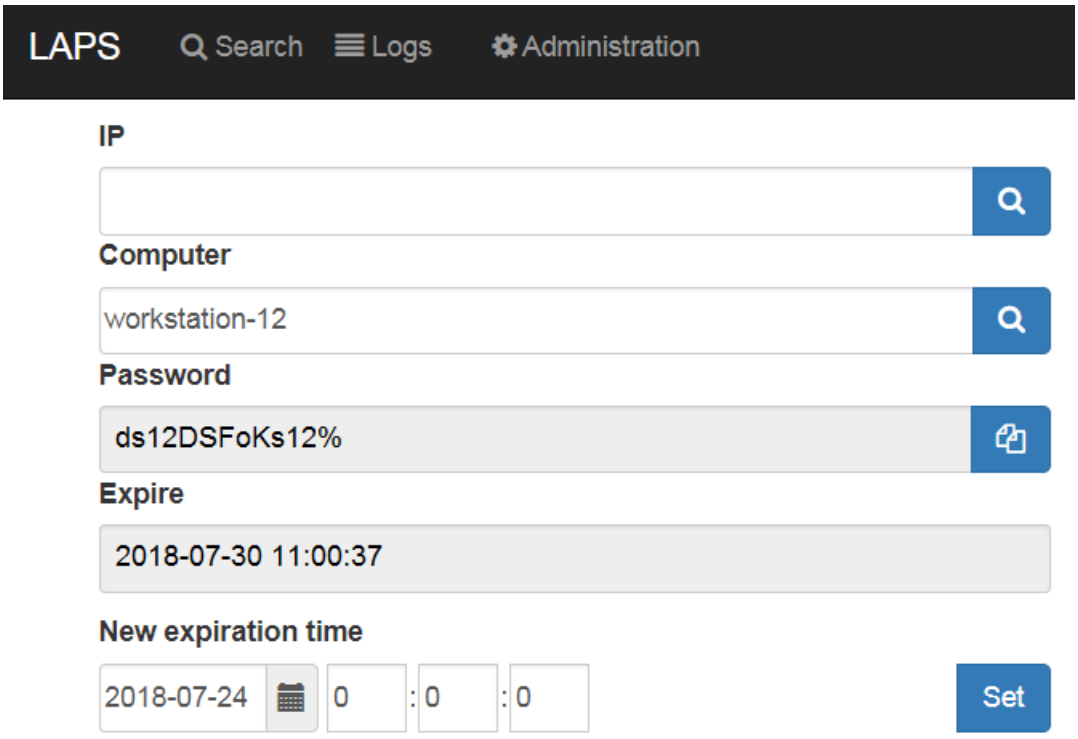
- 2FA or OTP only authentication
- Customizable capcha for brutforce attacks prevention
- Configurable maximum count of requests per seconds to authentications methods
- Configurable maximum count of requests per seconds to LAPS passwords accessing to prevent automatic exports of LAPS managed passwords
- Access to Active Directory via LDAP over SSL
- All secrets are saved in encrypted form
- CSRF protection
- User access token is bind to IP address of successful authentication. Access token has a configurable time limit
- Ability to schedule LAPS passwords backup in encrypted form in case of AD unavailability
- Audit all access to passwords managed by LAPS. It is possible to export LAPS logs in CEF format to external system via syslog

CHAPTER 1

Working with LAPS Portal

1.1 LAPS Passwords access

After successfully login you can get password of computer. It is possible to use computer name of IP address. If you use IP address LAPS portal do reverse DNS lookup to determine computer name



It is possible to mark computer as favorite to save time during next search. LAPS Portal also saves search history (computer names only).

1.2 Quick launch buttons

Warning: Quick launch buttons uses ActiveX that's why supported only in Internet Explorer

You create command templates in **My Profile -> Commands**. Here you can set command patterns to pass computer name and password to any command which can process it. For example to quick launch DameWare remote admin toll you can use following pattern:

```
"c:\program Files\DameWare Mini Remote Control 11.0 x64\dwrcc.exe" -c: -h: -a:1 -m:%pc
↪% -u:Administrator -p:%pwd%
```

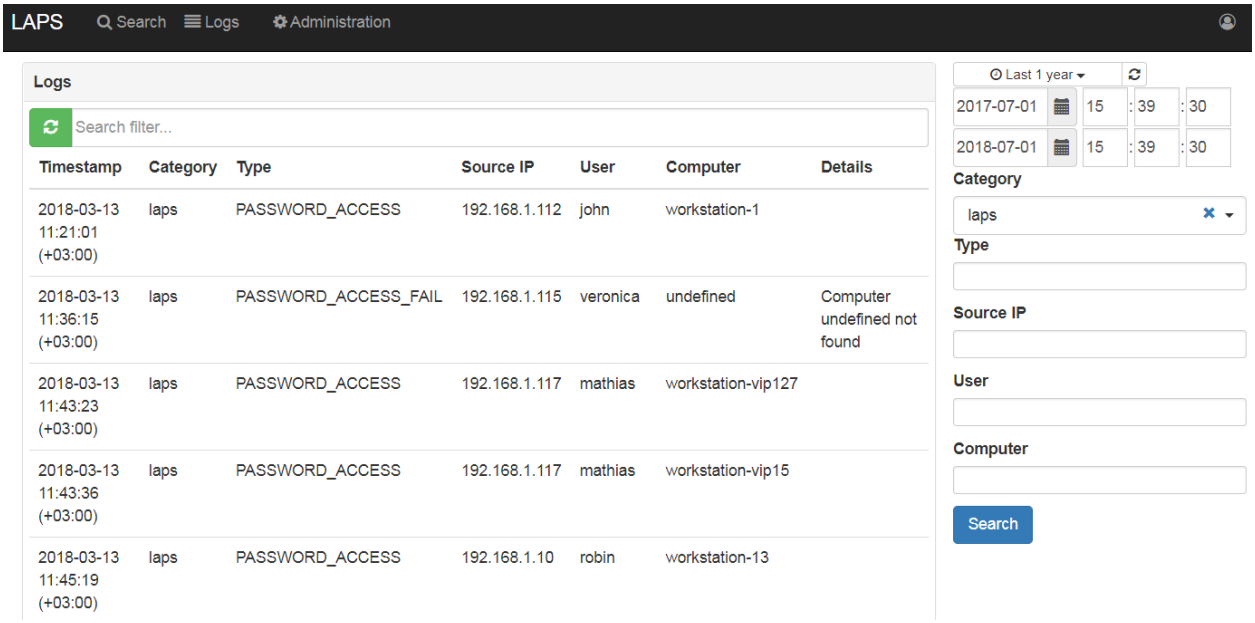
Templates supports following parameters:

- %pc% - computer name
- %pwd% - password
- %copypwd% - copy password to clipboard (will be deleted from command template after copy)

After command templates are configured quick launch button will be shown in LAPS passwords viewer.

1.3 LAPS security log

Portal has built in Log viewer where you can look for various events



CHAPTER 2

Installation in Unix

Installation is pretty simple, the only thing you need is to install Java JRE 1.8

1. Install Java JRE or JDK version 1.8
2. Create local user “laps” – this user will be used to run portal service:

```
useradd laps --shell /sbin/nologin --no-create-home
```

3. Create working directory for LAPS WebPortal and extract distributive:

```
mkdir /opt/laps
unzip /tmp/laps.zip /opt/laps
```

4. Change an owner of the directory and set correct access rights:

```
chown -R laps:laps /opt/laps
chmod -R u=rwx,g=rx,o-rwx /opt/laps
```

5. If java executable is not on PATH set correct path to java executable in /opt/laps/wrapper/conf/wrapper.conf:

```
wrapper.java.command = _____java
```

6. Install LAPS portal service. New service “laps” will be created.:

```
/opt/laps/wrapper/sh/installDaemon.sh
```

7. Run the service:

```
service laps start
```

8. Open in browser https://host:8443

CHAPTER 3

Installation in Windows

Installation is pretty simple, the only thing you need is to install Java JRE 1.8

1. Create local user “laps” – this user will be used to run portal service.
2. Allow user “laps” to work as a service:

```
gpedit.msc -> Local Policy -> User Rights Assignment -> Log on as a service: add␣
↪user "laps"
```

3. Create directory C:\laps\ and extract distributive.
4. Change the directories owner and set up appropriate access rights: user “laps” must have read and write access rights, other users except administrators must not have access to the directory
5. if java.exe is not on %PATH% set correct path to java executable in file C:\laps\wrapper\conf\wrapper.conf. As file path separator use *“/”*:

   wrapper.java.command = path_to_java_exe

6. Install LAPS portal service. New service “laps” will be created.:

```
C:\\laps\\wrapper\\bat\\installService.bat
```

7. If you have your own license file copy it to C:\laps_conf\license.txt. Default destribition includes a community license file.
8. Run the service:

```
net start laps
```

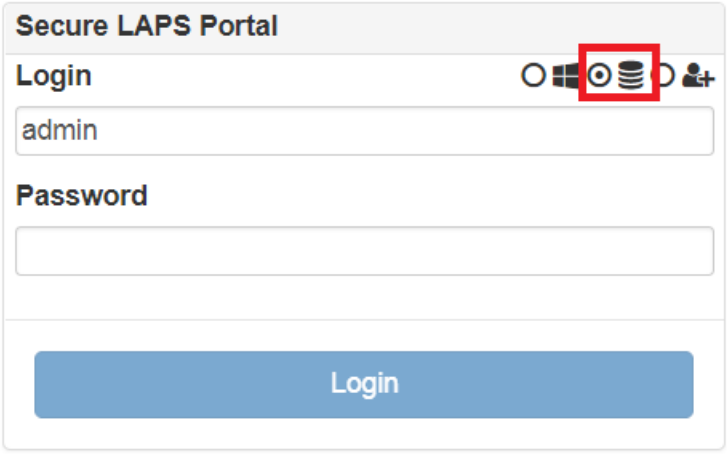
9. Open in browser https://host:8443

CHAPTER 4

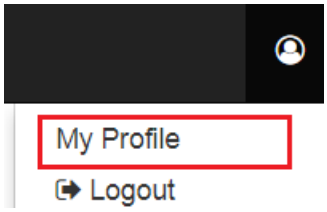
LAPS Portal administration

4.1 Accessing admin console

Right after initial setup LAPS Portal uses port 8443, open LAPS Portal in your browser https://host:8443. Select built-in authorization and login with admin/admin



Warning: Change default password in profile settings menu



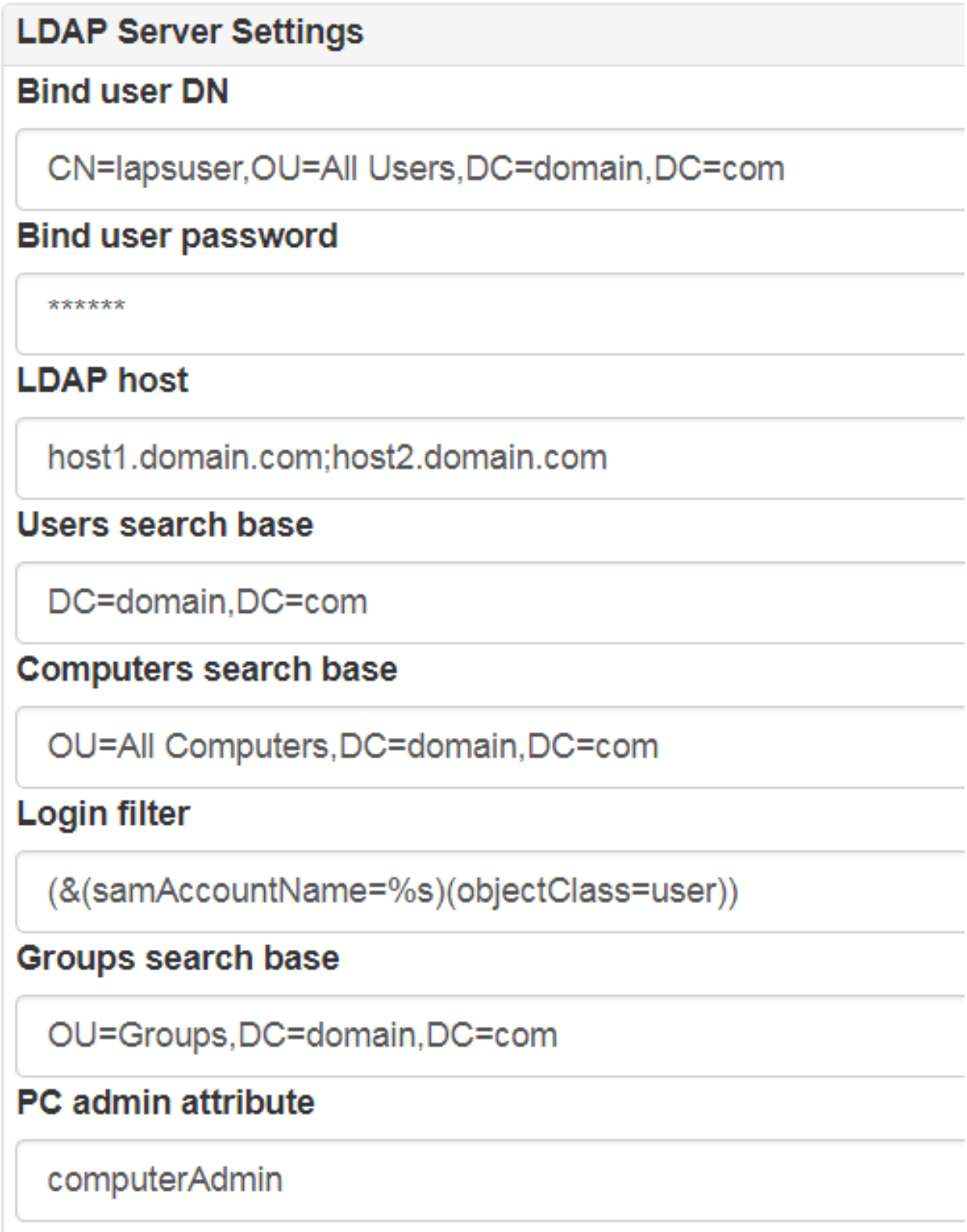
4.2 Active Directory integration

Go to **Administration->Communications->LDAP** and setup following settings:

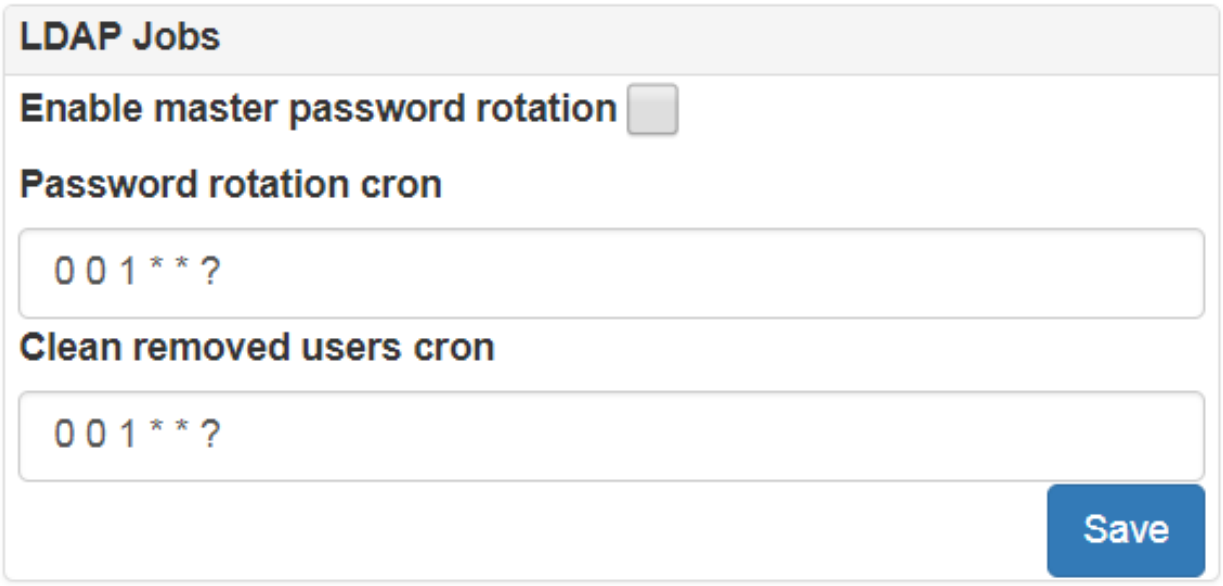
- bind user account which has access rights to get attributes ms-Mcs-AdmPwd and modify ms-Mcs-AdmPwdExpirationTime
- FQDN name of AD servers (it is allowed to set several servers divided by ";"")

> **Warning:** ms-Mcs-AdmPwd is a special attribute which could be accessed via ldap over **SSL** thats why it is impossible to use IP addresses

- Base OU for computers, users and groups searching
- Attribute of a computer which could contains an user or a group (group nesting is not supported) which will allow to get LAPS password of the computer. This mechanism does not connected with access control subsystem based on groups and containers



You can enable scheduled password rotation for bind user



4.3 Certificates

Go to **Administration->Communications->Certificates** and import AD servers certificate and CA certificates (all certificate chain must be imported). In case of other integration which uses ssl/tls protocol like LinOTP HTTP API, FortiAuthenticator and others please do not forget import theirs certificates as well. LAPS Portal supports X.509 DER encoded certificates.

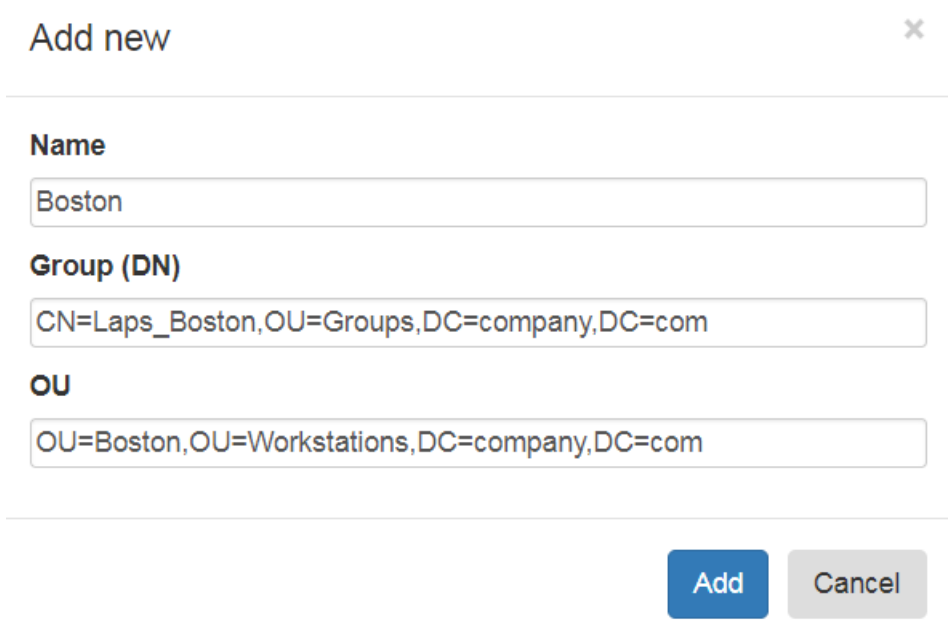
After fresh install LAPS Portal generates self-signed certificate which has alias "jetty". To replace self-signed certificate:

1. **Administration -> Communications ->Certificates** press "Generate CSR" button, enter DNS name of host where LAPS Portal is located and save generated certificated signing request file.
2. Generate certificated signed by externals CA using generated CSR file
3. Import CA's certificate
4. Import certificate signed by CA, set as alias DNS name of server
5. add string parameter "jetty_cert_alias" at engine.conf file with value of certificate alias
6. restart LAPS Portal

Warning: After certificates import do not forget to restart LAPS Portal

4.4 Access rights management

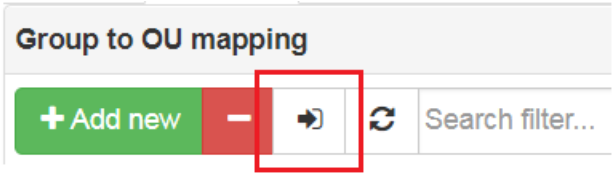
Go to **Administration->Security->Groups** and setup user group to OU mappings. You must use distinguished names of groups and OUs. Members of group will be able to get LAPS passwords of computers in the OU and sub OUs.



It is possible to import CSV file with groups and OUs mapping, file must be in following portal:

```
name of element;group DN;OU DN
forexample:
Boston;CN=LAPS_Boston,OU=Groups,DC=domain,DC=com;OU=Boston,OU=Computers,DC=domain,
↪DC=com
```

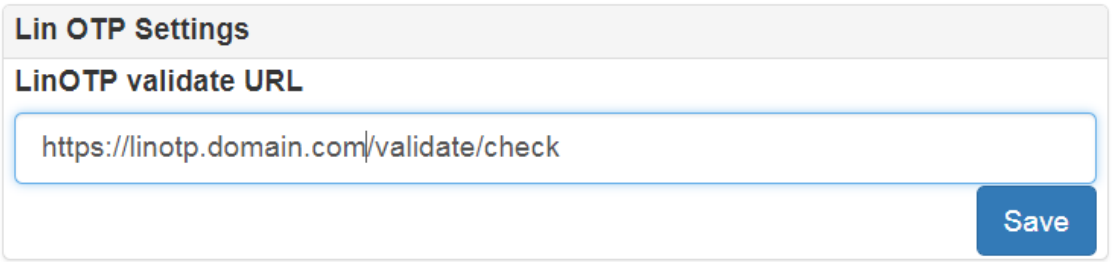
Import the file



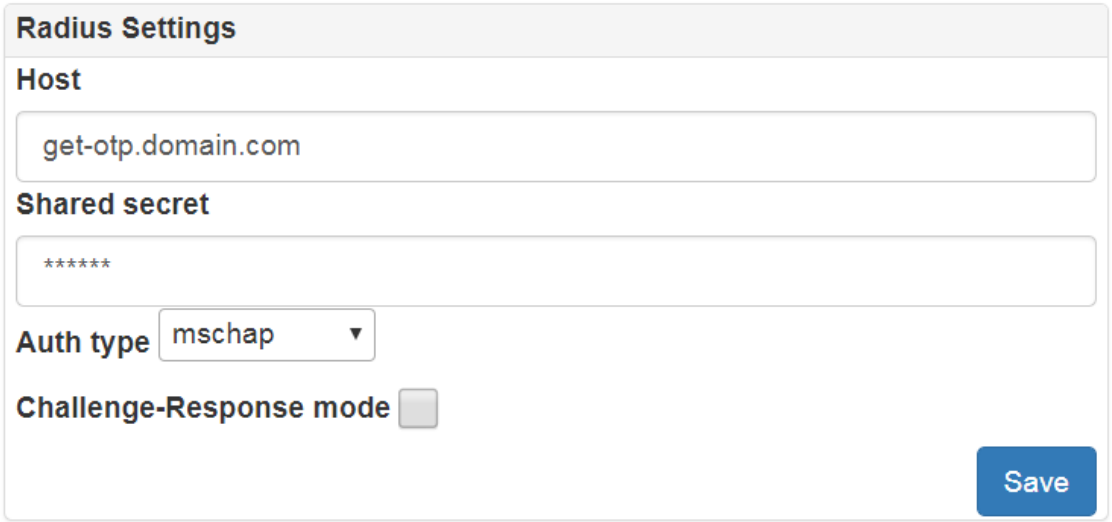
4.5 Authentication setup

Go to **Administration->Security->Authentication** and setup authentication parameters:

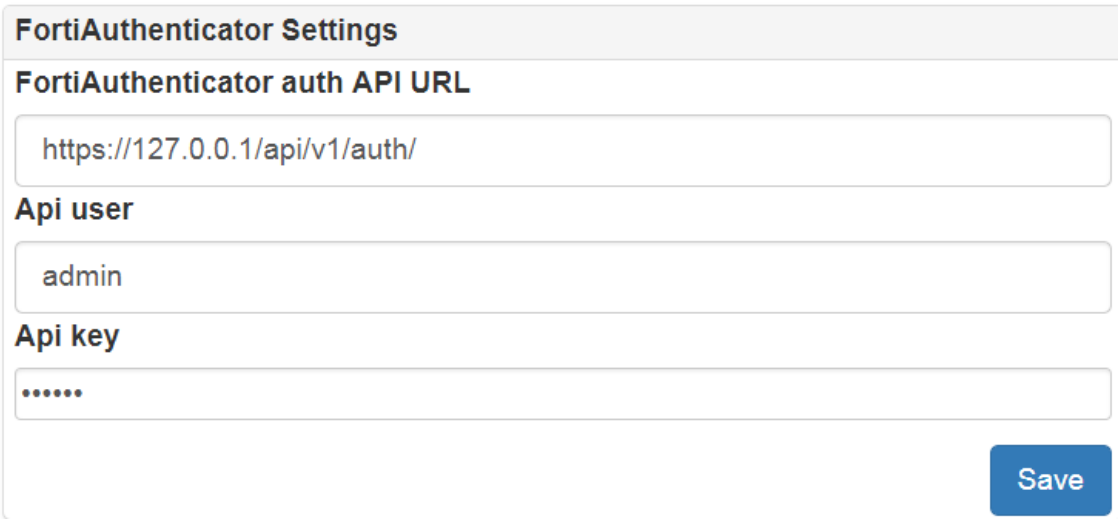
- Require or not password check for internal LAPS Portal users. **If you switch off this requirement then you must enable one time passwords (OTP) validation for this type of users!**
- Require or not password check for Active Directory users. Such approach could be recommended in case you will allow to use LAPS Portal from untrusted environment to eliminate risk of password stealing. **If you switch off this requirement then you must enable one time passwords (OTP) validation for this type of users!**
- Require or not OTP validation for AD users
- Require or not OTP validation for users stored in LAPS Portal
- **Type of OTP provider:**
  - linotp provider is used for integration with LinOTP via http API. You must setup LinOTP valudation URL



– radius provider. You must configure address, shared secret and authentication type: chap, mschap, pap, peap, eap-md5, eap-tls, eap-mschap



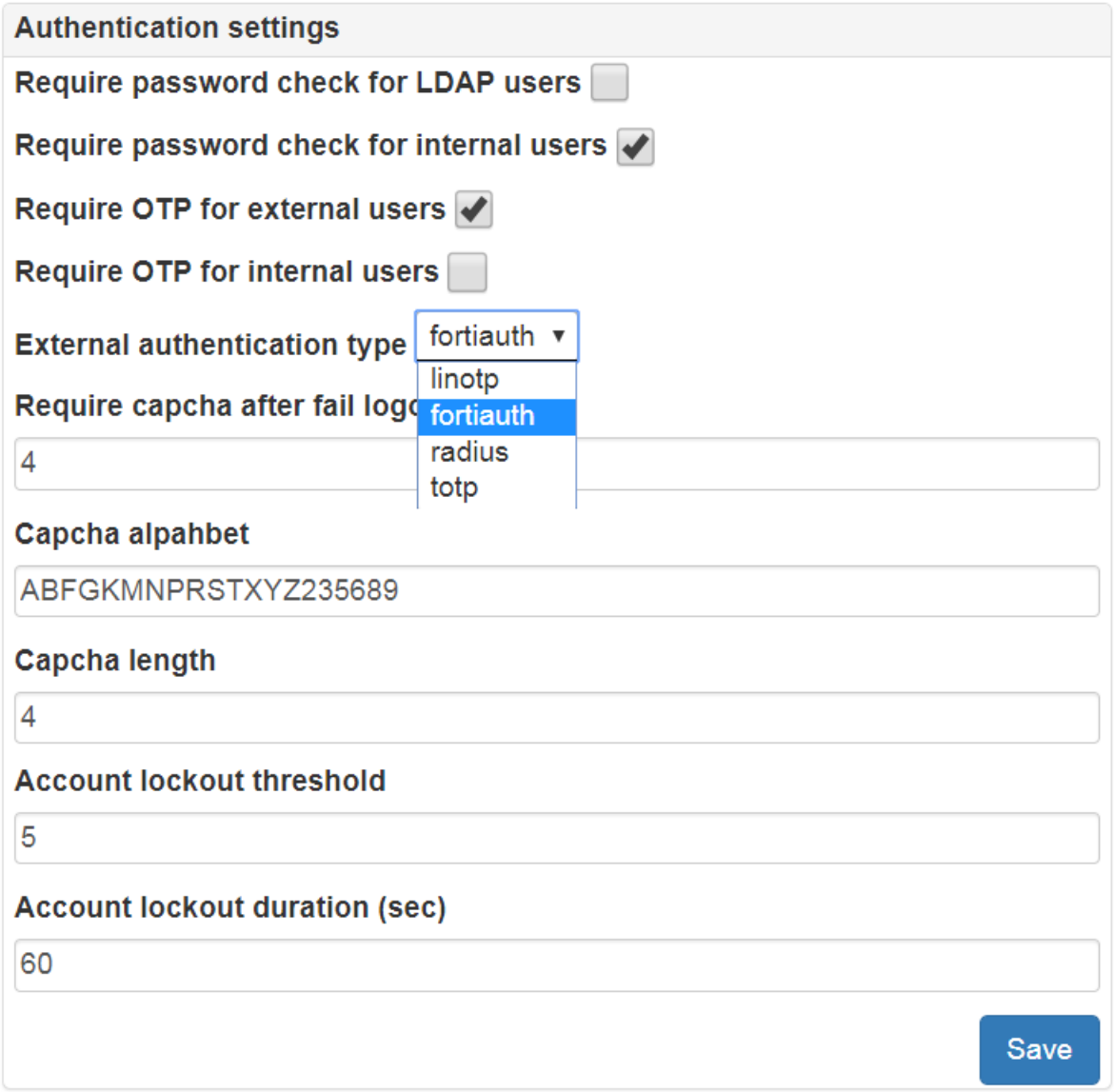
– fortiauth provider for integration with FortiAuthenticator



– totp provider which is built in to LAPS Portal. You can use this provider in case you do not have in your environment OTP system to enable two factor authentication for LAPS Portal. If you use this type of TOTP provider you will need to use mobile application like FreeOTP, Google Authenticator, etc.

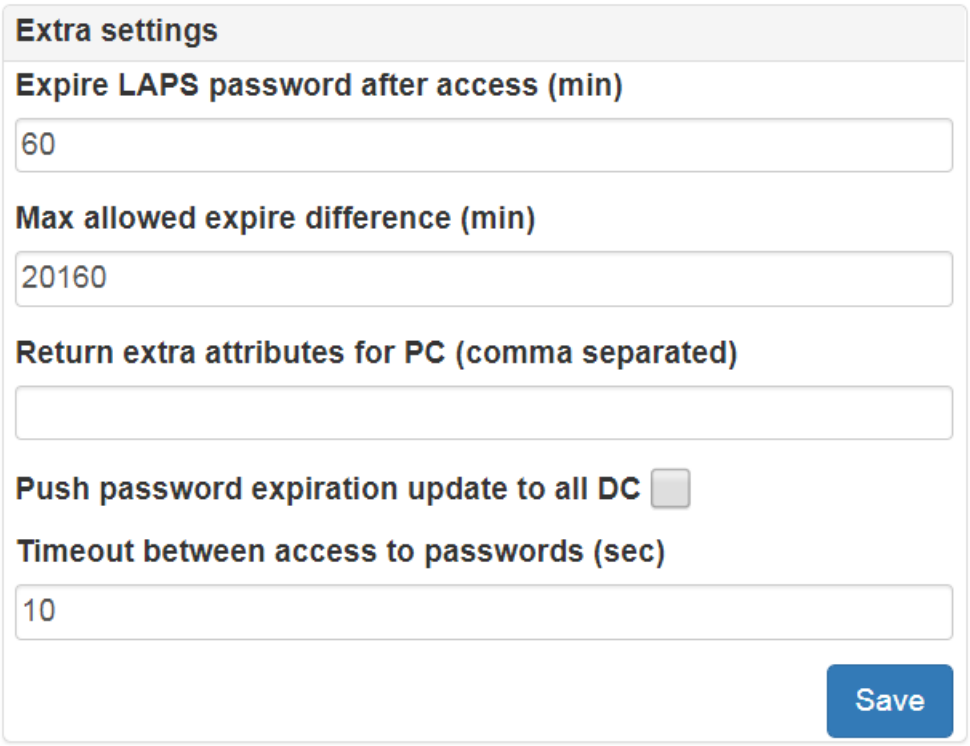
- Capcha generation requirements: capcha alphabet, unsuccessfull login attempts after capcha will be required

- Account lockout policy: Account lockout threshold (number of unsuccessfull login attempts) after user will unable to login during defined period of time



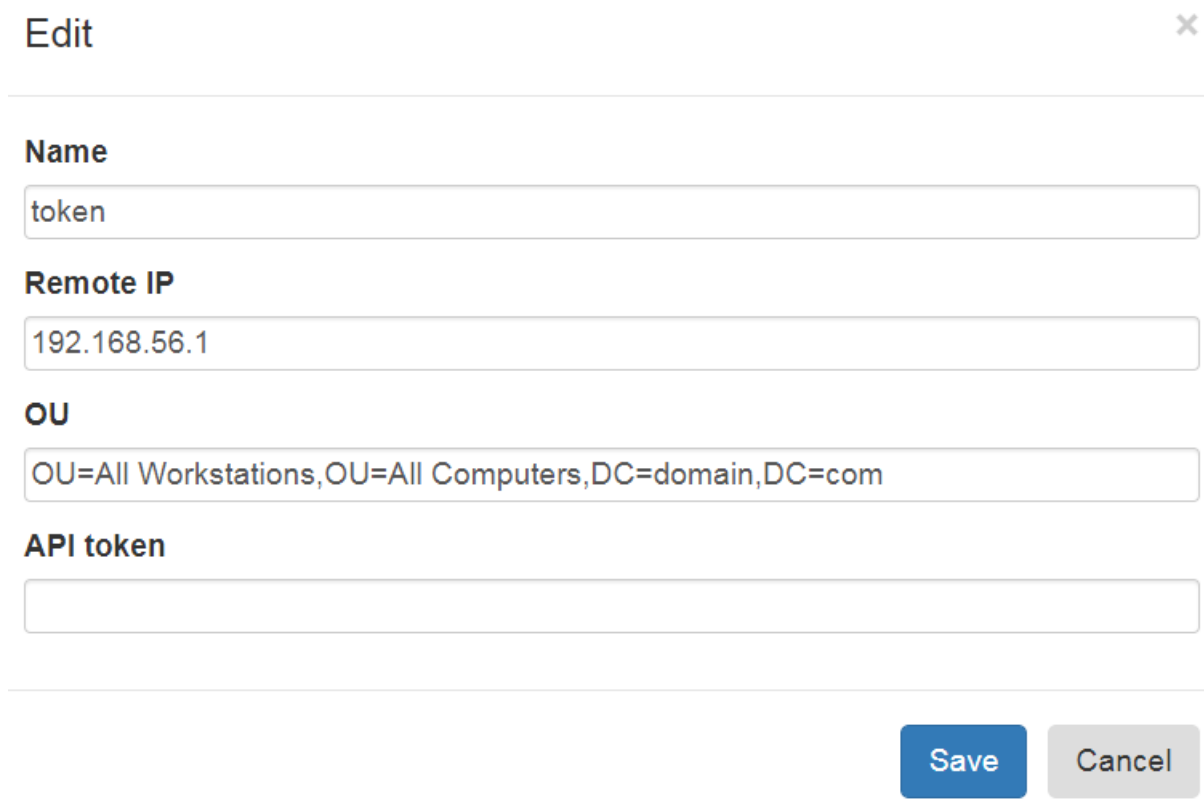
4.6 LAPS passwords expiration

Go to **Administration->Security->Extra** and configure automatic LAPS password rotation. After access to ms-Mcs-AdmPwd by any user LAPS portal will modify ms-Mcs-AdmPwdExpirationTime attribute. You can also configure maximum allowed time difference between current time and value which LAPS Portal user can setup in expire field. If you have more than one domain controller you can force modifing of ms-Mcs-AdmPwdExpirationTime attribute on all configured domain controllers. Optinally you can add timeout between attempts to get passwords. This timeout will prevent from retriving passwords in fast way. This timeout is not used for API access via tokens described below.



4.7 LAPS Portal API and tokens

If you have external systems like Endpoint Detection and Response which require access to passwords managed by LAPS you can use API provided by LAPS portal. To provide access LAPS Portal API you must configure access token. Each access token could be bind to specific IP address and additionally restricted by OU

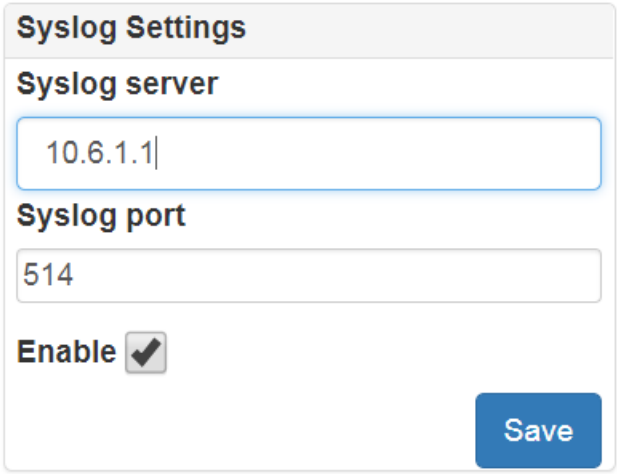


To get LAPS password with help of API you should use GET request to /passwordbytoken/{pc} and pass token in X-Auth cookie

```
GET /passwordbytoken/computer123
Content-Type: application/json
Cookie: X-Auth=APITOKEN
```

4.8 LAPS Portal and SIEM integration

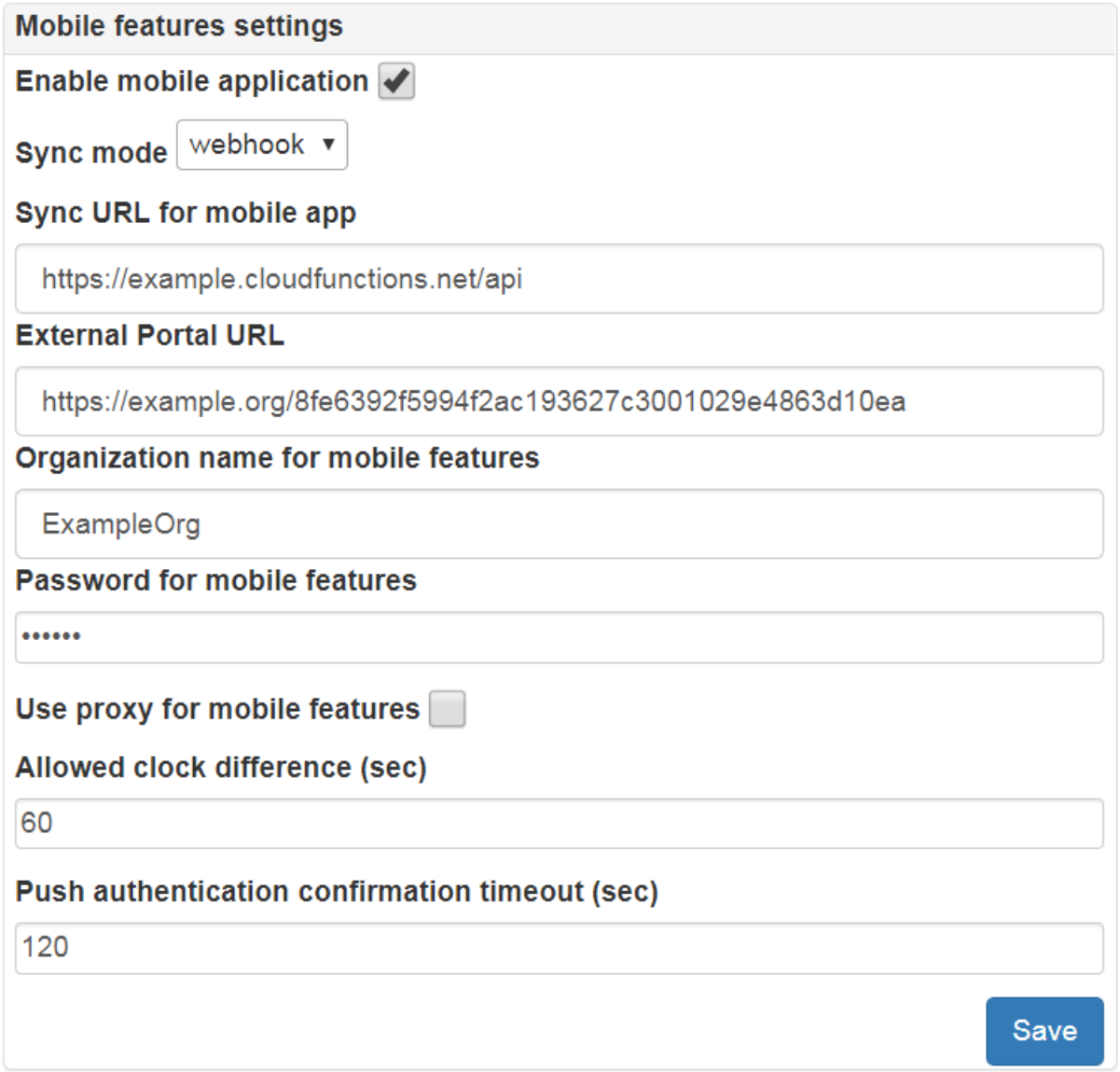
Go to **Administration->Communications->Syslog** and set IP of syslog receiver. LAPS Portal send logs in CEF format via UDP.



4.9 LAPS Portal mobile app settings

LAPS Portal has mobile client which works on Android and iOS devices. With help of mobile application it is possible to get passwords and login to LAPS Portal with help of confirmation at mobile device of authentication request which is delivered by push notification. Go to **Administration->Communications->Mobile** and perform configuration:

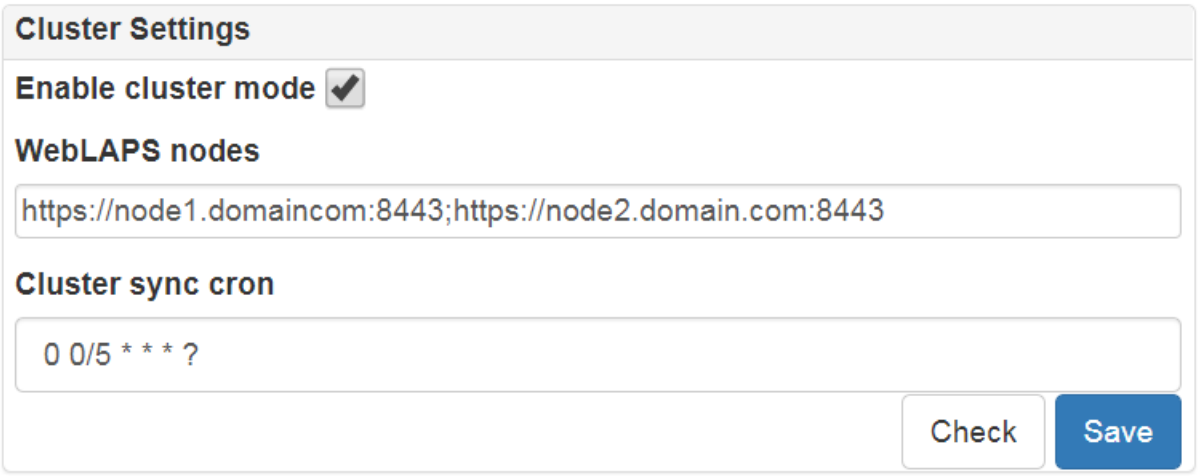
- Enable or disable mobile features of LAPS Portal
- Sync URL for mobile app - is URL which LAPS Portal uses to deliver authentication requests via push notifications. Contact to contact@weblaps.pro to get working URL
- External Portal URL - is an URL which will be used by mobile clients to work with LAPS Portal. The only endpoint which is required for mobile device is /api/mobile/fromdevice. In case if you do not plan to publish mobile API to Internet you can use following URL: https://domain.com/api/mobile and mobile application will automatically transform it to https://domain.com/api/mobile/fromdevice. If you plan to expose mobile API to Internet it is recommended to use reverse proxy with rewrite URL capabilities which will transform all requests in following way: https://example.org/8fe6392f5994f2ac193627c3001029e4863d10ea => https://domain.com/api/mobile. You can additionally allow only POST and OPTIONS methods
- Organization name and password is used by cloud service to deliver authentication requests via push notifications



4.10 LAPS Portal high availability mode

High availability mode allows you to join several nodes of LAPS Portal to single cluster and place them behind load balancer or reverse proxy. Please check requirements before using LAPS Portal in cluster mode:

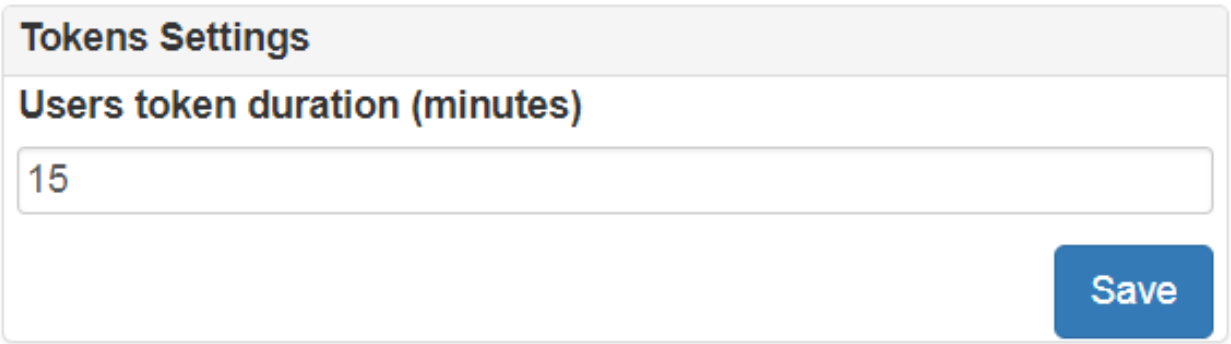
- all nodes must use external database engine
- all nodes must have same private key at keystore with alias “jetty”
- all nodes must use theirs own certificates generated by CA and certificate of CA must be imported to keystore
- load balancer must inject X-Forwarded-For header with valid source IP address



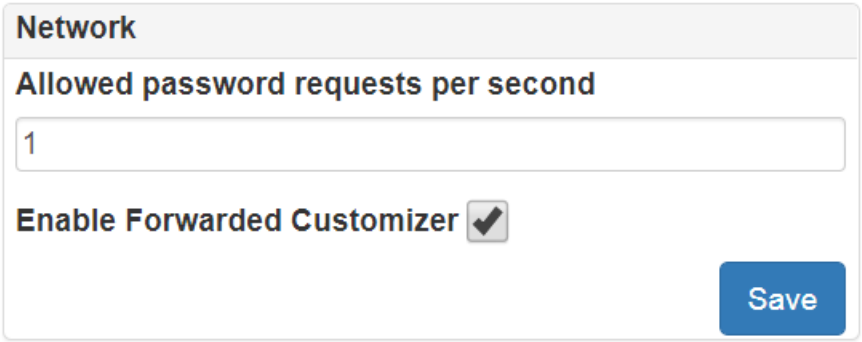
4.11 Extra settings

Go **Administration->Communications->Extra** and configure:

- User access token duration (maximum time of users inactivity)



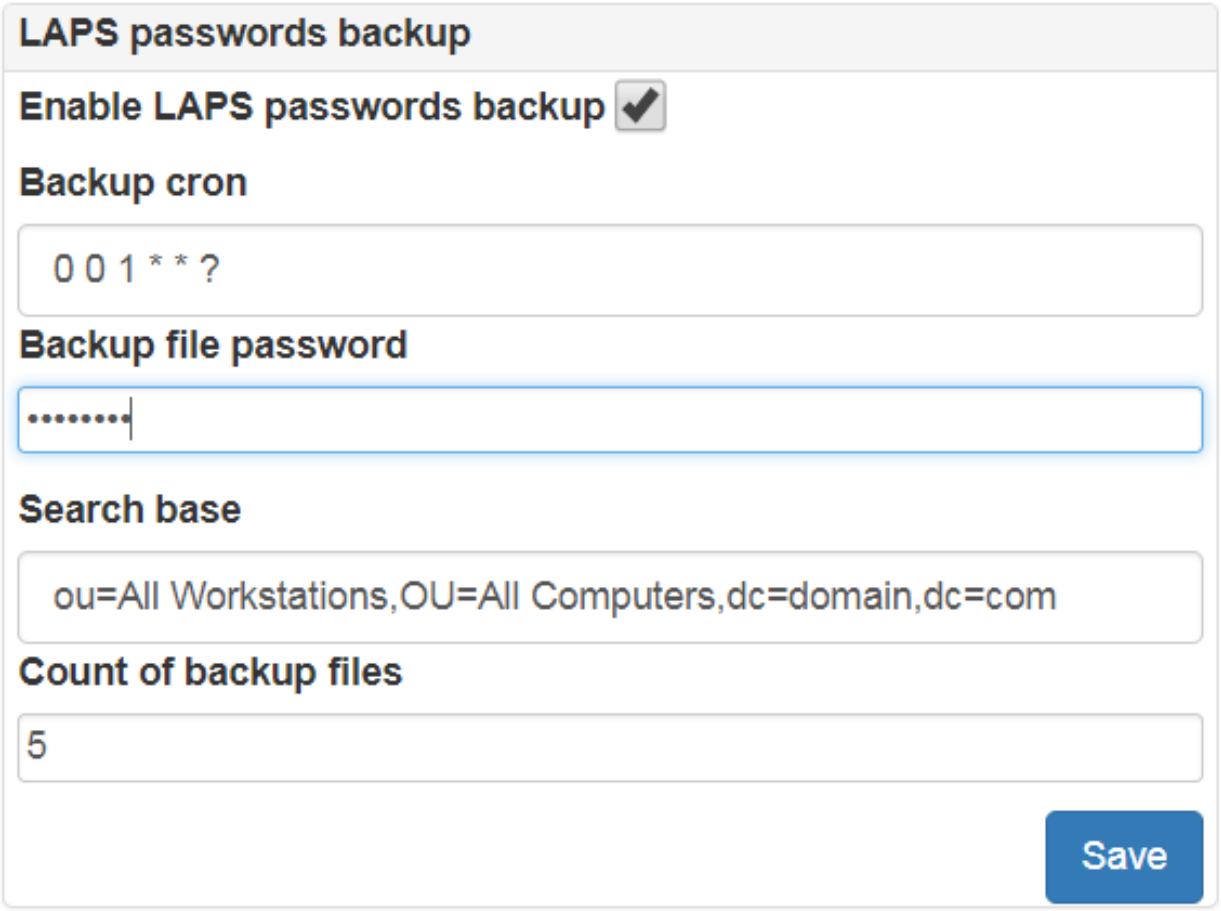
- Some sensitive API are protected by internal DoS filter. You can restrict maximum number of requests per second to this sensitive API related to authentication, password accessing
- Forwarded customizer is used to extract source IP address from X-Forwarded-For header which contains information of client IP address if LAPS Portal located behind a reverse proxy or a load balancer.



Backup passwords managed by LAPS

At **Administration->System->Laps Backup** you can configure automatic backup of passwords managed by LAPS. You can use saved passwords in case of AD unavailability. You can configure:

- ron exporession
- password which will be used to encrypt ZIP archive with computers passwords
- base DN of computers
- maximum count of archive files



CHAPTER 5

LAPS Portal maintenance

5.1 LAPS Portal restarting

To restart LAPS portal you can use:

- on unix systems:

```
service laps restart
```

- on windows systems:

```
open services.msc and restart laps service
```

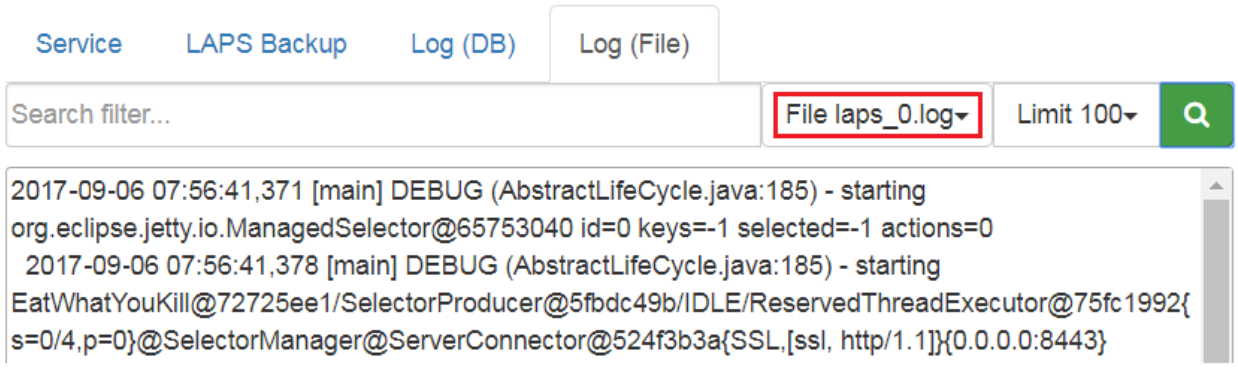
- via LAPS Portal GUI. Go to **Administration -> System -> Service** and press "Restart" button

5.2 Log files

LAPS portal creates following log files:

- logs/laps*.log
- logs/wrapper.log

You can view logs of LAPS Portal in **Administration -> System ->Log(File)**, select log file and press "Search" button



5.3 engine.conf file

File conf/engine.conf is JSON file which contains basic configuration options

Option	Value type	Description
basepath	string	path to directory where LAPS portal is located. This parameter is automatically filled by LAPS Portal itself
init_completed	boolean	flag which is set to true after first launching when default settings are configured
sslport	int	port used by LAPS Portal to serve TLS connection
key-store_pass	string	password for java ket storage file
jetty_cert_alias	string	alias of certificate which will be used by TLS engine
jdbc_driver	string	jdbc driver wor database management system used by LASP Portal
db_host	string	databse host
db_port	int	databse port
db	string	database name
db_username	string	database user
db_password	string	database password

5.4 LAPS Portal backup

To restore LAPS portal you should backup following files:

- conf/engine.conf (in case you modified default network port)
- conf/confdb.db – internal sqlite database which contains settings and event logs
- conf/license.txt - license activation file
- keystore/keystore.jks – certificate store
- backups/laps/* - backup files with passwords of computers managed by LAPS
- wrapper/conf/wrapper.conf – service/daemon configuration
- bin/log4j.properties – log level properties

5.5 Admin password reset

If you forget admin password you can reset it in following way:

- **on windows systems::** wrapper/bat runConsole.bat resetpass
- **on unix systems::** wrapper/sh ./runConsole.sh resetpass

5.6 Errors

5.6.1 AcceptSecurityContext

AcceptSecurityContext error can appear during establishing connection to ActiveDirectory:

```
[LDAP: error code 49 - 80090308: LdapErr: DSID-0C0903A9, comment:␣
↪AcceptSecurityContext error, data 52e, v1db1
```

For error code 49 reason of error shown in data field

data field code	description
525	User not found
52e	Wrong password
530	not allowed to login at this time
531	no access right to login to this computer
532	password expired
533	user account disabled
701	user account expired
773	password reset is required
775	user account is locked

5.6.2 SSLHandshakeException

javax.naming.CommunicationException javax.net.ssl.SSLHandshakeException indicates that LAPS Portal could not validate certificate chain during SSL/TLS hadshake. In case of following errors:

```
javax.naming.CommunicationException: simple bind failed: server.local:636 [Root␣
↪exception is javax.net.ssl.SSLHandshakeException: sun.security.validator.
↪ValidatorException: PKIX path building failed: sun.security.provider.certpath.
↪SunCertPathBuilderException: unable to find valid certification path to requested␣
↪target]
```

You should check whether all certificate chain imported into LAPS Portal. After importing certificates do not forget to restart LAPS Portal service.

In case this error appears during communication with AD Controllers you should also check how many certificates domain controller has with Server Authentication purpose. In normal situation AD Controller should have one personal certificate with Server Authentication purposes . According to https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx *"You should be planning on having only one certificate on each LDAP server (i.e. domain controller or AD LDS computer) with the purpose of Server Authentication. If you have legitimate reasons for using more than one, you may end up having certificate selection issues, which is discussed further in the Active Directory Domain Services Certificate Storage.* As workaround import all certificates with Server Authentication purposes to LAPS Portal

CHAPTER 6

LAPS Portal mobile application

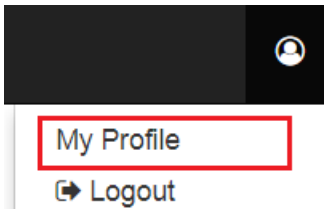
LAPS Portal has mobile clients which works under Android and iOS devices. Main features of LAPS mobile client:

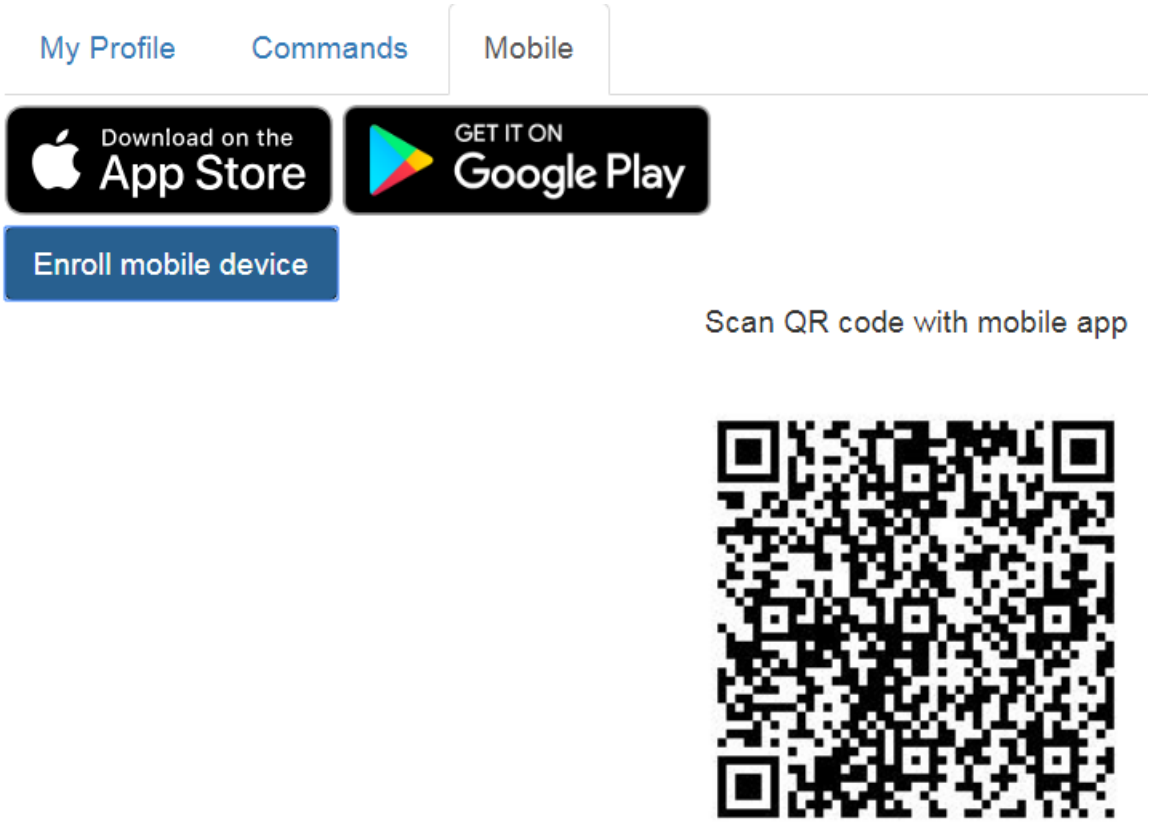
- secure access to passwords managed by MS LAPS: in addition to TLS encryption all passwords are additionally encrypted with AES algorithm with unique device key per user. This device key is generated during device enrollment process and stored in secure way at mobile device. On iOS key is stored directly in the KeyChain. On Android key itself is encrypted with random 256-bit AES master key which is encrypted with a device-generated RSA (RSA/ECB/PKCS1Padding) from the Android KeyStore. The combination of the encrypted RSA(AES(master key)) and AES(device key) are stored in SharedPreferences.
- PIN protection. If device has fingerprint scanner it will be automatically used by application
- ability to get LAPS passwords in a convenient and secure way using mobile device
- ability to setup password new expiration date
- login to LAPS Portal with help of confirmation of push notification

6.1 LAPS mobile application enrollment

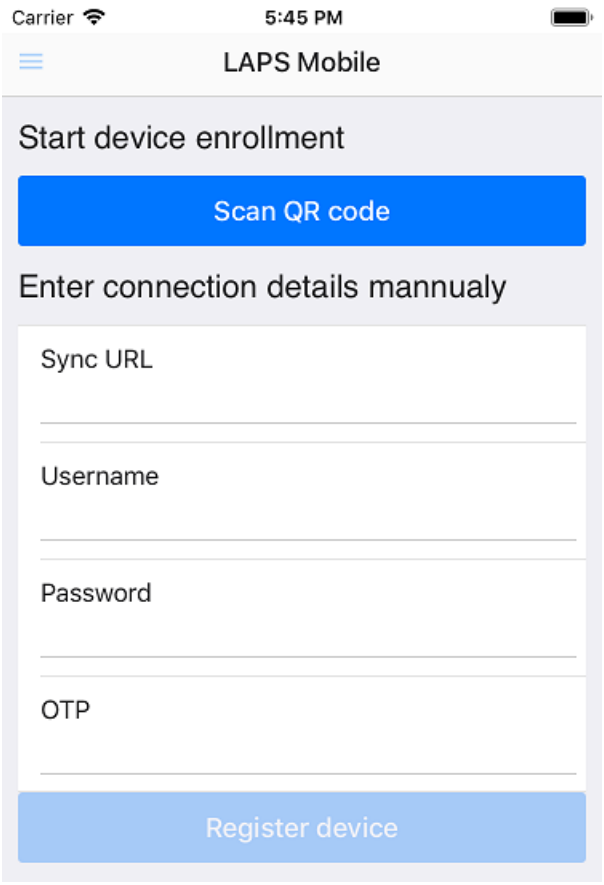
There are two way how to start use LAPS mobile application

1. Go to **Profile settings -> Mobile**, press “Enroll mobile device” and scan generated QR code at mobile device



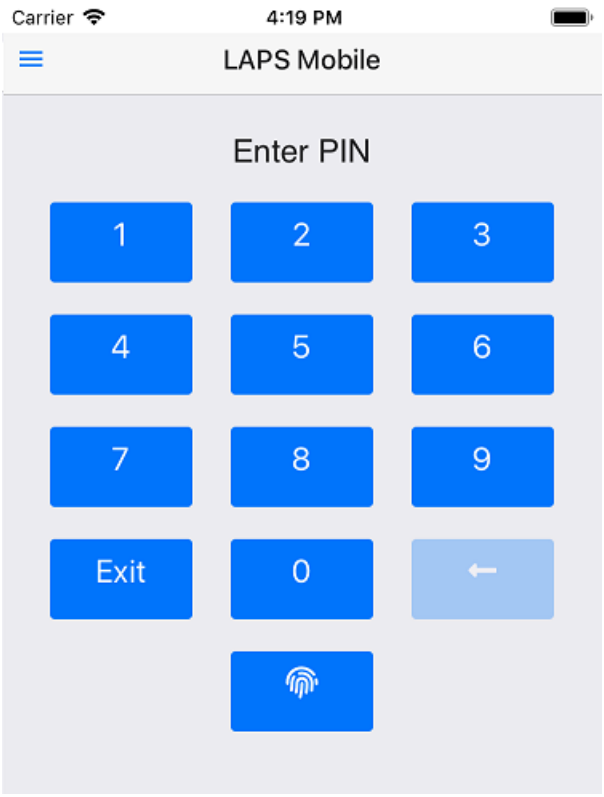


2. Enter External Portal URL configured at **Administration->Communications->Mobile** to mobile device URL field, fill username, password and OTP

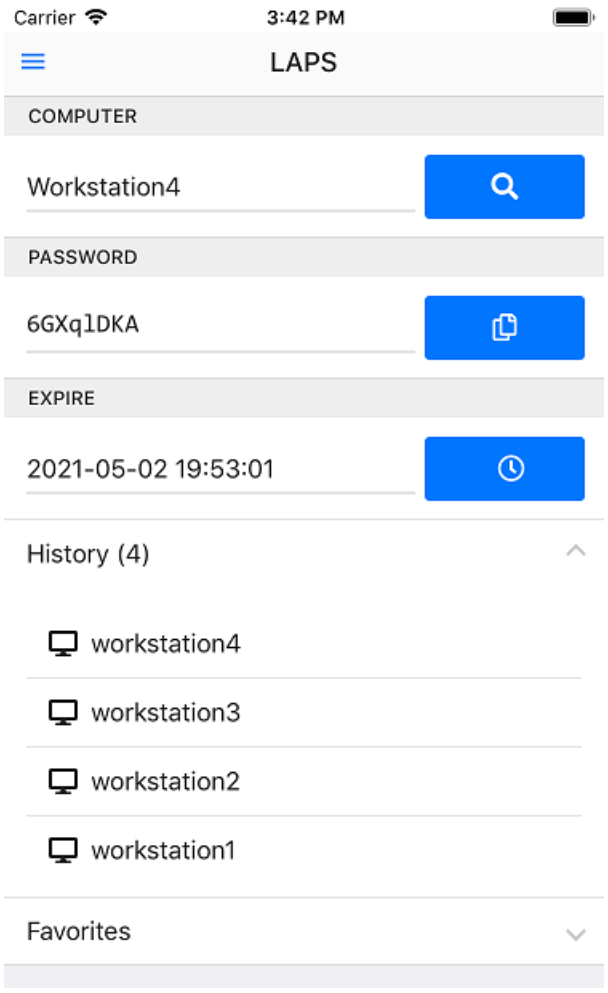


6.2 LAPS mobile application usage

1. Enter PIN or use your fingerprint to login to LAPS Mobile



1. Enter computer name and press find button


Carrier
3:42 PM
LAPS
COMPUTER
Workstation4
PASSWORD
6GXqlDKA
EXPIRE
2021-05-02 19:53:01
History (4)
workstation4
workstation3
workstation2
workstation1
Favorites