
WebLAPS Documentation

weblaps.pro

Aug 16, 2020

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
1.4	Just-in-time administration (JITA)	5
2	LAPS Portal mobile application	7
2.1	LAPS mobile application enrollment	7
2.2	LAPS mobile application usage	9
3	WebLAPS agent	13
3.1	WebLAPS agent installation	13
3.2	WebLAPS agent policy	14
3.3	WebLAPS agent access management	15
4	Installation Prerequisites	17
5	Installation in Unix	19
6	Installation in Windows	21
7	LAPS Portal administration	23
7.1	Accessing admin console	23
7.2	Active Directory integration	24
7.3	Certificates	26
7.4	Access rights for LAPS	26
7.5	JITA Roles	27
7.6	Authentication setup	28
7.7	LAPS passwords expiration	31
7.8	LAPS Portal API and tokens	32
7.9	LAPS Portal and SIEM integration	33
7.10	LAPS Portal mobile app settings	34
7.11	LAPS Portal high availability mode	35
7.12	LAPS.E, AdmPwd.E password encryption	36
7.13	Extra settings	37
8	LAPS Portal maintenance	39

8.1	LAPS Portal restarting	39
8.2	Log files	39
8.3	engine.conf file	40
8.4	LAPS Portal backup	40
8.5	Admin password reset	41
8.6	Errors	41
8.6.1	AcceptSecurityContext	41
8.6.2	SSLHandshakeException	41
8.6.3	SocketException	42
8.6.4	Unable to start service	42

WebLAPS is a web application which helps to secure windows environment with MS LAPS solution implemented. MS LAPS is effective tool 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.

WebLAPS could be used to implement just-in-time administration (JITA) approach recommended by MS when accounts of system administrators are added to privileged groups for defined period of time and automatically removed after.

WebLAPS has an agent which could be used to manage local user accounts at non domain joined computers. It also can automatically create managed user, rotate its password and control membership in defined groups.

WebLAPS 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.

WebLAPS 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.

WebLAPS 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 implemented. Currently following 2fa connectors implemented:

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

Security controls implemented in WebLAPS

- 2FA or OTP only authentication
- password encryption by LAPS.E or AdmPwd.E supported
- customizable captcha 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 access to passwords managed by LAPS. It is possible to export LAPS logs in CEF format to external system via syslog

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 or IP address. If you use IP address LAPS portal do reverse DNS lookup to determine computer name

The screenshot shows the LAPS Portal interface with a dark header bar containing the 'LAPS' logo and navigation links: 'Search' (with a magnifying glass icon), 'Logs' (with a list icon), and 'Administration' (with a gear icon). Below the header, the interface is divided into sections for inputting search criteria:

- IP**: A text input field with a blue search button (magnifying glass icon) to its right.
- Computer**: A text input field containing 'workstation-12' with a blue search button (magnifying glass icon) to its right.
- Password**: A text input field containing 'ds12DSFoKs12%' with a blue button (copy icon) to its right.
- Expire**: A text input field containing '2018-07-30 11:00:37'.
- New expiration time**: A date and time picker showing '2018-07-24' with a calendar icon, followed by time fields for hours ('0'), minutes ('0'), and seconds ('0'). A blue 'Set' button is to the right.

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 tool you can use following pattern:

```
"c:\program Files\DameWare Mini Remote Control 11.0 x64\dwrc.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

LAPS

Search

Logs

Administration

Logs

Search filter...

Timestamp	Category	Type	Source IP	User	Computer	Details
2018-03-13 11:21:01 (+03:00)	laps	PASSWORD_ACCESS	192.168.1.112	john	workstation-1	
2018-03-13 11:36:15 (+03:00)	laps	PASSWORD_ACCESS_FAIL	192.168.1.115	veronica	undefined	Computer undefined not found
2018-03-13 11:43:23 (+03:00)	laps	PASSWORD_ACCESS	192.168.1.117	mathias	workstation-vip127	
2018-03-13 11:43:36 (+03:00)	laps	PASSWORD_ACCESS	192.168.1.117	mathias	workstation-vip15	
2018-03-13 11:45:19 (+03:00)	laps	PASSWORD_ACCESS	192.168.1.10	robin	workstation-13	

Last 1 year

2017-07-01

15

39

30

2018-07-01

15

39

30

Category

laps

Type

Source IP

User

Computer

Search

1.4 Just-in-time administration (JITA)

Just-in-time administration (JITA) is an approach for minimizing the privileged account attack vector in a security strategy, combined with a precise definition of assigned authorizations. Every time an eligible users needs to perform a task which requires membership in privileged groups, they enable such membership for defined period of time. The membership expire after a specified time period, so that a malicious user can't steal the access.

After successfully login you can see JITA roles available at "JITA" part of portal.

My roles

Search filter...

Role	Description	Action
vmware		<div></div> <div></div>

At "My roles" panel you can start, stop or extend active JITA session. At start session dialog it is needed to set duration which should be less than maximum allowed TTL defined in role's configuration and justification describing a reason.

Start session vmware ×

Duration

↑

01

:

↑

00

:

↑

00

↓

↓

↓

Active till

Sun Aug 04 2019 17:24:02

Justification

Create new virtual server

Start

Cancel

Active JITA sessions of authenticated user are shown at “My active sessions” pannel. It is possible to stop or prolong active JITA session.

My active sessions ↻			
Search filter...			
Role	Started	Expiration	Action
vmware	2019-08-04 16:26:33	2019-08-04 16:27:31 <div></div>	<div>↻</div> <div>■</div>

LAPS Portal mobile application

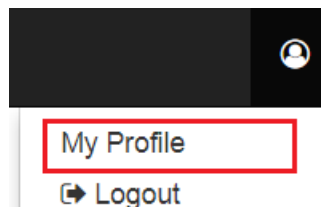
LAPS Portal has mobile client which works under [Android](#) and [iOS](#) devices. Main features of LAPS mobile client:

- 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



2.1 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




[My Profile](#) [Commands](#) [Mobile](#)



[Enroll mobile device](#)

Scan QR code with mobile app

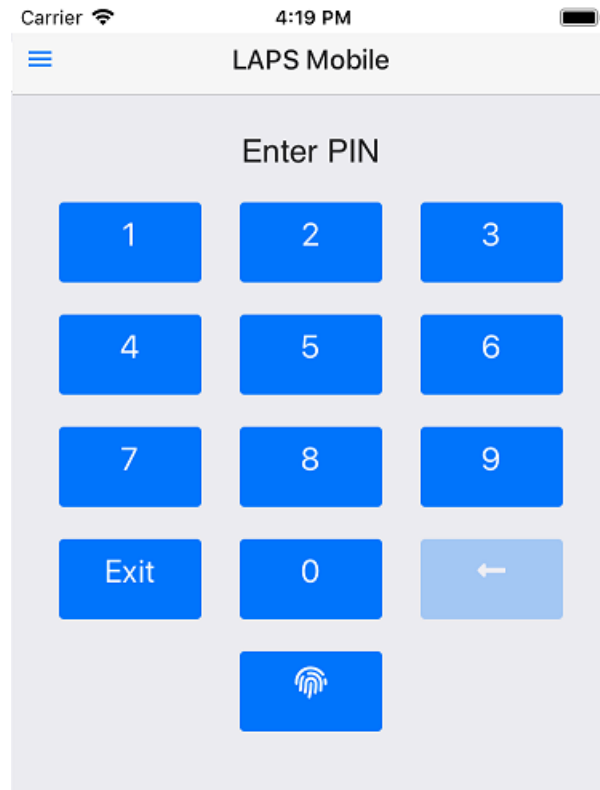


2. Enter External Portal URL configured at **Administration->Communications->Mobile** to mobile device URL field, fill username, password and OTP



The screenshot shows the LAPS Mobile application interface on a mobile device. At the top, the status bar displays 'Carrier', signal strength, '5:45 PM', and battery level. The app header is 'LAPS Mobile' with a menu icon on the left. The main content area is titled 'Start device enrollment' and contains two options: 'Scan QR code' (a blue button) and 'Enter connection details manually' (a light gray button). Below 'Enter connection details manually' is a form with four input fields: 'Sync URL', 'Username', 'Password', and 'OTP'. At the bottom of the form is a light blue button labeled 'Register device'.


2.2 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


6GXq1DKA 


EXPIRE


2021-05-02 19:53:01 


History (4) 

 workstation4

 workstation3

 workstation2

 workstation1

Favorites 

WebLAPS agent

WebLAPS agent is used to manage passwords of local users and control membership in local groups. It could be run on joined or non domain joined computers.

3.1 WebLAPS agent installation

Before you begin make sure that MS .NET Framework 4.5.1 is installed.

You can install WebLAPS agent using command line:

```
msiexec /i WebLAPSInstaller.msi /quiet /norestart SERVERURL=<serverurl> JOINKEY=<joinkey>
```

Parameter	Example	Description
SERVERURL	weblapspublic. host;https:// weblapsprivate. host	WebLAPS server URL. You can set multiple URLs delimited with “;” in case if you want to perform password rotation on remote computers outside of corporate network. WebLAPS agent will try to select first available server. If you use reversproxy you can publish URLs used by agent with mask /api/computers/remote/* so no other functionality will be available from internet.
JOINKEY	key- SECRETkey1	key validated once by WebLAPS during initial connection.
NOSSLCHECK		disable server certificate validation
GROUPID	6b2b6- ab66- 4592-be0a- 2dfcf317e58	You can manually set computer container ID which will be used by agent to get policy otherwise distribution rules will be used to determine container

3.2 WebLAPS agent policy

Go to **Administration -> Computers -> Policies** and select computer container, next press “Add new” button. You can configure multiple policies which will be applied to the same computer container. Policies are inherited from all parent containers.

The screenshot shows a web-based configuration form for a WebLAPS agent policy. The form is organized into several sections, each with a label and a corresponding input field or checkbox. The fields are as follows:

- Policy name:** A text input field containing "defaultAdministrator".
- Computer container:** A dropdown menu with "All computers" selected.
- Login:** A text input field containing "Administrator".
- Create user if not exists:** A checkbox that is checked.
- Manage password:** A checkbox that is checked.
- Group:** A text input field containing "Administrators".
- Allowed users in the group:** A text input field containing "DOMAIN\inventory;localadmin".
- Remove other users from the group:** A checkbox that is checked.
- Password age (hours):** A text input field containing "1".
- Password length:** A text input field containing "8".
- Require upper case:** A checkbox that is checked.
- Require numbers:** A checkbox that is checked.
- Require special symbols:** A checkbox that is checked.

At the bottom right of the form, there are two buttons: "Save" (in blue) and "Cancel" (in grey).

WebLAPS agent policy is applied to specified *local* user account. WebLAPS agent can automatically create managed user if it is not exists. For automatic password rotation please select **Manage password** checkbox and set “Password age”. You can automatically remove all users from defined group except approved. You can specify multiple approved users delimited with “;”. For domain user use following format: domain\login.

To view result settings for a container go to **Administration -> Computers -> Container Details** and select a computer container.

All computers/Russia

ID: bc96b2b6-ab66-4592-be0a-2dfcf317e58

Access groups:
No access groups

Agent policy:

Login: *msk-admin*

☒ create user if not exists ☒ manage password

☒ Remove users from group *group1* except *msk-admin* and *user1, user2*

Password age (hours): 2 length: 6 ☒ upper case ☒ numbers ☒ special symbols

Login: *Administrator*

☒ create user if not exists ☒ manage password

☒ Remove users from group *Administrators* except *Administrator* and *DOMAINinventory*

Password age (hours): 1 length: 8 ☒ upper case ☒ numbers ☒ special symbols

Login: *User*

☒ create user if not exists ☒ manage password

☒ Remove users from group *Users* except *User*

Password age (hours): 1 length: 8 ☒ upper case ☒ numbers ☒ special symbols

Login: *testUser*

☐ create user if not exists ☒ manage password

Password age (hours): 1 length: 8 ☒ upper case ☒ numbers ☒ special symbols

Distribution rules:
Rule type: name value: msk-.+

3.3 WebLAPS agent access management

Go to **Administration->Computers -> Access Groups** and setup user group to computer container mappings. You must use distinguished names of groups. Members of group will be able to get passwords managed by WebLAPS agent in the container and sub containers. If you have multiple policies for several managed users per one container you can additionally restrict managed .users to which passwords you provide access by filling **Allow access only to following subjects** parameter.

Edit ×

Computer container

Name

Users group (DN)

Allow access only to following subjects

Additionally you can provide access only for particular computer to an user or a group (group nesting is not supported) by editing computer object. This mechanism does not connected with access control subsystem based on groups and containers

Computer DELHI_PC properties ×

Managed by

Installation Prerequisites

Prior to installing the WebLAPS, the following requirements must be met:

1. Install Java JRE or JDK version 1.8
2. Check that java executable is on your system PATH. Following command must return no errors

`java -version`

if any error occurred please fix your Java installation <https://www.java.com/en/download/help/path.xml>

1. Make sure that network connection is open to port 636 (LDAPS) from weblaps host to domain controllers
2. Make sure that your LDAPS is configured at your domain controllers. LAPS stores passwords in special confidential attribute which is accessible only via secured connection. <https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx>
3. Prepare service user in AD and grant it permissions to read and reset passwords.
4. Export certificate of CA which signed certificate for LDAPS
5. import CA certificate at mobile devices if you want to use LAPS mobile app and you use your own CA to issue certificate for WebLAPS server.

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=rx,g=rx,o-rwx /opt/laps
chmod u+w /opt/laps/wrapper/tmp
chmod u+w /opt/laps/logs
chmod u+w /opt/laps/conf
chmod u+w /opt/laps/keystore
```

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

```
wrapper.java.command = path_to_java_executable
```

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

```
/opt/laps/wrapper/sh/installDaemon.sh
systemctl daemon-reload
```

7. Run the service:

```
service laps start
```

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

CHAPTER 6

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
```

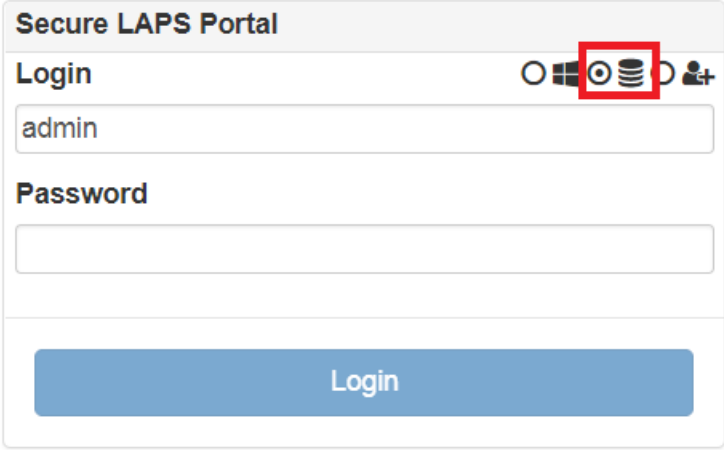
7. If you have your own license file copy it to C:\laps_conf\license.txt. Default distribution includes a community license file.
8. Run the service:

```
net start laps
```

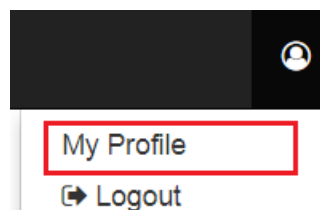
9. Open in browser <https://host:8443>

7.1 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



7.2 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

LDAP Server Settings

Bind user DN

CN=lapsuser,OU=All Users,DC=domain,DC=com

Bind user password

LDAP host

host1.domain.com;host2.domain.com

Users search base

DC=domain,DC=com

Computers search base

OU=All Computers,DC=domain,DC=com

Login filter

(&(samAccountName=%s)(objectClass=user))

Groups search base

OU=Groups,DC=domain,DC=com

PC admin attribute

computerAdmin

You can enable scheduled password rotation for bind user

LDAP Jobs

Enable master password rotation ☐

Password rotation cron

Clean removed users cron

Save

7.3 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

7.4 Access rights for LAPS

Go to **Administration->Security->LAPS 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.

Add new
×

Name

Group (DN)

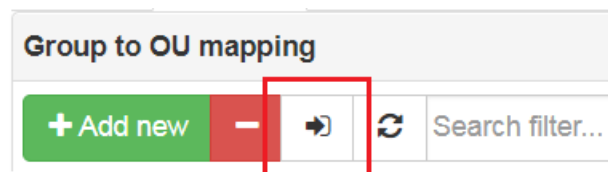
OU

Add Cancel

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



7.5 JITA Roles

Just in time administration (JITA) module activates privileged roles (membership in defined AD groups) to authorized user for finite amount of time. With such approach accounts of system administrators will be added to privileged groups or set of groups only after 2FA verification during portal login.

JITA roles are configured at **Administration->Security->LAPS Groups**. Each JITA role consist of role name, short description, role group distinguished name which is used to provide access to the role, role membership maximum TTL after which user account will be automatically removed from privileged groups and set of privileged groups.

Edit ×

Role name

Role description


Role group DN


Role membership maximum TTL (seconds)

Privileged groups DN

+

Privileged group

 cn=vmware-adm,ou=groups,dc=example,dc=com

 cn=vmware_distribs,ou=groups,dc=example,dc=com

Save

Cancel

7.6 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 validation URL

Lin OTP Settings**LinOTP validate URL****Save**

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

Radius Settings**Host****Shared secret****Auth type** **Challenge-Response mode** ☐**Save**

- fortiauth provider for integration with FortiAuthenticator

FortiAuthenticator Settings**FortiAuthenticator auth API URL****Api user****Api key****Save**

- duo provider for integration with Duo

DUO Settings

API hostname ★

Integration key ★

Secret key ★

Check TLS certificate ☒

Use proxy ☐

Save

- 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 be unable to login during defined period of time

Authentication settings

Require password check for LDAP users ☐

Require password check for internal users ☒

Require OTP for external users ☒

Require OTP for internal users ☐

External authentication type

fortiauth ▼
linotp
fortiauth
radius
totp

Require captcha after fail login ☐

Captcha alphabet
ABFGKMNPRSTXYZ235689

Captcha length
4

Account lockout threshold
5

Account lockout duration (sec)
60

Save

7.7 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 modifying of ms-Mcs-AdmPwdExpirationTime attribute on all configured domain controllers. Optionally you can add timeout between attempts to get passwords. This timeout will prevent from retrieving passwords in fast way. This timeout is not used for API access via tokens described below.

Extra settings

Expire LAPS password after access (min)

Max allowed expire difference (min)

Return extra attributes for PC (comma separated)

Push password expiration update to all DC ☐

Timeout between access to passwords (sec)

Save

7.8 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

Edit

✕

Name

token

Remote IP

192.168.56.1

OU

OU=All Workstations,OU=All Computers,DC=domain,DC=com

API token

Save

Cancel

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
```

7.9 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.

Syslog Settings

Syslog server

Syslog port

Enable ☒

Save

7.10 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

Mobile features settings

Enable mobile application ☒

Sync mode webhook ▾

Sync URL for mobile app

External Portal URL

Organization name for mobile features

Password for mobile features

Use proxy for mobile features ☐

Allowed clock difference (sec)

Push authentication confirmation timeout (sec)

Save

7.11 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

Cluster Settings

Enable cluster mode ☒

WebLAPS nodes

https://node1.domain.com:8443;https://node2.domain.com:8443

Cluster sync cron

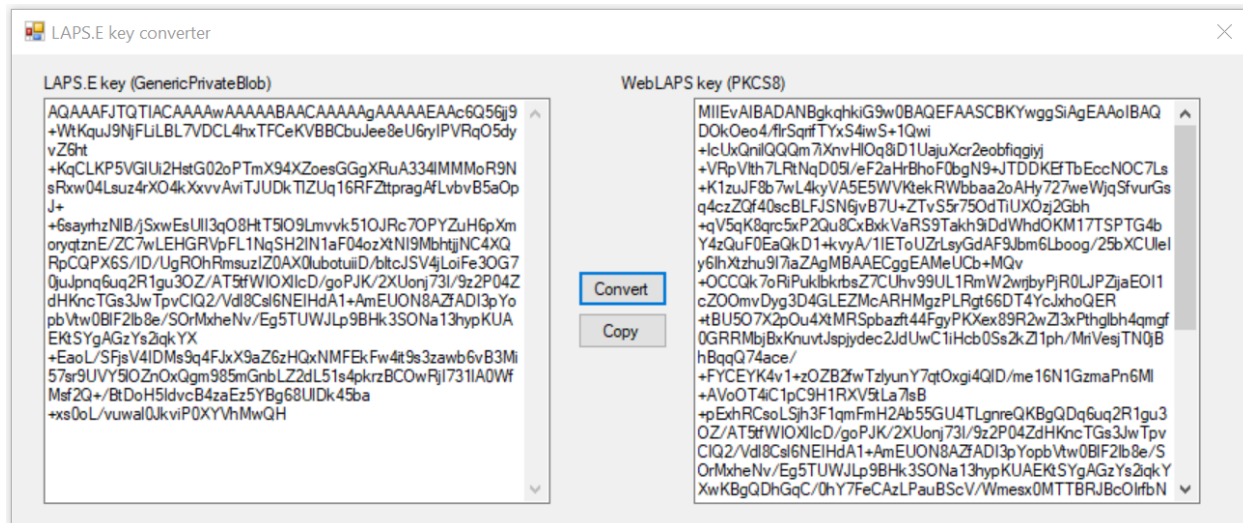
0 0/5 * * * ?

Check

Save

7.12 LAPS.E, AdmPwd.E password encryption

If you use password encryption with help of LAPS.E or AdmPwd.E it is needed to import private keys. It is needed to convert every private key usually located at c:\Program Files\AdmPwdSrc\CryptoKeyStorage or c:\Program Files\AdmPwd\PDs\CryptoKeyStorage from GenericPrivateBlob to PKCS#8 format with help of [KeyConverter](#) utility.



Next import converted private keys at **Administration->Security->Extra** and activate **Decrypt encrypted passwords (laps.e, AdmPwd.E)** checkbox.

Add new ×

Name

Private Key 1

Key ID

1

Key

```
8zktZqilP1bueWI58jSq9IL2DIZa875CTdYmme4p+pdKwnB7AhRDBXyBc9dC8bH4XANOGHEn2SGRSM0
R5NjpxKLLGjp+iglyLmAx/+PgIbfS7Z5YhAASbWD7leY2xTvp6HZZTzXu6xjU1bKø/LM3Wy/NMD1AHb2uSN
8eTyfLuRI0Rjlr90H/B3oahVA1vjWmRcMT+KkrrmcfsqoAPqHY/a8Uc+N82SZIblqcWRLQHzMQWcFWcjU
V/BdGhTmr4My75LzDjDVKZQDFLPMR5xS6E7FmmfJl//MR2fKD5J/nStZ+6Wxzeudnhz/Y212zr+08lskk5
XIsIC/o6SFeYKjiVoidNCaUzho14lpLoi+tUJKfZPKszrw
```

Add

Cancel

Warning: It is important to set right Key ID which is equals to a number at the beginning of private key's file name. For a file 1_Key.dat or 1_PrivateKey.dat Key ID is 1.

7.13 Extra settings

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

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

Tokens Settings

Users token duration (minutes)

15

Save

- 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.

Network

Allowed password requests per second

Enable Forwarded Customizer ☒

Save

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:

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

LAPS passwords backup

Enable LAPS passwords backup ☒

Backup cron

Backup file password

Search base

Count of backup files

Save

LAPS Portal maintenance

8.1 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
```

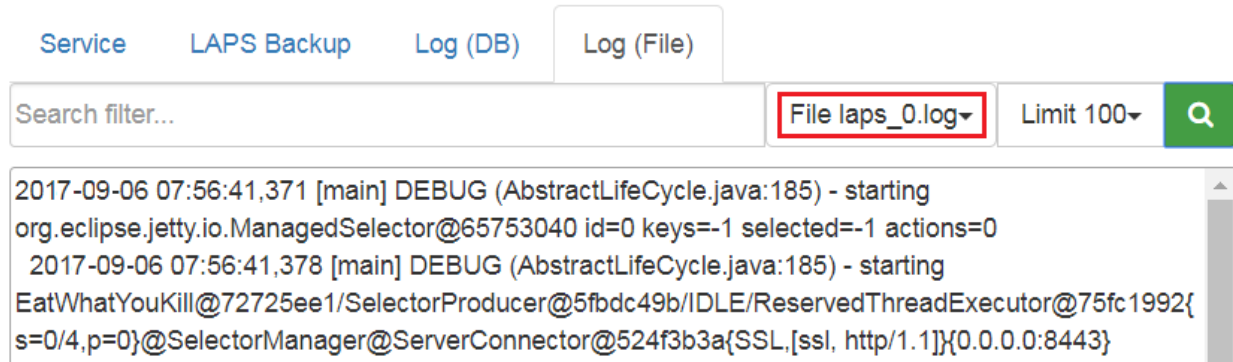
- via LAPS Portal GUI. Go to **Administration -> System -> Service** and press “Restart” button

8.2 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



8.3 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

8.4 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

8.5 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

8.6 Errors

8.6.1 AcceptSecurityContext

AcceptSecurityContext error can appear during establishing connection to ActiveDirectory:

```
[LDAP: error code 49 - 80090308: LdapErr: DSID-0C0903A9, comment:↵
↵AcceptSecurityContext error, data 52e, vldb1
```

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

8.6.2 SSLHandshakeException

javax.naming.CommunicationException javax.net.ssl.SSLHandshakeException indicates that LAPS Portal could not validate certificate chain during SSL/TLS handshake. 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

8.6.3 SocketException

java.net.SocketException indicates that there is LAPS Portal unable to establish TCP connection to domain controller. It could be caused by local or network firewall, problems in DNS resolution or that LDAPS is not configured on domain controller. In case of following error

```
Error connecting to LDAP javax.naming.CommunicationException: ad.domain.com:636 [Root exception is java.net.SocketException: Connection reset]
```

please check that you can connect on port 636 from host where WebLAPS is installed to domain controller. You can do it with telnet command:

```
telnet domain.controller.host 636
```

where domain.controller.host is a domain controller FQDN. Please check following article to be sure that LDAP over SSL is properly configured at your domain controller <https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx>

8.6.4 Unable to start service

WebLAPS service crashes, log/wrapper.log contains following lines:

```
INFO[wrapper]Service laps|20-05-21 17:58:41|could not start process 57 INFO[wrapper]Service laps|20-05-21 17:58:41|The parameter is incorrect. INFO[wrapper]Service laps|20-05-21 17:58:41|null/null/null SEVERE[wrapper]Service laps|20-05-21 17:58:41|failed to spawn wrapped process
```

Please check that java.exe file is on system path. In case if there are more than one JRE edit wrapperconfwrapper.conf, find following line

```
wrapper.java.command = ${ if (“${os.name}”.toLowerCase().startsWith(“windows”)) “java.exe”; else “java” }
```

and comment it with ‘#’. Next set wrapper.java.command to right path to java.exe file like this (replace with correct path to java.exe)

```
wrapper.java.command = c:/Program Files/Java/jre1.8.0_251/bin/java.exe
```