CYPHER.DOG®

Cypherdog Security Inc.
2040 Martin Ave.,
Santa Clara, CA 95050, USA

CE Business installation manual

Document version 3.0, 2024-03-07

Introduction

Cypherdog Encryption Business is built to guarantee secure transfer of data for corporate clients. The additional purpose of the Business edition is to allow license owners to manage the private keys of their users using their own infrastructure and use command line functions for bulk encryption and decryption operations.

Note: For simplified one page installation manual of Cypherdog Encryption Business please review last Appendix page.

Cypherdog Encryption Business is supporting the following use cases:

- Employee side:
  - Secure communication of the employees inside company and with external recipients using e-mail and other communication channels like MMS, drive file transfers, chat, etc.
  - Simple Command Line encryption/decryption activities to support work automation.
- Developer/Application side:
  - Command Line functionality for mass batch processes execution.
- Administrator side:
  - User's desktops reinstall / private key lost – for restore activities,
  - Decryption of the outgoing and incoming encrypted user communication on the corporate gateway level.

The installation process of the CE Business takes four steps:

1. Setting up backend services required to store and restore user's private keys.
2. Setting up CE Admin Panel to manage licence and user accounts.
3. Setting up services required for Command Line usage.
4. Setting up CE Business a GUI application and plugins for end users (employees).

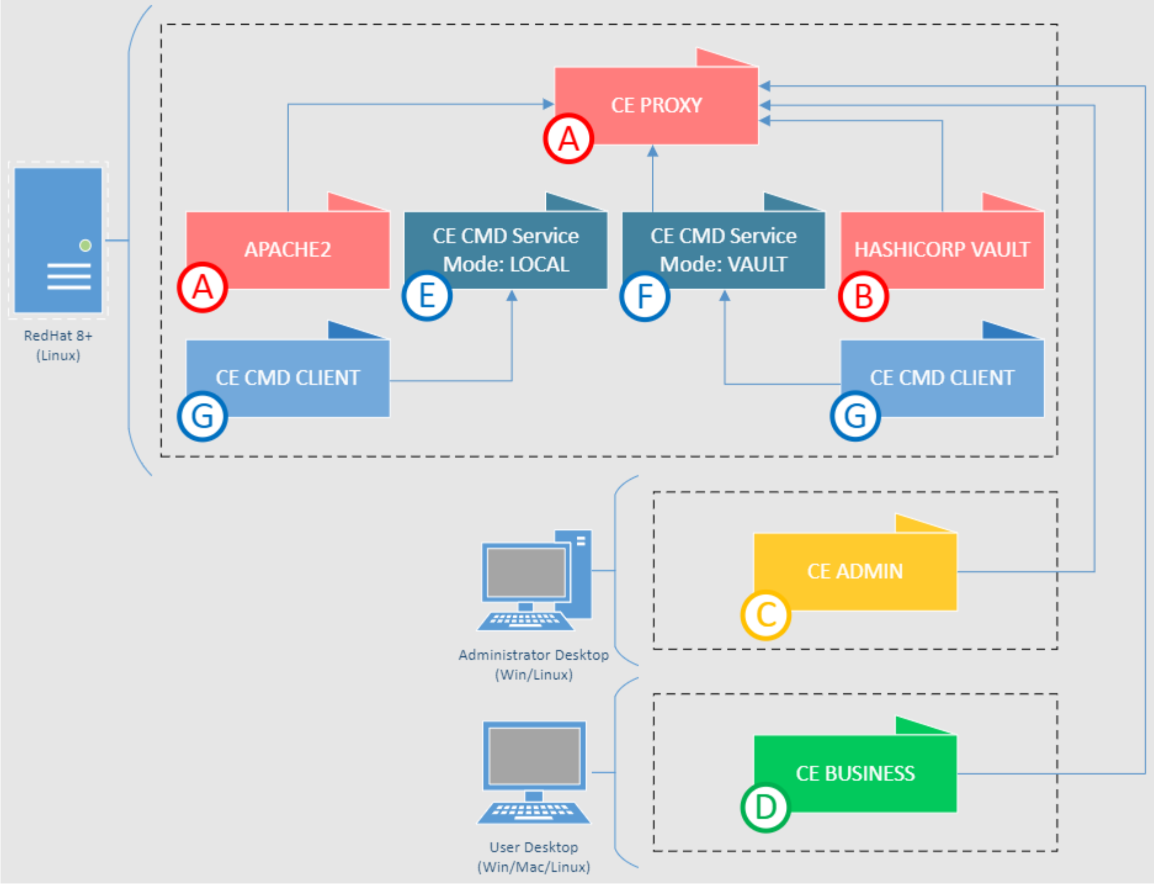
To fully use all system capabilities the following system components must be installed:

- Backend:
  - **CE Business Proxy**
  - **CE Business CMD Service**
  - **CE Business CMD Client**
  - **HashiCorp Vault**
- Administrator desktop:
  - **CE Business Admin (GUI app)**
- User Desktops:
  - **CE Business Application (GUI app)**

The system components can be installed in multiple configurations depending on the client requirements. The following section describes in what variants system components can be installed.

System components deployment variants

System components include services developed by Cypherdog Security Inc as well as other components delivered by other companies and operating systems. Thise services can be installed in variants depending on a client requirement, e.g., only support for GUI clients or only support for command line functions.



The schema above present six deployment groups. This manual describes deployment of those groups on three machines:

- Backend components: A + B + E + F + G (deployed on a single RedHat VM)
- Frontend component: C (deployed on an administrator’s desktop).
- Frontend component: D (deployed on user’s desktop).

If required clients can deploy system backend components (A + B + E + F + G) on separate machines.

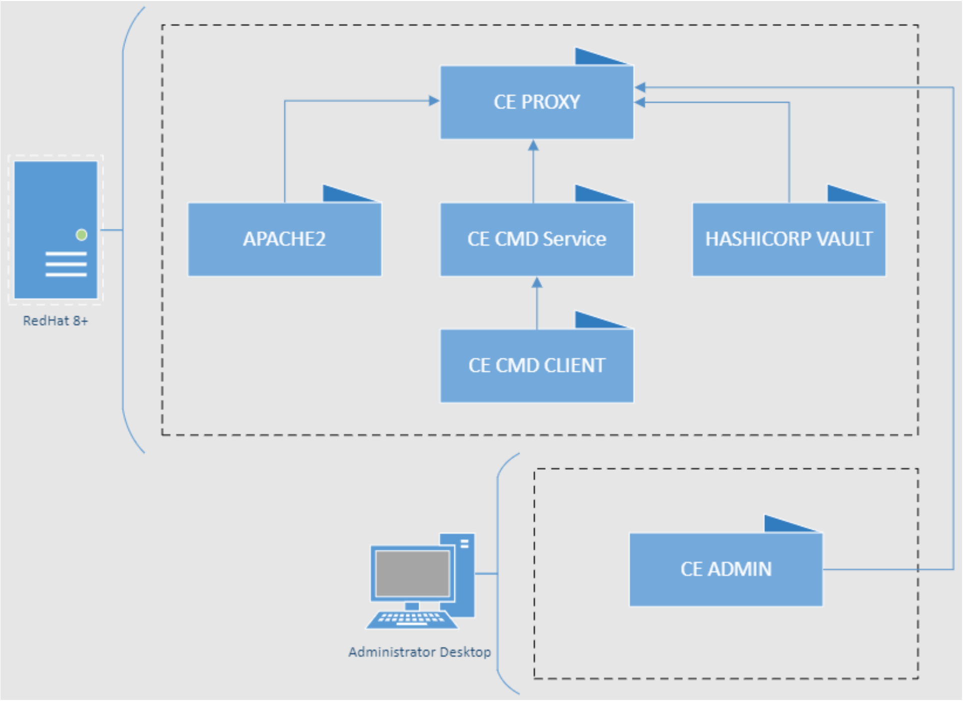
Deployment Group	Component Name	Component Purpose	Supported OS
A	CE Proxy	Supporting interconnection between system components	RedHat 8+
A	Apache2	Serving web content of CE Proxy	RedHat 8+
B	HashiCorp Vault	Storing user's private keys	RedHat 8+
C	CE Admin Panel	User & licence management	Win/Linux
D	CE Business	Core GUI application for end clients, pre-requisite to install CE Plugins. Can work also as standalone application without plugins.	Win/Mac/Linux
E	CE CMD Service Mode: LOCAL	Service managing authentication & crypto encrypt/decrypt operations (working with a single private key)	RedHat 8+
F	CE CMD Service Mode: VAULT	Service managing authentication & crypto decrypt operations (working with multiple private keys)	RedHat 8+
G	CE CMD CLIENT	Command Line utility to execute encryption / decryption calls on end-client terminals.	Win/Mac/Linux

The following deployment schemas outline three typical configurations for backend components:

- Default deployment schema (setup by included installation script, all services installed on one VM):
  - one VM: A + B + E + F + G
- Separated CMD Business Client deployment schema (CMD Clients installed on external machines):
  - 1'st VM: A + B + E + F
  - 2'nd VM: G
- Separated CMD Business Service deployment schema (CMD Server and CMD Clients installed on external machines):
  - 1'st VM: A + B
  - 2'nd VM: E + F
  - 3'rd VM: G

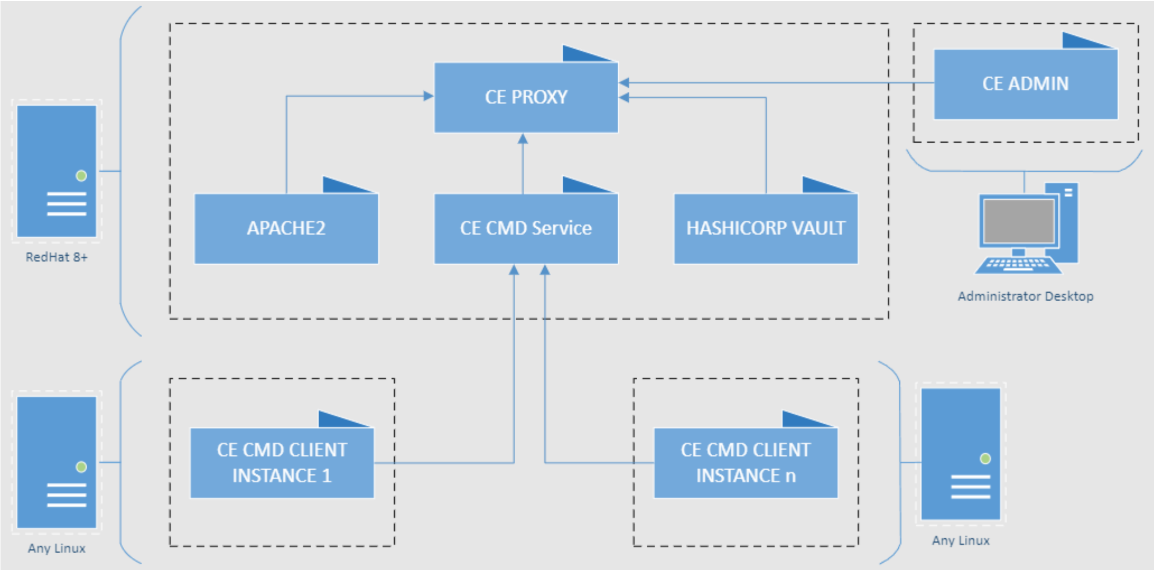
Default deployment schema [A + B + E + F + G]

This deployment schema is supported by CE Installer Package. All services coexist on one machine.



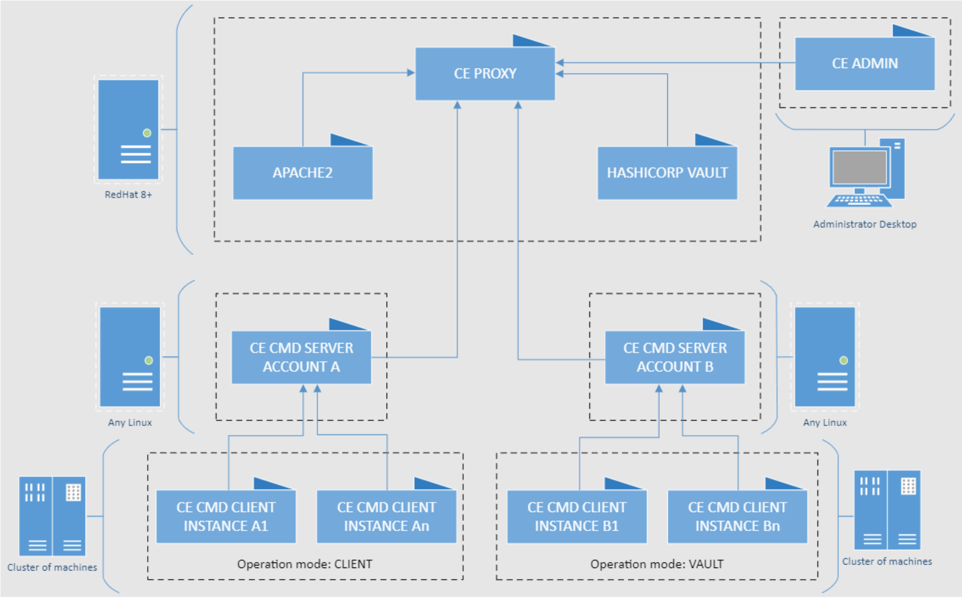
Separated CMD Business Client deployment schema [A + B + E + F | G]

This deployment schema is supported partially by CE Installer Package. All services coexist on one machine except CE CMD Client which is installed on one or more external machines.



Separated CMD Business Client deployment schema [A + B | E + F | G]

This deployment schema is supported partially by CE Installer Package. All main services coexist on one machine except CE CMD Service and CE CMD Client which are installed on one or more external machines.



Installation prerequisites

Backend services installation is compatible with RedHat from version 8 and above:

- One small VM (min. 4G RAM, 2xCPU) running Linux RedHat 8+ (*):
    - Backend:
        - **CE Business Proxy**
        - **CE Business CMD Service**
        - **CE Business CMD Client**
        - **HashiCorp Vault (**)**

(*) - dedicated server is not required, shared server with available resources can be used.
(**) - product of HashiCorp, Inc.

Frontend applications can be installed on all modern operating systems:

- One administrator desktop to install application for user's management (any modern computer Win/Linux with 2GB GB and 500MB free disk space):
    - **CE Business Admin Panel (GUI app)**
- User Desktops (any Win/Mac/Linux computer which is able to run latest Office applications, 500MB free disk space):
    - **CE Business Application (GUI app)**
    - **CE Business Application CMD (Command Line app)**

Installation of the main backend components [COMPONENT A, B]

The purpose of the CE Backend services is to set a communication layer between clients and Vault for private key management.

Main backend components are:

- CE PROXY [component A]
- HashiCorp Vault [component B]
- Apache2 [component A]

To install main backend components the following steps should be executed.

STEP 1 – set hostname

Check if hostname is including FQDN (machine name + domain)

```
# RedHat bash:
hostname
# If required set a new host name (replace text in bold)
sudo hostnamectl set-hostname your.proxy.com
```

STEP 2 – install CE Proxy

```
# RedHat bash:
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo https://rpm.cypher.dog/RHEL/cypherdog.repo
sudo yum install -y cdogp
```

STEP 3 – install HashiCorp Vault

Save the Vault root token for later use.

```
# RedHat bash:
sudo cdog-utils vault
sudo grep "Initial Root Token" /opt/vault/vault-init.log
#Initial Root Token: hvs.mseq0Mt0TuhvohVQpVN3W2s8
```

```
# RedHat bash:
sudo -E cdog-utils unseal
# Optional command for Vault unseal operation
```

STEP 4 – initialize CE Proxy credentials & run CE Proxy

Initialize CE Proxy credentials for “restore admin” and “proxy” users.

```
# RedHat bash:
sudo cdogp init -a admin -p proxy -u https://127.0.0.1:8200
#Set proxy account password
<Password_1>
#Repeat password
<Password_1>
#Set admin account password
<Password_2>
#Repeat password
<Password_2>
#Enter Vault token (with permissions to create an account, it may be root token)
hvs.mseq0Mt0TuhvohVQpVN3W2s8
#Restart CE Proxy service
sudo cdogp stop
sudo cdogp start &
```

STEP 5 – install Apache as external CE Proxy frontend

Install Apache service and save the password for trust distribution files.

```
# RedHat bash:
sudo cdog-utils apache
sudo /usr/sbin/setsebool -P httpd_can_network_connect 1
sudo apachectl restart
### Private key and certificates for CE Business GUI Aplication can be downloaded from the following URL's:
### - https://your.proxy.com/business.zip (ZIP file with password / all required files)
### - https://your.proxy.com/business.pfx (PKCS#12 file with password / all files except proxy cert)
### - http://your.proxy.com/business.pfx (PKCS#12 file with password / all files except proxy cert)
### - https://your.proxy.com/business_key_pass.der (DER file with password / only business private key)
### - https://your.proxy.com/proxy_cert.crt (CE Proxy certificate)
### - https://your.proxy.com/business_cert.crt (CE Business App certificate)
### - http://your.proxy.com/ca_cert.crt (CE Root CA certificate / http endpoint)
###
### Password for encrypted files: K773vqTDEDUb6wVasdds
### Please write down the password in case you would like to use the one of above files trust distribution.
### CE Root CA certificate: sha1 Fingerprint=9D:24:0C:18:82:C9:...
```

STEP 6 – validate services

To validate if all services are running, execute the following command (all three services should be up):

```
# RedHat bash:
sudo cdogp status
sudo vault status
sudo httpd -S|grep cypherdog
```

All configuration files for CE services are stored in the following directory:

- /opt/cypherdog/etc/

Note: if feasible Apache2 certificate should be replaced with a certificate which is widely trusted inside organization network. To replace Apache2 certificate administrator should modify the following configuration file:

- /etc/httpd/conf.d/cypherdog-ssl.conf

Installation of the CE Admin Panel [COMPONENT C]

The purpose of the CE Admin Panel application is to manage users (add, remove, block).

Step 1 – verity if the CE Proxy certificate is trusted

Application CE Admin Panel must be able to communicate with CE Proxy using TLS. If administrator used organization's PKI to deploy certificate for CE Proxy, then no further action is required. The best way to validate if certificate of CF Proxy is trusted from the administrator machine is to drop a proxy URL into browser which is using system trust store.

Installation of CE Adman Panel pan be executed by following with Step 3 actions.

Step 2 – download of the CE Proxy certificate

If the CE Proxy certificate is not trusted by administrator’s machine, then it must be downloaded. This certificate can be copied from Proxy server using by secure file transfer (file name ‘/opt/x509/ca_cert.crt’) or downloaded directly from Proxy server URL:

- http://**your.proxy.com**/ca_cert.crt

Since this endpoint is unprotected after download administrator must compare fingerprints of the server-side certificate and local certificate copy. What should be compared:

- server certificate fingerprint (Linux command syntax):
  - openssl x509 -noout -fingerprint -sha1 -inform pem -in ./ca_cert.pem
- with local certificate fingerprint (Windows command syntax):
  - Import-Certificate -FilePath ".\ca_cert.crt" -CertStoreLocation "Cert:\CurrentUser\My"

In case downloaded fingerprint is matching administrator can proceed to the next step.

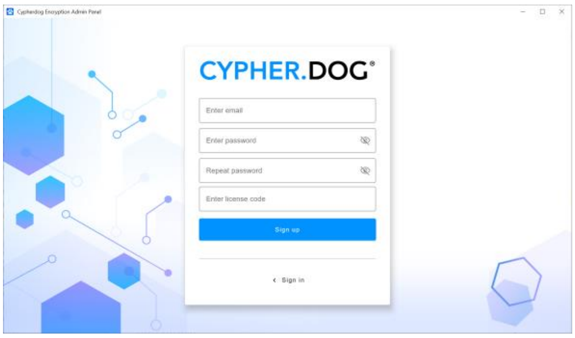
Step 3 – installation of the CE Admin Panel

The installation of CE Admin Panel can be executed on any Desktop (Win/Linux) by downloading and running the following installer (local administrator rights are required):

- https://packer.cdn.cypher.dog/download/business/admin/CE_Admin_windows-x64.exe

Next administrator should execute application and register a new Cypherdog account. During installation the following data should be provided:

- Administrator e-mail
- Administrator password
- License code



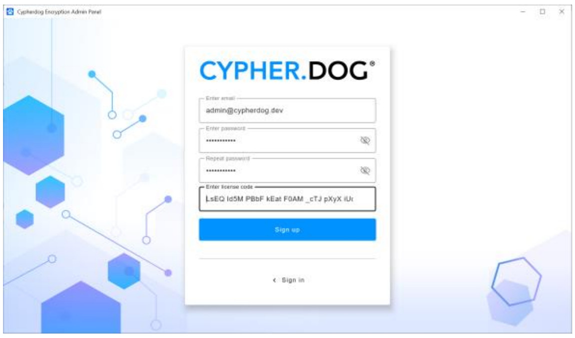
Cypherdog Encryption Admin Panel

Enter email

Enter password

Repeat password

Enter license code



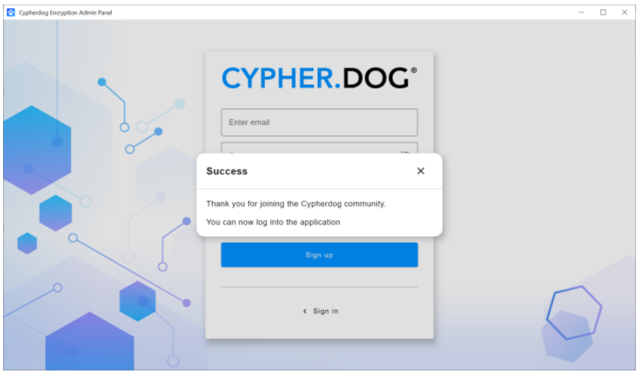
Cypherdog Encryption Admin Panel

Enter email: admin@cypherdog.dev

Enter password: ••••••••••••

Repeat password: ••••••••••••

Enter license code: LsEQ Id5M PBbF kEat F0AM _cTJ pXyX iUr

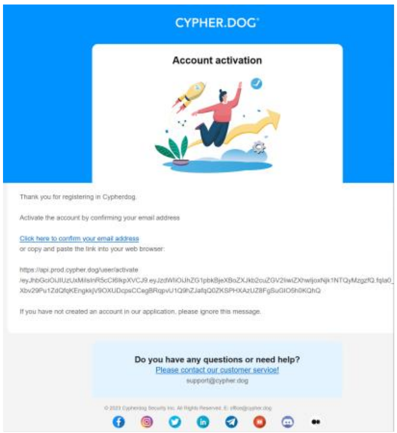


Success

Thank you for joining the Cypherdog community.

You can now log into the application

After providing the required data the system will register a new account and send activation link.



Account activation

Thank you for registering in Cypherdog.

Activate the account by confirming your email address

Click here to confirm your email address
or copy and paste the link into your web browser:

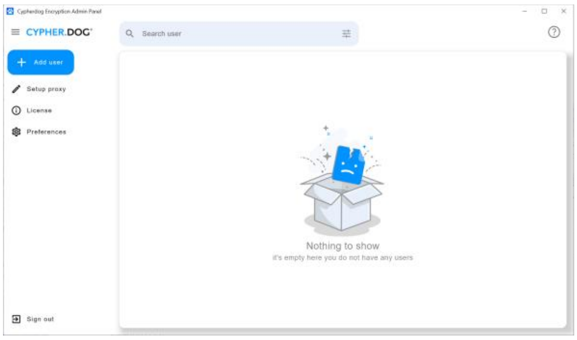
https://api.prod.cypher.dog/user/activate
/eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJhZG1pbkBjeXBoZXJkb2cuZGV2IiwiZXhwIjoxNjk1NTQyMzgzfQ.fqla0_
Xbv29Pu1ZdQfqKEngkkjV9OXUDcpsCCegBRqpvU1Q9hZJafqQ0ZKSPHXAzUZ8FgSuGIO5h0KQhQ

If you have not created an account in our application, please ignore this message.

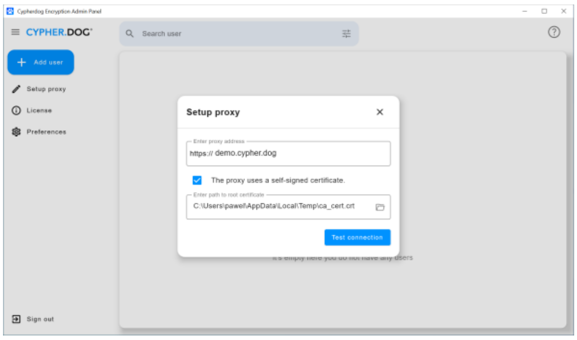
Do you have any questions or need help?
Please contact our customer service!
support@cypher.dog

© 2023 Cypherdog Security Inc. All Rights Reserved. E: office@cypher.dog

After activation link execution Cypherdog Encryption Admin Panel will be enabled. Next administrator should login into CE Admin Panel and configure connection to CE Proxy (“Setup proxy” option).



Nothing to show
It's empty here you do not have any users



Setup proxy

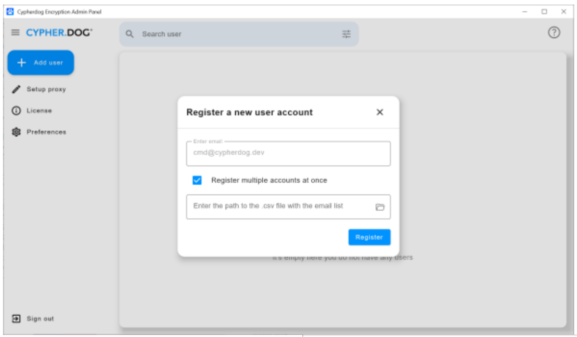
Enter proxy address: https:// demo.cypher.dog

☑ The proxy uses a self-signed certificate.

Enter path to root certificate: C:\Users\pawel\AppData\Local\Temp\ca_cert.crt

Test connection

Finally, administrator can add new users using “Add user” option. Users can be added manually one by one by or by bulk with CSV file.



Register a new user account

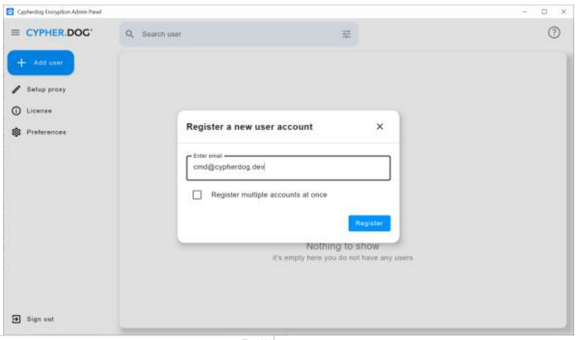
Enter email: cmd@cypherdog.dev

☑ Register multiple accounts at once

Enter the path to the .csv file with the email list

Register

it's empty here you do not have any users



Register a new user account

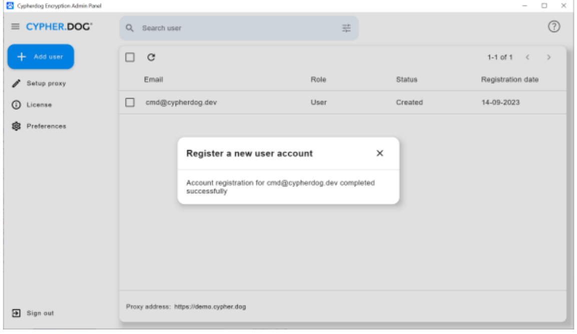
Enter email: cmd@cypherdog.dev

□ Register multiple accounts at once

Register

Nothing to show

it's empty here you do not have any users



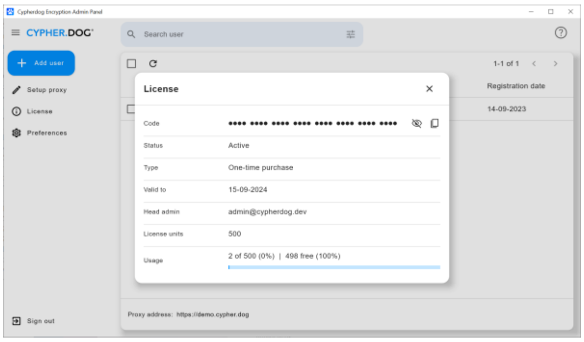
Email	Role	Status	Registration date
cmd@cypherdog.dev	User	Created	14-09-2023

Register a new user account

Account registration for cmd@cypherdog.dev completed successfully

Proxy address: https://demo.cypher.dog

With CE Admin Panel administrator can also review a licence use.



License

Code	•••• •••• •••• •••• •••• •••• •••• ••••
Status	Active
Type	One-time purchase
Valid to	15-09-2024
Head admin	admin@cypherdog.dev
License units	500
Usage	2 of 500 (0%) | 498 free (100%)

Proxy address: https://demo.cypher.dog

Installation of the Command Line functions [COMPONENT E, G]

The purpose of the CE CMD Service and CE CMD Client is to deliver functionality for encryption and decryption of text and files using only command line. Deployment of the CE CMD Service in the LOCAL mode means, that Command Line clients authenticated to this service will be able to use only one private key (one connected user account).

Main Command Line services components are:

- CE CMD Service in LOCAL Mode [component E]
- CE CMD Client [component G]

STEP 1 – Install CE CMD Service

To install command line services the following commands should be executed as a continuation of the previous bash session (provide password reset code received by an email):

```
# Run installation script and if asked provide password reset code received by an email
sudo CDOG_EMAIL=business@cypherdog.dev yum install -y cdogd
Installing Cypherdog Business Service
## Password change for user business@cypherdog.dev ##
## New auto-generated random password: nTz5bJdDbn252334dfw2!
Enter code from your mailbox (press double ENTER)
```

To validate if CE CMD Service is running, execute the following command (service should be up):

```
# RedHat bash:
sudo cdogd status
#Cdog service is running
```

Generate temporary authentication key for cdog command line utility:

```
# RedHat bash:
sudo cdogd key
#Key: 5rwkrZiJ1gNyNN-HtipPTI3Wj8rjyAirkWFTbLp
```

STEP 2 – Install CE CMD Client

Install client application and authorize it with previously generated key.

```
# RedHat bash:
sudo yum install -y cdog
sudo cdog auth --key=5rwkrZiJ1gNyNN-HtipPTI3Wj8rjyAirkWFTbLp --url=https://127.0.0.1:8220
```

To validate if command line option is configured properly operator can execute sample encryption command:

```
# RedHat bash:
sudo cdog verify -e admin@cypher.dog
# OK
sudo cdog encrypt –t <<< "TEST" -r admin@cypher.dog
# ---- BEGIN CYPHERDOG ENCRYPTED MESSAGE ---- ...
```

For more information about command line function please review the Command Line appendix.

Installation of the Command Line functions [COMPONENT F]

The purpose of the CE CMD Service in a VAULT Mode is to deliver functionality for decryption of text and files. Deployment of the CE CMD Service it the VAULT Mode means, that Command Line clients authenticated to this service will be able to use all or only part (depending on configuration) of user's private keys to decrypt information. No encryption is allowed in VAULT Mode. This mode is dedicated to being used by the organization gateway tools to monitor outgoing and incoming communication.

Installation of the component should be executed in the same way as for components E and G (see previous paragraph). After installation administrator should change the CE CMD Service configuration by editing ~/.cypherdog/cdog_service.properties file.

```
# RedHat bash:
sudo cat /opt/cypherdog/etc/cdogd.cnf |grep mode
application.mode=LOCAL
```

Value of the "application.mode" variable should be changed from LOCAL to VAULT. After change CE CMD Service should be restarted by execution the following command:

```
# RedHat bash:
sudo cdogd restart
```

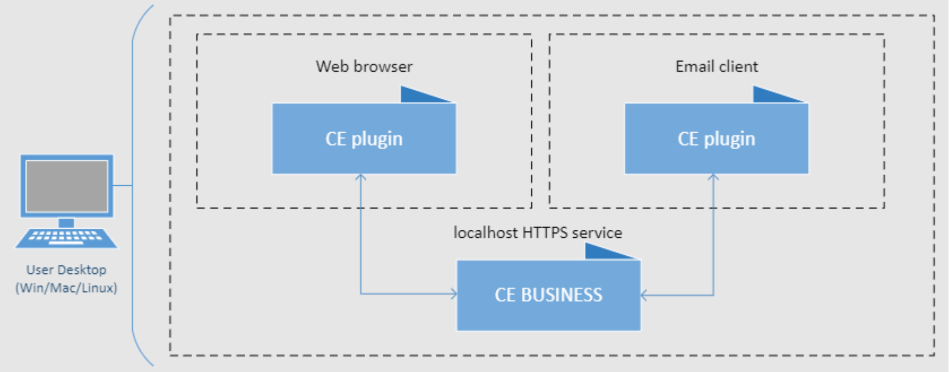
Operator could also review /opt/cypherdog/etc/cdogp.json configuration to limit CE Proxy access from CE CMD Service to the selected IP's and network segments if required. Detailed information about configuration file syntax and usage is placed in the appendix.

Installation of the CE Business [COMPONENT D]

CE Business is an end user application that allows encryption and decryption of files and messages. CE Business must be installed if end users would like to use browser plugin or mail program plugins.

Installation pre-requisites

Before installation can be executed administrator must prepare RSA private key and certificate issued for the following SANS: DNS:localhost and IP:127.0.0.1. This certificate must be trusted by the system. The purpose of this credential is to secure communication channel between CE Business application and its plugins what is presented on the drawing below.



Administrator can use own PKI system to issue such a credential or use credential generated during CE Proxy installation.

In case administrator choose to use own PKI, he should follow steps in the next paragraph (Step 1). In case administrator would like to reuse existing credential then he should pass to “Step 2”

Step 1 – generating certificate for CE Business

As a configuration for CSR generation /opt/x509/business-openssl.cnf can be used. Certificate should be issued for the following SANS:

- DNS: localhost
- IP: 127.0.0.1

Sample business-openssl.cnf openssl configuration file:

```
[ req ]
default_bits       = 2048
default_keyfile    = business_key.pem
distinguished_name = client_distinguished_name
req_extensions     = client_req_extensions
string_mask        = utf8only
[ client_distinguished_name ]
countryName         = Country Name (2 letter code)
countryName_default = US
stateOrProvinceName         = State or Province Name (full name)
stateOrProvinceName_default = CA
localityName         = Locality Name (eg, city)
localityName_default = Santa Clara
organizationName            = Organization Name (eg, company)
organizationName_default    = Cypherdog Security Inc.
commonName           = Common Name (e.g. server FQDN or YOUR name)
commonName_default   = Cypherdog Encryption BUSINESS
[ client_req_extensions ]
subjectKeyIdentifier = hash
basicConstraints     = CA:FALSE
keyUsage             = digitalSignature, keyEncipherment
subjectAltName       = @alternate_names
nsComment            = "OpenSSL Generated Certificate"
 [ alternate_names ]
DNS  = localhost
IP  = 127.0.0.1
```

Sample CSR generation command:

```
# Linux bash:
openssl req -batch -config business-openssl.cnf -newkey rsa:2048 -sha256 -nodes -out business_cert.csr -outform PEM
```

Next CSR should be signed by the trusted CA. Issued certificate should include the following entries:

```
# Linux bash:
openssl x509 -in business_cert.pem -text –noout | grep DNS
        DNS:localhost, IP Address:127.0.0.1
```

Finally, administrator should prepare a package in password protected PFX file. PFX file should include private key, certificate and all certificates from a trust chain. The following aliasing convention should be used:

```
# Linux bash:
openssl pkcs12 -password pass:<PASSWORD> -export -out ./business.pfx -name "client" \
-inkey ./business_key.pem -in ./business_cert.pem -certfile ./ca_cert.pem  -caname "root"
```

Generated “business.pfx” file can be used during CE Business installation in Step 3.

Administrator must check if:

- Business certificate is trusted by the target system
- Target system is trusting a certificate installed in CE Proxy Apache2 website.

Step 2 – use CE Business certificate generated during CE Proxy installation

In case administrator would like to use credential generated during CE Proxy installation no action is required.

The “business.pfx” file is available on the following endpoints:

- http://**your.proxy.com**/business.pfx
- https://**your.proxy.com**/business.pfx

The file can be appointed directly oy URL during CE Business installation. Note: password for “business.pfx” was printed during Apache service.

The CEE Business is a GUI application so it should be downloaded and installed on selected supported platform. Latest version of the CE Business application can be downloaded using the following link:

- https://packer.cdn.cypher.dog/download/business/desktop/CE_Business_windows-x64.exe

Preferred deployment for CE Business application is command line unattended installation mode. To execute such an installation on the user’s desktop the following command should be run.

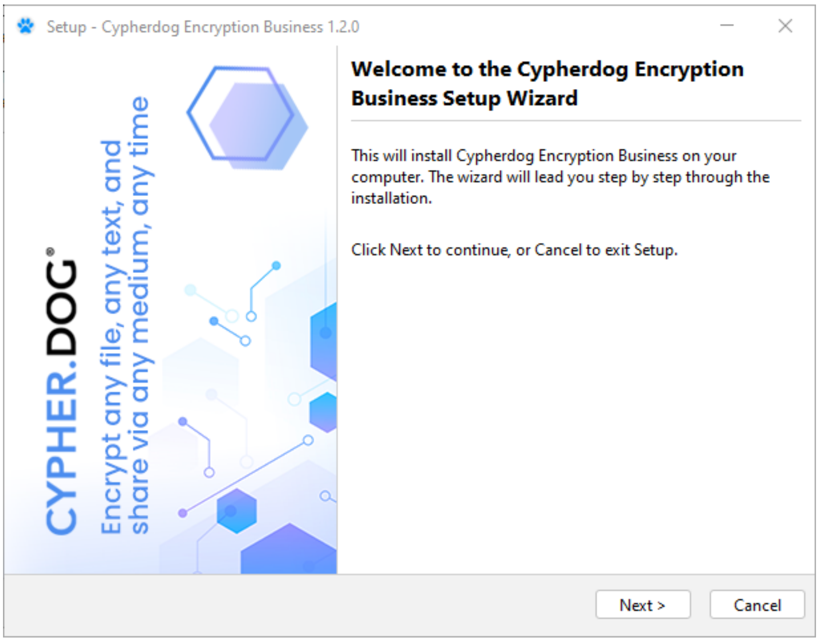
```
# Unattended command line CE Business installation mode (trust delivered from file)
.\CEE_Business_windows-x64.exe -q `
-Vpfx-file='c:\temp\business.pfx' `
-Vpfx-file-pass='TJDhWt7VKsSf3WFEg46R' `
-Vproxy-address='https://your.proxy.com'

# Unattended command line CE Business installation mode (trust delivered from known HTTPS endpoint)
.\CEE_Business_windows-x64.exe -q `
-Vpfx-url='https://your.proxy.com/business.pfx' `
-Vpfx-file-pass='TJDhWt7VKsSf3WFEg46R' `
-Vproxy-address='https://your.proxy.com'
```

```
# Unattended command line CE Business installation mode (trust delivered from unprotected HTTP endpoint)
.\CEE_Business_windows-x64.exe -q `
-Vpfx-url='http://your.proxy.com/business.pfx' `
-Vpfx-file-pass='TJDhWt7VKsSf3WFEg46R' `
-Vproxy-address='https://your.proxy.com'
```

Note: in case HTTPS endpoint is used as “Vpfx-url” parameter CE Proxy certificate must be issued by a well-known issuer.

After installation administrator's task is finished. End user (employee) can execute and initialize the CE Business application. The system will send to user password reset code by an e-mail. After application initialization user’s private key will be sent into Vault for backup and restore purposes.

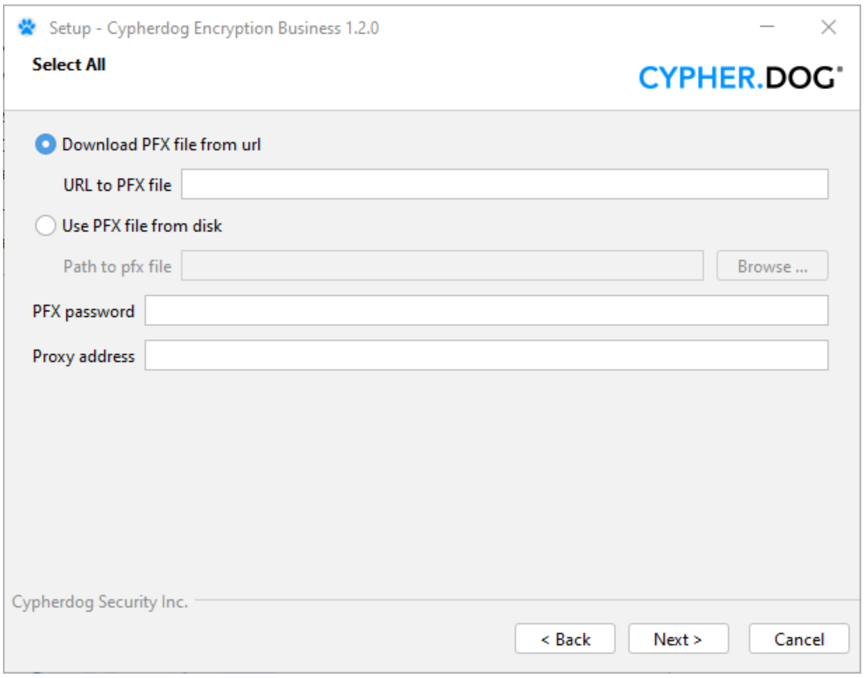
The CE Business application can be also installed using GUI. If no parameters will be provided, then application will ask about them during installation.


Setup - Cypherdog Encryption Business 1.2.0
CYPHER.DOG®
Encrypt any file, any text, and share via any medium, any time
Next >
Cancel

Welcome to the Cypherdog Encryption Business Setup Wizard

This will install Cypherdog Encryption Business on your computer. The wizard will lead you step by step through the installation.

Click Next to continue, or Cancel to exit Setup.



Select All

● Download PFX file from url

URL to PFX file

○ Use PFX file from disk

Path to pfx file

PFX password

Proxy address

[OPTIONAL STEP] Adding CE Root CA into user’s Desktop trust store (Windows)

In case administrator would like to add CE Root CA to the Windows trust store then the following procedure could must be executed:

- PowerShell script download
- Opening PowerShell terminal with Administrator privilege
- Download of the PowerShell script
- Execution of the PowerShell script

Executed script will download CE Root CA certificate, check its validity and add the certificate into trusted system store.

Script source:

- https://packer.cdn.cypher.dog/download/business/desktop/CE_Business_ADD_CE_ROOT_CA.ps1

```
# PowerShell console in Administrator mode
Start-Process powershell -Verb runAs
# Download script
Invoke-RestMethod `
–Uri "https://packer.cdn.cypher.dog/download/business/desktop/CE_Business_ADD_CE_ROOT_CA.ps1" `
| Out-File -Encoding ascii "CE_Business_ADD_CE_ROOT_CA.ps1"
# Run script, fingerprint can be found in the /opt/install/cdog_install.log (replace text in bold)
.\CE_Business_ADD_CE_ROOT_CA.ps1 -url 'your.proxy.com' -fingerprint '43:FA:0B:15:A0:78..'
```

To validate if the certificate was properly added to the user’s desktop machine trusted store the following command can be executed.

```
# List CEE Root certificate
Get-ChildItem -path cert:\LocalMachine\Root | select-string "CE Signing CA"
```

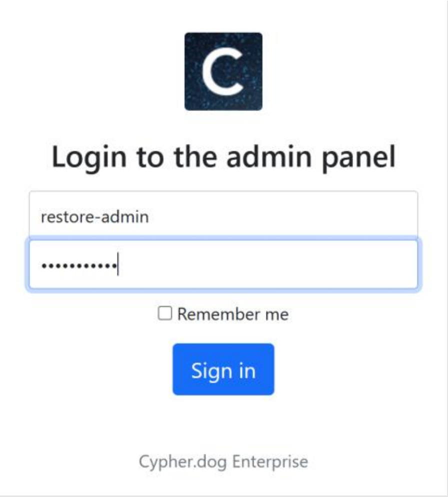
CE Business recovery setup by the administrator

In case the user’s private key is lost the administrator can re-run the installation and provide a token for private key restore.

To generate a restore token the operator should login into CE Proxy using browser. Login and password were provided CE Proxy initialization. If the default configuration was used, then CE Proxy should be accessible on the URL served by Apache2 service. To check active Apache2 URL execute the following command:

```
# RedHat bash:
httpd -S|grep cypher
```

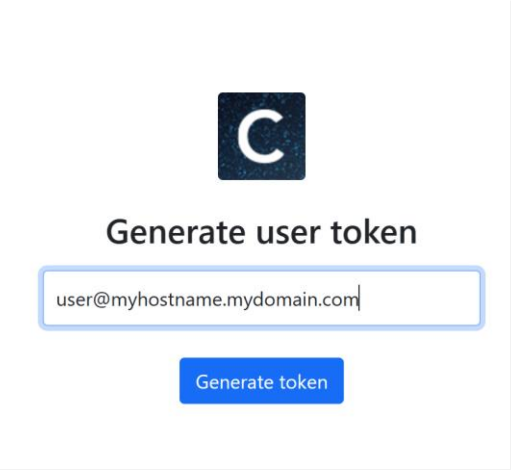
Administrator console for restore token generation.



Login to the admin panel

restore-admin

•••••••••••



Generate user token

user@myhostname.mydomain.com

Remarks

List of security guidelines for service administrators:

1. If possible, use separate dedicated VM for the CEE_Proxy and Vault deployments,
2. Open CE Proxy service port for connections only inside the company's internal network,
3. Do new CE Business application installations only inside the company's internal network (required for private key backup),
4. If an internal PKI infrastructure is available, then the following certificates can be created using company's CA (*):
   - vault_cert.pem
   - proxy_cert.pem
   - business_cert.pem (certificate generated per host or one for all hosts),
5. If no new installations of CE Business application are planned in a short time, then service CE Proxy should be stopped permanently.

(*) - for certificate requirements details review the following configuration files: proxy-openssl.cnf, vault-openssl.cnf, business-openssl.cnf. Mind that company's internal CA root certificate should be trusted by host which is a target for CE Business application installation.

Appendix - CE CMD Service – command syntax

```
/opt/cee/bin/cdogd

Usage:  [-hV] [--verbose] [COMMAND]

  -h, --help      Show this help message and exit.

  -V, --version   Print version information and exit.

      --verbose   Use this to see more logs

Commands:

  start     Start service

  stop      Stop service

  status    Check service status

  restart   Restart service

  config    Manage configuration file

  init      Use it to check is everything ready to start a service. It will

              validate keys and generate new one if needed.

  key       Generate a new vouch key, use it in the CLI application to get

              Authorization

 account    Manage account, change password

 verify    Verify that the email addresses provided have keys in the Cypherdog system
```

Command examples:

```
# Generate new private key

/opt/cee/bin/cdogd init

# Start the CE CMD Service

/opt/cee/bin/cdogd start

# Change cmd user password

/opt/cee/bin/cdogd account –p

# Generate temporary vouch key for the new CMD Client authorization

/opt/cee/bin/cdogd key
```

Appendix - CE CMD Client – command syntax

```
/opt/cee/bin/cdog --help
```

```
Usage:  [-hV] [--verbose] [COMMAND]

  -h, --help                 Show this help message and exit.

  -V, --version              Print version information and exit.

  --verbose                  Use this to see more logs

Commands:

  encrypt  Use it for file/text encryption. Only for service LOCAL mode.

  decrypt  Use it for file/text decryption

  auth     Authorize application

 verify   Verify that the email addresses provided have keys in the Cypherdog system
```

```
/opt/cee/bin/cdog encrypt --help
```

```
Usage:  encrypt [-htV] [-in=file] [-out=directory/file] [-r=emails...]...

Use it for file/text encryption. Only for service LOCAL mode.

  -in=file                   File to encrypt.

  -out=directory/file        Directory for the encrypted file/File for the encrypted text

  -r= emails...              Recipient emails.

  -t                         Use this flag if you want to encrypt a text message from a terminal or a
stream. Use the -out flag to specify a file for ciphertext or redirect it to a stream. Otherwise, the
ciphertext will be printed in the terminal.

  -h, --help                 Show this help message and exit.

  -V, --version              Print version information and exit.
```

```
/opt/cee/bin/cdog decrypt --help

Usage:  decrypt [-htV] [-in=file] [-out=directory/file] [-r=email]

Use it for file/text decryption

  -in=file                  File to decrypt.

  -out=directory/file       Directory for the decrypted file/File for the decrypted text

  -r= email                 Recipient email (only for vault mode)

  -t                        Use this flag if you want to decrypt a ciphertext from a terminal or a
stream. Use the -out flag to specify a file for decrypted message or redirect it to a stream. Otherwise,
the decrypted message will be printed in the terminal.

  -h, --help                Show this help message and exit.

  -V, --version             Print version information and exit.
```

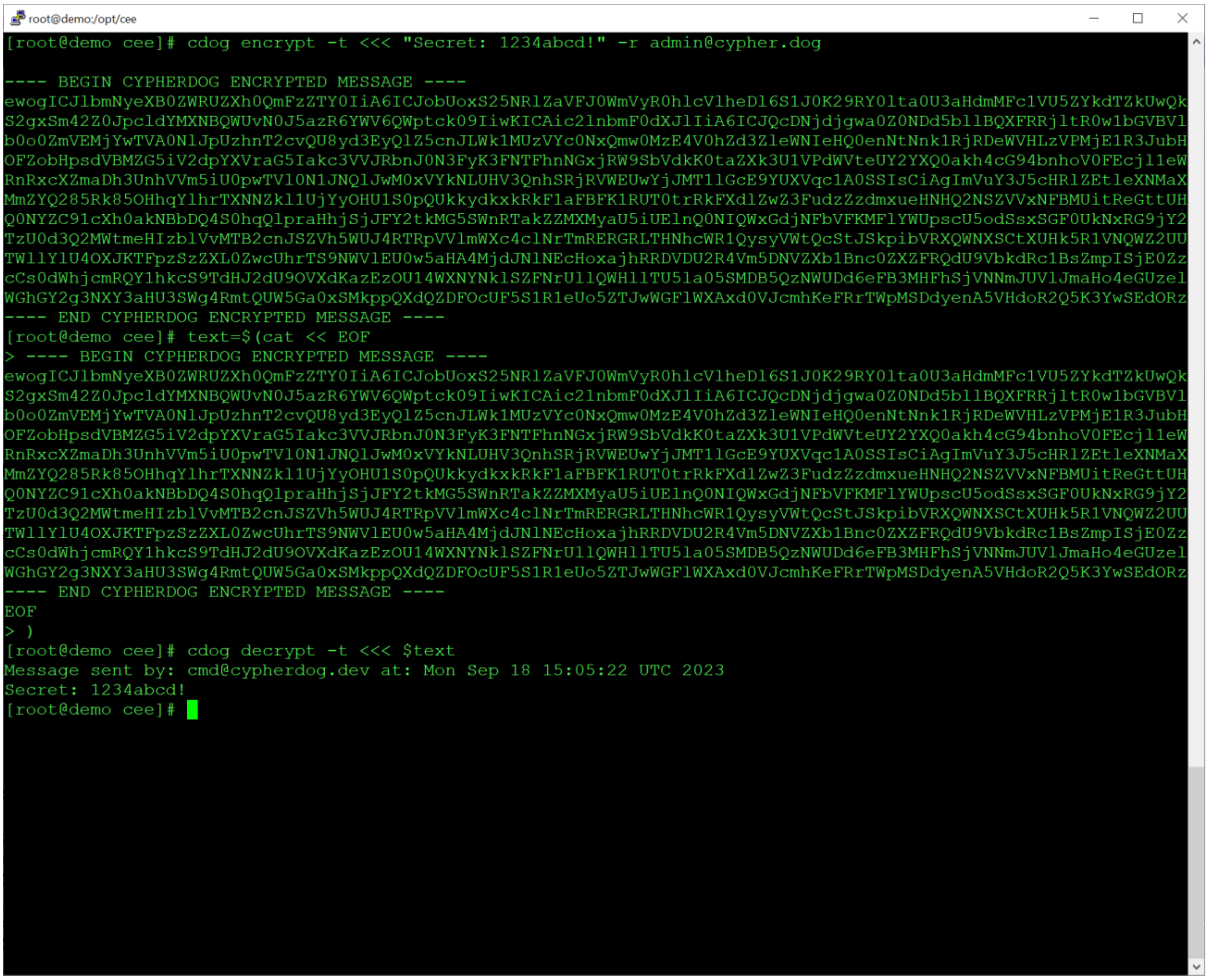
```
/opt/cee/bin/cdog auth --help

Usage:  auth [-hV] -k=vouch key from admin -u=service url

Authorize application

  -h, --help                Show this help message and exit.

  -k, --key=vouch key from admin

                            Vouch key for authorization init

  -u, --url=service url     Cypherdog CLI Service URL

  -V, --version             Print version information and exit.
```

```
/opt/cee/bin/cdog verify --help

Usage:  verify [-hV] [-e=<emails>]...

Verify that the email addresses provided have keys in the Cypherdog system

  -e= <emails>              emails address.

  -h, --help                Show this help message and exit.

  -V, --version             Print version information and exit.
```

Command examples:

```
cdog auth –k Qw8hYlXjw6KTsyxqizmlI9FLeLjhzz... –u https://ce.cmd.hostname

cdog encrypt -t <<< "Secret: 1234abcd!" -r admin@cypher.dog

cdog encrypt -in=./file.txt -out=./ -r admin@cypher.dog

cdog decrypt -in=./file2.txt.cdog -out=./

cdog verify –e admin@cypher.dog
```

```
Sample BASH output:
```



```
[root@demo cee]# cdog encrypt -t <<< "Secret: 1234abcd!" -r admin@cypher.dog

---- BEGIN CYPHERDOG ENCRYPTED MESSAGE ----
ewogICJlbmNyeXB0ZWRUZXh0QmFzZTY0IiA6ICJobUoxS25NRlZaVFJ0WmVyR0hlcVlheDl6S1J0K29RY0lta0U3aHdmMFc1VU5ZYkdTZkUwQk
S2gxSm42Z0JpcldYMXNBQWUvN0J5azR6YWV6QWptck09IiwKICAic2lnbmF0dXJlIiA6ICJQcDNjdjgwa0Z0NDd5bllBQXFRRjltR0w1bGVBVl
b0o0ZmVEMjYwTVA0NlJpUzhnT2cvQU8yd3EyQlZ5cnJLWk1MUzVYc0NxQmw0MzE4V0hZd3ZleWNIeHQ0enNtNnk1RjRDeWVHLzVPMjE1R3JubH
OFZobHpsdVBMZG5iV2dpYXVraG5Iakc3VVJRbnJ0N3FyK3FNTFhnNGxjRW9SbVdkK0taZXk3U1VPdWVteUY2YXQ0akh4cG94bnhoV0FEcjlleW
RnRxcXZmaDh3UnhVVm5iU0pwTVl0N1JNQlJwM0xVYkNLUHV3QnhSRjRVWEUwYjJMT1lGcE9YUXVqc1A0SSIsCiAgImVuY3J5cHRlZEtleXNMaX
MmZYQ285Rk85OHhqYlhrTXNNZkl1UjYyOHU1S0pQUkkydkxkRkF1aFBFK1RUT0trRkFXdlZwZ3FudzZzdmxueHNHQ2NSZVVxNFBMUitReGttUH
Q0NYZC91cXh0akNBbDQ4S0hqQlpraHhjSjJFY2tkMG5SWnRTakZZMXMyaU5iUElnQ0NIQWxGdjNFbVFKMFlYWUpscU5odSsxSGF0UkNxRG9jY2
TzU0d3Q2MWtmeHIzblVvMTB2cnJSZVh5WUJ4RTRpVVlmWXc4clNrTmRERGRLTHNhcWR1QysyVWtQcStJSkpibVRXQWNXSCtXUHk5R1VNQWZ2UU
TWllYlU4OXJKTFpzSzZXL0ZwcUhrTS9NWVlEU0w5aHA4MjdJNlNEcHoxajhRRDVDU2R4Vm5DNVZXb1Bnc0ZXZFRQdU9VbkdRc1BsZmpISjE0Zz
cCs0dWhjcmRQY1hkcS9TdHJ2dU9OVXdKazEzOU14WXNYNklSZFNrUllQWHllTU5la05SMDB5QzNWUDd6eFB3MHFhSjVNNmJUVlJmaHo4eGUzel
WGhGY2g3NXY3aHU3SWg4RmtQUW5Ga0xSMkppQXdQZDFOcUF5S1R1eUo5ZTJwWGFlWXAxd0VJcmhKeFRrTWpMSDdyenA5VHdoR2Q5K3YwSEdORz
---- END CYPHERDOG ENCRYPTED MESSAGE ----
[root@demo cee]# text=$(cat << EOF
> ---- BEGIN CYPHERDOG ENCRYPTED MESSAGE ----
ewogICJlbmNyeXB0ZWRUZXh0QmFzZTY0IiA6ICJobUoxS25NRlZaVFJ0WmVyR0hlcVlheDl6S1J0K29RY0lta0U3aHdmMFc1VU5ZYkdTZkUwQk
S2gxSm42Z0JpcldYMXNBQWUvN0J5azR6YWV6QWptck09IiwKICAic2lnbmF0dXJlIiA6ICJQcDNjdjgwa0Z0NDd5bllBQXFRRjltR0w1bGVBVl
b0o0ZmVEMjYwTVA0NlJpUzhnT2cvQU8yd3EyQlZ5cnJLWk1MUzVYc0NxQmw0MzE4V0hZd3ZleWNIeHQ0enNtNnk1RjRDeWVHLzVPMjE1R3JubH
OFZobHpsdVBMZG5iV2dpYXVraG5Iakc3VVJRbnJ0N3FyK3FNTFhnNGxjRW9SbVdkK0taZXk3U1VPdWVteUY2YXQ0akh4cG94bnhoV0FEcjlleW
RnRxcXZmaDh3UnhVVm5iU0pwTVl0N1JNQlJwM0xVYkNLUHV3QnhSRjRVWEUwYjJMT1lGcE9YUXVqc1A0SSIsCiAgImVuY3J5cHRlZEtleXNMaX
MmZYQ285Rk85OHhqYlhrTXNNZkl1UjYyOHU1S0pQUkkydkxkRkF1aFBFK1RUT0trRkFXdlZwZ3FudzZzdmxueHNHQ2NSZVVxNFBMUitReGttUH
Q0NYZC91cXh0akNBbDQ4S0hqQlpraHhjSjJFY2tkMG5SWnRTakZZMXMyaU5iUElnQ0NIQWxGdjNFbVFKMFlYWUpscU5odSsxSGF0UkNxRG9jY2
TzU0d3Q2MWtmeHIzblVvMTB2cnJSZVh5WUJ4RTRpVVlmWXc4clNrTmRERGRLTHNhcWR1QysyVWtQcStJSkpibVRXQWNXSCtXUHk5R1VNQWZ2UU
TWllYlU4OXJKTFpzSzZXL0ZwcUhrTS9NWVlEU0w5aHA4MjdJNlNEcHoxajhRRDVDU2R4Vm5DNVZXb1Bnc0ZXZFRQdU9VbkdRc1BsZmpISjE0Zz
cCs0dWhjcmRQY1hkcS9TdHJ2dU9OVXdKazEzOU14WXNYNklSZFNrUllQWHllTU5la05SMDB5QzNWUDd6eFB3MHFhSjVNNmJUVlJmaHo4eGUzel
WGhGY2g3NXY3aHU3SWg4RmtQUW5Ga0xSMkppQXdQZDFOcUF5S1R1eUo5ZTJwWGFlWXAxd0VJcmhKeFRrTWpMSDdyenA5VHdoR2Q5K3YwSEdORz
---- END CYPHERDOG ENCRYPTED MESSAGE ----
EOF
> )
[root@demo cee]# cdog decrypt -t <<< $text
Message sent by: cmd@cypherdog.dev at: Mon Sep 18 15:05:22 UTC 2023
Secret: 1234abcd!
[root@demo cee]#
```

CMD configuration files

Configuration files are located in the current user home directory under:

- /opt/cypherdog/etc/cdogp.json [CE Proxy configuration]
- /opt/cypherdog/etc/cdogd.cnf [CE CMD Service configuration]
- ~/.cypherdog/cdog.auth [CE CMD Client configuration]
- ~/.cypherdog/cdog.cnf [CE CMD Client configuration]

Sample configuration files content

CE Proxy Configuration

```
#cdogp.json
{
  "proxy.address": "localhost",
  "proxy.port": "8210",
  "certificate.path": "/opt/cypherdog/x509/proxy_bundle.pem",
  "private.key.path": "/opt/cypherdog/x509/proxy_key.pem",
  "proxy.vault.account.username": "proxy",
  "proxy.vault.account.password": "demoDEMO1234#",
  "vault.url": https://127.0.0.1:8200,
  "cidr.policies": [
    {
      "name": "ANY_ORIGIN",
      "CIDR": [
        "0.0.0.0/0"
      ]
    }
  ],
  "acl.policies": [
    {
      "name": "READ_ALL",
      "emails": [
        "*"
      ]
    }
  ],
  "api.keys": [
    {
      "value": "K7KMYd7EYQp_O8aCV9GghEQ9IZbjewxNBksU2bm_ikSc_AzBVxOMU7bkMEqiy19B",
      "name": "full_access_key",
      "acl.policy.name": "READ_ALL",
      "cidr.policy.name": "ANY_ORIGIN"
    }
  ]
}
```

CE CMD Service Configuration

```
#cdogd.cnf
server.address=127.0.0.1
proxy.key=K7KMYd7EYQp_O8aCV9GghEQ9IZbjewxNBksU2bm_ikSc_AzBVxOMU7bkMEqiy19B
proxy.port=8210
account.email=business@cypherdog.dev
application.mode=LOCAL
server.port=8220
server.ssl.certificate=/opt/cypherdog/x509/proxy_bundle.pem
account.password=WXBlgUUN8490Or2392123kaghs!
server.ssl.certificate-private-key=/opt/cypherdog/x509/proxy_key.pem
proxy.address=localhost
```

CE CMD Client configuration

```
#cdog.auth
3f596a96-d166-4e2c-846c-a3ec57950127:l4Ty22-y8_ZzrGMxkIPRSppopJZFKmb-6xy1sAomFAlxGFG94dnpUPlcAkPf3SvH[
#cdog.cnf
server.url=https\://127.0.0.1\:8220
```

Cypherdog Encryption Business - One Page Installation Manual

```
# == Core services: CE Proxy & Vault ==
# Execute in RHEL8+ BASH (backend hosting VM)
```

```
sudo hostnamectl set-hostname your.proxy.com
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo https://rpm.cypher.dog/RHEL/cypherdog.repo
sudo yum install -y cdogp
sudo cdog-utils vault
sudo grep "Initial Root Token" /opt/vault/vault-init.log
#Initial Root Token: hvs.mseq0Mt0TuhvohVQpVN3W2s8
sudo cdogp init -a admin -p proxy -u https://127.0.0.1:8200
sudo cdogp stop
sudo cdogp start &
sudo cdog-utils apache
sudo /usr/sbin/setsebool -P httpd_can_network_connect 1
sudo apachectl restart
```

```
# Install on Admin desktop for licence and users' management (*)
```

https://packer.cdn.cypher.dog/download/business/admin/CE_Admin_windows-x64.exe

```
# == Supporting services: CE CMD Business & CE CMD Client ==
# Execute in RHEL8+ BASH (backend hosting VM)
```

```
sudo CDOG_EMAIL=business@cypherdog.dev yum install -y cdogd
#Enter code from your mailbox (press double ENTER)
cdogd stop
cdogd start &
sudo cdogd key
#Key: 5rwkrZiJ1gNyNN-HtipPTI3Wj8rjyAirkWFTbLp
sudo yum install -y cdog
sudo cdog auth --key=5rwkrZiJ1gNyNN-HtipPTI3Wj8rjyAirkWFTbLp --url=https://127.0.0.1:8220
```

```
# == End user desktop CE Business Application / enabler for mobile app client ==
# Install on user desktop (*)
```

https://packer.cdn.cypher.dog/download/business/desktop/CE_Business_windows-x64.exe

```
.\CEE_Business_windows-x64.exe -q `
-Vpfx-file='c:\temp\business.pfx' `
-Vpfx-file-pass='TJDhWt7VKsSf3WFEg46R' `
-Vproxy-address='https://your.proxy.com'
```

(*) - workstation trust store must include trust chain for certificate configured on the CE Proxy endpoint. In case default installation in executed the following command will add the required trusted root certificate :

```
# Windows command line
# Download http://your.proxy.com/ca_cert.crt file using secure channel file and execute command below.
# If secure channel (like SFTP) cannot be used, then follow the instructions from this paragraph.
certmgr /add /c ca_cert.crt /s /r localMachine root
```

```
# Linux bash (RHEL):
sudo cp ca_cert.crt /etc/pki/ca-trust/source/anchors
sudo update-ca-trust extract
```