opentext™

TTP EMEA 2025

Protect CIFS share access with Multi-factor Authentication

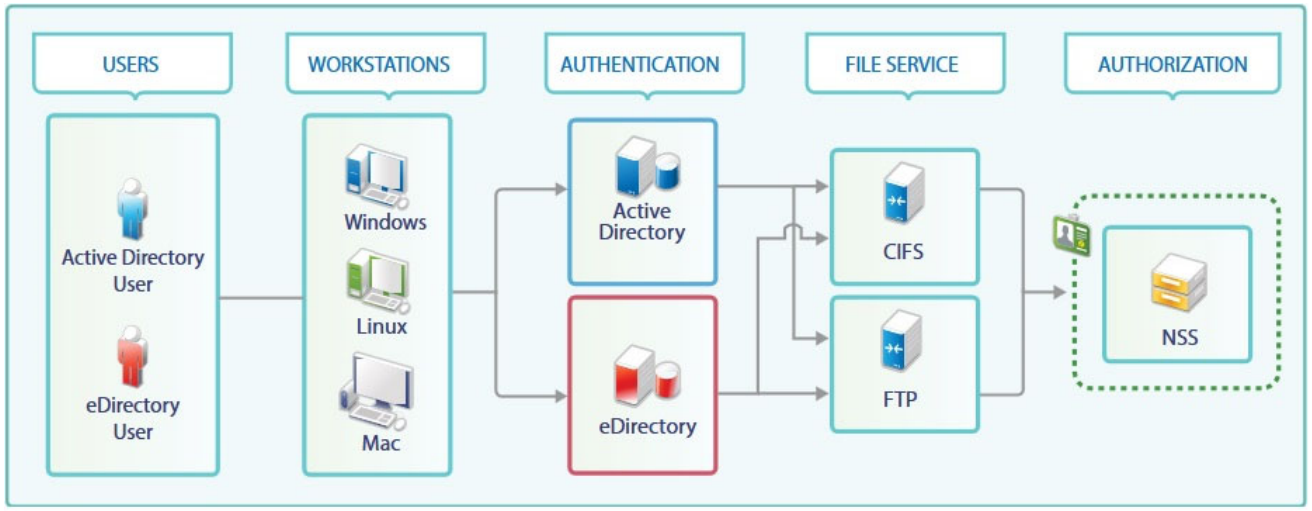
OES Multifactor Authentication Service

Mike Hunsche
Arun Subramanian R
Girish KS

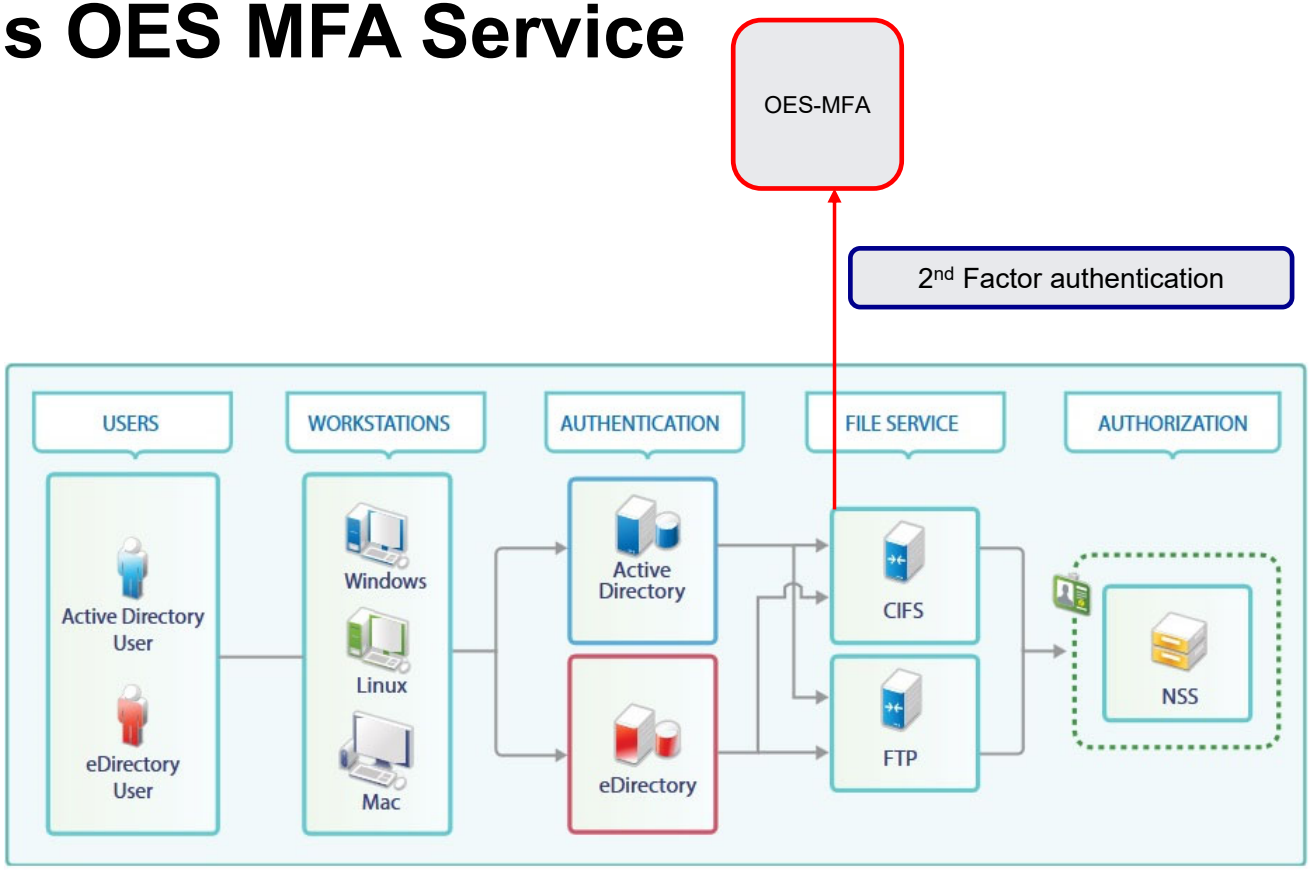
Agenda

- What is OES MFA Service
- OES MFA Architecture
- Components
- Key features
- Configuring MFA server and CIFS
- Demo
- What's next

What is OES MFA Service



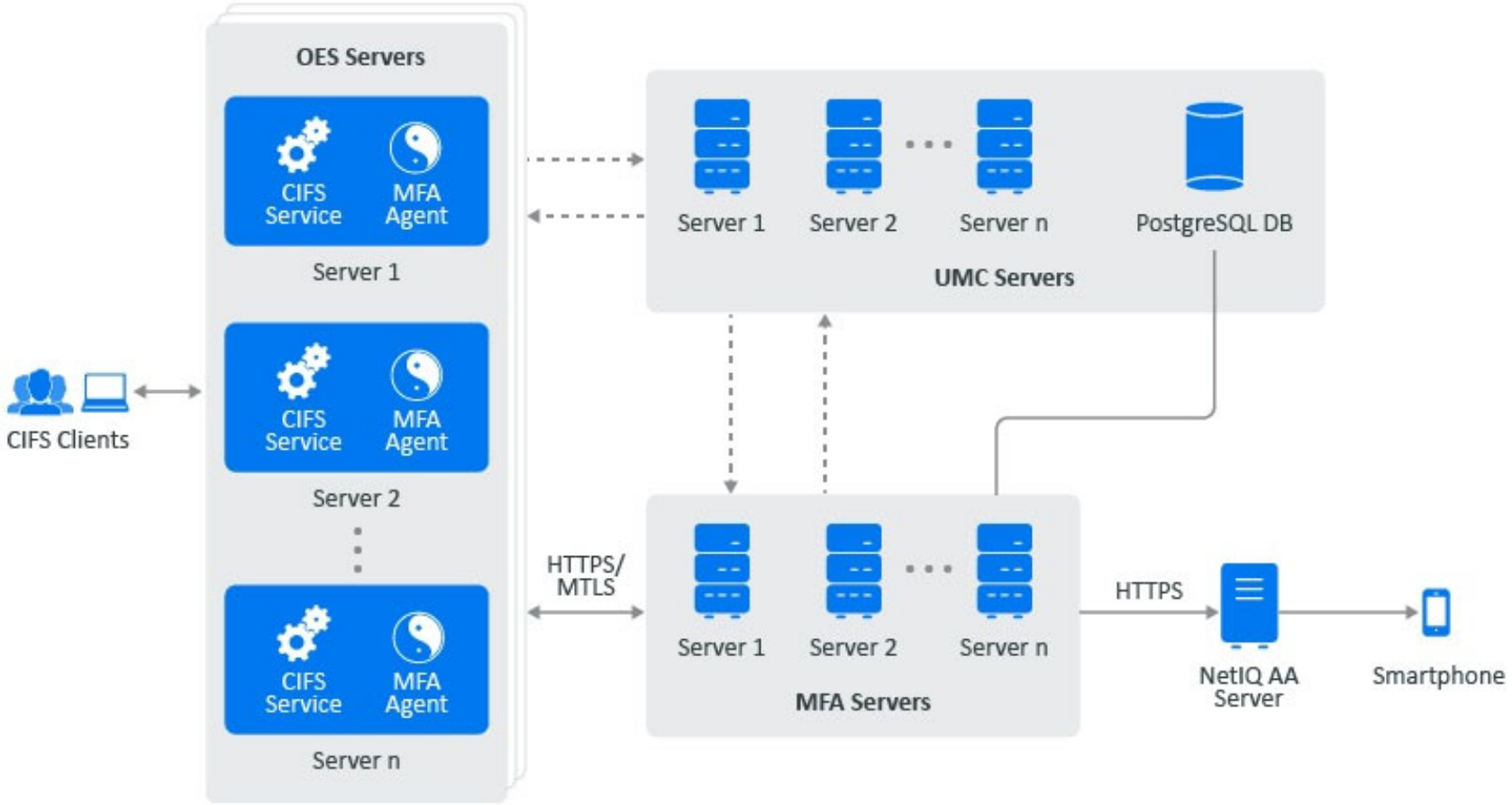
What is OES MFA Service



What is OES MFA Service

- A new service in OES which provides Multi Factor Authentication service to OES Services.
- Enables OES service to enforce MFA while users access the resources
- Currently, to be used by CIFS service.

OES MFA Service Architecture



Components

MFA Server

- One or more Centralized server(s)
- Install and run on any OES server

Pre-requisites

- UMC server – Database and service discovery
- NetIQ Advanced Authentication server
- eDir admin credentials for configuration

MFA Agent

- Runs in Every OES server (with CIFS)
- Interface between OES service and MFA server
- Service discovery and auto configuration

MTLS

- Uses eDirectory certificates by default
- MFA server run behind the Apache server

opentext™

Key features of OES MFA service

- Easy to enable MFA for OES services
- Minimize admin configuration and maintenance effort
- Can be extended for MFA Providers other than Advanced Authentication

Key features

- MFA can be triggered from a server (cifs server)
- Can work without a client
- High availability and fault tolerance
- Seamless (re-)connection on cluster fail-over
- Smartphone push as second factor of authentication
- Auto configuring OES to use OES MFA service
- Provides persistence of sessions
- Data Centric
  - Server or SMB Share level
  - Second factor trigger on Data(Share) access

Advanced authentication server config

- Endpoint – Endpoint ID and Endpoint secret
- Chain – Containing only smart phone push
- Event – Containing chain
- eDirectory Repository name - (optional)

Setting up an MFA server

1. Install OES-MFA pattern from yast
2. *mfa-server-cli service-config*

   eDirectory admin credentials and hostname confirmation
3. *mfa-server-cli auth-server --authSrvHost=<AA server details>*

   -- endPointID=<id> --endPointSecret=<secret>
4. *mfa-server-cli policy-config --event=<AA event name>*

   --eDirRepo=<Name of eDirectory repository in AA server>

mfa-server-cli print-config

systemctl status mfa-server.service

Setting up an MFA server

```
blr8-98-178:~ # mfa-server-cli print-config
------------------------------
mfa-server:-
------------------------------
hostAddress                          -    blr8-98-178.labs.blr.novell.com
port                                 -    3456
isConfigured                         -    true
clientCertCAPath                     -    /usr/share/pki/trust/anchors/SSCert.pem
enforceClientAuth                    -    true
mfaValidity                          -    960
isAuthSrvConfigured                  -    true
isPolicyConfigured                   -    true
------------------------------
logging:-
------------------------------
logLevel                             -    info
logFilePath                          -    /var/opt/novell/log/oes/mfaserver
logTimeStampFormat                   -    YYYY-MM-DD HH:mm:ss
------------------------------
database:-
------------------------------
isDbConfigured                       -    true
dbDialect                            -    postgres
dbHostName                           -    blr8-98-176.labs.blr.novell.com
dbPort                               -    5432
dbDataBaseName                       -    umc_edir_174
dbSchemaName                         -    public
------------------------------
auth_servers:-
------------------------------
authSrvHost                          -    oes226.multifactor.in
------------------------------
policy_config:-
------------------------------
eDirRepo                             -    null
event                                -    test_cifs_event
blr8-98-178:~ #
```


MFA agent

- No configuration required by default
- Service discovery
- ***mfa-agent-cli print-config***
  systemctl status mfa-agent.service

MFA agent

```
blr8-98-174:~ # mfa-agent-cli print-config
------------------------------
mfa-agent:-
------------------------------
enableServiceDiscovery                  -    true
clientCertPath                          -    /etc/ssl/servercerts/servercert.pem
clientCertKeyPath                       -    /etc/ssl/servercerts/serverkey.pem
logLevel                                -    info
logFilePath                             -    /var/opt/novell/log/oes/mfaagent
logTimeStampFormat                      -    YYYY-MM-DD HH:mm:ss
------------------------------
mfa-server:-
------------------------------
isConfigured                            -    true
mfaServerHosts                          -    blr8-98-178.labs.blr.novell.com
                                             blr8-98-176.labs.blr.novell.com
blr8-98-174:~ #
```

Configuring CIFS to use MFA

- Server level
  - novcifs –-mfa=yes/no
- Share level
  - novcifs -s –mfa=yes/no –n VOL1

Demo

- CIFS server MFA enabled using OES MFA service
  - Install OES-MFA server
  - Configure first MFA server
  - Configure a second MFA server
  - Configure CIFS to enforce MFA
  - CIFS share mapping with MFA enabled
  - MFA Validity

Demo

- Setup details
  - blr8-98-176 – UMC server, DB server
  - blr8-98-178 – MFA server 1
  - blr8-98-176 – MFA server 2
  - blr8-98-174 – CIFS server, MFA agent
  - Blr8-100-232 – Windows 10 client

Why Allow List

An Allow List in MFA exempts trusted entities from MFA process, simplifying access while maintaining security

Categories of Allow list

Allow List Types

- User
- Address
- Range
- Subnet
- User Group

Allow List Help page

```
blr8-111-72:~ # mfa-server-cli mfa-manage --help
mfa-server-cli mfa-manage

Manage MFA server:

mfa-server-cli mfa-manage
--deleteAllMfaSessions=<yes>
--printAllMfaSessions=<yes>
--allowlistType=<user/usergroup/address/
        range/subnet>
--addToAllowlist=<allowed list entry value>
--removeFromAllowlist=<allowed list entry
        value>
--printAllowlist=<yes>

Options:
  --help                 Show help                                    [boolean]
  --version              Show version number                          [boolean]
  --deleteAllMfaSessions  Delete all mfa sessions from DB
                                                  [string] [choices: "yes"]
  --printAllMfaSessions   Print all mfa sessions available in DB
                                                  [string] [choices: "yes"]
  --allowlistType         Type of the allowed list entry
          [string] [choices: "user", "usergroup", "address", "range", "subnet"]
  --addToAllowlist        Value of the allowed list entry               [string]
  --removeFromAllowlist   Value of the allowed list entry               [string]
  --printAllowlist        Type of the allowed list entry
                                                  [string] [choices: "yes"]
blr8-111-72:~ #
```


MFA Allow List Commands

- Adding to allow list
  - **mfa-server-cli mfa-manage --allowListType=<Type> --addToAllowlist=<Value>**
- Removing from allow list
  - **mfa-server-cli mfa-manage --allowListType=<Type> --removeFromAllowlist=<Value>**
- Print Allow list
  - **mfa-server-cli mfa-manage --printAllowlist=yes**

MFA Allow List commands Examples

- **Example to add user to Allow list**
  - mfa-server-cli mfa-manage --allowListType=user --addToAllowlist=cn=user,ou=ot,o=mf
  - mfa-server-cli mfa-manage --allowListType=user --addToAllowlist=win2k22dom\\aduser
- **Example to add IP address of client in allow list**
  - mfa-server-cli mfa-manage --allowListType=address --addToAllowlist=164.99.110.50
- **Example to add IP range to Allow list**
  - mfa-server-cli mfa-manage --allowListType=range --addToAllowlist=164.99.110.50-164.99.110.52
- **Example to add subnet to Allow list**
  - mfa-server-cli mfa-manage --allowListType=subnet --addToAllowlist=164.99.110.0/23
- **Example to add group to Allow list**
  - mfa-server-cli mfa-manage --allowListType=usergroup --addToAllowlist=cn=group,o=opentext
  - mfa-server-cli mfa-manage --allowListType=usergroup --addToAllowlist=win2k22dom\\adgroup

More Information

https://www.microfocus.com/documentation/open-enterprise-server/24.4/inst_oes_lx/mfa-server.html

Open Enterprise Server

twitter.com/opentext

linkedin.com/company/opentext

opentext.com


opentext™