



**Computação Científica Nacional
FCCN**

eduVPN com Autenticação Federada

Instalação e Configuração
eduVPN e Shibboleth Service Provider

2020/03/23

Versão 2.0

eduvpn@fccn.pt

Índice

Índice	2
1. ENQUADRAMENTO	3
2. INTRODUÇÃO	3
3. REQUISITOS.....	4
4. INSTALAÇÃO eduVPN	5
5. CONFIGURAR AUTENTICAÇÃO	11
5.1 AUTENTICAÇÃO LDAP.....	11
5.2 AUTENTICAÇÃO FEDERADA	11
5.2.1 INSTALAÇÃO DO SHIBBOLETH SERVICE PROVIDER	11
5.2.2 CONFIGURAÇÃO SHIBBOLETH SERVICE PROVIDER	13
5.2.2.1 CONFIGURAÇÃO SHIBBOLETH2.XML	14
5.2.3 eduVPN ACTIVAR AUTENTICAÇÃO SAML	15
5.2.4 CONFIGURAÇÃO NO FORNECEDOR DE IDENTIDADE.....	16
6 INSTALAR CLIENTE E LIGAR VPN.....	18

1. ENQUADRAMENTO

No contexto atual da pandemia COVID-19 em que o estudo e trabalho à distância assumem um papel cada vez mais importante, o acesso a recursos moderado através de aplicações VPN (Virtual Private Network) encontra-se sobre grande pressão.

Historicamente, os acessos VPN por serem um recurso limitado são apenas atribuídos a utilizadores que se encontrem em situações específicas. Com o alargar da necessidade a um número maior de utilizadores, a gestão do acesso VPN torna-se mais complexo.

A questão da escala coloca pressão na disponibilidade/capacidade do hardware existente, e no caso de existir uma limitação de licenças, será o orçamento de cada instituição a sofrer com a necessidade de aumentar bruscamente o número de licenças adquiridas a um determinado fabricante. É por isso importante explorar soluções alternativas, que permitam uma rápida implantação e que eventualmente possam funcionar em paralelo com as existentes. Neste contexto surge o projeto eduVPN, que é uma das atividades GÉANT. Este projeto disponibiliza uma APP que já está presente na Apple Store (macOS e iOS), no Google Play e na Microsoft Store.

Este documento técnico serve assim para que as instituições de forma autónoma, possam realizar a implantação dos seus concentradores EDUVPN de forma a compatibilizá-los com a arquitetura das suas redes privadas locais, onde depois facultam o acesso a serviços internos, com recurso a autenticação federada com as credenciais de cada instituição de origem.

2. INTRODUÇÃO

Este tutorial destina-se a administradores de sistema com conhecimentos em sistemas do tipo Unix/Linux, sintaxe XML, Servidores Web Apache e SSL e descreve o processo de instalação e configuração do serviço de VPN eduVPN versão 2.0, bem como o processo de integração da autenticação federada através da instalação e configuração de um fornecedor de serviço “*Shibboleth Service Provider*” versão 3.0.

De salientar, que algumas imagens neste documento refletem o exemplo da instalação do eduVPN para a FCCN (eduvpn.id.fccn.pt) e que nos exemplos onde é utilizado o “eduvpn.meu-dominio.pt” devem adaptar de acordo com a instalação para a vossa instituição.

Neste enquadramento o software eduVPN suporta as seguintes características:

- Suporta por completo IPv6 (não sendo possível desabilitar esta versão do protocolo);
- Suporta NAT ou endereçamento IP público;
- Possui um portal para os utilizadores gerirem as suas configurações dos seus dispositivos;
- Possui um portal de administração para gerir os utilizadores e ligações;
- Suporta vários modos de autenticação: Local, LDAP, RADIUS ou SAML;
- Disponibilização de cliente multiplataforma.

Para mais informações sobre os vários clientes já suportados consulte <https://app.eduvpn.org/>

Apps

Use the applications below to connect to your eduVPN server. See app.eduvpn.org for a full list of applications and release notes.

To use eduVPN, download the app for your device below!

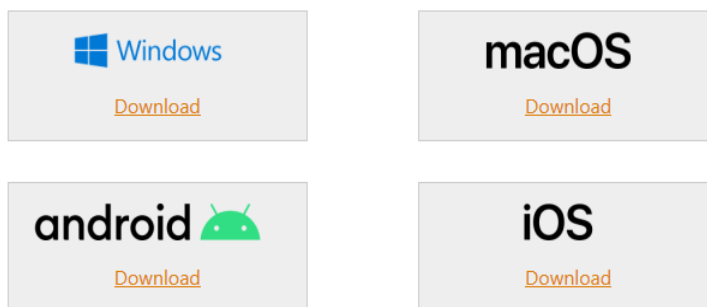


Figura 1 – eduVPN applications

3. REQUISITOS

O software eduVPN suporta vários sistemas operativos, no entanto este documento reflete a instalação num servidor Centos Linux 7.x 64-bit. Mais em: <https://github.com/eduvpn/documentation#supported-operating-systems>

Para uma instalação bem sucedida devem ser garantidos os seguintes requisitos:

- Servidor com um mínimo de 4 Cores e 4GB de RAM
- SELinux ativo (CentOS SELinux)
- Fixar endereçamento IPv4 e IPv6 (público) na interface externa;
- Permitir acessos a: tcp/80, tcp/443, udp/1194, tcp/1194 (O script de instalação, aplica as regras na firewall do sistema operativo);
- Definir o IP do DNS (*resolver*) para o servidor VPN
- Instalação do pacote de “software” NTP para garantir a sincronização de relógio do servidor. É essencial que um SP mantenha o relógio sincronizado, as mensagens de SAML incluem *timestamps* que são verificados pelos Fornecedores de Identidade (IdP's). Quando o atraso é superior a 5 minutos as mensagens são recusadas e os utilizadores impedidos de aceder

4. INSTALAÇÃO eduVPN

Executar os seguintes comandos no servidor a instalar:

```
$ curl -L -O https://github.com/eduvpn/documentation/archive/v2.tar.gz  
  
$ tar -xzf v2.tar.gz  
  
$ cd documentation-2
```

Assegurar que o SELinux se encontra ativo antes da execução do script de instalação.

Executar o script **deploy_centos.sh** como root

```
sudo -s  
  
# ./deploy_centos.sh
```

Durante a execução do script é necessário indicar alguma informação de configuração, como por exemplo a definição do *hostname* do Servidor VPN. Poderá ser definido o mesmo para a componente WebServer e para o OpenVPN Server, isto no caso de usar uma máquina para as duas funções.

```
[root@alali documentation-2]# ./deploy_centos.sh  
DNS name of the Web Server [alali.corp.fccn.pt]: eduvpn.ip.fccn.pt  
DNS name of the OpenVPN Server [eduvpn.ip.fccn.pt]:
```

NOTA: Não usar “localhost” como hostname ou um IP

Resumo da instalação e respetivas dependências:

```
Installed:
  vpn-server-api.noarch 0:2.1.2-1.el7
  vpn-server-node.noarch 0:2.1.1-1.el7
  vpn-user-portal.noarch 0:2.1.6-1.el7

Dependency Installed:
  libyaml.x86_64 0:3.5.12-1.el7
  php-IC-openvpn-connection-manager.noarch 0:1.0.3-2.el7
  php-fkooman-jwt.noarch 0:1.0.1-1.el7
  php-fkooman-secokie.noarch 0:2.0.1-8.el7
  php-mbstring.x86_64 0:5.4.16-46.1.el7_7
  php-pdo.x86_64 0:5.4.16-46.1.el7_7
  pkcs11-helper.x86_64 0:1.11-3.el7
  libsodium.x86_64 0:1.0.18-1.el7
  php-PsrLog.noarch 0:1.1.0-1.el7
  php-fkooman-oauth2-server.noarch 0:6.0.0-1.el7
  php-fkooman-sqlite-migrate.noarch 0:0.1.1-4.el7
  php-paragonie-constant-time-encoding.noarch 0:1.0.4-2.el7
  php-pest-libsodium.x86_64 0:1.0.7-1.el7
  t1lib.x86_64 0:5.1.2-14.el7
  openvpn.x86_64 0:2.4.8-1.el7
  php-bacon-qr-code.noarch 0:1.0.3-1.el7
  php-fkooman-otp-verifier.noarch 0:0.3.1-1.el7
  php-gd.x86_64 0:5.4.16-46.1.el7_7
  php-paragonie-random-compat.noarch 0:2.0.18-1.el7
  php-pest-radius.x86_64 0:1.3.0-1.el7
  php-IC-common.noarch 0:2.1.0-1.el7
  php-fedora-autoloader.noarch 0:1.0.0-1.el7
  php-fkooman-saml-sp.noarch 0:0.2.2-1.el7
  php-ldap.x86_64 0:5.4.16-46.1.el7_7
  php-password-compat.noarch 0:1.0.4-1.el7
  php-symfony-polyfill.noarch 0:1.5.0-1.el7

Complete!
IPv4 CIDR : 10.126.100.0/25
IPv6 prefix: fde8:744a:162a:6d3f::/64
DNS : 10.0.0.220, 10.0.0.221, 10.0.0.222
* Applying /usr/lib/sysetd.d/00-system.conf ...
* Applying /usr/lib/sysetd.d/10-default-yama-scope.conf ...
kernel.yama.ptrace_scope = 0
* Applying /usr/lib/sysetd.d/50-default.conf ...
kernel.sysrq = 16
kernel.core_uses_pid = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.promote_secondaries = 1
net.ipv4.conf.all.promote_secondaries = 1
fs.protected_hardlinks = 1
fs.protected_symlinks = 1
* Applying /etc/sysetd.d/70-vpn.conf ...
net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding = 1
* Applying /etc/sysetd.d/99-sysetd.conf ...
net.ipv4.conf.all.arp_notify = 1
* Applying /etc/sysetd.conf ...
net.ipv4.conf.all.arp_notify = 1
Generating a 2048 bit RSA private key
.....+++
```

```
#####  
# Portal  
#   https://eduvpn.id.fccn.pt/  
#   Regular User: demo  
#   Regular User Pass: choo9Ceijohb  
#  
#   Admin User: admin  
#   Admin User Pass: Chac3akooophe  
#####
```

Após a conclusão da instalação, é importante ter conhecimento da seguinte informação:

- **DOCUMENTAÇÃO OFICIAL DO EDUVPN**

- <https://github.com/eduvpn/documentation>
- <https://www.eduvpn.org/blog/>

- **INSTALAÇÃO EM GRANDE ESCALA**

- Para instalações em grande escala quando se prevê um grande numero de ligações VPN em simultâneo ou instalação de Servidores VPN em diferentes zonas geográficas consultar link: <https://www.eduvpn.org/blog/does-it-scale.html>

- **FIREWALL**

Por padrão, não há firewall entre o cliente VPN e o servidor VPN. Para o caso de querer usar a mesma interface para aceder por SSH ao servidor para fins de gestão, deve ser feita uma restrição adicional na firewall da máquina (no exemplo apenas os blocos 10.0.0.0/8 e fd00::/8 passam a ser autorizados).

```
// Only allow SSH access from 10.0.0.0/8 & fd00::/8  
// Make sure to remove 22 from "dst_port" in above rule  
[  
  'proto' => ['tcp'],  
  'src_net' => [  
    '10.0.0.0/8',  
    'fd00::/8',  
  ],  
  'dst_port' => [  
    22,      // SSH  
  ],  
],
```

Ver mais aqui: <https://github.com/eduvpn/documentation/blob/v2/FIREWALL.md>

- **FUTURAS ACTUALIZAÇÕES**

Para manter o eduVPN atualizado, basta correr:

```
sudo ./documentation-2/update_system_centos.sh
```

- **REINICIAR SERVIÇOS**

Executar o seguinte comando:

```
sudo ./documentation-2/apply_changes.sh
```

- **FICHEIROS LOG IMPORTANTES**

```
# mensagens de logging  
/var/log/messages  
  
# mensagens de logging httpd  
/var/log/httpd/  
  
# eventos de segurança  
/var/log/secure
```

- **ACTUALIZAR CERTIFICADO DO SERVIDOR WEB APACHE**

O serviço deve utilizar um certificado válido emitido por uma entidade certificadora reconhecida. Um certificado reconhecido garante aos utilizadores que o website é seguro e confiável através da criação de um canal criptográfico entre o servidor web e um navegador (browser).

1ª Passo - Gerar o Certificate Signing Request (CSR)

- ✓ Aceder à pasta **/etc/pki/tls/certs**

```
cd /etc/pki/tls/certs
```

- ✓ Execute o seguinte comando (exemplo, o que está a bold na caixa seguinte deve ser substituído face ao contexto da sua organização) na pasta **/etc/pki/tls/certs/**

```
openssl req -new -newkey rsa:2048 -nodes -out edupvpn_meu-dominio_pt.csr  
-keyout edupvpn_meu-dominio_pt.key -subj  
"/C=PT/ST=Lisboa/L=Lisboa/O=NOME DA MINHA ORGANIZAÇÃO/CN=edupvpn.meu-  
dominio.pt"
```

Para as instituições aderentes do Serviço RCTS Certificados é obrigatório que o campo "O" seja preenchido com o Nome da Organização registado no Protocolo RCTS Certificados. Devem ainda alterar o campo CN para corresponder ao hostname do serviço a integrar.

+ informações: [Serviço RCTS Certificados](#)

Após a execução deste comando são gerados dois ficheiros (os nomes serão distintos, adequando à sua organização):

- `eduvpn_meu-dominio_pt.key`: corresponde à chave Privada do Certificado
- `eduvpn_meu-dominio_pt.csr`: este ficheiro é utilizado para realizar o pedido de emissão de certificado.

✓ Coloque a chave privada na pasta `/etc/pki/tls/private`

```
mv eduvpn_meu-dominio_pt.key /etc/pki/tls/private
```

2ª Passo - Pedido de certificado na Digicert

As instituições aderentes ao serviço RCTS Certificados devem identificar o responsável da sua instituição pela emissão de certificados, para que o mesmo possa realizar o pedido no portal da Digicert (www.digicert.com). De salientar, que o pedido de certificados através da Digicert é possível até à data de 30 de abril de 2020. O serviço RCTS Certificados está em fase de mudança da entidade Certificadora. Para mais informação, consulte o espaço do [Serviço RCTS Certificados](#).

Após a emissão do certificado, receberá os seguintes ficheiros:

- `DigiCertCA.crt`
- `eduvpn_meu-dominio_pt.crt`

Grave os ficheiros na seguinte localização: `/etc/pki/tls/certs/`

Para validar o conteúdo do certificado gerado:

```
openssl x509 -in /etc/pki/tls/certs/eduvpn_meu-dominio_pt.crt -text -noout
```

Fingerprint do certificado:

```
openssl x509 -in /etc/pki/tls/certs/eduvpn_meu-dominio_pt.crt -fingerprint -sha1 -noout
```

3ª Passo Actualizar VirtualHost

Actualizar a configuração do VirtualHost para o serviço no ficheiro `/etc/httpd/conf.d/eduvpn.meu-dominio.conf`.

```
<VirtualHost *:443>
    ServerName https://eduvpn.meu-dominio.pt:443
    UseCanonicalName on
```



```
LogLevel warn
ErrorLog logs/eduvpn.meu-dominio.pt_ssl_error_log
# Do not log (valid) web browser requests
#TransferLog logs/eduvpn.meu-dominio.pt_ssl_access_log

SSLEngine on
    SSLProtocol all -SSLv2 -SSLv3
    SSLCipherSuite ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-
POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-
RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-
ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-
AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-
SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE-ECDSA-
DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-
SHA256:AES128-SHA:AES256-SHA:!DSS
    SSLHonorCipherOrder on
    SSLCompression off
    SSLCertificateKeyFile /etc/pki/tls/private/eduvpn_meu-dominio_pt.key
    SSLCertificateFile /etc/pki/tls/certs/eduvpn_meu-dominio_pt.crt
    SSLCertificateChainFile /etc/pki/tls/certs/DigiCertCA.crt

# Security Headers
Header always set Strict-Transport-Security "max-age=15768000"

# Redirect requests to the portal (302)
RewriteEngine on
RewriteRule    "^/$"    "/vpn-user-portal/"    [R]

<Location /vpn-user-portal>
    AuthType shibboleth
    ShibRequestSetting requireSession true
    Require shibboleth
</Location>

# disable Shibboleth for the API
<Location /vpn-user-portal/api.php>
    ShibRequireSession Off
</Location>

# disable Shibboleth for the OAuth Token Endpoint
<Location /vpn-user-portal/oauth.php>
    ShibRequireSession Off
</Location>

<VirtualHost>
```

Adicionar as seguintes opções (para que não anuncie detalhes da versão) no ficheiro /etc/httpd/conf/httpd.conf

```
ServerTokens Prod
ServerSignature off
```

Para efetuar um redirecionamento de pedidos vindos por http para https deverá adicionar ao ficheiro /etc/httpd/conf/httpd.conf o seguinte conteúdo:

```
RewriteEngine On
```

```
RewriteCond %{HTTPS} !=on  
RewriteRule ^/?(.*) https://%{SERVER_NAME}/$1 [R,L]
```

Ativar o serviço HTTP e validar as configurações com os seguintes comandos:

```
sudo systemctl enable httpd.service  
sudo apachectl configtest
```

Após as configurações realizar um restart do serviço apache, utilizando o seguinte comando:

```
sudo systemctl restart httpd.service
```

Para avaliar a instalação deve aceder via browser ao endereço definido no processo de instalação e utilizar as respetivas credenciais.

- Acesso ao website <https://eduvpn.meu-dominio.pt>

Sign In

Please sign in with your username and password.

5. CONFIGURAR AUTENTICAÇÃO

O portal eduVPN permite a integração da autenticação RADIUS, LDAP e SAML. No entanto, apenas é permitido ativar um método de autenticação no ficheiro de configuração. Nesta secção são apenas detalhadas as configurações da autenticação LDAP e SAML.

5.1 AUTENTICAÇÃO LDAP

Para ativar a autenticação via LDAP no portal VPN é necessário aceder ao ficheiro de configuração **/etc/vpn-user-portal/config.php** e alterar os seguintes parâmetros:

```
...  
  
'authMethod' => 'FormLdapAuthentication',  
  
'FormLdapAuthentication' =>  
    array (  
        'ldapUri' => 'ldaps://<IP DO LDAP>',  
        'bindDnTemplate' => 'meu-dominio\{{UID}}',  
        'userFilterTemplate' => '(sAMAccountName={{OpenVPN}})',  
        'permissionAttribute' => 'memberOf',  
        'baseDn' => 'OU=AAA,DC=meu-dominio,DC=pt',  
    ),  
    ...  
  
    ...
```

+Informações: [LDAP](#)

5.2 AUTENTICAÇÃO FEDERADA

A autenticação federada via SAML pode ser configurada utilizando Shibboleth ou mod_auth_mellon. Nesta secção é apenas detalhada a configuração SAML através da instalação e configuração do “Shibboleth Service Provider” versão 3.0. Para mais informações sobre a configuração mod_auth_mellon consulte o link: [MOD AUT MELLON](#).

5.2.1 INSTALAÇÃO DO SHIBBOLETH SERVICE PROVIDER

O projeto Shibboleth tem o seu próprio repositório que fornece os binários oficiais do Shibboleth Service Provider e suas dependências para distribuições Linux baseadas em RPM. Este repositório contém a versão atualizada do Fornecedor de Serviço Shibboleth SP. É recomendada a utilização dos pacotes deste repositório em detrimento dos que podem ser fornecidos pela distribuição do sistema operativo.

```
sudo curl -o /etc/yum.repos.d/security:shibboleth.repo  
http://download.opensuse.org/repositories/security:/shibboleth/CentOS\_7/security:shibboleth.repo
```

Para instalar o Shibboleth SP deve executar o seguinte comando:

```
sudo yum install shibboleth.x86_64
```

Se for pedido para confirmar se quer realmente instalar o Shibboleth e todas as suas dependências, responda com 'Y' para sim.

Após a instalação do pacote do Fornecedor de serviço é necessário efetuar um start e enable do daemon shibd:

```
sudo systemctl enable shibd.service  
sudo systemctl start shibd.service
```

Diretorias disponíveis após instalação

Após a instalação do Fornecedor de Serviço Shibboleth (SP) foram criadas as seguintes diretorias:

- ✓ **/etc/shibboleth**

Diretoria que contém os ficheiros de configuração do Shibboleth SP. O principal ficheiro de configuração é shibboleth2.xml.

- ✓ **/var/log/shibboleth**

Diretoria onde são armazenados os logs. O ficheiro de log mais importante é o shibd.log.

- ✓ **/run/shibboleth**

É a diretoria de Runtime onde os ID e os ficheiros de socket dos processos são guardados.

- ✓ **/var/cache/shibboleth**

Diretoria de cache onde são armazenados os ficheiros de backup da metadata e a listagem de certificados revogados pelo serviço SP.

Após a instalação execute os seguintes testes para validar a correta instalação do Fornecedor de Serviços:

- **Validar Shibboleth SP**

Execute o seguinte comando de forma a validar se o SP consegue efetuar o carregamento da configuração:

```
sudo shibd -t
```

É importante a última linha do output ser:

```
overall configuration is loadable, check console for non-fatal problems
```

As mensagens de nível de log WARN geralmente não são um problema, mas é necessário examinar o seu aparecimento.

▪ Teste mod_shib

Reinicie o web server

```
sudo systemctl restart httpd.service
```

Aceda ao URL: <https://eduvpn.meu-dominio.pt/Shibboleth.sso/Session>

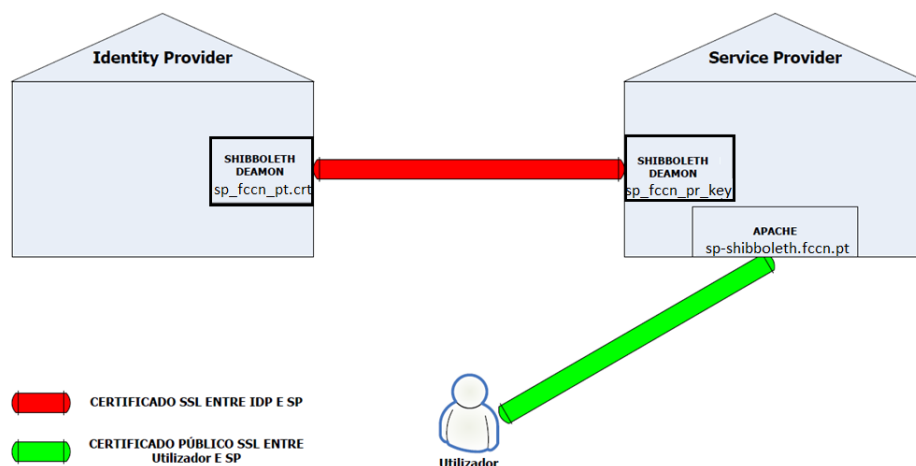
O web server (respetivamente o módulo Shibboleth) deverá retornar uma página com o seguinte:

A valid session was not found.

Esta mensagem mostra que o módulo Shibboleth se encontra carregado pelo web server e está a comunicar com o processo shibd.

5.2.2 CONFIGURAÇÃO SHIBBOLETH SERVICE PROVIDER

Apesar de tecnicamente possível que o software do SP utilize o mesmo par de chaves e certificados do Web Server para comunicar com o Fornecedor de Identidade, não é recomendado que sejam utilizadas as mesmas por razões de segurança.



Como tal, devem ser assegurados certificados distintos para o Servidor Web Apache e Shibboleth SP. O daemon Shibboleth (shibd) necessita de um certificado X.509 para assinar e cifrar mensagens SAML. É recomendado usar um certificado *self-signed* (auto-assinado), que é configurado de forma independente ao certificado SSL/TLS utilizado pelo web server.

Para gerar um novo certificado e a chave privada execute o seguinte comando:

```
sudo /etc/shibboleth/keygen.sh -f -u shibd -h sp-eduvpn-id.meu-dominio.pt  
-y 3 -e https://sp-eduvpn-id.meu-dominio.pt -o /etc/shibboleth/
```

5.2.2.1 CONFIGURAÇÃO SHIBBOLETH2.XML

O ficheiro principal de configuração do SP encontra-se no ficheiro `/etc/shibboleth/shibboleth2.xml` onde é necessário configurar os seguintes elementos:

- **<ApplicationDefaults .../>**

Este elemento é responsável por mapear os serviços por hostname onde o “*Service Provider*” controla o acesso.

```
<ApplicationDefaults entityID="https://eduvpn.meu-dominio.pt"  
REMOTE_USER="epn subject-id pairwise-id persistent-id"
```

- **<Sessions ../>**

Este elemento é responsável pela configuração das sessões estabelecidas com o “*Service Provider*”. Deve ser alterado o parâmetro `handleSSL` e `cookieProps` de acordo com o seguinte exemplo:

```
<Sessions lifetime="28800" timeout="3600" relayState="ss:mem"  
checkAddress="false" handlerSSL="true" cookieProps="https">
```

- **<SSO entityID .../>**

Este elemento é responsável por identificar o Fornecedor de Identidade para o qual o serviço deve redirecionar os utilizadores que não se encontram autenticados. É necessário alterar o parâmetro `entityID` para o identificador do Fornecedor de Identidade da vossa instituição e alterar o valor para SAML2 de acordo com o exemplo abaixo.

```
<SSO entityID="https://idp.meu-dominio.pt/idp/shibboleth">SAML2</SSO>
```

- **<MetadataProvider .../>**

Este elemento é responsável por identificar o ficheiro de metadados do Fornecedor de Identidade configurado no `<SSO entityID >`.

Alterar o elemento `<MetadataProvider` no ficheiro `shibboleth2.xml` com o seguinte conteúdo:

```
<MetadataProvider type="XML" validate="true" path="idp-meu-dominio-  
metadata.xml"/>
```

Na pasta **/etc/shibboleth/** é necessário criar o ficheiro **idp-meu-dominio-metadata.xml** que deve conter a informação de metadados do respetivo Fornecedor de identidade da instituição.

Após estas alterações deve reiniciar o Service Provider.

```
sudo systemctl restart shibd.service
```

Verifique o log para despiste de eventuais erros.

```
tail -f /var/log/shibboleth/shibd.log
```

5.2.3 eduVPN ACTIVAR AUTENTICAÇÃO SAML

Para ativar a autenticação federada no portal VPN é necessário aceder ao ficheiro de configuração **/etc/vpn-user-portal/config.php** e alterar e adicionar os seguintes parâmetros:

```
...  
'authMethod' => 'ShibAuthentication',  
...  
...  
'ShibAuthentication' => [  
    'userIdAttribute' => 'eduPersonPrincipalName',  
    'permissionAttribute' => 'entitlement',  
],  
'adminPermissionList' => ['http://eduvpn.org/permission/admin'],  
...  
...
```

Para que um utilizador tenha permissões de administrador no portal eduVPN é necessário que o atributo “entitlement” enviado pelo Fornecedor de identidade da instituição se encontre preenchido com o valor **http://eduvpn.org/permission/admin**.

É também permitido identificar os administradores do portal através do parâmetro “adminUserIdList” onde é necessário adicionar individualmente o ID do utilizador que nesta configuração corresponde ao valor do atributo “**eduPersonPrincipalName**”.

Para adicionar um utilizador é necessário adicionar no ficheiro de configuração `/etc/vpn-user-portal/config.php` o parâmetro `adminUserIdList` e preencher o array com os UserID dos utilizadores que devem ter acesso de administrador.

```
...  
'authMethod' => 'ShibAuthentication',  
...  
...  
'ShibAuthentication' => [  
    'userIdAttribute' => 'eduPersonPrincipalName',  
    'permissionAttribute' => 'entitlement',  
],  
'adminPermissionList' => ['http://eduvpn.org/permission/admin'],  
'adminUserIdList' =>  
    array (  
        0 => 'user_A@meu-dominio.pt',  
        1 => 'user_B@meu-dominio.pt',  
    ),  
...  
...
```

Para garantir o correto mapeamento dos atributos é necessário validar a existência das seguintes definições no ficheiro `/etc/shibboleth/attribute-map.xml`

```
...  
<!-- The SAML 2.0 NameID Format: -->  
  
<Attribute name="urn:mace:dir:attribute-def:eduPersonPrincipalName"  
id="eduPersonPrincipalName">  
    <AttributeDecoder xsi:type="ScopedAttributeDecoder" caseSensitive="false"/>  
</Attribute>  
  
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7" id="entitlement"/>  
    <Attribute name="urn:mace:dir:attribute-def:eduPersonEntitlement"  
id="entitlement"/>  
...  
...
```

5.2.4 CONFIGURAÇÃO NO FORNECEDOR DE IDENTIDADE

A autenticação no fornecedor de identidade obriga à integração dos metadados do serviço e configuração dos atributos necessários para autorização no eduVPN.

Para obter informação de metadados do serviço é necessário aceder ao seguinte url:

- <https://eduvpn.meu-dominio.pt/Shibboleth.sso/Metadata>

A informação de metadados do serviço deve ser copiado para um ficheiro **eduvpn.xml** na seguinte localização do fornecedor de identidade: **/opt/shibboleth-idp/metadata/**

No ficheiro **/opt/shibboleth-idp/conf/metadata-providers.xml** é necessário adicionar a seguinte linha:

```
<MetadataProvider id="LocalMetadata" xsi:type="FilesystemMetadataProvider"
metadataFile="%{idp.home}/metadata/eduvpn.xml"/>
```

Os atributos a libertar pelo fornecedor de Identidade ao serviço são os seguintes:

- [eduPersonPrincipalName](#)
- [entitlement](#)

Adicionar no ficheiro **/opt/shibboleth-idp/conf/attribute-filter.xml** a seguinte configuração:

```
<AttributeFilterPolicy id="eduVPNs">
<PolicyRequirementRule xsi:type="Requester" value="https://eduvpn.meu-dominio.pt"
/>

<AttributeRule attributeID="eduPersonEntitlement">
<PermitValueRule xsi:type="Value" value="http://eduvpn.org/permission/admin"
ignoreCase="true"/>
</AttributeRule>

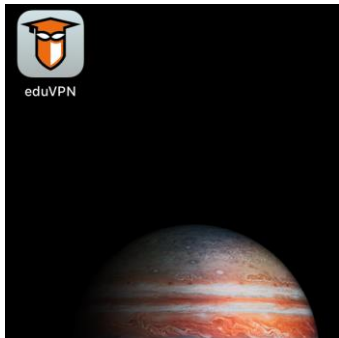
<AttributeRule attributeID="eduPersonPrincipalName">
<PermitValueRule xsi:type="ANY"/>
</AttributeRule>

</AttributeFilterPolicy>
```

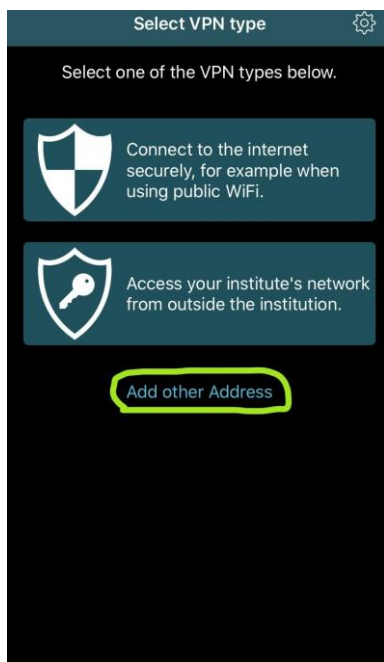
6 INSTALAR CLIENTE E LIGAR VPN

Esta secção descreve os passos necessário para ativar o acesso à VPN num ambiente IOs:

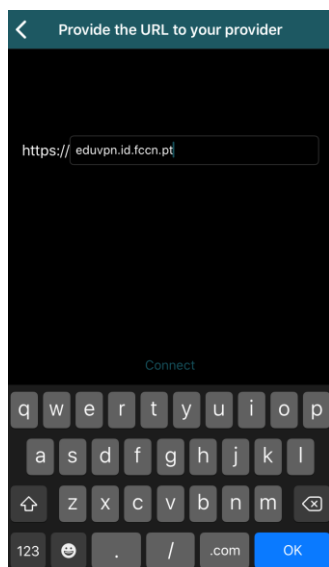
PASSO 1 - Instalação do cliente e abrir a aplicação (Clientes disponíveis em <https://app.eduvpn.nl>)



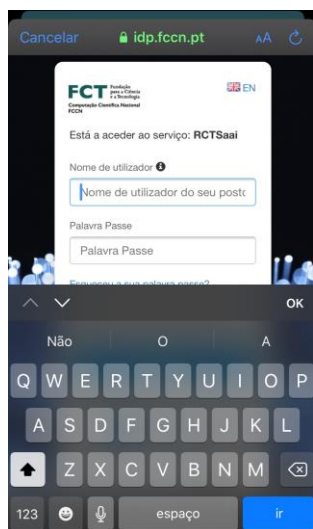
PASSO 2 - Selecionar “Add other Address”



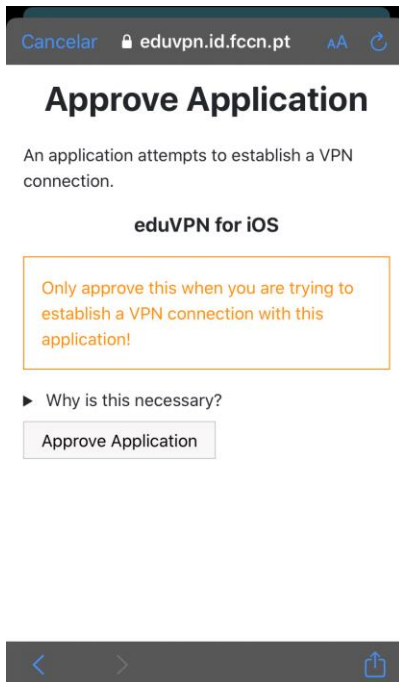
PASSO 3 - Introduzir o endereço da VPN de acordo com a instalação: eduvpn.meu-dominio.pt



PASSO 4 – Autenticar utilizando a conta institucional no Fornecedor de Identidade da sua Instituição



PASSO 5 - Aprovação da utilização de VPN no IOs



PASSO 6 – Ligação estabelecida

