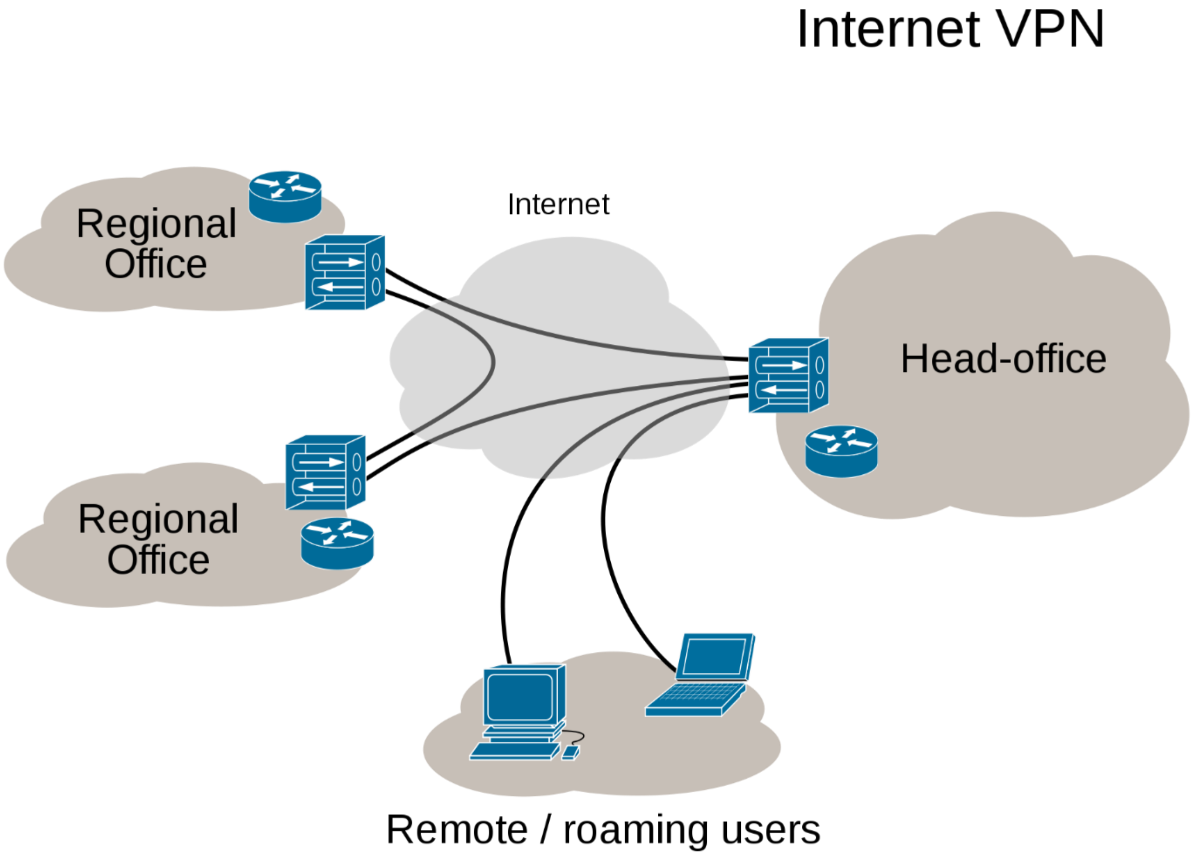
SSL-VPN (Web-Mode)

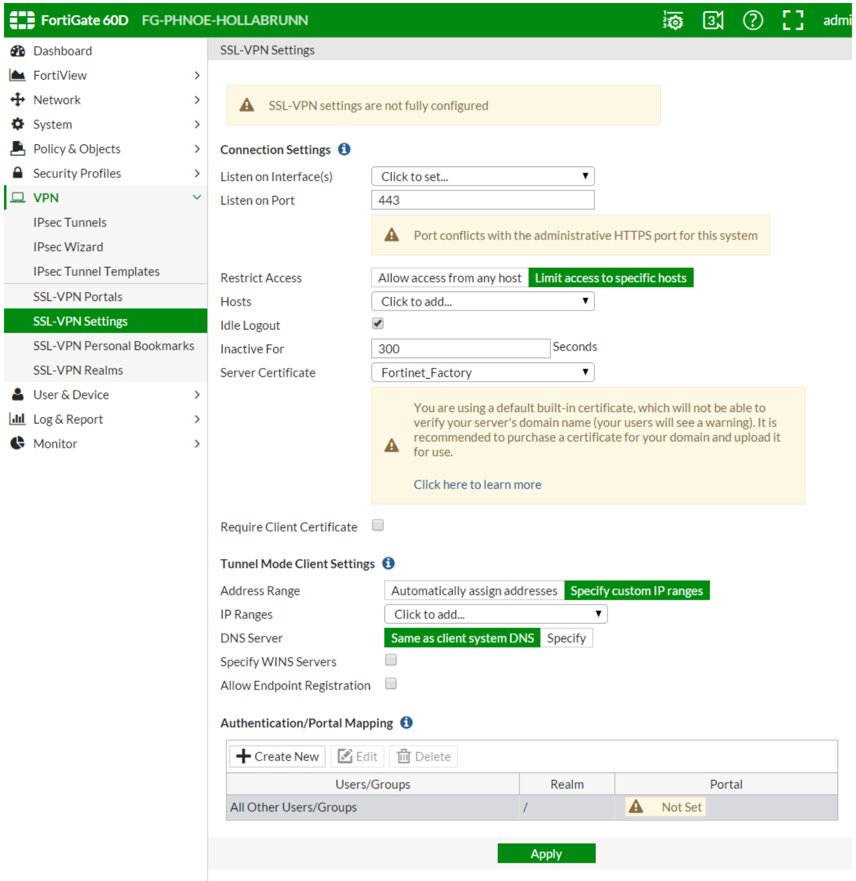


VPN Typen

- Site-to-Site
  - meist mit IPSec
  - eigenes Protokoll
  - spezielle Ports
- Road Warrior
  - IPSec auch möglich (Nachteile!)
  - SSL-VPN
    - Port 443 (=https)

SSL-VPN Portal auf Fortigate

- SSL-VPN Settings
  - Interface festlegen
  - Konflikt Management-Port!
  - Zertifikat
  - DHCP für VPN
  - User / Gruppen



SSL-VPN Settings

SSL-VPN settings are not fully configured

Connection Settings

Listen on Interface(s): Click to set...

Listen on Port: 443

Port conflicts with the administrative HTTPS port for this system

Restrict Access: Allow access from any host | Limit access to specific hosts

Hosts: Click to add...

Idle Logout: ☑

Inactive For: 300 Seconds

Server Certificate: Fortinet_Factory

You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and upload it for use.

Click here to learn more

Require Client Certificate: □

Tunnel Mode Client Settings

Address Range: Automatically assign addresses | Specify custom IP ranges

IP Ranges: Click to add...

DNS Server: Same as client system DNS | Specify

Specify WINS Servers: □

Allow Endpoint Registration: □

Authentication/Portal Mapping

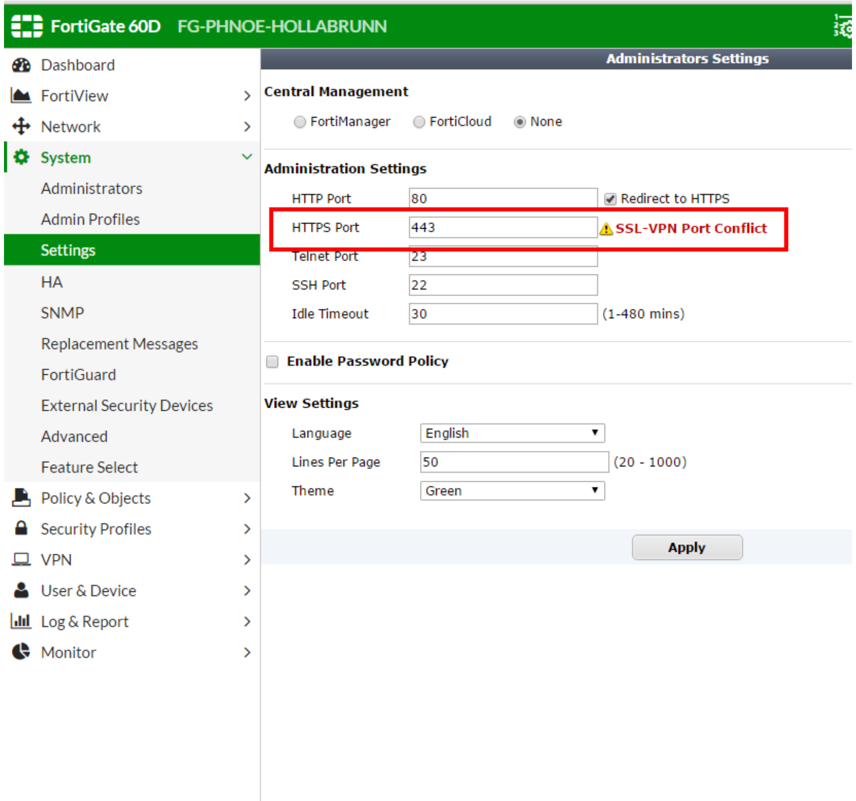
+ Create New | Edit | Delete

Users/Groups	Realm	Portal
All Other Users/Groups	/	Not Set

Apply

Management-Port verlegen

- SSL-VPN wird auf WAN Schnittstelle angeboten
  - Management auf WAN abdrehen
  - oder
  - Management auf WAN auf anderen Port verlegen



Administrators Settings

Central Management

○ FortiManager ○ FortiCloud ● None

Administration Settings

HTTP Port: 80 ☑ Redirect to HTTPS

HTTPS Port: 443 ⚠ SSL-VPN Port Conflict

Telnet Port: 23

SSH Port: 22

Idle Timeout: 30 (1-480 mins)

□ **Enable Password Policy**

View Settings

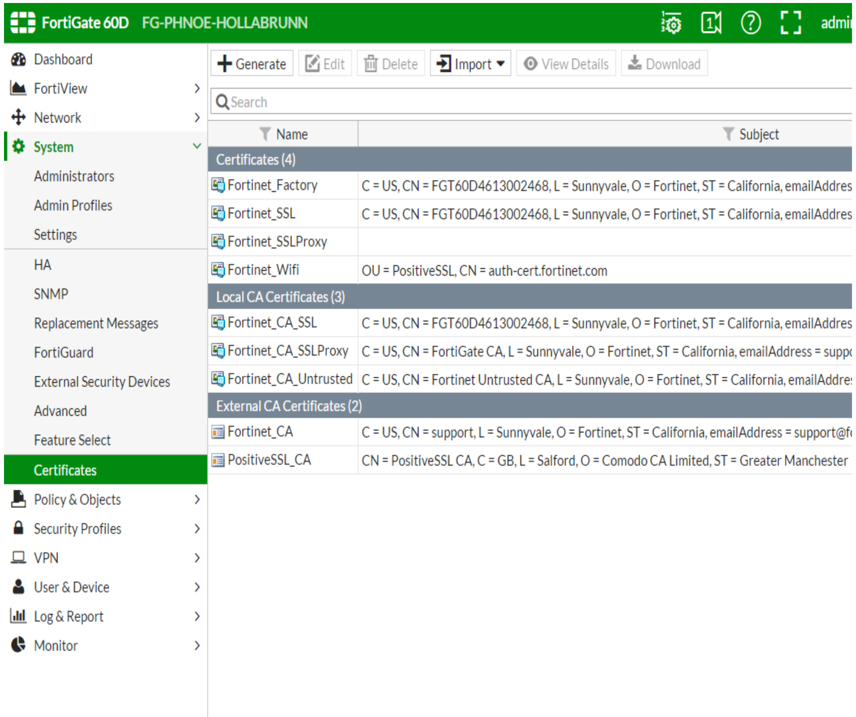
Language: English

Lines Per Page: 50 (20 - 1000)

Theme: Green

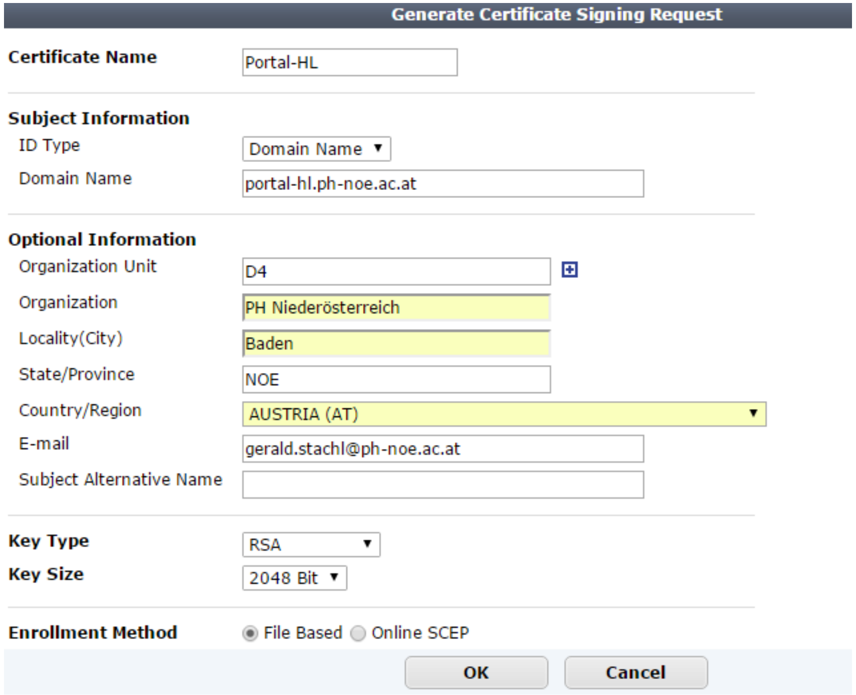
optional: Zertifikat importieren

- Feature Select:
  - Certificates aktivieren
- lokale Zertifikat generieren
- CSR signieren lassen
- Import
- VPN Settings: offizielles Zertifikat auswählen



Name	Subject
Certificates (4)	
Fortinet_Factory	C = US, CN = FGT60D4613002468, L = Sunnyvale, O = Fortinet, ST = California, emailAddres
Fortinet_SSL	C = US, CN = FGT60D4613002468, L = Sunnyvale, O = Fortinet, ST = California, emailAddres
Fortinet_SSLProxy	
Fortinet_Wifi	OU = PositiveSSL, CN = auth-cert.fortinet.com
Local CA Certificates (3)	
Fortinet_CA_SSL	C = US, CN = FGT60D4613002468, L = Sunnyvale, O = Fortinet, ST = California, emailAddres
Fortinet_CA_SSLProxy	C = US, CN = FortiGate CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = suppo
Fortinet_CA_Untrusted	C = US, CN = Fortinet Untrusted CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddre
External CA Certificates (2)	
Fortinet_CA	C = US, CN = support, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@f
PositiveSSL_CA	CN = PositiveSSL CA, C = GB, L = Salford, O = Comodo CA Limited, ST = Greater Manchester

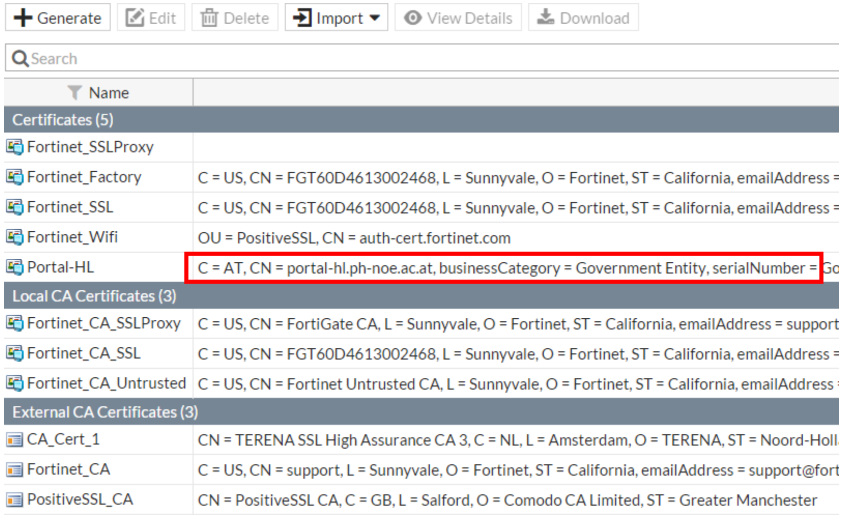
Zertifikat erzeugen



Generate Certificate Signing Request

Certificate Name	Portal-HL
Subject Information	
ID Type	Domain Name ▼
Domain Name	portal-hl.ph-noe.ac.at
Optional Information	
Organization Unit	D4 ⊞
Organization	PH Niederösterreich
Locality(City)	Baden
State/Province	NOE
Country/Region	AUSTRIA (AT) ▼
E-mail	gerald.stachl@ph-noe.ac.at
Subject Alternative Name	
Key Type	RSA ▼
Key Size	2048 Bit ▼
Enrollment Method	● File Based ○ Online SCEP

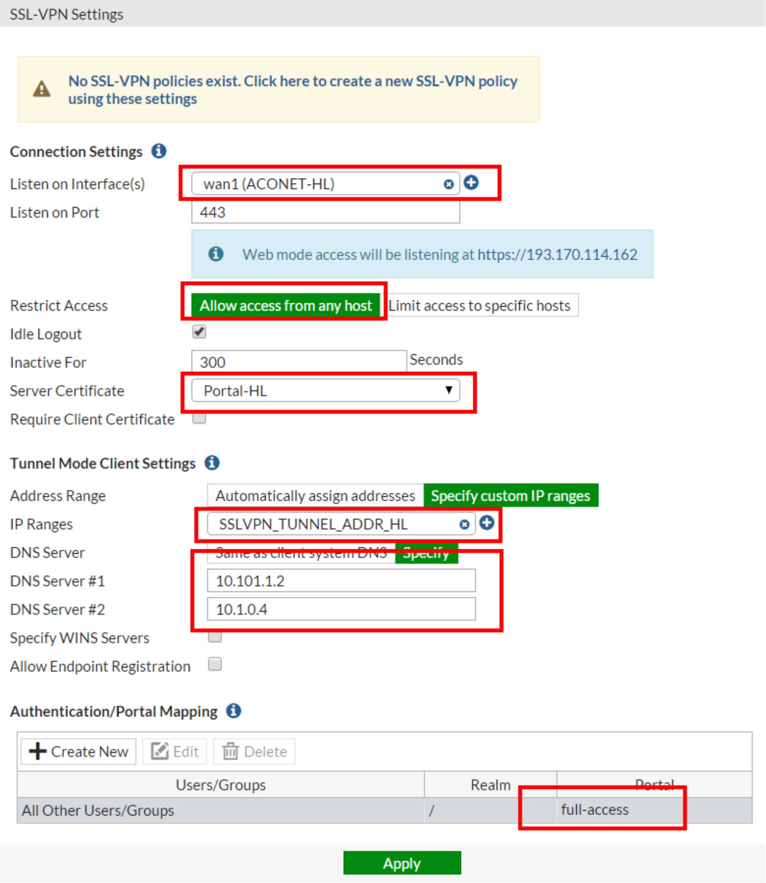
- CSR signieren lassen
- CA importieren
- Import Local Certificate



Name	
Certificates (5)	
Fortinet_SSLProxy	
Fortinet_Factory	C = US, CN = FGT60D4613002468, L = Sunnyvale, O = Fortinet, ST = California, emailAddress =
Fortinet_SSL	C = US, CN = FGT60D4613002468, L = Sunnyvale, O = Fortinet, ST = California, emailAddress =
Fortinet_Wifi	OU = PositiveSSL, CN = auth-cert.fortinet.com
Portal-HL	C = AT, CN = portal-hl.ph-noe.ac.at, businessCategory = Government Entity, serialNumber = Go
Local CA Certificates (3)	
Fortinet_CA_SSLProxy	C = US, CN = FortiGate CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support
Fortinet_CA_SSL	C = US, CN = FGT60D4613002468, L = Sunnyvale, O = Fortinet, ST = California, emailAddress =
Fortinet_CA_Untrusted	C = US, CN = Fortinet Untrusted CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddress
External CA Certificates (3)	
CA_Cert_1	CN = TERENA SSL High Assurance CA 3, C = NL, L = Amsterdam, O = TERENA, ST = Noord-Holl
Fortinet_CA	C = US, CN = support, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fort
PositiveSSL_CA	CN = PositiveSSL CA, C = GB, L = Salford, O = Comodo CA Limited, ST = Greater Manchester

VPN Settings

- Interface
- Zertifikat
- DHCP Pool für Clients
- DNS für Clients
- Zuweisung für Portal
  - Gruppe
- HINWEIS: noch keine Policy definiert



SSL-VPN Settings

No SSL-VPN policies exist. Click here to create a new SSL-VPN policy using these settings

Connection Settings

Listen on Interface(s)	wan1 (ACONET-HL)
Listen on Port	443
	Web mode access will be listening at https://193.170.114.162
Restrict Access	Allow access from any host / Limit access to specific hosts
Idle Logout	☑
Inactive For	300 Seconds
Server Certificate	Portal-HL ▾
Require Client Certificate	☐

Tunnel Mode Client Settings

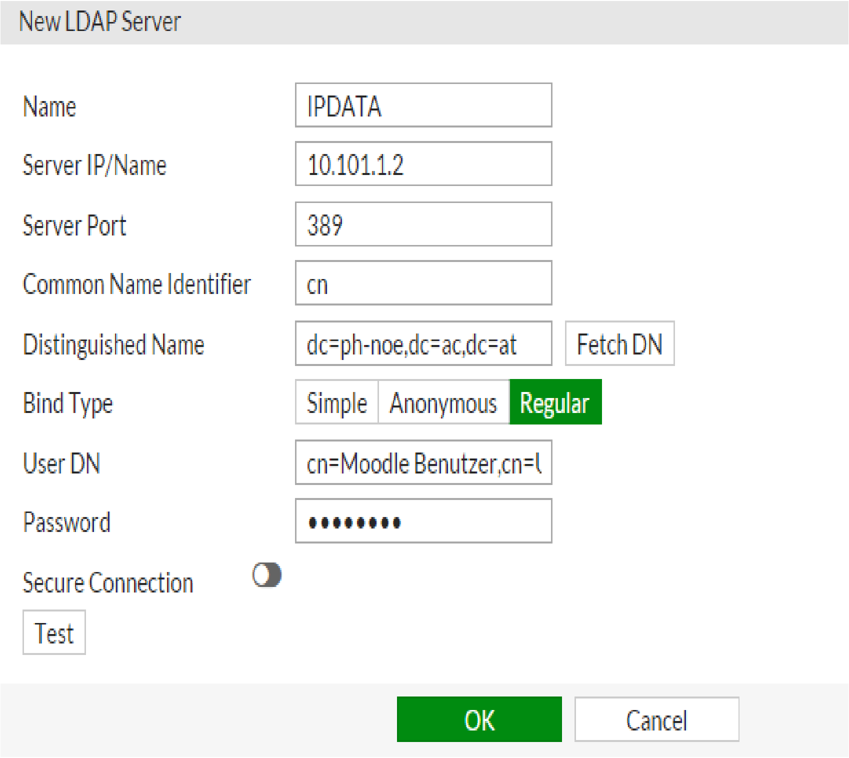
Address Range	Automatically assign addresses / Specify custom IP ranges
IP Ranges	SSLVPN_TUNNEL_ADDR_HL
DNS Server	Same as client system DNS / Specify
DNS Server #1	10.101.1.2
DNS Server #2	10.1.0.4
Specify WINS Servers	☐
Allow Endpoint Registration	☐

Authentication/Portal Mapping

Users/Groups	Realm	Portal
All Other Users/Groups	/	full-access

Benutzer / Gruppen

- LDAP Server definieren
- Bind User (im AD anlegen)
- mit LDAP Browser (auf einem Domänenrechner) auf AD zugreifen → LDAP Syntax

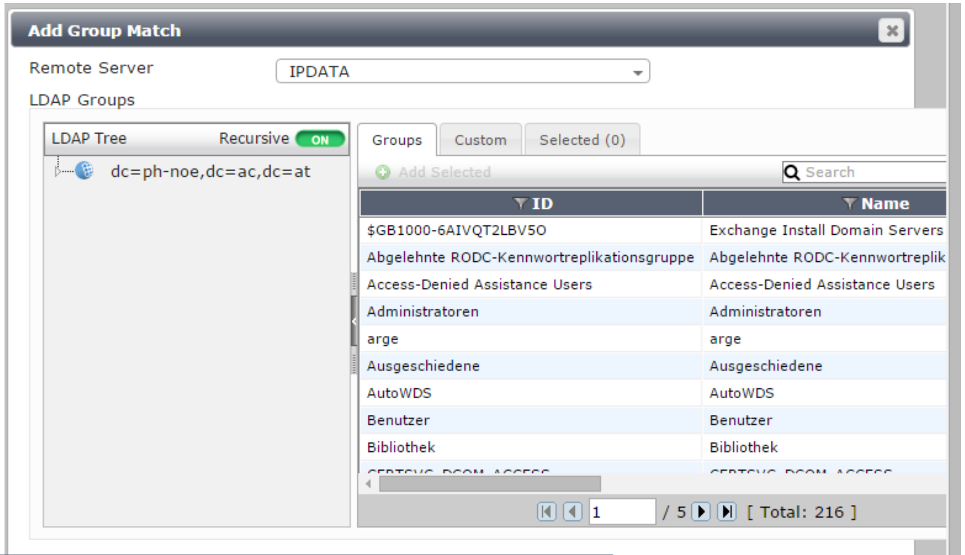


New LDAP Server

Name	IPDATA
Server IP/Name	10.101.1.2
Server Port	389
Common Name Identifier	cn
Distinguished Name	dc=ph-noe,dc=ac,dc=at Fetch DN
Bind Type	Simple Anonymous [✓ Regular]
User DN	cn=Moodle Benutzer,cn=l
Password	••••••••
Secure Connection	○

LDAP Gruppe importieren

- Lokale Gruppenbezeichnung vergeben
- Remote (LDAP) Gruppe verbinden



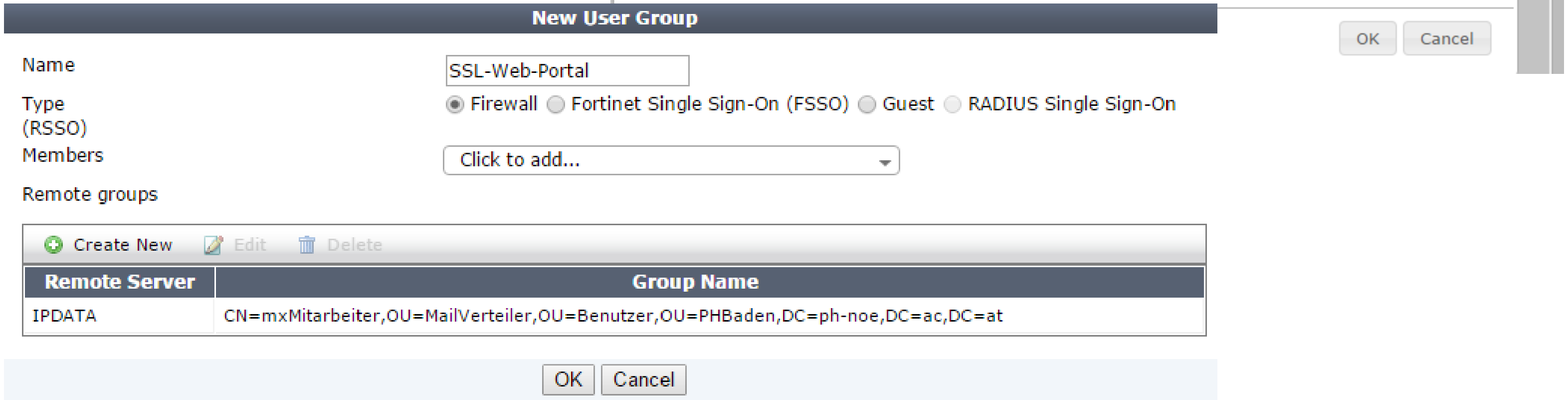
Add Group Match

Remote Server: IPDATA

LDAP Groups

ID	Name
$GB1000-6AIVQT2LBV5O	Exchange Install Domain Servers
Abgelehnte RODC-Kennwortreplikationsgruppe	Abgelehnte RODC-Kennwortreplik
Access-Denied Assistance Users	Access-Denied Assistance Users
Administratoren	Administratoren
arge	arge
Ausgeschiedene	Ausgeschiedene
AutoWDS	AutoWDS
Benutzer	Benutzer
Bibliothek	Bibliothek
CERTSVC_DCOM_ACCESS	CERTSVC_DCOM_ACCESS

1 / 5 [Total: 216]



New User Group

Name: SSL-Web-Portal

Type: ● Firewall ○ Fortinet Single Sign-On (FSSO) ○ Guest ○ RADIUS Single Sign-On (RSSO)

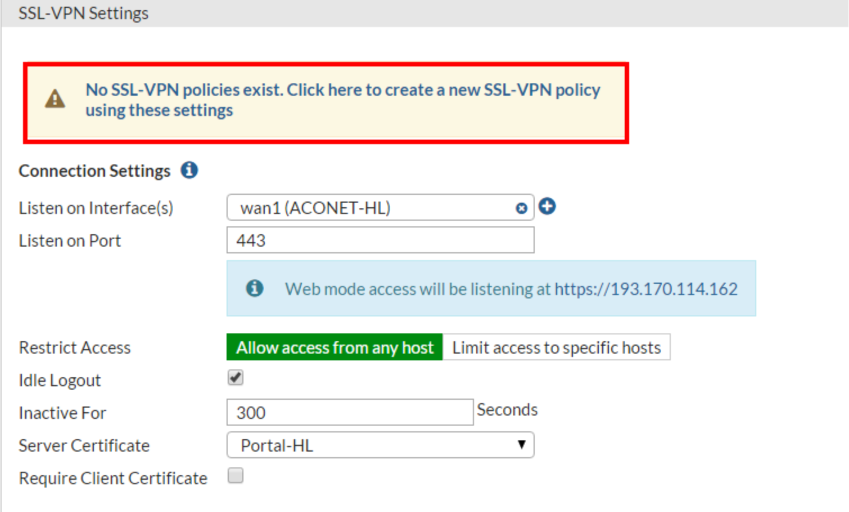
Members: Click to add...

Remote groups

Remote Server	Group Name
IPDATA	CN=mxMitarbeiter,OU=MailVerteiler,OU=Benutzer,OU=PHBaden,DC=ph-noe,DC=ac,DC=at

SSL-VPN Policy

- definiert Zugriff aus VPN in internes Netzwerk



SSL-VPN Settings

No SSL-VPN policies exist. Click here to create a new SSL-VPN policy using these settings

Connection Settings

Listen on Interface(s): wan1 (ACONET-HL)

Listen on Port: 443

Web mode access will be listening at https://193.170.114.162

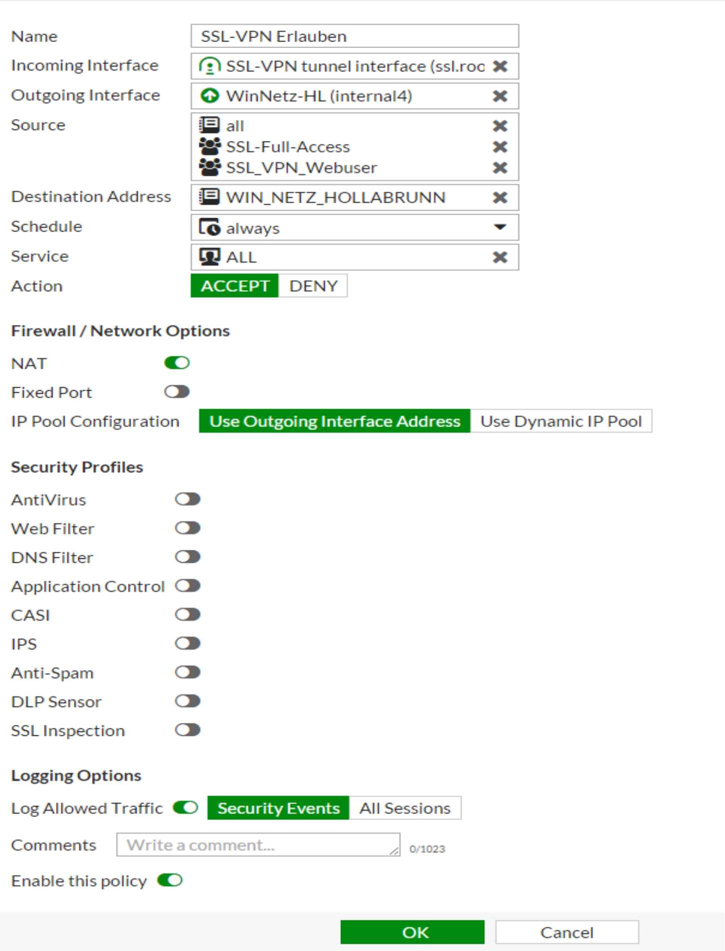
Restrict Access: [✓ Allow access from any host] Limit access to specific hosts

Idle Logout: ☑

Inactive For: 300 Seconds

Server Certificate: Portal-HL

Require Client Certificate: □



Name: SSL-VPN Erlauben

Incoming Interface: SSL-VPN tunnel interface (ssl.roo

Outgoing Interface: WinNetz-HL (internal4)

Source: all
SSL-Full-Access
SSL_VPN_Webuser

Destination Address: WIN_NETZ_HOLLABRUNN

Schedule: always

Service: ALL

Action: [✓ ACCEPT] DENY

Firewall / Network Options

NAT ●

Fixed Port ○

IP Pool Configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool

Security Profiles

AntiVirus ○

Web Filter ○

DNS Filter ○

Application Control ○

CASI ○

IPS ○

Anti-Spam ○

DLP Sensor ○

SSL Inspection ○

Logging Options

Log Allowed Traffic ● [✓ Security Events] All Sessions

Comments: Write a comment... 0/1023

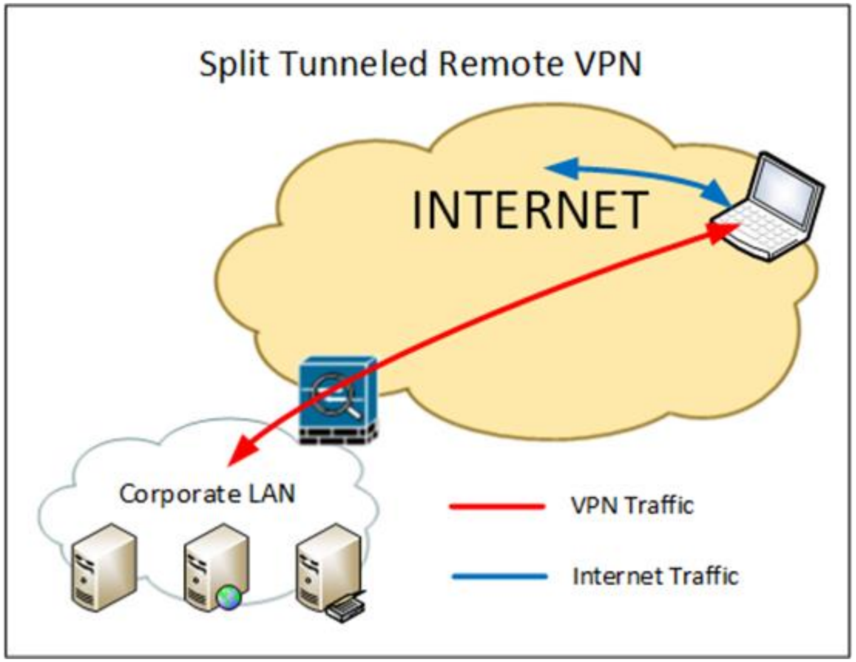
Enable this policy ●

SSL-VPN Policy

- mehrere Regeln, falls mehrere Outgoing Interfaces
  - sonst wird „Section View“ disabled!
- Incoming Interface: SSL-VPN tunnel interface
- z.B:
  - SSL-VPN-Erlauben-WIN-Netz
  - SSL-VPN-Erlauben-DMZ
  - …..

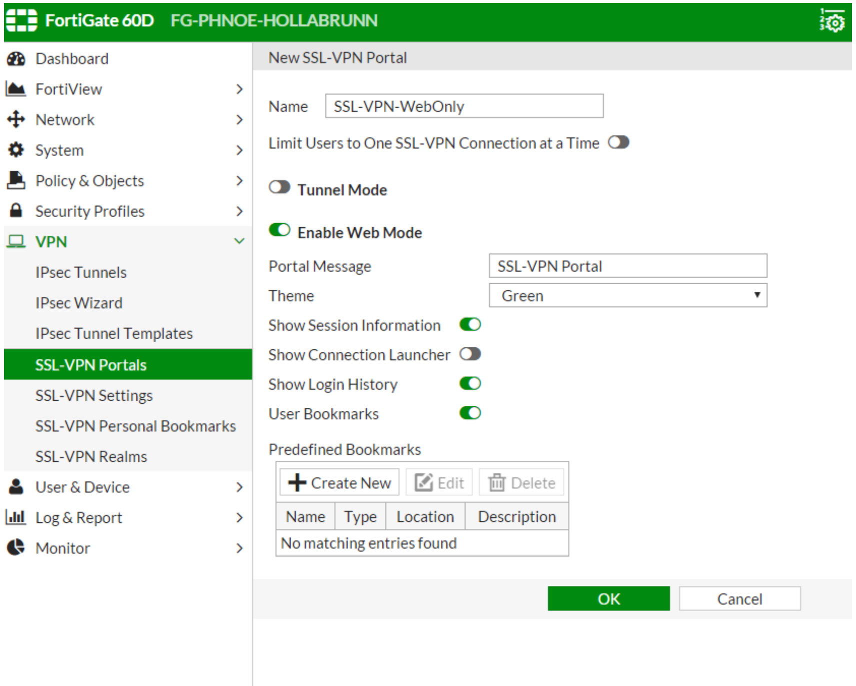
Split Tunnel

- Traffic ins Intranet → Tunnel
- Traffic ins Internet → NICHT durch Tunnel
- wenn Split Tunnel NICHT erlaubt:
  - bei aktiviertem VPN wird alles über Tunnel geleitet
  - Sicherheitsmaßnahmen greifen
  - zusätzliche Policy notwendig



Portal-Definitionen

- Web-Only
  - nur Webportal
  - kein Tunnelzugriff
  - Bookmarks



New SSL-VPN Portal

Name: SSL-VPN-WebOnly

Limit Users to One SSL-VPN Connection at a Time ○

○ Tunnel Mode

● Enable Web Mode

Portal Message: SSL-VPN Portal

Theme: Green

Show Session Information ●

Show Connection Launcher ○

Show Login History ●

User Bookmarks ●

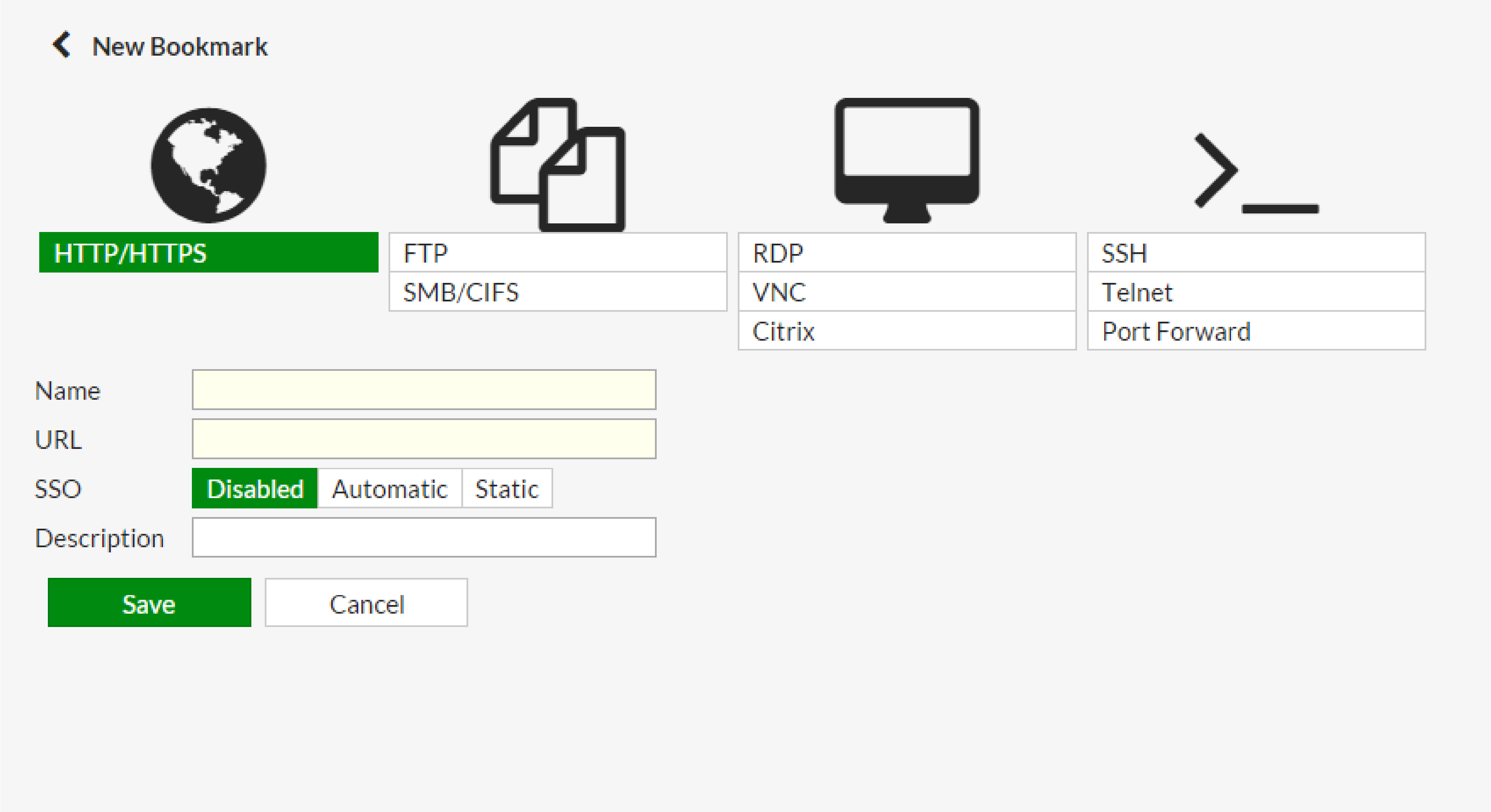
Predefined Bookmarks

+ Create New | Edit | Delete

Name	Type	Location	Description
No matching entries found			

OK | Cancel

Bookmarks-Übersicht



New Bookmark

HTTP/HTTPS

FTP
SMB/CIFS

RDP
VNC
Citrix

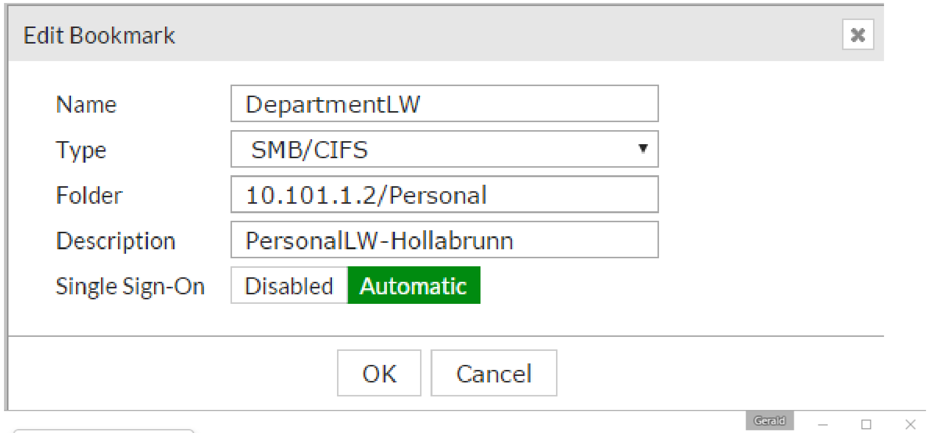
SSH
Telnet
Port Forward

Name
URL
SSO: [✓ Disabled] Automatic Static
Description

Save
Cancel

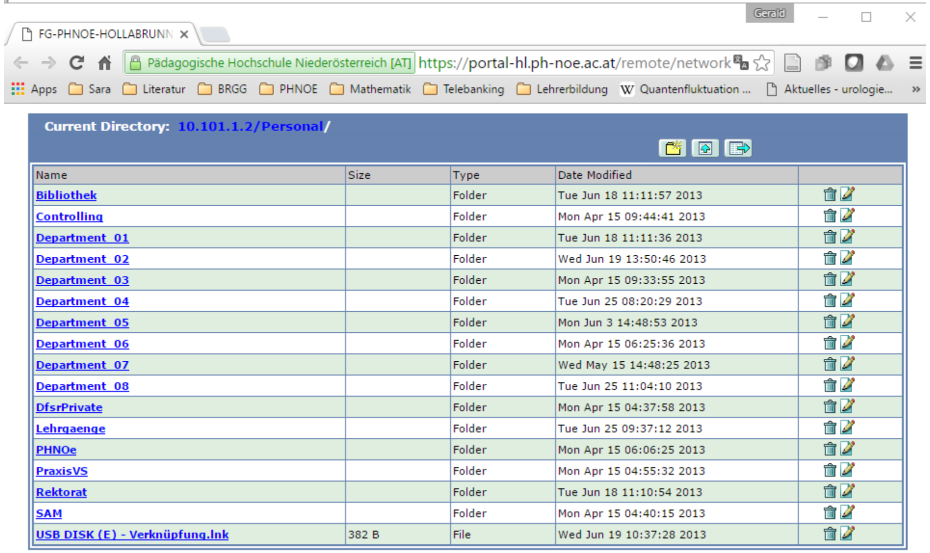
Bookmarks - CIFS

- SMB/CIFS
  - Webzugriff auf Windowsfreigabe
  - SSO
    - VPN-User wird zur Authentifizierung am Windowsserver verwendet



Edit Bookmark

Name	DepartmentLW
Type	SMB/CIFS ▼
Folder	10.101.1.2/Personal
Description	PersonalLW-Hollabrunn
Single Sign-On	Disabled [✓ Automatic]



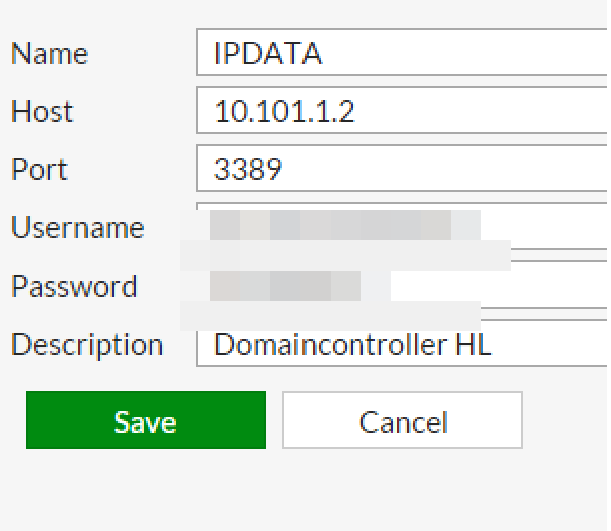
https://portal-hl.ph-noe.ac.at/remote/network

Current Directory: 10.101.1.2/Personal/

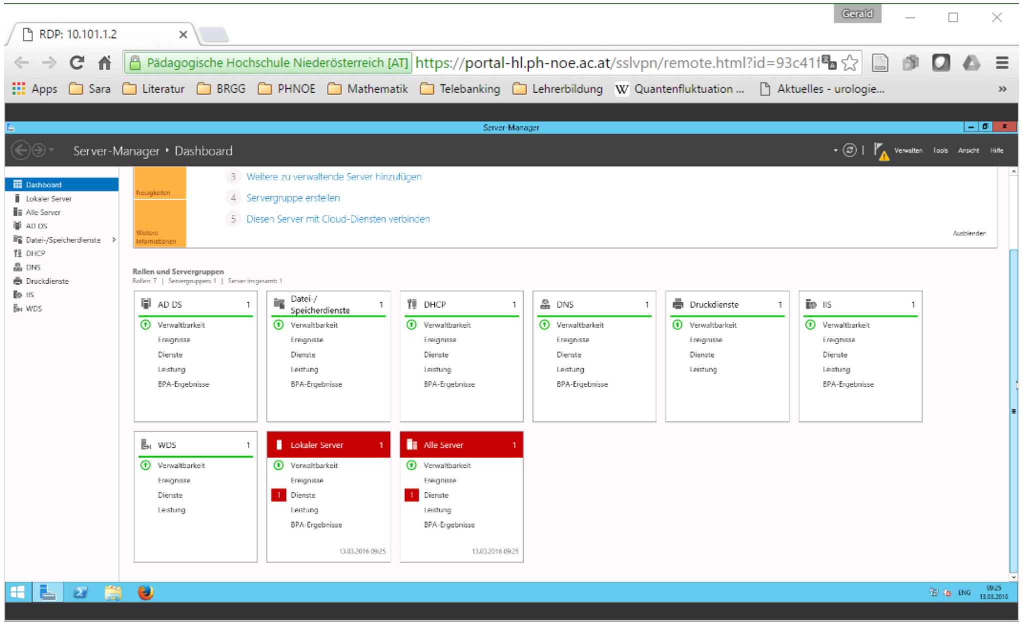
Name	Size	Type	Date Modified
Bibliothek		Folder	Tue Jun 18 11:11:57 2013
Controlling		Folder	Mon Apr 15 09:44:41 2013
Department_01		Folder	Tue Jun 18 11:11:36 2013
Department_02		Folder	Wed Jun 19 13:50:46 2013
Department_03		Folder	Mon Apr 15 09:33:55 2013
Department_04		Folder	Tue Jun 25 08:20:29 2013
Department_05		Folder	Mon Jun 3 14:48:53 2013
Department_06		Folder	Mon Apr 15 06:25:36 2013
Department_07		Folder	Wed May 15 14:48:25 2013
Department_08		Folder	Tue Jun 25 11:04:10 2013
DfsrPrivate		Folder	Mon Apr 15 04:37:58 2013
Lehrgaenge		Folder	Tue Jun 25 09:37:12 2013
PHNOe		Folder	Mon Apr 15 06:06:25 2013
PraxisVS		Folder	Mon Apr 15 04:55:32 2013
Rektorat		Folder	Tue Jun 18 11:10:54 2013
SAM		Folder	Mon Apr 15 04:40:15 2013
USB DISK (E) - Verknüpfung.lnk	382 B	File	Wed Jun 19 10:37:28 2013

Bookmarks - RDP

- Zugriff auf RDP über Browser



Name	IPDATA
Host	10.101.1.2
Port	3389
Username	[redacted]
Password	[redacted]
Description	Domaincontroller HL

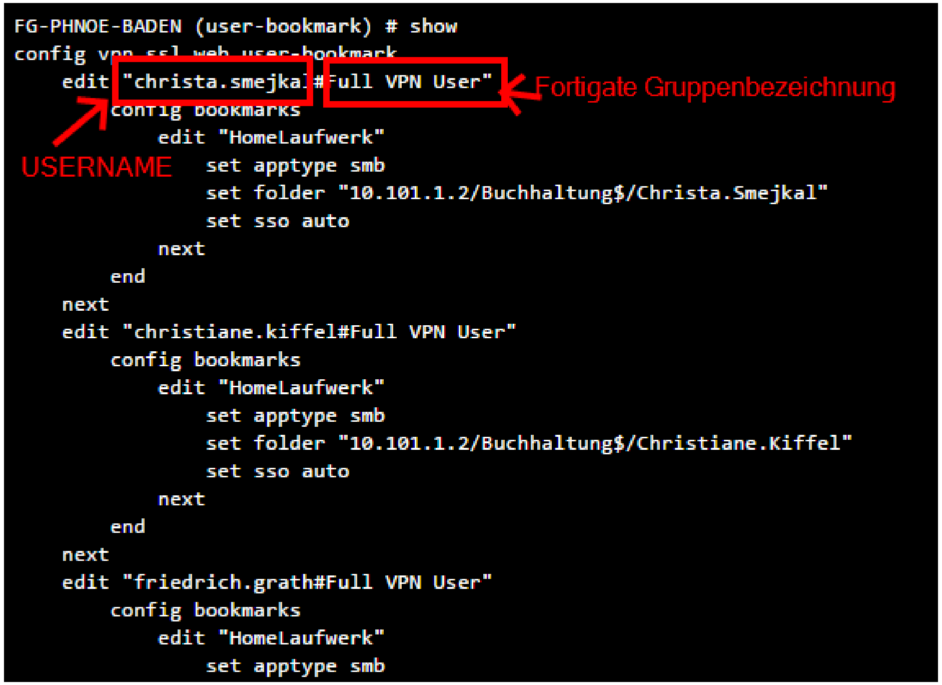


weitere Bookmarks

- http/https
  - Zugriff auf (interne) Webseiten: Switch,…
- VNC
- Citrix
- SSH
  - Konsolenzugriff auf (Linux) Server
  - Java notwendig!!

Bookmark auf User-Home?

- Problem: Für jeden Benutzer andere Freigabe
- Lösung: „Serienbrief“ ➔ CLI
- config vpn ssl web user-bookmark
- show



```
FG-PHNOE-BADEN (user-bookmark) # show
config vpn ssl web user-bookmark
    edit "christa.smejkal#Full VPN User"
        config bookmarks
            edit "HomeLaufwerk"
                set apptype smb
                set folder "10.101.1.2/Buchhaltung$/Christa.Smejkal"
                set sso auto
            next
        end
    next
    edit "christiane.kiffel#Full VPN User"
        config bookmarks
            edit "HomeLaufwerk"
                set apptype smb
                set folder "10.101.1.2/Buchhaltung$/Christiane.Kiffel"
                set sso auto
            next
        end
    next
    edit "friedrich.grath#Full VPN User"
        config bookmarks
            edit "HomeLaufwerk"
                set apptype smb
```

USERNAME

Fortigate Gruppenbezeichnung

Group-based SSL VPN bookmarks

- nur über CLI

```
config vpn ssl web portal
        edit "portal-name"
                set user-group-bookmark enable*/disable
        next
end
config vpn ssl web user-group-bookmark
        edit "group-name"
                config bookmark
                        edit "bookmark1"
                        ....
                        next
                end
        next
end
```