FortiAuthenticator Basic Troubleshooting

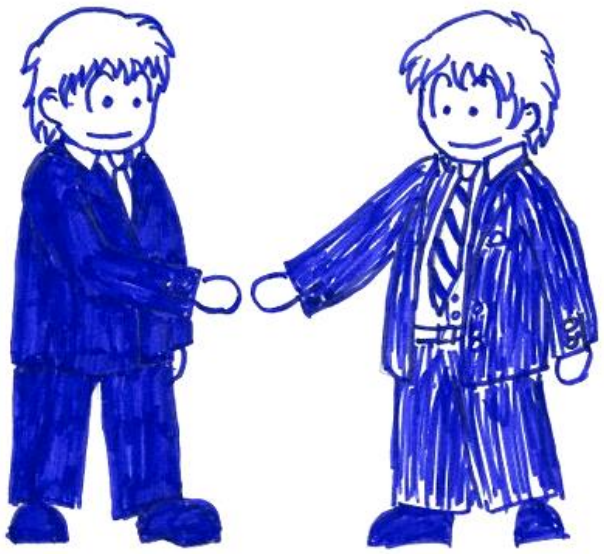
2025-10-29 Deborah Geisau

About myself

- Joined Fortinet in 2015
- Working out of Frankfurt TAC

- Started out in FortiGate technical support
- Stint with FortiAnalyzer/FortiManager support
- Joined Authentication team (FortiAuthenticator/FortiNAC) in 2019, Escalation Engineer

About the Round Table Tech Talk

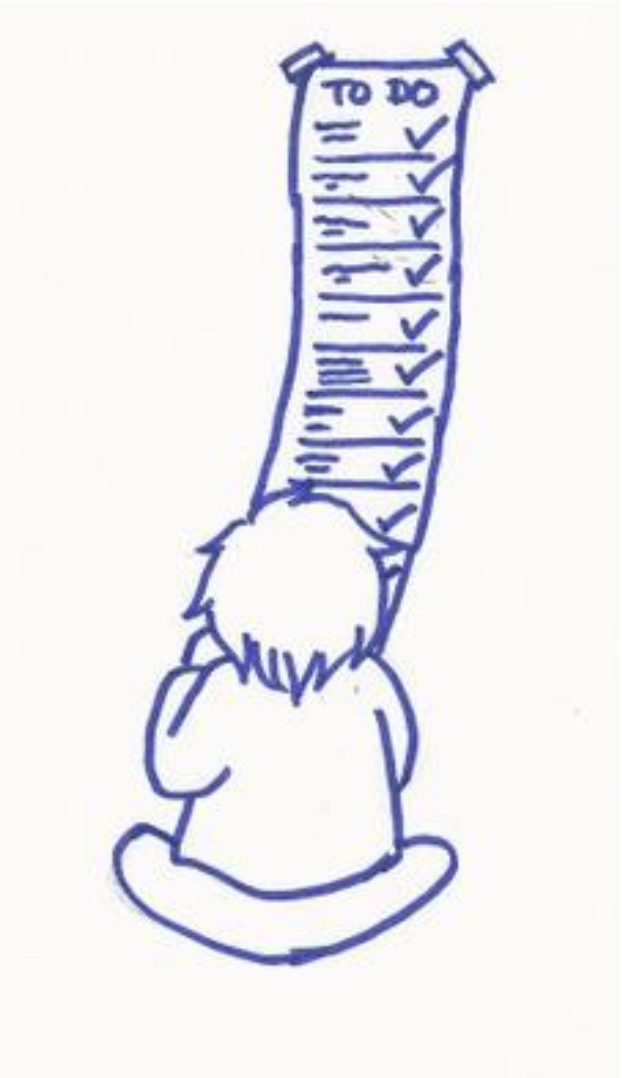


- **This is recorded!**
- Planned duration: 120 minutes
- Slides and Recording will be made available within five business days

- Questions:
  - » Submit any time in Question pane or raise your hand
  - » Answers at the end of each section
  - » More complex questions may be deferred
- Dedicated lab and question section at the end

Overview

- Introduction to FortiAuthenticator
- FortiAuthenticator GUI
  - » Navigation
  - » Monitor & Logs
  - » Debug Reports
- FortiAuthenticator “/debug”
- FortiAuthenticator CLI
- How to troubleshoot
- Involving Fortinet Technical Support
- Lab Demonstration, additional questions



Introduction to FortiAuthenticator

What is FortiAuthenticator?

- Fortinet Authentication solution
  - » On-premise, Cloud (FortiTrustID), Subscription starting in firmware version 8.0
  - » Hardware or VM
- AAA: Authentication, Authorization, Accounting
  - » Identity Management
  - » RADIUS, 2FA, SAML, FSSO, Portals….

Primary Use cases: RADIUS

- RADIUS: common authentication protocol for WiFi/Wired/VPN authentication

- Act as RADIUS server
- User authentication
  - » Local user
  - » Remote user (LDAP, other RADIUS)
- Provide two-factor options
  - » FortiToken, Email, SMS, FIDO2
- 802.1x, EAP

Primary Use cases: FSSO

- FSSO: Fortinet Single-Sign-On, detect logins in Windows AD

- Act as FSSO Collector Agent
- Polling mode
  - » Filter on event IDs
- DC Agent mode
  - » Needs standalone DC Agent installation!
- Additional options:
  - » FSSO Mobility Agent
  - » Syslog, RADIUS Accounting

Primary Use cases: SAML

- SAML: HTTPS/portal-based authentication standard, works via redirects

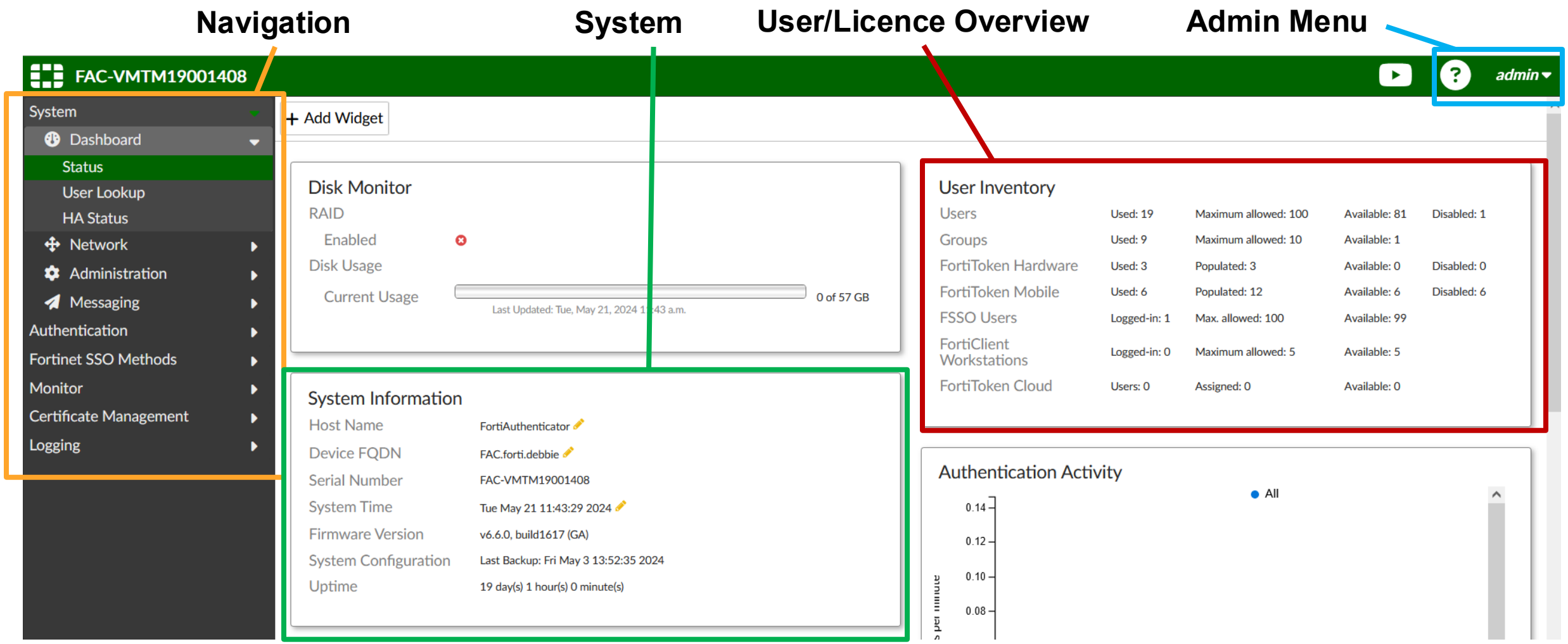
- Function as SAML Identity Provider or Proxy
- User Authentication
- Provide two-factor options
  - » FortiToken, Email, SMS, FIDO2
- Also:
  - » OAuth
  - » SCIM

Other Use Cases

- Captive & Self-Service Portal
- Radius Accounting (Usage Profiles)
- Certificate Management
- LDAP Server
- TACACS+ Server
- Guest Management
  - » FortiGuest integration in 8.0

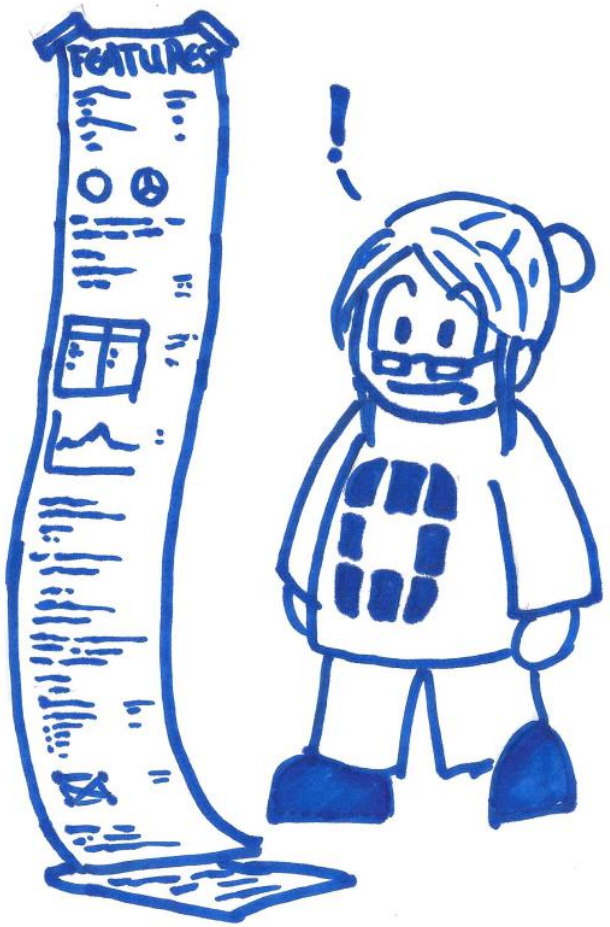
FortiAuthenticator GUI

Landing Page



Navigation

- System
  - » Administration, HA, Interfaces, Network, …
- Authentication
  - » User Management, Remote Servers, Authentication services
- Fortinet SSO (Methods)
  - » All FSSO-related settings
- Monitor
  - » A (tiny) bit like FortiView, more detail to follow
- Certificate Management
  - » Local server/CA certificates, trusted CA, user certificates
- Logging
  - » Logs, Logging settings, Debug repots, more detail in a bit

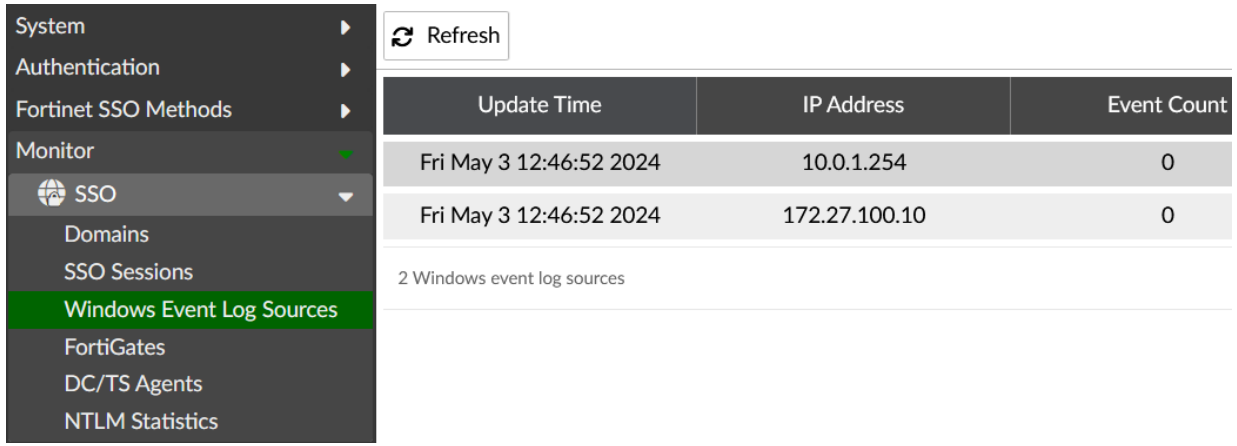


Tip: FortiAuthenticator admin guide roughly follows GUI layout in its chapters/organization!

Monitor section

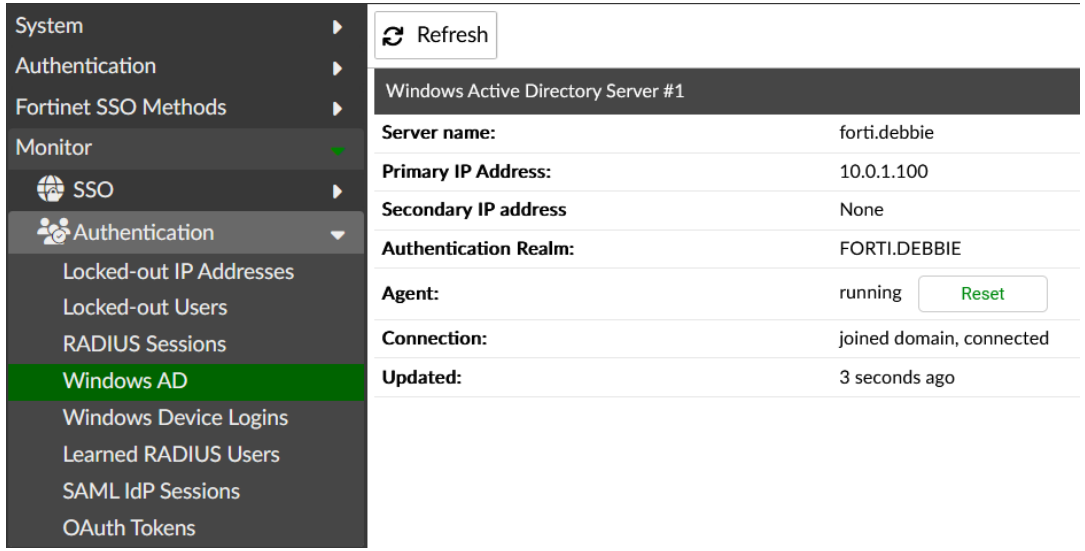
SSO (FSSO Statistics)

- FSSO sessions
- DC Agent/TS Agent connection
- Polling status
- FortiGate connection



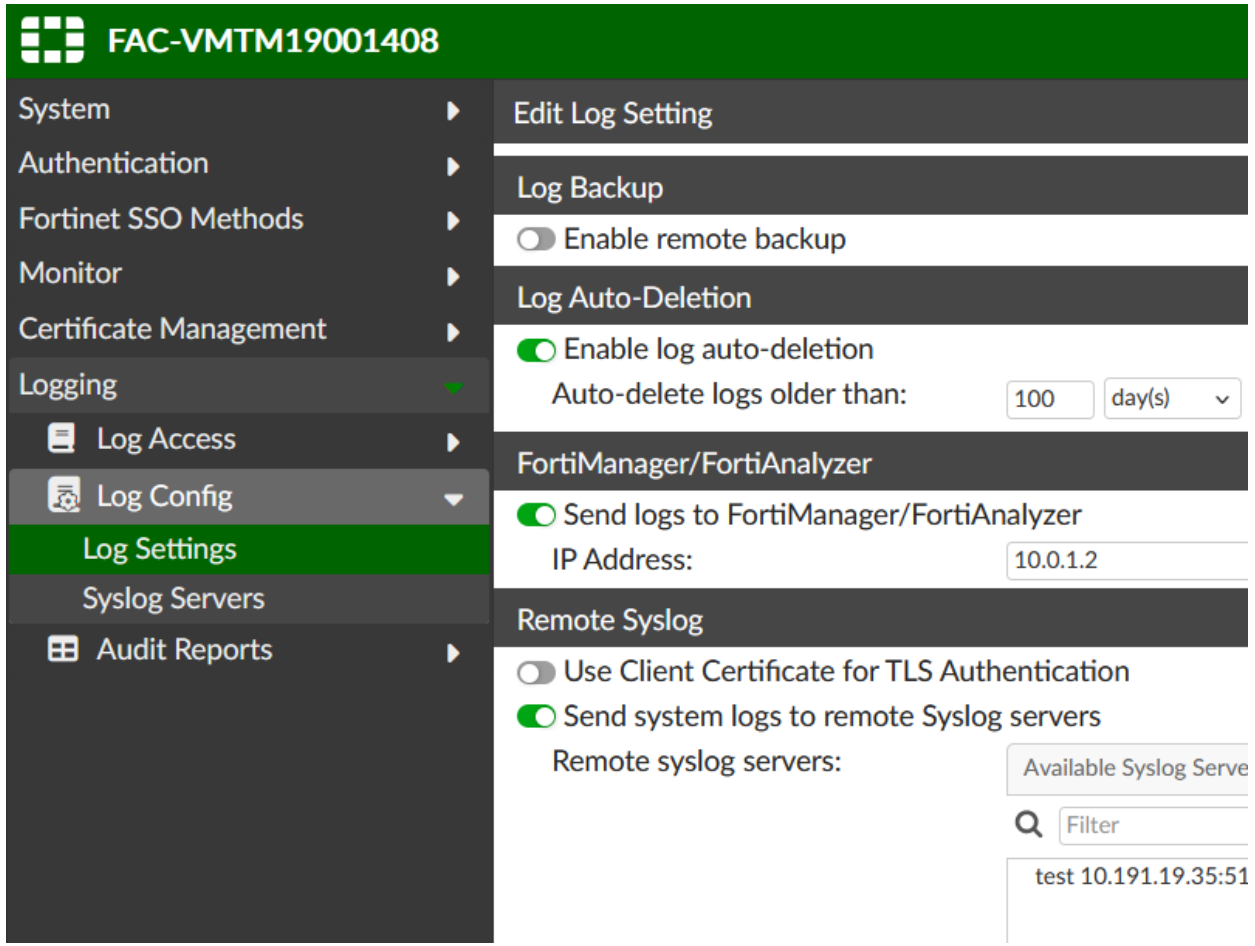
Authentication

- Windows domain connection
- Locked-out users/IP
- SAML IdP session
- ...



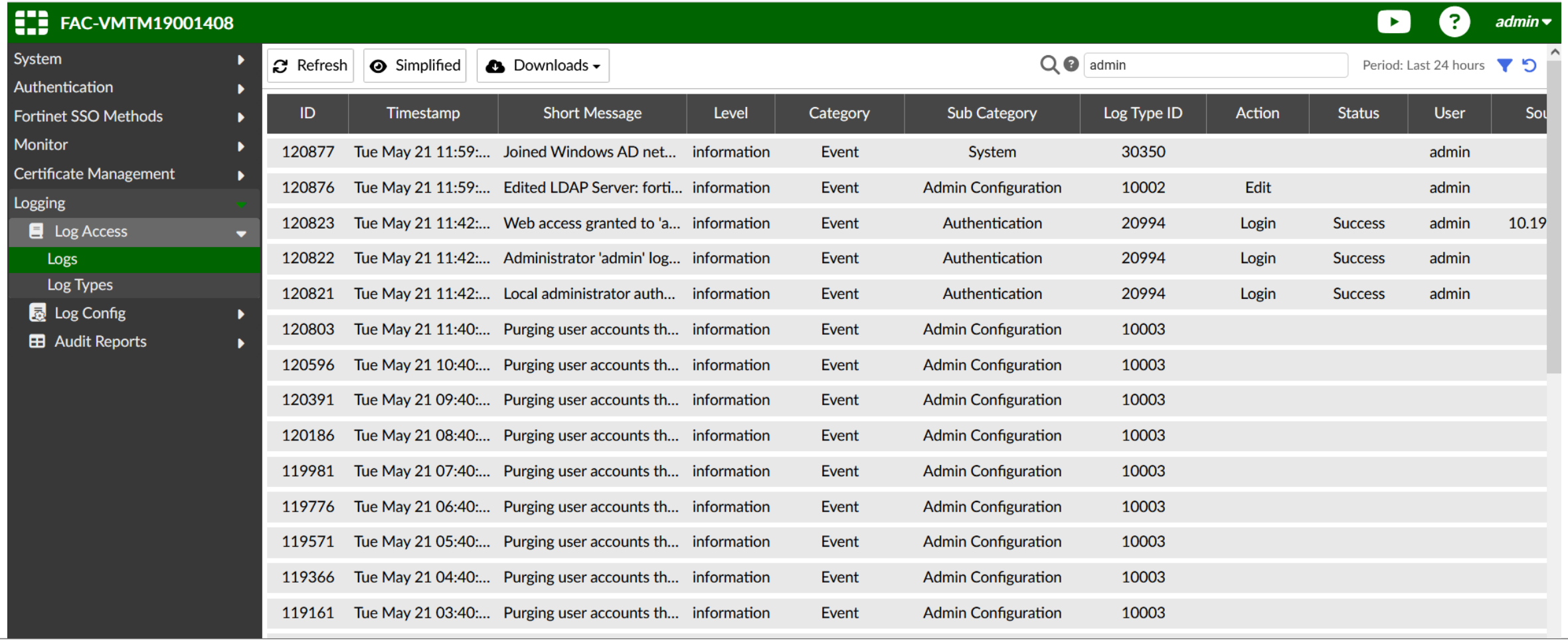
Logging

- View log settings
  - » Logging to remote syslog server
  - » Logging to FortiAnalyzer/Manager
- View logs stored locally on device
  - » Filter on fixed time (last 24h, last 7 days, …)
  - » Filter on string
- Download debug reports/logs
  - » Reports can be decrypted by TAC
  - » Summary/other categories



Logging

- Filter: Last 24h, string “admin”

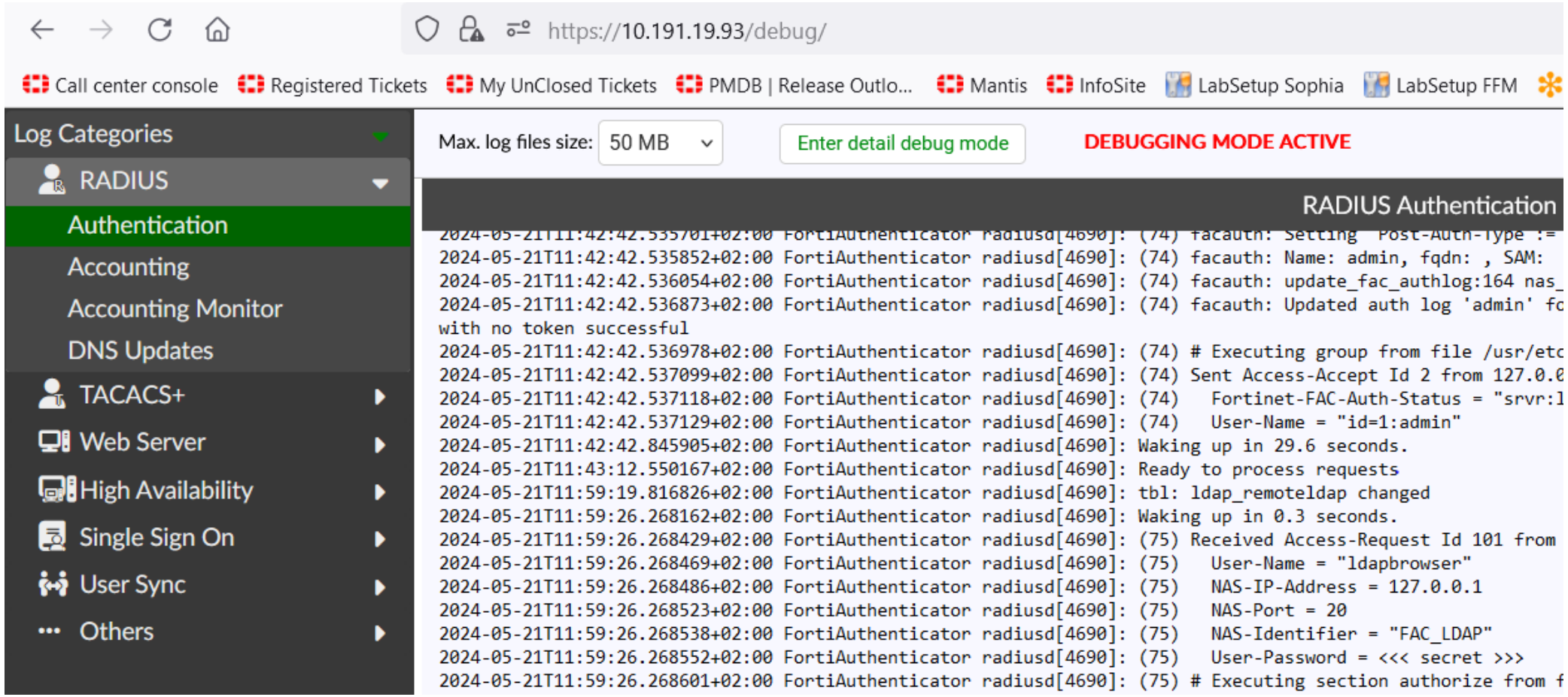


ID	Timestamp	Short Message	Level	Category	Sub Category	Log Type ID	Action	Status	User	Sou
120877	Tue May 21 11:59:...	Joined Windows AD net...	information	Event	System	30350			admin	
120876	Tue May 21 11:59:...	Edited LDAP Server: forti...	information	Event	Admin Configuration	10002	Edit		admin	
120823	Tue May 21 11:42:...	Web access granted to 'a...	information	Event	Authentication	20994	Login	Success	admin	10.19
120822	Tue May 21 11:42:...	Administrator 'admin' log...	information	Event	Authentication	20994	Login	Success	admin	
120821	Tue May 21 11:42:...	Local administrator auth...	information	Event	Authentication	20994	Login	Success	admin	
120803	Tue May 21 11:40:...	Purging user accounts th...	information	Event	Admin Configuration	10003				
120596	Tue May 21 10:40:...	Purging user accounts th...	information	Event	Admin Configuration	10003				
120391	Tue May 21 09:40:...	Purging user accounts th...	information	Event	Admin Configuration	10003				
120186	Tue May 21 08:40:...	Purging user accounts th...	information	Event	Admin Configuration	10003				
119981	Tue May 21 07:40:...	Purging user accounts th...	information	Event	Admin Configuration	10003				
119776	Tue May 21 06:40:...	Purging user accounts th...	information	Event	Admin Configuration	10003				
119571	Tue May 21 05:40:...	Purging user accounts th...	information	Event	Admin Configuration	10003				
119366	Tue May 21 04:40:...	Purging user accounts th...	information	Event	Admin Configuration	10003				
119161	Tue May 21 03:40:...	Purging user accounts th...	information	Event	Admin Configuration	10003				

FortiAuthenticator “/debug”

/debug Overview

- Navigate to URL path https://<FortiAuthenticator>/debug/



/debug Navigation

- Layout varies depending on firmware version!
- Separated into sections
  - » Individual log files can be downloaded
  - » Log file size can be adjusted
  - » **Time format varies between local and GMT!**

- **RADIUS Authentication debug log**

RADIUS Debug Log

- **FortiAuthenticator treats nearly all authentication as RADIUS**
  - » RADIUS
  - » Admin login
  - » Portals
  - » SAML
  - » LDAP
  - » ...

- Non-RADIUS authentication is translated to RADIUS
  - » Request from 127.0.0.1 to 127.0.0.1:1812
  - » Debug output may include information on the non-RADIUS authentication
- In case of authentication issues, **always check RADIUS debug**

NAS-Identifier

- FortiAuthenticator uses NAS-Identifier in local RADIUS Access-Requests to indicate source of authentication request

- For example:
  - » FAC_GUI: Admin login, legacy self-servie
  - » FAC_GUEST: Captive Portal
  - » LDAP: LDAP service
  - » SAML: FortiAuthenticator acting as IdP
  - » TAC_PLUS: TACACS+

NAS-Identifier examples

Captive Portal

```
2024-09-12T14:48:30.140235+01:00 FortiAuthenticator radiusd[3020]: (8) Received Access-Request Id 73 from 127.0.0.1:38495 to
127.0.0.1:1812 length 82
2024-09-12T14:48:30.140247+01:00 FortiAuthenticator radiusd[3020]: (8) User-Name = "debbie"
2024-09-12T14:48:30.140250+01:00 FortiAuthenticator radiusd[3020]: (8) NAS-IP-Address = 127.0.0.1
2024-09-12T14:48:30.140254+01:00 FortiAuthenticator radiusd[3020]: (8) NAS-Port = 20
2024-09-12T14:48:30.140257+01:00 FortiAuthenticator radiusd[3020]: (8) NAS-Identifier = "FAC_GUEST:5:10.0.0.2"
```

Admin Login

```
2022-12-21T16:43:07.655615+01:00 FortiAuthenticator radiusd[1340]: (39) Received Access-Request Id 187 from
127.0.0.1:46983 to 127.0.0.1:1812 length 92
2022-12-21T16:43:07.655671+01:00 FortiAuthenticator radiusd[1340]: (39) User-Name = "matanaskovic"
2022-12-21T16:43:07.655683+01:00 FortiAuthenticator radiusd[1340]: (39) Gandalf-Calling-Line-ID-1 = "10.5.63.254"
2022-12-21T16:43:07.655704+01:00 FortiAuthenticator radiusd[1340]: (39) NAS-IP-Address = 127.0.0.1
2022-12-21T16:43:07.655742+01:00 FortiAuthenticator radiusd[1340]: (39) NAS-Port = 20
2022-12-21T16:43:07.655752+01:00 FortiAuthenticator radiusd[1340]: (39) NAS-Identifier = "FAC_GUI"
```

Enabling RADIUS Debug

- **Disabled by default starting from 6.5.0!**
- Enabled via GUI:
  - » Enter debug mode (usually enough)
  - » Enter detail debug mode (very noisy)
  - » Disable on same button
- Enabled via CLI
  - » `debug radius 1 (enable)`
  - » `debug radius 2 (detailed)`
- **Does not disable automatically!**
  - » `debug radius 0`
- Disables with reboot

Example: Captive Portal error

- Incoming Captive Portal request is matched into an incorrect policy

```
2024-09-12T14:48:30.139333+01:00 FortiAuthenticator radiusd[3020]: Waking up in 0.6 seconds.
2024-09-12T14:48:30.140235+01:00 FortiAuthenticator radiusd[3020]: (8) Received Access-Request Id 73 from 127.0.0.1:38495 to
127.0.0.1:1812 length 82
2024-09-12T14:48:30.140247+01:00 FortiAuthenticator radiusd[3020]: (8) User-Name = "debbie"
2024-09-12T14:48:30.140250+01:00 FortiAuthenticator radiusd[3020]: (8) NAS-IP-Address = 127.0.0.1
2024-09-12T14:48:30.140254+01:00 FortiAuthenticator radiusd[3020]: (8) NAS-Port = 20
2024-09-12T14:48:30.140257+01:00 FortiAuthenticator radiusd[3020]: (8) NAS-Identifier = "FAC_GUEST:5:10.0.0.2"
2024-09-12T14:48:30.140259+01:00 FortiAuthenticator radiusd[3020]: (8) User-Password: ******
2024-09-12T14:48:30.140262+01:00 FortiAuthenticator radiusd[3020]: (8) # Executing section authorize from file /usr/etc/raddb/
sites-enabled/default
2024-09-12T14:48:30.140746+01:00 FortiAuthenticator radiusd[3020]: (8) facauth: ===>NAS IP:127.0.0.1
2024-09-12T14:48:30.140756+01:00 FortiAuthenticator radiusd[3020]: (8) facauth: ===>Username:debbie
2024-09-12T14:48:30.140759+01:00 FortiAuthenticator radiusd[3020]: (8) facauth: ===>Timestamp:1615556910.139096, age:1ms
2024-09-12T14:48:30.141537+01:00 FortiAuthenticator radiusd[3020]: (8) facauth: ERROR: The AP of portal policy 5 does not contain
client 10.0.0.2
2024-09-12T14:48:30.141547+01:00 FortiAuthenticator radiusd[3020]: (8) Invalid user (facauth: The AP of portal policy 5 does not
contain client 10.0.0.2 [debbie] (from client localhost port 20)
```

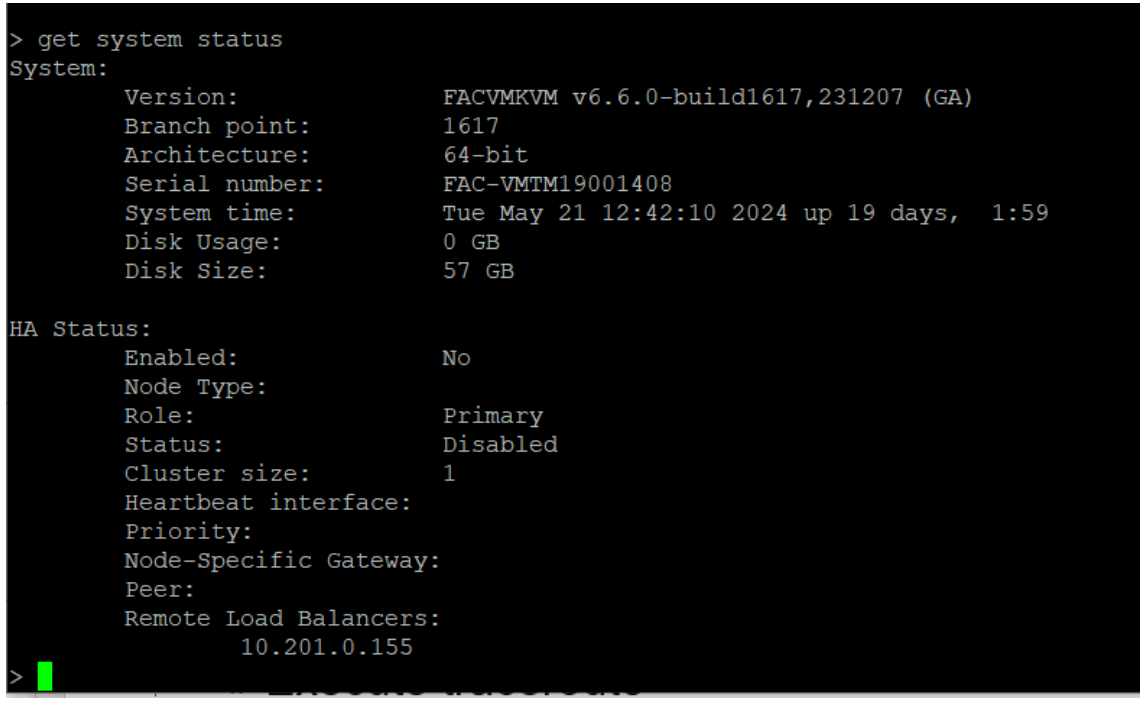
Other important debug logs

- Web Server
  - » WAD: displays any output generated by wad demon, more in CLI section
  - » Apache: GUI/HTTPS daemon, relevant for SAML, GUI errors
  - » **8.0 adds two categories, SAML and Generic API**
- High Availability
  - » Slony: Active-Passive cluster daemon
  - » LB HA/LB Sync: Load-Balancing cluster daemons
- Single Sign On
  - » FSSO Agent: Collector Agent debug
- Others:
  - » GUI: Additional info to Apache, relevant for SAML, GUI errors

FortiAuthenticator CLI

CLI troubleshooting

- **Very limited compared to FortiGate!**
- Basic interface, routing, DNS configuration
  - » Also HA configuration, but **DO NOT TOUCH**, can lead to sync issues
- Basic troubleshooting commands
  - » `show`
  - » `get system status`
  - » `execute ping`
  - » `execute traceroute`
  - » `execute dig/nslookup`
  - » `execute iptables`



Packet capture

- In GUI, under System > Network
  - » Very limited, no filtering options, max 4000 packets
- `execute tcpdump <options> <filter>`
  - » Same syntax as tcpdump in Linux systems, output to CLI

```
> > execute tcpdump -i any -c 10 port 443
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
14:01:24.132558 port1 In  IP 10.191.31.254.61838 > 10.191.19.93.https: Flags [S], seq 3335950034, win 64896, op
tions [mss 1352,nop,wscale 8,nop,nop,sackOK], length 0
```

- `execute tcpdumpfile <options> <filter>`
  - » Same syntax as tcpdump –w in Linux systems
  - » Output to a pcap file,
    download finished file from https://<FAC>/debug/pcap-dump/

Diagnose commands

```
> diagnose netlink route
default via 10.191.31.254 dev port1
10.0.0.0/24 dev port4 proto kernel scope link src 10.0.0.1
10.0.1.0/24 dev port2 proto kernel scope link src 10.0.1.1
10.191.16.0/20 dev port1 proto kernel scope link src 10.191.19.93
10.200.0.0/24 via 10.0.1.3 dev port2
172.27.100.0/24 dev port3 proto kernel scope link src 172.27.100.123
192.168.220.0/24 via 10.0.1.3 dev port2
>
```

- `diagnose netlink [...]`
  - » Routing table, ARP table
  - » Interface statistics
- `diagnose web restart`
  - » Restart web service (GUI, Portals, SAML)
- `diagnose authentication restart`
  - » Restart RADIUS service (All user authentication!)
- `debug radius 0/1/2`
  - » RADIUS debug mode: disable, enable, detailed debugging mode
  - » Output to RADIUS Authentication log in /debug
- `diagnose system wad debug crash read`
  - » crashlog (starting in 6.5)
- `diagnose system wad [...]`
  - » Lots of wad debug options, output to WAD debug file in /debug

`wad` daemon - 1

- `wad` daemon was added in 6.5.0
- Copied from FortiGate/FortiProxy
  - » Copied some nonsensical debug category names as well
- `wad` daemon handles:
  - » webservice (http/https) related stuff
  - » API, GUI, Portals, …
  - » DNS, Push notification, FortiTokenCloud
  - » (Some) database stuff
  - » Some user login caching in 6.6.3
  - » SAML, SCIM

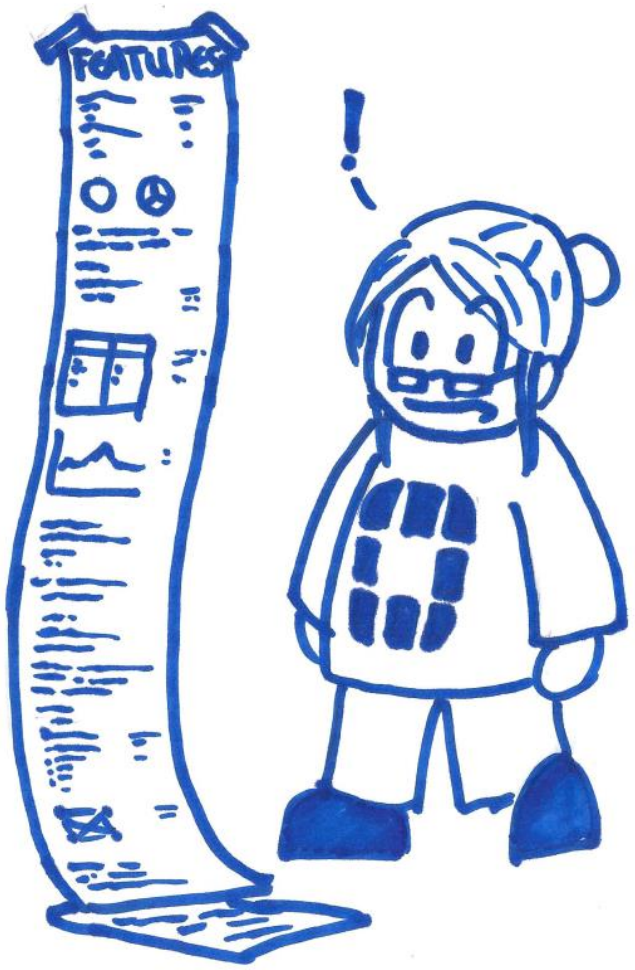
wad daemon - 2

- wad daemon does NOT handle:
  - » RADIUS authentication
  - » LDAP/TACACS+ service
  - » FSSO
- wad daemon info:
  - » diagnose system wad test list
  - » diagnose system wad test restart
  - » diagnose system wad test command <>
- wad crash log:
  - » diagnose system wad debug crash read

```
> diagnose system wad debug enable category
  session              Enable wad session trace.
  packet               Enable wad packet trace.
  dispatcher           Enable wad dispatcher trace.
  http                 Enable wad http trace.
  http2                Enable wad http2 trace.
  ssl                  Enable wad ssl trace.
  policy               Enable wad policy trace.
  auth                 Enable wad auth trace.
  sys                  Enable wad sys trace.
  video                Enable wad video trace.
  memblk               Enable wad memblk trace.
  vs                   Enable wad vs trace.
  detail               Enable wad detail trace.
  info                 Enable wad info trace.
  config               Enable wad config trace.
  dns                  Enable wad dns trace.
  jumper               Enable wad jumper trace.
  ftcd                 Enable wad ftcd trace.
  pgclient             Enable wad pgclient trace.
  db_listener          Enable wad db_listener trace.
  ftcd_client          Enable wad ftcd_client trace.
  auth_client          Enable wad auth_client trace.
  pushd                Enable wad pushd trace.
  rest_api             Enable wad rest_api trace.
> diagnose system wad debug enable category
```

`wad` Debug – dump in CLI

- **Log to WAD debug file by default**
- `diagnose system wad debug all`
  - » Enable all categories, VERY NOISY!
- `diagnose system wad debug enable cat <>`
  - » Enable specific categories
- `diagnose system wad debug enable level verbose`
  - » Enable verbose output
- `diagnose system wad debug pts enable`
  - » Enable output to be dumped in CLI as well, **log the SSH session!**
- `diagnose system wad debug clear`
  - » Reset wad debug settings
- `diagnose system wad debug pts clear`
  - » Disable CLI output



`wad` Debug Categories - 1

- `wad` daemon debug has many categories
  - » Inherited from FortiGate/FortiProxy
  - » Enabled by default: jumper, pushd, ftcd
- Useful categories
  - » dns, video: DNS lookup
  - » pushd: push notification
  - » ftcd, ftcd_client: FortiTokenCloud
  - » scim_api, scim_client: SCIM
  - » rest_api: REST API
  - » jumper: Proxy, certificate-related output

`wad` Debug Categories - 2

Disclaimer: Not fully documented what each category does in FortiAuthenticator, please take this with a grain of salt!

Situationally useful

- memblk: memory allocation
- vs: virtual server/proxy, used by SCIM/SAML
- session, packet: packet dump, session info
- http, http2: HTTP session info
- ssl: SSL session info
- auth, auth_client: user authentication, caching
- pgclient, db_listener: Database-related output

Unclear function

- detail
- info
- config
- sys
- policy

How to troubleshoot

General Troubleshooting

- **Understand the context!**

- When was it first noticed?
  - » Did anything happen just before, like reboot, upgrade?
  - » Error messages?
- New/Modified configuration, or no change?
  - » Happened after config change?
- Random? Is there a pattern?
  - » Happened once, or more often?
  - » Specific or random users affected?

- **Any existing troubleshooting doc/KB that covers same/similar setup or issue?**

How to tell if it's a FortiAuthenticator issue

- **Just because FortiAuthenticator gives an error message does not mean the issue is located on it!**
  - » Could also be logging an error returned by a remote server, for example
- Try to bypass FortiAuthenticator
  - » Use a different authentication server/Collector Agent/local user instead
  - » Does issue disappear?
- Does the relevant authentication request/traffic even reach FortiAuthenticator?
  - » If yes, does Authenticator reply?
- Double-check configuration against available guides
- Verify that firmware versions are compatible

Basic checks – System and Configuration

- System
  - » Licence limitations reached?
  - » Resource usage ok?
  - » NTP ok?
  - » **Uptime?**
- Configuration
  - » New/modified configuration? **What guides were followed?**
  - » Any error messages during configuration?
- Release Notes
  - » Known issues for that firmware version?
- Upgrade history
  - » Visible in firmware upload screen
  - » Was upgrade path followed?

Basic checks - Network

- Is FortiAuthenticator even reachable from the client/user/etc?
- If yes, does it reply?
  - » **If yes, presumably at least basic routing is fine**
- **Packet capture!**
- Check network/interface settings!
  - » show system interface
  - » dia netlink route
  - » dia netlink arp list
- Check connectivity
  - » Ping, traceroute
  - » nslookup, dig
- **HA A-P clusters can have unexpected default route that interferes with routing!**
  - » Check if node-specific gateway is defined in HA settings
  - » If possible, disable the setting and create static routes via HA interface instead

Basic checks – Logs

- Any obvious errors in logs?
  - When did the issue happen?
  - **Check all logs around that time!**
- If it's a reoccurring issue, any log pattern that lines up?
- Compare against FortiGate User Event Logs
  - FortiGate logs individual user login/logout events
  - Should line up with FortiAuthenticator logs and/or debug
- Any obvious errors in debug log?
  - Verify debug log level, may not show anything useful if log level is too high
  - Search for strings like 'error', 'fail', 'timeout', 'warning'

Authentication issues

- **Enable RADIUS debug**
  - » Via CLI or GUI
- Trigger authentication issue again if possible
  - » Any output/errors in RADIUS Authentication log?
- Any patterns?
  - » Specific users, specific times, specific group memberships?
  - » Specific clients (FortiGates, third-party RADIUS clients, …)?
- If remote authentication server is involved
  - » Packet capture!
  - » Double-check for network issues of any sort

HA issues

- **Clusters can take a few minutes to form!**
  - » Errors in debug log during this time are expected!
  - » Errors should disappear after a few minutes!
- Check /debug -> HA
  - » Slony in case of active-passive cluster
  - » LB in case of load-balancing cluster
- Packet capture on HA interfaces
  - » Do NOT filter for IP; FortiAuthenticator HA daemon also communicates in 169.254.x.x range!
- Secondary (passive) node can be accessed on HA interface!
  - » Usually needs a host in the same subnet as HA interface though
- 8.0 adds an override feature to determine which node is primary when cluster recovers from a failover

More advanced setups

FSSO issues

- FortiAuthenticator logs, DNS, Routing, NTP
- Set log level „debug“ in FSSO Settings
  - » This restarts FSSO, so loses all FSSO sessions!
  - » Revert after troubleshooting!
- Check FSSO in /debug section
- Check FSSO debug on FortiGate

SAML issues

- FortiAuthenticator logs, DNS, Routing, NTP
- Check Web Service in /debug section
- **Check RADIUS Authentication log!**
- SAML debug in client browser
  - » SAML tracer plugins
- SAML debug in Service Provider

Involving Fortinet Support

When to involve Fortinet Support

- **First:**
  - Check available documentation
  - Perform at least basic troubleshooting
  - Verify that configuration is correct
  - Only then!
- When referring an issue to support, please include:
  - Any troubleshooting already performed
  - Any logs, screenshots, configuration backup, etc
  - Consulted documentation
  - Debug reports
  - Any lab results

Useful debug reports

- Debug reports also contain log files NOT available in /debug
- When referring a case to Fortinet Technical Support, always ask:
  - Summary (General overview; this may time out in larger deployments!)
  - System (HA, memory, CPU)
  - Authentication (RADIUS debug log, ensure RADIUS debug is enabled before collecting)
- Optionally include (depending on issue):
  - SSO (FSSO)
  - API (FortiAuthenticator Windows/OWA Agent)
  - WAD (Anything that involves HTTPS, like SAML, API, FortiGuard, push notification…)
  - GUI (Web issues like Internal Server Error)
  - DB (suspected database issues)
  - …

Lab/Questions

Lab demonstrations

- Monitor section
- View/filter logs
- /debug section
- Basic CLI commands
- Packet capture

- Anything else?
- Other questions?

The End

- **We made it!**
- **Thank you very much!**

- Any remaining questions?
- Further resources:
  - community.fortinet.com
  - docs.fortinet.com
- There will be a quick survey – any feedback/suggestions for improvement would be much appreciated!

Useful Articles

- How to work with FortiAuthenticator Technical Support https://community.fortinet.com/t5/FortiAuthenticator/Troubleshooting-Tip-How-to-work-with-FortiAuthenticator/ta-p/191656
- How to run a Packet Capture with FortiAuthenticator https://community.fortinet.com/t5/FortiAuthenticator/Technical-Tip-How-to-run-a-Packet-Capture-with/ta-p/196764
- Basic FortiAuthenticator troubleshooting https://community.fortinet.com/t5/FortiAuthenticator/Troubleshooting-Tip-Basic-FortiAuthenticator-troubleshooting/ta-p/337001
- Best Practices on hardening FortiAuthenticator https://community.fortinet.com/t5/FortiAuthenticator/Technical-Tip-Best-practices-on-hardening-FortiAuthenticator/ta-p/274443