

Duo Security Cheat Sheet

Legend: **Underlined Green** = Linked URL
Blue = Highlight, command, etc.
Orange = To be replaced by client-specific details



Best Practices

- 1. Check the current software version against the latest release and **recommend an upgrade** if a newer version is available.
- 2. Refer to the **TCE Troubleshooting Playbook** for in-depth guidance on how to approach an issue.
- 3. Check the **TCE Dashboard** or relevant comms to determine if this a known issue
- 4. Check the **Troubleshooting Scope Job Aid** to help demonstrate next steps with data



Information Gathering

- 1. Enable **Debug Logging**
 - a. Note the username, timestamp, and timezone.
- 2. Get the **Support Tool output or debug logs**.
 - a. The Support Tool output is available for **WinLogon, Duo Unix, Authproxy, ADFS/OWA/RD Web/RD Gateway, Duo Desktop**, and the **DNG Config Checker**.
- 3. Gather screenshots and recordings, WireShark PCAP, **HAR files**, SAML Traces, and use **DiagIC** to analyze these details and provide known issues that are documented.
- 4. Cross-reference **Kibana** for any internal logging
- 5. Check the **Escalation Checklist**
- 6. Use your **Lab** to test, if applicable

Remember to sanitize any configs and have the customer reset if they shared secrets or PWs!



Authproxy

Note: The Authenticon Proxy communicates with Duo’s service on TCP port 443. Firewall needs to be configured to permit traffic outbound.
See the **IP Ranges Knowledge Base** article for ore details..

Service Management:

- If the is failing to start, check Event Viewer -> Application and Services

Network Port Verification:

- Run the command: netstat -anop | findstr portNumberHere to ensure only one service is listening per server section in the proxy configuration.

Special Configuration:

- Use port 18120 in the server configuration if Network Policy Server (NPS) or other RADIUS servers exist

Certificate Verification:

- The ssl_ca_certs_file must include the issuing CA’s certificate (usually intermediate) and the Trusted Root CA certificate.
- Use acert.exe to verify the certificate being used.

MS-CHAPv2 Usage:

- If using MS-CHAPv2, you must configure a RADIUS Client with RADIUS Server Mode. Note that this does not allow for append mode or passcodes.

Logging and Communication:

Log interpretation:

- Logs use "C" for Client and "S" for Server.
 - Example 1: C->S indicates the proxy as a Client sent a request to your Active Directory (AD) as the Server.
 - Example 2: C<-S indicates the proxy as a Client received a response from your Domain Controller (DC).

LDAP and LDAPS:

- The AD DC presents its “leaf” cert when the authproxy reaches out to it
- ssl_ca_certs_file needs to contain leaf cert’s issuing CA’s cert (usually intermediate), and its Trusted Root CA cert. Use acert.exe to verify the cert being used.

Wireshark Analysis:

- Use the Wireshark filter: tcp.port == 636 && tls.handshake to examine TLS handshake details.



Debug Log Locations

Wordpress:

Update the config file wp-config.php with:

```
define('WP_DEBUG', true);
define('WP_DEBUG_LOG', true);
define('WP_DEBUG_DISPLAY', false);
```

Set the global variable at wp-content/plugins/duo/duo_wordpress.php to:

```
$DuoDebug = true;
```

Logs will generate at wp-content/debug.log.



RD Gateway:

Create a new REG_DWORD value called **Debug** at

HKEY_LOCAL_MACHINE\SOFTWARE\Duo Security\DuoTsg with the value set to 1

Logs will appear in C:\ProgramData\Duo Security\DuoTsg\DuoTsg.log

Epic:

Create a new DWORD value named **EpicEnableDebugLogging** at

HKLM\Software\Policies\Duo Security\Duo Epic Hyperdrive with the value set to 1

The file is named "DuoEpicHyperdrive.log" and is saved to the current user's %TEMP% directory (e.g., C:\Users\DuoUser\AppData\Local\Temp)

RD Web and OWA:

Create a new REG_DWORD value called **Debug** at

HKEY_LOCAL_MACHINE\SOFTWARE\Duo Security\DuoRdweb with the value set to 1

Events are written as entries in the "Duo IIS Integration" event log under "Applications and Services Logs" in the Event Viewer

DNG:

Run these commands to get the portal and DNS logs output:

1. docker logs network-gateway-portal > portal.log.
2. docker logs network-gateway-dns > dns.log

Note: You can also use --since and --until with relative timestamps

DuoConnect (DNG):

Add -log <path to log file> to the ProxyCommand DuoConnect line in

~/.ssh/config, e.g. -log ~/duoconnect.log or -log c:\users\xyzy\duoconnect.log

The log will be written to the duoconnect.log file in the user's home directory.

- For RDP and SMB relay connections, check the **KB article 6852!**

DAG (Fed Only):

Windows: C:\inetpub\wwwroot\dag\log\dag.log

Linux: Run command: docker-compose -p access-gateway -f access-gateway-1.5.10.yml logs -f > Dag.log

macOS Logon:

If logging levels need to be changed, run the following command as an administrator, specifying the -integer value as 0 for informational, 1 for debug, or 2 for trace:

```
sudo plutil -replace debug -integer 1
/private/var/root/Library/Preferences/com.duosecurity.maclogon.plist
```

macOS 10.12 and later - Reproduce the issue then run the following command:

```
log show --predicate='eventMessage contains "SecurityAgent" or
eventMessage contains "authorizationhost" or eventMessage contains
"MacLogon"' --last 2h > ~/Desktop/maclogon.log
```

You will need to adjust two variables:

- ~/Desktop/maclogon.log is the file location where the logs will be saved
- --last 2h should be the time range in which you recreated the issue.

macOS 10.11 and earlier

Reproduce the issue. The logs are located at /var/log/system.log



Cloud


Traffic destined toward API hostnames (api-xxxxxx.duosecurity.com), where xxxxxx is the CustDNS.

Note: The Authenticon Proxy communicates with Duo’s service on TCP port 443. Firewall(s) needs to be configured to permit traffic outbound.

Troubleshooting Cloud Issues

- Use an alternative network (e.g., mobile hotspot) to rule out local network issues.
- Verify that the device or network can reach Duo’s API host endpoint:
 - Note: ICMP is disabled; ping and traceroute are not applicable
 - Verify connectivity by ensuring the endpoint https://api-xxxxxx.duosecurity.com/auth/v2/ping is reachable.
 - For detailed steps, refer to **KB 1337**.
 - On macOS and Linux devices, run curl -V to test.
 - ex. curl https://api-xxxxxx.duosecurity.com/auth/v2/ping
 - On Windows devices, use Powershell to run Invoke-WebRequest -Uri https://api-xxxxxx.duosecurity.com/auth/v2/ping
 - ex. Invoke-WebRequest -Uri https://api-xxxxxx.duosecurity.com/auth/v2/ping

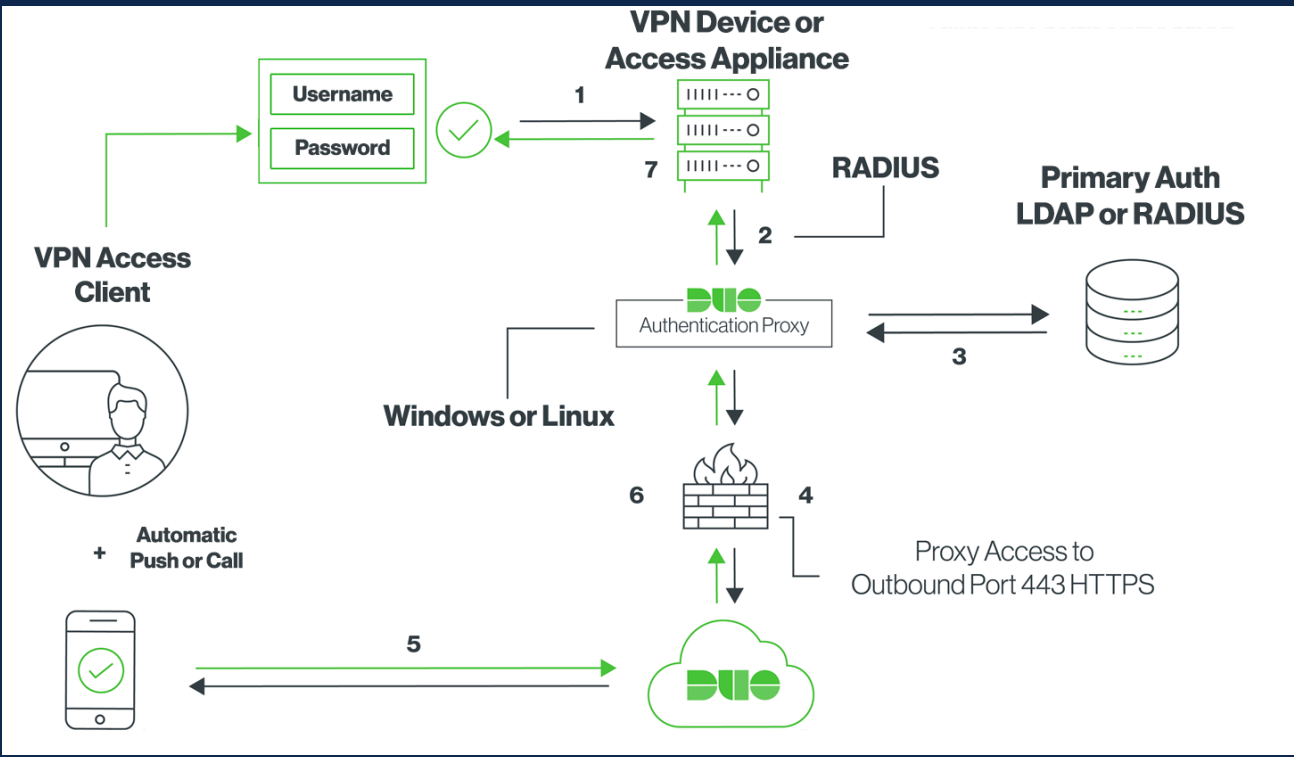
- Use the following CLI commands to verify that the Duo API hostname correctly resolved to an IP Address:
 - nslookup <hostname> | Check if a domain resolves and shows the corresponding IP address
 - dig <hostname> | Provide details DNS query details, such as IP address, query time, and DNS server used.

- **TLS Inspection:**
 - Download Wireshark and select Capture to get network details.
 - In the filter section, type tcp.port == 443 && tls.handshake
 - Analyze the output for signs of an HTTP proxy or firewall modifying traffic (ex. different certificate presentation, multiple TLS handshakes, TCP RST packets).
- **TLS Version Verification:**
 - Locate the Client Hello and Server Hello packets in Wireshark
 - Select the Client Hello packet from the info column in Wireshark
 - Verify the TLS version offered in the Version field (should be 1.2 or greater)
 - Select the Server Hello packet form the info column in Wireshark
 - Verify the TLS version selected by the server in the Version field
- **Check Cipher Suites:**
 - Ensure the Client Hello contains supported Ciphers. Refer to the **KB 2152**.
- **Certificate Verification:**
 - Click the icon  beside the “https://” in the browser bar and verify the certificate is issued to *.duosecurity.com by “DigiCert with SHA2 High Assurance Server CA.”

Troubleshooting Tools

Tool	Use
Connectivity Tool	Diagnose and troubleshoot network connectivity issues between the Authentication Proxy and other components, such as RADIUS servers or Active Directory
Support Tool	Collect logs and configuration files from the Authentication Proxy to gather details

Authentication Proxy Diagram



1. Primary authentication initiated to application or service
2. Application or service sends authentication request to the Duo Security Authentication Proxy
3. Primary authentication using Active Directory or RADIUS
4. Duo Authentication Proxy connection established to Duo Security over TCP port 443
5. Secondary authentication via Duo Security’s service
6. Duo Authentication Proxy receives authentication response
7. Application or service access granted