

Configuring TekRADIUS with Cisco ASA's, AnyConnect, Active Directory and Google Authenticator

Secure 2Fa VPN - Proof of Concept (POC) – August 2020

Author	Greg.Roberts@Sussexpartnership.nhs.uk
Edited by	Yasin KAPLAN (KaplanSoft)
Version	1.0
Date	11/08/2020
Company	Sussex Partnership NHS Foundation Trust (UK)

Introduction

This document is a high-level introduction to using TekRADIUS alongside a Cisco ASA / AnyConnect environment with Active Director and Google Authenticator to deliver secure 2 Factor VPN.

This document won't go into detailed TekRADIUS Installation steps or SQL Server Configuration and will assume that both are installed and Microsoft SQL server is configured.

Supporting Guides

As this document is only High Level, it is designed to be used alongside all of the supporting documentation provided by KaplanSoft.

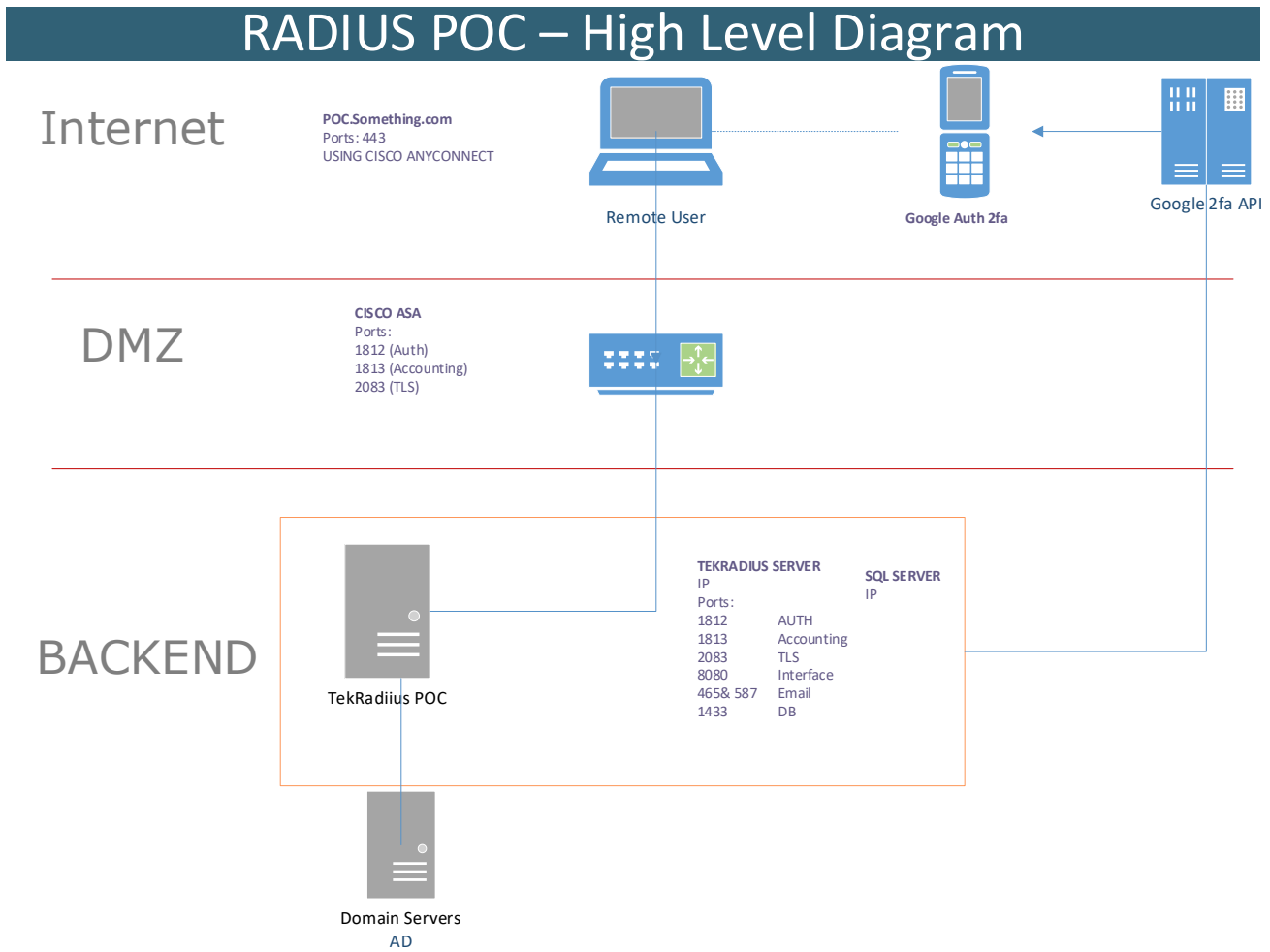
- <https://www.kaplansoft.com/TekRADIUS/Docs/Manual.pdf>
- <https://www.kaplansoft.com/tekradius/Docs/2FA.pdf>
- <https://www.kaplansoft.com/tekradius/Docs/Google-Authenticator.pdf>
- <https://www.kaplansoft.com/TekRADIUS/Docs/Parallels-2FA.pdf>

Version Specifics

This Proof of Concept System uses:

- Cisco ASA (ASA 55x5-X)
 - Working on: asa964-36-smp-k8.bin / firmware 9.6(4)36
- Cisco AnyConnect 4.6.00362
 - Windows 10 Laptop for testing 1803 – OS Build 17134.1304
- TekRadius SP (Trial), version 5.5.4.25
- Android - For Google Auth Client

High Level Design

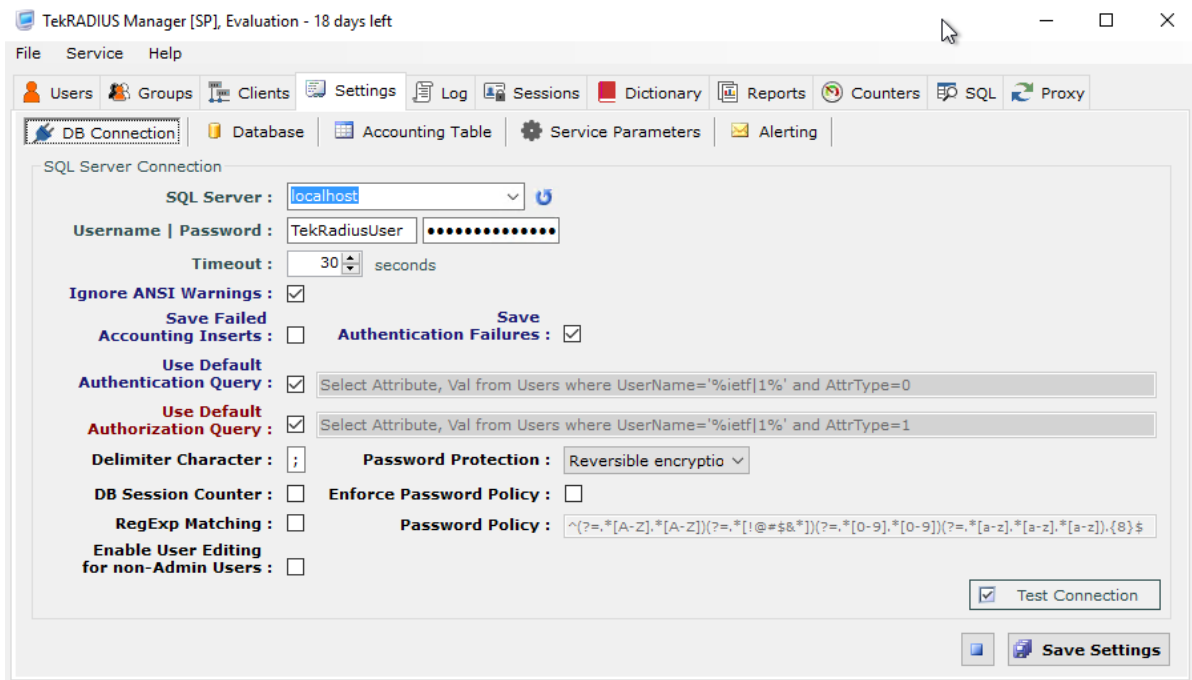


Configuration

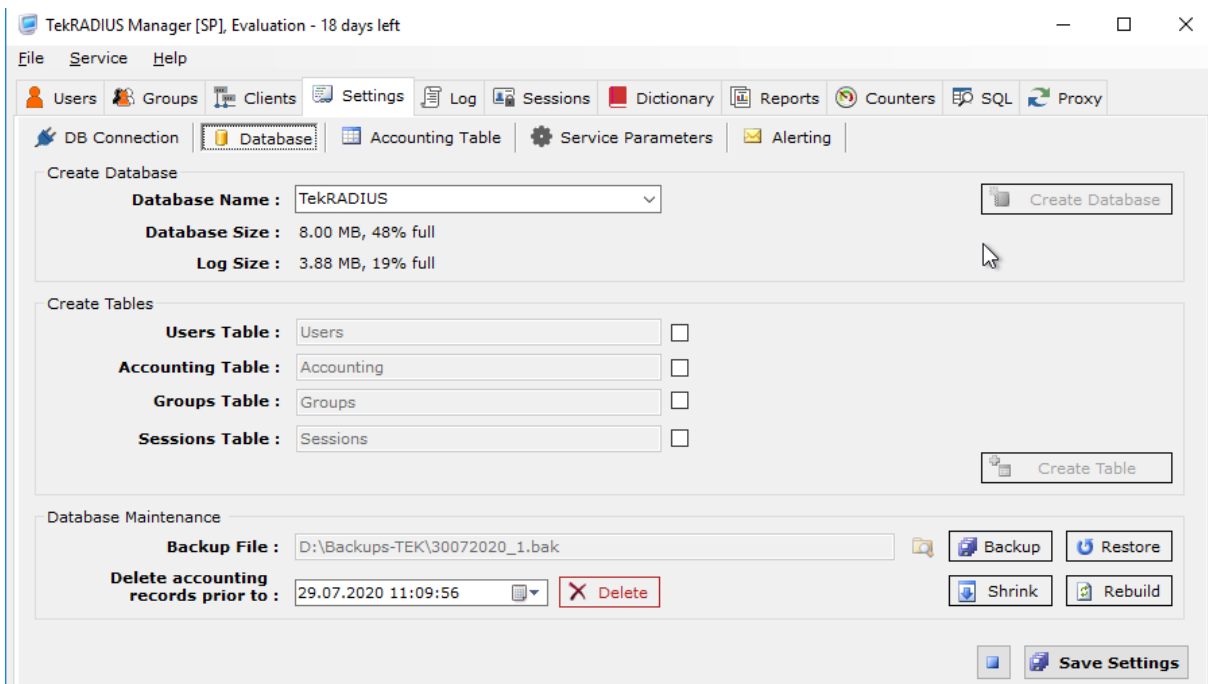
The below sections highlight key configuration settings required, or show screenshots of the local configuration. You will need to adapt the IP addresses and ports to suit your needs.

TekRADIUS

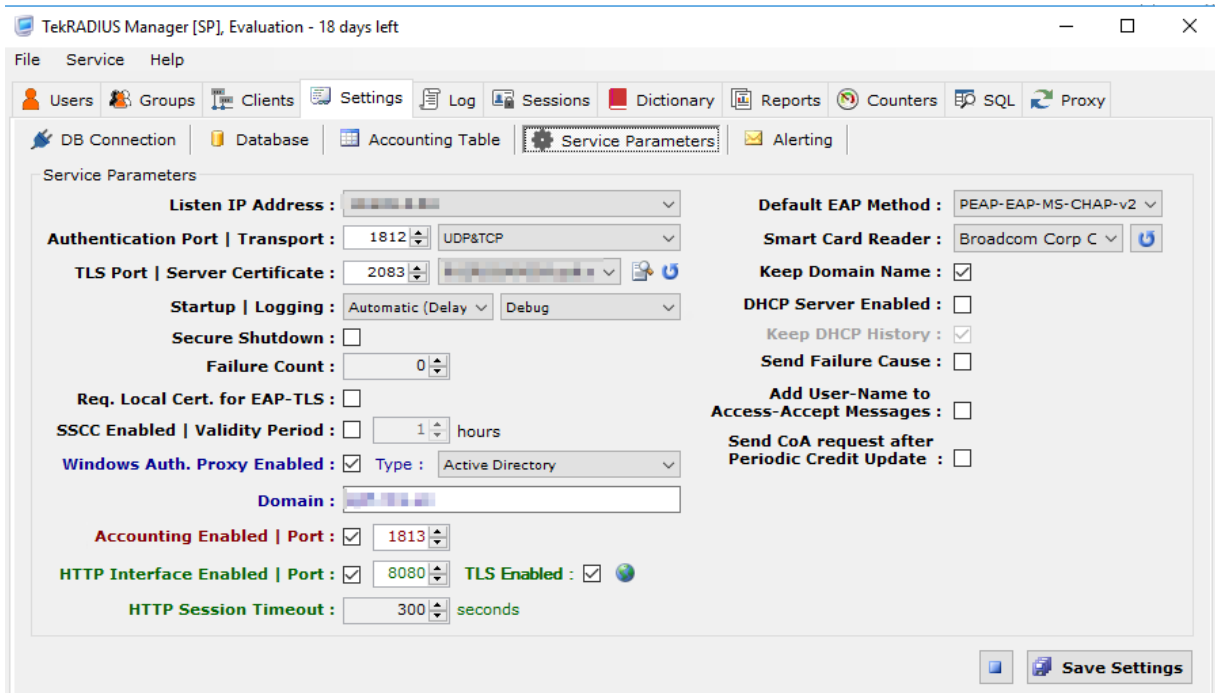
DB Connection



Database



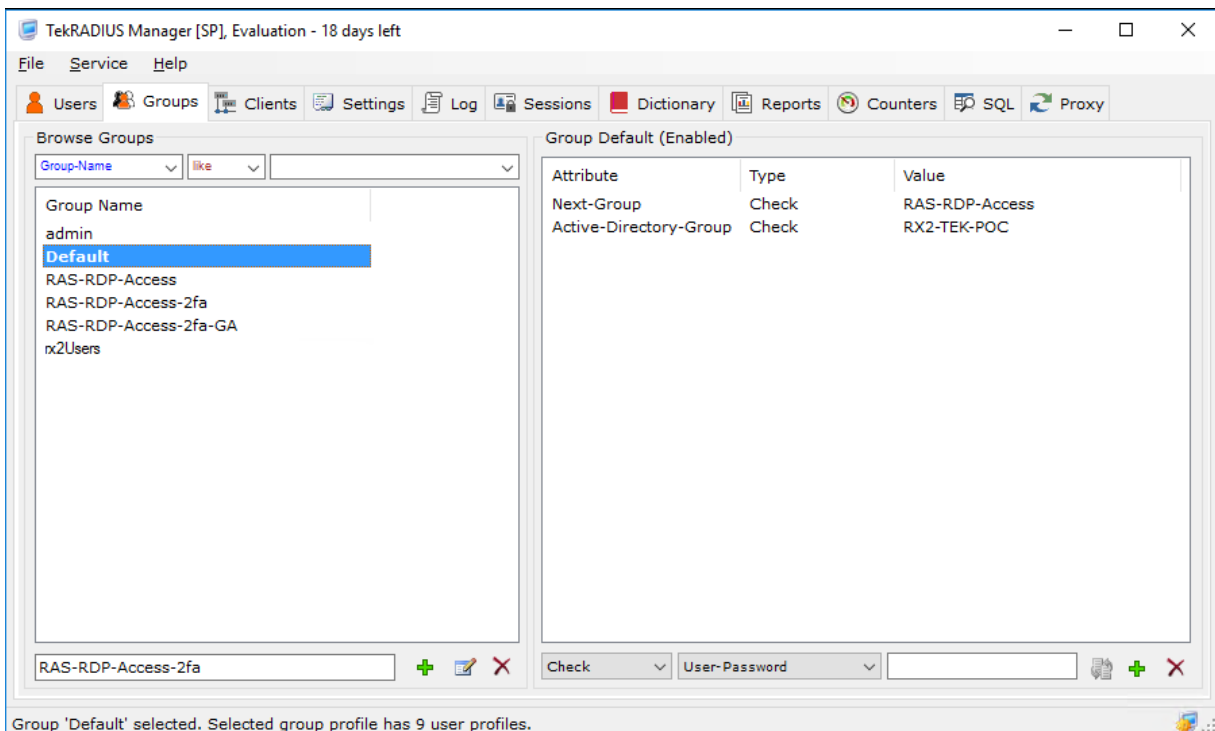
Service Setting



Groups

Create groups as follows

- Default
- RAS-RDP-Access
- RAS-RDP-Access-2fa
- RAS-RDP-Access-2fa-GA



Configuring TekRADIUS with Cisco ASA's, AnyConnect, Active Directory and Google Authenticator

Attribute	Type	Value
NAS-IP-Address	Check	[Redacted]
Next-Group	Check	RAS-RDP-Access-2fa
Active-Directory-Group	Check	RX2-TEK-RAS
Success-Reply-Type	Check	Accept

Attribute	Type	Value
NAS-IP-Address	Check	[Redacted]
Next-Group	Check	RAS-RDP-Access-2fa-GA
Active-Directory-Group	Check	RX2-TEK-2fa
Success-Reply-Type	Check	Challenge
Reply-Message	Success-Reply	Please enter your Google Auth...
Reply-Message	Failure-Reply	Active directory Authentication E...

Ensure that your AD user you wish to use, is added to the active directory group Above (In this case – RX2-TEK-2fa)

Attribute	Type	Value
NAS-IP-Address	Check	[Redacted]
Next-Group	Check	rx2Users
Authentication-Method	Check	Google-Authenticator

No other settings are required to test.

Cisco ASA

Sample redacted configuration:

```
tunnel-group TEKRAIUS type remote-access
tunnel-group TEKRAIUS general-attributes
address-pool VPN-DHCPCLIENTS
authentication-server-group TEKRAIUS
default-group-policy GroupPolicyNAME
tunnel-group TEKRAIUS webvpn-attributes
group-alias TEKRAIUS enable
```

Configuring TekRADIUS with Cisco ASA's, AnyConnect, Active Directory and Google Authenticator

```
group-policy GroupPolicyNAME internal
group-policy GroupPolicyNAME attributes
wins-server none
dns-server value 192.168.0.1 192.168.2.1
vpn-tunnel-protocol ssl-client
default-domain value Your.Domain.com
aaa-server TEKRADIUS protocol radius
aaa-server TEKRADIUS (inside) host 10.1.2.3
timeout 60
key *****
authentication-port 1812
accounting-port 1813
```

Cisco AnyConnect

Sample XML Profile

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
  <ClientInitialization>
    <UseStartBeforeLogon UserControllable="false">>false</UseStartBeforeLogon>
    <AutomaticCertSelection UserControllable="false">>true</AutomaticCertSelection>
    <ShowPreConnectMessage>>false</ShowPreConnectMessage>
    <CertificateStore>Machine</CertificateStore>
    <CertificateStoreMac>All</CertificateStoreMac>
    <CertificateStoreOverride>>true</CertificateStoreOverride>
    <ProxySettings>IgnoreProxy</ProxySettings>
    <AllowLocalProxyConnections>>false</AllowLocalProxyConnections>
    <AuthenticationTimeout>12</AuthenticationTimeout>
    <AutoConnectOnStart UserControllable="false">>false</AutoConnectOnStart>
    <MinimizeOnConnect UserControllable="true">>false</MinimizeOnConnect>
    <LocalLanAccess UserControllable="false">>false</LocalLanAccess>
    <DisableCaptivePortalDetection UserControllable="false">>false</DisableCaptivePortalDetection>
    <ClearSmartcardPin UserControllable="false">>true</ClearSmartcardPin>
    <IPProtocolSupport>IPv4</IPProtocolSupport>
    <AutoReconnect UserControllable="false">>true
      <AutoReconnectBehavior
UserControllable="false">DisconnectOnSuspend</AutoReconnectBehavior>
    </AutoReconnect>
    <SuspendOnConnectedStandby>>false</SuspendOnConnectedStandby>
    <AutoUpdate UserControllable="false">>false</AutoUpdate>
    <RSA SecurIDIntegration UserControllable="false">Automatic</RSA SecurIDIntegration>
    <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
    <LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
    <WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
    <LinuxVPNEstablishment>LocalUsersOnly</LinuxVPNEstablishment>
    <AutomaticVPNPolicy>>false</AutomaticVPNPolicy>
    <PPPEXclusion UserControllable="false">Automatic
      <PPPEXclusionServerIP UserControllable="false"></PPPEXclusionServerIP>
```

Configuring TekRADIUS with Cisco ASA's, AnyConnect, Active Directory and Google Authenticator

```
</PPPExclusion>
<EnableScripting UserControllable="false">>false</EnableScripting>
<BackupServerList>
    <HostAddress>HostAddress1.Something.com</HostAddress>
    <HostAddress>HostAddress2.Something.com</HostAddress>
    <HostAddress>HostAddress3.Something.com</HostAddress>
</BackupServerList>
<EnableAutomaticServerSelection UserControllable="false">>false
    <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
    <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>false</AllowManualHostInput>
</ClientInitialization>
<ServerList>
    <HostEntry>
        <HostName>HostAddress1.Something.com</HostName>
        <HostAddress>HostAddress1.Something.com</HostAddress>
        <BackupServerList>
            <HostAddress>HostAddress1.Something.com</HostAddress>
            <HostAddress>HostAddress2.Something.com</HostAddress>
            <HostAddress>HostAddress3.Something.com</HostAddress>
        </BackupServerList>
    </HostEntry>
    <HostEntry>
        <HostName>HostAddress2.Something.com</HostName>
        <HostAddress>HostAddress2.Something.com</HostAddress>
        <BackupServerList>
            <HostAddress>HostAddress1.Something.com</HostAddress>
            <HostAddress>HostAddress2.Something.com</HostAddress>
            <HostAddress>HostAddress3.Something.com</HostAddress>
        </BackupServerList>
    </HostEntry>
    <HostEntry>
        <HostName>HostAddress3.Something.com</HostName>
        <HostAddress>HostAddress3.Something.com</HostAddress>
        <BackupServerList>
            <HostAddress>HostAddress1.Something.com</HostAddress>
            <HostAddress>HostAddress2.Something.com</HostAddress>
            <HostAddress>HostAddress3.Something.com</HostAddress>
        </BackupServerList>
    </HostEntry>
    <HostEntry>
        <HostName>TEKRADIUS_TEST.Something.com</HostName>
        <HostAddress>TEKRADIUS_TEST.Something.com</HostAddress>
    </HostEntry>
</ServerList>
</AnyConnectProfile>
```

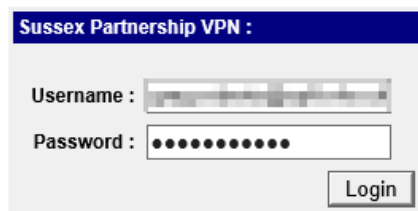
Microsoft SQL

Configuration set as per: <https://www.kaplansoft.com/TekRADIUS/Docs/Manual.pdf>

TekRADIUS User Registration (Google Auth)

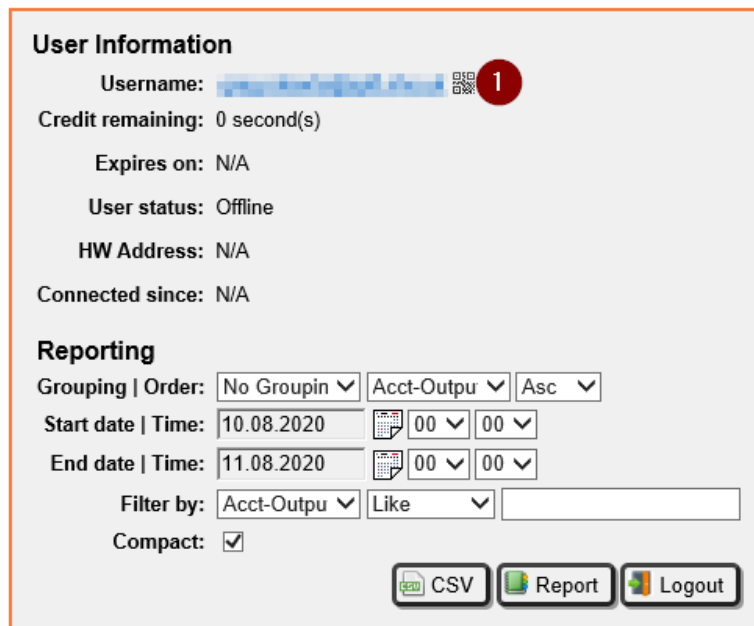
Go to URL: **http(s)://<IP address of TekRADIUS installed machine>:8080/**

Login using your Active Directory username and password. (Ensuring the user is added to the correct AD group above)

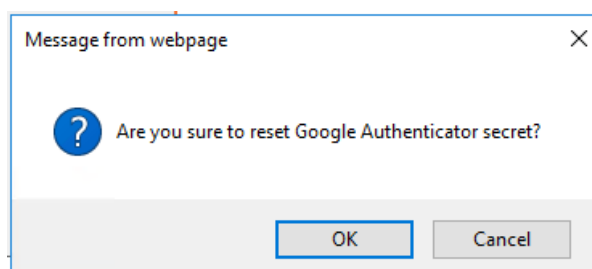


Click the small QR Code icon next to the username (1)

TekRADIUS User Reports




Accept the browser popup message (OK in this example, but each browser may be different):



Using your Phone's QR code scanner, scan the QR code now shown. (1)

TekRADIUS User Reports

User Information

Username: greg.roberts@spft.nhs.uk 


Credit remaining: 0 second(s)

Expires on: N/A

User status: Offline

HW Address: N/A

Connected since: N/A



Reporting

Grouping | Order:

Start date | Time:

End date | Time:

Filter by:

Compact:

Note: Each time you load a new QR code the old one(s) will be invalidated.

Testing

Load up Cisco AnyConnect

Select the server required, based on your AnyConnect xml profiles, and click connect.

