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.

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

# **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
  - $\circ$   $\:$  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

| 🥃 TekRADIUS Manager [SP], Evaluation - 18 days left  | 2              | -           |           |
|--|----------------|-------------|-----------|
| File Service Help  | 20             |             |           |
| 👗 Users 🕷 Groups 🏢 Clients 🗐 Settings 🗐 Log 🗳 Sessions 📕 Dictionary 🖾 Reports 🔊 Counters                     | BO SQL         | 2 Proxy     |           |
| 📝 DB Connection 🔋 Database 🔠 Accounting Table 🔹 Service Parameters 🖂 Alerting                                |                |             |           |
| SQL Server Connection  |                |             |           |
| SQL Server : localhost 🗸 😈   |                |             |           |
| Username   Password : TekRadiusUser  |                |             |           |
| Timeout : 30 seconds   |                |             |           |
| Ignore ANSI Warnings : 🗸   |                |             |           |
| Save Failed Save<br>Accounting Inserts : Authentication Failures : 🗹   |                |             |           |
| Use Default Authentication Query:  Select Attribute, Val from Users where UserName='%ietf 1%' and AttrType=0 |                |             |           |
| Use Default<br>Authorization Query :   |                |             |           |
| Delimiter Character : ; Password Protection : Reversible encryptio ~   |                |             |           |
| DB Session Counter : 🗌 Enforce Password Policy : 🗌   |                |             |           |
| RegExp Matching :         Password Policy :         ^(?=,*[A-Z],*[A-Z])(?=,*[!@#\$&*])(?=,*[0-9],*[0-9])     | 9])(?=,*[a-z], | *[a-z],*[a- | z]).{8}\$ |
| Enable User Editing  |                |             |           |
|  |                | Test Conr   | nection   |
|  |                | 🗿 Save      | Settings  |

### Database

| FekRADIUS Manager [SP], Evaluation - 18 days left  | -            |           | ×  |
|--|--------------|-----------|----|
| <u>F</u> ile <u>S</u> ervice <u>H</u> elp  |              |           |    |
| 👗 Users 🛎 Groups 腪 Clients 🗐 Settings 🗐 Log 🗳 Sessions 📕 Dictionary 👜 Reports 🔊 Counters 月 | 🗭 SQL 🎅 Prox | У         |    |
| 🗩 DB Connection 🛛 🚺 Database 🗮 Accounting Table 🛛 🏶 Service Parameters 🖂 Alerting          |              |           |    |
| Create Database  |              |           |    |
| Database Name : TekRADIUS  | Create I     | Database  |    |
| Database Size : 8.00 MB, 48% full  |              |           |    |
| Log Size : 3.88 MB, 19% full   | 3            |           |    |
| Create Tables  |              |           |    |
| Users Table : Users  |              |           |    |
| Accounting Table : Accounting  |              |           |    |
| Groups Table : Groups  |              |           |    |
| Sessions Table : Sessions  |              |           | _  |
|  | Create       | Table     |    |
| Database Maintenance   |              |           |    |
| Backup File: D:\Backups-TEK\30072020_1.bak   | 🗊 Backup 🔮   | Restore   |    |
| Delete accounting<br>records prior to : 29.07.2020 11:09:56                                | 😺 Shrink 🔮   | Rebuild   |    |
|  | 🔳 🗿 Sav      | e Setting | js |

## Service Setting

| 🥃 TekRADIUS Manager [SP], Evaluation - 18 days left – 🛛  | ×   |
|--|-----|
| File Service Help  |     |
| 💄 Users 🔱 Groups 📜 Clients 🗐 Settings 🗐 Log 🗳 Sessions 📕 Dictionary 🚇 Reports 🔊 Counters 🗊 SQL ぞ Proxy |     |
| 💉 DB Connection 🔋 Database 🔲 Accounting Table 🛛 🏟 Service Parameters                                   |     |
| Service Parameters   |     |
| Listen IP Address : Default EAP Method : PEAP-EAP-MS-CHAP-v2 v   | 1   |
| Authentication Port   Transport : 1812 🖕 UDP&TCP V Smart Card Reader : Broadcom Corp C V               | 5   |
| TLS Port   Server Certificate : 2083 🛊 🛛 Keep Domain Name : 🗸  |     |
| Startup   Logging : Automatic (Delay $\lor$ Debug $\lor$ DHCP Server Enabled :                         |     |
| Secure Shutdown : 🗌 Keep DHCP History : 🗸  |     |
| Failure Count : 0 🔶 Send Failure Cause :   |     |
| Req. Local Cert. for EAP-TLS :   |     |
| SSCC Enabled   Validity Period :   |     |
| Windows Auth. Proxy Enabled : V Type : Active Directory V Periodic Credit Update :                     |     |
| Domain : Domain :  |     |
| Accounting Enabled   Port : 🔽 1813   |     |
| HTTP Interface Enabled   Port : 🗹 🛛 😵 💭 TLS Enabled : 🗹 🎯  |     |
| HTTP Session Timeout : 300 📩 seconds   |     |
| Save Sett  | ngs |

# Groups

### Create groups as follows

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

|                                      | ungs j= Log e |   | essions Dictionary (    |               | y counters by SQL       | FIOXY |  |
|--------------------------------------|---------------|---|-------------------------|---------------|-------------------------|-------|--|
| Browse Groups                        |               |   | Group Default (Enabled) |               |                         |       |  |
| Group Name                           |               | 4 | Attribute<br>Next-Group | Type<br>Check | Value<br>RAS-RDP-Access |       |  |
| admin                                |               |   | Active-Directory-Group  | Check         | RX2-TEK-POC             |       |  |
| Default                              |               |   |                         |               |                         |       |  |
| RAS-RDP-Access<br>RAS-RDP-Access-2fa |               |   |                         |               |                         |       |  |
| RAS-RDP-Access-2fa-GA                |               |   |                         |               |                         |       |  |
|                                      |               |   |                         |               |                         |       |  |
|                                      |               |   |                         |               |                         |       |  |

| Lusers           | 歶 Groups      | Clients | 🗐 Settings | 🗐 Log |        | Sessions | E Dictionary   | E Reports      | 🔊 Cou  | nters   | 🗊 sql     | 2 Proxy      |       |
|------------------|---------------|---------|------------|-------|--------|----------|----------------|----------------|--------|---------|-----------|--------------|-------|
| Browse           | Groups        |         |            |       |        | Group    | RAS-RDP-Acces  | s (Enabled)    |        |         |           |              |       |
| Group-Nan        | ne 🗸 🔤        | e ~     |            |       | $\sim$ | Attribu  | te             | Туре           |        | Value   |           |              |       |
| Group            | Name          |         |            |       |        | NAS-I    | P-Address      | Check          |        | 10.00   |           |              |       |
| admin<br>Default |               |         |            |       |        | Next-0   | Group          | Check          |        | RAS-R   | RDP-Acce  | ss-2fa       |       |
|                  |               |         |            |       |        | Active   | Directory-Grou | p Check        |        | RX2-T   | EK-RAS    |              |       |
| RAS-RDP-Access   |               |         |            |       |        |          | ss-Reply-Type  | Check          |        | Accep   | t         |              |       |
| RAS-RE           | OP-Access-2fa | 1       |            |       |        |          |                |                |        |         |           |              |       |
| RAS-RE           | OP-Access-2fa | i-GA    |            |       |        |          |                |                |        |         |           |              |       |
| rx2Users         |               |         |            |       |        |          |                |                |        |         |           |              |       |
|                  |               |         |            |       |        |          |                |                |        |         |           |              |       |
|                  |               |         |            |       |        |          |                |                |        |         |           |              |       |
|                  |               |         |            |       |        |          |                |                |        |         |           |              |       |
| Lusers           | 😹 Groups      | Clients | 🗐 Settings | 🗐 Log |        | Sessions | E Dictionary   | Reports        | 🔊 Cour | nters   | 🗊 SQL     | 2 Proxy      |       |
| Browse           | Groups        |         |            |       |        | Group F  | AS-RDP-Acces   | s-2fa (Enabled | d)     |         |           |              |       |
| Group-Nan        | ne 🗸 🛤        | e 🗸     |            |       | $\sim$ | Attribu  | te             | Type           |        | Value   |           |              |       |
| Group            | Name          |         |            |       |        | NAS-IF   | -Address       | Check          |        |         |           |              |       |
| admin            | Nume          |         |            |       |        | Next-G   | iroup          | Check          |        | RAS-R   | DP-Acces  | s-2fa-GA     |       |
| Default          |               |         |            |       |        | Active   | Directory-Grou | p Check        |        | RX2-TE  | EK-2fa    |              |       |
| RAS-RI           | DP-Access     |         |            |       |        | Succes   | s-Reply-Type   | Check          |        | Challer | nge       |              |       |
| RAS-R            | DP-Access-2   | 2fa     |            |       |        | Reply-   | Message        | Success-R      | teply  | Please  | enter yo  | ur Google Au | uthe  |
| RAS-RI           | DP-Access-2fa | a-GA    |            |       |        | Reply-   | Message        | Failure-Re     | ply    | Active  | directory | Authenticati | ion F |
| rx2Users         |               |         |            |       |        |          |                |                |        |         |           |              |       |
|                  |               |         |            |       |        |          |                |                |        |         |           |              |       |
|                  |               |         |            |       |        |          |                |                |        |         |           |              |       |

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



No other settings are required to test.

### Cisco ASA

#### Sample redacted configuration:

tunnel-group TEKRADIUS type remote-access tunnel-group TEKRADIUS general-attributes address-pool VPN-DHCPCLIENTS authentication-server-group TEKRADIUS default-group-policy GroupPolicyNAME tunnel-group TEKRADIUS webvpn-attributes group-alias TEKRADIUS enable 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/XMLSchemainstance" 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> <RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration> <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement> <LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement> <WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment> <LinuxVPNEstablishment>LocalUsersOnly</LinuxVPNEstablishment> <AutomaticVPNPolicy>false</AutomaticVPNPolicy> <PPPExclusion UserControllable="false">Automatic <PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>

```
</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>
        <HostEntrv>
                <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>
        </HostEntrv>
        <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: <u>https://www.kaplansoft.com/TekRADIUS/Docs/Manual.pdf</u>

# 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)

| Sussex Partne | ership VPN :              |
|---------------|---------------------------|
|               |                           |
| Username :    | provide the particular of |
| Password :    | •••••                     |
|               | Login                     |

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

| User Informatio    | on                              |
|--------------------|---------------------------------|
| Username:          |                                 |
| Credit remaining:  | 0 second(s)                     |
| Expires on:        | N/A                             |
| User status:       | Offline                         |
| HW Address:        | N/A                             |
| Connected since:   | N/A                             |
| Reporting          |                                 |
| Grouping   Order:  | No Groupin V Acct-Outpu V Asc V |
| Start date   Time: | 10.08.2020                      |
| End date   Time:   | 11.08.2020                      |
| Filter by:         | Acct-Outpu V Like V             |
| Compact:           | $\checkmark$                    |
|                    | 📾 CSV 🕒 Report 📲 Logout         |

### **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 Informatio    | on                              |   |
|--------------------|---------------------------------|---|
| Username:          | greg.roberts@spft.nhs.uk        |   |
| Credit remaining:  | 0 second(s)                     |   |
| Expires on:        | N/A 📝 🙍                         |   |
| User status:       | Offline 1                       |   |
| HW Address:        | N/A 📐 🚠                         |   |
| Connected since:   |                                 |   |
| Reporting          |                                 |   |
| Grouping   Order:  | No Groupin 🗸 Acct-Outpu 🗸 Asc 🗸 |   |
| Start date   Time: | 10.08.2020                      |   |
| End date   Time:   | 11.08.2020                      |   |
| Filter by:         | Acct-Outpu 🗸 Like 🗸             |   |
| Compact:           | $\checkmark$                    |   |
|                    | 🔤 CSV 💷 Report 📲 Logout         | ] |

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.

| 🔇 Cisco AnyC  | onnect Secure Mobility Client            | — |         | ×     |  |
|---------------|--|---|---------|-------|--|
|               | VPN:<br>Ready to connect.<br>remote-test |   | Connect |       |  |
| <b>\$</b> (i) |  |   |         | cisco |  |

| 🕥 Cisco Any | Connect Sec                      | ure Mobility Client                    | - 🗆                                   | ×                  |
|-------------|----------------------------------|--|---------------------------------------|--------------------|
|             | VPN:<br>Please entr              | er your username and pa                | ssword.<br>Connect                    |                    |
| Cisc        | o AnyConne                       | ct   remote-test.                      | · · · · · · · · · · · · · · · · · · · | altalt<br>sco<br>X |
|             | Please enter                     | r your username and pas                | sword.                                |                    |
|             | Group:                           | TEKRADIUS                              | ~                                     |                    |
|             | Username:                        | username                               |                                       |                    |
|             | Password:                        |  |                                       |                    |
|             |                                  | OK                                     | Cancel                                | _                  |
| 🕥 Cisco Any | Connect Sec                      | ure Mobility Client                    | -                                     | $\times$           |
|             | VPN:                             | est.                                   | Continue                              | 2                  |
| 🕥 Ci        | sco AnyCon                       | nect   remote-test.                    | - interesting                         | ×                  |
|             | Answer:<br>Please er<br>Time Pas | Ter your Google Authen<br>sword (OTP). | ticator One                           |                    |
|             |                                  |  |                                       |                    |