webdyn

flexitron group

ROUTER TITAN

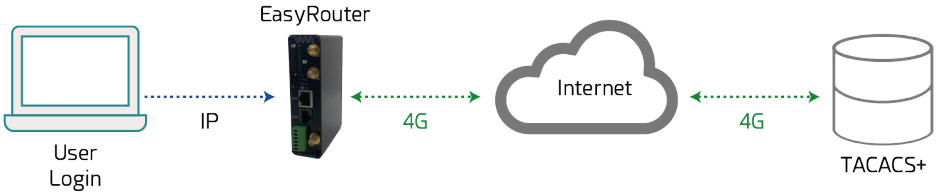
Nota de aplicación 74

Autenticación y autorización mediante TACACS+

Autenticación y autorización mediante TACACS+

Detalles del escenario

Los routers Titan permiten diversas maneras de autenticar y autorizar a los usuarios. Permite una autenticación de tipo local, donde es el propio router Titan quien se encarga de comprobar que un determinado usuario y password introducidos son correctos. Además permite la autenticación y autorización remotas por TACACS+ o por LDAP, donde es un servidor externo quien realiza esas tareas. En esta nota de aplicación se mostrará un ejemplo de configuración de acceso a la GUI del usuario por HTTP de forma local y remota por TACACS+.



1. Descripción del escenario de ejemplo

En este ejemplo se pretende configurar un dispositivo WEBDYN-EASY-ROUTER con autenticación LOCAL y autenticación por TACACS+. En este ejemplo se configurará una cuenta LOCAL de nivel administrador para poder acceder al router vía GUI (HTTP) localmente en caso de problemas de conectividad.

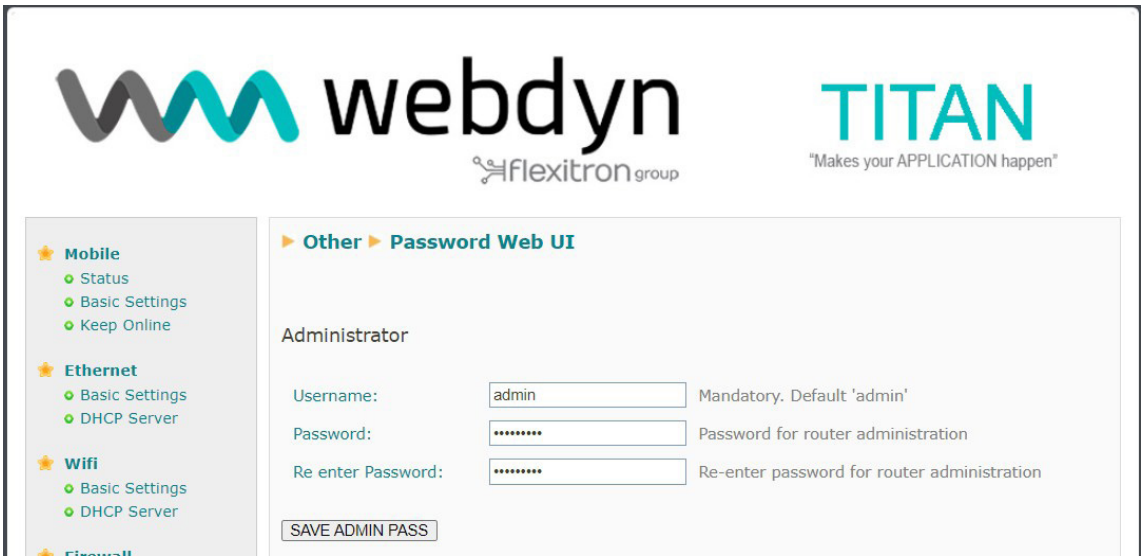
Adicionalmente se requiere configurar el router para permitir la autenticación y autorización mediante un servidor TACACS+ remoto para el acceso al router vía GUI (HTTP). En este ejemplo con TACACS+ se pretende crear una cuenta con un usuario de nivel “admin” y tres usuarios de nivel “user”, es decir, con acceso limitado a la configuración del router.

En este ejemplo se da por hecho que el dispositivo WEBDYN-EASY-ROUTER ya está correctamente configurado para tener conectividad a Internet.

2. Configuración de los usuarios LOCALES

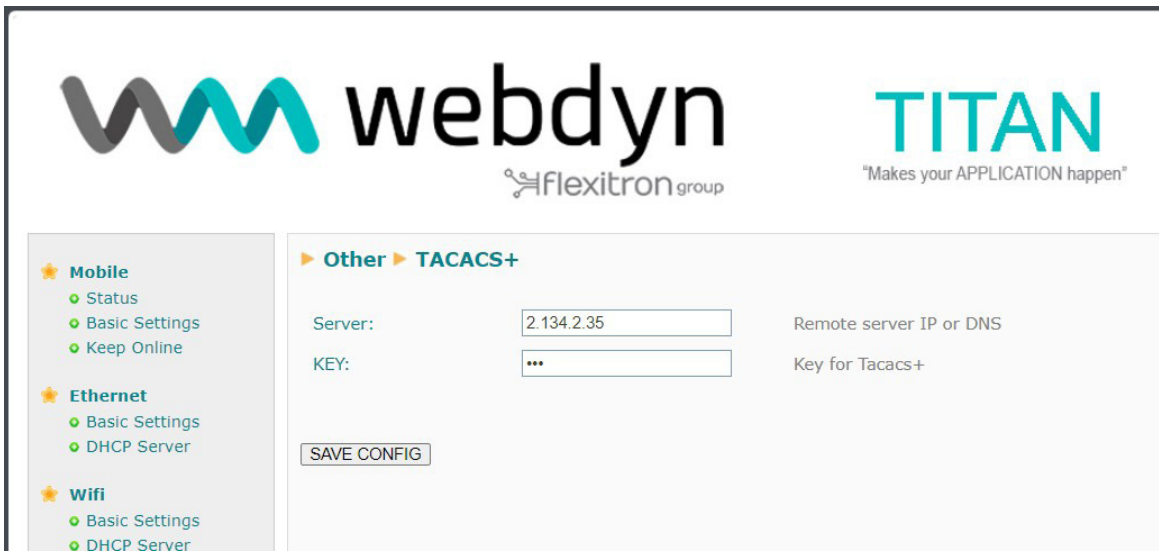
La configuración local de usuarios se realiza desde la sección “Other-Passwords Web UI” Desde ahí pueden configurarse 3 usuarios. Uno con nivel “admin”, otro con nivel “general user” y otro con nivel “guest”.

En este ejemplo únicamente vamos a tener un usuario con nivel admin, por lo que creamos el usuario “admin” con password, por ejemplo, “add788*12”

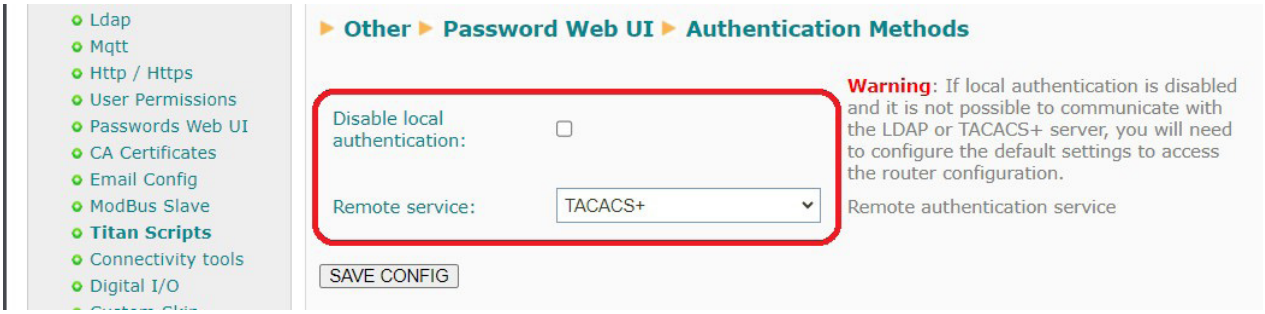


3. Configuración de los usuarios con TACACS+

Para la configuración TACACS+ lo primero que debe configurarse es la sección de conexión con el servidor TACACS+. Para ello debe acudirse al menú "Other - Tacacs+". La configuración es bastante simple, debemos introducir únicamente la DNS o IP del servidor TACACS+ y un password, que en este ejemplo será "mtx"



Ahora debe especificarse que la autenticación del servicio GUI (HTTP) además realizarse tanto localmente como vía TACACS+. Eso se hace desde el menú "Other - Other - Passwords Web UI". En la parte inferior de esa pantalla debe escogerse, en la opción "Remote Service", el valor "TACACS+". La casilla "Disable local authentication" no debe seleccionarse en este escenario, pues se pretende que la autenticación LOCAL siga funcionando.



Hecho esto tan sólo queda reiniciar el WEBDYN-EASY-ROUTER para que tome la nueva configuración.

4. Configurando un servidor TACACS+

Para este ejemplo se va a utilizar y configurar el servidor Tacacs+ de www.tacacs.net

Tal y como se indicó en el inicio, se van a utilizar 4 usuarios, uno con el role de administrador y los otros 3 con el role de usuario general.

Usuario	Password	Role
user1	mypass1	admin
user2	mypass2	user
user3	mypass3	user
user4	mypass4	user

En el fichero “authentication.xml” tendremos definidos 3 grupos: “webdynadmin”, “webdynuser” y “webdynguest”, dentro de los cuales deben incluirse los 4 usuarios apropiados (user1, user2, user3, user4). Este sería un ejemplo de fichero “authenticacion.xml”:

```
<?xml version=”1.0” encoding=”utf-8”?>
<!-- Version 1.2 -->
<Authentication  xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance”  xmlns:xsd=”http://www.
w3.org/2001/XMLSchema”>
        <UserGroups>
                <UserGroup>
                        <Name>webdynadmin</Name>
                        <AuthenticationType>File</AuthenticationType>
                        <Users>
                                <User>
                                        <Name>user1</Name>
                                        <LoginPassword ClearText=”mypass1” DES=””> </
LoginPassword>
                                        <EnablePassword ClearText=”” DES=””></EnablePassword>
                                        <CHAPPassword ClearText=”” DES=””> </CHAPPassword>
                                        <OutboundPassword ClearText=”” DES=””> </
OutboundPassword>
                                </User>
                        </Users>
                </UserGroup>

                <UserGroup>
                        <Name>webdynuser</Name>
                        <AuthenticationType>File</AuthenticationType>
                        <Users>
                                <User>
                                        <Name>user2</Name>
                                        <LoginPassword ClearText=”mypass2” DES=””> </
LoginPassword>
                                        <EnablePassword ClearText=”” DES=””></EnablePassword>
                                        <CHAPPassword ClearText=”” DES=””> </CHAPPassword>
                                        <OutboundPassword ClearText=”” DES=””> </
OutboundPassword>
                                </User>
                                <User>
                                        <Name>user3</Name>
                                        <LoginPassword ClearText=”mypass3” DES=””> </
LoginPassword>
                                        <EnablePassword ClearText=”” DES=””></EnablePassword>
                                        <CHAPPassword ClearText=”” DES=””> </CHAPPassword>
                                        <OutboundPassword ClearText=”” DES=””> </
OutboundPassword>
                                </User>
```

```
                    <User>
                        <Name>user4</Name>
                        <LoginPassword ClearText="mypass4" DES=""> </
LoginPassword>
                        <EnablePassword ClearText="" DES=""></EnablePassword>
                        <CHAPPassword ClearText="" DES=""> </CHAPPassword>
                        <OutboundPassword ClearText="" DES=""> </
OutboundPassword>
                    </User>
                </Users>
            </UserGroup>

            <UserGroup>
                <Name>webdynguest</Name>
                <AuthenticationType>File</AuthenticationType>
                <Users>
                </Users>
            </UserGroup>
        </UserGroups>
</Authentication>
```

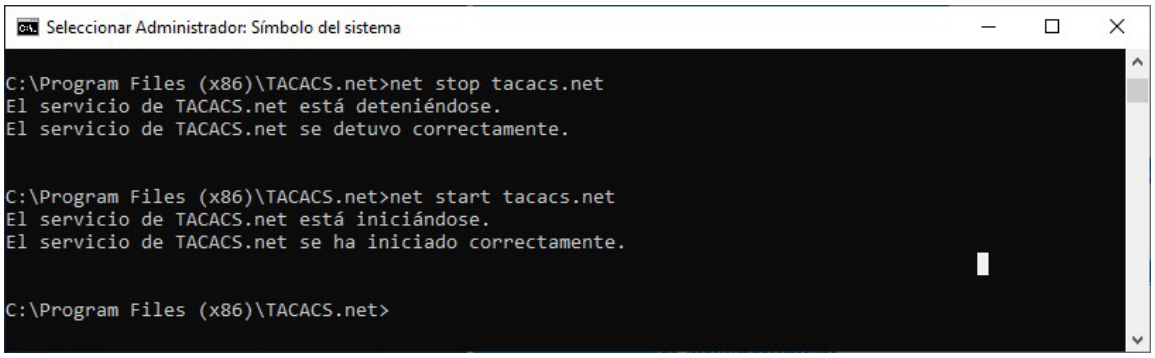
En el fichero "authorization.xml" tendremos definidos los servicios permitidos para cada usuario. Recordemos que los servicios que pueden configurarse en el servidor de Tacacs+ o LDAP son:

"webdyn_http_admin", "webdyn_http_user", "webdyn_http_guest", "webdyn_telnet_admin", "webdyn_ssh_admin". Ningún otro está permitido o es reconocido por los equipos WEBDYN.

```
<?xml version="1.0" encoding="utf-8"?>
<!-- Version 1.2 -->
<Authorizations xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.
w3.org/2001/XMLSchema">
    <Authorizations>

        <Authorization>
            <UserGroups>
                <UserGroup>webdynadmin</UserGroup>
            </UserGroups>
            <Services>
                <Service>
                    <Set>service=webdyn_http_admin</Set>
```

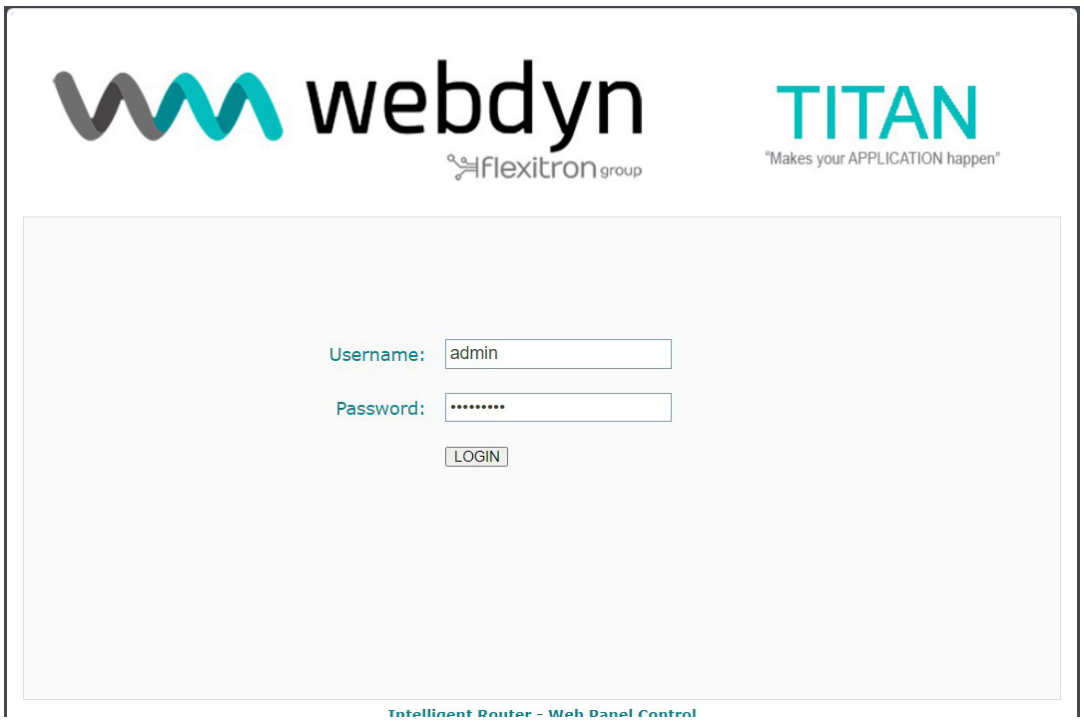
```
                </Service>
                <Service>
                        <Set>service=webdyn_telnet_admin</Set>
                </Service>
                <Service>
                        <Set>service=webdyn_ssh_admin</Set>
                </Service>
        </Services>
</Authorization>

<Authorization>
        <UserGroups>
                <UserGroup>webdynuser</UserGroup>
        </UserGroups>
        <Services>
                <Service>
                        <Set>service=webdyn_http_user</Set>
                </Service>
        </Services>
</Authorization>

<Authorization>
        <UserGroups>
                <UserGroup>webdynguest</UserGroup>
        </UserGroups>
        <Services>
                <Service>
                        <Set>service=webdyn_http_guest</Set>
                </Service>
        </Services>
</Authorization>

    </Authorizations>
</Authorizations>
```

Una vez hecho esto, se puede reiniciar en caso necesario, el servidor de Tacacs+, pues basta con parar el servicio e iniciarlo de nuevo:

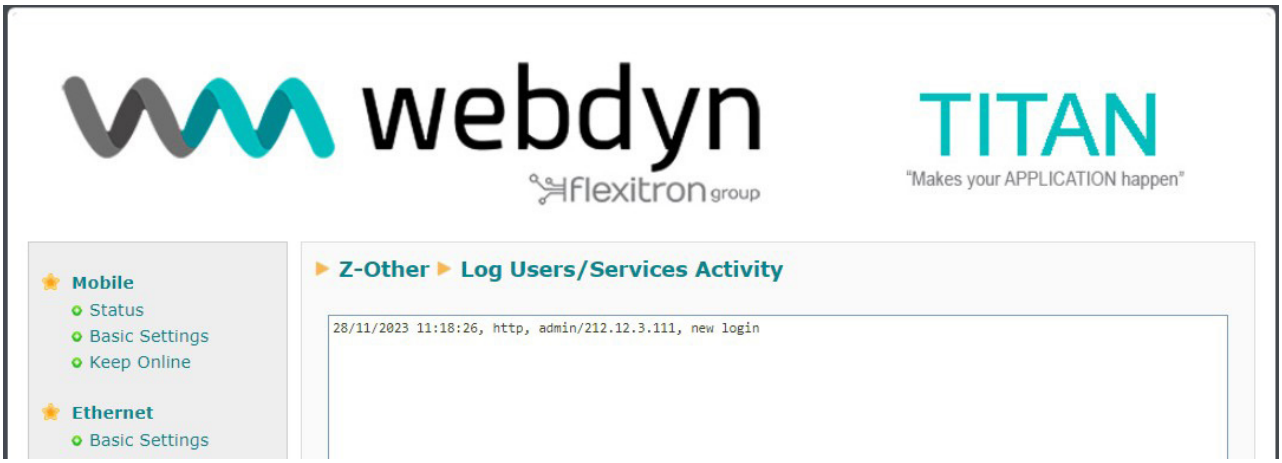


5. Probando el servidor Tacacs+

Con todo configurado ya es posible comprobar el funcionamiento de la autenticación por TACACS+. Para ello basta con ir a la pantalla de inicio de sesión. Primero, comprobaremos que la autenticación local con el usuario/password que se configuró en el punto 2 anterior (admin / add788*12) funciona. Nota: recuerde que si desea acceder remotamente al router vía 4G (es decir, sin utilizar un cable Ethernet), tendrá que habilitar la opción “Remote Webserver management” en la sección “Mobile - Basic Settings”



Si todo es correcto podrá acceder al equipo tras introducir el user y password y podrá ver la acción de logueo en el equipo al final de la página del menú: “Other - Passwords Web UI”



Ahora puede probarse también el control de acceso mediante TACACS+. Para ello debe volverse a la página de inicio de sesión. En este caso introduciremos el usuario user1 / mypass1 , que también tiene role de administrador. Si todo funciona correctamente, podrá observarse el registro de logueo del usuario "user1", en el cual se indica que ha sido autenticado vía "Tacscs+".

¿Más dudas?

Escríbenos tus consultas a **soporte@matrix.es**