webdyn

flexitron group

ROUTER TITAN

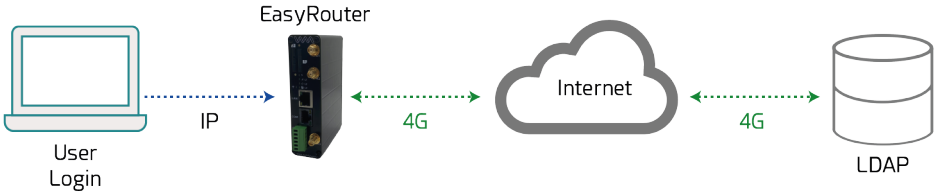
Nota de aplicación 75

Autenticación y autorización mediante LDAP

Autenticación y autorización mediante LDAP

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 LDAP.



1. Descripción del escenario de ejemplo

En este ejemplo se pretende configurar un dispositivo WEBDYN-EASY-ROUTER con autenticación LOCAL y autenticación por LDAP. 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.

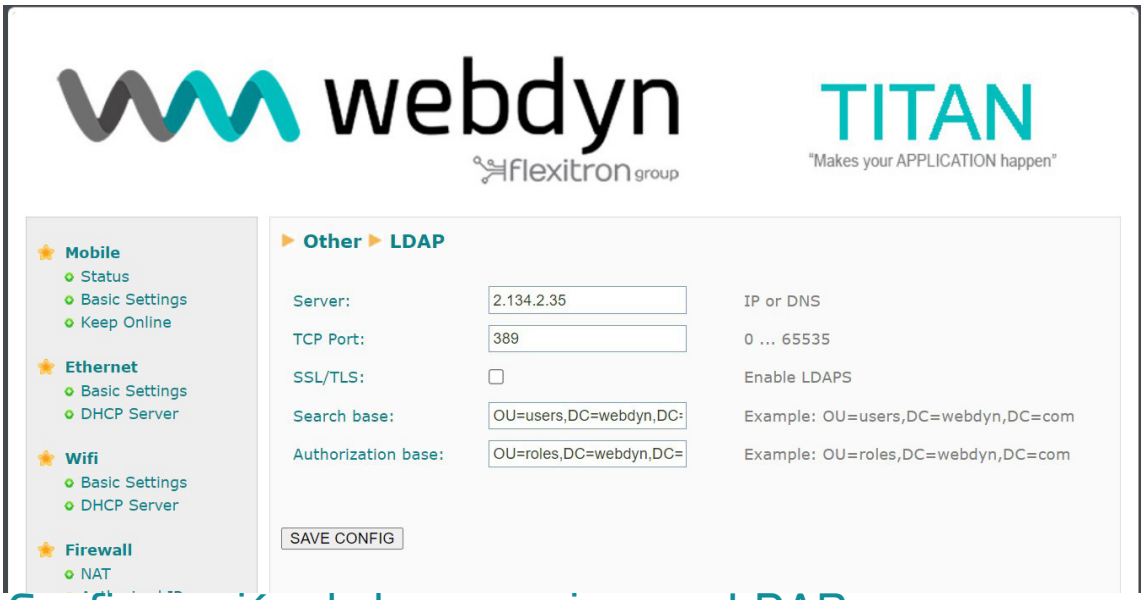
Adicionalmente se requiere configurar el router para permitir la autenticación y autorización mediante un servidor LDAP remoto para el acceso al router vía GUI (HTTP). En este ejemplo con LDAP se pretende crear una cuenta con un usuario de nivel “admin” y tres usuarios de nivel “user”, es decir, con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

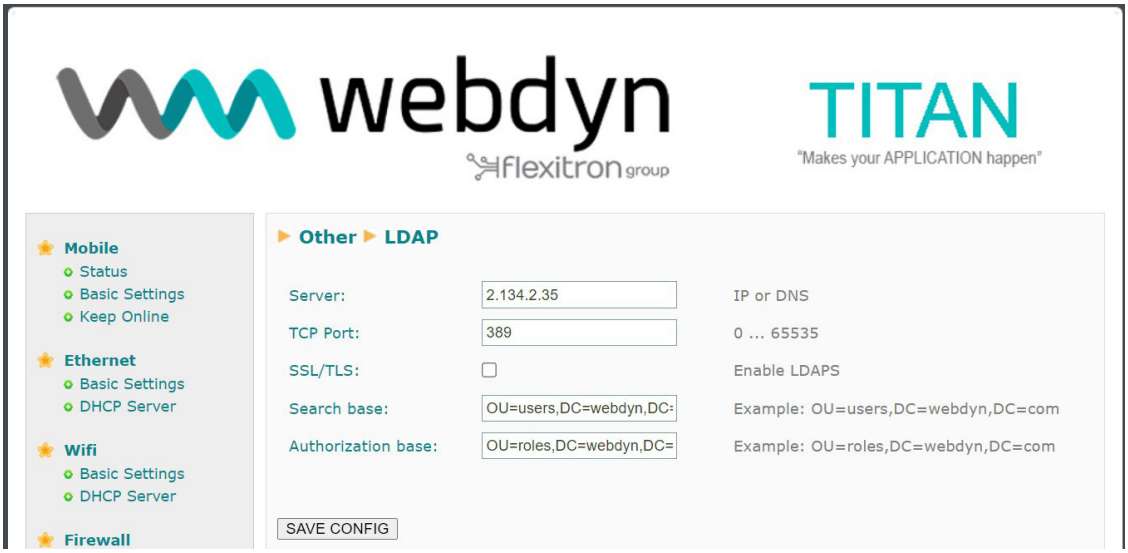
La configuración local de usuarios se realiza desde la sección “Other - Passwords Web UI” Desde ahí pueden configurarse 3 usuarios. Uno con nivel “admin”, otro con nivel “general user” y otro con nivel “guest”.

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”

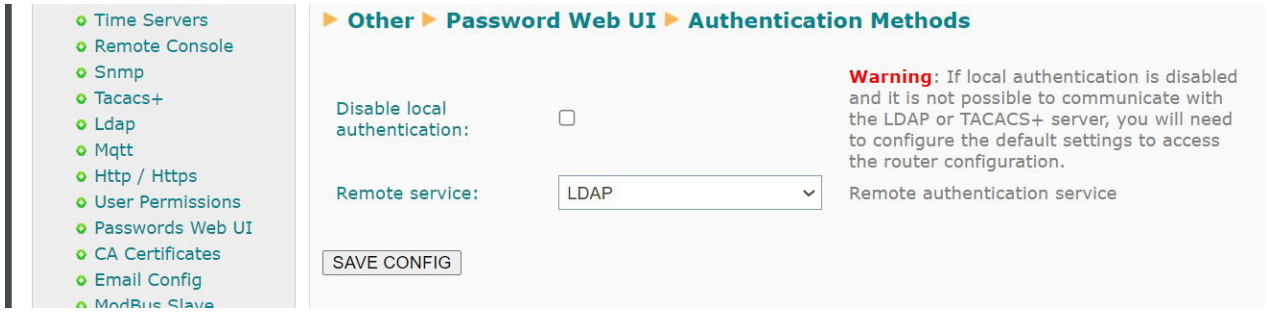


3. Configuración de los usuarios con LDAP

Para la configuración LDAP lo primero que debe configurarse es la sección de conexión con el servidor LDAP. Para ello debe acudirse al menú "Other - Ldap". La configuración es bastante simple, debemos introducir únicamente la DNS o IP del servidor LDAP, el puerto TCP a utilizar, indicar si se va a utilizar SSL/TLS (marcando la casilla en caso afirmativo), el campo "Search Base" (DN base para la búsqueda de usuarios en el servidor LDAP) y el campo "Authorization Base" (DN base para comprobar si un usuario tiene, dentro de un atributo "memberOf", un CN (Common Name) que coincida con el servicio requerido (webdyn_http_admin, webdyn_http_user, webdyn_http_guest, webdyn_telnet_admin ó webdyn_ssh_admin).



Ahora debe especificarse que la autenticación del servicio GUI (HTTP) además realizarse tanto localmente como vía LDAP. 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 "LDAP". 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 el servidor LDAP

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

4.1 Autenticación

El valor indicado anteriormente del campo de configuración “Search Base” era:

OU=users,DC=webdyn,DC=com

Debe asegurarse que es la base correcta del DN para la búsqueda de usuarios en su servidor LDAP.

4.2 Autorización

El router Titan realizará una búsqueda de un valor DN (Distinguised Name) correcto del atributo “memberOf”. En dicha búsqueda se comprobará si existe un DN con el CN (Common Name) webdyn_http_admin, webdyn_http_user, webdyn_http_guest, webdyn_telnet_admin ó webdyn_ssh_admin seguido del resto que conforma el DN (el parámetro Authorization Base). Por ejemplo, los DN completos en el servidor para esta nota de aplicación serían:

CN=webdyn_http_admin,OU=roles,DC=webdyn,DC=com

CN=webdyn_user_admin,OU=roles,DC=webdyn,DC=com

CN=webdyn_guest_admin,OU=roles,DC=webdyn,DC=com

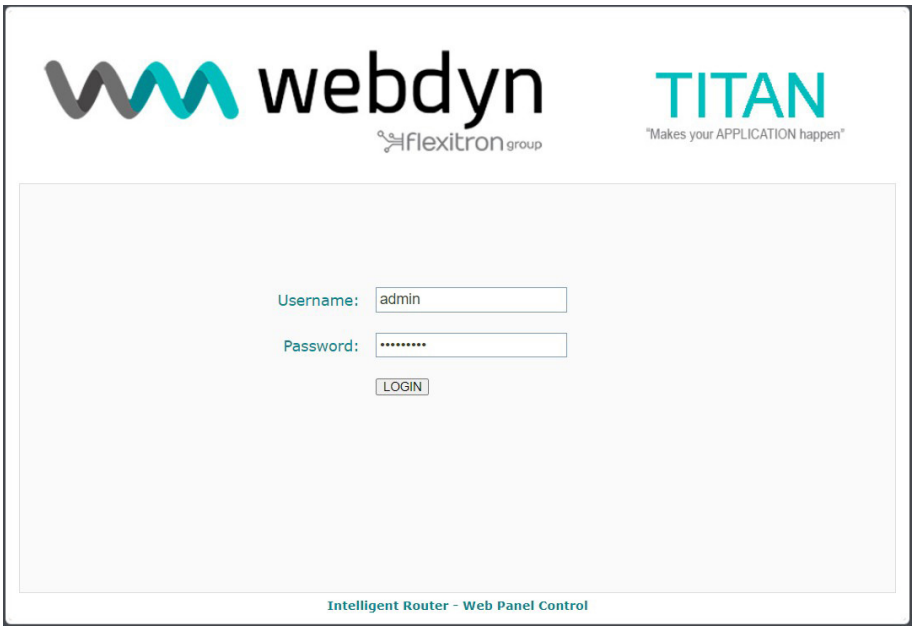
CN=webdyn_telnet_admin,OU=roles,DC=webdyn,DC=com

CN=webdyn_ssh_admin,OU=roles,DC=webdyn,DC=com

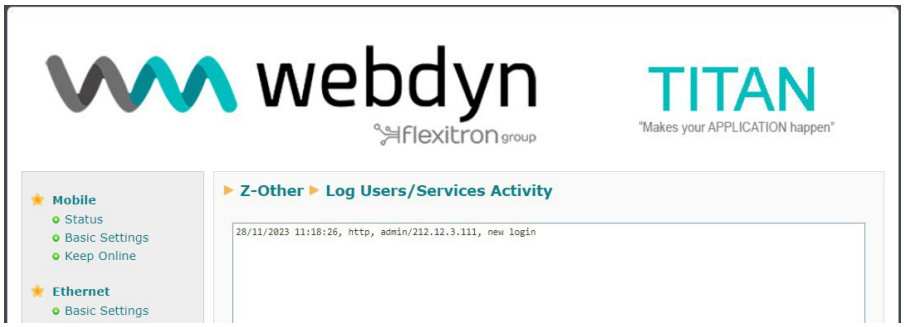
Por ejemplo, un usuario autenticado tendría autorización de “admin” para http si es miembro (atributo memberOf) del DN CN=webdyn_http_admin,OU=roles,DC=webdyn,DC=com

5. Probando el servidor LDAP

Con todo configurado ya es posible comprobar el funcionamiento de la autenticación por LDAP. 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 LDAP. 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 “LDAP”.

¿Más dudas?

Escríbenos tus consultas a **iotsupport@mtxm2m.com**