

Configurar una VPN L2TP/IPsec

Manual visual per crear una connexió VPN amb el client integrat de Windows 11. Inclou dues opcions: autenticació IPsec amb certificat i autenticació amb clau precompartida.

Windows 11

Interfície gràfica

L2TP/IPsec

Temps estimat: 10 minuts



Quina opció has d'utilitzar?

Utilitza exactament el mètode indicat per l'administrador de la VPN.

- **Amb certificat:** el certificat es valida durant la connexió; en entorns com Mikrotik normalment no cal instal·lar-lo manualment abans.
- **Amb clau precompartida:** requereix una clau IPsec o PSK.
- En tots dos casos normalment també cal usuari i contrasenya.

Tot el procés es fa des de la interfície de Windows 11.

No cal obrir CMD, PowerShell ni modificar el registre. Els noms dels menús poden aparèixer en català, castellà o anglès segons l'idioma del sistema.

Dades necessàries

Demana aquestes dades a l'administrador de la VPN abans de crear el perfil.



Servidor VPN

Nom DNS o adreça IP pública del servidor, per exemple *vpn.empresa.cat*.



Credencials d'usuari

Nom d'usuari i contrasenya. El format pot ser usuari, correu electrònic o DOMINI\usuari.



Certificat o clau PSK

Necessites un dels dos mètodes. No són intercanviables.



Connexió a Internet

La VPN s'estableix sobre una connexió d'Internet que ja ha d'estar operativa.

Certificat

VALIDACIÓ AUTOMÀTICA

Windows negocia la capa IPsec amb certificat. En entorns com MikroTik, el certificat es pot gestionar o validar durant la connexió i normalment no cal instal·lar-lo manualment abans.

Clau precompartida

PSK

Windows utilitza una clau comuna proporcionada per l'administrador. La PSK és diferent de la contrasenya de l'usuari.

PAS COMÚ

Crear la connexió VPN

Aquests primers passos són iguals per als dos mètodes.

1

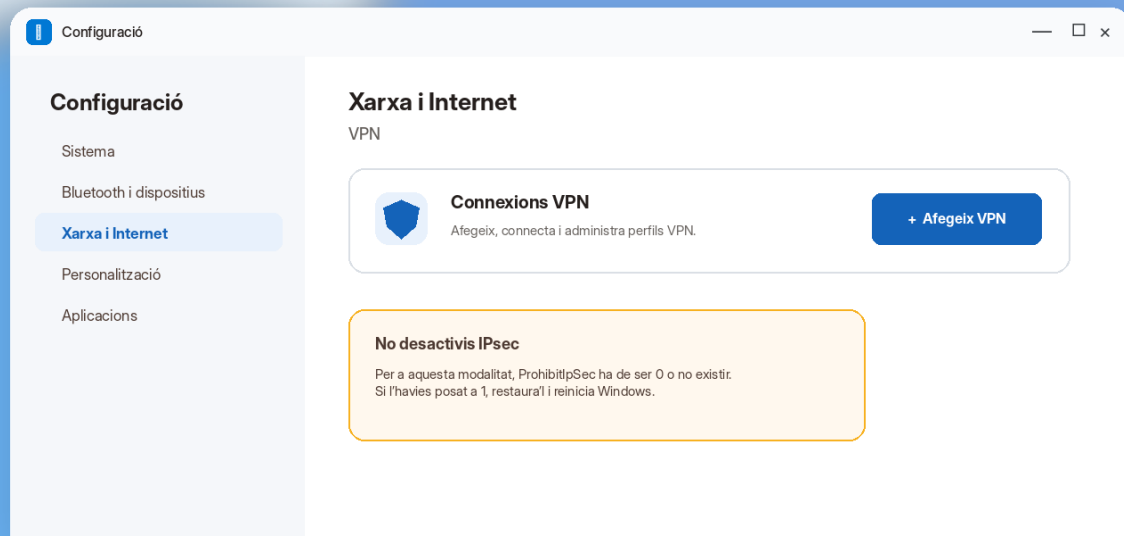
Obre la configuració de VPN

Obre **Inici** → **Configuració** → **Xarxa i Internet** → **VPN**. Prem **Afegeix VPN**.

1

Afegeix una connexió VPN

Configuració de Windows 11 per a L2TP/IPsec



Ruta de Windows 11 per crear un perfil VPN nou.

2

Emplena les dades comunes

Al formulari **Afegeix una connexió VPN**, emplena els camps següents:

Proveïdor de VPN	Windows (integrat).
Nom de connexió	Un nom descriptiu, per exemple "VPN Empresa".
Nom o adreça del servidor	El DNS o la IP facilitats per l'administrador.
Tipus de VPN	Desplega la llista i tria una de les dues opcions L2TP/IPsec explicades a continuació.

Desplega «Tipus de VPN» i selecciona el mètode in

Agregar una conexión VPN

Proveedor de VPN

Windows (integrado) ▾

Nombre de conexión

Nombre de servidor o dirección

Tipo de VPN

Automático

IKEv2

Protocolo de túnel de sockets seguros (SSTP)

L2TP/IPsec con certificado

L2TP/IPsec con clave previamente compartida

Protocolo de túnel punto a punto (PPTP)

Contraseña (opcional)

Guardar

Cancelar

La captura muestra les dues opcions que utilitzarem en aquest manual.

OPCIÓ 1

L2TP/IPsec amb certificat

Selecciona aquesta opció quan l'administrador t'indiqui que la VPN utilitza autenticació IPsec amb certificat. En entorns com MikroTik, aquesta validació es pot resoldre durant la connexió i no cal haver instal·lat prèviament un certificat de manera manual.

1

Selecciona el mètode amb certificat

No cal configurar cap certificat manualment des d'aquesta pantalla. Si l'administrador t'ha indicat que la VPN funciona **amb certificat**, simplement selecciona aquest mètode i completa la resta de camps del perfil.

Important: en entorns MikroTik el certificat es lliura o es valida durant la connexió. Per tant, en aquest manual no cal fer cap importació prèvia ni seleccionar manualment cap fitxer de certificat.

2

Selecciona «L2TP/IPsec amb certificat»

Al camp **Tipus de VPN**, tria **L2TP/IPsec amb certificat**.

Opció 1 · L2TP/IPsec amb certificat

Agregar una conexi3n VPN

Proveedor de VPN

Windows (integrado)

Nombre de conexi3n

Nombre de servidor o direcci3n

Tipo de VPN

Automático

IKEv2

Protocolo de túnel de sockets seguros (SSTP)

L2TP/IPsec con certificado

L2TP/IPsec con clave previamente compartida

Protocolo de túnel punto a punto (PPTP)

Contraseña (opcional)

Guardar

Cancelar

Opci3n correcta quan la capa IPsec s'autentica mitjançant certificat.

3

Configura l'inici de sessi3

Al camp **Tipus d'informaci3 d'inici de sessi3**, selecciona el mètode indicat per l'administrador. En la majoria de configuracions L2TP/IPsec amb certificat continuaràs utilitzant **Nom d'usuari i contrasenya** per autenticar l'accés a la VPN.

El certificat protegeix i autentica la negociaci3 IPsec. Les credencials d'usuari poden continuar sent necessàries per validar la sessi3 VPN.

4

Desa el perfil

Introdueix l'usuari i la contrasenya si vols deixar-los guardats, o deixa'ls en blanc perquè Windows els demani en connectar. Prem **Desa**.

OPCIÓ 2

L2TP/IPsec amb clau precompartida

Selecciona aquesta opció quan l'administrador t'hagi proporcionat una clau IPsec compartida, també anomenada PSK.

1

Selecciona «L2TP/IPsec amb clau precompartida»

Al camp **Tipus de VPN**, tria **L2TP/IPsec amb clau precompartida**.

Opció 2 · L2TP/IPsec amb clau precompartida

Agregar una conexión VPN

Proveedor de VPN

Windows (integrado)

Nombre de conexión

Nombre de servidor o dirección

Tipo de VPN

Automático

IKEv2

Protocolo de túnel de sockets seguros (SSTP)

L2TP/IPsec con certificado

L2TP/IPsec con clave previamente compartida

Protocolo de túnel punto a punto (PPTP)

Contraseña (opcional)

Guardar

Cancelar

En algunes traduccions pot aparèixer com "clau prèviament compartida".

2

Introdueix la clau IPsec

En seleccionar aquesta opció apareixerà un camp nou per escriure la **clau precompartida**. Copia-la exactament, respectant majúscules, minúscules, símbols i espais.

No confonguis les credencials: la clau precompartida protegeix la negociació IPsec i sol ser comuna per als usuaris. La contrasenya personal s'utilitza després per autenticar el teu compte.

3

Selecciona «Nom d'usuari i contrasenya»

Al camp **Tipus d'informació d'inici de sessió**, selecciona habitualment **Nom d'usuari i contrasenya**.
Introdueix les credencials o deixa-les en blanc perquè Windows les demani en connectar.

4

Desa el perfil

Revisa el servidor, el tipus de VPN i la clau precompartida. Prem **Desa**.

POSADA EN SERVEI

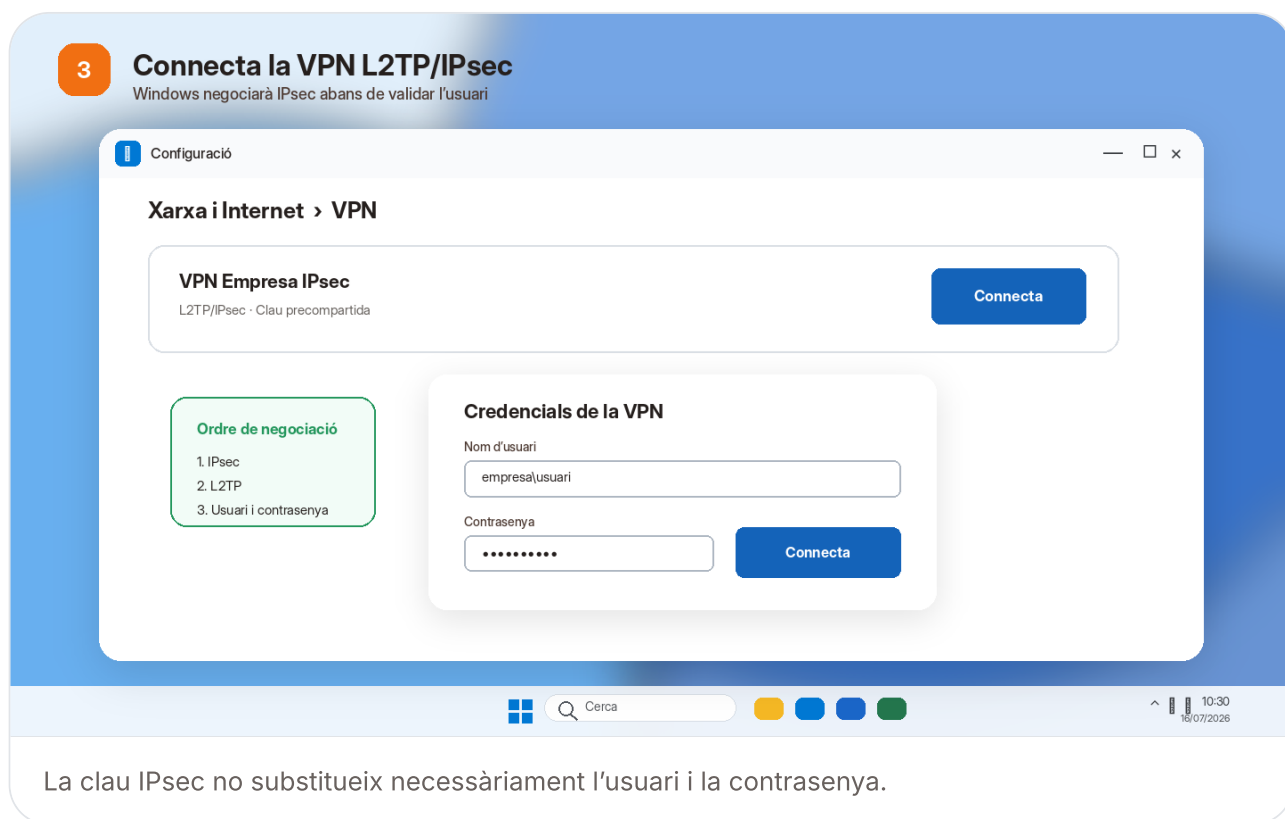
Connectar i comprovar la VPN

El procés de connexió és el mateix amb certificat i amb clau precompartida.

1

Connecta el perfil

Torna a **Configuració** → **Xarxa i Internet** → **VPN**. Obre el perfil creat i prem **Connecta**. Introdueix l'usuari i la contrasenya si Windows els demana.

**2**

Comprova l'estat

Quan la connexió s'hagi establert, Windows mostrarà l'estat **Connectada**. Prova l'accés a un recurs intern, com ara un servidor, una aplicació o una adreça IP de la xarxa corporativa.

5

Comprova que la VPN està connectada

L'estat ha de mostrar «Connectada»



Configuració

Xarxa i Internet > VPN



VPN Empresa IPsec

Connectada

Adreça del servidor: vpn.empresa.cat

Desconnecta

Prova de funcionament

- Obre un recurs intern de l'empresa
- Comprova DNS i rutes
- Verifica que no hi hagi errors d'accés

Connexió ràpida

També pots connectar-te des del panell de xarxa de la barra de tasques.



Cerca



10:30

10/07/2026

Una VPN pot aparèixer connectada però necessitar rutes o DNS correctes per accedir als recursos interns.

INCIDÈNCIES HABITUALS

Solució de problemes

Comprovacions bàsiques sense utilitzar ordres ni modificar el registre.

Error 789 durant la negociació L2TP/IPsec

Revisa que hagi seleccionat el mètode correcte. Amb certificat, confirma amb l'administrador que el MikroTik o el servidor VPN està lliurant o validant correctament el certificat durant la connexió. Amb PSK, torna a escriure la clau precompartida exactament.

Error 691: usuari o contrasenya incorrectes

La capa IPsec ha pogut iniciar-se, però el servidor no accepta les credencials. Revisa el nom d'usuari, el domini, la contrasenya i els permisos del compte.

Error 809: el servidor no respon

Comprova que el nom del servidor sigui correcte i que Internet funcioni. L'administrador haurà de revisar el tallafoc, el NAT i la comunicació L2TP/IPsec, habitualment UDP 500, 4500 i 1701.

Problemes amb l'opció de certificat

En aquest escenari no cal importar manualment cap certificat. Si la connexió amb certificat falla, revisa que hakis escollit **L2TP/IPsec amb certificat** i demana a l'administrador que comprovi la configuració del MikroTik o del servidor VPN.

La VPN connecta però no accedeix als recursos interns

La connexió pot estar establerta però faltar rutes, resolució DNS o permisos. Prova l'adreça IP interna d'un servidor i facilita el resultat a l'administrador.

El botó «Desa» està desactivat

Normalment falta algun camp obligatori: proveïdor, nom de connexió, servidor, tipus de VPN o clau precompartida. Revisa també el camp de tipus d'inici de sessió.

Documentació tècnica consultada

- [Connectar-se a una VPN a Windows — Microsoft Support](#)
- [Tipus de connexió VPN de Windows — Microsoft Learn](#)
- [Opcions d'autenticació VPN — Microsoft Learn](#)
- [Clau precompartida per a L2TP/IPsec — Microsoft Learn](#)

La captura del selector de tipus de VPN ha estat facilitada pel client i s'ha incorporat al manual. Les altres captures són recreacions orientatives pròpies; la interfície pot variar segons l'edició, l'idioma i les actualitzacions de Windows 11.