

Integrated Windows Authentication

Integrated Windows Authentication (IWA) is a Trustelem authentication using the Kerberos token of the user Windows session.

The point is to authenticate on Trustelem to access the apps, not to add MFA on Windows login.

For a user point of view, it's a passwordless authentication:

- when a user logs in to his computer, he receives a Kerberos token from Active Directory.
 - when the user goes to Trustelem, the browser sends the Kerberos token from the computer to Trustelem.
 - Trustelem sends the Kerberos token to Active Directory in order to validate it.
- If everything is ok, the user is logged in, with his identity based on the Kerberos token.

Trustelem admin configuration

The option « **Integrated Windows Authentication** » under **security tab** (<https://admin-mydomain.trustelem.com/app#/security>) must be enabled.

In addition, you need to check the following points:

- the IP range of your internal network must be properly set and the user authentication must come from this network (IWA is only enabled on the internal zone).
- the authentications must be done through <https://mydomain.trustelem.com> (Trustelem admin console does not allow IWA).
- a Trustelem ADConnect connector linked to your Active Directory (on a Windows machine) must be active and running.
- the user whose Windows session is running must have been previously imported from your Active Directory server.

Note: your logs (<https://admin-mydomain.trustelem.com/app#/logs>) will have a login failure entry with the users identity if a user from your domain is identified by IWA but was not registered with Trustelem.

Server configuration

- Connect to one of your servers as a domain administrator.
- Open a command interpreter and enter the following command, after replacing 'trustelem-user' with the name of the user running Trustelem ADConnect connector, and 'mydomain' by the name of your Trustelem subscription domain:

```
setspn -s HTTP/mydomain.trustelem.com trustelem-user
```

Client configuration

Enabling IWA on your clients is a browser-specific operation.

Google Chrome (with GPO)

Internet Explorer / Edge (with GPO)

Firefox (with GPO)

Internet Explorer / Edge (local configuration)

Firefox (local configuration)

Revision #11

Created 1 July 2022 08:16:34 by WALLIX Admin

Updated 8 November 2023 08:02:46 by WALLIX Admin