Question:

How to configure the central user administration with Simatic Logon to use local Windows users or users of an Active Directory (domain) in a PC with WinCC Runtime Advanced or Simatic HMI panel (e.g. Comfort Panel)?

Solution:

In the following, I would like to give you an understanding of how Simatic Logon must be configured so that the logon can be carried out with a Windows or domain user from a panel or WinCC RT Advanced PC.

The Logon Server for a WinCC Runtime Advanced or a HMI panel is installed centrally on a computer in the network. Also, it is possible, the Simatic Logon Server PC is in a different subnet (VLAN). Then you have to configure the gateways for the routing between the networks. (but it can also be installed on the same computer as the WinCC Runtime Advanced is installed)

HMI Panels or a WinCC RT Advanced communicate with Simatic Logon exclusively via the Simatic Logon Remote Access Service (SLRA) when logging on.

When installing the Simatic Logon Server, please note that if it is a domain, the PC must first be included in the domain before installing the Simatic Logon Server. Simatic Logon performs various necessary configuration steps or adjustments to the Windows during installation. If the PC is subsequently integrated into the domain, the requirements change, and the settings previously made are rendered unusable. Simatic Logon must then be uninstalled and reinstalled.

To use the Simatic Logon login in an HMI project, the project is opened in WinCC Comfort/Advanced and the runtime settings are called up. You can now activate the use of Simatic Logon under User Management in Runtime-settings. Then you can choose whether the logon is performed via a Windows domain or Windows computer.

If "Windows Computer" is selected, enter the IP or the name of the computer on which Simatic Logon is installed in the "Server Name" field. Here a DNS server is no problem for the name resolution in case of the HMI panels with Windows CE. (we advise to use IP address instead server name) If Simatic Logon is also installed locally on a WinCC Runtime Advanced PC, "localhost" can also be entered as an alternative. The port is already preset to 16389. This is the port through which the Simatic Logon Remote Access Service communicates with the panels or RT Advanced. If "Windows Domain" has been selected, the name of the domain must be entered in the next field.

The last item to select is whether you want to use encrypted or unencrypted transmission between Simatic Logon and HMI panel. If the checkbox "Encrypted transmission" is not checked, the checkbox for insecure connection must be checked in the configuration console of the Simatic Logon server (tab Certificate).

When using "Encrypted transmission", the check mark for TLS encryption must be set in the logon server. Only one of the two options in Simatic Logon Server must be selected. If both options are checked, the Logon Server always requires an encrypted transmission. But for this to work, a certificate must be created and included. You will find detailed instructions in the following article.

https://support.industry.siemens.com/cs/de/de/view/109480490

In order to log on to the Runtime with the desired Windows / domain users and to use the permissions of the Runtime groups, you create different user groups in the HMI project and assign the desired permissions to these groups. In addition, the same groups must now be created on the PC with the Simatic Logon Server or, if logon via domain is configured, on the domain controller.

The desired Windows / domain users can now be added to these groups. Please make sure that each user can only be assigned to one of these groups. The configuration of the HMI project and the Simatic Logon Server is now complete. Please check the groups in your domain or Windows user administration. Maybe the groups "Users" or "Administrators" are be available. The same groups are be available in the project. The Windows / domain users are standardly also members of this groups in Windows or in domain. So they are be members in more than one used group for runtime.

Finally, only the necessary licenses must be stored on the computer with the Simatic Logon Server. One of these licenses is the Simatic Logon Service license. This is currently version V1.6 and licenses the Simatic Logon Server itself.

In this case the Simatic Logon Remote Access license is required additionally. This is available in versions for 3 or 10 clients. So, if you have 3 clients (Panels or RT Advanced), 3 devices can always log on simultaneously via Simatic Logon. If you have more clients, you can use the license for 10 clients or an additional 3 client license. The licenses add up.

Under the following link you will find a detailed application example for user login in WinCC and for login with RFID card reader.

User login in WinCC:
https://support.industry.siemens.com/cs/de/de/view/109738532

Registration with RFID card reader:
https://support.industry.siemens.com/cs/de/de/view/99808171