Configuring Google Chrome in Kiosk Mode on a XP504

Level 4	1 – Fundamental – No previous experience necessary 2 – Basic – Basic knowledge recommended 3 – Advanced – Reasonable knowledge required 4 – Expert – Good experience recommended

Powering Business Worldwide

Services

For service and support, please contact your local sales organisation.

Contact details: Eaton.com/contacts
Service page: Eaton.com/aftersales

Original Application Note

Original document is the German version of this document.

Translation

All non-German language versions of this document are translations of the original application note.

1. Edition 2025, publication date 07/2025

DANGER!
DANGEROUS ELECTRICAL VOLTAGE!

Before commencing the installation

- Installation requires qualified electrician
- Disconnect the power supply of the device.
- Ensure that devices cannot be accidentally retriggered
- Verify isolation from the supply
- Ground and short-circuit.
- Cover or enclose neighboring units that are live.
- Follow the engineering instructions (IL) of the device concerned.
- Only suitably qualified personnel in accordance with EN 50110-1/-2 (VDE 0105 part 100) may work on this device/ system.
- Before installation and before touching the device ensure that you are free of electrostatic charge.
- The functional earth (FE, PES) must be connected to the protective earth (PE) or to the potential equalizing. The system installer is responsible for implementing this connection.
- Connecting cables and signal lines should be installed so that inductive or capacitive interference do not impair the automation functions.
- Install automation devices and related operating elements in such a way that they are well protected against unintentional operation.
- Suitable safety hardware and software measures should be implemented for the I/O interface so that a line or wire breakage on the signal side does not result in undefined states in the automation devices.
- Ensure a reliable electrical isolation of the low voltage for the 24 V supply. Only use power supply units complying with IEC 60364-4-41 or HD 384.4.41 S2 (VDE 0100 part 410).
- Deviations of the mains voltage from the nominal value must not exceed the tolerance limits given in the technical data, otherwise this may cause malfunction and dangerous operation.
- Emergency-Stop devices complying with IEC/EN 60204-1 must be effective in all operating modes of the automation devices. Unlatching the emergency switching off devices must not cause restart.
- Built-in devices for enclosures or cabinets must only be run and operated in an installed state, desk-top devices or portable devices only when the housing is closed.
- Measures should be taken to ensure the proper restart of programs interrupted after a voltage dip or failure. This should not cause dangerous operating states even for a short time. If necessary, emergency switching off devices should be implemented
- Wherever faults in the automation system may cause damage to persons or property, external measures must be implemented to ensure a safe operating state in the event of a fault or malfunction (for example, by means of separate limit switches, mechanical interlocks, etc.).

Disclaimer

The information, recommendations, descriptions, and safety notations in this document are based on Eaton's experience and judgment and may not cover all contingencies. If further information is required, an Eaton sales office should be consulted. Sale of the product shown in this literature is subject to the terms and conditions outlined in the applicable Terms and Conditions for Sale of Eaton or other contractual agreement between Eaton and the purchaser. THERE ARE NO UNDERSTANDINGS, AGREEMENTS, WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE OR MERCHANTABILITY, OTHER THAN THOSE SPECIFICALLY SET OUT IN ANY EXISTING CONTRACT BETWEEN THE PARTIES. ANY SUCH CONTRACT STATES THE ENTIRE OBLIGATION OF EATON. THE CONTENTS OF THIS DOCUMENT SHALL NOT BECOME PART OF OR MODIFY ANY CONTRACT BETWEEN THE PARTIES. As far as applicable mandatory law allows so, in no event will Eaton be responsible to the purchaser or user in contract, in tort (including negligence), strict liability, or otherwise for any special, indirect, incidental, or consequential damage or loss whatsoever, including but not limited to damage or loss of use of equipment, plant or power system, cost of capital, loss of power, additional expenses in the use of existing power facilities, or claims against the purchaser or user by its customers resulting from the use of the information, recommendations, and descriptions contained herein. The information contained in this manual is subject to change without notice.

Content

1 Introduction

The following user note provides Step-by-Step instructions how to configure the Google-Chrome browser in kiosk-mode on a XP504.

The kiosk-mode is a special mode for applications, when the user should not have access to the OS or other applications. The user can't close the configured application or change any settings of the device. This mode is used for example on devices in stores or other terminals in public places.

2 Approach

2.1 Installation of the Google-Chrome browser

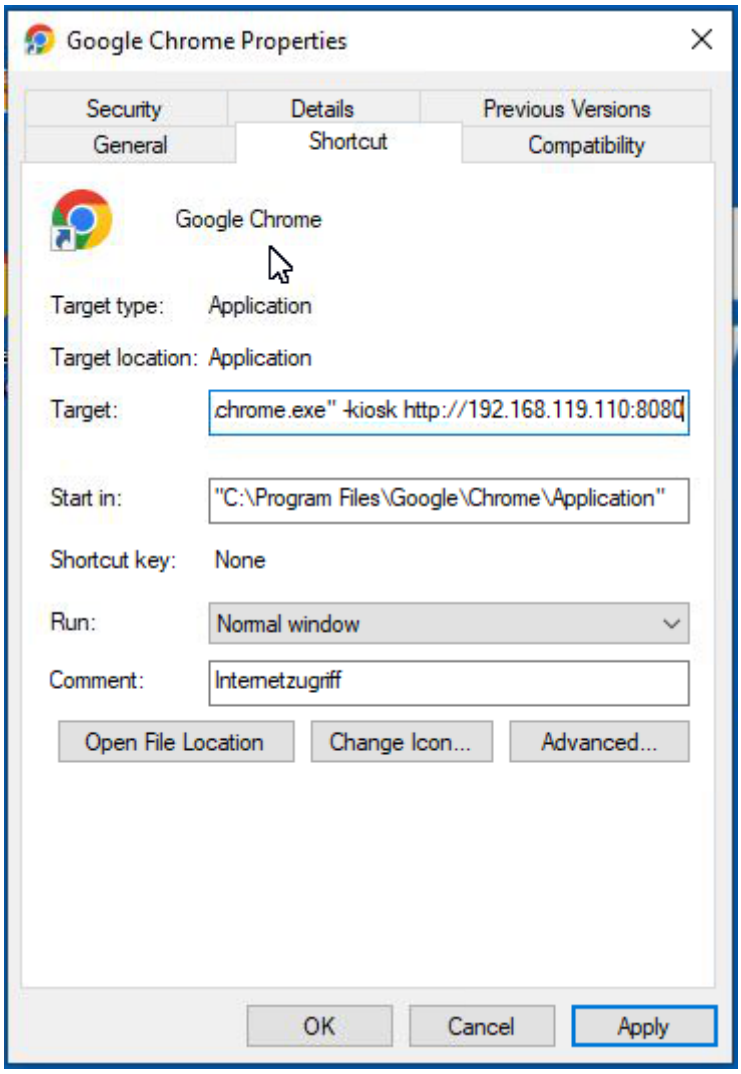
First of all, install the Google-Chrome browser on the XP504 by using a standalone setup-file. You can download it from the google homepage.

2.2 Run Google-Chrome browser in kiosk-mode

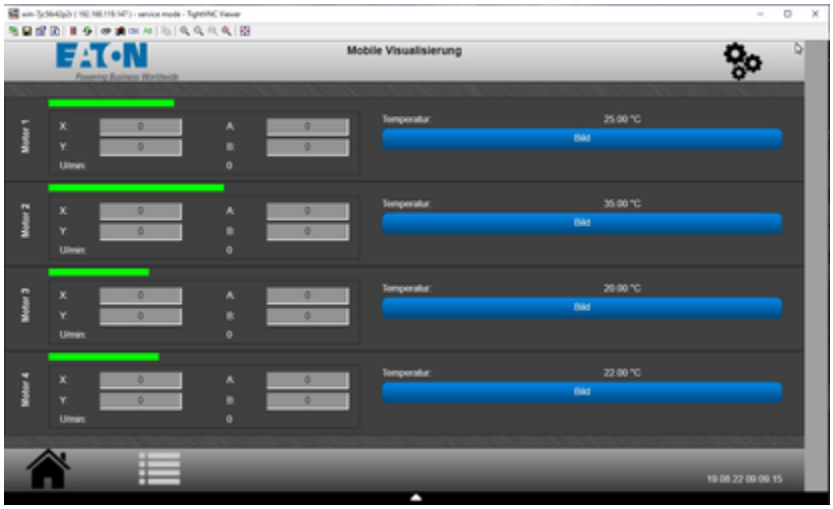
Basically you can run the Google-Chrome browser directly in kiosk-mode by using an additional parameter in the call. You can also predefine a URL to open a default webpage.

For example:

"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -kiosk http://192.168.119.110:8080



Double click on the Google-Chrome icon will open the bowser in kiosk-mode and load the predefined webpage (here a Galileo web-visualization):



In this case the user can close the browser and get access to the Windows desktop using a mouse or a keyboard. To prevent that, Windows provides another method which is described in the next section.

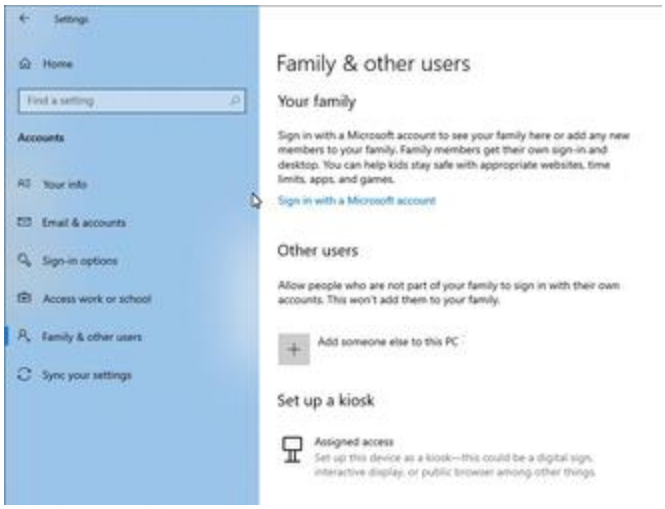
2.3 Configure kiosk-mode for an additional user to prevent access to the Windows-interface

To enable this variant, you will have to:

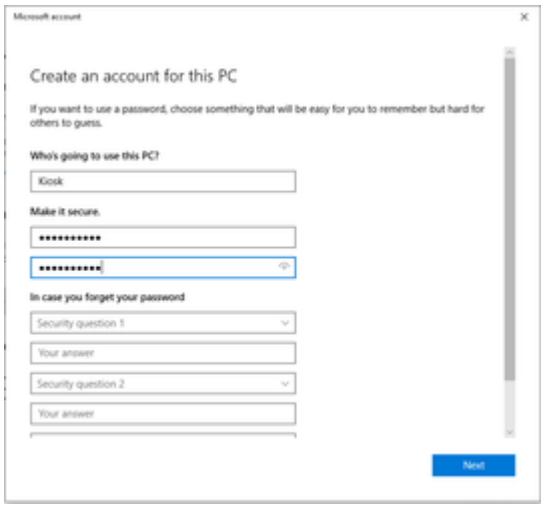
- create a new account on the XP504
- Activate Shell Launcher in Windows features
- customize prepared script
- run script on XP504

2.3.1 Create a new account on the XP504

Go to Settings → Accounts → Family & other users and add a new user to the PC



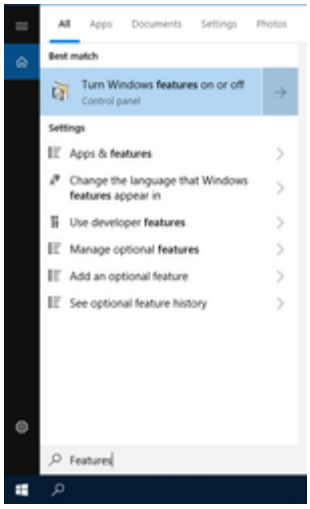
Fill out the form:



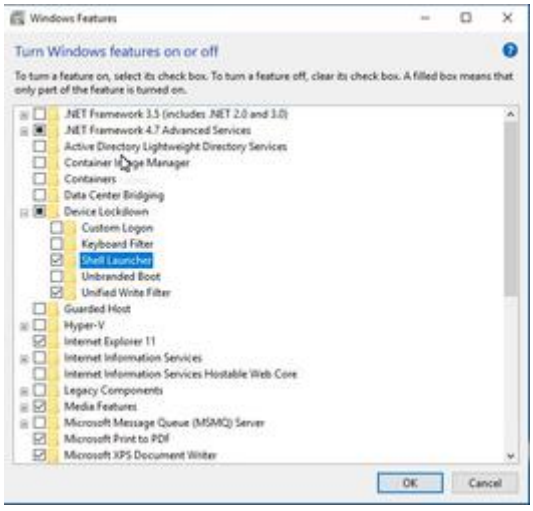
User is now available:

2.3.2 Activate Shell Launcher in Windows features

After adding a new user, please activate the Shell Launcher in Windows features.



Device Lockdown → Shell Launcher



If you confirm with OK, the feature will be activated.

2.4 Customize prepared script

In this example an existing script from Microsoft ist used and adapted to our needs. The whole script can be viewed here:

Use Shell Launcher to create a Windows 10/11 kiosk (Windows 10/11) - Configure Windows | Microsoft Docs

The customized script:

```
# Check if shell launcher license is enabled
function Check-ShellLauncherLicenseEnabled
{
   [string]$source = @"
using System;
using System.Runtime.InteropServices;

static class CheckShellLauncherLicense
{
   const int S_OK = 0;

   public static bool IsShellLauncherLicenseEnabled()
   {
      int enabled = 0;

      if (NativeMethods.SLGetWindowsInformationDWORD("EmbeddedFeature-ShellLauncher-
Enabled", out enabled) != S_OK) {
         enabled = 0;
      }

      return (enabled != 0);
   }

   static class NativeMethods
   {
      [DllImport("Slc.dll")]
      internal static extern int
SLGetWindowsInformationDWORD([MarshalAs(UnmanagedType.LPWStr)]string valueName, out int
value);
   }

}
"@

   $type = Add-Type -TypeDefinition $source -PassThru

   return $type[0]::IsShellLauncherLicenseEnabled()
}

[bool]$result = $false
```

```
$result = Check-ShellLauncherLicenseEnabled
"`nShell Launcher license enabled is set to " + $result
if (-not($result))
{
   "`nThis device doesn't have required license to use Shell Launcher"
   exit
}

$COMPUTER = "localhost"
$NAMESPACE = "root\standardcimv2\embedded"

# Create a handle to the class instance so we can call the static methods.
try {
   $ShellLauncherClass = [wmiclass]"\\$COMPUTER\${NAMESPACE}:WESL_UserSetting"
   } catch [Exception] {
   write-host $_.Exception.Message;
   write-host "Make sure Shell Launcher feature is enabled"
   exit
   }


# This well-known security identifier (SID) corresponds to the BUILTIN\Administrators group.

$Admins_SID = "S-1-5-32-544"

# Create a function to retrieve the SID for a user account on a machine.

function Get-UsernameSID($AccountName) {

   $NTUserObject = New-Object System.Security.Principal.NTAccount($AccountName)
   $NTUserSID = $NTUserObject.Translate([System.Security.Principal.SecurityIdentifier])

   return $NTUserSID.Value

}

# Get the SID for a user account named "Cashier". Rename "Cashier" to an existing account on your
system to test this script.

$Cashier_SID = Get-UsernameSID("KIOSK")

# Define actions to take when the shell program exits.

$restart_shell = 0
$restart_device = 1
$shutdown_device = 2

# Examples. You can change these examples to use the program that you want to use as the shell.

# Set Internet Explorer as the shell for "Cashier", and restart the machine if Internet Explorer is
closed.
```

$ShellLauncherClass.SetCustomShell($Cashier_SID, "c:\program files\google\chrome\application\chrome.exe -kiosk 192.168.119.110:8080", ($null), ($null), $restart_shell)

Enable Shell Launcher

$ShellLauncherClass.SetEnabled($TRUE)

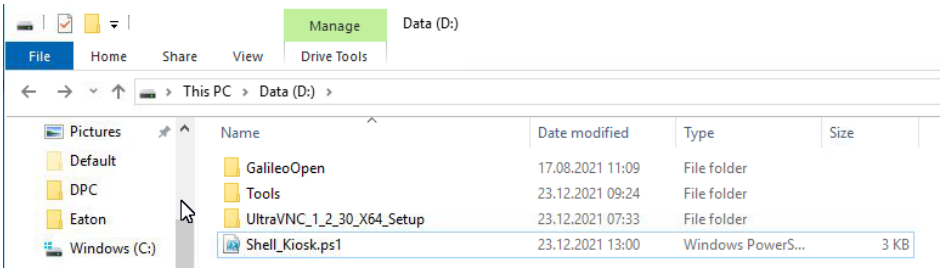
$IsShellLauncherEnabled = $ShellLauncherClass.IsEnabled()

"`nEnabled is set to " + $IsShellLauncherEnabled.Enabled

You can copy this script into an editor and save it as *.ps1 file or you can use this prepared file:

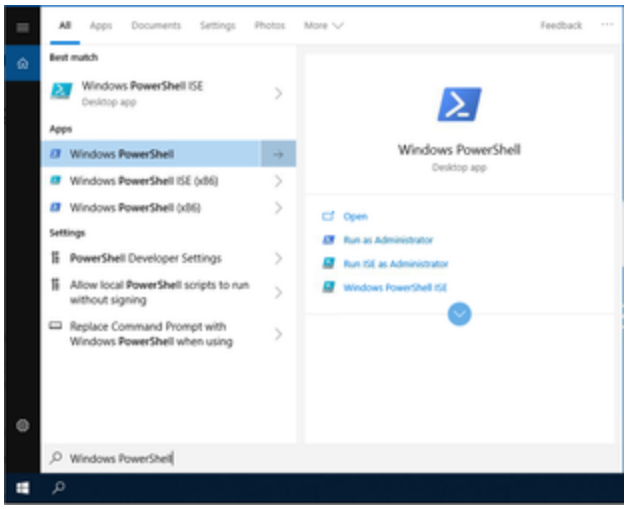
Please adapt the URL in line 89 as needed:

Copy the file/script to the device e.g. on drive D:\:



2.5 Run script on XP504

Now we are going to execute the script on the XP504. For this you have to log in as administrator (use account: XP504). Start the Windows Powershell as administrator:



Change to drive D:\ and execute the script:

```
PS D:\> cd d:\
PS D:\> _\Shell_Kiosk.ps1
```

In case the execution of scripts is disabled on the device, please use this command to enable it:

```
.\Shell_Kiosk.ps1 : File D:\Shell_Kiosk.ps1 cannot be loaded because running scripts is disabled on this system. For more information, see about_Execution_Policies at
https:/go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\Shell_Kiosk.ps1
+ ~~~~~~~~~~~~~~~~
    + CategoryInfo          : SecurityError: (:) [], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess
```

```
PS D:\> Set-ExecutionPolicy RemoteSigned

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose you to the security risks described in the about_Execution_Policies help
topic at https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): A
PS D:\>
```

Call the script again:

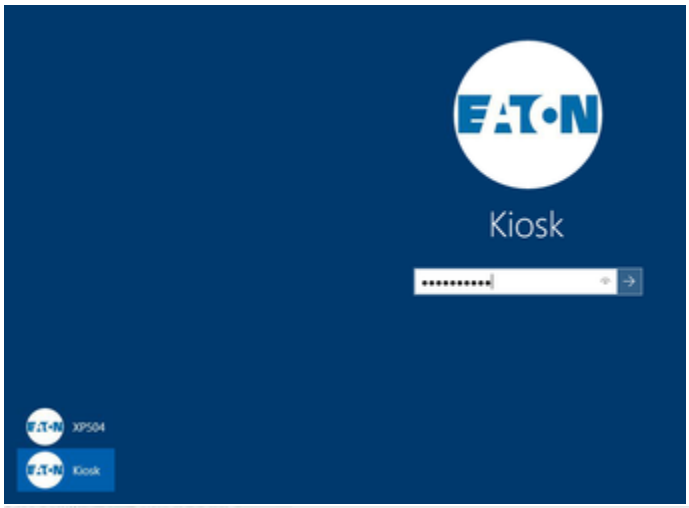
```
PS D:\> .\Shell_Kiosk.ps1
WARNING: The generated type is not public.

Shell Launcher license enabled is set to True

Enabled is set to True
PS D:\>
```

The shell is now configured and you can reboot the device.

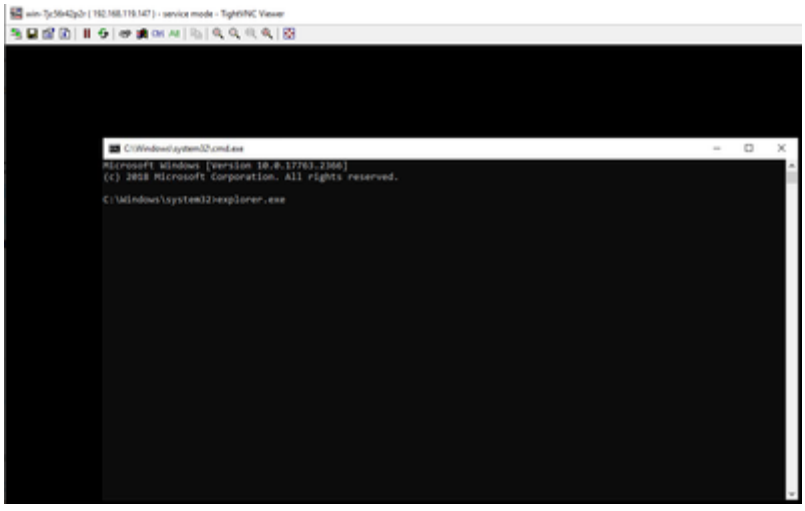
Login as user "Kiosk" and the browser will start directly with the defined URL.



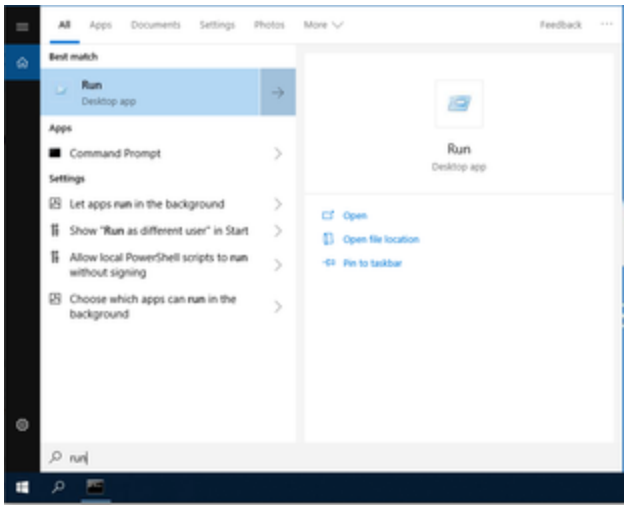
Now the user don't have access to Windows OS and clothing the browser will reopen it again.

2.6 Automatic Login

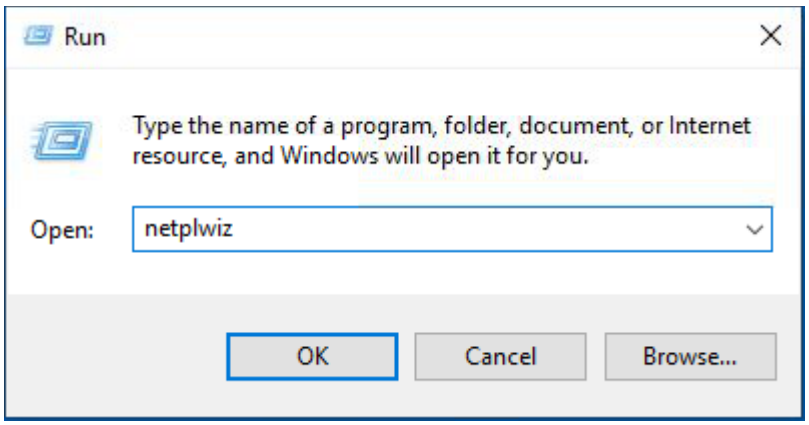
To avoid entering a password when logging in you can configure the "Automatically sign in" for the user "Kiosk". For this please sign out and login with user "XP504". After loggin in, the command line is displayed. Type in explorer.exe to continue:



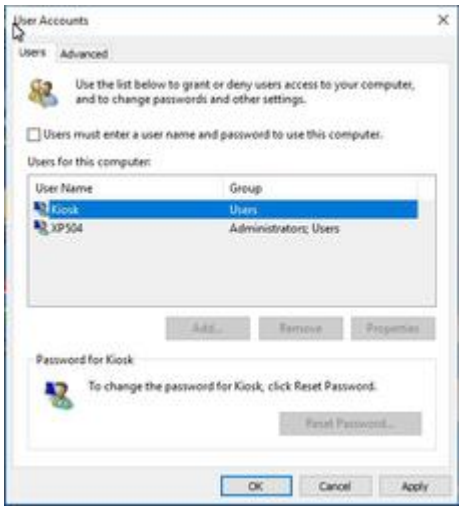
Minimize the command line and start the application "Run":



Open "netplwiz":



Select user "Kiosk" and deactivate the option "Users must enter a user name and password to use this computer":



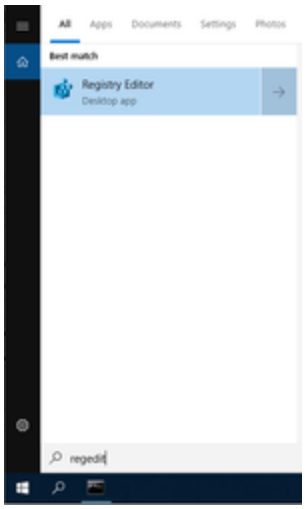
Put in the user credentials and confirm with OK:

When rebooting the XP504, the user "Kiosk" is now automatically logged in.

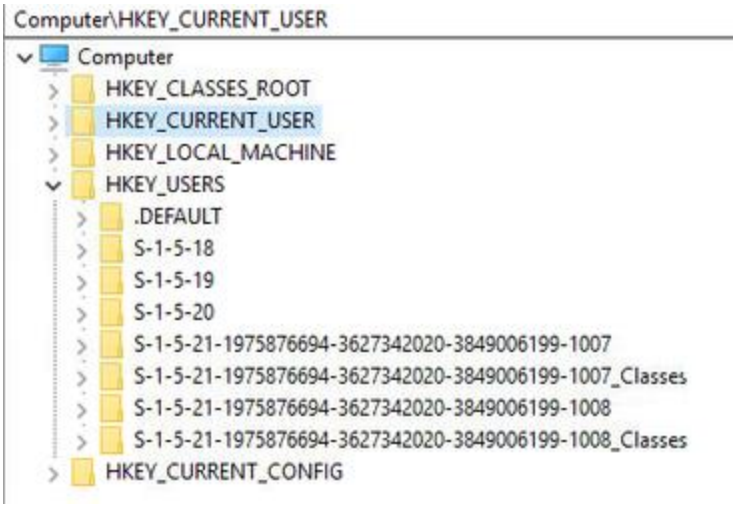
2.7 Disable Screen Lock

Due to inactivity, the user is automatically logged out after some time. To disable this screen lock, please do the following:

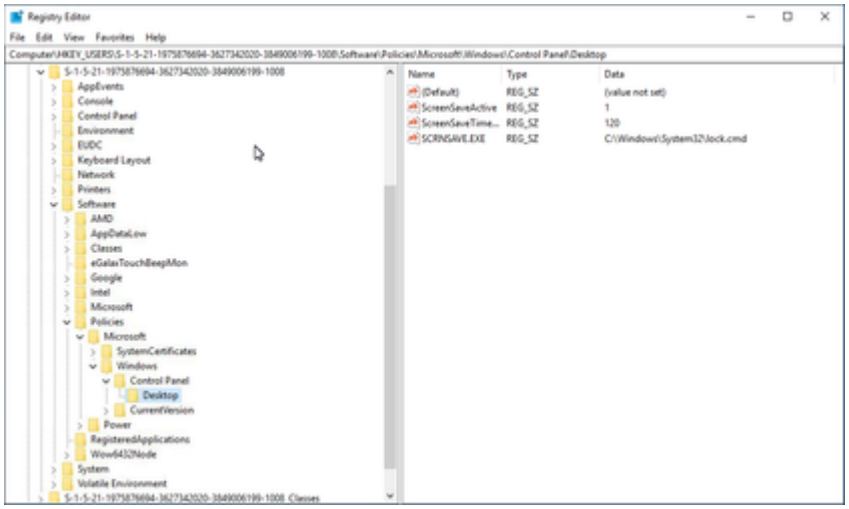
Open "regedit":



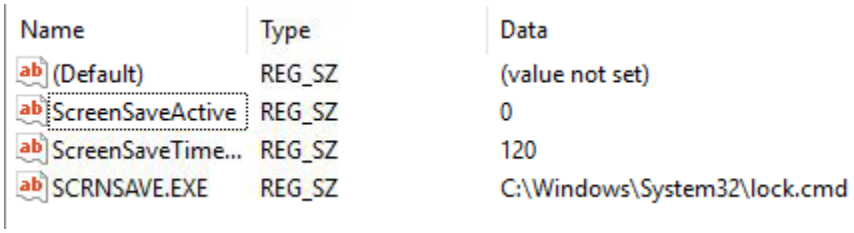
Open HKEY_USERS. There should be two users defined with a long SID. First one (here xx-1007) is user "XP504" and the second one is user "Kiosk":



Navigate to HKEY_USERS\S-1-5-21-xx-1008\Software\Policies\Microsoft\Windows\Control Panel\Desktop



Set value for "ScreenSaveActive" to "0":



This setting will only deactivate the Lock Screen for user "Kiosk".

Eaton is an intelligent power management company dedicated to improving the quality of life and protecting the environment for people everywhere. We are guided by our commitment to do business right, to operate sustainably and to help our customers manage power – today and well into the future.
By capitalizing on the global growth trends of electrification and digitalization, we're accelerating the planet's transition to renewable energy, helping to solve the world's most urgent power management challenges, and doing what's best for our stakeholders and all of society.

Founded in 1911, Eaton has been listed on the NYSE for nearly a century.
We reported revenues of $19.6 billion in 2021 and serve customers in more than 170 countries.

For more information, visit Eaton.com. Follow us on Twitter and LinkedIn.

Eaton Industries GmbH
Hein-Moeller-Str. 7- 11
D-53115 Bonn

07/2025 AP050021EN

Powering Business Worldwide