Application Note 07/2025 AP050021DE

Konfiguration des Google-Chrome Browsers im Kiosk-Modus auf dem XP504

Level 4	1 – Fundamental – keine weiteren Kenntnisse nötig 2 – Basic – Grundwissen empfehlenswert 3 – Fortgeschritten – Grundwissen notwendig 4 – Expert – Praxiserfahrung in dem Thema empfehlenswert

Powering Business Worldwide

Services

Für Service und Support kontaktieren Sie bitte Ihre lokale Vertriebsorganisation.

Kontaktdaten: Eaton.com/contacts
Service Seite: Eaton.com/aftersales

Original Application Note

Die deutsche Ausführung dieser Application Note ist das Original.

Übersetzung des Originaldokuments

Alle nicht deutschen Sprachausgaben dieses Application Note sind Übersetzungen der Original Application Note.

1. Auflage 2025, Redaktionsdatum 07/2025

GEFAHR!
GEFÄHRLICHE ELEKTRISCHE SPANNUNG!

Vor Beginn der Installationsarbeiten

- Installation erfordert Elektro-Fachkraft.
- Gerät spannungsfrei schalten
- Gegen Wiedereinschalten sichern
- Spannungsfreiheit feststellen
- Erden und kurzschließen
- Benachbarte, unter Spannung stehende Teile abdecken oder abschranken.
- Die für das Gerät angegebenen Montagehinweise (IL) sind zu beachten.
- Nur gemäß EN 50110-1/-2 (VDE 0105 Teil 100) qualifiziertes Personal darf Eingriffe an diesem Gerät/System vornehmen.
- Achten Sie bei Installationsarbeiten darauf, dass Sie sich statisch entladen, bevor Sie das Gerät berühren.
- Die Funktionserde (FE, PES) muss an die Schutzerde (PE) oder den Potentialausgleich angeschlossen werden. Die Ausführung dieser Verbindung liegt in der Verantwortung des Errichters.
- Anschluss- und Signalleitungen sind so zu installieren, dass induktive und kapazitive Einstreuungen keine Beeinträchtigung der Automatisierungsfunktionen verursachen.
- Einrichtungen der Automatisierungstechnik und deren Bedienelemente sind so einzubauen, dass sie gegen unbeabsichtigte Betätigung geschützt sind.
- Damit ein Leitungs- oder Aderbruch auf der Signalseite nicht zu undefinierten Zuständen in der Automatisierungseinrichtung führen kann, sind bei der E/A-Kopplung hard- und softwareseitig entsprechende Sicherheitsvorkehrungen zu treffen.
- Bei 24-Volt-Versorgung ist auf eine sichere elektrische Trennung der Kleinspannung zu achten. Es dürfen nur Netzgeräte verwendet werden, die die Forderungen der IEC 60364-4-41 bzw. HD 384.4.41 S2 (VDE 0100 Teil 410) erfüllen.
- Schwankungen bzw. Abweichungen der Netzspannung vom Nennwert dürfen die in den technischen Daten angegebenen Toleranzgrenzen nicht überschreiten. Andernfalls sind Funktionsausfälle und Gefahrenzustände nicht auszuschließen.
- NOT-AUS-Einrichtungen nach IEC/EN 60204-1 müssen in allen Betriebsarten der Automatisierungseinrichtung wirksam bleiben. Entriegeln der NOT-AUS-Einrichtungen darf keinen Wiederanlauf bewirken.
- Einbaugeräte für Gehäuse oder Schränke dürfen nur im eingebauten Zustand, Tischgeräte oder Portables nur bei geschlossenem Gehäuse betrieben und bedient werden.
- Es sind Vorkehrungen zu treffen, dass nach Spannungseinbrüchen und -ausfällen ein unterbrochenes Programm ordnungsgemäß wiederaufgenommen werden kann. Dabei dürfen auch kurzzeitig keine gefährlichen Betriebszustände auftreten. Ggf. ist NOT-AUS zu erzwingen.
- An Orten, an denen in der Automatisierungseinrichtung auftretende Fehler Personen- oder Sachschäden verursachen können, müssen externe Vorkehrungen getroffen werden, die auch im Fehler- oder Störfall einen sicheren Betriebszustand gewährleisten beziehungsweise erzwingen (z. B. durch unabhängige Grenzwertschalter, mechanische Verriegelungen usw.).

Gewährleistungsausschluss und Haftungsbeschränkung

Die Informationen, Empfehlungen, Beschreibungen und Sicherheitshinweise in diesem Dokument basieren auf den Erfahrungen und Einschätzungen der Eaton Corp. Und berücksichtigen möglicherweise nicht alle Eventualitäten.

Wenn Sie weitere Informationen benötigen, wenden Sie sich bitte an ein Verkaufsbüro von Eaton. Der Verkauf der in diesen Unterlagen dargestellten Produkte erfolgt zu den Bedingungen und Konditionen, die in den entsprechenden Verkaufsrichtlinien von Eaton oder sonstigen vertraglichen Vereinbarungen zwischen Eaton und dem Käufer enthalten sind. Es existieren keine Abreden, Vereinbarungen, Gewährleistungen ausdrücklicher oder stillschweigender Art, einschließlich einer Gewährleistung der Eignung für einen bestimmten Zweck oder der Marktgängigkeit, außer soweit in einem bestehenden Vertrag zwischen den Parteien ausdrücklich vereinbart. Jeder solche Vertrag stellt die Verpflichtung von Eaton abschließend dar.

Der Inhalt dieses Dokumentes wird weder Bestandteil eines Vertrages zwischen den Parteien noch führt er zu dessen Änderung. Eaton übernimmt gegenüber dem Käufer oder Nutzer in keinem Fall eine vertragliche, deliktische (einschließlich Fahrlässigkeit), verschuldensunabhängige oder sonstige Haftung für außergewöhnliche, indirekte oder mittelbare Schäden, Folgeschäden bzw. –verluste irgendeiner Art – unter anderem einschließlich, aber nicht beschränkt auf Schäden an bzw. Nutzungsausfälle von Geräten, Anlagen oder Stromanlagen, von Vermögensschäden, Stromausfällen, Zusatzkosten in Verbindung mit der Nutzung bestehender Stromanlagen, oder Schadensersatzforderungen gegenüber dem Käufer oder Nutzer durch deren Kunden – infolge der Verwendung der hierin enthaltenen Informationen, Empfehlungen und Beschreibungen. Wir behalten uns Änderungen der in diesem Handbuch enthaltenen Informationen vor. Fotos und Abbildungen dienen lediglich als Hinweis und begründen keine Verpflichtung oder Haftung seitens Eaton.

Inhalt

1 Allgemeines

Der folgende Anwenderhinweis ist eine Schritt für Schritt Beschreibung um den Google-Chrome Browser im Kiosk-Modus auf einem Gerät zu betreiben.

Der Kiosk-Modus ist ein spezieller Modus für Applikationen, wenn der Benutzer keinen Zugriff zum Betriebssystem oder anderen Applikationen haben soll. Der Benutzer kann die konfigurierte Applikation dann nicht schließen oder Änderungen an den Geräte-Einstellungen vornehmen. Dieser Modus wird z.B. auf Geräten in Kaufhäusern oder Terminals an öffentlichen Plätzen verwendet.

2 Vorgehen

2.1 Installation des Google-Chrome Browsers

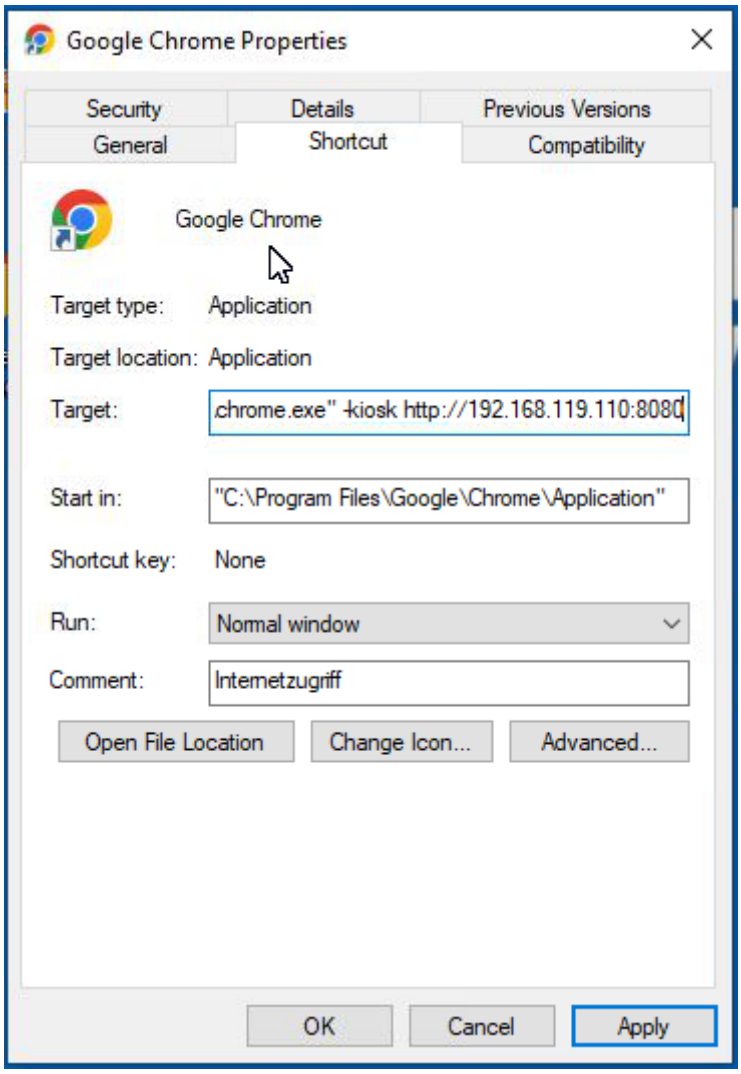
Zunächst wird der Google-Chrome Browser als Standalone Applikation auf dem XP504 installiert. Sie können ihn von der Google Homepage herunterladen

2.2 Starten des Google-Chrome Browsers im Kiosk-Modus

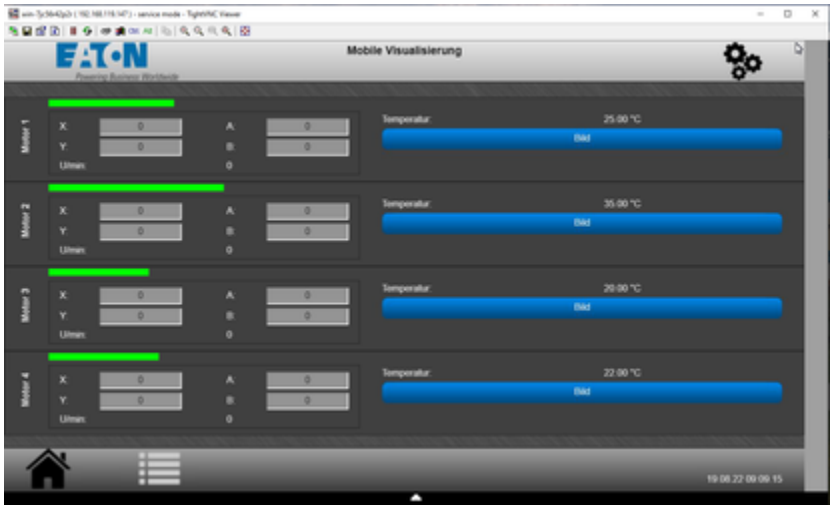
Grundsätzlich kann der Google-Chrome Browser direkt im Kiosk-Modus gestartet werden, wenn man zusätzliche Parameter im Aufruf hinzufügt. Hier kann auf eine vordefinierte URL eingetragen werden, um eine Default-Webseite aufzurufen.

Zum Beispiel:

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



Ein Doppelklick auf das Google-Chrome Icon öffnet so den Browser im Kiosk-Modus und lädt die vordefinierte Webseite (hier eine Galileo-Webvisualisierung):



In diesem Fall kann der Benutzer jedoch den Browser mit Hilfe einer Maus oder Tastatur schließen und gelangt auf die Windows-Oberfläche. Um das zu verhindern, bietet Windows eine andere Möglichkeit, die im nächsten Abschnitt beschrieben ist.

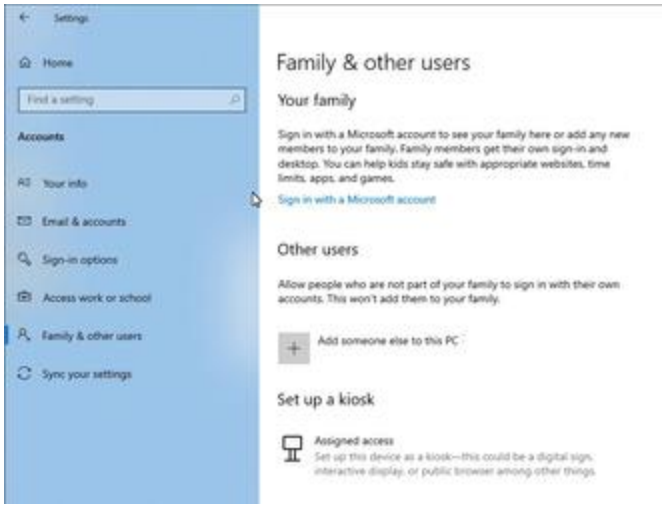
2.3 Konfiguration des Kiosk-Modus für einen zusätzlichen Benutzer, um den Zugriff auf die Windows-Oberfläche zu verhindern

Um diese Variante zu ermöglichen, sind folgende Schritte erforderlich:

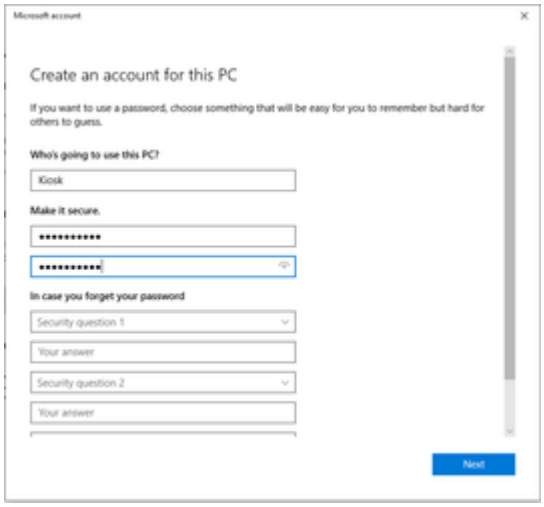
- Erstellen eines neuen Accounts auf dem XP504
- Aktivieren des Shell Launchers in den Windows Features
- Anpassen des vorbereiteten Skripts
- Ausführen des Skripts auf dem XP504

2.3.1 Einen neuen Account auf dem XP504 erstellen

Gehe zu Settings → Accounts → Family & other users und füge einen neues Benutzer zu dem PC hinzu



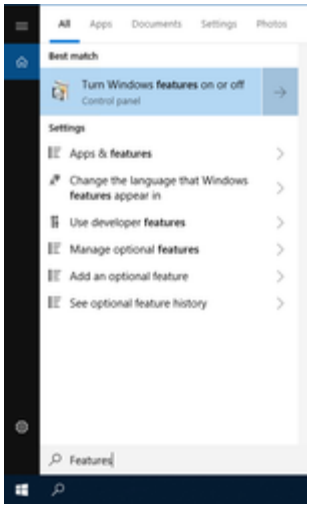
Fülle die erforderlichen Zeilen aus:



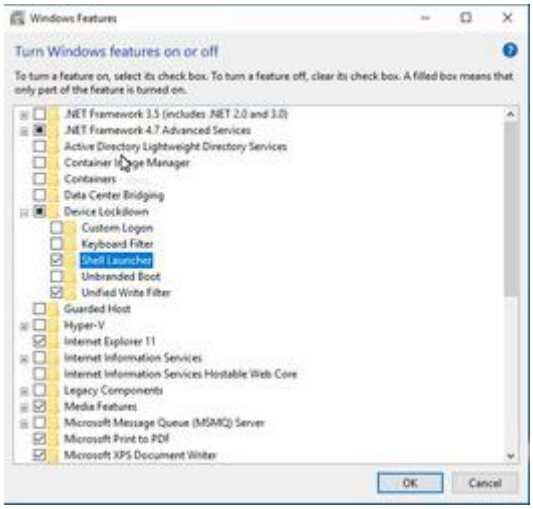
Der Benutzer ist nun verfügbar:

2.3.2 Aktivieren des Shell Launchers in den Windows Features

Nachdem der neue Benutzer hinzugefügt ist, wird der Shell Launcher in den Windows Features aktiviert:



Device Lockdown → Shell Launcher



Die Aktivierung des Features mit OK bestätigen.

2.4 Anpassen des vorbereiteten Skripts

In diesem Beispiel wird ein vorhandenes Skript von Microsoft verwendet und für unsere Anforderungen angepasst. Das vollständige Skript kann unter nachfolgendem Link eingesehen werden:

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

Das nachfolgende Skript ist für den Benutzer "Kiosk" angepasst:

```
# 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)

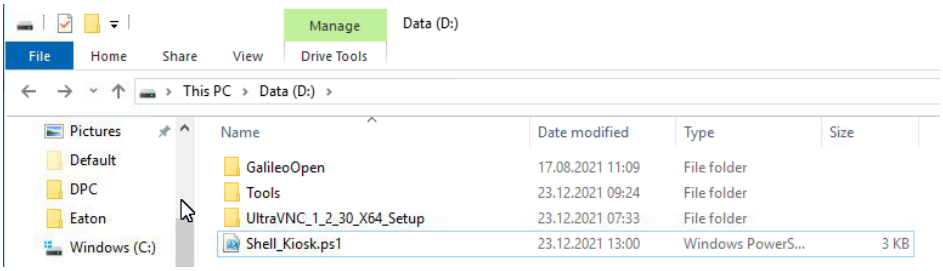
$IsShellLauncherEnabled = $ShellLauncherClass.IsEnabled()

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

Das oben aufgeführte Skript kann in einen Editor kopiert und als *.ps1 Datei abgespeichert werden. Alternativ kann auch das folgende Skript verwendet werden:

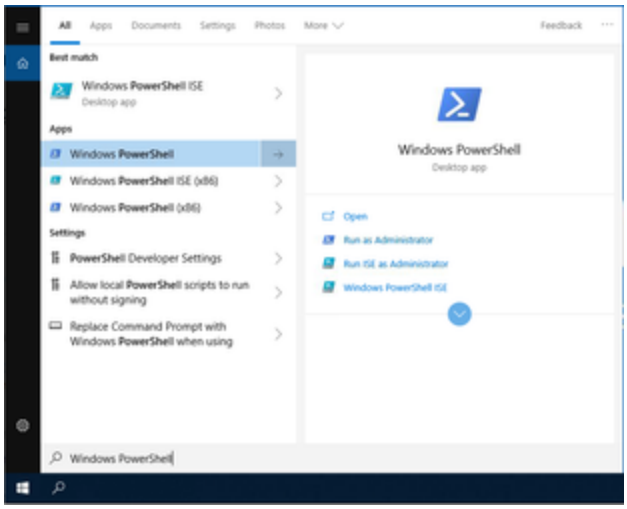
Anpassungen an der URL in Zeile 89 sind entsprechend den Anforderungen vorzunehmen:

Kopiere die Datei/das Skript auf das XP504, z.B. auf Laufwerk D:\



2.5 Ausführen des Skripts auf dem XP504

Nun wird dieses Skript auf dem XP504 ausgeführt. Dafür muss man als Administrator (verwende den Account XP504 hierfür) eingeloggt sein. Starte anschließend die Windows Powershell als Administrator:



Wechsel zum Laufwerk D:\ und starte das Skript:

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

Im Falle, dass die Ausführung von Skripten auf dem Gerät deaktiviert ist, führe bitte folgenden Befehl (Set-ExecutionPolicy RemoteSigned) aus, um diese zu aktivieren:

```
.\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:\>
```

Starte das Skript erneut:

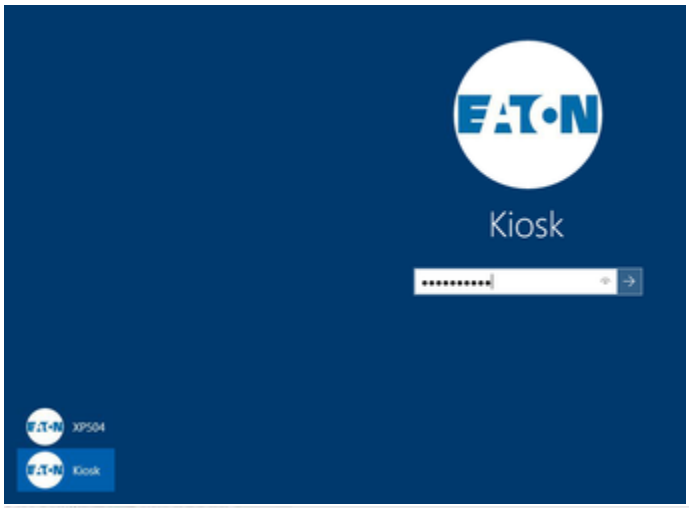
```
PS D:\> .\Shell_Kiosk.ps1
WARNING: The generated type is not public.

Shell Launcher license enabled is set to True

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

Die Konfiguration ist nun abgeschlossen und das Gerät muss neu gestartet werden:

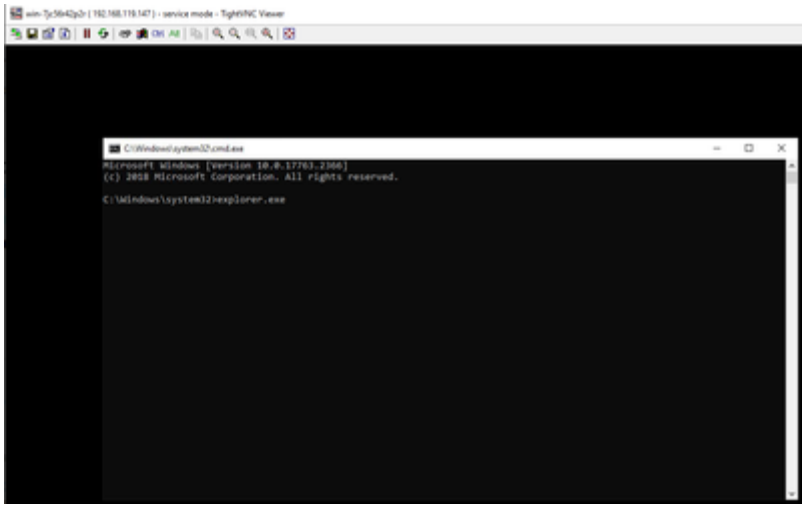
Das Einloggen mit dem zuvor neu angelegten Benutzer "Kiosk" startet direkt den Browser mit der definierten URL.



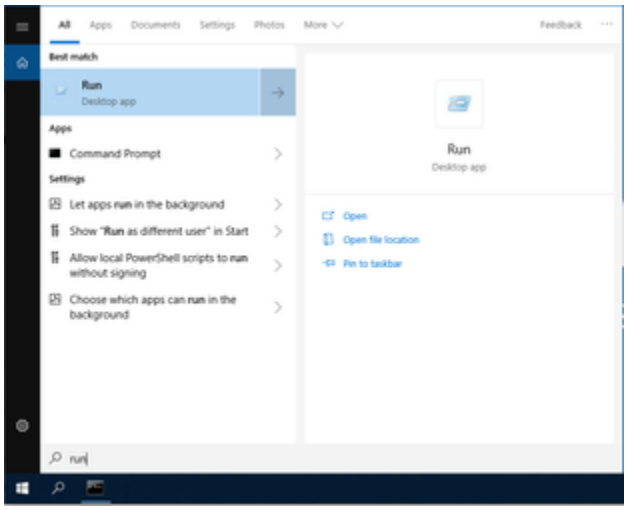
Nun hat der Benutzer keine Möglichkeit auf die Windows Oberfläche zu gelangen. Wird der Browser geschlossen, so wird dieser direkt automatisch neu geöffnet.

2.6 Automatischer Login

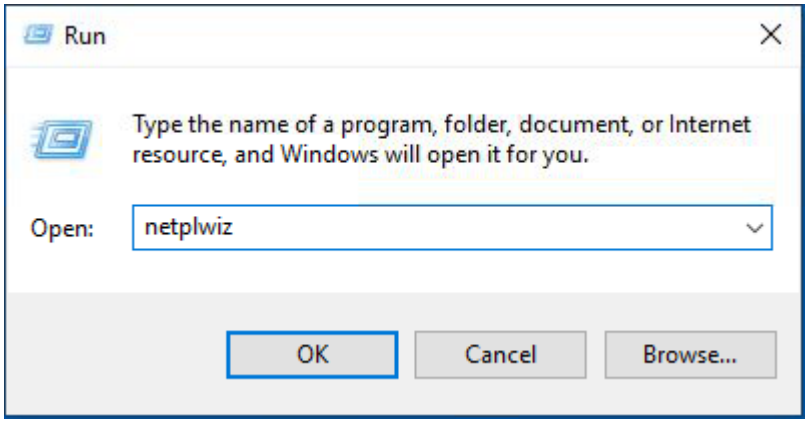
Um die Eingabe eines Passworts beim Einloggen zu umgehen, kann ein automatischer Login für den Benutzer "Kiosk" konfiguriert werden. Hierfür muss man sich als user "XP504" einloggen. Nach dem Einloggen wird folgende Kommandozeile angezeigt. Diese kann mit dem Befehl explorer.exe beendet werden:



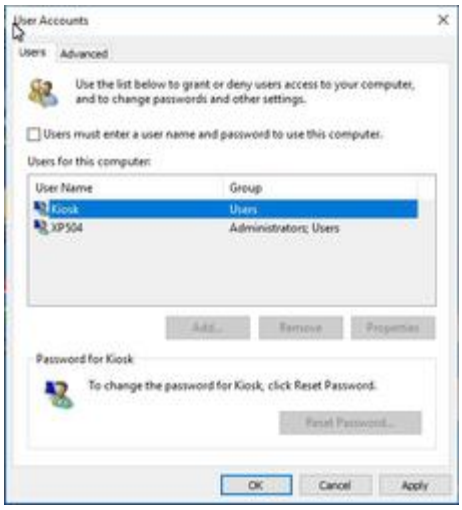
Minimiere die Kommandozeile und starte die Applikation "Run":



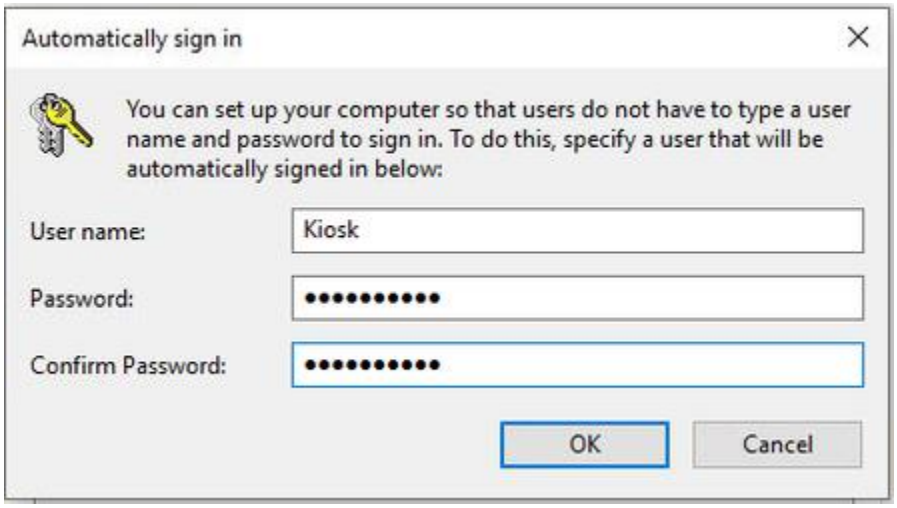
Öffne"netplwiz":



Wähle den Benutzer "Kiosk" aus und deaktiviere die Option "Users must enter a user name and password to use this computer":



Trage die Benutzer- und Passwortinformationen Put ein und bestätige im OK:

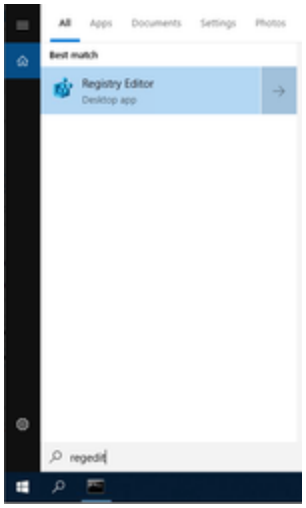


Wenn das XP504 nun neu gestartet wird, so wird der Benutzer "Kiosk" automatisch eingeloggt.

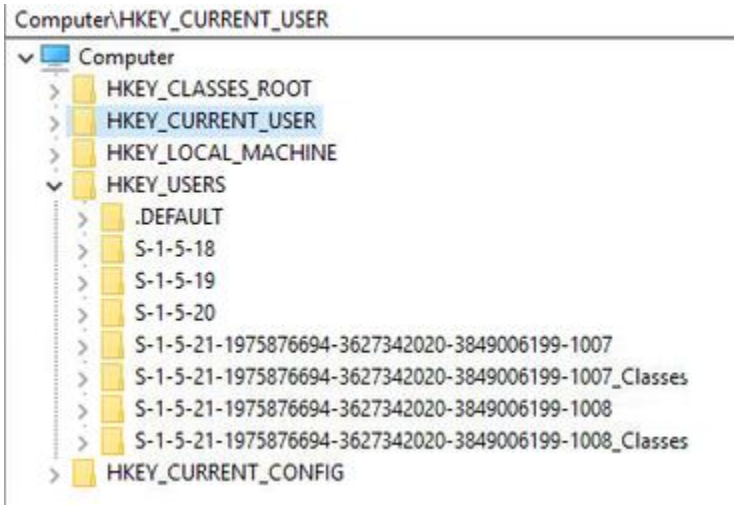
2.7 Bildschirmsperre deaktivieren

Nach einer bestimmten Zeit der Inaktivität, wird der Benutzer automatisch ausgeloggt. Um die Bildschirmsperre zu deaktivieren, kann folgendermaßen vorgegangen werden:

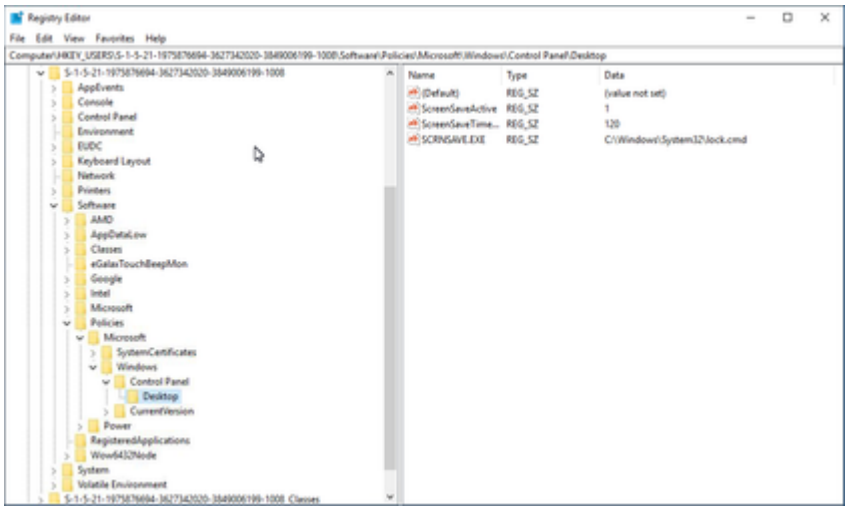
Öffne"regedit":



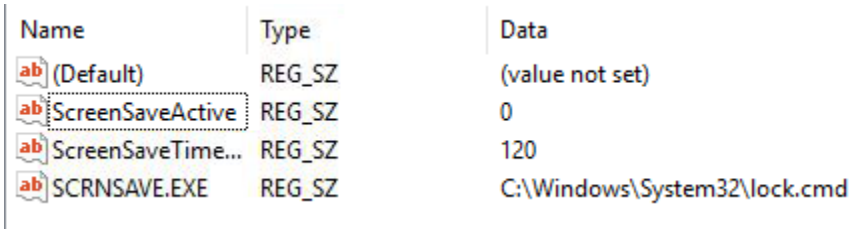
Öffne HKEY_USERS. Hier sollten nun zwei Benutzer definiert sein. Jeder Benutzer hat eine lange SID. Die erste (hier xx-1007) ist der Benutzer "XP504" und die zweite (hier xx-1008) der Benutzer "Kiosk":



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



Setze den Wert für "ScreenSaveActive" auf "0":



Name	Type	Data
(Default)	REG_SZ	(value not set)
ScreenSaveActive	REG_SZ	0
ScreenSaveTime...	REG_SZ	120
SCRNSAVE.EXE	REG_SZ	C:\Windows\System32\lock.cmd

Diese Einstellung wird die Bildschirmsperre nur für den Benutzer "Kiosk" deaktivieren.

Eaton ist ein intelligentes Energiemanagementunternehmen, das sich dem Ziel verschrieben hat,
für mehr Lebensqualität zu sorgen und die Umwelt zu schützen. Wir handeln verantwortlich und nachhaltig und -unterstützen unsere Kunden beim Energiemanagement – heute und in Zukunft.
Wir setzen auf die globalen Wachstumstrends Elektrifizierung und Digitalisierung und beschleunigen so die Umstellung der Welt auf erneuerbare Energien, tragen zur Lösung der weltweit dringendsten Herausforderungen im Energiemanagement bei und setzen uns für das Beste für unsere Stakeholder und die ganze Gesellschaft ein.

Das 1911 gegründete Unternehmen Eaton ist seit fast einem Jahrhundert an der NYSE notiert.
Im Jahr 2021 verzeichneten wir einen Umsatz von 19,6 Milliarden US-Dollar und wir sind in über 170 Ländern vertreten.

Weitere Informationen finden Sie unter Eaton.com. Folgen Sie uns auf Twitter und LinkedIn.

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

07/2025 AP050021DE

Powering Business Worldwide