Microsoft Windows 2-Factor Logon (Credential Provider) v2.0.1

Check out the **latest version of the SecureAuth Credential Provider**

Introduction

Use the SecureAuth Credential Provider to protect Windows Desktops and Servers with an additional 2-Factor Authentication module.

Companies and organizations use the SecureAuth Credential Provider to enhance typical Windows Logon functions by adding a 2-Factor Authentication requirement to the username and password validation.

SecureAuth IdP Credential Provider supports usage of the following features:

- **OATH OTP** Multi-Factor Authentication method provided by a SecureAuth mobile, desktop, or browser app, or a third-party hardware token
- **online and offline mode**
- **Logon and Unlock Windows functions**

Prerequisites

SecureAuth IdP	SecureAuth App Enrollment Realm	Windows Devices / Components
Version 8.0 +	(i.e. OATH Provisioning Realm, SecureAuth998) completely configured beforehand • SecureAuth IdP 9.0.x • SecureAuth IdP 8.2.x • SecureAuth IdP 8.1.x • SecureAuth IdP 8.0.x	• Windows 7, 8, and 8.1 for desktops (32-bit or 64-bit support) • Windows 2008 for servers (32-bit or 64-bit support) • Windows 2008 R2, 2012, 2012 R2 for servers (64-bit only support) • .NET 4.5 Framework • SSL certificate that matches the FQDN of the SecureAuth IdP appliance

Do not install the Credential Provider on the SecureAuth IdP appliance

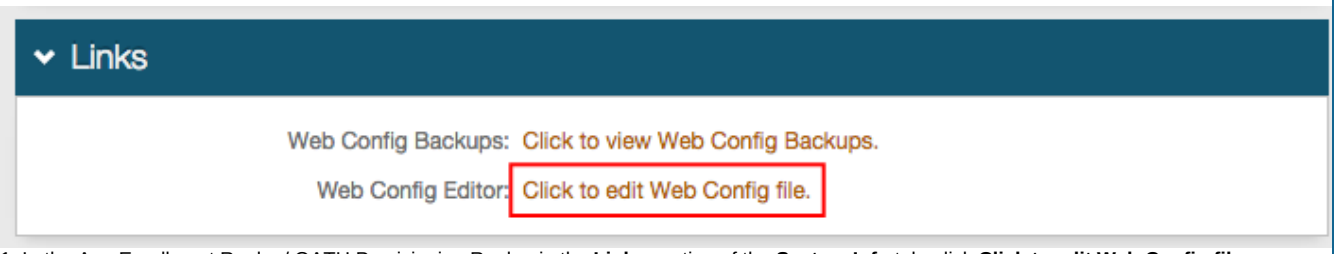
This can cause a deadlock condition and disable access to the appliance

The Credential Provider only supports the **OATH Seed** mode (single OATH seed value) and **not** OATH Token mode (multiple OATH seed values)

SecureAuth IdP Configuration Steps

Execute the following configuration steps in addition to the configuration steps in the **App Enrollment / OATH Provisioning Realm**

System Info



1. In the App Enrollment Realm / OATH Provisioning Realm, in the **Links** section of the **System Info** tab, click **Click to edit Web Config file**

2. In the **web.config file**, verify that the **<system.serviceModel>** section of the authentication realm appears as follows:

NOTE: For SecureAuth IdP versions 8.0.1 and lower, **useRequestHeadersForMetadataAddress** must be added manually

```
<system.serviceModel>
    <behaviors>
        <serviceBehaviors>
            <behavior>
                <useRequestHeadersForMetadataAddress/>
            </behavior>
        </serviceBehaviors>
    </behaviors>
</system.serviceModel>
```

For 9.0.2 Deployments

If using SecureAuth IdP version 9.0.2, then add the following app setting to the web.config:

```
<add key="CpValidateOTP" value="False" />
```

Click **Save** once the configurations have been completed and before leaving the **System Info** page to avoid losing changes

Windows 2-Factor Logon for Desktop Setup Steps

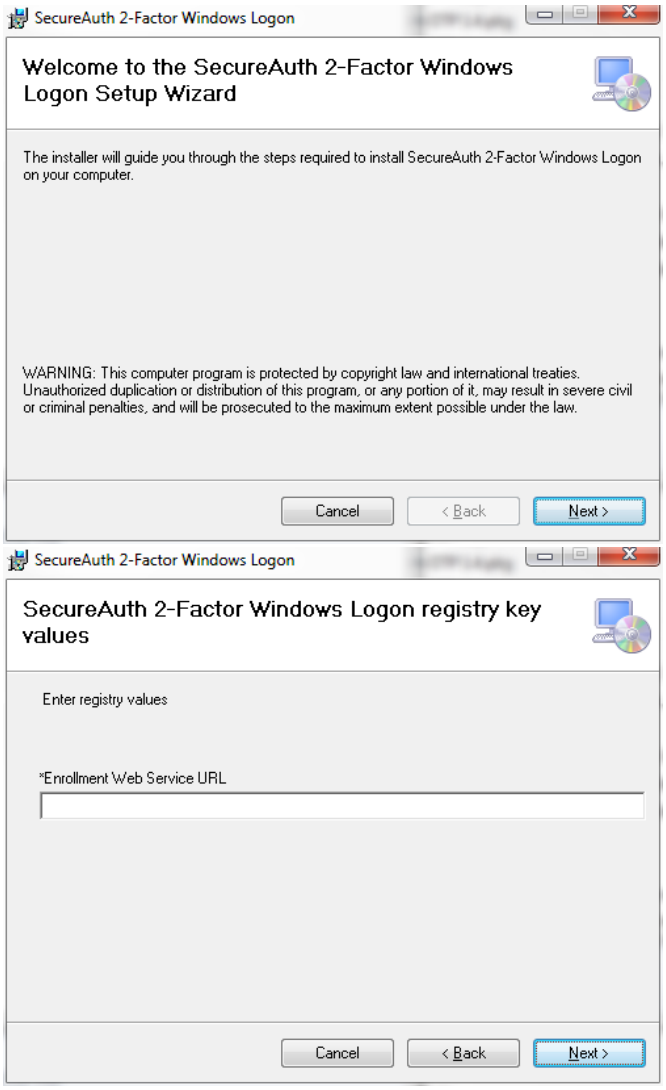
The SecureAuth Credential Provider installer supports the **Wizard install mode** and **silent mode** installation

Prior to deploying the Credential Provider, confirm that **https://<SecureAuthIdPFQDN>/secureauth998/WebService/profilews.svc** resolves without SSL certificate errors from the workstation on which the Credential Provider is being installed

1. Contact **SecureAuth Support** to obtain the latest SecureAuth Credential Provider installer

Wizard Mode

SecureAuth 2-Factor Windows Logon



2. Execute the **SecureAuth 2-Factor Windows Logon** (Credential Provider) installer
3. Set the **Enrollment Web Service URL** to the **SecureAuth IdP appliance enrollment URL**, which must include the full path as per the following example:

    https://secureauth.company.com/secureauth998/WebService/profilews.svc

4. Click **Next** to complete the installation

Silent Mode

The silent mode is intended for enterprise administrators who leverage software distribution tools or group policies for MSI distribution / installation

2. Open a **Command Prompt** with the privileges to execute the installer and type in the following:

```
msiexec /i "msi-path\SecureAuth_2-Factor_Windows_Logon_Installer.msi" /qn /l* SecureAuthOut.txt
CmdOtpSeedURL=https://secureauth.company.com/secureauth998/webservice/profilews.svc
```

Replace **msi-path** with the actual path of the file, e.g. C:\users\admin\downloads

Replace **secureauth.company.com** with the actual Fully Qualified Domain Name (FQDN) of the SecureAuth IdP appliance

Replace **secureauth998** with the actual SecureAuth App Enrollment Realm if using a different realm for the OATH Seed Enrollment

3. Review the **C:\SecureAuthOut.txt** text file for any failure or error messages

End-user Experience

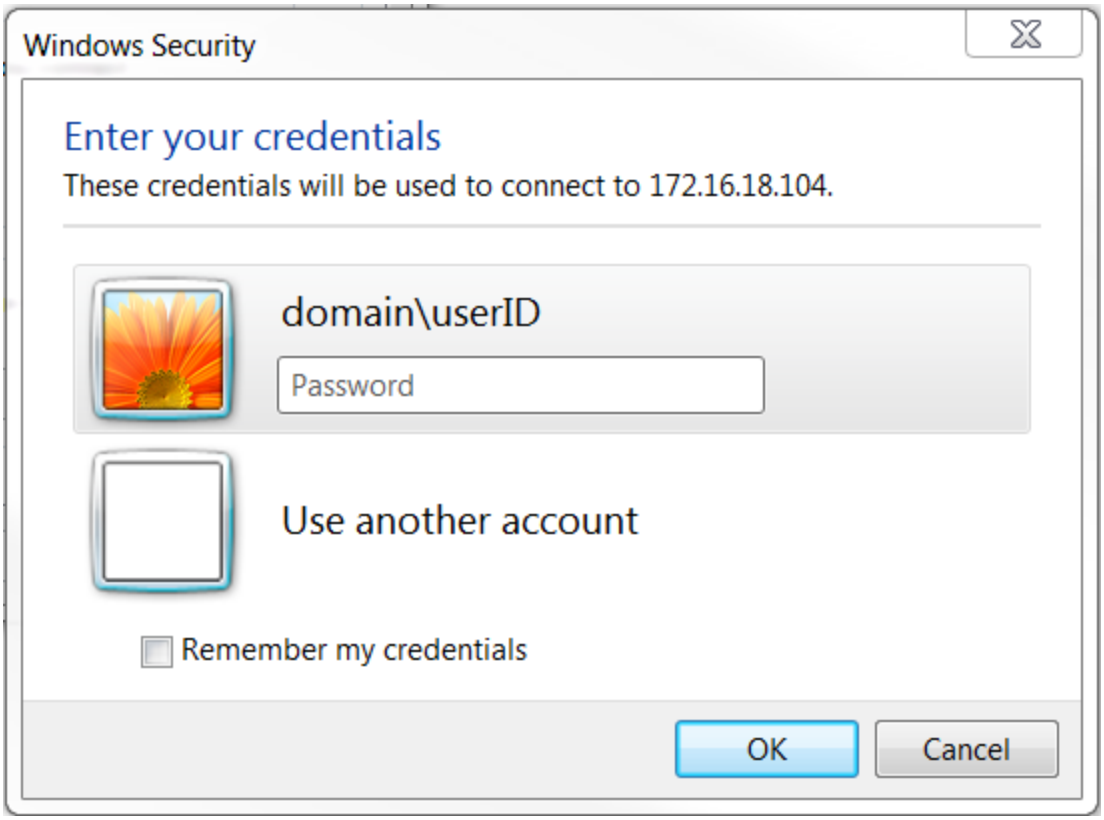
Windows Desktop Login

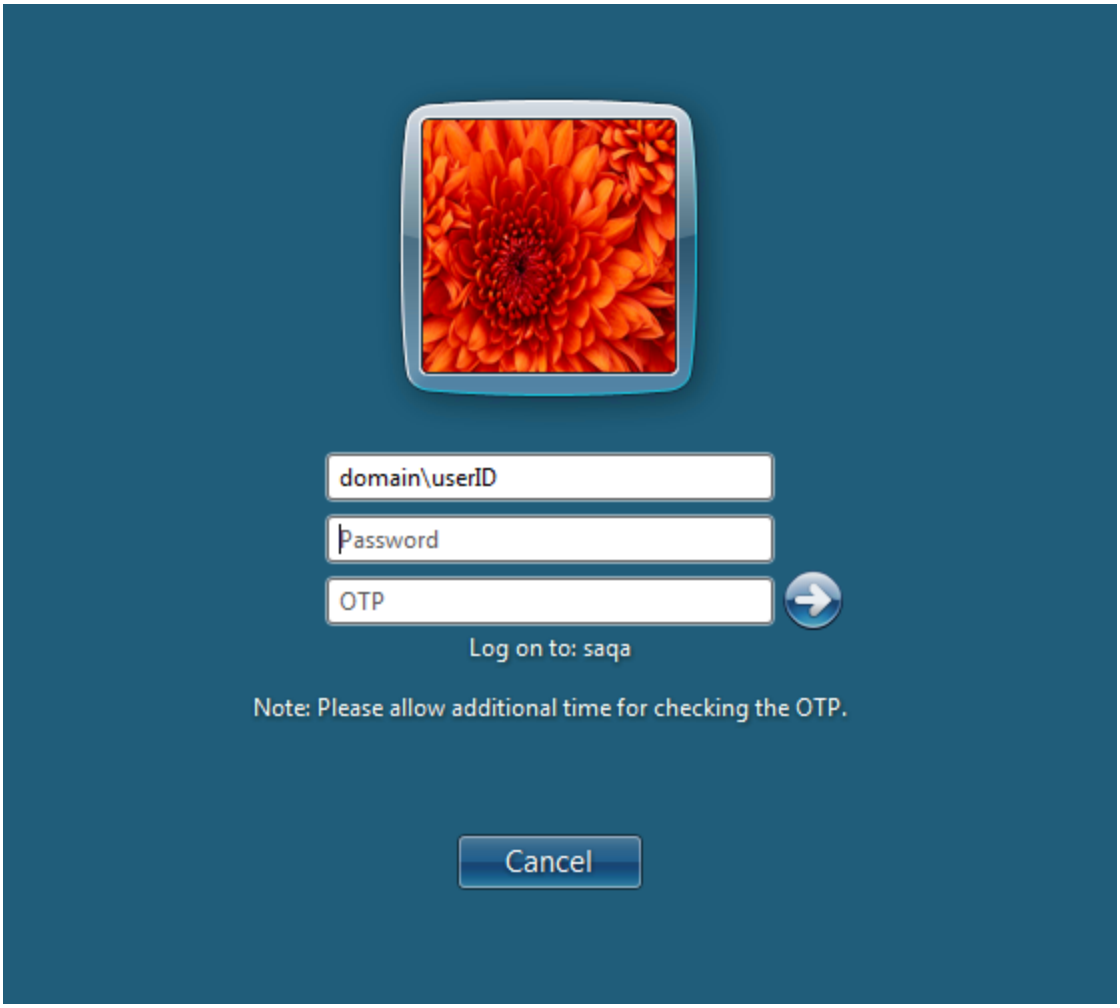
For the initial logon, specify the **domain name** in the **Username** field, e.g. **Domain\Username**

The login screen displays three text boxes, one for **Username**, one for **Password**, and one for **OTP**

Windows Server Login

In some configuration scenarios, client-side authentication (ID and password only) may be required before being challenged by the Credential Provider


Windows Security
Enter your credentials
These credentials will be used to connect to 172.16.18.104.
domain\userID
Password
Use another account
Remember my credentials
OK
Cancel



Optional Server Installation Step

Disable Network Level Authentication (NLA) to allow only locally-stored users to access the VM

Consult the System Administrator on the corporate policy and procedure of disabling NLA

The requirement for OTP can be changed for console or RDP sessions

See the logging section below for the required registry settings

References

- Remote Desktop Connection 6.0 message:

  https://support.microsoft.com/en-us/help/941641/remote-desktop-connection-6-0-prompts-you-for-credentials-before-you-e

- Windows Server 2016 / Windows 10 connection message:

  http://blog.zmarzly.me/windows-server-2016-windows-10-the-connection-cannot-proceed-because-authentication-is-not-enabled/

(Optional) Credential Provider Preferences

The Credential Provider (by default) requires 2-Factor Authentication for the local console and for RDP sessions

To change the settings:

1. Select **Start** and search for **regedit**

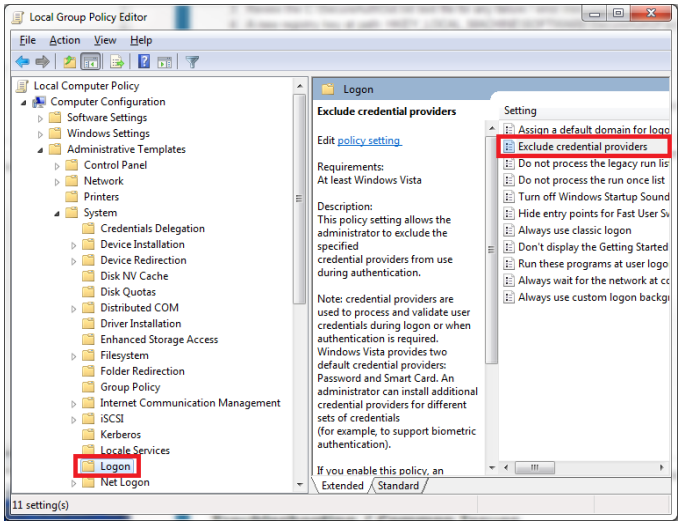
2. In the **Registry Editor**, navigate to **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **SecureAuth2FactorCP**

3. Double-click on each of the registry settings (more information in the section below), enter one of the following options for each, and click **OK**:

otpRDP: Default is 2

- otpEnableForRDP = 0 > SecureAuth CP only enforces for local console 2-Factor login
- otpEnableForRDP = 1 > SecureAuth CP only enforces for RDP session 2-Factor login
- otpEnableForRDP = 2 > SecureAuth CP enforces for both local and RDP 2-Factor login

(Optional) Disabling other logon methods to enforce SecureAuth 2-Factor Authentication

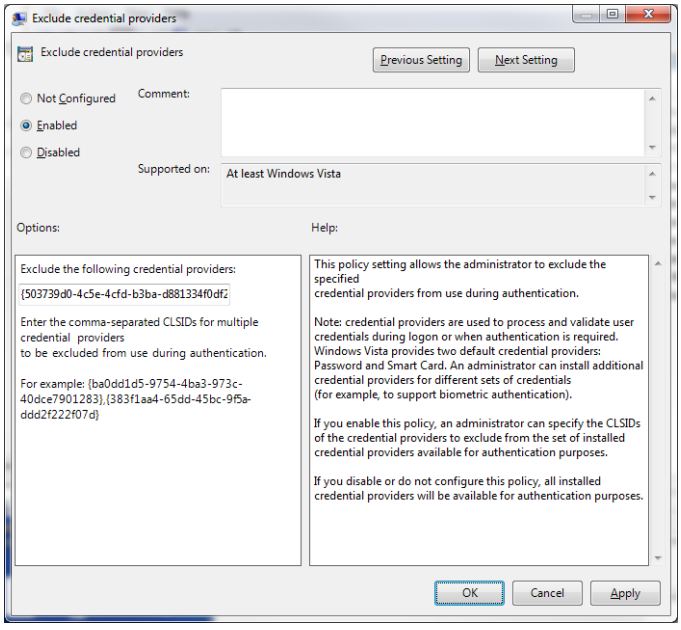


1. Open **gpedit.msc**

2. Navigate to **Local Group Policy Editor** > **Computer Configuration** > **Administrative Templates** > **System** > **Logon** > **Exclude credential providers**

3. Select **Enable** and then add the following string to the **Exclude the following credential providers** text box:

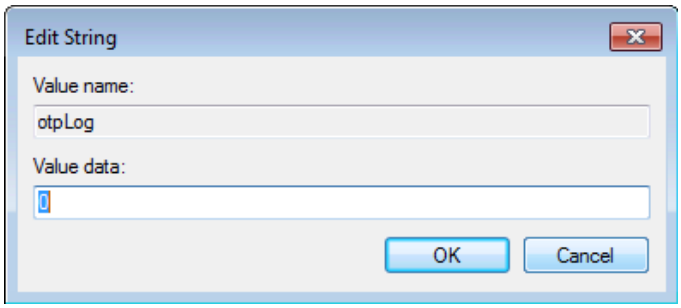
```
{1b283861-754f-4022-ad47-a5eaaa618894},{1ee7337f-85ac-45e2-a23c-37c753209769},{2135f72a-90b5-4ed3-a7f1-8bb705ac276a},{25CBB996-92ED-457e-B28C-4774084BD562},{3dd6bec0-8193-4ffe-ae25-e08e39ea4063},{600e7adb-da3e-41a4-9225-3c0399e88c0c},{60b78e88-ead8-445c-9cfd-0b87f74ea6cd},{8FD7E19C-3BF7-489B-A72C-846AB3678C96},{94596c7e-3744-41ce-893e-bbf09122f76a},{BEC09223-B018-416D-A0AC-523971B639F5},{cb82ea12-9f71-446d-89e1-8d0924e1256e},{e74e57b0-6c6d-44d5-9cda-fb2df5ed7435},{F8A0B131-5F68-486c-8040-7E8FC3C85BB6},{503739d0-4c5e-4cfd-b3ba-d881334f0df2},{6f45dc1e-5384-457a-bc13-2cd81b0d28ed},{8bf9a910-a8ff-457f-999f-a5ca10b4a885},{AC3AC249-E820-4343-A65B-377AC634DC09}
```



4. Click **OK**

5. Restart the computer

(Optional) Activate Logging



By default, the logging feature is turned off

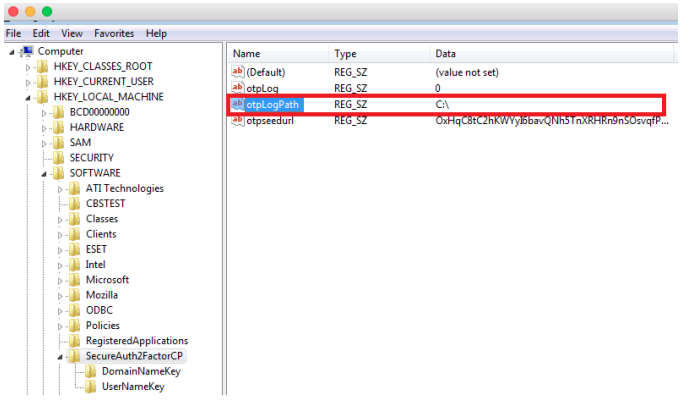
1. To turn on logging for troubleshooting, select **Start** and search for **regedit**

2. In the **Registry Editor**, navigate to **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **SecureAuth2FactorCP**

3. Double-click on each of the registry settings, enter one of the following options for each, and click **OK**:

- **otpLog:** Default is 0
  - Enter 1 to enable logging
  - Enter 0 to disable logging

- **otpLogPath:**Default is **%windir%\Temp** (e.g. C:\Windows\Temp)
  - Path where SecureAuth stores the log files



4. If **1** is entered to turn on logging in step 3, then click on **otpLogPath** and enter the location to where the log file is saved

If contacting SecureAuth Support, then send the following logs:

- **OTPCredentialProvider.txt:** Used by Support during the initial troubleshooting to analyze what has occurred
- **OTPManager.txt** and **OTPSeedCalc.txt**: Contain code that SecureAuth developers review to troubleshoot complex issues

Uninstall Configuration Steps

Wizard Mode

1. Double-click the **SecureAuth 2-Factor Windows Logon** installer

2. Select **Remove** and then click **Next** to complete

Silent Mode

Enter the following in the **Command Prompt**:

```
msiexec /x "msi-path\SecureAuth_2-Factor_Windows_Logon_Installer.msi" /q
```

Replace **msi-path** with the actual path of the file, e.g. C:\users\admin\downloads

Troubleshooting / Common Issues

If additional OTP text box does not display after restart

An additional restart may be required

Error Messages and What They Mean

An internal system error occurred - please contact your system administrator: This typically indicates that something has been misconfigured, or a component is not registered or is missing. It could also mean that a catastrophic error has occurred, such as a memory allocation error or a disk full situation that needs the attention of an administrator. Uninstall and reinstall is recommended.

Invalid Username, Password, or One-Time Password: This typically indicates that either the incorrect credentials were entered or that the user did not perform the initial logon when on the domain. The client computer must be able to reach the SecureAuth IdP appliance and the domain for the initial logon so that the seed values can be cached in the registry and so that the computer can be used offline.

An invalid username was entered - please try again: This indicates that the username could not be parsed due to invalid syntax (e..g,, "\", "\username", "domain\").

Release Notes

Release Date	May 22, 2015
Version	2.0.1

What's New	32-bit Windows support (previously 64-bit support only)	
	Ability to toggle requirement for 2-Factor Authentication on RDP sessions versus console login	
Resolved Issues	Installation not completing properly on some Windows Systems	
Known Issues	901	When performing runas function or mapping network drive, the ID and password fields are not present
	872	Login using UPN format is not supported
	871	User is not prompted to change password when password expires