Login for Windows configuration guide v1.0.4

Introduction

Security Notice
A critical security vulnerability affects SecureAuth Login for Windows version 1.0. SecureAuth recommends all users upgrade to version 1.0.1 (or later) immediately.

Login for Windows, available in SecureAuth IdP version 9.2 and later only, adds SecureAuth’s multi-factor authentication to the Windows desktop and remote server login experience.

See the Release notes to learn about new features, enhancements, resolved issues, known issues, and hotfixes.

This product supports the following authentication methods:

- Timed Passcode
- Voice Call
- Passcode sent via SMS / Text Message
- Passcode sent via Email
- One-time Passcode via Push Notification
- Login Notification via Push Notification
- YubiKey HOTP Device Passcode
- YubiKey OATH-TOTP Device Passcode
- Passcode from Help Desk
- Security Questions (knowledge-based questions and knowledge-based answers)


In addition to the supported multi-factor authentication methods, Login for Windows supports the following setups and features:

- Offline mode login
- Multi-factor authentication for desktops and remote servers
- Multi-factor authentication for single users only and multi-users
- Users in bypass group can skip multi-factor authentication
- Bypass group lookup on a domain other than user's domain
- Password expiration notification
- Password Reset link to SecureAuth IdP realm or 3rd party service
- Multiple login capability
- Endpoint identified during login multi-factor authentication request
- Use Third-party Credential Providers
- YubiKey HOTP support for 2-Factor Authentication
- YubiKey OATH-TOTP support for first-time authentication
- TOTP 2-Factor Authentication
- Cached user credentials, which let users sign in with fewer clicks
- Installation API validation, to ensure successful login to Login for Windows
- Adaptive Authentication
- Validated with FIPS 140-2 compliant cryptographic libraries

DISCLAIMERS:

- Login for Windows does not support non-domain joined devices. Issues pertaining to account synchronization are the responsibility of the customer and not SecureAuth.
  If a computer is not domain-joined AND all local users are blocked by Adaptive Authentication OR are not Active Directory members on SecureAuth IdP, end users receive the following message: Access is denied for all users on this computer.

- Login for Windows supports the samAccountName login name format if using Microsoft Active Directory (AD); in this use case, userPrincipalName (UPN) is not supported.
  UPN is supported at login if running Login for Windows with a non-AD profile store containing OATHSeed/OATHToken/PNToken. In this use case, samAccountName is not supported, so the multi-factor authentication lookup will fail and the user will be unable to use other multi-factor authentication methods.

- Login for Windows users might be unable to complete the self-service password reset process because of default Internet Explorer settings in the operating systems on Windows Server versions 2008 R2 and 2012 R2.
  The Login for Windows Self-Service Password Reset feature does not function in environments that use a proxy to access SecureAuth IdP. Contact SecureAuth Support and inquire about workarounds. Note this feature differs from the inline password reset feature that is used when a user’s password expires. The inline password reset feature functions properly in proxy environments.
Prerequisites

Administrator

Login for Windows requires SecureAuth IdP version 9.2 or later.

Setup requirements

1. Ensure SecureAuth IdP v9.2 or later is running and is using a SHA2 or later certificate bound to Microsoft Internet Information Services (IIS). For example, in the IIS Management Console’s Default Web Site section, check the Site Bindings section to ensure the https://443 type and port settings have a valid and trusted SHA2 certificate selected, as shown in the following image:

2. Create a realm or access an existing realm where more than one multi-factor authentication is required.

   NOTE: Do not configure this realm for Single Sign-on.

3. Configure these SecureAuth IdP Web Admin tabs: Overview, Data, Workflow, Multi-Factor Methods, Post Authentication, and Logs.

4. Ensure target end-user machines are running any of the following supported OS versions:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows OS versions:</td>
<td>• Windows Server 2008 R2 (64-bit)</td>
<td></td>
</tr>
<tr>
<td>• Windows 7 (32/64-bit)</td>
<td>• Windows Server 2012 (64-bit)</td>
<td></td>
</tr>
<tr>
<td>• Windows 8.1 (32/64-bit)</td>
<td>• Windows Server 2012 R2 (64-bit)</td>
<td></td>
</tr>
<tr>
<td>• Windows 10 (64-bit)</td>
<td>• Windows Server 2016 (64-bit)</td>
<td></td>
</tr>
</tbody>
</table>

NOTE: To use the proxy bypass feature with Windows, a proxy server and proxy bypass list must be configured. See Login for Windows Installer Configuration for information about configuring the proxy server and proxy bypass list.

Verify TLS 1.1 and TLS 1.2 enablement via GPO on Windows Server OS

Verify TLS 1.1 and TLS 1.2 are enabled via the Group Policy Object (GPO) to ensure a streamlined and secure login experience for users logging on a Remote Desktop.

The external article How to Enable TLS 1.1 and TLS 1.2 in Internet Explorer via Group Policy provides instructions on how to enable TLS 1.1 and TLS 1.2.

NOTE: TLS 1.1 and TLS 1.2 are not enabled by default on Windows Server 2008 R2.
End-user

First-time usage requirements

Login for Windows requires end users to use one OATH-based method (i.e., TOTP, YubiKey), if at least one method is available to end users. If at least one OATH-based method is not available to end users, they can use any other available method.

To meet this requirement, end users must use one of the following accounts provisioned with a SecureAuth IdP realm that enables their device to generate timed passcodes for multi-factor authentication:

- SecureAuth Authenticate App on a phone or tablet or
- YubiKey HOTP or TOTP security key. Refer to the YubiKey HOTP Device Provisioning and Multi-Factor Authentication Guide or the YubiKey OATH-TOTP Device Provisioning and Multi-Factor Authentication Guide to ensure all requirements are met. To ensure that supported YubiKey devices are used, see the “YubiKey” section of the SecureAuth Compatibility Guide.

Thereafter, end users can use Login for Windows to log in when working online and offline.

NOTE: If end users are currently using the SecureAuth Credential Provider, they do not need to uninstall it before installing Login for Windows.

SecureAuth IdP Web Admin configuration

Data tab

1. Create a new realm and configure a data store on the Data tab.

2. In the Membership Connections Settings section, under Group Permissions, select True from the Advanced AD User Check dropdown.

3. Select Bind from the Validate User Type dropdown.
4. In the Profile Fields section, enter **adminDescription** in an unused **Aux ID**—**Aux ID 3** in this example—and make the field **Writable**.

5. If using a single OATH seed for end-user multi-factor authentication (see sample Post Authentication page image), then map Fields to **OATH Seed** and **OATH Tokens** Properties, as shown in the Profile Fields image below.
<table>
<thead>
<tr>
<th>Property</th>
<th>Source</th>
<th>Field</th>
<th>Data Format</th>
<th>Writable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groups</td>
<td>Default Provider</td>
<td>memberOf</td>
<td></td>
<td></td>
</tr>
<tr>
<td>First Name</td>
<td>Default Provider</td>
<td>givenName</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aux ID 2</td>
<td>Default Provider</td>
<td></td>
<td>Plain Text</td>
<td></td>
</tr>
<tr>
<td>Aux ID 3</td>
<td>Default Provider</td>
<td>adminDescription</td>
<td>Plain Text</td>
<td>✓</td>
</tr>
<tr>
<td>Aux ID 4</td>
<td>Default Provider</td>
<td></td>
<td>Plain Text</td>
<td></td>
</tr>
<tr>
<td>OATH Seed</td>
<td>Default Provider</td>
<td>description</td>
<td>Advanced Encryption</td>
<td>✔</td>
</tr>
<tr>
<td>One Time OATH List</td>
<td>Default Provider</td>
<td>postalAddress</td>
<td>Plain Text</td>
<td>✓</td>
</tr>
<tr>
<td>Fingerprints</td>
<td>Default Provider</td>
<td>audio</td>
<td>Plain Binary</td>
<td>✓</td>
</tr>
<tr>
<td>Push Notification Tokens</td>
<td>Default Provider</td>
<td>jpegPhoto</td>
<td>Plain Binary</td>
<td>✓</td>
</tr>
<tr>
<td>OATH Tokens</td>
<td>Default Provider</td>
<td>registeredAddress</td>
<td>Plain Binary</td>
<td>✓</td>
</tr>
<tr>
<td>Access Histories</td>
<td>Default Provider</td>
<td></td>
<td>Plain Binary</td>
<td></td>
</tr>
<tr>
<td>Behavior Biometrics</td>
<td>Default Provider</td>
<td></td>
<td>Plain Text</td>
<td></td>
</tr>
</tbody>
</table>
SecureAuth recommends setting OATH Tokens. If OATH Tokens is not set, users might receive a failure message when attempting to authenticate by using TOTP after their device wakes from sleep mode while online. The failure occurs because a second factor method is sent at different times between the device being connected to the internet and disconnected from the internet, which causes the timed passcodes to be out of sync.

6. Click **Save**.

**Optional: Adaptive Authentication tab**

Use **Adaptive Authentication** to control the user login experience and to mitigate security risks.

The order of priority to handle user authentication login requests using Adaptive Authentication is as follows:

A. Threat Service
B. IP allow list / deny list
C. Geo-location
D. Geo-velocity
E. User / Group

**NOTE:** See Group Bypass configuration notes in the [Login for Windows Installer configuration](#) section for information about using Adaptive Authentication with the group bypass feature.

---

**Multi-Factor Methods tab**

7. In the Multi-Factor Configuration section, configure the multi-factor authentication methods you want enabled.

8. Click **Save**.
Multi-Factor Configuration

Phone Settings

Phone Field 1: One-Time Passcode via Phone
Phone Field 2: One-Time Passcode via Mobile
Phone Field 3: Disabled
Phone Field 4: Disabled
Phone/SMS Selected: Voice
Phone/SMS Visible: True
Default Phone Country Code:
Phone Mask (Regexp):

Multi-Factor Settings

Inline Initialization:
- Missing Phone
- Missing Email
- Missing KB Answers
- Missing PIN

Auto-Submit When One Avail: Enabled

OTP Length: 6

Multi-Factor Throttling

- Enable multi-factor throttling
  - Only allow 5 failed attempts
    - in 30 Minutes
  - Block use of multi-factor until time limit has expired
  - Lock user account after exceeding attempts

Store attempt count in Browser Session
Optional: Security Questions setup

Set up Security Questions so users can authenticate by answering knowledge-based questions (KBQ). Security Questions gives users the option to log into devices without requiring a phone or token.

Follow steps in the Knowledge-based Authentication (KBA / KBQ) as 2-Factor Authentication Method Configuration Guide to set up knowledge-based questions for end users.

System Info tab

9. Open the web.config file, located at D:\SecureAuth\SecureAuth1 on the appliance.

10. Add the following line under <appSettings>:

   `<add key="OTPFieldMapping" value="AuxID#" />

   NOTE: In this example, AuxID3 is used because this Property was selected and configured on the Data tab in step 4.

11. Save the changes before exiting from the file.
<add name="OracleServer" connectionString="Data Source=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=localhost)(PORT=1522)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=[DBName]))); User Id=[username];Password=[password]"
    providerName="OracleProvider" />
</connectionStrings>

API tab

12. In the API Key section, click Generate Credentials.

The API ID and API Key are required and used in the config.json file for all scenarios of using this product.

13. In the API Permissions section, select Enable Authentication API.

NOTE: It is not recommended to enable Identity Management options since the password reset function uses an IdP realm or third party password reset URL—not the Identity Management API.
14. Click **Save** once the configuration is complete.

15. Select **Enable Login for Endpoints API**, and then click **Configure Login for Endpoints Installer**.

**Login for Windows Installer Configuration**

16. On the Login for Endpoints Installer Configuration page, select **Windows** as the **Endpoint Operating System**.

17. Select the **Endpoint Type** to specify that either a single user or multiple users can log on the device.

   **NOTE:** For the single user selection, once the user has successfully logged on the endpoint online, thereafter the user can log on the endpoint offline without an Internet connection.

18. Enter the **IdP Hostname**.

19. Under Multi-Factor Authentication Settings, specify whether the user must use multi-factor authentication to access the device from a desktop and / or remote desktop session.

20. If any user group is allowed to bypass multi-factor authentication, enable the bypass option and list the user group(s).

   **Group Bypass configuration notes:**
   - If using Adaptive Authentication AND the group bypass feature, Adaptive Authentication takes precedence for handling the user's login request and group bypass is checked next.
   - In a multi-forest AD environment, the user account must be included on each domain to bypass multi-factor authentication on any domain.
   - Login for Windows supports the group bypass feature when users are online and offline. An internal group cache performs validations when Active Directory is unreachable.
   - The group specified must be a top-level group; nested groups are **not** supported.

   **If using a proxy bypass, you must configure the proxy server and proxy bypass list, which is a list of hosts to use to bypass the proxy.**

   **Proxy Server and Proxy Bypass List configuration notes:**
   - The following order is used:
     - A. "proxy_server" and "proxy_bypass" configuration from config.json file. These settings are derived from entries made in the Web Admin Login for Endpoints Installer Configuration section.
     - B. Windows proxy configuration. See the Netsh.exe and ProxyCfg.exe Proxy Configuration Tools article on the Microsoft website.

21. If enabling **Password Reset**, specify either the SecureAuth IdP realm or the web page URL the user can access for resetting a password.

22. If **Alternate Credential Providers** are permitted, specify if non-SecureAuth credential providers and other credential providers, such as card scanners, can be used.
Alternate Credential Provider notes:

- By enabling alternate credential providers, users will be able log in without using the Login for Windows credential provider, and potentially bypass multi-factor authentication.
- Enabling alternate credential providers is only recommended in test environments, to let testers bypass Login for Windows so they can readily access their machines.
- If the default Windows Credential Provider is enabled, users will see their normal login prompt and will have to manually select a different login option in order to use Login for Windows.

23. Click **Download Installer Config** to download the JSON file (config.json). The JSON file must first be configured before it can be used with the MSI file, as described in the Installation section of this guide.

NOTE: *Before* installation, config.json must be edited if the end-user is not always required to use multi-factor authentication for logging on a local console and/or remote console. See the **Set end-user access level** section for access level settings and configuration.
Login for Endpoints Installer Configuration

Configure and download the installer config for Login for Endpoints

Endpoint Operating System

- **Windows**
- **Mac OS**

Endpoint Type

- **Single user login (laptops, single-user desktops)**
  Single-user machines will remember the last user who logged in, default to their account, fill in their username, and cache their CATH seed.

- **Multiple user login (servers, multi-user kiosks)**
  Multi-user machines will not show who has previously logged in, but will cache a user's CATH seed for later use.

IdP Hostname

Enter the hostname of the IdP to use in the configuration

company.secureauth.com

Multi-Factor Authentication Settings

Require Multi-factor Authentication when:

- Logging in with physical access
- Logging in via Remote Desktop Protocol

Bypass Multi-factor Authentication when:

- Users are a member of the following groups:
  
  Add groups separated by commas or line breaks

Password Reset

- Enable update password link on the login interface.

  - **Use SecureAuth password reset realm**
    142. Self Service Page

  - **Point to other password reset site**
    Enter the site URL
Pre-installation steps

Optional: Set end-user access level

Login for Windows requires the end-user to use multi-factor authentication by default to access the local console or remote console in an RDP session.

Before installing Login for Windows on the end-user's (target) machine, the config.json file must be edited if you want to change the end-user's login access level setting.

Change the user's access level

1. Find the config.json file you downloaded in step 23 of the Web Admin Configuration section of this document, and copy that file to the Temp folder on the target machine.

2. Start a text editor such as Notepad++ and edit the access_level in the file, changing the value to a pertinent value:
   - 0 = Multi-Factor Authentication always required
   - 1 = Multi-Factor Authentication required for local access only
   - 2 = Multi-Factor Authentication required for remote access only
   - 3 = Multi-Factor Authentication never required. This setting is used for Self-service Password Reset (SSPR) only.

3. Save the configuration.

SSPR is completed in SecureAuth IdP. After the password reset, the local machine still must contact Active Directory to verify the password change. After verification, the new password is available on the local machine.

Verify "allow_self_signed" setting

Setting "allow_self_signed" to True is commonly used in test or lab environments in which the server has a self-signed certificate. This setting is not supported in a production environment because it introduces critical security risks, namely the potential "Man in the middle" attack which grants users access to a system without validating their credentials, and lets unauthorized users steal OATH seeds.

Find the config.json file you downloaded in step 23 of the Web Admin Configuration section of this document, and verify the setting for "allow_self_signed". You may need to change this setting based on how users will log on your environment.

Note that after installing an endpoint with "allow_self_signed" set to True, this setting remains effective until Login for Endpoints is uninstalled and then reinstalled using a configuration file with "allow_self_signed" set to False.

Verify "version" setting
If you have set up an IdP realm to use HOTP or TOTP, set "version" to "v2" in the config.json file. This keeps end users from receiving an error message that they must "change password at next login" or that their expired password fails without allowing them to change the expired password. You must also complete the settings in the Data tab.

Find the config.json file you downloaded in step 23 of the Web Admin Configuration section of this document and edit it.

In the config.json file, find the "version" key and set it to "v2", as follows:

"version": "v2",

```
{
    "multiple_user": false,
    "idm_ssp_url": "https://localhost/SecureAuth2",
    "idm_ssp_label": "Password Reset",
    "alternate_providers": [],
    "version": "v2",
    "platform": "windows",
    "type": "idp",
    "apis": [
        { "id": "", "secret": "", "host": "https://localhost/SecureAuth2" },
        { "id": "", "secret": "", "host": "https://localhost/SecureAuth3" }
    ],
    "access_level": 0,
    "group_bypass": [],
    "allow_self_signed": false,
    "enabled_on_uac": true
}
```

Optional: Enable failover to one or more backup SecureAuth IdP instances

You can set Login for Windows to failover to one or more alternate IdP instances automatically if the main IdP instance fails. You can specify up to five backup instances and set the order that they are used.

Find the config.json file you downloaded in step 23 of the Web Admin Configuration section of this document and edit it.

1. Specify the IdP instance to failover to by replacing the "api_id", "api_secret", and "host" keys with a new "apis" array.

2. In the config.json file, replace the "api_id" and "api_secret" keys and set the host to specify a single or multiple backup IdP instances.

To specify a single backup IdP instance, edit the file as follows:

"apis": [
    { "id": "", "secret": "", "host": "https://localhost/secureauth#" }
],

Where secureauth# is your single backup IdP instance.

To specify multiple backup IdP instances, edit the file as follows:

"apis": [
    { "id": "", "secret": "", "host": "https://localhost/secureauth2" },
    { "id": "", "secret": "", "host": "https://localhost/secureauth3" }
],
The backup IdP instance is chosen in the order listed in the array. An IdP instance must be online or it is ignored and the next instance is used. In the above example, "secureauth2" will be chosen first, then "secureauth3".

Optional: Enable MFA for User Account Control (UAC) setting

You can enable or disable the UAC option based on how you want users to log on your environment.

- If you enable the UAC setting, users who log on as administrator (with "Run as administrator"), on the same machine used to log into a regular user account, will be required to authenticate again.
- If you disable the UAC setting, users who log on as administrator (with "Run as administrator"), on the same machine used to log into a regular user account, will not be required to authenticate again.
- "Run as administrator" with MFA is not supported on Windows 7 (x86 and x64) and Windows Server 2008 R2.

See [How User Account Control works](https://www.microsoft.com) on the Microsoft website to learn more about UAC.

Find the config.json file you downloaded in step 23 of the Web Admin Configuration section of this document and edit it.

In the config.json file, add the "enabled_on_uac" key and set it to "true" or "false", as follows:

```json
"enabled_on_uac": true
"enabled_on_uac": false
```
Installation steps

Download and run the Login for Windows MSI package

1. Download the Login for Windows.zip file to the target machine (laptop, desktop, server, etc.).

2. Unzip the file.

3. Within the Login for Windows folder, find the .msi file for your machine, either SecureAuthLogin-1.x.x-x64.msi or SecureAuthLogin-1.x.x-x86.msi. Place the file in the Temp folder.

Install Login for Windows

**IMPORTANT:** On a Windows server, SecureAuth Login for Windows should only be installed or uninstalled from a console session and not an RDP session.

1. Find the config.json file which you downloaded in step 23 of the Web Admin Configuration section of this document, and copy that file to the Temp folder on the target machine.

   **NOTE:** You may have already performed this step if you changed the user’s access level in the Set End-user Access Level section above.

2. On the target machine, run the following command line with administrator permissions, using the file name of your .msi file and correct path of that file on your machine, as in this example:

   ```
   msiexec /i "C:\Temp\SecureAuthLogin-1.0.4-x64.msi" /L*V "C:\Temp\install.log" /qn CONFIG="C:\Temp\config.json"
   ```

3. Log off the target machine.

After this installation, SecureAuth Login for Windows appears on the next login session.

**NOTES:**

- If using Login for Windows in a PCI environment, see Login for Windows SSL configuration requirements if Login for Windows is not installing on a machine.
- If reinstalling Login for Windows immediately after uninstalling the software, the "Failed to write configuration" message will appear if the installer is not finished performing cleanup tasks, such as removing the C:\ProgramData\SecureAuth directory.

SecureAuth IdP transaction log information
The Login for Windows software issues a User-Agent HTTP Request Header when the Application Programming Interface interacts with SecureAuth IdP. The following items are included in the User-Agent string:

- Login for Windows software version
- OS version
- Computer name (hostname)
- Time Zone
- IP address
- MAC address

For example:

SecureAuthLogin for Windows 10.5.2 (Windows 10 Pro x64 6.2.9200; LT-JSMITH; (UTC-05:00) Eastern Standard Time; 111.22.333.44; 0f:10;35:7a:81:4e)

**Uninstallation**

On the target machine, run the following command line with administrator permissions, using the file name of your .msi file and correct path of that file on your machine:

```bash
msiexec /x "<msi>" /L*V "uninstall.log" /qn
```

Alternatively, you can manually uninstall using the Windows "Programs and Features" menu. Use the following table to map the installation version number to the public product version:

<table>
<thead>
<tr>
<th>Installation version number</th>
<th>Public product version</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.11.6</td>
<td>1.0.4</td>
</tr>
<tr>
<td>10.11.5</td>
<td>1.0.3</td>
</tr>
<tr>
<td>10.11.4</td>
<td>1.0.2</td>
</tr>
<tr>
<td>10.10.5</td>
<td>1.0.0</td>
</tr>
</tbody>
</table>

**End-user login experience on Windows 10**

**Known Issues**

- If using a proxy that becomes unavailable, Login for Windows behaves as if it is offline. This issue might impact laptop users who connect their laptops to networks in which the proxy is unavailable.
- The Self-service Password Reset might not function correctly for certain operating systems. On Windows Server versions 2008 R2 and 2012 R2, users are unable to complete the self-service password reset process due to default Internet Explorer settings in the operating systems.

**First-time login experience**

1. Enter your username on the Windows login screen.

2. The first time end users log in, Login for Windows shows only OATH-based methods (for example, TOTP, HOTP YubiKey), if at least one method is available to end users. If at least one OATH-based method is not available to end users, they can use any other available method. This could be a method that uses the SecureAuth Authenticate App on your mobile device or another device provisioned with the SecureAuth IdP realm to supply timed passcodes, such as an HOTP YubiKey.

   After selecting a timed authentication option and entering your password, TOTP and HOTP passcode options will be available for you to use when logging on this machine offline.

   If you do not have an authentication method that provides a timed passcode, then select any other option available to you.
3. Show or hide the passcode so that, as you type, you see characters instead of dots.

   a. Focus on the passcode field and enter characters to see the following "eye" icon displayed.

   b. Click the icon and hold it until the dots in the field turn to characters.
   c. To hide the passcode, click and hold the icon until the characters turn to dots.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Timed passcode from app</strong>&lt;br&gt;Enter password&lt;br&gt;Timed passcode from app&lt;br&gt;Enter passcode</td>
<td>This method and &quot;Passcode from token&quot; are displayed at first login, if available. If not available, all available methods are displayed. &lt;br&gt;&lt;br&gt;For this option:&lt;br&gt;1. If there is more than one provisioned OATH OTP app, select the device.&lt;br&gt;2. Enter your Windows Password.&lt;br&gt;3. Click the arrow to log on Windows.</td>
</tr>
<tr>
<td>Option</td>
<td>Steps</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Passcode from voice call**                | 1. Select the phone number if more than one mobile phone is included in your user profile.  
                                           | 2. Enter your Windows Password.                                           
                                           | 3. Click the arrow to log on Windows.                                     |
| **Passcode from SMS / text**                | 1. Select the phone number if more than one mobile phone is included in your user profile.  
                                           | 2. Enter your Windows Password.                                           
                                           | 3. Click the arrow to log on Windows.                                     |
| **Passcode from email**                     | 1. Select the email address if more than one address is included in your user profile.  
                                           | 2. Enter your Windows Password.                                           
                                           | 3. Click the arrow to log on Windows.                                     |
| **Passcode from notification**              | 1. Select the mobile device on which the provisioned SecureAuth Authenticate app is installed.  
                                           | 2. Enter your Windows Password.                                           
                                           | 3. Click the arrow to log on Windows.                                     |
| **Approve login notification on mobile**    | 1. Select the mobile device on which the provisioned SecureAuth Authenticate app is installed.  
                                           | 2. Enter your Windows Password.                                           
                                           | 3. Click the arrow to log on Windows.                                     |
### Contact help desk for passcode

For this option:

1. Select the phone number to use for contacting the help desk.
2. Enter your Windows Password.
3. Click the arrow to log on Windows.

### Passcode from token

This method and “Timed passcode from app” are displayed at first login, if available. If not available, all available methods are displayed.

For this option:

1. If there is more than one provisioned token, select the device on which the provisioned SecureAuth passcode app is stored.
2. Enter your Windows Password.
3. Click the arrow to log on Windows.

---

### Subsequent login experience

When logging on the same machine in subsequent sessions, the Login for Windows page includes a selection of all multi-factor authentication methods for which you enrolled.

- The login screen defaults to the authentication method used in the last login session.

To show characters as you type a passcode instead of seeing dots, refer to step 3.
**Sign-in option icons | Fields | Instructions**

<table>
<thead>
<tr>
<th>Sign-in option icons</th>
<th>Fields</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Sign-in option icons" /></td>
<td><img src="image2.png" alt="Fields" /></td>
<td><strong>Answers to Security questions</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Answer both questions with your predefined answers. You must answer both questions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the arrow to log on Windows.</td>
</tr>
</tbody>
</table>
### Timed passcode from app
1. In the Enter passcode field, enter the OATH OTP from your SecureAuth One-time Passcode app.
2. Click the arrow to log on Windows.

### Contact help desk for passcode
1. Enter the passcode received by contacting the help desk.
2. Click the arrow to log on Windows.

### Approve login notification on mobile
1. Accept the login notification sent to the SecureAuth Authenticate app on your mobile device.

### Passcode from notification
1. Enter the passcode sent to the SecureAuth Authenticate app on your mobile device.
2. Click the arrow to log on Windows.

### Passcode from email
1. Enter the passcode sent to your email address.
2. Click the arrow to log on Windows.

### Passcode from voice call
1. Enter the passcode received by a voice call to your mobile phone.
2. Click the arrow to log on Windows.
Admin login experience

Login for Windows requires you to enter a multi-factor authentication method when you log in to a privileged account as an administrator (with "Run as administrator") on the same machine used to log into a regular user account. See the options by right-clicking over an executable or holding the Shift key over a short cut.

Select one of the options and then enter the admin password.
Users with access to privileged accounts are not prompted for additional MFA when logging into their normal user accounts; however, it is possible to configure UAC policies to prompt administrators for a password or MFA method when they log into their normal user accounts. See UAC - Require a Password for Administrator.

To show characters as you type a passcode instead of seeing dots, click and hold the "eye" icon to the right of the characters.

Release notes

New features and enhancements

Version: 1.0.4
Release Date: April 23, 2019
Last Updated: May 28, 2019
Compatibility: SecureAuth IdP versions 9.2 or later
Group Bypass support can be enabled for MFA on desktops and laptops for end users when they are online and offline.

End users can show characters for passcodes when logging on.

Login for Windows supports failover for up to 5 backup IdP instances.

Login for Windows requires a MFA method when logging into a privileged account as an administrator (with "Run as administrator"). By default, users with access to privileged accounts are not prompted for additional MFA when logging into normal user accounts.

Admins can set up Security Questions so users can authenticate by answering knowledge-based questions (KBQ).

Login for Windows supports YubiKey version 5.0.

Access is denied for all users on a computer if the computer is not domain-joined AND all local users are blocked by Adaptive Authentication OR are not Active Directory members on SecureAuth IdP.

Several minor one-time passcode (OTP) enhancements and fixes were completed.

Administrators can enable or disable the User Account Control (UAC) option based on how they want users to log on the environment.

Resolved issues

SMS / Voice telephone numbers are masked for registered multi-factor authentication methods.

Manual uninstallation from the "Programs and Features" menu on Windows 10 succeeds.

End users no longer need to change password at next login to keep expired passwords from failing with TOTP or HOTP. Login for Windows customers on SecureAuth IdP 9.2 or 9.3 must apply a hotfix to take advantage of this fix. (See Hotfixes.)

End users no longer receive a failure message when attempting to authenticate by using TOTP after their device wakes from sleep mode while online.

End users are no longer given a private IP address when Adaptive Authentication is used in an RDP session.

A non-local user whose account is not found in Active Directory receives on-screen guidance about how to fix and proceed.

A SecureAuth file called .saconfig is no longer created after a Login for Windows installation failure.

The last user displays only when the "multiple_user" flag is set to false.

End users connecting to Login for Windows for the first time and through an RDP connection are offered appropriate MFA options instead of an "offline MFA" message.

Adaptive "Skip to post-authentication" and "Skip two factor authentication" options no longer refuse to log on the last user on Windows 8.

If offline MFA methods are not enabled for an account and end users attempt to log in while offline, they will receive a login error message with guidance.

Login for Windows and the IdP realm clock cycles are aligned so clock skew no longer occurs between TOTP codes generated by hard and software tokens sharing the same OATH Seed.

Login for Windows accepts connections when certificates are self-signed because the value of "allow_self_signed" is no longer ignored.

When SecureAuth IdP encounters a malformed email string that lacks an at symbol (@), IdP returns the string as a Login for Windows email.

End users cannot use an OTP more than once, even if it is in a valid time range because each OATH list is assigned locally to each machine.

End users logged onto Login for Windows who use RDP to connect to the same machine will see a standard Windows "Unlock the PC" message when using the knowledge-based MFA method.
| CP-574 | After Login for Windows is first installed, end users who select the Switch User button see “Other User” once instead of twice. |
| CP-575 | End users can log on using YubiKey the first time, without receiving an error message. |
| CP-578 | Login for Windows will automatically retry a connection if it detects an offline state. Offline states can occur because of initial no-connection states, such as when a device is in sleep mode. |
| CP-594 | End users receive a better error message with guidance when attempting to log in while offline, but offline methods were not set up. |
| CP-598 | End users can successfully log in when they are members of a valid bypass group. |

### Known issues

| CP-288 | Login for Windows performance degrades when loading the login screen in the offline mode on Windows 10. |
| CP-488 | End users can log into their machines with sAMAccountName attributes only. Attributes other than sAMAccountName are not supported. |

### Hotfixes

| CP-418 | EE-1088 | End users no longer need to change password at next login to keep expired passwords from failing with TOTP or HOTP. Login for Windows customers on SecureAuth IdP 9.2 or 9.3 must apply a hotfix to take advantage of this fix. |

**Affected SecureAuth IdP Version(s):** 9.2 or 9.3

**Support Information:** Contact SecureAuth Support (support.secureauth.com, support@secureauth.com, or 1-866-859-1526) to have the latest hotfix installed on your SecureAuth IdP v9.2.x or v9.3.x appliance.

---

### New features and enhancements

| CP-459 | A warning message now appears to end users if the 'allow_self_signed' flag is enabled in config.json. |

### Resolved issues

| CP-447 | An empty screen without login functionality no longer appears after installation. |

### Known issues

<p>| CP-288 | Login for Windows performance degradation when loading the login screen in the offline mode on Windows 10. |
| CP-386 | SMS / Voice telephone numbers are not completely masked for registered multi-factor authentication methods. |
| CP-414 | User details are missing when choosing a registered user on the “Other user” login screen |</p>
<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-416</td>
<td>Manual uninstallation from the &quot;Programs and Features&quot; menu on Windows 10 results in an error.</td>
</tr>
<tr>
<td>CP-443</td>
<td>User is given a private IP address when Adaptive Authentication is used in an RDP session.</td>
</tr>
<tr>
<td>CP-447</td>
<td>Non-local user whose account is not found in Active Directory receives an empty login screen.</td>
</tr>
<tr>
<td>CP-457</td>
<td>User is blocked by Adaptive Authentication on Windows Server 2012 R2 and receives an error message if no alternate providers are configured.</td>
</tr>
<tr>
<td>CP-470</td>
<td>The last user displays even with the multiple_user flag set.</td>
</tr>
<tr>
<td>CP-472</td>
<td>Adaptive Authentication login error after Login for Windows installation on Windows 7.</td>
</tr>
</tbody>
</table>

### Resolved issues and enhancements

**Version 1.0.2 - Release Date: June 13, 2018**

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-187</td>
<td>RDP users utilizing NLA (Network Level Authentication) no longer receive a second prompt after providing credentials to the RDP client.</td>
</tr>
<tr>
<td>CP-267</td>
<td>The multi-factor authentication device order now remains consistent on subsequent login attempts.</td>
</tr>
<tr>
<td>CP-320</td>
<td>Login for Windows now remembers the most recently entered login username on a non-server.</td>
</tr>
<tr>
<td>CP-340</td>
<td>An active hover link now appears when attempting to select another multi-factor authentication method.</td>
</tr>
<tr>
<td>CP-339</td>
<td>The correct HOTP icon now appears on passcode entry window.</td>
</tr>
<tr>
<td>CP-379</td>
<td>Log details have been added to help troubleshoot common installation errors.</td>
</tr>
<tr>
<td>CP-388</td>
<td>Users in offline mode now correctly receive Multi-Factor options that are usable offline.</td>
</tr>
<tr>
<td>CP-393</td>
<td>Re-installing Login for Windows now applies configuration file updates.</td>
</tr>
<tr>
<td>CP-398</td>
<td>The installer error message for a missing configuration file has been revised for clarification.</td>
</tr>
</tbody>
</table>
First-time users must now use an OATH-based method (if enrolled in one) to ensure at least one OATH seed is cached for offline use.

The most recently used multi-factor authentication device now appears when logging on/off Windows 7 or Windows 10.

SADiag.exe no longer returns an error when ‘set logging off’ and ‘test api’ log level settings are used.

The installer now accepts a relative path to the configuration file during a silent installation.

The correct username now appears on the lock screen on Windows 7 / Windows Server 2008.

### Known issues

<table>
<thead>
<tr>
<th>CP-386</th>
<th>SMS / Voice telephone numbers are not completely masked for registered multi-factor authentication methods.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-414</td>
<td>User details are missing when choosing a registered user on the &quot;Other user&quot; login screen</td>
</tr>
<tr>
<td>CP-416</td>
<td>Manual uninstallation from the &quot;Programs and Features&quot; menu on Windows 10 results in an error.</td>
</tr>
</tbody>
</table>

### Resolved issues

- **Incorrect IP address used for Adaptive Authentication**

  When logging on locally, SecureAuth IdP now correctly uses the endpoint's public-facing IP address instead of a local adapter IP address.

  In this issue, a private IP address was being used which prevented IP-related Adaptive Authentication features from functioning properly. Remote / RDP logins were not impacted by this issue.

- **AD bad password count incorrectly incremented**

  When attempting to log on using a bad password, the bad password count now increments appropriately – i.e. one time for each login attempt.

  In this issue, the Active Directory bad password count would increment multiple times for a single login attempt, causing the user to be locked out immediately or sooner than anticipated. In certain scenarios, the bad password count incremented once for each OATH seed-based multi-factor authentication method – e.g. for each app-based OTP or hardware token.

- **Re-installation breaks login functionality**

  Login for Windows can now be re-installed on the same machine.
In this issue, the Login for Windows software could become corrupted if re-installed on a machine which already had the software installed. This issue prevented users from logging in and required the user to boot up the machine in safe mode to repair the software.

- **Non-proxy aware**

  Beta support is now available for proxies in Login for Windows – see Login for Windows Installer Configuration to configure Login for Windows 1.0.1 for use with a proxy. Note the known issues when using a proxy in the 1.0.1 release.

  This issue affected environments in which direct access to the SecureAuth IdP appliance is blocked and users must use a proxy.

- **Login failure for users with a space in sAMAccountName**

  The issue has been resolved for users who were unable to log in if a space exists in their sAMAccountName property.

- **Users in a bypass group unable to use Self-Service Password Reset function**

  The Self-Service Password Reset link now appears for users who are in a bypass group.

**Known issues**

- **Installation requires an absolute path to the configuration file**

  The installer does not accept a relative path to the configuration file, which prevents deploying the installer from a directory that cannot be defined in advance (such as when using a Group Policy).

- **Potential offline lockout for new users**

  To use the offline mode, a user must first use an OATH-based authentication method – such as a one-time code (OTP) generated by the SecureAuth Authenticate App – at least one time while online in order to cache the OATH seed used for authenticating the user. SecureAuth recommends instructing users how to enable the offline mode before they attempt to go online.

  A future release of Login for Windows will address the potential new user lockout issue by providing guidance to users during the login process.

- **Double prompting for RDP logins**

  Users utilizing NLA (Network Level Authentication) when logging on a system with RDP enabled may still be prompted for a username and password once the session is established.

- **Self-service Password Reset function is non-proxy aware**

  The Self-service Password Reset feature – which opens a browser to a Self-Service Password Reset page – does not function in environments using a proxy to access SecureAuth IdP.

  In these scenarios, contact SecureAuth Support and inquire about workarounds.

  Note this feature differs from the inline password reset feature that is used when a user’s password expires – this feature functions properly in proxy environments.

- **Self-service Password Reset may not function correctly for certain Operating Systems**
On Windows Server versions 2008 R2 and 2012 R2, users are unable to complete the self-service password reset process due to default Internet Explorer settings in the operating systems.

- Offline endpoint when proxy is unavailable

  Use of any proxy configured for Login for Windows becomes mandatory. If the proxy is unavailable, Login for Windows behaves as if it is offline.

  This issue may impact laptop users who connect their laptops to networks in which the proxy is unavailable.

- Re-installing Login for Windows does not apply configuration file updates

  Re-running the installer with a new or updated configuration file does not result in configuration changes made to the current installation. Administrators must uninstall and then re-install Login for Windows to apply the new settings.

- SMS and Voice numbers are not correctly masked

  Users prompted for multi-factor authentication can view the full telephone number for a registered multi-factor authentication method.

- Incorrect username shown on lock screen

  Users in a bypass group are shown the wrong username on a Windows 7 workstation lock screen.

Version 1.0 - Release Date: February 1, 2018

The new Login for Windows product gives end users a secure login experience on a Windows workstation, or on a remote Windows server, using a SecureAuth multi-factor authentication method. This product, with FIPS 140-2 compliant cryptographic libraries, is newly designed and engineered and replaces the Credential Provider application. After the initial setup and first-time usage, the end-user subsequently logs on without a password by just using a 2-Factor Authentication method.

Related documentation

YubiKey HOTP Device Provisioning and Multi-Factor Authentication Guide
YubiKey OATH-TOTP Device Provisioning and Multi-Factor Authentication Guide
Login for Windows configuration guide v1.0.3
Login for Mac configuration guide v1.0.3
SecureAuth Credential Provider Configuration Guide, v2.8.5
Login for Endpoints Configuration Guide v1.0.2
Login for Windows SSL configuration requirements