Login for Windows v20.03 configuration guide

Updated April 14, 2020

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, adds SecureAuth's multi-factor authentication to the Windows desktop and remote server login experience.

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

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 OATH-HOTP Device Passcode
- YubiKey OATH-TOTP Device Passcode
- YubiKey OTP Passcode (Yubico OTP protocol)
- Passcode from Help Desk
- Security Questions (knowledge-based questions and answers)
- Symbol-to-Accept
- Passwordless (as a first factor)
- Fingerprint Recognition
- Face Recognition

NOTE: Methods delivered via push notification require the use of the SecureAuth Authenticate mobile app.

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 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 third-party service
- Multiple login capability
- Endpoint identified during login multi-factor authentication request
- YubiKey HOTP and OATH-TOTP support for two-factor authentication
- YubiKey OTP Passcode (Yubico OTP protocol)
- TOTP two-factor authentication
- Passwordless (as a first factor)
- Fingerprint Recognition
- Face Recognition
- Cached user credentials, which let users sign in with fewer clicks
- Installation API validation, to ensure successful login to Login for Windows
- Adaptive Authentication
- Use a primary credential provider different from the SecureAuth credential provider
- SecureAuth Authenticate app is compliant with FIPS 140-2

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 (AD) 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; 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/OAHTToken/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.

- With the exception of the Microsoft-provided credential providers, SecureAuth does not support other third-party credential providers installed on the same computer as the Login for Windows credential provider.

- SecureAuth did not certify Windows 7 and Windows Server 2008 with Login for Windows v20.03 because Microsoft deprecated both operating systems as end-of-life. Be aware of the following:
- Login for Windows v20.03 works on Windows 7, but SecureAuth does not certify that all features are supported.
- Only Login for Windows security fixes will be released in the near future.
- SecureAuth recommends upgrading to an officially supported version of Windows.

---

**Prerequisites**

**Administrator**

- Login for Windows requires SecureAuth IdP version 9.2 or later or SecureAuth® Identity Platform version 19.07 or later
- To use biometric fingerprint and face (iOS only) recognition, Login for Windows requires SecureAuth Identity Platform v19.07 or later, using the 2019 theme (see Setting the default theme for new realms).
- To use Symbol-to-Accept through SecureAuth Authenticate mobile app, Login for Windows requires SecureAuth Identity Platform v19.07 or later.
- To use the Passwordless workflow, Login for Windows requires Windows 10 version 1607 or later OR Identity Platform version 19.07 or later running on Windows 10 version 1607
- Available to sites running the Prevent package
- To use a primary credential provider different from the SecureAuth credential provider, Login for Windows requires the following:
  - SecureAuth IdP 9.2 or later OR Identity Platform version 19.07 or later
  - Windows sites running the SecureAuth Protect or Prevent package
- If you will customize the Login for Windows experience by setting or changing configuration options, see the Login for Windows configuration options section to download a PDF with all available options.

**Setup requirements**

1. Ensure SecureAuth IdP v9.2 or later is running and is using a SHA2 or later third-party publicly trusted 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 in the SSL certificate field. The following example shows the SSL connection being terminated on the SecureAuth server.

   ![Site Bindings](image)

   Alternatively, you can also terminate the SSL connection on the load balancer, and then your publicly-trusted certificate will reside on the load balancer.

   ![Edit Site Binding](image)

   **Note**
   
   Do not remove the SecureAuth certificates from the certificates console or the SecureAuth appliance will no longer function.

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>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows OS versions:</td>
<td>• Windows 8.1 (32/64-bit)</td>
<td>• Windows Server 2012 (64-bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 10 (64-bit)</td>
<td>• Windows Server 2012 R2 (64-bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Windows Server 2016 (64-bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Windows Server 2019 (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.

**End user**

**First-time usage requirements**

End users can log in without second-factor authentication for the number of attempts set by the administrator. This allows end users to log in with a password only so they can set up their two-factor authentication methods before they must authenticate to access their device. After end users set up 2FA, the following is the authentication workflow.

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, but offline login will not be available.

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.

Additionally, consider the following requirements for end users:

- If using Passwordless as a first factor, end users must ensure the following:
  - Run Windows 10 build 1607 or later
  - Connect a fingerprint reader to the computer

- If using face recognition, available for iOS mobile phones only, end users must complete the following:
  - Enable their iOS mobile phone Face Recognition setting
  - Download and set up the SecureAuth Authenticate App
  - Sites upgrading from SecureAuth v9.2 to the Identity Platform v19.07: End users who already use the Authenticate app and want to add the ability to accept biometric push notifications to use face (iOS) or fingerprint recognition must first reconnect the account for their mobile device.

- If using fingerprint recognition, end users must complete the following:
  - Enable their iOS or Android mobile phone Fingerprint setting
  - Download and set up the SecureAuth Authenticate App
  - End users who already use the Authenticate app and want to add the ability to accept biometric push notifications to use face (iOS) or fingerprint recognition must first reconnect the account for their mobile device.

NOTE: If end users are using the SecureAuth Credential Provider and the admin upgrades to a later version of Login for Windows, end users do not need to uninstall the SecureAuth Credential Provider before installing Login for Windows.

---

**SecureAuth IdP Web Admin configuration**
Use the following sections to set up Login for Windows with SecureAuth IdP version 9.2 or 9.3.

If your team will set up and use Login for Windows with the cloud or hybrid model of SecureAuth Identity Platform version 19.07 or later, see SecureAuth Identity Platform configuration.

Data tab

Do not use the same realm for SecureAuth RADIUS server and Login for Windows because the OTPFieldMapping app key in web.config is used differently in the two products.

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.

In the Profile Fields section, enter adminDescription in an unused Aux ID field—Aux ID 3 in this example—and make the field Writable.

4. 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.
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. Save the changes.

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:

1. Threat Service
2. IP whitelist / blacklist
3. Geo-location (redirect option not available)
4. Geo-velocity (redirect option not available)
5. User / Group (redirect option not available)

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

1. In the Multi-Factor Configuration section, configure the multi-factor authentication methods you want enabled.
2. Save the changes.
## Multi-Factor Configuration

### Phone Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Field 1</td>
<td>One-Time Passcode via Phone</td>
</tr>
<tr>
<td>Phone Field 2</td>
<td>One-Time Passcode via Phone</td>
</tr>
<tr>
<td>Phone Field 3</td>
<td>Disabled</td>
</tr>
<tr>
<td>Phone Field 4</td>
<td>Disabled</td>
</tr>
<tr>
<td>Phone/SMS Selected</td>
<td>Voice</td>
</tr>
<tr>
<td>Phone/SMS Visible</td>
<td>True</td>
</tr>
</tbody>
</table>

### 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 for each user
- 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

1. Open the web.config file, located at D:\SecureAuth\SecureAuth1 on the appliance, and decrypt the web.config file.
2. 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.

3. Save the changes.

API tab
1. In the API Key section, click **Generate Credentials**.

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

   ![API Key Section](image)

2. In the API Permissions section, select **Enable Authentication API**.

   **NOTE:** It is not recommended to enable **Identity Management** options because the password reset function does not use the Identity Management API. The password reset function uses an IdP realm or third party password reset URL.

   ![API Permissions Section](image)

3. Click **Save** once the configuration is complete.

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

---

**SecureAuth Identity Platform configuration**

Use the following sections to set up Login for Windows with the cloud and hybrid model of SecureAuth Identity Platform version 19.07 or later.

If your team will set up and use Login for Windows with SecureAuth IdP version 9.2 or 9.3, see **SecureAuth IdP Web Admin configuration**.

You will configure the Identity Platform and the Classic IdP Experience to use Login for Windows. If your team wants to use biometric identification (face (iOS only) or fingerprint recognition), you must complete the following set up. Only the Identity Platform v19.07 or later supports biometric identification; additionally, you must use the 2019 theme (see **Setting the default theme for new realms**). You will set up the authentication API in the Classic IdP Experience; this is necessary until feature parity is achieved with the Identity Platform.

**Prerequisites**

The following steps must be completed before you can set up MFA methods; some steps are specific to cloud and they are called out accordingly. Most active sites will have performed the first two steps already and can begin at "Set up a policy."

1. **Cloud:** Download and install the SecureAuth Connector on your Windows data store server to begin the Identity Platform deployment.

   See **Data Stores** for a discussion and prerequisites. See **Install the SecureAuth Connector** for prerequisites and steps.

2. Add a data store.

   See **Add an Active Directory data store** or **Add a SQL Server data store** for steps.
In Map Data Store Properties, enter **adminDescription** in an unused ID field—**Aux ID 3** for endpoints—and set the data format to **plain text**. Later in these steps, you will map this field to the OTP Validation Property, which is used for end user authentication.

**Set up a policy**

Policies in the Identity Platform allow you to define rules to authenticate and block your users to certain applications. See [How policies are used in the Identity Platform](#) to learn about policies.

If you have an existing policy or default policy that will meet your security needs, you can use that policy; otherwise, you can set up a new policy specifically for endpoints.

1. **Set up a policy for Login for Windows.**

   On the left side of the Identity Platform page, click **Policies**. Click **Add New Policy** and give the policy a name. Add a minimum of two authentication rules.

2. **Select the MFA methods that you want to enable for the new Login for Windows policy that you created in the previous step.** The MFA methods will be available to your end users as their end user login workflow experience.
Open the policy you created in the previous step and select the **Multi-Factor Methods** tab. Define the login workflow and multi-factor methods settings for the policy and **save** the choices. The following image shows the available MFA methods available in Login for Windows.

3. Optional: Set up rules to prompt or skip MFA when end users authenticate by comparing rules like their country, group access, and more.

On the policy page, select the **Authentication Rules** tab. See [Adaptive authentication rules settings in a policy](#) to learn more about setting rules.
If you make changes, be sure to save the changes.

**Authentication Rules**

Configure your adaptive authentication policy by combining and ordering rules. Rules are honored from top to bottom.

If you make changes, be sure to save the changes.

**Blocking Rules**

Configure blocking rules to ensure security for your resources

4. Optional: Set up rules to evaluate behaviors that will cause an end user to be blocked from authenticating in, such as IP range, group access, and more.

On the policy page, select the **Blocking Rules** tab. See **Blocking rules settings in a policy** to learn more about rules.

If you make changes, be sure to save the changes.

**Blocking Rules**

Configure blocking rules to ensure security for your resources

5. Save the policy.

**Add an application**

Use the Application Manager tool to select an application template from over 500 applications in the library, then use the common components to customize each new application integration. See **Application Manager overview** to learn more.

1. Add a Security Assertion Markup Language (SAML) application. Later, you will edit the SAML application in the Classic IdP Experience to work with Login for Windows.

On the left side of the Identity Platform page, click **Application Manager** and then click **Add an Application**. On the list of applications, select **SAML Application**.

2. On the Application Details screen, set up the application to be used by endpoints products, such as Login for Windows.
3. On the Connections Settings screen, under IdP Signing Certificate, click Select Certificate. Select an IdP signing certificate. (You do not need to set up anything else on the page. You are setting up a realm to add endpoints options in the Classic IdP Experience.)

The IdP-initiated signing certificate integrates the SAML application with IdP so that the login process starts at the Identity Platform.

After end users successfully authenticate, they are asserted back to the Login for Windows application.

4. Add the application.

On the Connections Settings screen, at the bottom, click Add Application. You will receive a success message when the application is added.
5. Check the Information for Service Providers screen to ensure the information is correct, and then click **Continue to Summary**.

6. Check the summary information. If you need to edit, click the pencil icon to the right of the field to be edited. Be sure to click **Update Settings** in each screen that you change.

**API**

Set up the authentication API in the Classic IdP Experience.

1. Open the Classic IdP Experience.

   On the Identity Platform page, click the **Admin** pull-down menu and select **Go to Classic Experience**.

2. Search for the endpoints application you created previously.
3. Select the application you created previously.

4. Generate API credentials.

   In the Admin Overview page, click the API tab on the top menu bar.

   The Application ID and Application Key are required and used in the config.json file for all scenarios using Login for Windows. The Identity Platform contains an endpoints API; the config.json file calls the Identity Platform endpoints API.

   On the top section, API Key, click Generate Credentials.

5. Set up the authentication API for Login for Windows. In the API Permissions section, complete the following:
   a. Select Enable Authentication API.
   b. Add Aux ID 3 to the OTP Validation Property to map it to the setting you completed in Map Data Store Properties.
      You must specify an auxiliary ID (AUX ID) to communicate with the Identity Platform to validate one-time passcodes (OTPs) from email, phone calls, SMS, Helpdesk, and Notification Passcode.
c. Select Enable Login for Endpoints API, and then click Configure Login for Endpoints Installer.

6. Click Save, located on the left side of the page, at the bottom.

Login for Windows Installer Configuration

1. On the Login for Endpoints Installer Configuration page, select Windows as the Endpoint Operating System.
2. Select the Endpoint Type to specify that either a single user or multiple users can log on the device.
   - Single user: The last user logged into the endpoint login screen is remembered and does not need to log in again.
   - Multiple users: Each user must enter their username to log in.
   
   NOTE: For the single user selection, after the user has successfully logged on the endpoint online, thereafter the user can log on the endpoint when offline without an Internet connection.
3. Enter the IdP Hostname.
4. 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.
5. If any user group is allowed to bypass multi-factor authentication, enable the bypass option and list the user groups.
5. **Select Users are a member of the following groups.** Add the user groups in the fill-in field.

![Multi-Factor Authentication Settings](image)

6. Alternatively, you can add groups manually by adding the group_bypass key to the config.json file, described in **Optional: Add groups that can bypass MFA**.

**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 Active Directory (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 AD is unreachable.

* Users who need to log in without being prompted for additional MFA must belong to a local or domain group that is set up in the bypass option. Add local users only to the local group.

* 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. A "proxy_server" can be configured on the Windows OS, but if present as a root parameter in the config.json file, takes precedence over the OS setting. The format to configure the proxy is: "http://[user[:password]@[]host[:port]]" Parameters surrounded by [ ] are optional. Both "user" and "password" are not supported on HTTP clients on Login for Windows version 19.06 and earlier, or on 19.09.xx or later that choose to use the legacy HTTP client by setting "legacy_http_communication": true in the config.json file.

B. The "proxy_bypass" is a semicolon-separated list of server names or IP addresses to be excluded from proxy usage, for example: ".acme.sec;.lore.sec;.acme-ppi.com;10...;192.168." Each item in the list must be one of the following:

* Fully-qualified domain name (FQDN)
* Full IP address
* Partial IP address with the following forms: Class A example = 10.* or Class B example = .16. or Class C example = .168.*
* Sub-domain name of a parent domain, where the parent is ".parent.domain.name" The following is an example of a domain that uses direct communication with mail.google.com, but does not communicate with google.com itself: *.google.com

C. Windows proxy configuration. See the [Netsh.exe and ProxyCfg.exe Proxy Configuration Tools](#) article on the Microsoft website.

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

7. **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 to 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 to use Login for Windows.

8. 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.
Pre-installation steps

Use the following settings to customize the Login for Windows experience.

Verify "allow_self_signed" setting

Setting "allow_self_signed" to true should be used only in test or lab environments where the server has a self-signed certificate.

- When set to false, only valid certificates are accepted.
- When set to true, all certificate validations will be turned off. The HTTP client then will accept valid certificates, self-signed certificates, expired certificates, certificates with invalid root certificates without matching common names, etc. to establish communication.

Do not set this key to true in a production environment. In production, the key 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. If the key is set to true in production, the following warning message is displayed: Warning! 'allow_self_signed' is enabled.

Find the config.json file you downloaded in step 8 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 Windows is uninstalled and then re-installed 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 8 of the Web Admin Configuration section of this document and edit it. Find the "version" key and set it to v2, as follows:

"version": "v2",

Login for Windows configuration options

Download the following PDF document, which contains a table of all configuration options for Login for Windows. Be sure to check the configuration version listed under "conf_version," to ensure that the optional settings you want to use are supported. Login for Windows supports three configuration versions; the conf_version value (either 1, 2, or 3) defines the config.json file.

The options supported are listed in the following table. Save the PDF to a folder of your choice by right-clicking over the image and selecting Save link as.

Optional: Set end user access level

Compatible with: conf_version 1 and later

Login for Windows requires the end user to use multi-factor authentication by default to access the local console or remote console in a Remote Desktop protocol (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 8 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 only for Self-service Password Reset (SSPR) where SecureAuth is the primary credential provider.

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.

4 = Use a primary credential provider different from the SecureAuth credential provider. This setting is also used for SSPR, where end users can update their password by clicking the Password Reset icon:

   Login for Windows is the password reset credential provider.

3. Save the configuration.

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

Compatible with: conf_version 2 and later

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 8 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: Add groups that can bypass MFA
Compatible with: conf_version 1 and later

Users who need to log in as local admins without being prompted for additional MFA must belong to a local or domain group that is set up in the config.json file, in the “group_bypass” key. Add local users only to the local group. Users in this group must including a warning stating the group names are case sensitive and need to match AD exactly.

Find the config.json file you downloaded in step 8 of the Web Admin Configuration section of this document and edit it. Add the "group_bypass" key and set it as follows:

"group_bypass" can include the following:

- group name: For groups of the domain on which the machine is joined; for example, "BypassGroup"
  Note that group names must match Active Directory exactly.
- domain\\groupname: For groups that are part of a specific domain; for example, "customerDomain\\BypassGroup"
- .\\groupname: For local machine groups; for example, "\.\ Administrators"

You can also set up bypass groups in the SecureAuth IdP API page, in the Multi-Factor Authentication Settings section, described in step 5.

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

Compatible with: conf_version 2 and later

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.

See How User Account Control works on the Microsoft website to learn more about UAC.

Find the config.json file you downloaded in step 8 of the Web Admin Configuration section of this document and edit it. Add the "enabled_on_uac" key and set it to true or false, as follows:

"enabled_on_uac": true
"enabled_on_uac": false
Optional: Disable Adaptive login

Compatible with: conf_version 2 and later

The adaptive_enabled key is set to true by default so that administrators can install and modify Login for Windows. Disable this key to false to ensure that an admin or other user is never restricted. This key acts similar to Adaptive Authentication settings in SecureAuth IdP, where you can restrict admins and users from logging in in several ways, for example, by username, group, IP, etc.

- If the option is not set or removed, the default behavior is the same as if it were set to true.

Find the config.json file you downloaded in step 8 of the Web Admin Configuration section of this document and edit it. Add the "adaptive_enabled" key and set it to false or reset it to true, as follows:

```
"adaptive_enabled": false
"adaptive_enabled": true
```
Compatible with: conf_version 2 and later

SecureAuth uses OATH seeds to validate OTPs when end users log in. Most use cases require SecureAuth to store OATH seeds; if seeds are not stored, end users will not be able to log in while offline. In a scenario where, for example, a server is always online, you might not want to cache the OATH seed, to prevent the seed from leaking or being stolen.

Use the store_seeds key in the config.json file to disable the OATH seed cache, and Login for Windows will not store OATH seeds. The first-time login experience is disabled in this scenario because it is used to store OATH seeds, which are not required for this option.

- The option is true by default.
- If the option is removed, the default behavior is the same as if it were set to true.

Find the config.json file you downloaded in step 8 of the Web Admin Configuration section of this document and edit it. Add the "store_seeds" key and leave it true or set it to false, as follows:

```
"store_seeds": true
"store_seeds": false
```

Optional: Enable custom message for end users locked out

Compatible with: conf_version 2 and later

Enable this option so that end users receive customized assistance when they are locked out of their accounts or their password or passcode is incorrect or expires. Administrators can set a custom assistance string in the config.json file to guide end users so they have next steps after an issue occurs during login.

- The option must be added manually.
- If the option is not added, an error message will be displayed.

Find the config.json file you downloaded in step 8 of the Web Admin Configuration section of this document and edit it. Add the "custom_error_message" key and enter your custom assistance message. The following message is an example:

```
"custom_error_message": "For assistance, please contact Acme helpdesk at 949-555-1212, help@acmeco.com, or https://helpdesk.acmeco.com."
```

```json
{
    "access_level": 0,
    "alternate_providers": [ "{}" ],
    "apis": [ {
        "host": "https://localhost.gosecureauth.com/secureauth3",
        "id": "",
        "secret": "",
        "enabled_on_uac": false,
        "idm_sspr_label": "Password Reset",
        "idm_sspr_url": "https://localhost.gosecureauth.com/secureauth2",
        "multiple_user": false,
        "platform": "windows",
        "type": "idp",
        "conf_version": 2,
        "version": "v2",
        "adaptive_enabled": true,
        "store_seeds": true
    }
},
```
Optional: Set time period between authentication and next MFA log in

Compatible with: conf_version 2 and later

Set this option to establish the time period between end user authentication and the next MFA log in. Administrators can set a custom duration by adding "bypass_interval" in the config.json file.

- The option must be added manually.
- The time period is set in seconds. Entering 0 (zero) as the time period disables the option.
- If the option is not added, end users must authenticate in after each screen lock.
- When the option is set, end users must authenticate in after a screen lock that exceeds the defined time period. For example, if the time period is set for 3600 seconds (one hour) and an end user locks the screen and goes to lunch for an hour and 15 minutes, that end user must authenticate in after returning from lunch.
- After end users initially log in or unlock their screen with appropriate MFA, the session time period is reset to the defined "bypass_interval."

Find the config.json file you downloaded in step 8 of the Web Admin Configuration section of this document and edit it. Add the "bypass_interval" key and enter your custom time period. The following time period is an example:

*bypass_interval": 3600

Optional: Hide button to retry connection when Login for Windows offline

Compatible with: conf_version 3 and later

Set this option to hide the button to retry the connection on the login screen when Login for Windows is offline. Administrators can add the "hide_retry_option" key in the config.json file.
Find the config.json file you downloaded in step 8 of the Web Admin Configuration section of this document and edit it. Add the "hide_retry_option" key and hide the retry button, as in the following example:

```
"hide_retry_option": false
```

Optional: Set passwordless authentication

Compatible with: conf_version 3 and later

Set the "passwordless_enabled" key in the config.json file to enable or disable passwordless authentication as a first factor. End users can use a fingerprint reader to authenticate by using any enrolled fingerprint. (This setting does not enable the second factor biometric identification available to end users through the SecureAuth Authenticate app. See Use fingerprint recognition on mobile for instructions.)

- The option must be added manually.
- The option is false by default.
- If the option is removed, the default behavior is the same as if it were set to false.
- Passwordless as a first factor is available for Windows 10 users only; if the key is set to true for a different OS, the setting will have no effect.

Find the config.json file you downloaded in step 8 of the Web Admin Configuration section of this document and edit it. Add the "store_seeds" key and leave it true or set it to false, as follows:

```
"passwordless_enabled": true
"passwordless_enabled": false
```

Optional: Configure number of password-only login attempts

Compatible with: conf_version 4 and later

Set this option to establish the number of password-only login attempts that end users are allowed. Administrators can set a custom number of attempts in "login_attempts" in the config.json file. After end users set up their second-factor methods, they can dismiss the password-only login screen.
• The option must be added manually.
• The login_attempts value can be any rational number; there is no maximum. Entering 0 (zero) disables the option.
• If the option is not added, end users must always authenticate with 2FA.
• Invalid login attempts are not counted; if end users mistype a password, the number of login attempts is not decremented.
• If end users accidentally indicate that they are ready to authenticate with 2FA but they are not, they can move back into the workflow to log in with password only.
• After end users set up 2FA, they must indicate on the UI that they no longer need to log in with a password only; otherwise, they are presented with the password-only login screen until they dismiss it permanently or reach the maximum number of password-only login attempts set by the admin.

Login is determined in the following order:

1. Adaptive authentication: If set in SecureAuth IdP to block an end user, the end user cannot log in regardless of how many login_attempts are set.
2. Local settings: Checks, such as access_level and bypass_interval, are considered.
3. login_attempts: If set, the number of login_attempts are considered next.
4. group_bypass and any second factor: These login settings are considered last.

If any of the settings change, for example, an adaptive rule is changed or users no longer belong to a bypass group, end users automatically receive a 3 minute time period to enter their password. After 3 minutes, a message stating, Password logon attempt timed out, is displayed. End users are then redirected to the 2FA login screen.

Find the config.json file you downloaded in step 8 of the Web Admin Configuration section of this document and edit it. Add the "login attempts" key and enter the number of password-only login attempts. The following attempt number is an example:

```
"login_attempts": 3
```

```json
{
   "access_level": 0,
   "adaptive_enabled": true,
   "apis": [
      {
         "host": "https://endpoint01.gosecureauth.com/SecureAuth19",
         "id": "",
         "secret": "",
      
      },
   "bypass_interval": 0,
   "conf_version": 4,
   "login_attempts": 3,
   "custom_error_message": "",
   "enabled_on_uac": true,
}
```

Read about how this setting impacts end users in First login with password only.

---

Installation and upgrade steps

The following sections describe how to upgrade and install Login for Windows.

Upgrade Login for Windows

Login for Windows supports upgrading from version 1.0.4 to 20.03.xx without uninstalling before installing the latest version.

• Upgrading from version 1.0.3 to 20.03.00 is supported but the cache is cleared. After the upgrade, the first available second factor will be selected by default instead of the previous second factor the user entered.
- Upgrading from 1.0.2 or earlier, first uninstall Login for Windows before installing 20.03.xx. Upgrading from earlier than 1.0.2 to 20.03.00 is not supported.

- If end users are using the SecureAuth Credential Provider and the admin upgrades to a later version of Login for Windows, end users do not need to uninstall the SecureAuth Credential Provider before installing Login for Windows.

### 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-20.03.00-x64.msi or SecureAuthLogin-20.03.00-x86.msi. Place the file in the Temp folder.

### Install Login for Windows

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

1. Find the config.json file which you downloaded in step 8 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-20.03.00-x64.msi" /L*V "C:\Temp\install.log" /qn CONFIG="C:\Temp\config.20.03.00.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:

SecureAuth Login for Windows 20.03.00 (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)

### Login for Windows error logs

Error logs are displayed in the following locations.

- Information related to installation is written in the `install.log` file:
  ```
  %temp%\install.log
  ```
- Information related to logging in is written in the `login.log` file
  ```
  C:\ProgramData\SecureAuth\login.log
  ```

The `login.log` log file displays system information, such as the type and version of the operating system, the version of Login for Windows your organization is running, and more as shown in the following image:
After you view the `login.log` file, then connect later through RDP, you might notice what look like inconsistencies because the log file will have new start lines and threads. This is expected behavior because connecting through RDP causes new instances of the credential provider to be created, which causes the new start lines and threads.

**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.

---

**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 version 2012 R2, users are unable to complete the self-service password reset process due to default Internet Explorer settings in the operating systems.

**First login with password only**

End users can log in without second-factor authentication for the number of attempts set by the administrator in the config.json file, in the `login_attempts` value. This allows end users to log in with a password only (without using second-factor authentication), and typically occurs after the Login for Windows installation. End users can then access their device to set up their two-factor authentication methods, such as PIN creation and answers to Security Questions, before they must authenticate to access their device.

**Use case:** Password-only login is especially useful for one or more new employees who have been issued a laptop on their first day of employment. For example, if Login for Windows is already installed on the laptops and the admin has not set a "login_attempts" value, new employees might not be able to log in to their computer if they cannot connect to the SecureAuth IdP realm to register their mobile phone or self-service page to enter a phone number.

**Workflow:** End users are prompted to log in with their username and password only. The login screen indicates how many password-only login attempts remain, as shown in the following image. Using the image as an example, end users who want to log in with password only enter their password in the field next to number 1. After end users set up their second-factor methods, they are ready to authenticate so they click the message next to number 2, which dismisses the password-only screen and opens the 2FA login screen. Thereafter, the 2FA login screen opens for end users.
First-time login experience

1. Enter your username on the Windows login screen.

To authenticate by using a different primary credential provider, proceed to instructions for logging in when using a different primary credential provider.

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.

If the end users need to login when their machine is offline, they must choose an OATH-based method during the first login. After end users select a timed authentication option and enter their password, TOTP and HOTP passcode options will be available for them to use when logging on the machine offline.

End users with more than one mobile phone or YubiKey provisioned can select which device or token to use when online. When logging on the machine offline, any OATH-based method that was used online will be available for use.
If you do not have an authentication method that provides a timed passcode, then select any other option available to you.

End users who already use the Authenticate app and want to add the ability to accept biometric push notifications to use face (iOS) or fingerprint recognition must first reconnect the account for their mobile device.

You can provision either "Approve login" or "Symbol-to-Accept." The following image shows the login screen with the "Approve login notification on mobile" option; if "Symbol-to-Accept" is set, end users will see the "Passcode from Symbol-to-Accept" option in place of the "Approve login notification on mobile" option on the login dropdown. (On the SecureAuth Authenticate mobile app, the icons will be different, but both icons will have a tool tip that reads "Approve login").

If you are authenticating through a different primary credential provider (that is, not the SecureAuth credential provider), you will see the login screen offered by that credential provider. The different primary credential provider supports offline mode, for end users who need to login when their machine is offline.

The following image shows an example of a login screen, but yours will look different.
1. Sign in.

The image shows two sign-in options, a Microsoft credential provider (the key icon) and a Microsoft Smart Card credential provider (the card icon). To sign in, you could click the icon with your preferred method. If your site offers one kind of sign-in option, then only that option will be displayed for you to sign in with.

Additionally, if you can sign in as "Other user", a multi-user credential login provided by that credential provider will be displayed. After specifying who you are, click the **Sign-in options** link to choose which multi-user credential you want to use to sign in.

b. You have completed your authentication login process. You can disregard the remaining end user steps in this section and in "Subsequent login experience." Your login experience will remain the same as the one provided by your primary credential provider.

c. Notice the placement of the Password Reset icon on the lower left. To update your password, click the icon. Login for Windows is the password reset credential provider, and requires online network access.

2. 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>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Timed passcode from app</strong></td>
</tr>
</tbody>
</table>

This method and "Passcode from token" are displayed at first login, if available. If not available, all available methods are displayed.

1. Log on Login for Windows with your Windows password.
2. If there is more than one provisioned OATH OTP app, select the device.

   If you have enrolled more than one device to accept OATH OTP passcodes, select the device to send the passcode to.
3. Click the arrow to log on Windows.

<table>
<thead>
<tr>
<th>Instructions</th>
</tr>
</thead>
</table>

| Passcode from voice call |

1. Log on Login for Windows with your Windows password.
2. Select the phone number if more than one mobile phone is included in your user profile.
3. Click the arrow to log on Windows.

Passcode from SMS / text
1. Log on Login for Windows with your Windows password.
2. Select the phone number if more than one mobile phone is included in your user profile.
3. Click the arrow to log on Windows.

Passcode from email
1. Log on Login for Windows with your Windows password.
2. Select the email address if more than one address is included in your user profile.
3. Click the arrow to log on Windows.

Passcode from notification
1. Log on Login for Windows with your Windows password.
2. Select the mobile device on which the provisioned SecureAuth Authenticate app is installed.
3. Click the arrow to log on Windows.

Approve login notification on mobile
1. Log on Login for Windows with your Windows password.
2. Select the mobile device on which the provisioned SecureAuth Authenticate app is installed.
3. Click the arrow to log on Windows.

Contact help desk for passcode
Log on Login for Windows with your Windows password.
Select the phone number to use for contacting the help desk.
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.

1. Log on Login for Windows with your Windows password.
2. If there is more than one provisioned token, select the device on which the provisioned SecureAuth passcode app is stored.
   If you have enrolled more than one token to accept passcodes, select the token to send the passcode to.
   To find your YubiKey version, see **Identifying Your YubiKey** on the Yubico website.
3. Click the arrow to log on Windows.

**Passcode from YubiKey**
This method and "Timed passcode from app" are displayed at first login, if available. If not available, all available methods are displayed.

1. Log on Login for Windows with your Windows password.
2. Plug in the YubiKey and tap it to receive a passcode from the device.
   If offline, end users can choose an OATH-based method they used when online.
3. Click the arrow to log on Windows.

**Use passwordless as first factor**
This method and "Timed passcode from app" are displayed at first login, if available. If not available, all available methods are displayed.

End users must have a fingerprint reader installed on their computer and must enroll at least one fingerprint to use passwordless as a first factor.

For this option:

1. Log on Login for Windows with your Windows password.
   If offline, end users can choose an OATH-based method they used when online.
2. The SecureAuth Fingerprint Recognition Setup screen opens so end users can enroll the fingerprints they want to use.
   Thereafter, to add or remove fingerprints, open the enrollment app: Start menu > SecureAuth > Fingerprint Enrollment
   Instructions for enrolling fingerprints is in the SecureAuth Onboarding Toolkit, in the SecureAuth End User Experience document.
3. Log out.
4. Log on Login for Windows with a password.
5. In subsequent logins, end users can use an enrolled fingerprint (without a password) to authenticate.

End users with external fingerprint readers should not disconnect the reader from their computer before logging out; doing so will cause an error to be displayed: **Fingerprint data not found**. The error is an "unknown identity" signal that the reader sends to the driver; however, the fingerprint data will be found when the reader is connected to the same computer.

---

### Use fingerprint recognition on mobile

End users must use the Authenticate mobile app to use fingerprint recognition. For this option:

1. Log on Login for Windows with your Windows password.
2. Select the mobile phone on which the provisioned SecureAuth Authenticate app is installed to send a request to the mobile app.
3. Provide a fingerprint on the SecureAuth mobile app to approve the request.
4. Login for Windows receives the fingerprint information and you are authenticated.
5. Click the arrow to log on Windows.

### Use face recognition on mobile

End users must use the Authenticate mobile app to use face recognition. This option is available to users on iOS mobile phones. For this option:

1. Log on Login for Windows with your Windows password.
2. Select the mobile device on which the provisioned SecureAuth Authenticate mobile app is installed to send a request to the mobile app.
3. Show your face on the SecureAuth mobile app to approve the request.
4. Login for Windows receives the face information and you are authenticated.
5. 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.

You can provision either "Approve login" or "Symbol-to-Accept. The following image shows the login screen with the "Approve login" icon; if "Symbol-to-Accept" is set, end users will see the "Symbol-to-Accept" icon in place of the "Approve login" icon on the login screen. (On the SecureAuth Authenticate mobile app, the icons will be different, but both icons will have a tool tip that reads "Approve login").
### Answers to Security questions

1. Answer both questions with your predefined answers. You must answer both questions.
2. Click the arrow to log on Windows.

### Timed passcode from app

1. Log on Login for Windows with a password.
2. In the Enter passcode field, enter the OATH OTP from
Multiple user credential:

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.

Passcode from SMS / text
1. Enter the passcode sent via SMS to your mobile phone.
2. Click the arrow to log on Windows.

Passcode from Symbol-to-Accept
End users must use the Authenticate mobile app to receive symbols.
1. Receive the set of 4 symbols sent to the Authenticate mobile app on your mobile device.
2. One symbol will display on your Windows desktop or laptop.
3. On the Authenticate mobile app, tap the symbol that matches the one displayed on your desktop or laptop.

Passcode from token
1. Log on with your Windows password.
2. Plug in the token and tap or press it to receive a passcode from the device.

If online, end users with multiple tokens enrolled can choose any MFA method available, including multiple tokens. (End users with multiple provisioned tokens will have the extra step of selecting the appropriate token.)

If offline, end users can choose an OATH-based
<table>
<thead>
<tr>
<th>Multiple user credential:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Passcode from YubiKey</strong></td>
</tr>
<tr>
<td>1. Log on Login for Windows with your Windows password.</td>
</tr>
<tr>
<td>2. Plug in the YubiKey and tap it to receive a passcode from the device.</td>
</tr>
<tr>
<td>If offline, end users can choose an OATH-based method they used when online.</td>
</tr>
<tr>
<td>3. Click the arrow to log on Windows.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Single user credential:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use fingerprint recognition on mobile</strong></td>
</tr>
<tr>
<td>End users must use the Authenticate mobile app to use fingerprint recognition.</td>
</tr>
<tr>
<td>1. Log on Login for Windows with your Windows password.</td>
</tr>
<tr>
<td>2. Select the mobile phone on which the provisioned SecureAuth Authenticate app is installed to send a request to the mobile app.</td>
</tr>
<tr>
<td>3. Provide a fingerprint on the SecureAuth mobile app to approve the request.</td>
</tr>
<tr>
<td>4. Login for Windows receives the fingerprint information and you are authenticated.</td>
</tr>
<tr>
<td>5. Click the arrow to log on Windows.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Multiple user credential:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use face recognition on mobile</strong></td>
</tr>
<tr>
<td>End users must use the Authenticate mobile app to use fingerprint recognition. This option is available to users on iOS mobile phones.</td>
</tr>
</tbody>
</table>
Multiple user credential:

1. Log on Login for Windows with your Windows password.
2. Select the mobile device on which the provisioned SecureAuth Authenticate mobile app is installed to send a request to the mobile app.
3. Show your face on the SecureAuth mobile app to approve the request.
4. Login for Windows receives the face information and you are authenticated.
5. 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.

Select one of the options and then enter the admin password.
Release notes

New features and enhancements

Version: 20.03
Release Date: April 14, 2020
Compatibility: SecureAuth IdP v9.2.x or later, and the SecureAuth Identity Platform v19.07 or later. Additionally, biometric fingerprint and face (iOS only) recognition require SecureAuth Identity Platform v19.07 or later, using the 2019 theme.

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 password or MFA 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.
If the "login_attempts" attribute is set in conf_version 4 in the config.json file, end users are allowed to log in with a password only for a set number of times. This enables end users to have time to set up their 2FA methods, such as PIN creation and answers to Security Questions, before they must authenticate to access their device.

If any settings that determine login are changed, for example, an adaptive rule is changed or users no longer belong to a bypass group, end users automatically receive a 3 minute time period to enter their password.

When end users click the "Click to update your password" link on the login screen, they are directed to a Login for Windows SSPR login screen that opens in a modern browser, Chromium version 79.1.36, and not in Internet Explorer.

Improvements to login performance were completed.

The installation version number now matches the public version release value; for example, if the public product version is 20.03.01, then the installation version number, which is visible if you uninstall Login for Windows manually, is also 20.03.01. (In previous versions of Login for Windows, the versions were different, but now they match.)

The error log displays system information, such as the type and version of the operating system, the version of Login for Windows your organization is running, and more.

Resolved issues

**Fingerprint recognition works correctly when an administrator is running in Run as administrator mode.**

**Login for Windows SSL certificate hostname validation works correctly with a SecureAuth IdP configured for Login for Windows.**

**End users assigned a recently created YubiKey can log in to Login for Windows on the first attempt, even if they have not previously logged in to SecureAuth IdP with the YubiKey.**

**Sites using MFA throttling are no longer locked out of their accounts after successful logins.**

Known issues

**End users with external fingerprint readers should not disconnect the reader from their computer before logging out; doing so will cause an error to be displayed:** **Fingerprint data not found.** The error is an "unknown identity" signal that the reader sends to the driver; however, the fingerprint data will be found when the reader is connected to the same computer.

The fingerprint feature works as designed. When the reader is disconnected and sends the "unknown identity" signal, the code does not differentiate between the signal and an unrecognized finger touch.

The error log will have new start lines and threads if connecting through RDP; RDP connections cause new instances of the credential provider to be created, which causes the new start lines and threads.

When upgrading to the Identity Platform v19.07 or later, admins must use the 2019 theme and end users who already use the SecureAuth Authenticate app must reconnect their accounts to add the ability to accept biometric push notifications to use face (iOS) or fingerprint recognition through the mobile app.

**Workaround:** None

Version 19.09.03 - Release Date: February 4, 2020
Resolved issue

| CP-837 | Login for Windows accepts only a valid certificate with a hostname that matches the hostname for the connected SecureAuth IdP URL configured for Login for Windows.

Known issue

| TW-926 | When upgrading to the Identity Platform v19.07 or later, admins must use the 2019 theme and end users who already use the SecureAuth Authenticate app must reconnect their accounts to add the ability to accept biometric push notifications to use face (iOS) or fingerprint recognition through the mobile app.

Workaround: None

Version 19.09.02 - Release Date: December 10, 2019

Resolved issue

Version: 19.09.02
Release Date: December 10, 2019
Compatibility: SecureAuth IdP v9.2.x or later, and the SecureAuth Identity Platform v19.07 or later

| CP-797 | Organizations that chain realms with Login for Windows before showing a self-service password reset page (SSPR) now see the second multi-factor authentication page correctly.

Known issue

| TW-926 | When upgrading to the Identity Platform v19.07 or later, admins must use the 2019 theme and end users who already use the SecureAuth Authenticate app must reconnect their accounts to add the ability to accept biometric push notifications to use face (iOS) or fingerprint recognition through the mobile app.

Workaround: None

Version 19.09.01 - Release Date: November 5, 2019

New features and enhancements

Version: 19.09.01
Release Date: November 5, 2019
Compatibility: SecureAuth IdP v9.2.x and later, and the SecureAuth Identity Platform v19.07 and later. Additionally, biometric fingerprint and face (iOS only) recognition require SecureAuth Identity Platform v19.07 or later, using the 2019 theme.
Windows administrators can change the user access level to 4, which then uses a different primary credential provider. This setting is also used for SSPR, where end users can click the Password Reset icon to update their password. Windows sites must be running the SecureAuth Protect or Prevent package to use this option.

Resolved issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-773</td>
<td>Passwordless authentication as a first factor succeeds on Windows Hello.</td>
</tr>
<tr>
<td>CP-779</td>
<td>After end users log in, the mouse cursor works correctly.</td>
</tr>
</tbody>
</table>

Known issue

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TW-926</td>
<td>When upgrading to the Identity Platform v19.07 or later, admins must use the 2019 theme and end users who already use the SecureAuth Authenticate app must reconnect their accounts to add the ability to accept biometric push notifications to use face (iOS) or fingerprint recognition through the mobile app.</td>
</tr>
<tr>
<td></td>
<td>Workaround: None</td>
</tr>
</tbody>
</table>

New features and enhancements

Version: 19.09
Release Date: October 8, 2019

Compatibility: SecureAuth IdP v9.2.x and v9.3.x and the SecureAuth Identity Platform v19.07. Additionally, consider the compatibility for the following features:

- Biometric fingerprint and face (iOS only) recognition and Symbol-to-Accept through SecureAuth Authenticate mobile app are compatible with SecureAuth Identity Platform v19.07 or later. Additionally, biometric fingerprint and face (iOS only) recognition require SecureAuth Identity Platform v19.07 or later, using the 2019 theme.
- Passwordless authentication as a first factor works with SecureAuth IdP v9.2.x and v9.3.x and the SecureAuth Identity Platform v19.07, with Windows 10 build 1607 or later.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-560</td>
<td>End users can authenticate into Login for Windows with an enrolled fingerprint as a first factor, without using a password.</td>
</tr>
<tr>
<td>CP-625</td>
<td>Administrators can install Login for Windows on Windows 2019 servers.</td>
</tr>
<tr>
<td></td>
<td>End users can authenticate into Login for Windows with an enrolled fingerprint or face as a second factor by using the</td>
</tr>
</tbody>
</table>
SecureAuth Authenticate mobile app.

After end users initially log in or unlock their screen with appropriate MFA, the session time period is reset to the defined "bypass_interval" in the config.json file.

### Resolved issues

<table>
<thead>
<tr>
<th>CP</th>
<th>Issue Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-647</td>
<td>When end users use the Symbol-to-Accept method and tap Deny or the wrong symbol, the error message is displayed immediately.</td>
</tr>
<tr>
<td>CP-670</td>
<td>If the &quot;hide_retry_option&quot; attribute is false in conf_version 3 in the config.json file, the button to retry the connection is hidden on the login screen when Login for Windows is offline.</td>
</tr>
<tr>
<td>CP-683</td>
<td>Members of a valid local bypass group can log in without entering a second factor, even if the group includes a domain user that is not local.</td>
</tr>
<tr>
<td>CP-690</td>
<td>Login for Windows supports proxy authentication with a proxy username and password on the proxy_url.</td>
</tr>
<tr>
<td>CP-709</td>
<td>Login succeeds for end users who log in through RDP while in a valid bypass group to bypass the second factor.</td>
</tr>
<tr>
<td>CP-714</td>
<td>When end users log in using Passcode from Token, then log out and switch to a different user, then log out and switch back to the original user, the Passcode from Token choice is correctly selected.</td>
</tr>
<tr>
<td>CP-720</td>
<td>Credentials work correctly when installing Login for Windows on Windows 8.1, Server 2012 R2 or Windows v1.</td>
</tr>
<tr>
<td>CP-724</td>
<td>If an end user submits an empty password change screen, an error message with guidance text is displayed.</td>
</tr>
<tr>
<td>CP-725</td>
<td>Logging in using multi-user credential in Login for Windows works correctly and end users are no longer asked for a second factor to log in.</td>
</tr>
<tr>
<td>CP-735</td>
<td>When a proxy is not configured in the config.json file, but a proxy server is present on the operating system configuration, the new HTTP client will use the proxy server even though it is not in the config.json file.</td>
</tr>
<tr>
<td>CP-739</td>
<td>If a Windows 7 end user denies a SecureAuth Authenticate request on a mobile device, then selects OK on the Login for Windows user interface, the Password and 2FA fields are displayed correctly.</td>
</tr>
</tbody>
</table>

### Known issue

| TW-926 | When upgrading to the Identity Platform v19.07 or later, admins must use the 2019 theme and end users who already use the SecureAuth Authenticate app must reconnect their accounts to add the ability to accept biometric push notifications to use face (iOS) or fingerprint recognition through the mobile app. |

Workaround: None
## New features and enhancements

**Version**: 19.06  
**Compatibility**: SecureAuth IdP v9.2.x and v9.3.x and the SecureAuth Identity Platform v19.07

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>102</td>
<td>A new custom &quot;bypass_interval&quot; key in the config.json files enables administrators to establish the time period between end user authentication and the next MFA log in.</td>
</tr>
<tr>
<td>63</td>
<td>A new &quot;custom_error_message&quot; key in the config.json file enables administrators to set a custom assistance string to guide end users so they have next steps after an issue occurs during login.</td>
</tr>
<tr>
<td>75</td>
<td>A new &quot;store_seeds&quot; key in the config.json file is set to <code>true</code> by default; Login for Windows will store OATH seeds, which allows end users to log in when offline.</td>
</tr>
<tr>
<td>39</td>
<td>Login for Windows supports end users authenticating by using Symbol-to-Accept as a second factor. End users must use the Authenticate mobile app to receive symbols.</td>
</tr>
<tr>
<td>14</td>
<td>Login for Windows supports YubiKey in Yubico protocol One-time Passcode mode for end users.</td>
</tr>
<tr>
<td>17</td>
<td>Group Bypass support can be enabled for users who need to log in as local admins without being prompted for additional MFA.</td>
</tr>
<tr>
<td>78</td>
<td>A new option in Login for Windows retries the connection if an offline state is detected during the first login.</td>
</tr>
</tbody>
</table>
Login for Windows first-time login for TOTP and HOTP offers a new option where end users with more than one TOTP device or HOTP token can select the device they will use. This improves performance and removes the timeout error in certain login scenarios.

Several improvements were made to optimize logging.

A new `adaptive_enabled` key in the config.json file is set to `true` by default so that administrators can install and modify Login for Windows without being blocked from completing these actions.

**Resolved issues**

<table>
<thead>
<tr>
<th></th>
<th>Login for Windows supports upgrading from version 1.0.4 to 19.06 without uninstalling before installing the latest version. (Upgrading from version 1.0.3 to 19.06 is supported but the cache is cleared. After the upgrade, the first available second factor will be selected by default instead of the previous second factor the user entered.)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th></th>
<th>The bypass group feature supports Local domain.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Members of a valid bypass group can successfully login without providing two-factor authentication.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Login for Windows is installed with a valid config.json file.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Login for Windows end users can enter characters and numbers to authenticate in, with resolution of Microsoft Windows 10 Build 1903 &quot;getFieldOptions&quot; issue.</th>
</tr>
</thead>
</table>
### Known issues

| CP-153 | In Login for Windows with Push Passcode enabled, if a notification uses multiple steps, for example, SMS/Text, end users who enter the wrong password will still receive a passcode. When an end user enters the passcode, the authentication will fail and the end user will get another chance to log in with a correct password. This issue relates to how credentials are collected and submitted for processing over the Internet; however, this is the expected behavior. |

### 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 the hotfix to take advantage of this fix. |
| CP-514 EE-1082 | Login for Windows supports YubiKey One-time Passcode for end users. The supported YubiKey is known as Yubico OTP or Yubico Cloud mode. Login for Windows customers on SecureAuth IdP 9.2 or 9.3 must apply the 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.

### Version 1.0.4 - Release Date: April 23, 2019

### New features and enhancements

**Version:** 1.0.4

**Compatibility:** SecureAuth IdP versions 9.2 or later

| CP-214 | Group Bypass support can be enabled for MFA on desktops and laptops for end users when they are online and offline. |
| CP-269 | End users can show characters for passcodes when logging on. |
| CP-271 | Login for Windows supports failover for up to five backup IdP instances. |
| CP-399 | Login for Windows requires a multi-factor authentication 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.

<table>
<thead>
<tr>
<th>CP</th>
<th>Admins can set up Security Questions so users can authenticate by answering knowledge-based questions (KBQ).</th>
</tr>
</thead>
<tbody>
<tr>
<td>-484</td>
<td>Login for Windows supports YubiKey version 5.0.</td>
</tr>
<tr>
<td>-516</td>
<td>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.</td>
</tr>
<tr>
<td>-540</td>
<td>Several minor one-time passcode (OTP) enhancements and fixes were completed.</td>
</tr>
<tr>
<td>-555</td>
<td>Administrators can enable or disable the UAC option based on how they want users to log on the environment.</td>
</tr>
</tbody>
</table>

Resolved issues

<table>
<thead>
<tr>
<th>CP</th>
<th>SMS / Voice telephone numbers are masked for registered multi-factor authentication methods.</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-386</td>
<td>Manual uninstallation from the &quot;Programs and Features&quot; menu on Windows 10 succeeds.</td>
</tr>
<tr>
<td>P-416</td>
<td>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.)</td>
</tr>
<tr>
<td>P-418</td>
<td>End users no longer receive a failure message when attempting to authenticate by using TOTP after their device wakes from sleep mode while online.</td>
</tr>
<tr>
<td>P-421</td>
<td>End users no longer given a private IP address when Adaptive Authentication is used in an RDP session.</td>
</tr>
<tr>
<td>P-443</td>
<td>A non-local user whose account is not found in Active Directory receives on-screen guidance about how to fix and proceed.</td>
</tr>
<tr>
<td>P-447</td>
<td>A SecureAuth file called .saconfig is no longer created after a Login for Windows installation failure.</td>
</tr>
<tr>
<td>Page</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>470</td>
<td>The last user displays only when the &quot;multiple_user&quot; flag is set to false.</td>
</tr>
<tr>
<td>471</td>
<td>End users connecting to Login for Windows for the first time and through an RDP connection are offered appropriate MFA options instead of an &quot;offline MFA&quot; message.</td>
</tr>
<tr>
<td>474</td>
<td>Adaptive &quot;Skip to post-authentication&quot; and &quot;Skip two factor authentication&quot; options no longer refuse to log on the last user on Windows 8.</td>
</tr>
<tr>
<td>476</td>
<td>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.</td>
</tr>
<tr>
<td>490</td>
<td>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.</td>
</tr>
<tr>
<td>542</td>
<td>Login for Windows accepts connections when certificates are self-signed because the value of &quot;allow_self_signed&quot; is no longer ignored.</td>
</tr>
<tr>
<td>544</td>
<td>When SecureAuth IdP encounters a malformed email string that lacks an at symbol (@), IdP returns the string as a Login for Windows email.</td>
</tr>
<tr>
<td>552</td>
<td>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.</td>
</tr>
<tr>
<td>569</td>
<td>End users logged onto Login for Windows who use RDP to connect to the same machine will see a standard Windows &quot;Unlock the PC&quot; message when using the knowledge-based MFA method.</td>
</tr>
<tr>
<td>574</td>
<td>After Login for Windows is first installed, end users who select the Switch User button see &quot;Other User&quot; once instead of twice.</td>
</tr>
<tr>
<td>575</td>
<td>End users can log on using YubiKey the first time, without receiving an error message.</td>
</tr>
<tr>
<td>578</td>
<td>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.</td>
</tr>
</tbody>
</table>
|      | End users receive a better error message with guidance when attempting to log in while offline, but offline methods were not
**Known issues**

<table>
<thead>
<tr>
<th>CP-288</th>
<th>Login for Windows performance degrades when loading the login screen in the offline mode on Windows 10.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-488</td>
<td>End users can log into their machines with sAMAccountName attributes only. Attributes other than sAMAccountName are not supported.</td>
</tr>
</tbody>
</table>

**Version 1.0.3 - Release Date: September 17, 2018**

**New features and enhancements**

Version: 1.0.3

Compatibility: SecureAuth IdP versions 9.2

| 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**

<table>
<thead>
<tr>
<th>CP-288</th>
<th>Login for Windows performance degradation when loading the login screen in the offline mode on Windows 10.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-386</td>
<td>SMS / Voice telephone numbers are not completely masked for registered multi-factor authentication methods.</td>
</tr>
<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>
<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-</td>
<td>User is blocked by Adaptive Authentication on Windows Server 2012 R2 and receives an error message if no alternate</td>
</tr>
</tbody>
</table>
Resolved issues and enhancements

Version 1.0.2 - Release Date: June 13, 2018

Version: 1.0.2  
Compatibility: SecureAuth IdP versions 9.2

<table>
<thead>
<tr>
<th>Issue</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>
<tr>
<td>CP-400</td>
<td>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.</td>
</tr>
<tr>
<td>CP-403</td>
<td>The most recently used multi-factor authentication device now appears when logging on / off Windows 7 or Windows 10.</td>
</tr>
</tbody>
</table>
### CP-408
SADiag.exe no longer returns an error when 'set logging off' and 'test api' log level settings are used.

### CP-410
The installer now accepts a relative path to the configuration file during a silent installation.

### CP-411
The correct username now appears on the lock screen on Windows 7 / Windows Server 2008.

### Known issues

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-386</td>
<td>SMS / Voice telephone numbers are not completely masked for registered multi-factor authentication methods.</td>
</tr>
<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

**Version 1.0.1**

**Release Date:** May 14, 2018

#### Correct fixed issues

**Version:** 1.0.1

**Compatibility:** SecureAuth IdP versions 9.2

**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**

**Version**: 1.0  
**Compatibility**: SecureAuth IdP versions 9.2

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 two-factor authentication method.

---

**Related documentation**

- YubiKey HOTP Device Provisioning and Multi-Factor Authentication Guide
- YubiKey OATH-TOTP Device Provisioning and Multi-Factor Authentication Guide
- SecureAuth Compatibility Guide
- Login for Windows v19.09.03 configuration guide
- Login for Mac v20.03.01 configuration guide
Login for Windows SSL configuration requirements