Login for Endpoints Configuration Guide v1.0.2

For the latest versions of this document see:

- Login for Windows configuration guide v1.0.4
- Login for Mac configuration guide v1.0.3

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.

Introduction
Login for Endpoints (available in SecureAuth IdP version 9.2+ only) adds SecureAuth’s Multi-Factor Authentication to the Windows desktop and remote server login experience, and the Mac desktop login experience. This product was introduced in SecureAuth IdP version 9.2 and supports these authentication methods:

- Timed Passcode
- Voice Call
- Passcode sent via SMS / Text Message
- Passcode sent via Email
- One-time Passcode via Push Notification
- Login Notification via Push Notification
- YubiKey HOTP Device Passcode
- Passcode from Help Desk

**NOTE:** Methods delivered via Push Notification require the use of the SecureAuth Authenticate App

In addition to the supported Multi-Factor Authentication methods, Login for Endpoints supports these setups / features for Windows and / or Mac:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows</th>
<th>Mac</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline mode login</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Multi-Factor Authentication for desktops and / or remote servers</td>
<td>x</td>
<td>N/A</td>
</tr>
<tr>
<td>Multi-Factor Authentication for single users only and / or multi-users</td>
<td>x</td>
<td>N/A</td>
</tr>
<tr>
<td>Users in bypass group can skip Multi-Factor Authentication</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Bypass group lookup on a domain other than user's domain</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Password expiration notification</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Password Reset link to SecureAuth IdP realm or 3rd party service</td>
<td>x</td>
<td>N/A</td>
</tr>
<tr>
<td>Multiple login capability</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Endpoint identified during login Multi-Factor Authentication request</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Use Third-party Credential Providers</td>
<td>x</td>
<td>N/A</td>
</tr>
<tr>
<td>YubiKey HOTP support for 2-Factor Authentication</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>TOTP 2-Factor Authentication</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Cached user credentials let users sign in with fewer clicks</td>
<td>x</td>
<td>N/A</td>
</tr>
<tr>
<td>Installation API validation</td>
<td>x</td>
<td>N/A</td>
</tr>
<tr>
<td>Adaptive Authentication</td>
<td>x</td>
<td>N/A</td>
</tr>
<tr>
<td>Non-domain server support</td>
<td>x</td>
<td>N/A</td>
</tr>
<tr>
<td>Validated with FIPS 140-2 compliant cryptographic libraries</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

**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.
- Login for Endpoints ONLY supports the `samAccountName` login name format; `userPrincipalName` (UPN) is not supported. Note that UPN is supported at login, but if using a non-AD profile store containing OATHSeed/OATHToken/PNToken but not `samAccountName`, then the Multi-Factor Authentication lookup will fail and the user will not be able to use other Multi-Factor Authentication methods.

**NOTE:** If you are currently using the SecureAuth Credential Provider, you do not need to uninstall before installing Login for Windows.

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

   ![Site Bindings](image)

   ![Edit Site Binding](image)

2. Create a New Realm or access an existing realm on which more than one Multi-Factor Authentication is required.

   **NOTE:** This realm should **not** be configured for Single Sign-on.

3. Configure the following tabs on the Web Admin in preparation for configuring Login for Endpoints:
   - **Overview** – the description of the realm and SMTP connections must be defined
   - **Data** – an enterprise directory must be integrated with SecureAuth IdP
   - **Workflow** – the way in which users will access the target must be defined
   - **Multi-Factor Methods** – the Multi-Factor Authentication methods that will be used to access the target must be defined
   - **Post Authentication** – the target resource or post authentication action must be defined
   - **Logs** – the logs that will be enabled or disabled for this realm must be defined

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

<table>
<thead>
<tr>
<th>Supported OS Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows OS versions:</strong></td>
</tr>
<tr>
<td>• Windows 7 (32/64-bit)</td>
</tr>
<tr>
<td>• Windows 8.1 (32/64-bit)</td>
</tr>
<tr>
<td>• Windows 10 (64-bit)</td>
</tr>
<tr>
<td><strong>Windows Server OS versions:</strong></td>
</tr>
<tr>
<td>• Windows Server 2008 R2 (64-bit)</td>
</tr>
<tr>
<td>• Windows Server 2012 (64-bit)</td>
</tr>
<tr>
<td>• Windows Server 2012 R2 (64-bit)</td>
</tr>
<tr>
<td>• Windows Server 2016 (64-bit)</td>
</tr>
<tr>
<td><strong>Minimum macOS versions:</strong></td>
</tr>
<tr>
<td>• macOS High Sierra 10.13.2</td>
</tr>
<tr>
<td>• macOS Sierra 10.12.6</td>
</tr>
</tbody>
</table>

   **NOTE:** See [SecureAuth Compatibility Guide](#) for OS and SecureAuth IdP version support information.

   **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.

   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.
Login for Windows

End-user: First-time Usage Requirements

SecureAuth strongly recommends using a timed passcode the first time you use Login for Windows to access the network.

To meet this requirement, you must have an account provisioned with a SecureAuth IdP realm that enables your device to generate timed passcodes for Multi-Factor Authentication:

- SecureAuth Authenticate App
- YubiKey HOTP Device – refer to the YubiKey HOTP Device Provisioning and Multi-Factor Authentication Guide to ensure all requirements are met.
- YubiKey TOTP Device – refer to the YubiKey OATH-TOTP Device Provisioning and Multi-Factor Authentication Guide to ensure all requirements are met.

Thereafter, you can use Login for Windows in the offline mode.

Login for Mac

Admin: User Account and Mac Workstation Requirements

Active Directory Profile Configuration on the Mac

The end-user Active Directory profile must be accurately configured on the Mac so that the endpoint can retrieve the AD end-user profile during the login process.

Preconfigured Enterprise WiFi System Level Policy

In an enterprise WiFi environment, before setting up Login for Mac on end-user workstations, the system level policy must be configured to allow the Mac to connect to the enterprise WiFi. This setup lets Login for Mac fetch the OATH seed which is used to authenticate the end-user.

Prevention of YubiKey Device Usage Conflicts

If an end-user is already using a YubiKey device for YubiKey Multi-Factor Authentication on a SecureAuth IdP realm, the OATH seed and associated YubiKey device must be removed from the end-user's account in order to prevent a conflict when the end-user attempts to use a YubiKey device for HOTP authentication. (See the steps under End-user Multi-Factor Authentication in the YubiKey Multi-Factor Authentication Configuration Guide to remove the YubiKey device from the user account profile.)

Prevent and Troubleshoot End-user Lockouts

End-users can be locked out of their Mac workstations due to any of these factors:

- Network Setup Issues
- Login for Endpoints Installer Misconfiguration
- End-user Mac Configuration Issues

Expand the section below for more information:
Network Setup Issues

Matching Active Directory Profiles Required

Active Directory must include an account profile for each end-user, and that profile must match the AD profile set up on the Mac in order for the Mac endpoint to retrieve the AD profile.

Login for Endpoints Installer Misconfiguration

Edits Made in config.json File

If the configured config.json file is edited, caution must be taken to ensure Unicode characters — instead of UTF-8 characters — are not entered and saved in the file. This scenario might occur if text is copied from another source and pasted into the file, and could result in an end-user being locked out of the Mac due to a misconfigured endpoint.

End-user Mac Configuration Issues

Misconfigured Active Directory Profile on Mac

If the end-user’s new Mac has a misconfigured Active Directory account profile, the endpoint will not be able to retrieve the end-user’s AD profile to complete the login process.

Lockout with Secure, Automatic Enterprise WiFi Endpoint Connection

If the endpoint is set to automatically connect to a secure, enterprise WiFi, and has not yet been configured to connect to a SecureAuth IdP realm, then the end-user will be locked out of logging on the Mac.

In this scenario, the Mac may need to be reset by the administrative user who can bypass the login endpoint in order to reset the machine.

Lockout without OATH Seed for YubiKey HOTP Device or Network Connectivity

If a YubiKey HOTP device is used for logging on the Mac, but the machine does not have an OATH seed stored on it or network connectivity, then the endpoint must wait for an available network connection.

If the end-user is attempting to log on for the first time, and the Mac does not have WiFi configured or is not using a wired connection, then the end-user will be locked out of logging on the Mac.
Users Disabled in Active Directory

If an end-user is disabled on Active Directory, the local account will not know the history of the AD account, and the user will not be able to log on the Mac.

End-user: Account and Mac Workstation Requirements

IMPORTANT: Before Installing Login for Mac

Your local username and password on the Mac must be the same as your Active Directory username and password. If you are using a different local username than your Active Directory username, then you will need to contact IT to synchronize the IDs.

If the IDs are synchronized, be sure you can log on the Mac before installing Login for Mac.

First-time Usage Requirements

The first time you use Login for Mac to log on the network:

A timed passcode is required. You must have an account provisioned with a SecureAuth IdP realm that enables your device to generate timed passcodes for Multi-Factor Authentication:

- SecureAuth Authenticate App
- YubiKey HOTP Device – refer to the YubiKey HOTP Device Provisioning and Multi-Factor Authentication Guide to ensure all requirements are met.

Your Mac must either be hardwired to the network, or you must have a preconfigured WiFi connection within range to which your Mac can be manually connected.

Thereafter, you can use Login for Mac in the offline mode.

SecureAuth IdP Web Admin Configuration

Data
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 False from the Advanced AD User Check dropdown.

3. Select Bind from the Validate User Type dropdown.
<table>
<thead>
<tr>
<th>Property</th>
<th>Source</th>
<th>Field</th>
<th>Data Format</th>
<th>Writable</th>
</tr>
</thead>
<tbody>
<tr>
<td>OATH Seed</td>
<td>Default Provider</td>
<td>description</td>
<td>Advanced Encryption</td>
<td>✔️</td>
</tr>
<tr>
<td>One Time OATH List</td>
<td>Default Provider</td>
<td>postalAddress</td>
<td>Plain Text</td>
<td>✔️</td>
</tr>
<tr>
<td>Fingerprints</td>
<td>Default Provider</td>
<td>audio</td>
<td>Plain Binary</td>
<td>✔️</td>
</tr>
<tr>
<td>Push Notification Tokens</td>
<td>Default Provider</td>
<td>jpegPhoto</td>
<td>Plain Binary</td>
<td>✔️</td>
</tr>
<tr>
<td>OATH Tokens</td>
<td>Default Provider</td>
<td>registeredAddress</td>
<td>Plain Binary</td>
<td>✔️</td>
</tr>
<tr>
<td>Aux ID 2</td>
<td>Default Provider</td>
<td>objectGUID</td>
<td>Plain Text</td>
<td></td>
</tr>
<tr>
<td>Aux ID 3</td>
<td>Default Provider</td>
<td>adminDescription</td>
<td>Plain Text</td>
<td>✔️</td>
</tr>
<tr>
<td>Aux ID 4</td>
<td>Default Provider</td>
<td>postOfficeBox</td>
<td>Plain Text</td>
<td>✔️</td>
</tr>
<tr>
<td>Biometrics</td>
<td>Default Provider</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

5. If using a single OATH seed for end-user Multi-Factor Authentication, then map Fields to `OATH Seed` and `OATH Tokens` Properties, as shown in the sample image.

Click **Save** once the configuration is complete and before leaving the Data page to avoid losing changes.
6. In the Multi-Factor Configuration section, configure the Multi-Factor Authentication methods you want enabled.

Click **Save** once the configuration is complete and before leaving the Multi-Factor Methods page to avoid losing changes.
7. On the System Info tab, in the Links section, **Click to edit Web Config file.**

8. In the Web Config Editor section, under `<appSettings>`, add this line:

   ```xml
   <add key="OTPFieldMapping" value="AuxID3" />
   ```

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

   **Click Save** once the configuration is complete and before leaving the Web Config Editor page to avoid losing changes.
9. In the API Key section, click **Generate Credentials**.

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

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

   ![API Permissions section](image)

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

11. Select **Enable Login for Endpoints API**, and then click **Configure Login for Endpoints Installer**.
Adaptive Authentication can be used with Login for Windows 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
4. Geo-velocity
5. User / Group

**NOTE:** See Group Bypass Configuration Notes in the Login for Windows Installer Configuration section for information about using Adaptive Authentication with the group bypass feature.
Endpoint Operating System

- **Windows**

Endpoint Type

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

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

IdP Hostname

Enter the hostname of the IdP to use in the configuration

```plaintext
company.secureauth.com
```

Multi-Factor Authentication Settings

Require Multi-factor Authentication when:

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

Bypass Multi-factor Authentication when:

- **☐** Users are a member of the following groups:

  Add groups separated by commas or line breaks

Password Reset

- **✓** Enable update password link on the login interface.

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

  - **Point to other password reset site**
    - **Enter the site URL**
12. On the Login for Endpoints Installer Configuration page, select **Windows** as the **Endpoint Operating System**.

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

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

14. Enter the **IdP Hostname**.

15. 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.

16. If any user group is allowed to bypass Multi-Factor Authentication, enable the bypass option and list the user group(s).
Group Bypass Configuration Notes

Adaptive Authentication used with Group Bypass

If using Adaptive Authentication AND the group bypass feature, the group bypass feature takes precedence for handling the user’s login request.

Multi-Forest AD Environment and Group Bypass

In a multi-forest AD environment, the user account must be included on each domain in order to bypass Multi-Factor Authentication on any domain.

Proxy Server and Proxy Bypass List Configuration

If using a proxy bypass, you must configure the proxy server and proxy bypass list – i.e. a list of hosts to use to bypass the proxy.

The following order is used:

1. "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.

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

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

**IMPORTANT**: By enabling alternate credential providers, users will be able log in without using the Login for Windows credential provider, and potentially bypass Multi-Factor Authentication.

Enabling alternate credential providers is only recommended in test environments, to let testers bypass Login for Windows so they can readily access their machines.

If the default Windows Credential Provider is enabled, users will see their normal login prompt and will have to manually select a different login option in order to use Login for Windows.

19. Click **Download Installer Config** to download the JSON file (config.json) which 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 **OPTIONAL: Set End-user Access Level** section for access level settings and configuration.
Login for Endpoints Installer Configuration

Configure and download the installer config for Login for Endpoints

Endpoint Operating System

- [ ] Windows
- [x] Mac OS

IdP Hostname

Enter the hostname of the IdP to use in the configuration

company.secureauth.com

Multi-Factor Authentication Settings

Require Multi-factor Authentication when:
- [x] Logging in with physical access
- [x] Logging in via Remote Desktop Protocol

Bypass Multi-factor Authentication when:
- [ ] Users are a member of the following groups:

Add groups separated by commas or line breaks

Download Installer Config
12. On the Login for Endpoints Installer Configuration page, select **Mac OS** as the **Endpoint Operating System**.

13. Enter the **IdP Hostname**.

14. Under Multi-Factor Authentication Settings, specify whether or not the user must use Multi-Factor Authentication to access the Mac from a desktop and / or via remote access from another Mac device.

   If any user group is allowed to bypass Multi-Factor Authentication, enable the bypass option and list the user group(s).

![Tip]

A user group on another domain can be bypassed via the Mac authentication plugin and Pluggable Authentication Modules (PAM) installed on the end-user's workstation.

In this scenario, the Open Directory API can be used by specifying the user group and domain.

15. Click **Download Installer Config** to download the JSON file (config.json) that will be used with the PKG file, as described in the Installation section of this guide.

   **NOTE:** Before installation, the config.json file 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 **OPTIONAL: Set End-user Access Level** section for access level settings and configuration.

   Also in this **OPTIONAL** section, find information about enabling Multi-Factor Authentication when using SSH for remote login access to a Mac.

---

**OPTIONAL: Set End-user Access Level**
Login for Windows Access Level Configuration

Login for Windows requires the end-user to use Multi-Factor Authentication by default to access the local console or remote console in an RDP session.

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

Change the User's Access Level

1. Find the config.json file which you downloaded in step 19 of the Web Admin Configuration section of this document, and copy that file to the Temp folder on the target machine.
2. Start a text editor such as Notepad++ and edit the access_level in the file, changing the value to a pertinent value:
   - 0 = Multi-Factor Authentication always required
   - 1 = Multi-Factor Authentication required for local access only
   - 2 = Multi-Factor Authentication required for remote access only
   - 3 = Multi-Factor Authentication never required. This setting is used for Self-service Password Reset (SSPR) only.

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.

3. Save the configuration.
Login for Mac Access Level Configuration

Login for Mac by default requires the end-user to use Multi-Factor Authentication to access the local console and a remote console in an SSH session.

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

**Change the User’s Access Level**

1. Find the config.json file which you downloaded in step 15 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 Sublime Text and edit the `access_level` in the file, changing the value to a pertinent value:

   - 0 = Multi-Factor Authentication always required
   - 1 = Multi-Factor Authentication required for local access only
   - 2 = Multi-Factor Authentication required for remote access only
   - 3 = Multi-Factor Authentication never required – this setting is used for Self-service Password Reset (SSPR) only

3. Save the configuration.

---

**Enable and Use Multi-Factor Authentication for Remote Access (SSH)**

1. On the Mac, go to Settings, select Sharing, and then enable Remote Login.

2. After making this setting, SSH into the machine via `ssh username@hostname` – example: `ssh jsmith@170.17.0.150`

3. Enter your password, and you will be prompted for Multi-Factor Authentication.

---

**Installation**

**Login for Windows Installation**

**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 — SecureAuthLogin-1.x.x-x64.msi or SecureAuthLogin-1.x.x-x86.msi — and place that file in the Temp folder.
Install Login for Windows

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

1. Find the config.json file which you downloaded in step 19 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 OPTIONAL section above.

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

   ```
   msiexec /i "C:\Temp\SecureAuthLogin-1.0.0-x64.msi" /L*V "C:\Temp\install.log" /qn
   CONFIG="C:\Temp\config.json"
   ```

3. Log off the target machine.

   **NOTE:** 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 unstalling 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.

**NOTE:** A config.json file with the "allow_self_signed" setting enabled should not be distributed to end-user machines since potential security vulnerabilities may result. The "allow_self_signed" setting should only be enabled in a test environment, and should be disabled in conf.xml once testing is complete.

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.

**NOTE:** 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.
Uninstallation

1. 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:

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

   **NOTE:** Manual installation on Windows 10 using the "Programs and Features" menu will result in an error.

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 UserAgent string:

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

For example:

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

**NOTE:** A config.json file with the "allow_self_signed" setting enabled should *not* be distributed to end-user machines since potential security vulnerabilities may result. The "allow_self_signed" setting should only be enabled in a test environment, and should be disabled in conf.xml once testing is complete.

**WARNING:** Do not install Login for Mac version 1.0 on any MacOS Sierra machine (10.12.x) in a domain-joined system on which FileVault encryption is used on the boot volume – this may render the operating system unbootable and require recovery.

**Copy the JSON File to a Specified Folder**

1. Find the config.json file which you downloaded in step 14 of the Web Admin Configuration section of this document.

   **NOTE:** You may have already performed this step if you changed the user's access level in the OPTIONAL section above.

2. Copy that file to a specified folder on the target machine.

**Download the Login for Mac ZIP File to the Specified Folder**

1. Download the Login for Mac .zip file to the target machine.

2. Unzip this file which contains the SecureAuthLogin-1.x.pkg and SecureAuthLogin-1.x-Uninstaller.pkg files.

3. Copy these files to the same folder as the config.json file on the target machine.

**Run the Login for Mac Installer Package**

1. Double-click SecureAuthLogin-1.x.pkg to start the installation wizard for the application.

2. Log Out of the target machine.

   **NOTE:** After this installation, SecureAuth Login for Mac appears on the next login session.

---

**End-user Experience**

**Login for Windows End-user Experience**
**Known Issues**

- On Windows 10 desktops, a Login Notification request cancelled on the desktop—but accepted on the SecureAuth Authenticate app on a mobile device—still gives the user login access on the machine. This issue has been raised with Microsoft, but at this time remains unaddressed by them.

- On Windows Server versions 2008 R2 and 2012 R2, users may be unable to complete the self-service password reset process due to default Internet Explorer settings in the operating systems.

- If using a proxy which becomes 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.

- 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.

- The 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.

---

**Windows 10: First-time Login Experience**
1. Enter your username on the Windows login screen.

2. The first time you use Login for Windows, SecureAuth recommends selecting a timed passcode authentication option from the list of Multi-Factor Authentication methods for which you have enrolled. This could be one 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 a YubiKey.

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

   If you do not have an authentication method that provides a timed passcode, then select any other option available to you.
**Timed passcode from app**

For this option:

1. If there is more than one provisioned OATH OTP app, select the device.

2. Enter your Windows Password.

3. Click the arrow to log on Windows.

**Passcode from voice call**

For this option:

1. Select the phone number if more than one mobile phone is included in your user profile.

2. Enter your Windows Password.

3. Click the arrow to log on Windows.
Passcode from SMS / text

For this option:

1. Select the phone number if more than one mobile phone is included in your user profile.

2. Enter your Windows Password.

3. Click the arrow to log on Windows.

Passcode from email

For this option:

1. Select the email address if more than one address is included in your user profile.

2. Enter your Windows Password.

3. Click the arrow to log on Windows.
Passcode from notification

For this option:

1. Select the mobile device on which the provisioned SecureAuth Authenticate app is installed.

2. Enter your Windows Password.

3. Click the arrow to log on Windows.

Approve login notification on mobile

For this option:

1. Select the mobile device on which the provisioned SecureAuth Authenticate app is installed.

2. Enter your Windows Password.

3. Click the arrow to log on Windows.
Contact help desk for passcode

For this option:

1. Select the phone number to use for contacting the help desk.

2. Enter your Windows Password.

3. Click the arrow to log on Windows.

Passcode from token

For this option:

1. If there is more than one provisioned token, select the device on which the provisioned SecureAuth passcode app is stored.

2. Enter your Windows Password.

3. Click the arrow to log on Windows.
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.
Timed passcode from app

1. In the Enter passcode field, enter the OATH OTP from your SecureAuth One-time Passcode app.

2. Click the arrow to log on Windows.

Contact help desk for passcode

1. Enter the passcode received by contacting the help desk.

2. Click the arrow to log on Windows.
Approve login notification on mobile

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


Passcode from notification

1. Enter the passcode sent to the SecureAuth Authenticate app on your mobile device.

2. Click the arrow to log on Windows.
Passcode from email

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

Passcode from voice call

1. Enter the passcode received by a voice call to your mobile phone.
2. Click the arrow to log on Windows.
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 Token

1. Plug in the token to receive a passcode from the device.
2. Click the arrow to log on Windows.
IMPORTANT:

- The enterprise WiFi connection must be disabled on the Mac in order to log on to the domain. A public WiFi connection or a wired connection can be used for Internet access.
- If you are included in a bypass group, you should patiently wait for the network group to be fully connected before logging on.

1. Enter your domain username and password on the Mac login screen.
2. When using Login for Mac for the first time, you must supply a timed passcode from either the SecureAuth Authenticate App on your mobile device or another device provisioned with the SecureAuth IdP realm to supply timed passcodes, such as a YubiKey. This window (pictured left) only appears the first time you use Login for Mac.

Enter the passcode that appears on the device, and then click Submit.

NOTE: After successfully logging on the Mac using a timed passcode, timed passcodes from that device can be used for login access in the offline mode, i.e. when the Mac is not connected to the Internet.

3. Log Out of the Mac.
4. Log back on the Mac, and select an authentication option from the list of Multi-Factor Authentication methods for which you have previously enrolled.

   **NOTE**: If your list of available authentication options is lengthy, you may need to scroll down the list if the option you wish to choose does not appear on the main page.

5. Optionally, check the **Remember my selection** box if you want to use this same authentication method the next time you log on the Mac.

6. Click **Submit** to access the Mac on the network.

   **NOTE**: Authentication method workflows are described in the sub-sections below.

   No matter which option you choose, you can return to this selection window by clicking the link: **I want to choose a different two-factor authentication method**.
Receive passcode from notification

When selecting this option, the Enter Passcode window appears.

1. Enter the passcode that was sent to the SecureAuth Authenticate App on your mobile device.

2. Click Submit to log on the Mac.
Approve login notification

When selecting this option, the Waiting for Your Approval window appears.

1. Accept the login notification sent to the SecureAuth Authenticate App on your mobile device to log on the Mac.
Enter timed passcode from app

When selecting this option, the Enter Passcode window appears.

1. Enter the OATH OTP from your SecureAuth OTP App.

2. Click Submit to log on the Mac.
Receive passcode

When selecting this option, the Enter Passcode window appears.

1. Enter the passcode sent via SMS to your mobile phone.
2. Click Submit to log on the Mac.
Receive passcode

When selecting this option, the Enter Passcode window appears.

1. Enter the passcode sent to your email address.

2. Click Submit to log on the Mac.
Receive passcode

When selecting this option, the Enter Passcode window appears.

1. Enter the passcode received by a voice call to your mobile phone.

2. Click **Submit** to log on the Mac.

Additional Methods Options
Contact the help desk

When selecting this option, the Enter Passcode window appears.

1. Input the passcode supplied by the help desk.

2. Click Submit to log on the Mac.
Enter passcode - HOTP Device

When selecting this option, the Enter Passcode window appears.

1. With the YubiKey HOTP device inserted in the machine, tap / press the device to populate the passcode in the field.

2. Click Submit to log on the Mac.

Release Notes

Release Date: June 13, 2018

Version 1.0.2

Login for Windows

Resolved Issues and Enhancements
<table>
<thead>
<tr>
<th>CP-187</th>
<th>RDP users utilizing NLA (Network Level Authentication) no longer receive a second prompt after providing credentials to the RDP client.</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>CP-408</td>
<td>SADiag.exe no longer returns an error when 'set logging off' and 'test api' log level settings are used.</td>
</tr>
<tr>
<td>CP-410</td>
<td>The installer now accepts a relative path to the configuration file during a silent installation.</td>
</tr>
<tr>
<td>CP-411</td>
<td>The correct username now appears on the lock screen on Windows 7 / Windows Server 2008.</td>
</tr>
</tbody>
</table>

**Known Issues**
Resolved Issues and Enhancements

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-309</td>
<td>Login for Mac .pkg files have been renamed for consistency with Login for Windows .msi file names.</td>
</tr>
<tr>
<td>CP-317</td>
<td>Login for Mac now validates the configuration file correctly.</td>
</tr>
<tr>
<td>CP-327</td>
<td>The initial Multi-Factor Authentication method window now shows a selected option.</td>
</tr>
<tr>
<td>CP-359</td>
<td>The installation failure log (Command+L) now identifies a missing configuration file.</td>
</tr>
<tr>
<td>CP-379</td>
<td>Log details have been added to help troubleshoot common installation errors.</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-390</td>
<td>Users are no longer locked out on Sierra 10.12.x machines with a FileVault encrypted drive.</td>
</tr>
<tr>
<td>CP-392</td>
<td>Device names receiving push requests now appear on Login for Mac waiting screens.</td>
</tr>
</tbody>
</table>

Known Issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP-346</td>
<td>Bypass groups are only enforced when a system is online and can check group membership.</td>
</tr>
<tr>
<td>CP-386</td>
<td>SMS / Voice telephone numbers are not completely masked for registered Multi-Factor Authentication methods.</td>
</tr>
</tbody>
</table>

Release Date: May 14, 2018

Version 1.0.1

Login for Windows
Resolved Issues

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

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

Login for Mac

Known Issues

- **Login failure for users with a space in sAMAccountName**
  
  The issue for users who are unable to log in if a space exists in their sAMAccountName property cannot be resolved because macOS does not support using spaces in login names.

- **Critical issue with FileVault on Sierra**
  
  Do not install Login for Mac 1.0 on MacOS ‘Sierra’ (10.12.x) in a domain-joined system that uses FileVault encryption on the boot volume; this may render the system unbootable and require recovery.

- **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.

- **Additional Authentication methods may be hidden**
  
  Since many MacOS configurations do not display a scrollbar, users who are prompted to select an authentication method may not know there are additional methods available to them if they do not see them on the screen currently displayed.

- **Multi-Factor Authentication only prompts users at login**
  
  Login for Mac does not currently support prompting users for additional factors when unlocking the screen of an already logged-in user.

- **Offline login may not complete**
  
  Users attempting to login offline for a second time using a TOTP code (after logging on and logging off) may have their machine after entering the code.

- **Login for Mac will install on unsupported MacOS versions**
  
  Login for Mac is only supported and tested on MacOS versions 10.12.x (Sierra) and 10.13.x (High Sierra), but currently the installer allows installation to proceed on versions 10.10.x and 10.11.x.
Version 1.0

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

Related Documentation

- YubiKey HOTP Device Provisioning and Multi-Factor Authentication Guide
- SecureAuth Credential Provider Configuration Guide
- Login for Windows SSL configuration requirements
- Login for Windows configuration guide v1.0.4
- Login for Mac configuration guide v1.0.3
- How to convert an OATH Seed to an OATH Token

https://docs.secureauth.com/display/SAT/Login+for+Endpoints+Configuration+Guide+v1.0.2#expand(LoginforWindowsAccessLevelConfiguration)

SecureAuth Authenticate App