# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents</td>
<td>1</td>
</tr>
<tr>
<td>IT Security Services</td>
<td>2</td>
</tr>
<tr>
<td>Google 2-Step Verification</td>
<td>3</td>
</tr>
<tr>
<td>Google Authenticator App</td>
<td>4</td>
</tr>
<tr>
<td>Google Prompt</td>
<td>6</td>
</tr>
<tr>
<td>Google Phone call / text</td>
<td>7</td>
</tr>
<tr>
<td>Windows 10 Absolute Installation Instructions</td>
<td>8</td>
</tr>
<tr>
<td>InCommon Certificate Services</td>
<td>10</td>
</tr>
</tbody>
</table>
Google 2-Step Verification

Open your Google Account and select **Manage your Google Account**

Select **Security** in the navigation panel on the left side

Under "**Signing in to Google**", select **2-Step Verification > Get Started**

You will now have the option of several authentication methods that you can use.

The related articles describe each of the common setups for the additional verification method.
Google Authenticator App

You can use the Google Authenticator app to receive codes. You can still receive codes without an internet connection or mobile service. Android devices require that your Android version is 4.4 and up and that you have turned on 2-Step Verification already on Google.

Once you have entered an alternative method for 2FA, you can also change your preferred method to an Authenticator app. Go back through the first initial steps and click the 2-Step Verification button on your Security page.

You will then see more information about your chosen method and how to add more security to your account. Navigate down to Add more second steps to verify it’s you where you will see the option Authenticator app. Click on Set up

You will then be prompted to select what type of phone you have. Click on the appropriate option (Android or iPhone).

Go into the Authenticator App on your phone and select Set up account

Once you have set up your account, you need to click on the little ‘+’ button at the top right of your phone screen. This will give you the option to either scan a bar code or do a manual entry.

Your browser should be showing a bar code that you can scan from your phone to automatically link the Google account. If you are having trouble scanning, select the Can’t Scan It? option and follow the instructions to do a manual entry which will involve entering the given key into the app.

Once you have linked the accounts, you will be prompted to enter the 6-digit code from the app. Then select Verify.
You will now be able to authenticate your account when you sign in to Google by entering the 6-digit code from the app which refreshes about every 30 seconds.
Google Prompt

Google prompts are push notifications you'll receive on Android phones that are signed in to your Google account and iPhones with the Gmail app or Google app signed in to your Google account. Based on the device and location info in the notification, you can either allow the sign in if you requested it by tapping Yes or block the sign in attempt if you didn't request it by tapping No.

If you don't see a notification on your device, make sure you are signed in to your Google account on your phone.

If you select 2-Step Verification and your default screen is asking for information about your phone, you can select Show more options at the bottom of your screen to get additional choices. Then, select Google Prompt.

Your phone needs to be signed in to your Google account in order to receive a notification. It should appear automatically at the top of your phone's screen and then you can click on the notification. Click Yes and then your browser should automatically verify you and add this authentication method as your new default.

Android

1. Open the Settings app on your phone
2. Tap Accounts, then Add Account
3. Select Google and sign in

iPhone

1. Get the Google or Gmail app from the App Store
2. Sign in with your Google Account
Input the phone number that you want to associate with this Google Account. Then select whether you would like to receive codes by **Text message** or **Phone call**.

If you chose Text message, then you will receive a text with a verification code that you will enter in the following field on the webpage. You only need to input the numbers after G-. (For example, G-123456 can be entered here as 123456). Once you have entered the code, click **Next**.

If you chose a Phone call, then you will receive a call with a verification code that needs to be entered into the website. If you do not answer the call, you will be left a voicemail. Once you have entered the code click **Next**. *The call may show up listed as Potential Spam*
Windows 10 Absolute Installation Instructions

Contact the IT Service Desk for Access to the Software Downloads

The Absolute software service provides centralized management of URI's Absolute Data and Device Security (DDS) service — formerly known as CompuTrace. Absolute DDS is designed to track, manage, and secure mobile computers and devices for better data protection, easier IT asset management, and managed computer theft recovery. This article is a step-by-step guide on how to install Absolute on Windows 10.

1. Once you receive the Software Downloads link from the IT Service Desk, click on **Absolute**

2. Click on **Windows_Agent** from the list

3. Open the **Computrace.msi** file

4. Once the installation wizard opens up, click **Next** on it

5. Click **Yes** to the Computrace Installation Module User Control popup

6. Click **Yes** to the rpcnet User Control popup

7. Click **Close** to exit the wizard
Congratulations! You've successfully installed Absolute for Windows 10.
InCommon Certificate Services

Overview

The University of Rhode Island has partnered with InCommon Federation which allows the University to obtain digital certificates at an affordable annual fee. The cost is completely covered by Information Technology Services as certificates are deployed as part of our enterprise license agreement with InCommon. There is no charge to the University community who request digital certificates for the purposes of securing Internet traffic. The InCommon license entitles the University to an unlimited number of electronic certificates for all URI domains and servers.

Secure Sockets Layer (SSL) is a security protocol used to provide two-way encryption for unencrypted protocols like HTTP & FTP. SSL certificates also provide a way for clients to validate that the server or domain they are connecting to is authentic. The certificates are certified to work with all mainstream operating systems and web browsers.

Requests

Certificate requests can be sent to security@uri.edu with attached Certificate Signing Requests (CSR) generated with a key length of at least 2048 bits. ITS/Information Security staff may ask for validation of any request for service or record creation under this system. Validation would normally be by telephone to a department supervisor.

You must include:

- Server name
- Web server platform and version (e.g., Apache/Mod SSL, MS IIS)
- Name, address, email address, and phone number of the responsible person
- Appropriate CSR
- Certificate characteristics (e.g., duration typically one, two, or three years)

When filling out Certificate Information, you must specify:

- Organization: University of Rhode Island
- City/locality: Kingston
- State/province: Rhode Island
  - You must write out "Rhode Island" because "RI" is not recognized as a state
- Country: US

If your host name or website has multiple DNS entries, a separate certificate for each is not necessary. Please include Subject Alternative Names (SAN) in your CSR and note its use in your request.

What are Wildcard Certificates

In an effort to reduce university risk, the Information Security Office will not issue wildcard certificates for any production sub-domains.

NOTE: Most requests are processed within 24 - 48 hours. In some cases, it can take up to 72 hours for new requests to be fulfilled. Please plan accordingly.

Help

InCommon Certificate Service Support:

Certificate Service Support

Password resets: If you are an AAD, your password expires and needs to be changed every 90 days. The Certificate Manager will let you know when it's time for an update. If you are not in the CM regularly, we recommend you set a reminder on your calendar every 85 days or so to log...

InCommon Information Repository:

Certificate Service Repository

The following documents describe the operational practices and general terms and conditions for using the InCommon Certificate Service. The InCommon Certificate Service wiki includes additional technical information, Certificate manager administrator and user guides Sectigo maintains all of the following InCommon Technical Guides: Initiating Domain Control Validation (DCV) Introduction to Auto-Installer SSL Web Service API SSL...

Congratulations! You've successfully learned about InCommon Certificate Services