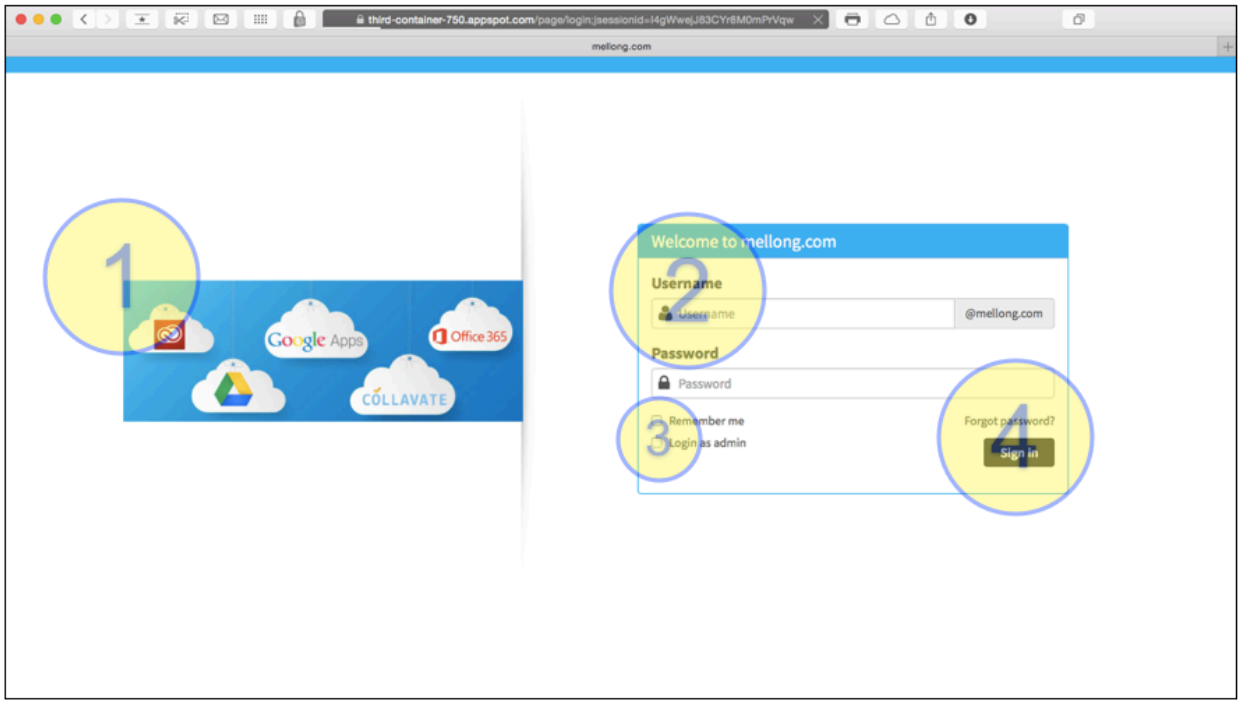
Killer ID Single Sign On App Admin/User Guide

NETKILLER

KillerID Quick Start and User Guide

A. Unified Login Page



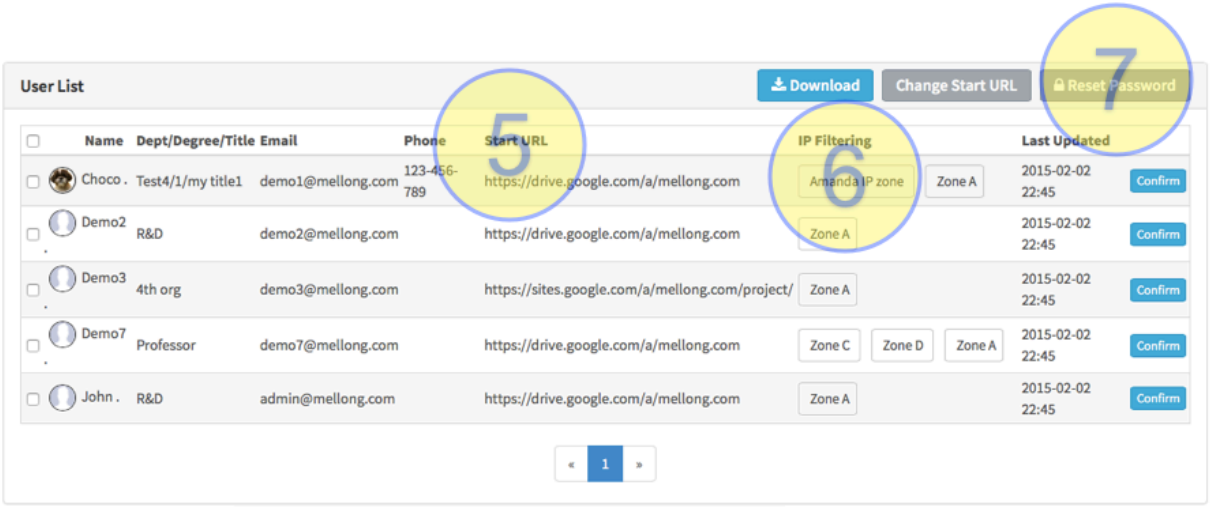
1. The Single Sign On page is optimized for both PC and Mobile devices. When using a computer, the organization's logo will appear on the left (1). The logo image is resized accordingly to device screen when using Single Sign On via mobile devices.

2. The login process is now simpler. Now, you can login using either an email address or an ID as seen in the screenshot above (2).

3. You can save your login ID (3), and administrators can sign in as administrators by checking 'login as admin' (3).

4. If you forget your password, you can retrieve it by having it sent to a backup email address (4). If you also forget the backup email address, you can ask your system admin to reset your password.

B. Administrator Mode: User Management Table

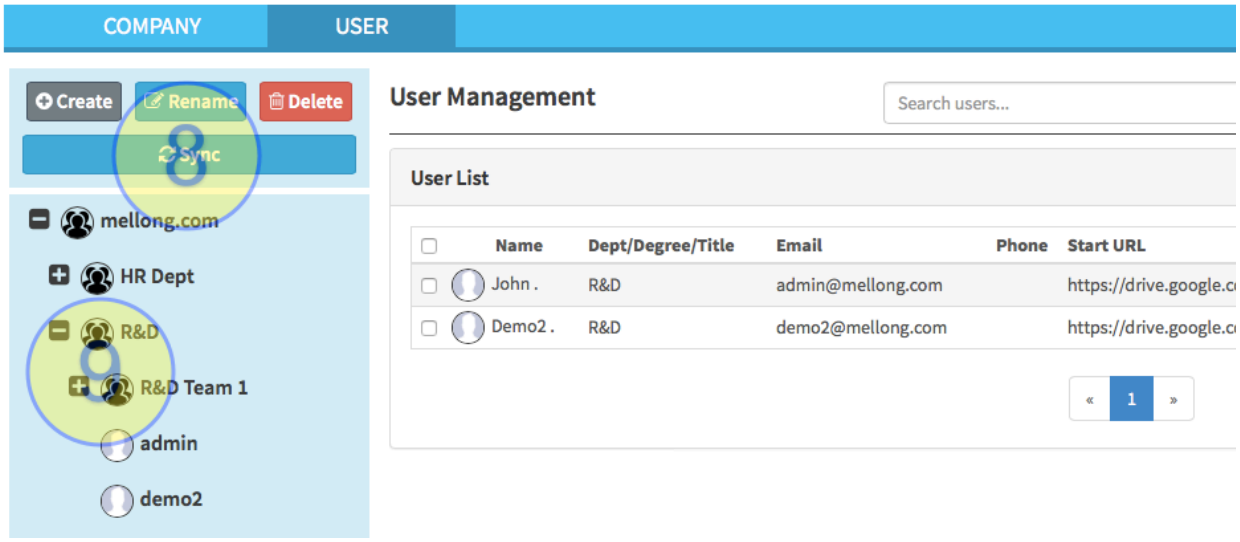


1. After synchronization with the users list in G Suite, users will be listed by organization/department.

2. Setup user's Start URL (5). You can set the address link for users to login directly to certain applications such as G Suite, the Company's Portal, or an Intranet.

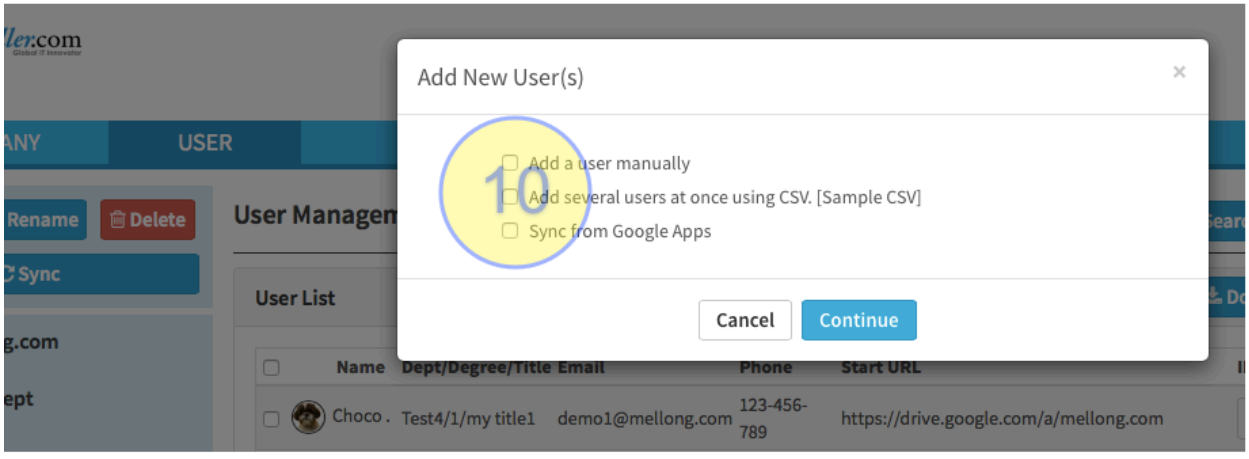
3. You can add an IP Filter so that only users logging in from certain IP addresses can access the system (6). The administrator can create and set a range of IP addresses and allocate those to certain teams or individuals.

4. The system admin can reset passwords of selected users (7).



5. By clicking the ‘sync’ button (8), you can log into your Killer ID and load your G Suite organization chart information.

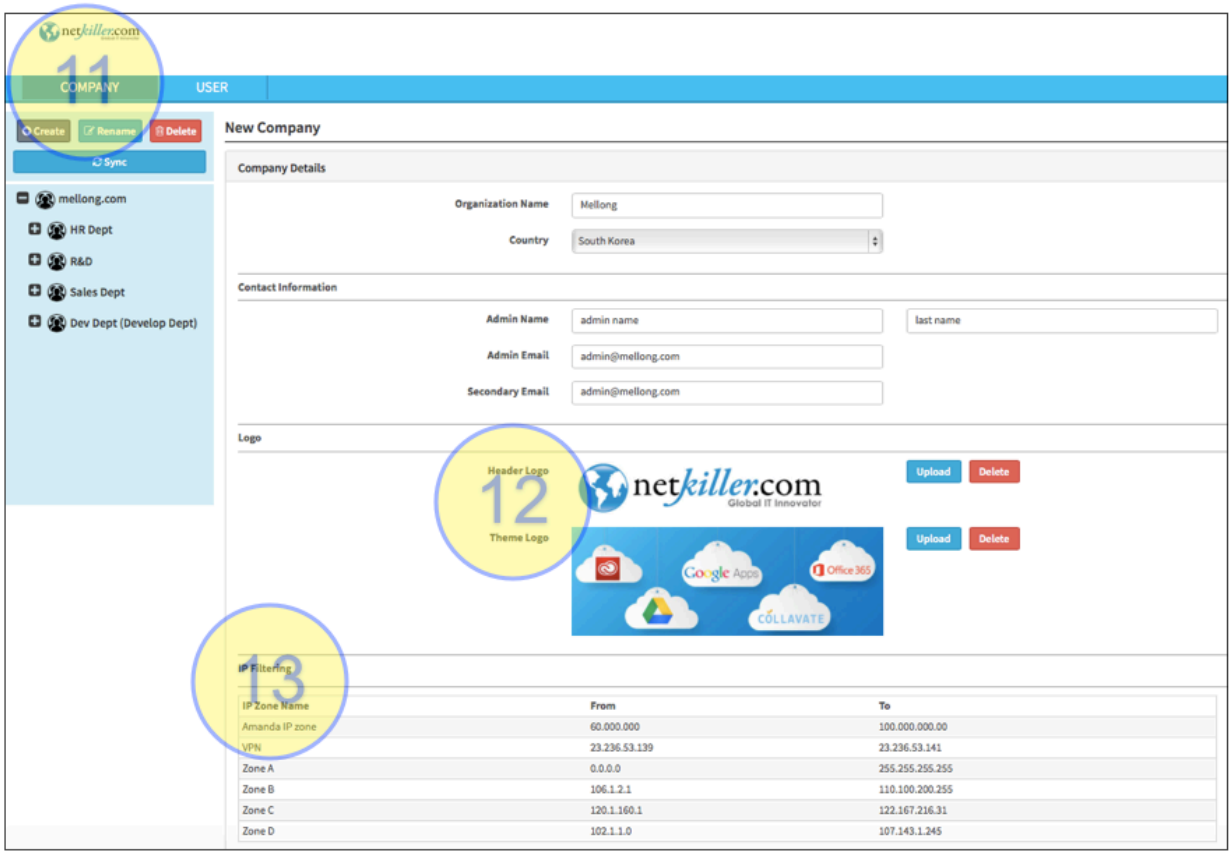
6. By clicking on the ‘+’ or ‘-’ buttons you can look at hierarchical relationships. By clicking on a certain organization, you can view users of that organization (9).



7. You can add users in three ways by clicking ‘Add New User(s)’:
    i. Add a user manually;
    ii. Add several users at once using CSV; or
    iii. Sync from G Suite.

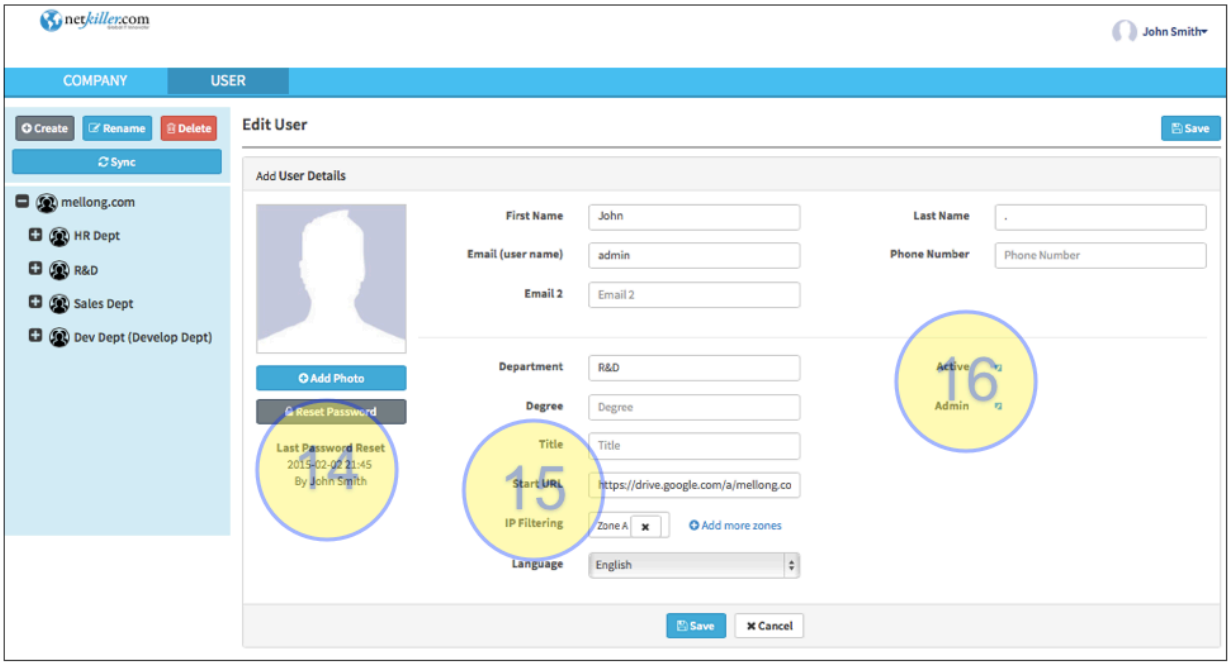
Using CSV is especially convenient for setting up users' personal information, password, and start URL when there are many users to add at once.

*** Note**: To download the CSV file, please use the 'Download' feature located in the User list.



8. Within the COMPANY tab (11), you can upload a company profile, theme and/or logo (12). The full logo appears upon logging in on a PC, and just the logo header appears when using a mobile device. The default image setup in G Suite appears if the administrator does not upload a logo.

9. You can setup an IP Filter to limit access to certain IP addresses (13). These limits are necessary to protect the domain from unwanted intrusion and distractions.



10. With the ‘User Detail’ page, you can check the time when the profile photo was uploaded, or when the last password changes were made (14). Backup email for password retrieval and personal details are also inputted here.

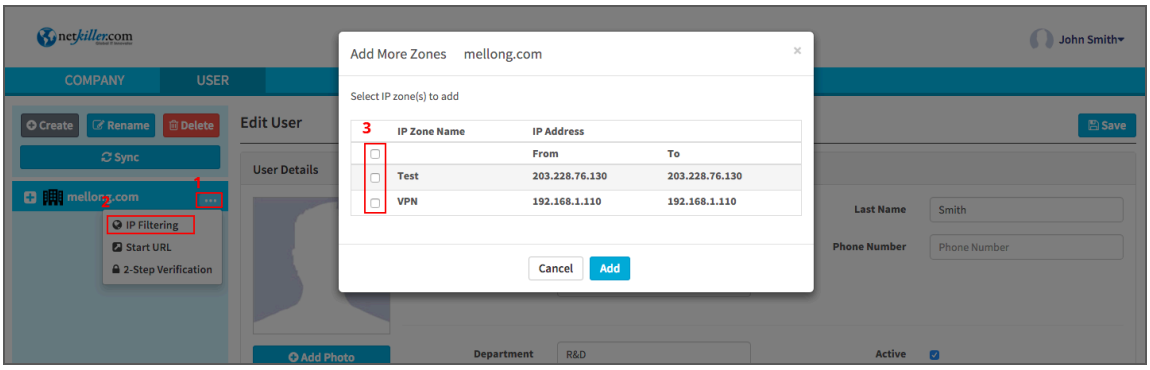
11. Set up the Start URL and IP zones for each user here (15).

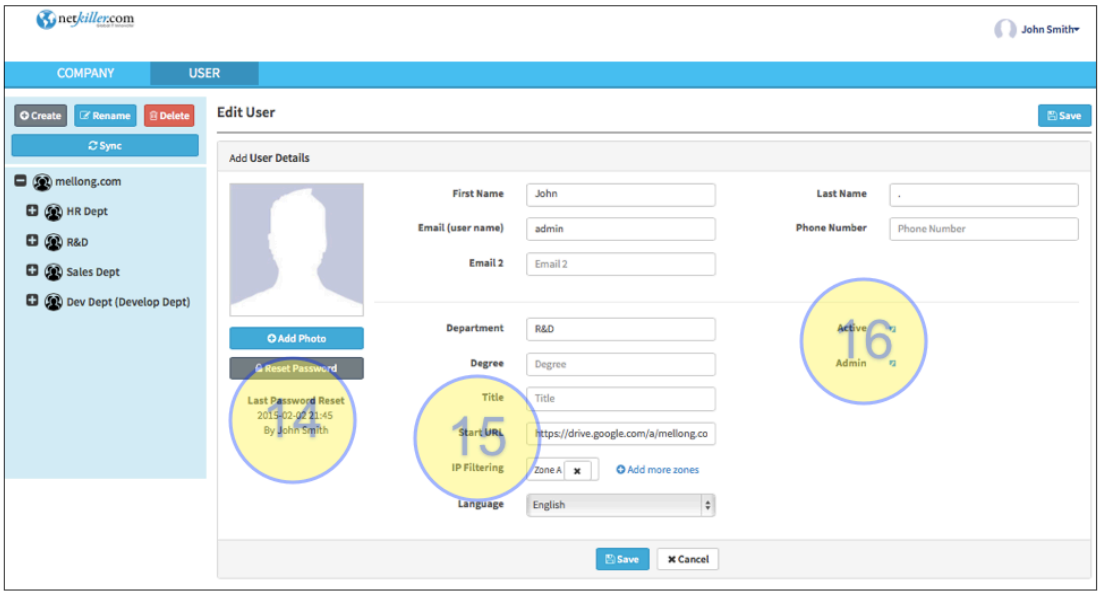
12. You can manage access of the account and also set a user as the systems admin if necessary (16).

13. Preset IP zones to assign login IP zones for each user here (13). Administrators can assign preset IP zones to specific users to deny access from set IP zones to easily control access.

<u>Organization/Domain-wide IP filtering setup</u>

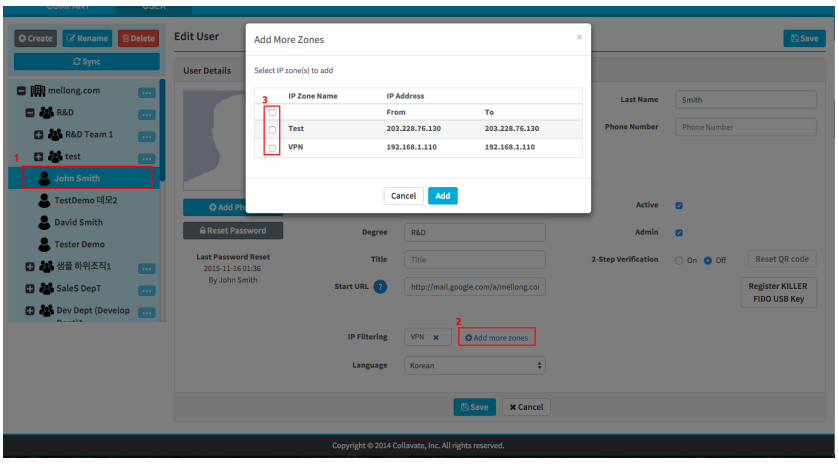
- From the left side of the USER tab, click on the first listed organization (or a specific organization) to setup IP filtering.
- Clicking on the first listed organization will apply the settings to all users within your domain





14. In the Add User Details page, a user's profile image can be uploaded and the history of password changes can be viewed (14). Password recovery email and detailed personal information can be added as well.

15. A user's Start URL and IP Zone can be assigned selectively (15).



User-by-user IP Filtering

- From Killer ID Admin Console, Go to USER tab, then select a user from the left. Next, click Edit on the top-right corner. Then go to IP filtering section and select a specific IP Zone for the user.

The user's IP access will be limited to the set IP Zone.

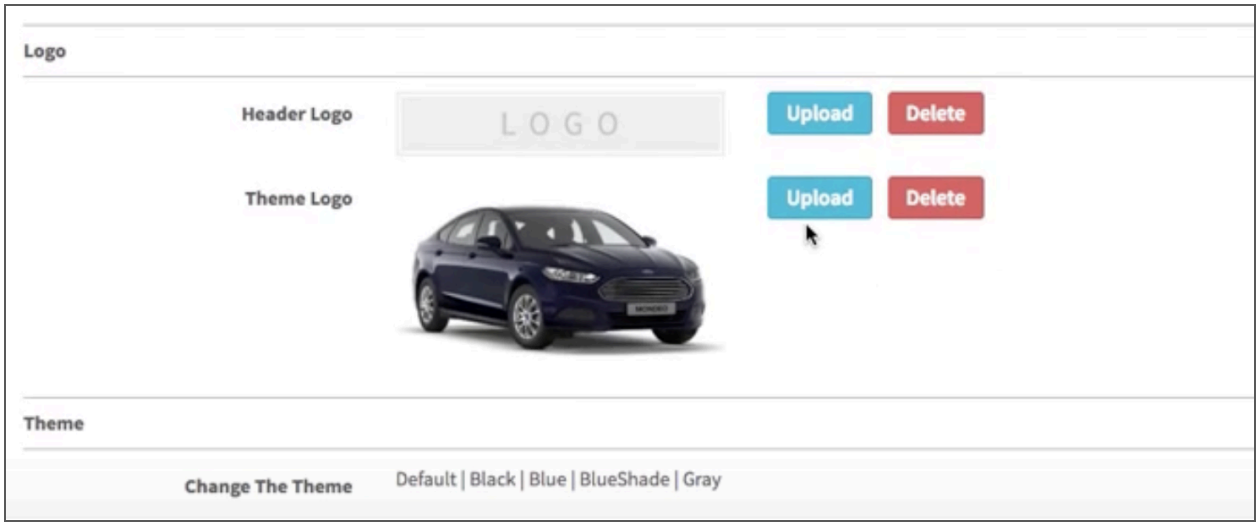
16. The user can be activated or assigned administrator role (16).

17. Password expiry policy can be set to require passwords for individual accounts to be changed every set interval of days. The interval can be customized by entering in the number of days in the "Enter the Days" box. The policy can be enforced or disabled by turning "Password Change Rule Setting" On and Off.

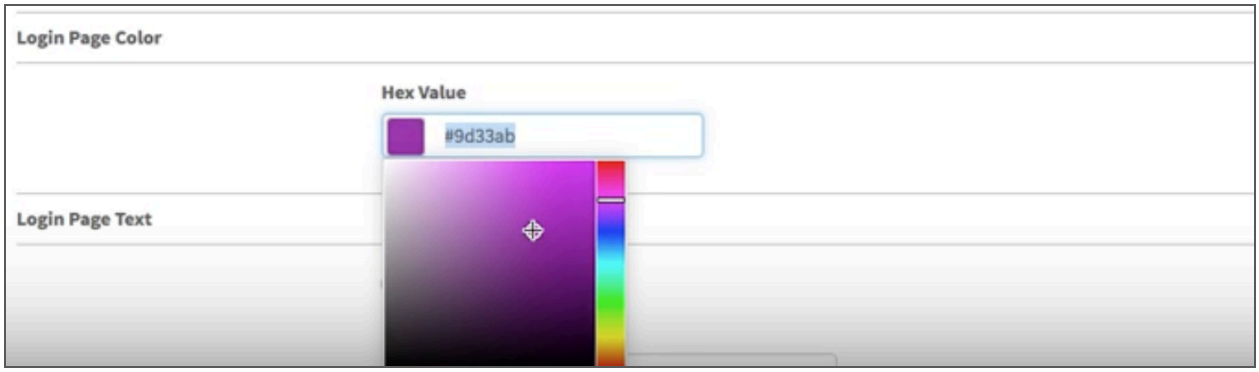
C. Unified Login Page Theme Customization

An admin can customize the login page to fit the company's logo or color themes.

Go to Company tab and located the Logo section. Then upload Header and Theme Logo. Also, you can change the theme to Default, Black, Blue, BlueShade, and Gray.

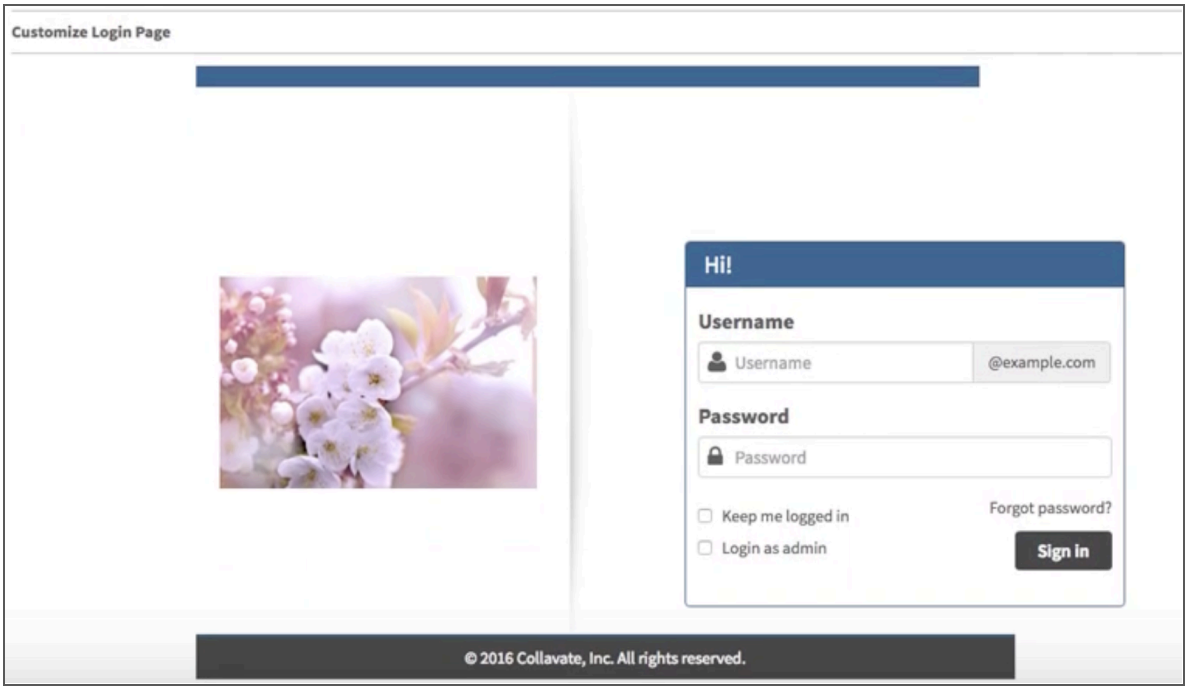


You can customize the theme palette by going to the Login Page Color section and choosing the color from the palette or inputting the web color code.



You can also edit Login Page Text. From the "Login Page Text" section, change the welcoming message by typing your greeting message into the "Customize:" box.

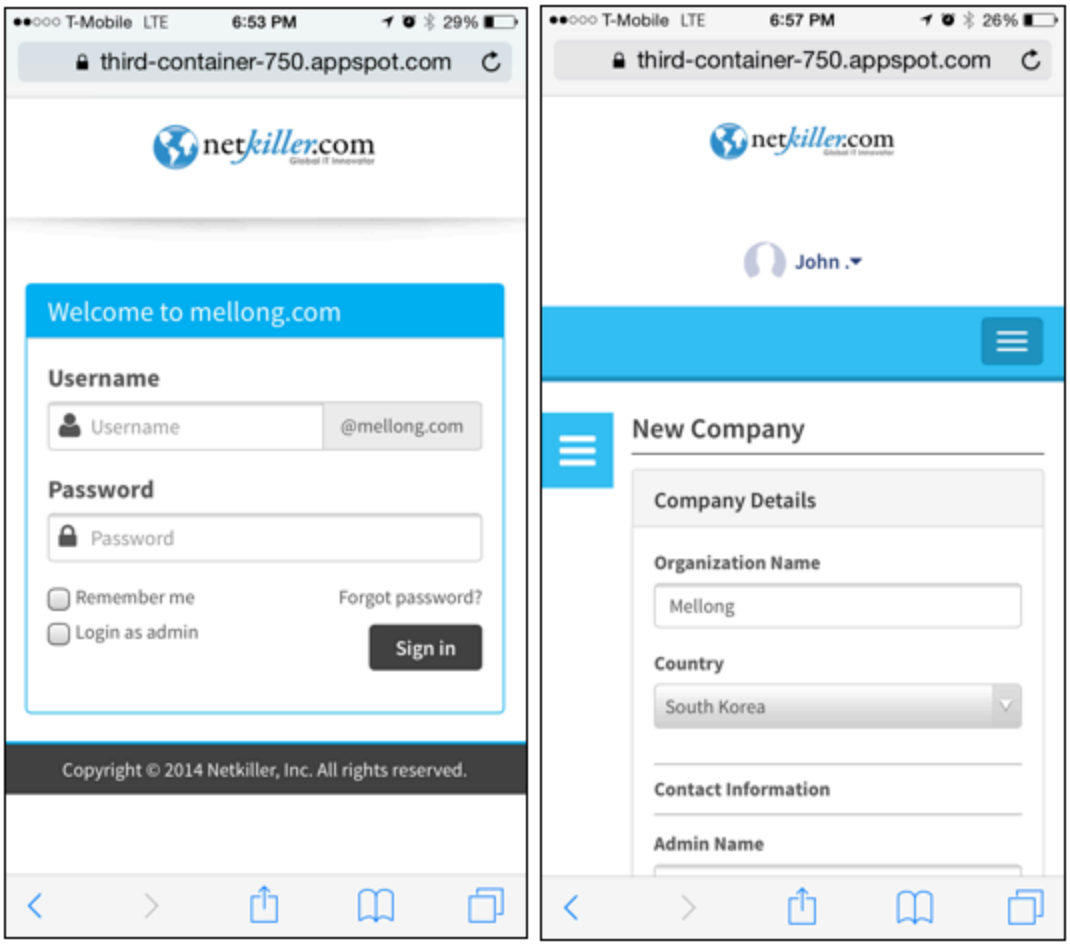
Changes can be previewed from the “Customize Login Page” section.



To apply such changes, click “Save” below.

D. Mobile User Support

When a user logs in to G Suite via mobile web browser, Killer ID login is activated as it would in a PC environment. When using a smartphone, an optimized login screen appears (see below), and takes you to the Start URL when successfully logged in.



[The system admin can manage the company's profile information, and also manage users in a mobile environment.]

Sign in to your G Suite account via Killer ID in Android:

Here is how to add your G Suite account using Killer ID:

1) **Android 2.1-2.3 users:**
    a) Go to Settings > Accounts and sync > Add account > Google and select Next.
    b) In the bottom corner, select Menu > Browser sign-in.
    c) In Google global login page, type in your username@domain and password and click Sign In.
        i) Your password doesn't have to be correct here.
    d) The page will be redirected to Killer ID login page.
    e) Type in your Killer ID username and password and click Sign In.
    f) Permit Grant Access if you're asked to grant access for your device (so it can stay signed in to your account).
    g) Your account will be added to your Android device.

2) **Android 3.0-4.4.4 users:**
    a) Go to Settings > Add account > Google and select Next.
    b) Select Existing account > Menu > Browser sign-in.
    c) In Google global login page, type in your username@domain and password and click Sign In.
        i) Your password doesn't have to be correct here.
    d) The page will redirect to Killer ID login page.
    e) Type in your Killer ID username and password and click Sign In.
    f) Permit Grant Access if you're asked to grant access for your device (so it can stay signed in to your account).
    g) Your account will be added to your Android device.

3) **Android 5.0+ users:**
    a) Go to Settings > Accounts > Add account > Google.
    b) Enter your G Suite email address, leave the password field blank, and click Sign in.
    c) You will be redirected to your KillerID login page. Enter your Killer ID username and password here.
    d) Permit Grant Access if you're asked to grant access for your device (so it can stay signed in to your account).
    e) Your account will be added to your Android device.

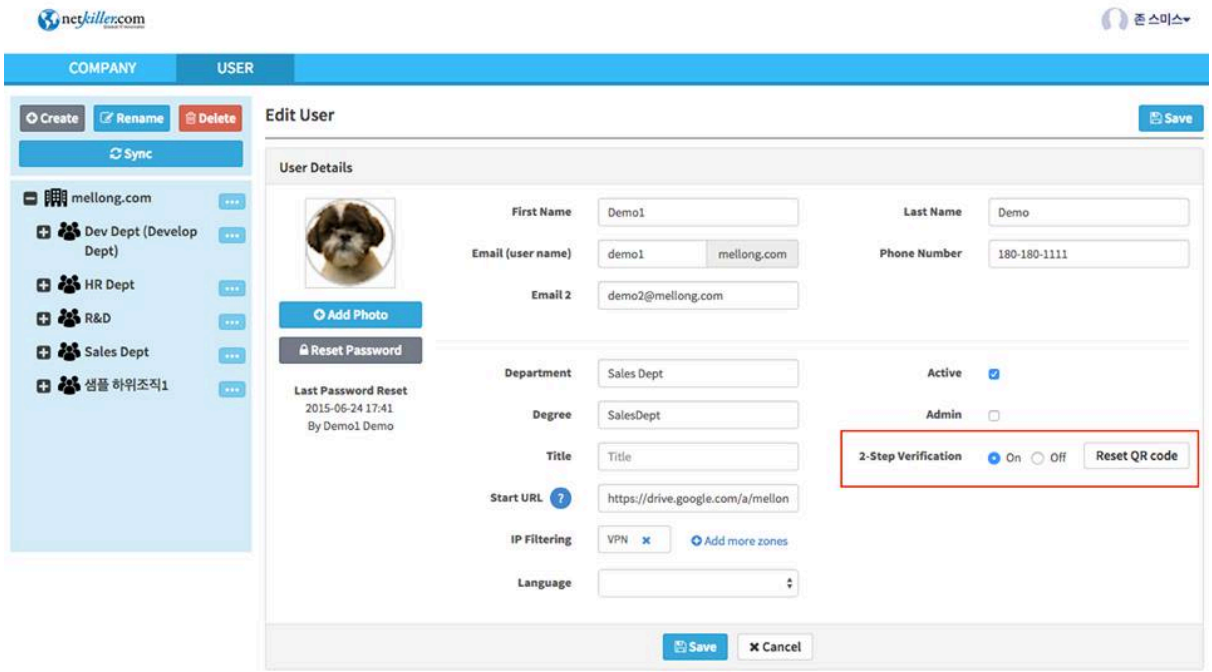
E. Setting up Killer ID’s 2-Step Verification

Two step verification feature requires you to enter a temporary password after you login to maximize the security. KillerID’s 2-Step Verification is created using Google’s OTP feature. With this, users can use KillerID without having to sacrifice safety and security, which Google’s OTP provides.

[Killer ID’s 2-Step Verification Procedure]

Step 1.

An administrator can activate/deactivate the two-step verification feature at the user level or on an organizational level.

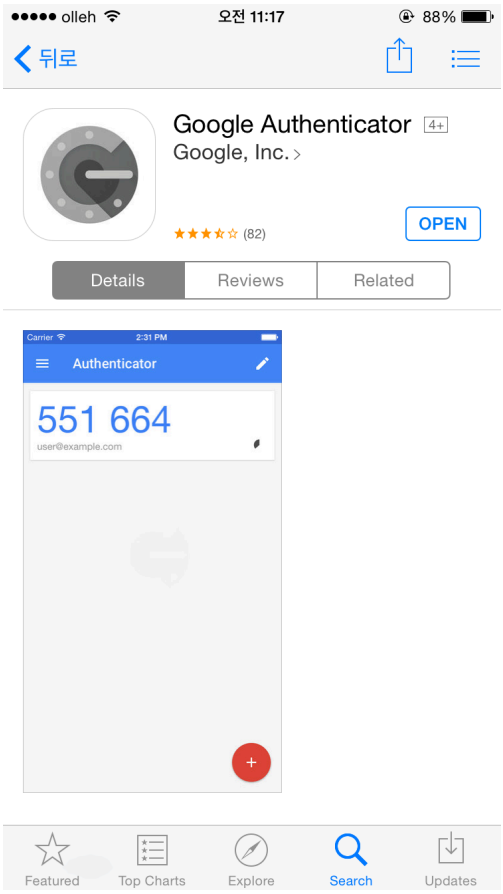


The administrator can reset the two-step Verification code for each user.

Step 2.

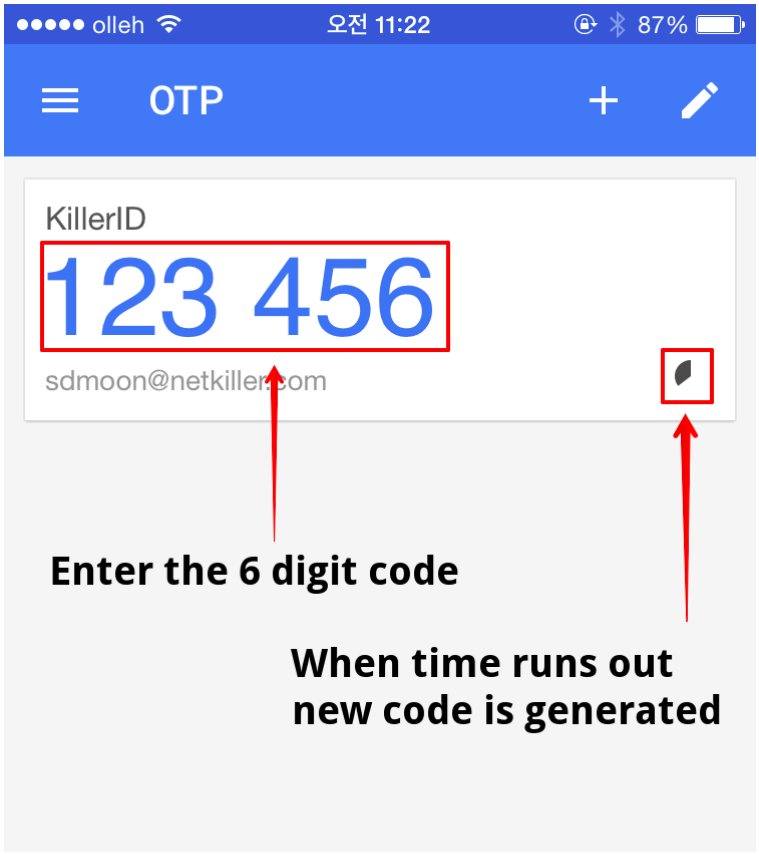
To use Killer ID’s 2-Step verification, install Google’s OTP application on your smartphone.

* Android: https://goo.gl/uhjTu
* iOS: https://goo.gl/uE5QvK



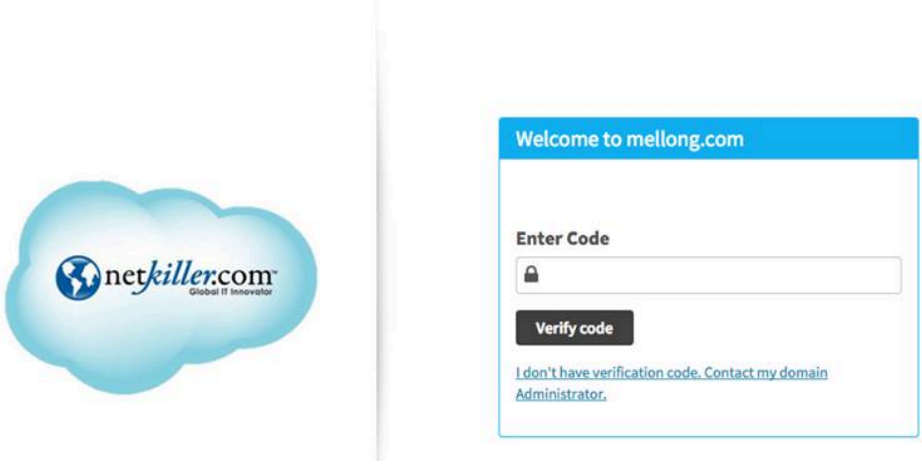
Step 3.

Activated users will see a QR code when logging into Killer ID for the first time. By scanning the QR code, the Killer ID code (6 digits) is then added to the Google Authenticator.



Step 4.

Enter the 6 digit code on the OTP application and login.

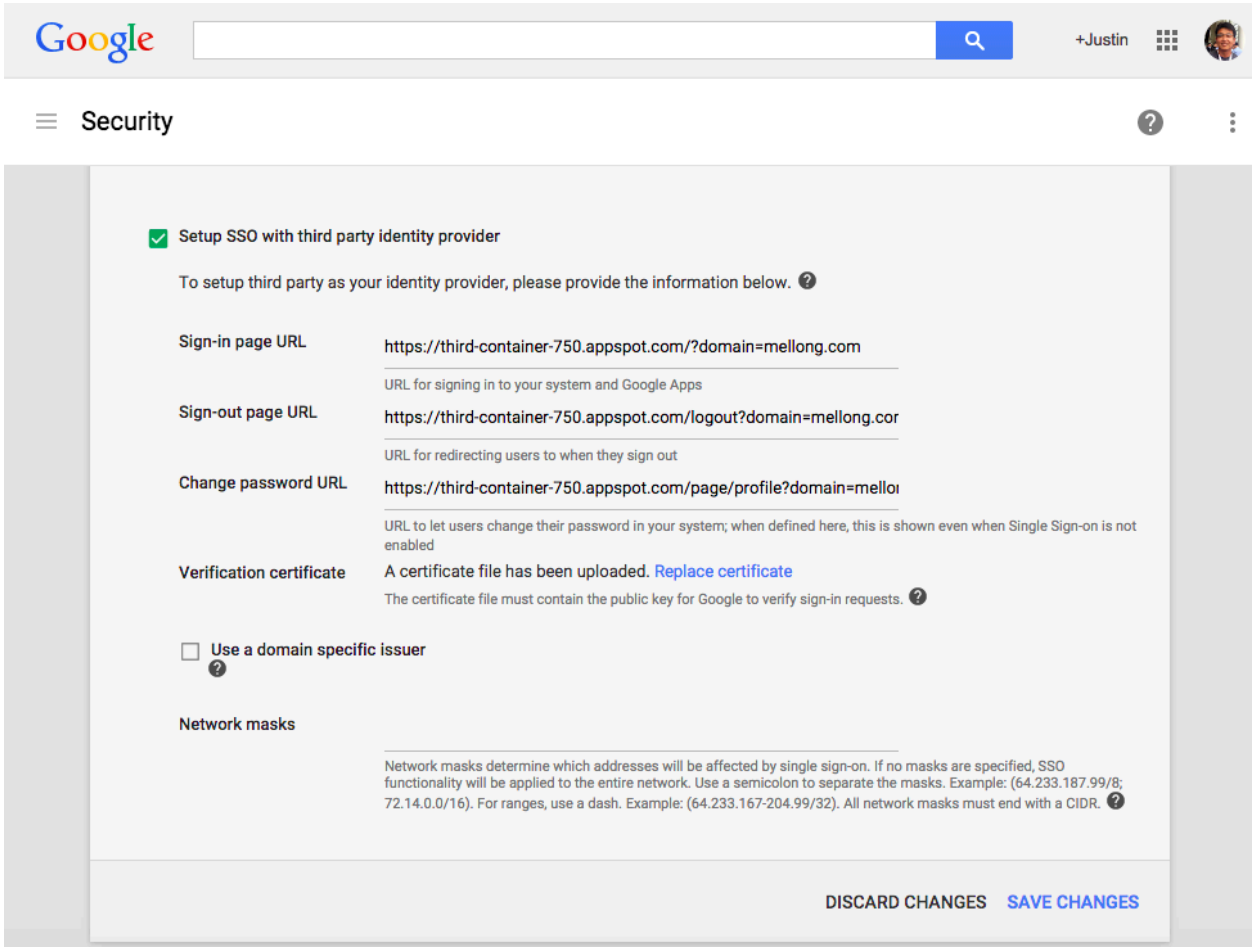


* Backup codes that can be used when you don't have access to your phone. SMS OTP will also be available very soon.

Contact us and experience the fortified security feature of **Killer ID** now!

F. G Suite Setting - Synchronization with Killer ID Single Sign On Service

You can setup Killer ID by going to the Single Sign On Settings menu within the G Suite's Admin Console. (Security > Set up single sign-on (SSO) section)



After turning on Killer ID and uploading the key from the Verification Certificate, enter the information below in each section.

** **Note #1**: This key is provided by Netkiller Support Team via email.*

- Sing-in page URL: https://id.netkiller.com/a/**mellong.com**
- Sign-out page URL: https://id.netkiller.com/a/**mellong.com**/logout
- Change password URL: https://id.netkiller.com/page/a/**mellong.com**/profile

> *** Note #2**: The domain name, mellong.com, which appears in the links above, is a placeholder and should be replaced with the organization's domain. For example if a company's G Suite main domain is abc.com, you would replace mellong.com with abc.com.

When logging into G Suite after setting up Killer ID, the user will be directed to the Single Sign On login screen: (https://id.netkiller.com/a/**mellong.com**), instead of the normal G Suite login site

When a user logs out of G Suite, he or she will be redirected to the Killer ID service screen. When a user needs to change their password, the user will be directed to the Killer ID password settings page.

> *** Note**: When using Killer ID, the G Suite administrator logs in using Killer ID by default. However, logging in using a normal Google screen instead of the Killer ID screen is also possible for situations where accessing Killer ID may not be possible. The Killer ID administrator does not have to be the G Suite Super Admin unless the Super Admin wants to synchronize G Suite with Killer ID.

G. Separate Password for each G Suite Application

G Suite has a two-step verification process for setting/changing password individually for each application. With Killer ID, a two-step verification process is not necessary, and you are still able to set individual passwords for each application.

Killer ID only unifies the login process in G Suite. It does not directly control the login processes for applications with their own protocols such as IMAP, POP3, Outlook or other email applications.

G Suite users using Killer ID can use an independent password when accessing other applications. Those users will have no problems using G Suite related mobile apps.

H. KillerID and VPN Connection

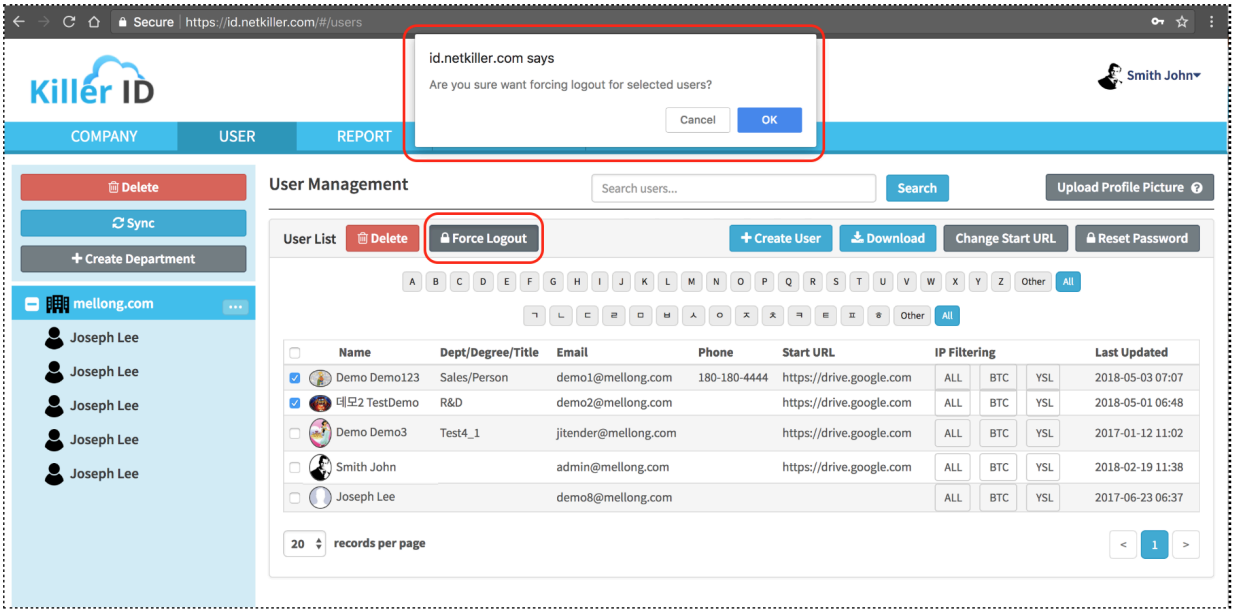
Killer ID's IP allocation feature is even more effective when used together with VPN.

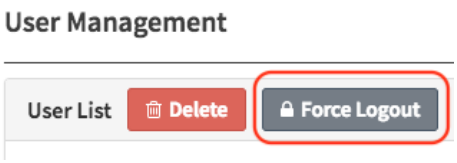
Such a connection allows the domain admin to set login parameters that only allows login from within the company. When users are outside of work, you can set the IP protocols so that they can only login using the company's VPN.

For VPN options, Netkiller recommends Open VPN. This is an affordable VPN service, and in such areas as China where G Suite access is not guaranteed, you can login to Killer ID only through approved VPN service providers.

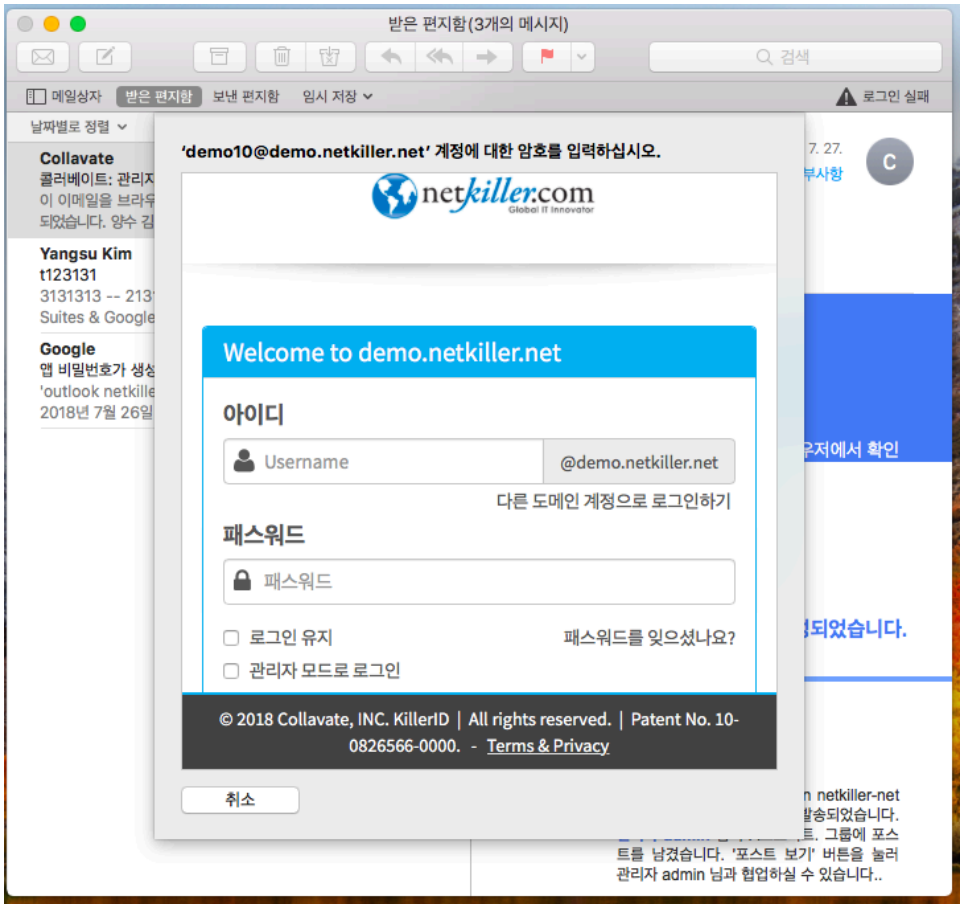
I. Enforcing Session Logout

With KillerID's session logout feature, admin can log out all sessions of G Suite users . Admin can select user(s) and click 'Force Logout' button to immediately log out all sessions of selected user(s).

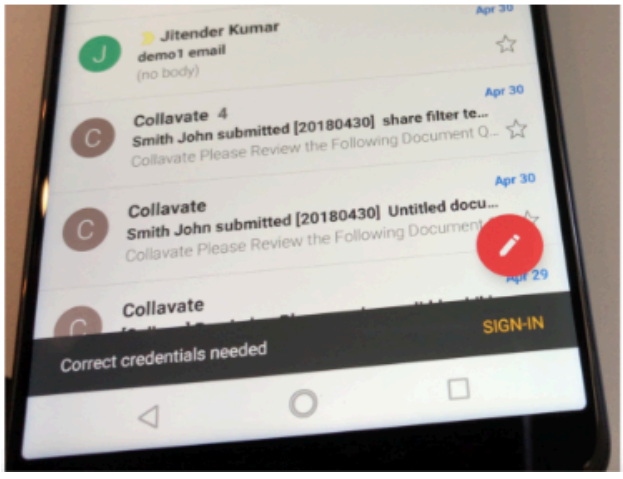


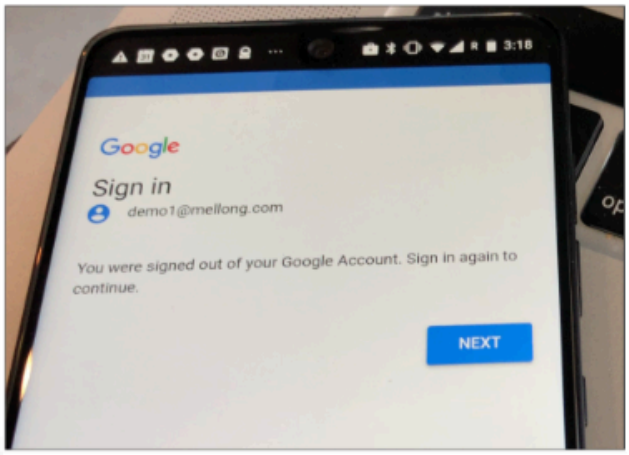


Select the target users to apply and press the Force Logout button. Those users will immediately log out from the desktop web browsers, PC sync app as well as mobile devices as shown in the screen below.



<Instant logout from Email clients such as Apple mail, Outlook, Thunderbird>





<Instant log out from iOS & Android Phones>

Even if G Suite MDM (Mobile Device Management) is configured on the smartphone, logout is immediately executed as shown in the screen above. G Suite user may can login again with user's Killer ID credential.

Automated Timeout during non-business hours or policy setup for session timeout function will be available in near future. (Or, can be customized with additional fee, upon request)

http://www.netkiller.com