Configuration Guide
Proofpoint VAP

Version 1.0
September 2019

Okta Inc.
100 First Street
San Francisco, CA 94105

info@okta.com
1-888-722-7871

Table of Contents

What Is This Document

This document is intended for Okta sales engineers, partners, and or customers looking to understand and configure the Okta and Proofpoint Very Attacked People (VAP) integration.

Who Is Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,000 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 6,550 organizations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers.

Who Is Proofpoint

Proofpoint, Inc. (NASDAQ:PFPT) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps customers around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including over 50% of the Fortune 1000, rely on Proofpoint to mitigate their most critical security and compliance risks across email, the cloud, social media, and the web. No one protects people, the data they create, and the digital channels they use more effectively than Proofpoint.

What Is a VAP

A VAP–or a Very Attacked Person–is a user who has been identified by Proofpoint's TAP product as being highly targeted by attacks and/or are highly susceptible to attacks.

Proofpoint offers Targeted Attack Protect (TAP) which helps you stay ahead of attackers with an innovative approach that detects, analyzes, and blocks advanced threats before they reach your inbox. This includes ransomware and other advanced email threats delivered through malicious attachments and URLs; As well as zero-day threats, polymorphic malware, weaponized documents, and phishing attacks.

One of the features of TAP is the ability to produce an Attack Index for a user. When a threshold of Attack Index is reached, a user is known as a Very Attacked Person or **VAP**.

Your security teams need to know who your most attacked people are in order to protect them against the threats that target them.

The Proofpoint Attack Index helps identify these targeted people. It also surfaces targeted or interesting ransomware threats from the noise of threat activity that you see every day. This index is a weighted composite score of all threats sent to an individual in your organization. It scores threats on a scale of 0-1000 based on four factors:

- Threat actor sophistication
- Spread and focus of attack targeting
- Type of attack
- Overall attack volume

With the Attack Index, you can understand the risks your users face. You can then prioritize the most effective way to resolve threats. You also receive reporting and metrics to assess both individual and overall user risk.

Focused Security with Okta and Proofpoint's VAP

With Okta as the center of your digital world, you can now apply focused security controls on the users who need it the most. The benefit of applying focused security controls should appeal to anyone who has ever had to deploy more stringent security policies to a broad audience, and especially to those who had to rescind those same policies due to negative user impact.

The integration between Proofpoint's VAP and Okta allows an administrator to synchronize the users that Proofpoint has identified as Very Attacked with a group in Okta. This group can then be incorporated into various policy enforcement rules in Okta allowing an Okta administrator to extend additional levels of protection to these Very Attacked People.

When set up, the integration will create a group in an organization's Okta org named **VAP Group**. This group will be populated and synchronized once per day.

The setup of the integration is performed by Proofpoint support on behalf of the organization.

When the synchronization runs daily it will:

- Identify the users that are in the 90 day VAP list and add them to the **VAP Group**
- Identify the users that are in the 7 day VAP list and add them to the **VAP Group**
- Remove users who no longer meet this criteria

To enforce policies an admin should refer to the following for guidance and suggestions on appropriate mitigation steps to take.

- This document
- Okta product documents relative to:
    - Sign-on
    - Recovery
    - App assignment
    - App access
    - Factor enrollment
    - Factor enforcement
    - Password policy
    - Group push

Configure Proofpoint

Follow the steps below to collect the information required by Proofpoint

Proofpoint requires your Okta Org URL and an API Token to enable this integration. The API Token will be used to create the **VAP Group** group within Okta and will subsequently add and remove users from that group. The minimum Okta privilege required by this integration is Group Admin. Once the **VAP Group** has been created you can further reduce the scope of privileges by restricting the API Token user to only administer the **VAP Group.**

Generate an API Token for Proofpoint

1. (Optional) Create a “Service Account” user in Okta
2. Assign a minimum of the Org Admin (or Organization Administrator) role to the target user
3. (Optional) Sign into Okta as the newly created user
4. Follow this guide to Create an API Token
5. Provide API Token and Okta org URL to Proofpoint support
6. (Optional)
    a. After the Proofpoint setup is performed, change the Okta role of the Service Account user to a Group Admin AND only allow updates to the **VAP Group**

Configure Okta: Suggestions

Review the steps below to get an idea of the policies you can apply to the **VAP Group**

Okta policies allow control of various elements of security, including end-user passwords, the authentication challenges a user receives, the devices they can use, and from what locations. A policy can be based on a variety of factors, such as location, group definitions, and authentication type.

In this section we will provide general guidance on policies that could logically be applied to your **VAP Group** based on the reasons users would be members of the **VAP Group**–they are presumed to be at a higher degree of risk than other users in the organization.

- ❏ Strict Password or Account Recovery Policy
- ❏ High Assurance Factor Enrollment
- ❏ Require MFA on Sensitive Applications
- ❏ Restrict Access to Highly Sensitive Applications
- ❏ Assign an Informative Bookmark

These policies are suggestions only and not intended to be an exhaustive list. You should evaluate the needs of your organization and users when considering policies, and then combine the advanced features from Okta like Dynamic zones, ThreatInsight, Behavior and Risk based conditions with the Proofpoint VAP integration to create a security policy custom tailored to your organization. The result will be increased security without the sacrifice of useability. (No, not all heroes wear capes; if you do, that's ok too.)

*Use your **VAP Group** as an early pilot group*

Zero Trust theory says we should trust nothing and verify everything. Zero Trust is also a journey and taking a step forward is better than standing in place while planning the perfect leap. With that in mind you can think of your **VAP Group** as an early pilot group for deploying new policies. The process of testing and getting feedback on new policies can take on a life of its own. Incorporating the **VAP Group** as an early pilot audience in your process will help extend the protections offered by new policies to the group most in need as soon as possible.

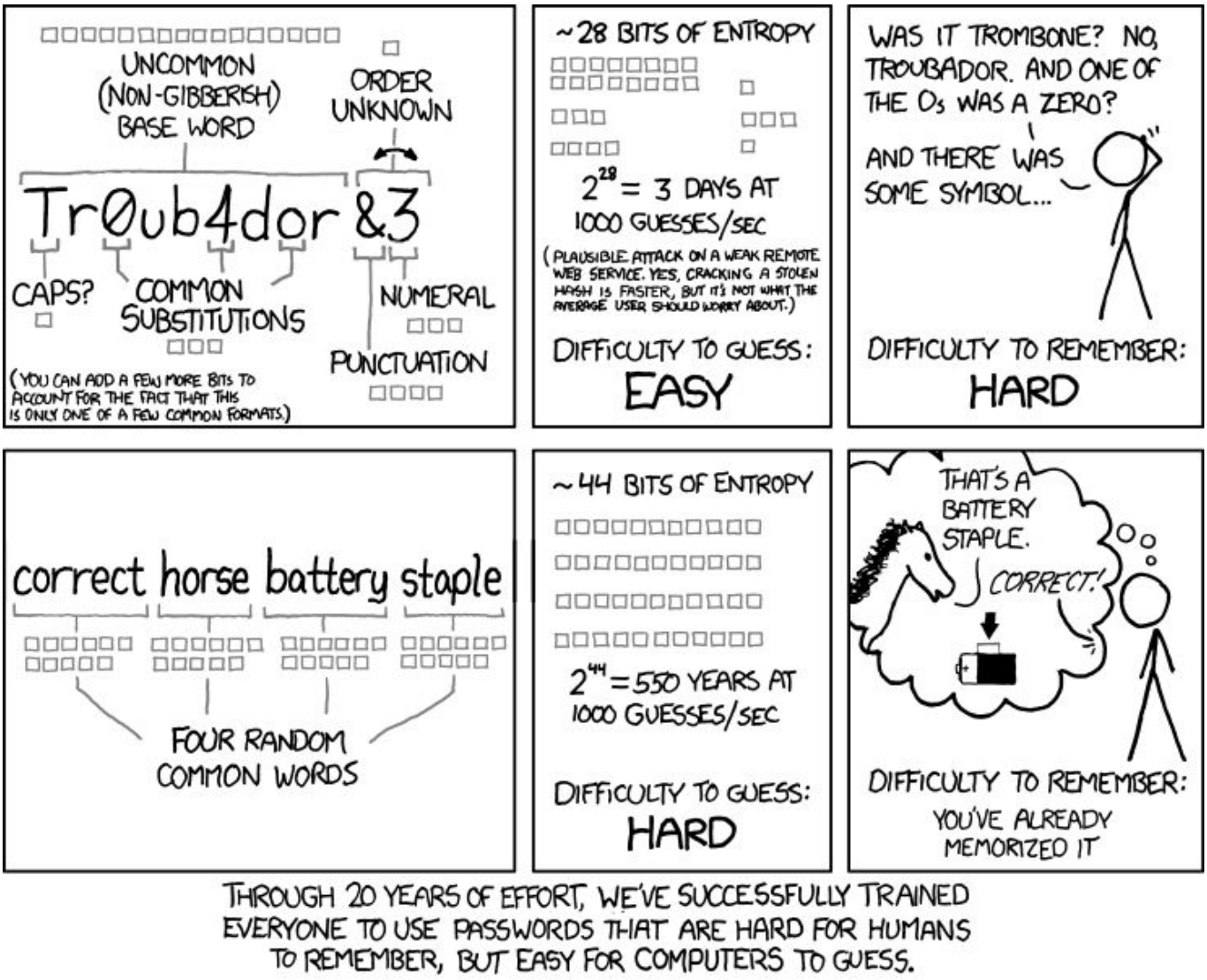
Strict Password Policy

Refer to most recent guidance such as NIST or PCI that is relevant to your company or industry.

Recent studies show that increased character complexity requirements actually reduce password strength and worse, encourage users to adopt bad password practices.

A strict or otherwise differentiated password policy can be useful to protect these Very Attacked People in your organization.

Consider longer length passwords or passphrases like *correct horse battery staple*:

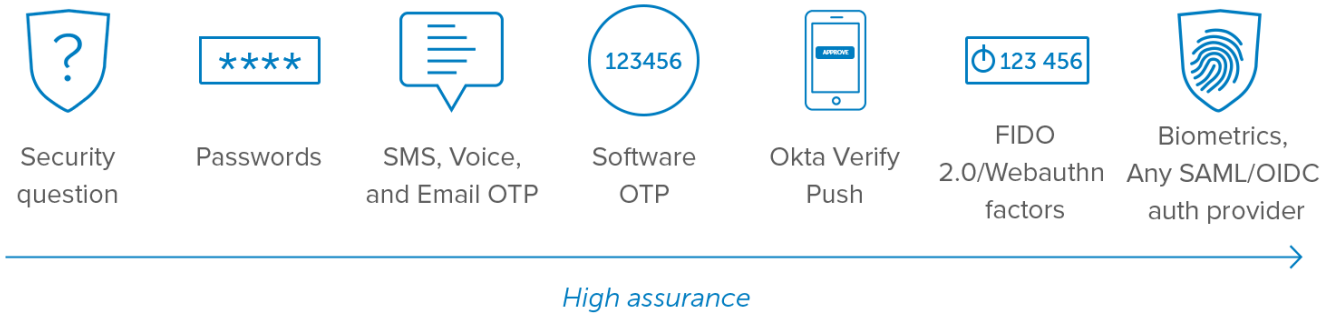


(Image source: xkcd.com, Password Strength, Creative Commons CC BY-NC 2.5)

Follow the **Creating Group Password Policies** section of Okta's Security Policies Product Documentation. When creating the Group Password policy, apply it to the **VAP Group** and configure as a higher precedence policy than would otherwise apply.

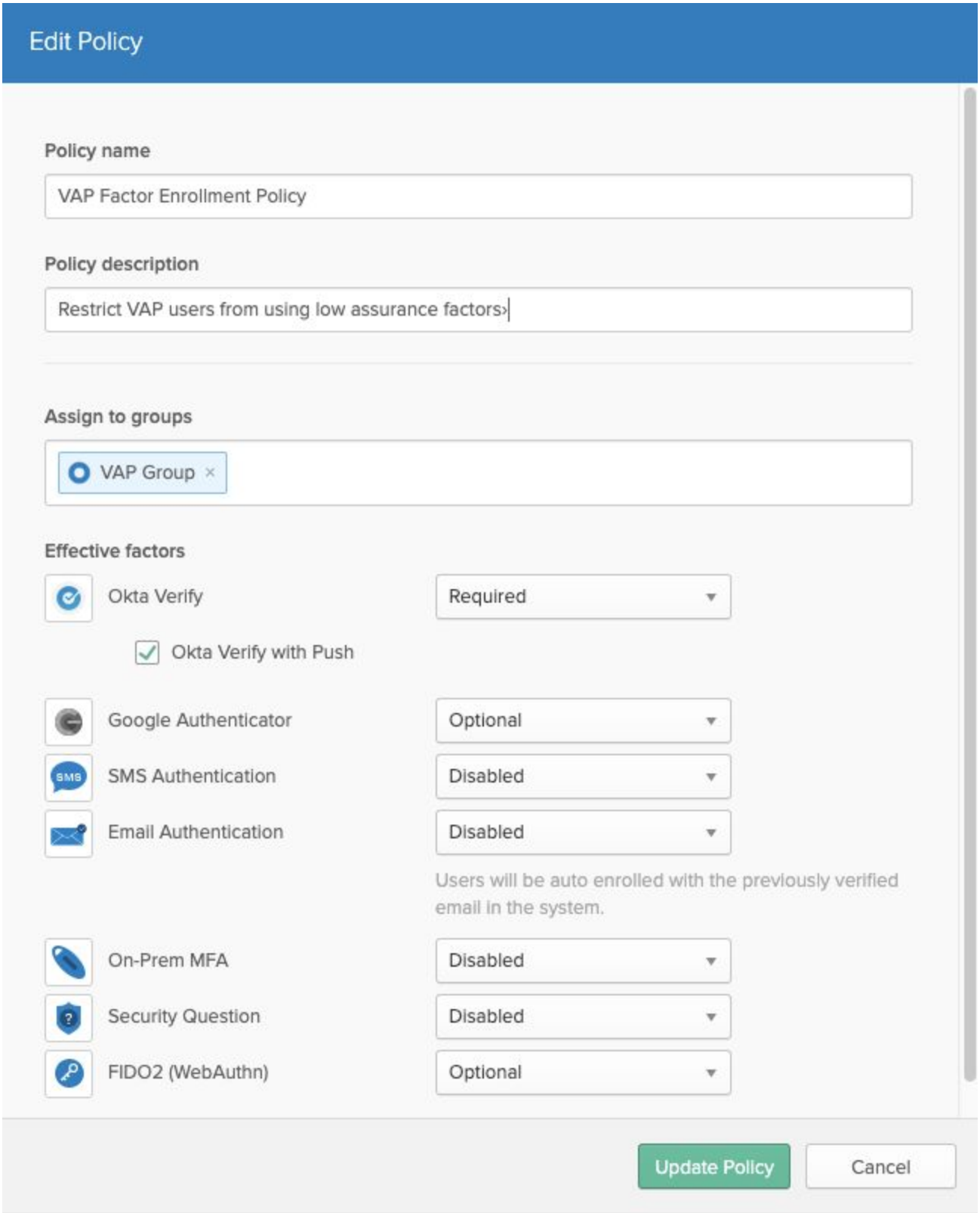
High Assurance Factor Enrollment

Any factor is better than no factor, but not all factors are created equally.

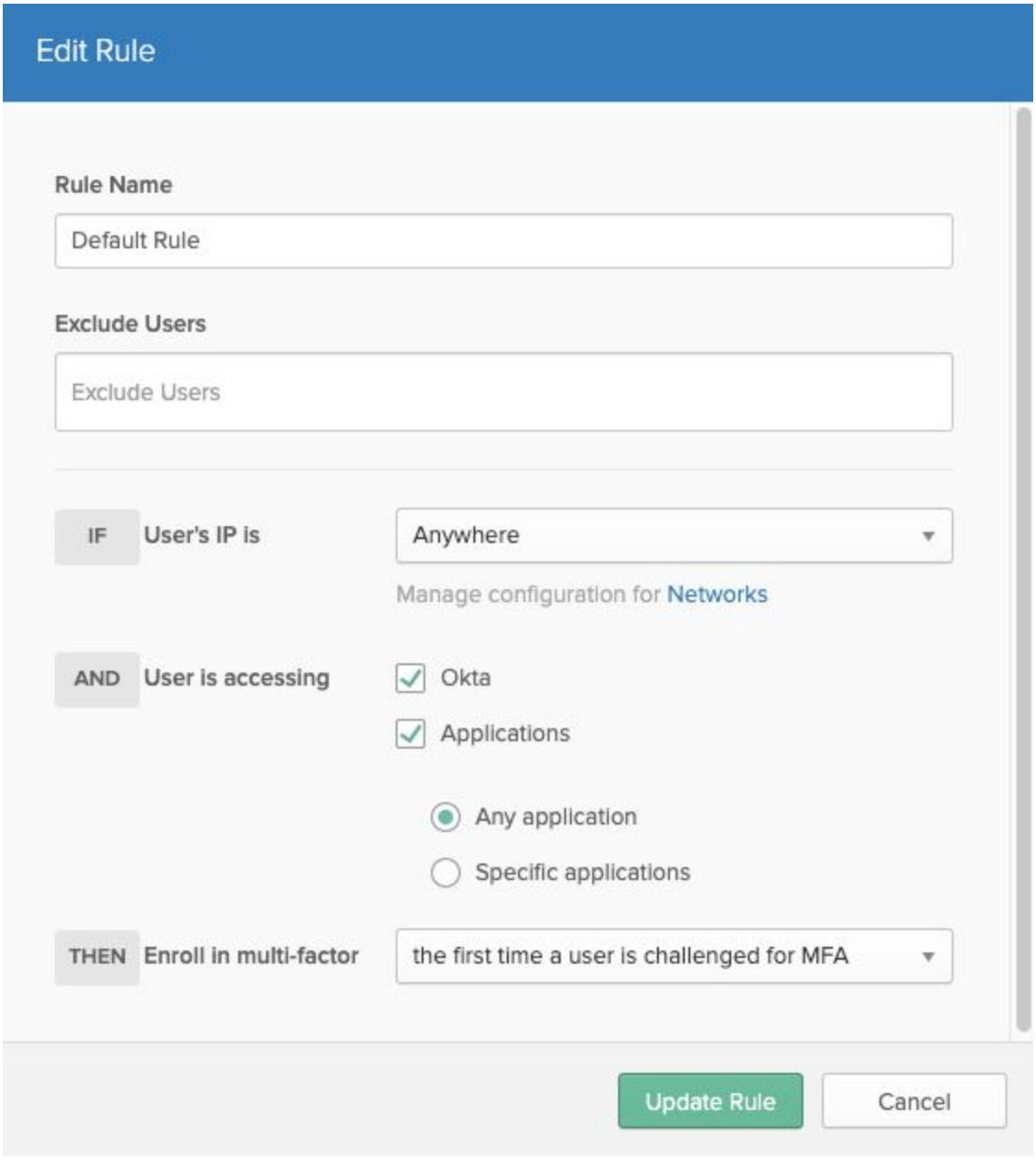


It isn't always practical to do widespread enforcement of high assurance multifactor authentication; applying the high assurance requirements to your Very Attacked people will give you the most "bang for your buck" by protecting those users facing the most imminent threat.

Follow the **Multifactor Policies** section of our Multifactor Authentication Product Documentation. When creating the Factor Enrollment policy apply it to the **VAP Group** and configure as a higher precedence policy than would otherwise apply.



In addition to defining the entitled factors you can also define rules to control the behavior of when and how enrollment occurs.



Require MFA on Sensitive Applications

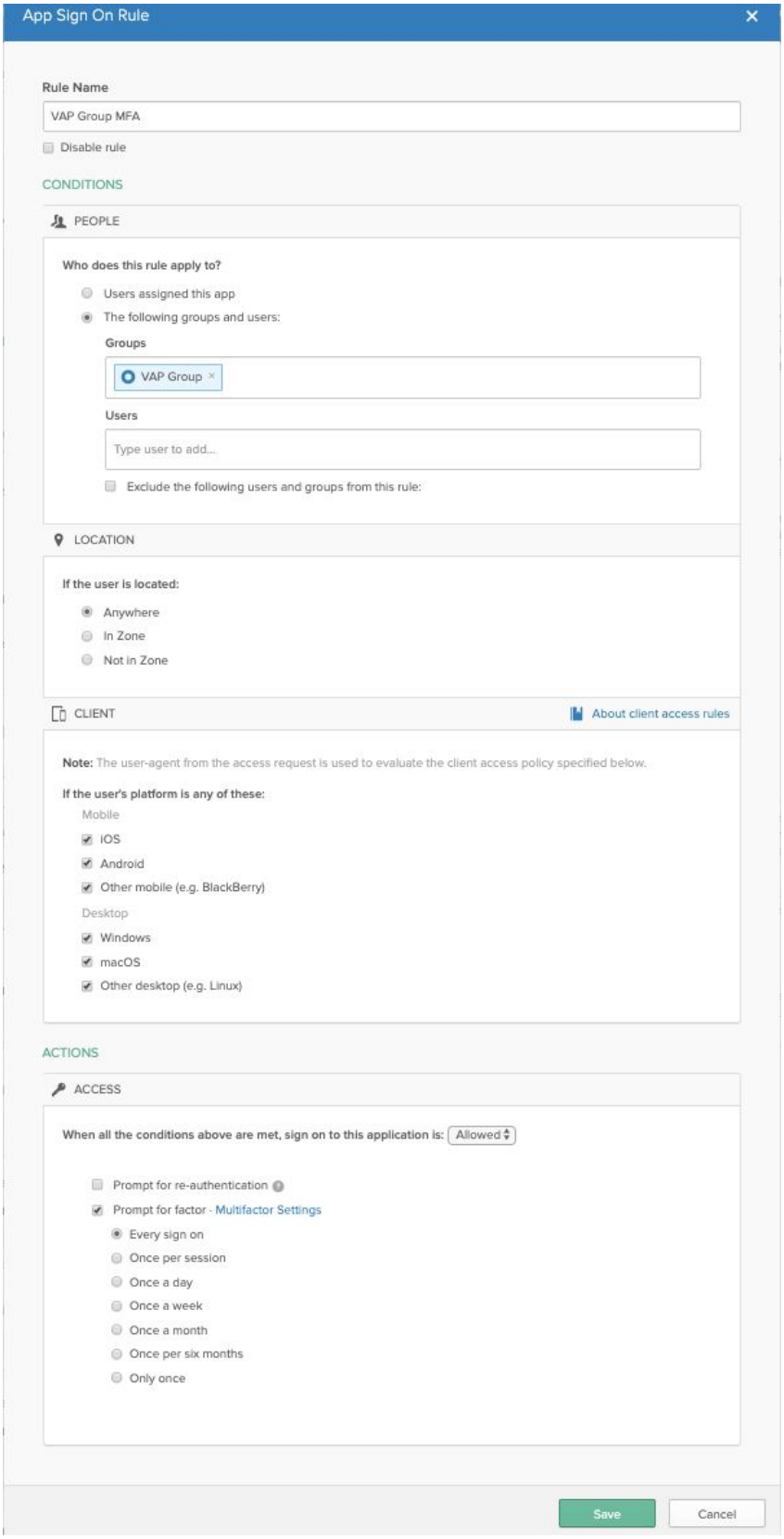
Walking the line between security and usability can feel like you are walking on a tightrope. Too much security and your users reject your efforts and you have to unwind configurations. Too little security puts an organizations' data at risk.

Applying a heightened security policy for specific sensitive applications and only to the users in the **VAP**

Group is a pragmatic approach to taking that next step across the high wire of security.

Follow the steps in the Add Sign On policies for applications product documentation to define a more stringent policy (e.g. Prompt for Factor on every sign on) for sensitive applications. The first condition of these policies should specify that it only applies to the **VAP Group**.

Note: The conditions of group membership can be combined with other conditions such as Network Location, Device Type and more.

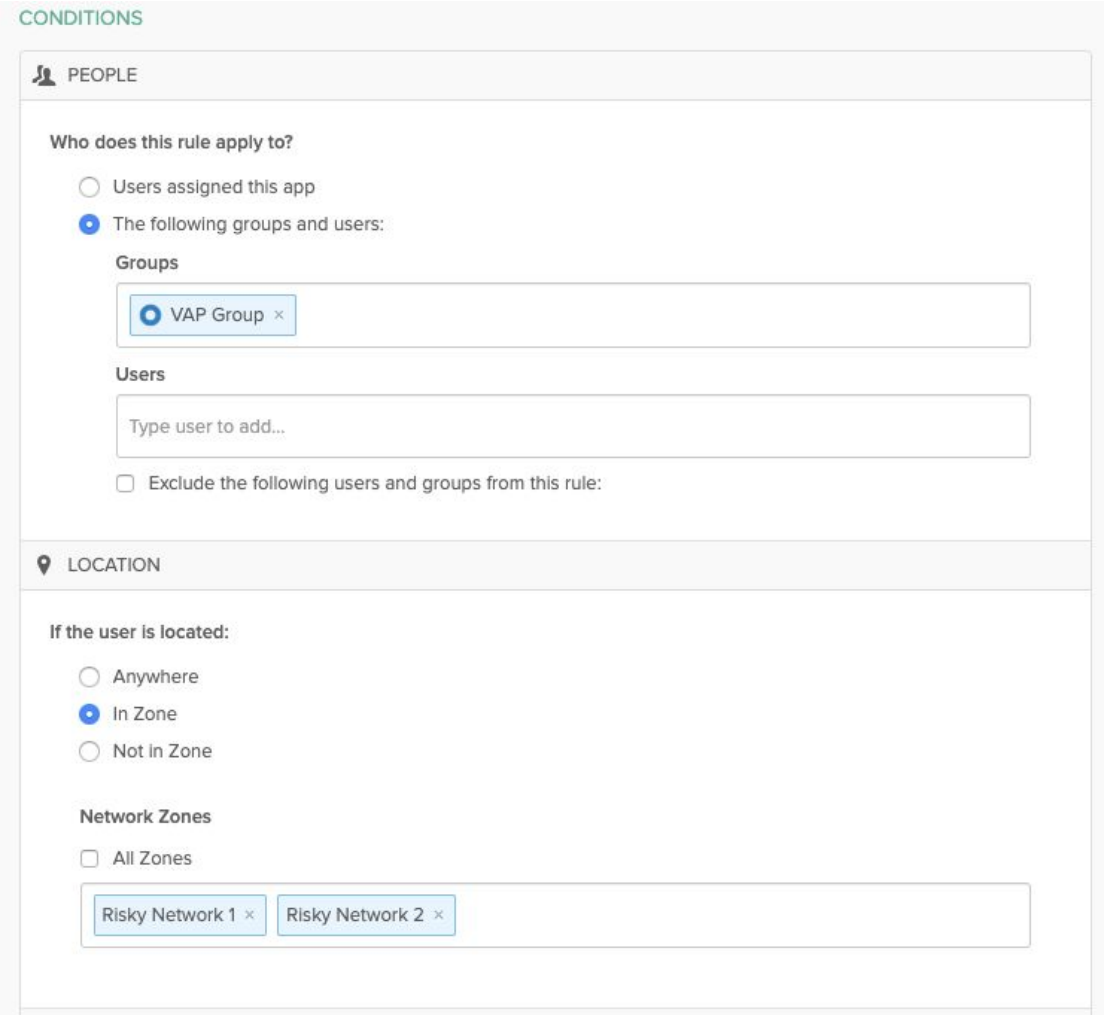

App Sign On Rule
Rule Name
VAP Group MFA
Disable rule
CONDITIONS
PEOPLE
Who does this rule apply to?
Users assigned this app
The following groups and users:
Groups
VAP Group
Users
Type user to add...
Exclude the following users and groups from this rule:
LOCATION
If the user is located:
Anywhere
In Zone
Not in Zone
CLIENT
About client access rules
Note: The user-agent from the access request is used to evaluate the client access policy specified below.
If the user's platform is any of these:
Mobile
iOS
Android
Other mobile (e.g. BlackBerry)
Desktop
Windows
macOS
Other desktop (e.g. Linux)
ACTIONS
ACCESS
When all the conditions above are met, sign on to this application is: Allowed
Prompt for re-authentication
Prompt for factor · Multifactor Settings
Every sign on
Once per session
Once a day
Once a week
Once a month
Once per six months
Only once
Save
Cancel

Restrict Out of Area Access to Certain Applications

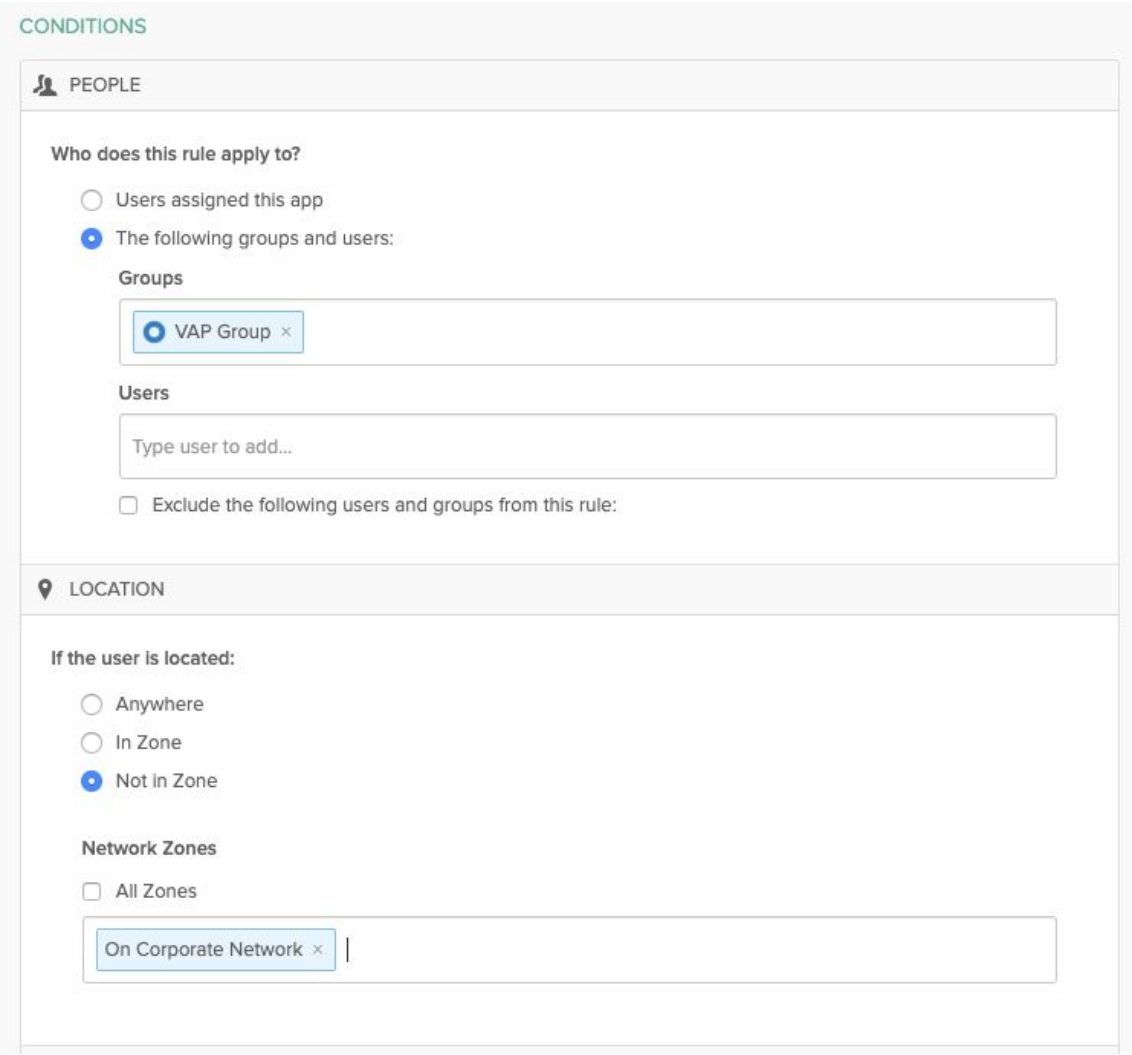
Taking things a step further than requiring MFA to access sensitive applications used by very attacked users, we can restrict access to an application entirely if a user is coming in from a Tor or anonymizer proxy, an unknown or otherwise risky network location.

Depending on your needs the conditions of this rule could be written as either:

- A member of the **VAP Group** connecting from a known risky network



- Or, a member of the **VAP Group** not connecting from a known good network



Refer to the production documentation on Network Security in Okta to identify or define the right network zones and then follow the steps in the Add Sign On policies for applications product documentation to define a policy to deny access to sensitive applications for **VAP Group** users matching the network conditions you desire.

Assign an Informative Bookmark

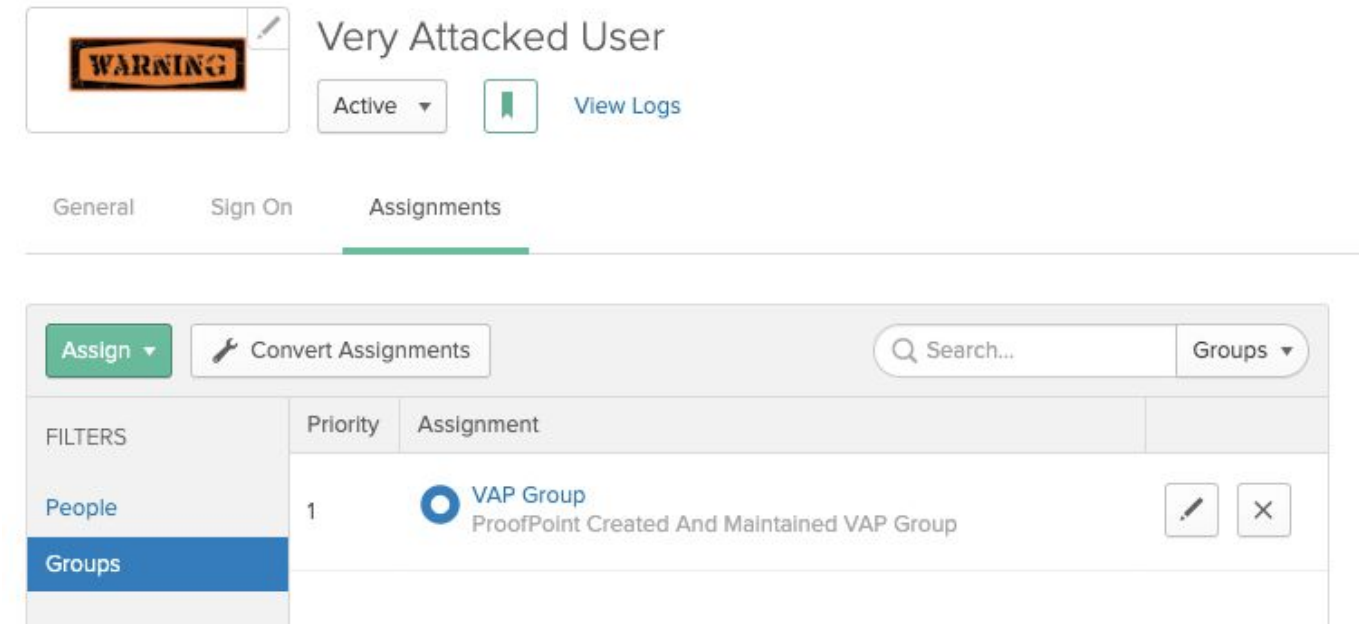
Has anyone ever told you that you didn't communicate the impact of a change well enough? Add this idea to the Emails, Blogs, and bulletin board messages you already have.

Assign users from the **VAP Group to** a bookmark application in Okta to catch their attention; extra credit for having the bookmark app link to a knowledge article providing further insight into the reasons they are considered Very Attacked and the changes they should expect to see in Okta because of it.

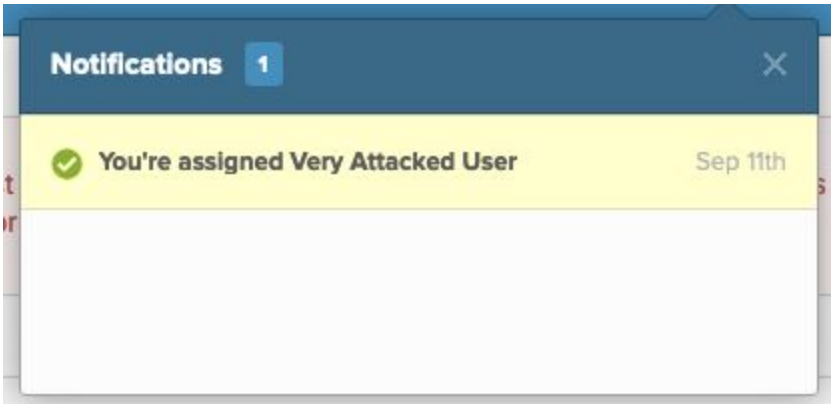
Follow the steps in the How to Create a Bookmark App article.

Assign this new app to the **VAP Group** as shown below:

(Optional - Upload an eye catching icon for this bookmark app)



The next time a user signs into their Okta Dashboard they will receive a notification of the new achievement they have unlocked



References

Frequently Asked Questions or Known Issues

FAQ	
1	Q: Can I exclude users from policies?
	A: Yes ● Create a group in Okta and place users you'd like excluded from the policy in this group (e.g. ***VAP Exception Group***) ● When defining policies with rules targeted at the **VAP Group**, create offsetting policies with rules targeted at the ***VAP Exception Group*** at a higher priority (top of the list), thus excluding users in the ***VAP Exception Group*** from restrictions targeted at the **VAP Group** For more information refer to the Okta Security Policies guide section **Understanding Policy Evaluation**
2	Q: Does a Factor enrollment policy affect factors enrolled before the policy was applied?
	A: Yes If a factor enrollment policy is applied to a user that denies enrollment in a specific factor, Okta will not allow the user to use that factor to satisfy an MFA challenge.

Links to Relevant Material from Okta and Third-Party Knowledge Base Articles, Etc.

Links		
Owner	Details	Link
Okta	Create an API Token	https://developer.okta.com/docs/guides/create-an-api-token/overview/
Okta	Configure Okta Security Policies	https://help.okta.com/en/prod/Content/Topics/Security/Security_Policies.htm
Okta	Configure App Based Sign On Policies	https://help.okta.com/en/prod/Content/Topics/Security/App_Based_Signon.htm
Proofpoint	Proofpoint Launches the Attack Index	https://www.proofpoint.com/us/corporate-blog/post/proofpoint-launches-attack-index-help-companies-better-protect-their-very
Proofpoint	How the Proofpoint Attack Index Reveals Your Most Targeted Users	https://www.proofpoint.com/us/security-awareness/post/which-your-users-are-being-targeted-and-are-you-making-it-worse
Proofpoint	Which of Your Users Are Being Targeted … and Are You Making It Worse?	https://www.proofpoint.com/us/corporate-blog/post/how-proofpoint-attack-index-reveals-your-most-targeted-users

XKCD	Password Strength (correct horse battery staple)	https://xkcd.com/936/