Guidelines and Best Practices for

Defending Against Password Threats

okta

Summary of Best Practices

Tip: To focus on specific threats, refer to:

- Appendix A: To focus on specific threats
- Appendix B: Guidelines for detecting and monitoring threats in flight

Multi-Factor Authentication

- ✓ Implement MFA for all users.
- ✓ Implement behavioral capabilities to reduce MFA fatigue and MFA rubber stamping.
- ✓ Use the strongest MFA factors available for employees in roles with access to critical systems and material information (Okta Verify Push paired with TouchID/FaceID, FIDO U2F, and Windows Hello).
- ✓ For Employees in non-critical areas, use factors that strike a good balance on cost, effectiveness, and convenience (Okta Verify with Push).
- ✓ Enforce MFA for partners after inbound federation.
- ✓ Use sign-on policies to granularly deny suspicious access from specific groups.
- ✓ Reorder security policies and rules from most to least restrictive.
- ✓ Limit MFA enrollment to specific network zones. You can allow enrollment only from specific zones such as your intranet and deny enrollment from risky networks such as Tor exit nodes, network anonymizers, and from countries where you don’t expect access.
- ✓ Configure enrollment in MFA for "the first time a user signs in" and avoid using the option "the first time a user is challenged for MFA".
- ✓ In addition, on the MFA enrollment policy, select at least one MFA factor as required.
- ✓ Communicate with your organization and close entry points to systems without MFA.
- ✓ On Office 365, do not use legacy authentication and the POP and IMAP protocols.

Password Policies

- Turn on common password check.
- Review your password complexity and make sure that your policy strikes a balance between security and usability and doesn't conflict with systems where you're provisioning passwords.
- Update password policies to prevent username, first, and last name, from being used in passwords.
- Raise user awareness on tools like PassProtect and Have I Been Pwned?.
- Tweak the password age and lockout to enforce rotation, mitigate the risk of credential stuffing, and prevent brute force attacks.
- If you use delegated authentication, make sure your lockout policy in Okta doesn't exceed the integrated system (LDAP or AD) password lockout count.
- For AD or LDAP mastered users, make sure that your AD/LDAP password policies don't conflict with the Okta policies.

Network Zones

- Understand how Network Zones work.
- Implement blacklist rules for Tor exit nodes and countries in which you don't have users but see attempted access to Okta.
- Combine network blacklisting with Sign-On policies to improve access blocks. Use blacklist zones to deny access for the entire tenant regardless of user context. Use Sign-On policies to deny access for specific groups of users from specific locations.
- Integrate your security analytics system with Okta to detect, correlate events with other systems, and respond to network-related security events.
- When buying a security analytics system, choose a solution that can:
    - Identify botnet attacks by correlating logs from different systems
    - Read Okta signs such as Okta ThreatInsight
    - Write configurations in Okta such as add users to risky groups or update network zones.

Application Configuration

- Use group membership rules to simplify security management in Okta.
- Use groups to determine who gets access to applications, who is assigned a certain role in an app, and who gets subjected to security policies.
- For apps, whenever possible, use group assignments instead of direct user assignments.
- When possible, use an HR master to drive your account provisioning and revocation.
- Whenever possible, implement Single Sign-On to your systems using federation protocols and implement SAML encryption.
- Close all entry points without MFA, especially legacy entry points that do not support Multi-Factor Authentication.
- For applications integrated with both federation and provisioning, consider provisioning randomly generated passwords.

User Awareness

- Enable email security notifications and train your users to notify security if they see unexpected notifications.
- Customize email notifications and offer your users a simple way – i.e. hotline or form – to trigger security alerts and investigations.
- In addition to your corporate MFA factor options, give your users the option to enroll in and use more secure factors at their own expense.
- Raise user awareness on how to read and respond to suspicious email notifications and Okta verify prompts.

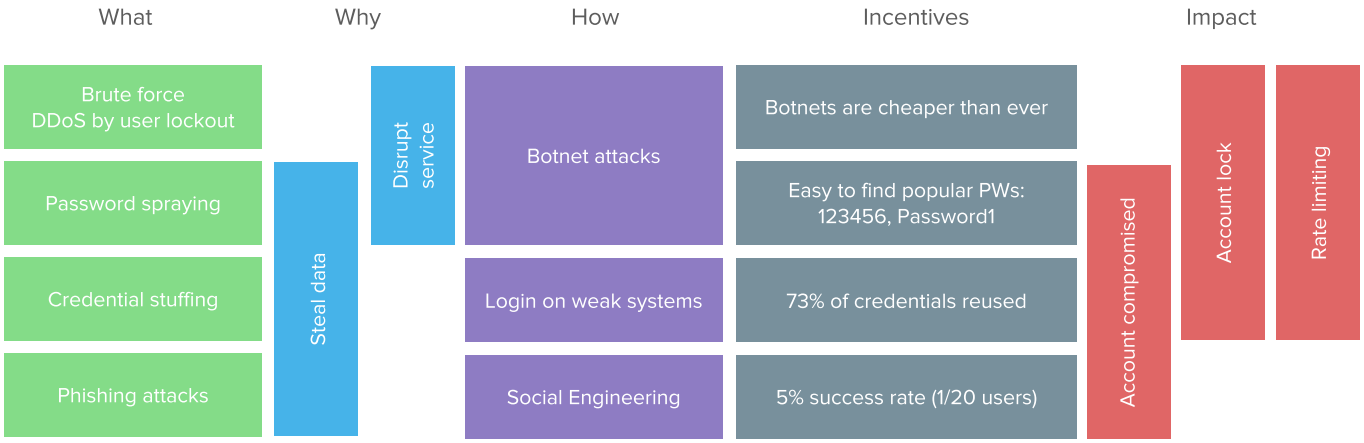
To focus on specific threats

- To focus exclusively on Office 365 legacy authentication attacks, read this document.
- To focus exclusively on phishing attacks, click here.
- To focus exclusively on credential stuffing, click here.
- To focus exclusively on botnet attacks (brute force and password spraying), click here.

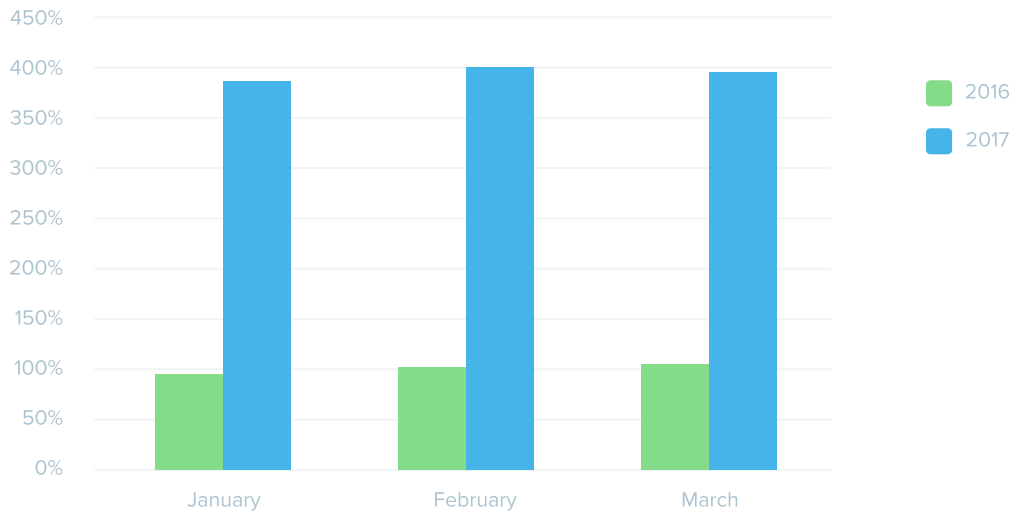
Index

Introduction

Passwords are subject to social engineering, common patterns, and intelligent guessing. Attackers try to exploit password weaknesses to steal data and disrupt services in different ways:



In the password threat landscape, the entire software industry is seeing a steady rise in the frequency of password attacks:



Observed accounts under attack during the first three months of 2016 and 2017
Microsoft Security Intelligence Report: Volume 22

This document provides a list of security controls along with guidelines and best practices to configure your Okta org and mitigate password attacks divided into the following sections:

- Implement Multi-Factor Authentication
- Improve Password Policies
- Configure Network Zones
- Improve Provisioning
- Improve User Awareness

Scope & Limitations

This document provides:

- A list of recommendations and best practices to improve your security posture towards password attacks.
- The security controls listed on this document address both the Okta UI and Okta API. (i.e.: The Sign-On policies and factor sequencing are applicable to the login page as well as the /authn API endpoint)
- A starting point for securing your service against Phishing, Credential Stuffing, Brute Force, and Password Spraying attacks.

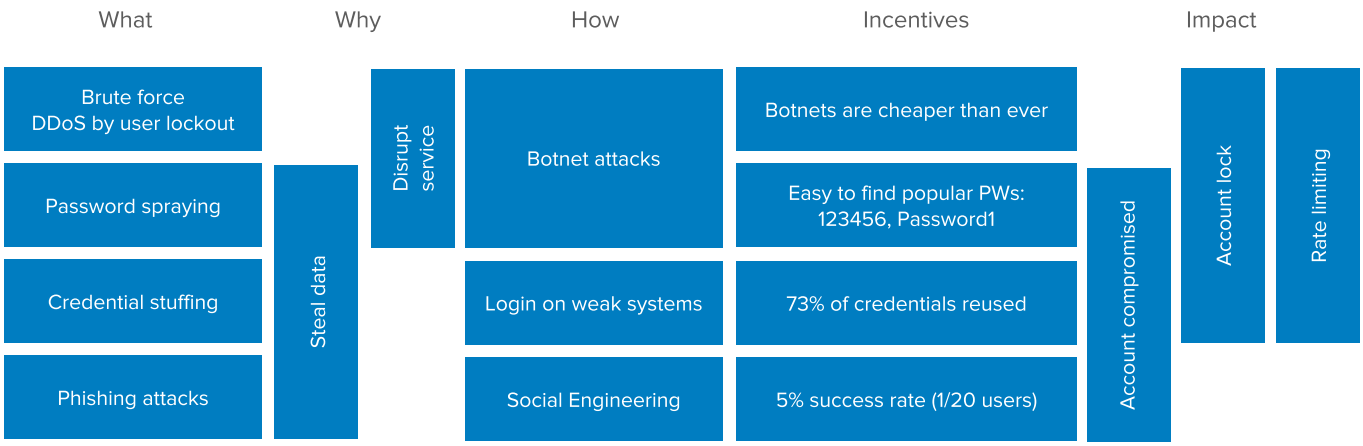
This document DOES NOT provide:

- Step-by-step instructions on how to protect your tenant.
- Guaranteed elimination or mitigation of security risks.
- Commitment, obligation, or promise to deliver any product and is intended to only outline the general product development plans.

When implementing additional security controls, be mindful of balancing security and user experience, especially on customer-facing solutions. Some security features – such as requiring Windows Hello upon authentication – may severely impact your customer access and cause financial impact.

Implement Multi-Factor Authentication

Multi-Factor Authentication (MFA) is the most effective security control against password attacks. If implemented correctly, MFA eliminates the dependency on passwords as the single authentication mechanism for users. The use of MFA – especially with strong 2nd-factor authentication mechanisms such as Okta Verify with Push Notification and FIDO U2F keys – drastically reduces the incentives for attackers looking to compromise accounts and steal data.



Threats, attack methods, incentives, and impacts that are mitigated with Multi-Factor Authentication

The next sections provide guidelines on how to implement MFA effectively.

Licenses Required

The guidelines listed in this section are associated with the following features and products:

Workforce Identity Products*

Features	SSO	ASSO	MFA	AMFA	UD	LCM
Use MFA for all users	✓	✓	✓	✓	✓	✓
Use Sign-On Policies (Pre-authentication sign on policy evaluations)	✓	✓	✓	✓	✓	✓
Use strong factors: Okta Verify with Push, Windows Hello, and FIDO U2F			✓	✓		
Enforce MFA for Partners	✓	✓	✓	✓	✓	✓
Implement Behavioral Policies		✓		✓		
Allow/Deny MFA Enrollment on specific IPs and Geo-Locations			✓	✓		
Allow/Deny MFA Enrollment on Tor exit nodes and Proxy Anonymizers				✓		
Enforce MFA on RADIUS	✓	✓	✓	✓		
Enforce MFA on LDAP					✓	

**Workforce Identity Products: Single Sign-On (SSO), Adaptive Single Sign-On (ASSO), Multi-Factor Authentication (MFA), Adaptive Multi-Factor Authentication (AMFA), Universal Directory (UD), and Lifecycle Management (LCM)*

Configure MFA for all users

According to the 2017 Verizon Data Breach Investigation Report, 81% of data breaches are caused by weak or stolen credentials. Therefore, MFA is table stakes for account security within your company. **You should implement MFA for all users to mitigate account compromise**.

Implementing MFA for all users may lead to MFA fatigue and increases the chances of users rubber stamping MFA challenges. **To mitigate MFA fatigue and rubber stamp, consider implementing behavioral capabilities** for new devices, new location, and velocity.

With these behaviors set, a user will not be prompted for MFA on login when they are signing in from a context already recognized.

In addition, when implementing MFA, **consider using strong MFA factors** based on the user department, role and risk:

	Password only	Security question	SMS, Voice, Email	Software OTP	Physical OTP	Push verification	Yubikey	U2F	Windows Hello
Security	Weak	Weak	Moderate	Moderate	Moderate	Good	Good	Great	Good
Deployability	Great	Great	Good	Good	Poor	Good	Moderate	Good	Poor
User experience	Good	Moderate	Good	Moderate	Poor	Great	Good	Good	Great

Each MFA factor provides different levels of security, deployability, and user experience

You can use the following guidelines to select the appropriate factors:

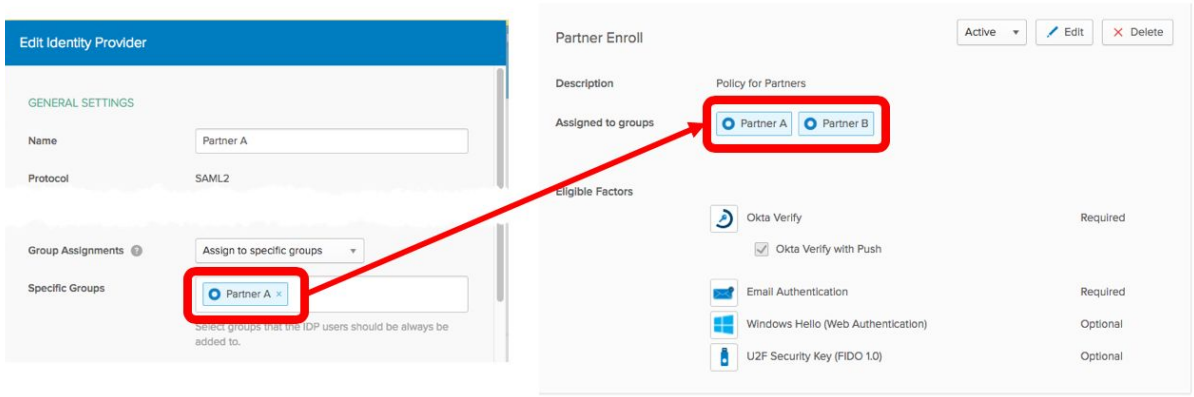
- **Employees in departments and roles with access to critical systems and material information** – i.e. Engineering and the C-Suite – **should use the strongest factors available**: Okta Verify Push paired with TouchID/FaceID, FIDO U2F, and Windows Hello.
- Employees in non-critical areas can use factors that strike a good balance between cost, effectiveness, and convenience. (i.e. Okta Verify with Push).

In addition, **some factors provide additional security value** on specific configurations:

- **FIDO U2F Keys** validate website authenticity during the MFA process, which mitigates man-in-the-middle attacks.
- **Okta Verify with Push and Windows Hello** can validate the user biometrics using fingerprint and face id during the MFA process.
- **Voice calls** can be configured to reach the corporate landline. This may be a good option for a backup factor tied to your office location.

Enforce MFA for partners with inbound federation

Okta supports enforcing MFA after the inbound federation. You should leverage this feature to enforce your own MFA policies after the partner's Identity Provider authentication. To configuring this, add your partners to a specific group on the Identity Provider configuration and then associate the same group with MFA policies:

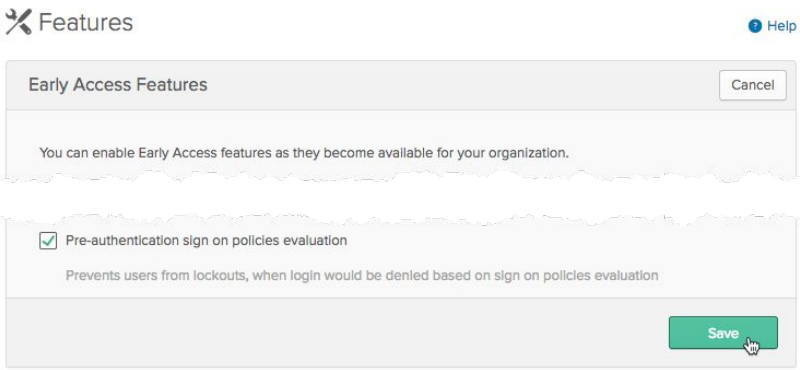


Inbound Federation and MFA policy linked via Group Membership

This configuration mitigates account compromises from partners with a weak security posture.

Use Sign-On Policies to deny suspicious access

The Okta Sign-On policies are used to determined how users will sign into Okta and their session timeout based on groups membership and network zones. With Pre-authentication sign on policy evaluations, the policy can also deny user authentication on specific conditions. This feature can be enabled on the feature manager (under Settings > Features):

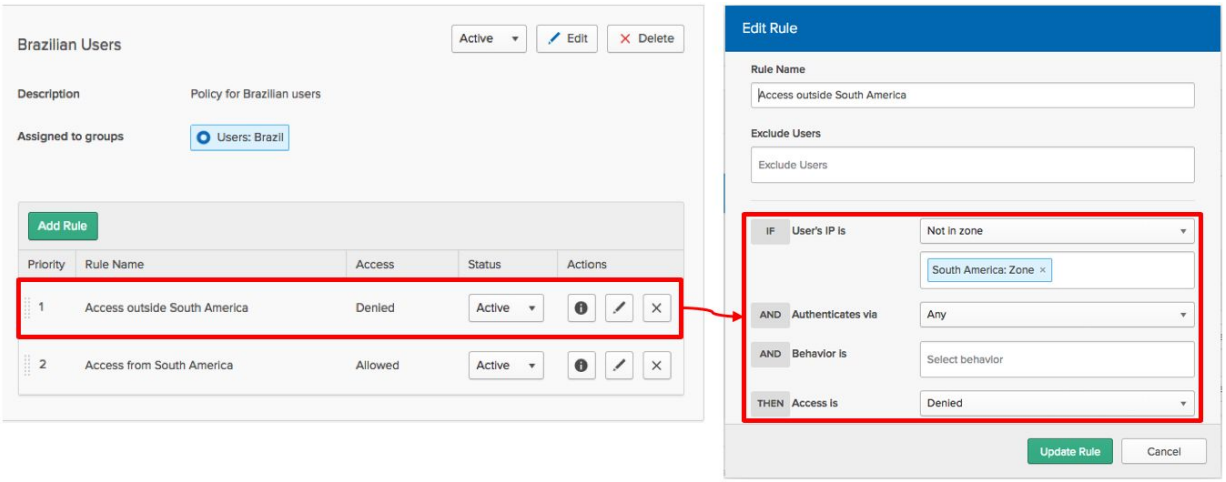


Feature Manager: Enabling Pre-authentication sign on policy evaluation

Use sign-on policies to granularly deny suspicious access from specific groups.

Examples:

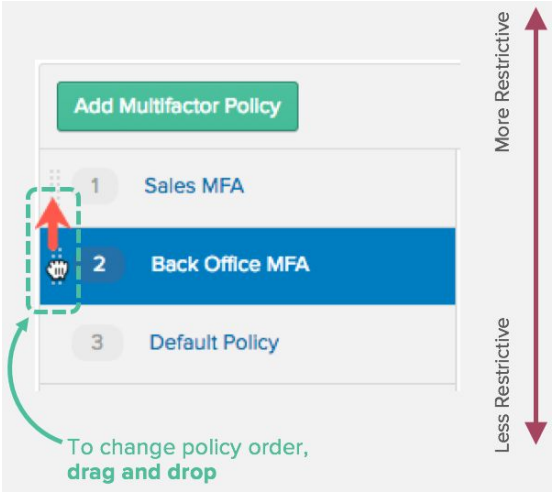
- Users from Brazil cannot login outside of South America.
- Users from the Operations team cannot login outside the office.



Example of a Sign-On Policy denying access for Brazilian users when access is from outside South America

Reorder security policies and rules from most to least restrictive

The Okta Policy Framework evaluates and enforces policies – MFA Enrollment, Sign-On, and Password policies – and rules sequentially. For example, if you have two policies mapped to the same user, the second policy will not be executed. All policies have associated rules that follow the same principle. While the specifics of policy rules are different for each policy type, rules are always context-scoped and policies are group-scoped. For that reason, **always keep the most restrictive policies on the top, followed by the least restrictive policies**:

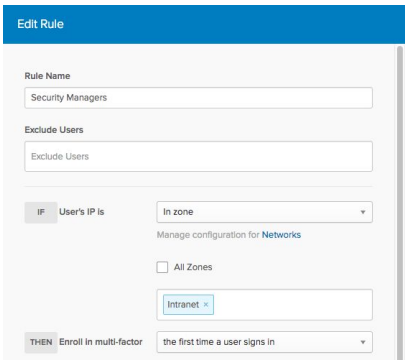


Okta policies are evaluated and enforced from top-to-bottom

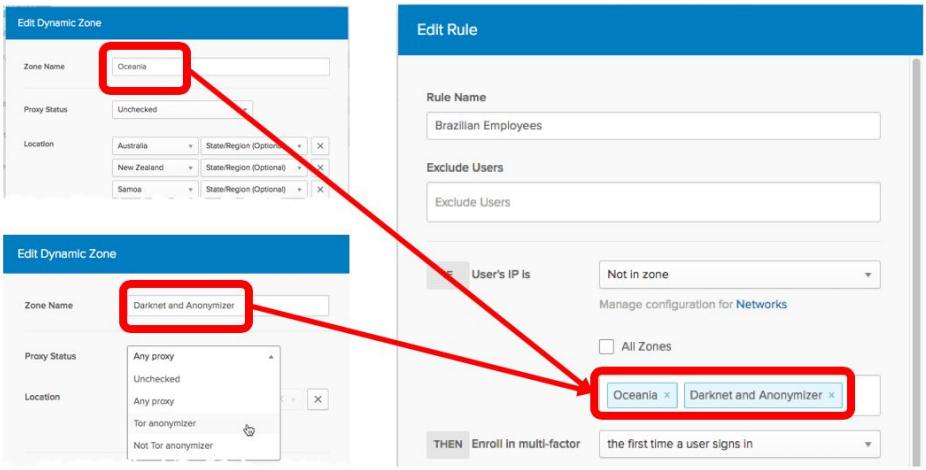
Enroll in MFA only on higher assurance

Okta supports limiting the MFA enrollment to specific network zones. Y**ou should use this mechanism to secure the enrollment in two different ways**:

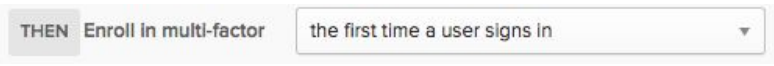
- **Allow Enrollment only from specific network zones**: You can limit users to enroll in MFA only when they are in safe network zones, such as in your intranet:



- **Deny enrollment from risky networks**: You can deny MFA enrollment based on network zones. This option is great for avoiding enrollments from the Darknet, Network Anonymizers, and from specific countries where you don't expect legitimate access:



In addition, **configure enrollment in MFA for "the first time a user signs in" and avoid using the option "the first time a user is challenged for MFA"**. This reduces the time frame where a user does not have an MFA prompt enrolled and also mitigates the risk of prompting users for enrollment on a potentially risky situation, where you are prompting a user for MFA.

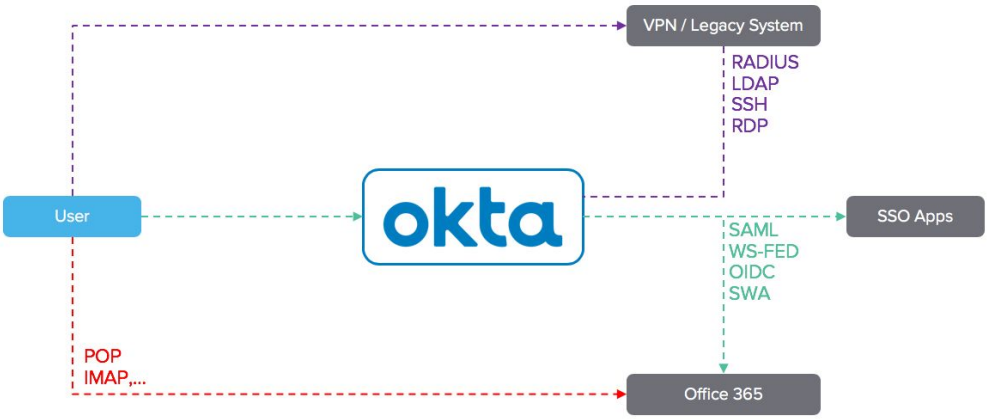


Select at least one factor as required during the MFA enrollment

The Okta MFA enrollment policies support selecting multiple MFA factors for enrollment as mandatory or optional. Users will not be prompted to enroll in MFA unless your policy has at least one factor required. Therefore, **on the MFA enrollment policy settings, select at least one MFA factor as required**.

Close entry points without MFA

To have an effective MFA strategy, you should close entry points to your systems without MFA implemented:



Entry points for authentication with and without MFA

The diagram above shows 3 types of access to systems:

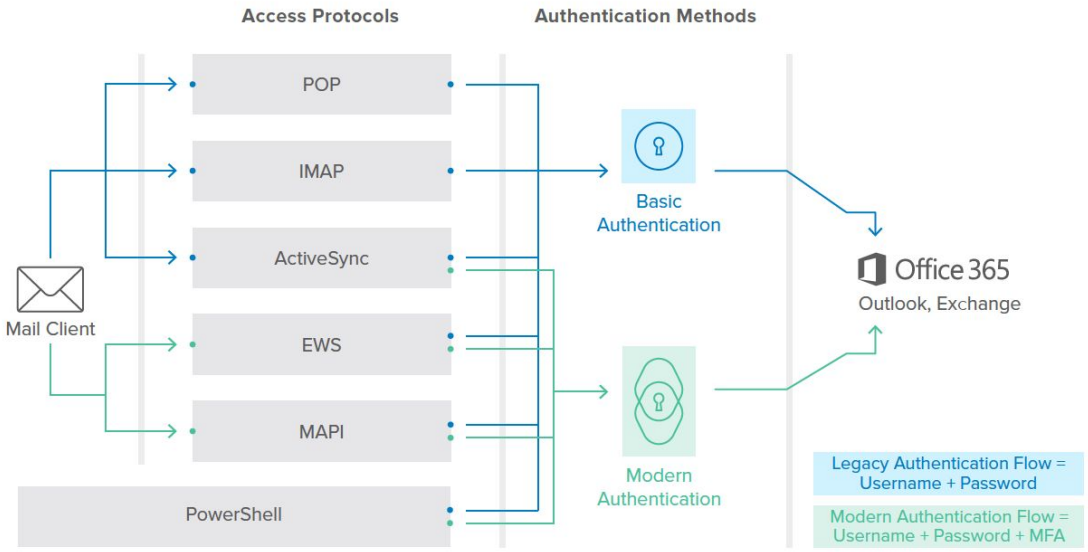
- **Access with MFA provided by Okta** (green): You can integrate Web applications into Okta SSO with MFA using the OIN and standards-based integrations like SAML, WS-FED, OpenID Connect, and SWA.
- **Systems and Servers that don't support SSO** (purple): For systems and servers that don't support Okta's SSO protocols – i.e. Legacy Web Applications, VPNs, Network Appliances, Linux Server, and Windows Server – you can integrate with Okta and MFA using backend protocol integrations offered by Okta such as RADIUS, LDAP, SSH, and RDP.
- **Access applications on legacy applications that don't support MFA** (red): Some applications – most popularly, Office 365 – provide insecure legacy protocols where MFA is not supported (such as POP and IMAP). For these cases, you should communicate with your organization, gradually retire the legacy protocols, and use modern options that support Multi-Factor Authentication. On Office 365 for example, Microsoft recommends using Modern Auth, that works with Multi-Factor Authentication provided by Okta. For guidance on implementing modern authentication on Office 365 and using Okta for MFA, please review this document.

Secure O365 legacy protocols

Okta's customers commonly use a combination of single sign-on (SSO), automated provisioning, and multi-factor authentication (MFA) to protect their Office 365 tenants against credential attacks. However, Office 365 uses several authentication methods, including methods that do not support Multi-Factor Authentication:

- **Basic Authentication**
  Basic Authentication, in the Office 365 suite, is a legacy authentication method that relies solely on username and password. It has proven ineffective and is not recommended for the modern IT environments especially when authentication flows are exposed to the internet as is the case for Office 365. It has become increasingly common for attackers to abuse these legacy authentication methods to compromise business email accounts.

- **Modern Authentication**
  To address the common security concerns and end user experience requirements associated with Office 365 deployments, Microsoft introduced the Active Directory Authentication Library (ADAL) for Office 365 client applications, referred to as Modern Authentication. Modern Authentication helps secure Office 365 resources using multi-factor authentication, certificate-based authentication, and SAML-based logins (such as federation with Okta), for a true single sign-on experience.



Office 365 support for access protocols and authentication methods

In addition to the authentication methods, Office 365 supports multiple protocols that are used by clients to access Office 365. In the context of authentication, these protocols fall into two categories:

- **Legacy Authentication Protocols**
  Protocols like POP, and IMAP, which do not support modern authentication methods are referred to as legacy authentication protocols.
- **Modern Authentication Supported Protocols**
  Protocols like Exchange ActiveSync, EWS, MAPI and PowerShell, which support both basic and modern authentication methods are referred to as modern authentication supported protocols in the context of this document.

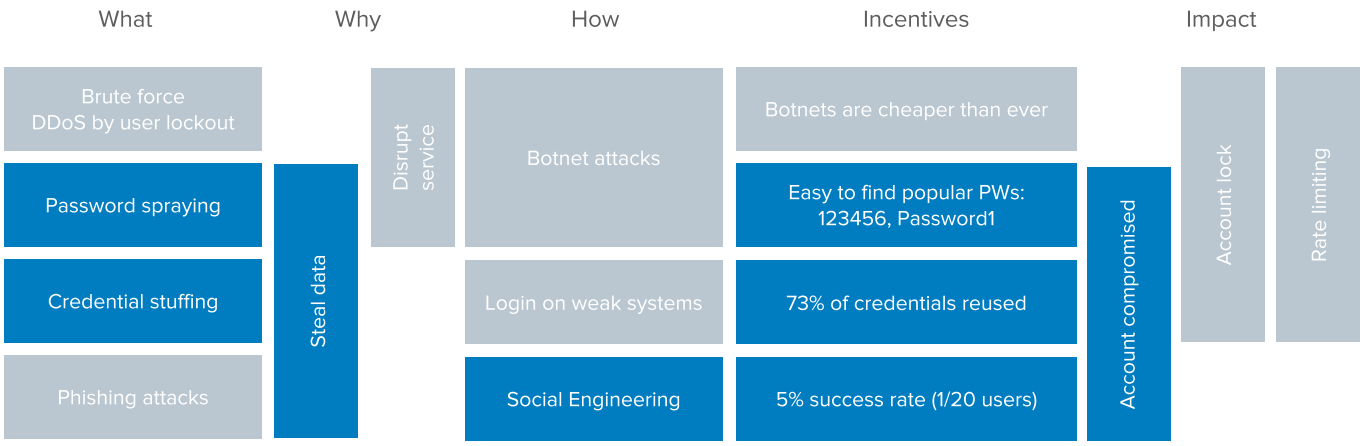
To better protect Office 365 accounts, you should:

- Stop using the legacy protocols POP and IMAP.
- Use only modern authentication with MFA on the remaining protocols: Active Sync, EWS, MAPI, and PowerShell.

For more details on how you can secure an Office 365 deployment federated with Okta, see the Securing Office 365 with Okta white paper.

Improve Password Policies

Good password policies reduce the use of common/repeated passwords and enforce regular password rotation, which mitigates account compromise due to password spraying and credential stuffing.



Threats, attack methods, incentives, and impacts that are mitigated with tweaking your Password Policies

The next sections cover how to tweak your password policies in Okta for security efficacy.

Licenses Required

The guidelines listed in this section are associated with the following features and products:

Workforce Identity Products*

Features	SSO	ASSO	MFA	AMFA	UD	LCM
Use MFA for all users	✓	✓	✓	✓	✓	✓
Use Sign-On Policies (Pre-authentication sign on policy evaluations)					✓	✓

**Workforce Identity Products: Single Sign-On (SSO), Adaptive Single Sign-On (ASSO), Multi-Factor Authentication (MFA), Adaptive Multi-Factor Authentication (AMFA), Universal Directory (UD), and Lifecycle Management (LCM)*

Turn on common password check

Okta Password Policy: Common password checkbox

The common password check option validates against a list of common passwords, regularly updated by Okta, that should not be used in order to prevent password spraying attacks. To mitigate account compromise caused by password spraying attacks, **you should use the common password check feature on all your password policies**.

Review password complexity

The use of the correct password complexity reduces the odds of credential stuffing and password spraying without driving up password reset calls.

When updating the password requirements, make sure your password policy:

- **Strikes a balance between security and usability.** The use of overly complex passwords drives up help-desk calls and can lead users to write down passwords.
- **Doesn't conflict with systems where you're provisioning passwords.**

Some companies will use external recommendations as a starting point to define their password complexity. As an example, the SANS Institute considers a strong password as one that:

- Has at least 15 characters
- Has uppercase and lowercase letters, numbers, and special characters
- Doesn't include dictionary words or patterns such as sequential numbers or letters
- Is unique from other accounts owned by the user

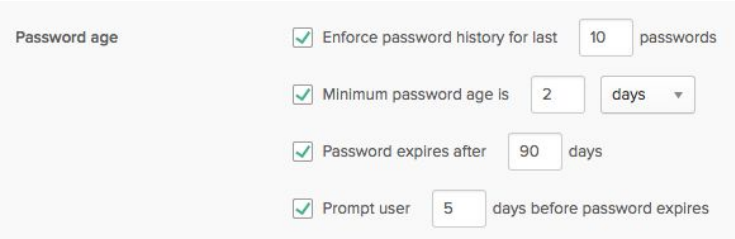
In addition to the traditional complexity filters, the Okta password complexity settings offer options that you can use to comply with the SANS recommendation. In addition to SANS recommendations, you can use other Okta features such as avoiding user attributes – username, first, and the last name – as part of the password:

Okta Password Policy: Complexity requirements

In addition, encourage your users to adopt tools like PassProtect. PassProtect works by checking passwords against the Have I Been Pwned? API service to see whether or not the password you are using in any web login has been breached in the past.

Review password age

The password age feature coupled with a good password rotation strategy reduces the probability of users reusing the same credentials on personal accounts and corporate resources. **You should enable the password age on policies to enforce rotation and mitigate the risk of credential stuffing**.



Okta Password Policy: Password Age requirements

Review password lockout

The use of password lockout mitigates account compromise and **is considered a must to prevent brute force attacks**. Tweak your password lockout policy according to your needs. If you use delegated authentication, make sure your lockout policy in Okta doesn't exceed the integrated system (LDAP or AD) password lockout count.

Configuration for Active Directory or LDAP mastered users

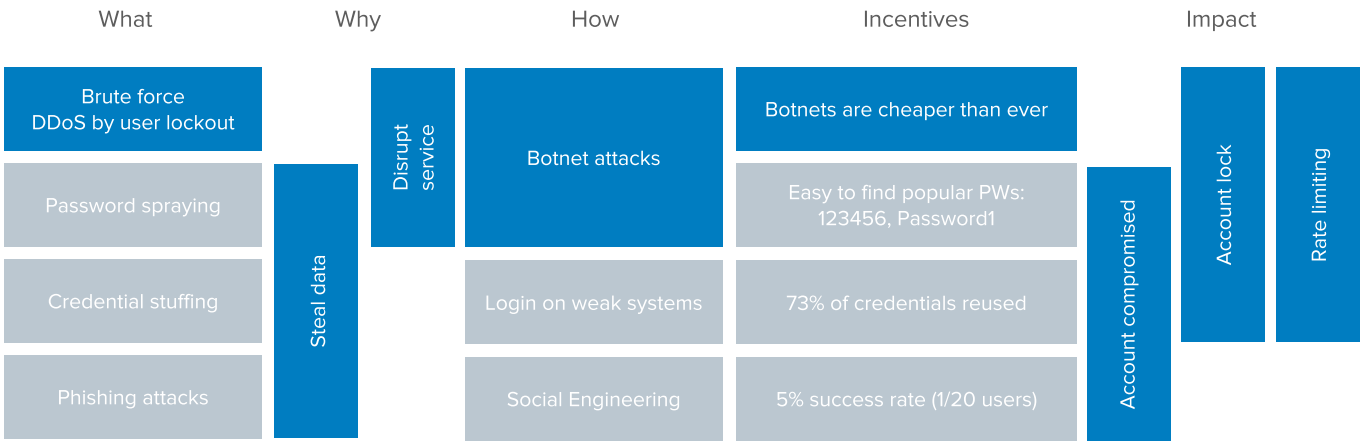
For AD or LDAP mastered users, **ensure that your AD/LDAP password policies don't conflict with the Okta policies. This includes**:

Attributes	Recommendation
Minimum Length **Password Complexity** **Password Age**	Use the same requirements as AD or LDAP
Password Lockout	Lockout lower than the AD or LDAP lock. **This prevents a desktop account lockout in case of an account lock in Okta.*

For more information, see security policies documentation.

Configure Network Zones

Network zones help reduce the threat surface for password attacks and can reduce attacks from specific regions that may disrupt your service.



Threats, attack methods, incentives, and impacts that are mitigated with Network Zones

Licenses Required

The guidelines listed in this section are associated with the following features and products:

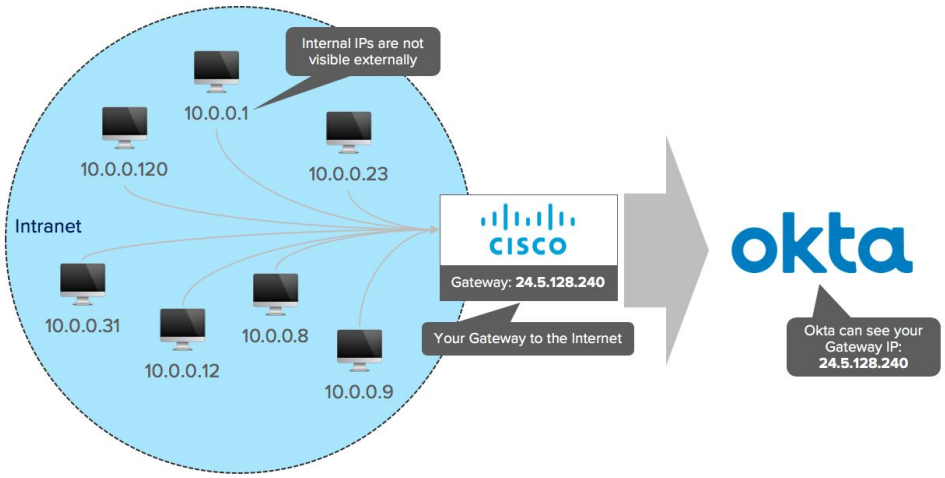
Workforce Identity Products*

Features	SSO	ASSO	MFA	AMFA	UD	LCM
Implement Zones based on IPs and Geo-Location	✓	✓	✓	✓	✓	✓
Implement Zones based on Tor exit nodes and Proxy Anonymizers		✓		✓		
Use Sign-On Policies (Pre Authentication Evaluation Policies)	✓	✓	✓	✓	✓	✓
Integrate with Security Analytics Systems	✓	✓	✓	✓	✓	✓

**Workforce Identity Products: Single Sign-On (SSO), Adaptive Single Sign-On (ASSO), Multi-Factor Authentication (MFA), Adaptive Multi-Factor Authentication (AMFA), Universal Directory (UD), and Lifecycle Management (LCM)*

Understand how Network Zones work

For network rules, Okta identifies the Internet Gateway IPs:

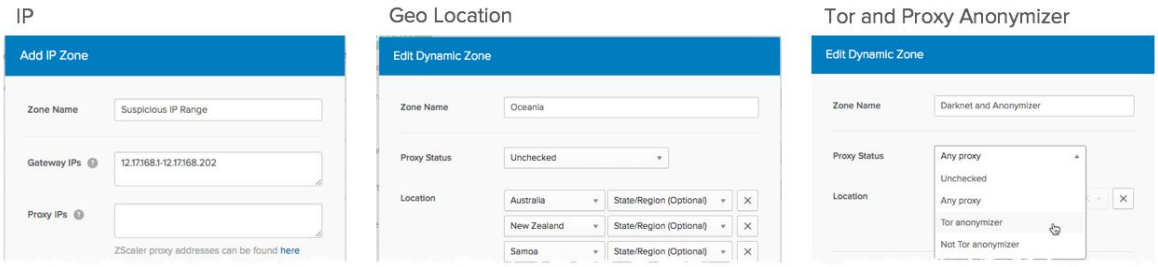


How Okta detect Gateway IPs

For every single request, Okta matches the Gateway IP with geolocation and IP reputational data (provided by IP2Location and MaxMind), records the geolocation information in the System Log, and applies your network rules.

Implement Network Zones

You can implement network zones to deny access to Okta from specific IPs, IP ranges, geolocations, Tor exit nodes, and network anonymizers:



Types of Network Zones supported by Okta

To reduce the threat surface for password attacks and botnet attacks from specific regions, implement blacklist zones for:

- Countries you don't have users located in but from which you see attempted access to Okta.
- Tor exit nodes.

Combine Network Zones with Sign-On Policies

In addition to implementing network zones, **combine network blacklisting with Sign-On policies to improve access blocks**.

- **Use blacklist zones to deny access for the entire tenant** regardless of user context.
- **Use Sign-On policies to deny access for specific groups of users from specific locations.**

For more information about Sign-On policies, review the section Use Sign-On Policies to deny suspicious access.

Integrate with Security Analytics Systems

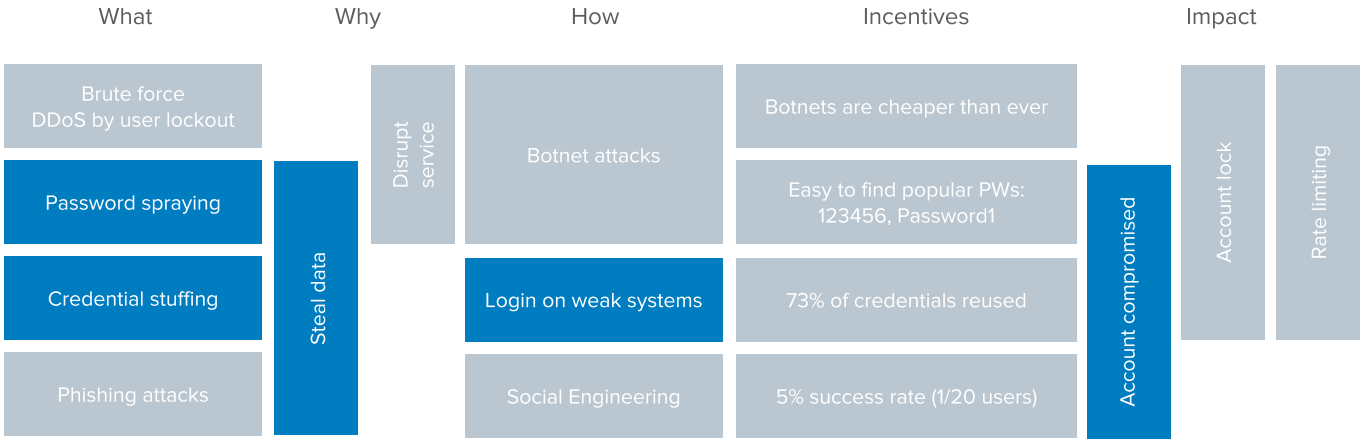
Whenever possible, integrate your security analytics system with Okta to detect, correlate events with other systems, and respond to network-related security events. Okta supports multiple security analytics systems, including:

Solution (and documentation)	Detect Events in Okta	Update configuration in Okta
Splunk (Okta Identity Add-on)	✓	✓
ServiceNow (Security Incident Response)	✓	✓
LogRhythm	✓	✓
ExaBeam	✓	✓
BetterCloud	✓	✓
Securonix (SNYPR)	✓	
Rapid7 (InsightIDR)	✓	
IBM (qRadar)	✓	
AlienVault (USM Anywhere)	✓	
Sumologic	✓	

If you're buying a security analytics system, consider choosing a solution that can identify botnet attacks in correlation with other systems, that can read events from Okta (including Okta ThreatInsight), and that can write configurations in Okta (such as add users to risky groups or update network zones).

Improve App Config

Implementing the correct application integration configuration with Okta together with tight deprovisioning and account automation reduces the number of accounts and privileges that can be compromised, therefore reducing the user and application threat surface.



Threats, attack methods, incentives, and impacts that are mitigated with a tight Provisioning and App Configuration

The next sections provide guidance on how you can tighten account provisioning and deprovisioning in your Okta org.

Licenses Required

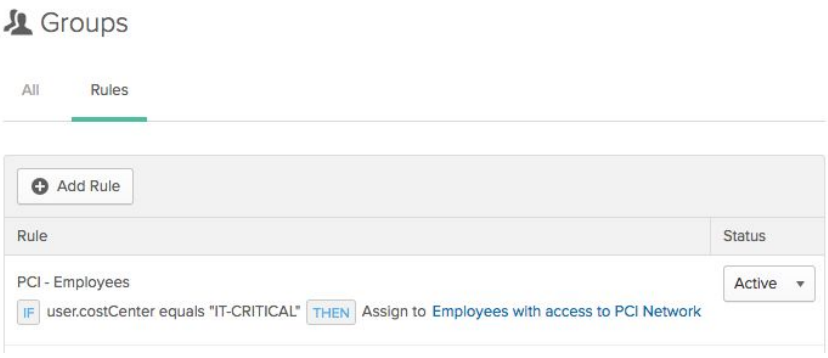
The guidelines listed in this section are associated with the following features and products:

	Workforce Identity Products*					
Features	**SSO**	**ASSO**	**MFA**	**AMFA**	**UD**	**LCM**
Single Sign-On to Apps	✓	✓	✓	✓		✓
Group Membership Rules						✓
Account Provisioning						✓
HR as a Master						✓
Attribute Mapping/Transformation					✓	✓

**Workforce Identity Products: Single Sign-On (SSO), Adaptive Single Sign-On (ASSO), Multi-Factor Authentication (MFA), Adaptive Multi-Factor Authentication (AMFA), Universal Directory (UD), and Lifecycle Management (LCM)*

Use Group Membership Rules

Group Membership Rules automate adding and removing group members based on user attributes:

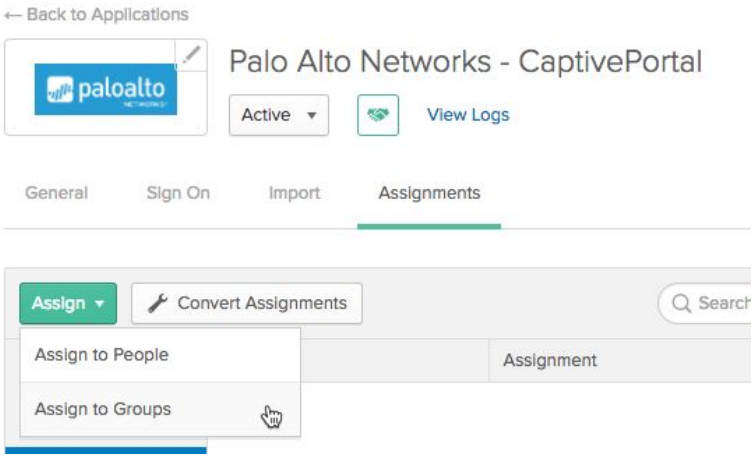


Group membership rule in Okta

Consider using group membership rules, coupled with group assignments for policies – MFA, Password – and applications to simplify security management in Okta.

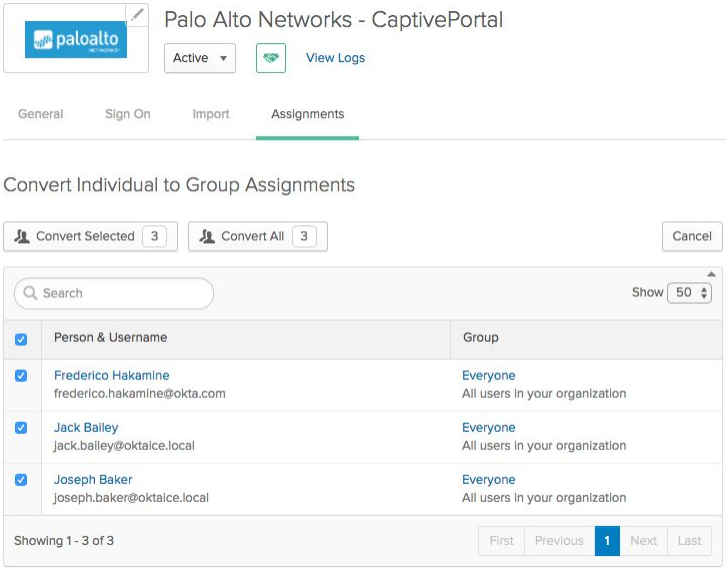
Use groups for Policies and App assignments

Okta can use groups to determine who gets access to applications, who is assigned a certain role in an app, and who gets subjected to security policies. The groups are enforced by default on policies. For apps, when possible, make sure you use group assignments instead of direct user assignments.



Assign applications to Group instead of users

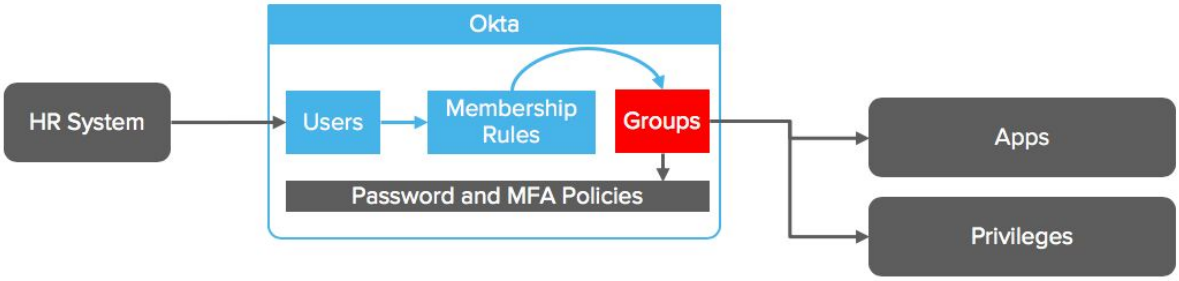
If you already have users assigned to apps, Okta offers the group assignment feature. You can convert application access and user properties settings so that individually owned applications become group managed:



Group assignment features

Use HR-driven IT Provisioning

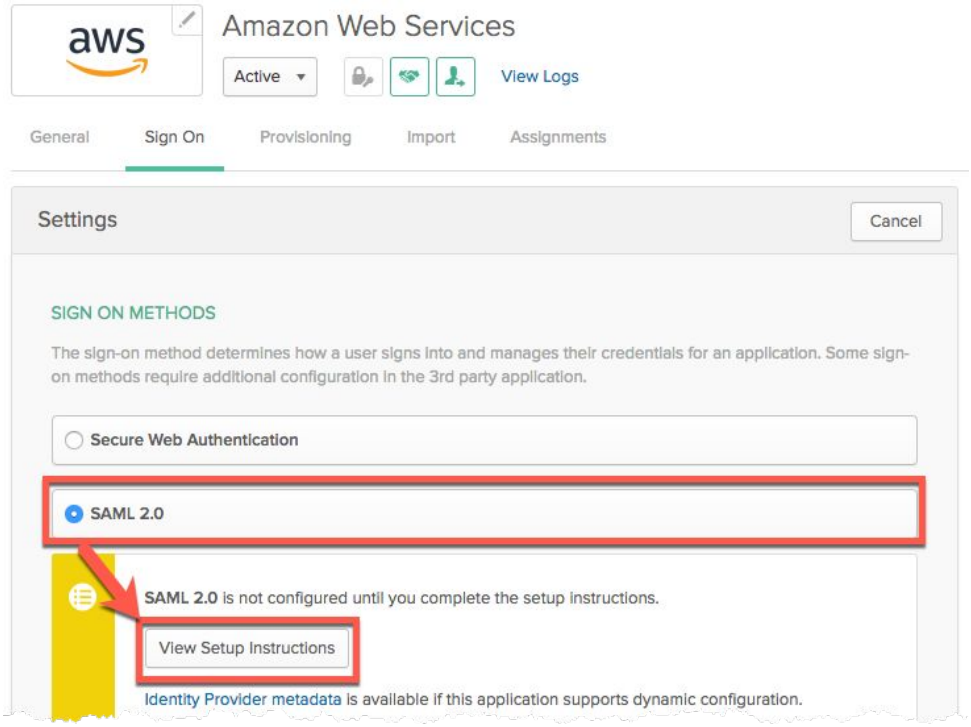
HR-driven IT Provisioning (also known as HR mastering) allows you to import users directly from HR systems to Okta. It automates user onboarding, updates, and offboarding. **When possible, use an HR-driven IT Provisioning to drive your account provisioning and revocation**. By combining the HR data with group rules and assignments, you have automatic account deprovisioning and security policy updates any time a user record is updated:



Combine HR-driven IT Provisioning with group rules and assignments to automate account lifecycle

Improve Application SSO and Provisioning configuration

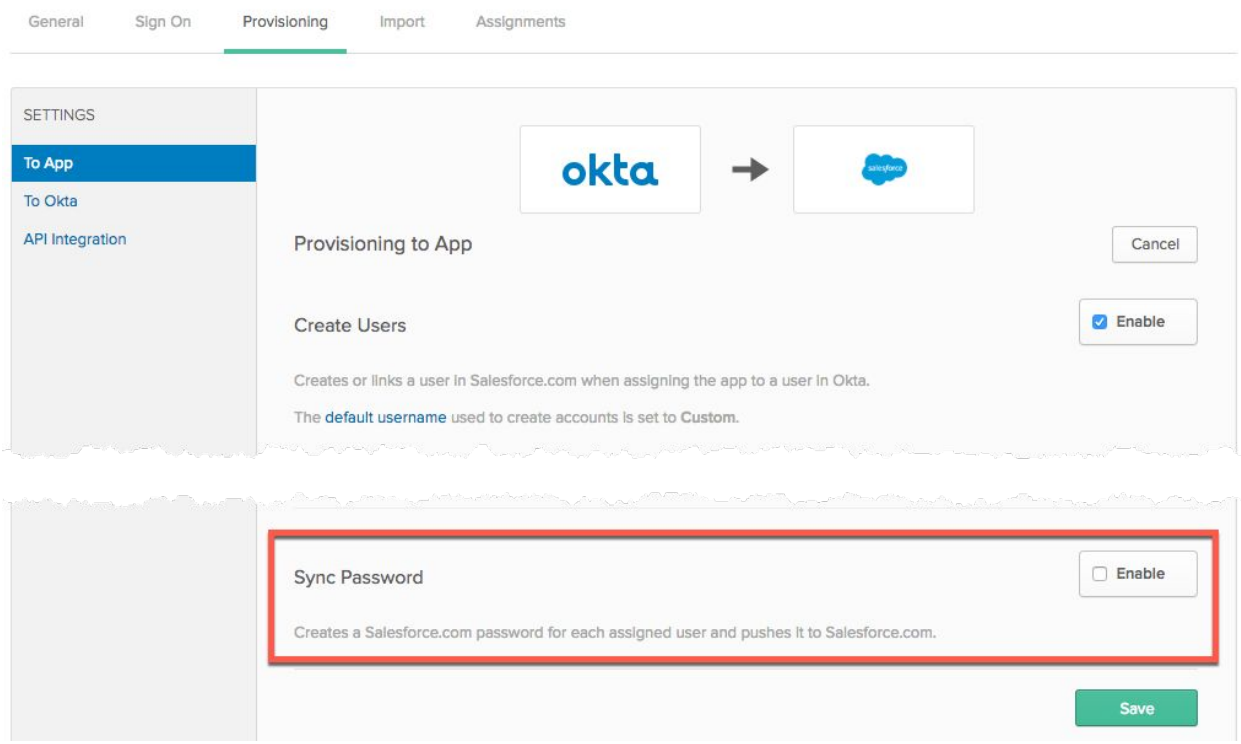
Okta supports providing Single Sign-On to applications using different methods. This includes federation protocols like SAML, OpenID Connect, and WS-Fed as well as SWA, an integration based on password-vault for authentication (similar to password managers like Dashlane and 1Password). **Whenever possible, integrate with systems using federation protocols and implementing SAML encryption**.



Whenever possible, use federation protocols for integrating apps. The Setup Instructions will help you configure the integration.

Also, whenever possible, use the recommendations from Implement MFA: Close entry points without MFA to close legacy entry points without Multi-Factor Authentication to applications.

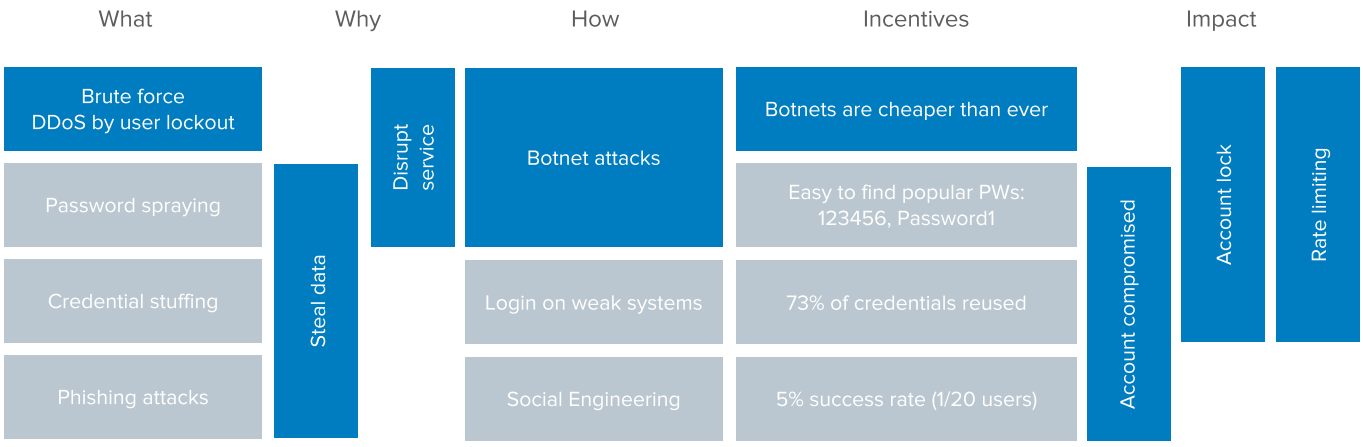
For provisioning, Okta offers an option for pushing passwords to applications. **For applications integrated with both federation and provisioning, consider provisioning a randomly generated password**. This helps to avoid propagating the user password to systems that should support only federated authentication.



Sync Password option in Provisioning

Improve User Awareness

Educating your employees on information security, how to identify suspicious events, and how to notify the security team helps with mitigating account compromise on their personal and professional accounts and reduce the risk of Social Engineering attacks.



Threats, attack methods, incentives, and impacts that are mitigated with user awareness

The next sections provide guidelines on how to improve your user awareness using Okta. **These guidelines should be followed in conjunction with administrative controls such as having an end-user security awareness program.**

Licenses Required

The guidelines listed in this section are associated with the following features and products:

Workforce Identity Products*

Features	SSO	ASSO	MFA	AMFA	UD	LCM
End-User Notifications	✓	✓	✓	✓	✓	✓
Use strong factors: Okta Verify with Push, Windows Hello, and FIDO U2F			✓	✓		

**Workforce Identity Products: Single Sign-On (SSO), Adaptive Single Sign-On (ASSO), Multi-Factor Authentication (MFA), Adaptive Multi-Factor Authentication (AMFA), Universal Directory (UD), and Lifecycle Management (LCM)*

Enable Email Notifications

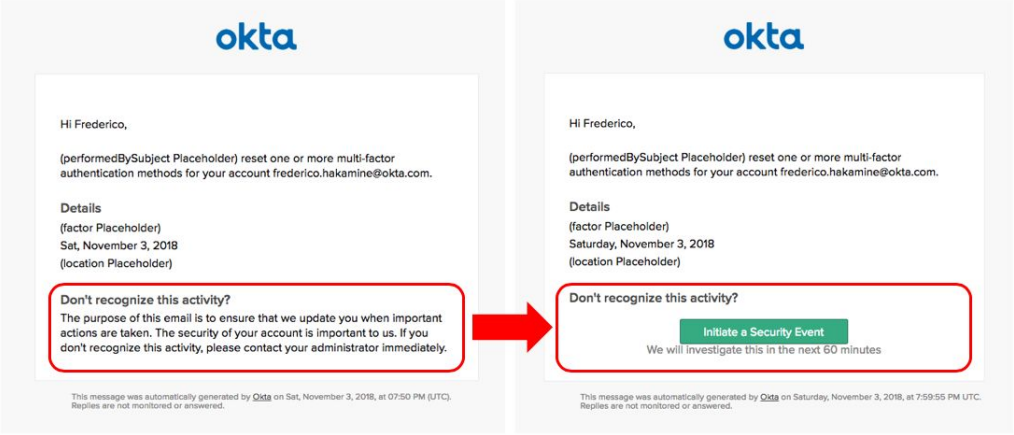
Okta can send e-mail notifications to end-users on the following events:

- Forgot Password Requested
- Forgot Password Denied
- Reset Password Requested
- Reset Password Denied
- Unlock Account Requested
- Unlock Account Requested (when the account is not unlocked)
- Change email confirmation
- Sign-On from a new device
- MFA Factor enrolled
- MFA Factor Reset

Enable the email notifications and train your users to notify security if they receive an unexpected, suspicious notification so that your security team can initiate the appropriate investigation.

Customize actions in security notifications

In addition to enabling email notifications, **consider customizing the email message and offer your users a simple way – i.e. hotline or form – to trigger security alerts and investigations**:



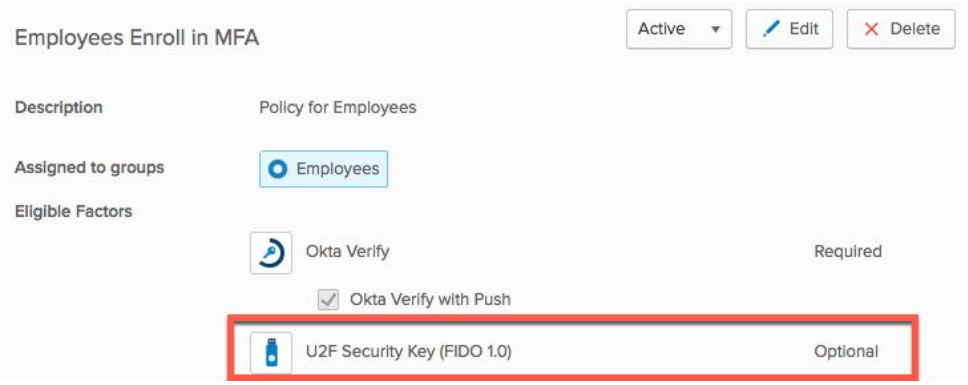
Email notification: After implementing a link to quickly start a security event

This will encourage users to interact with security when they identify a suspicious notification.

Encourage adoption of the strongest MFA factors available

As part of your security strategy, you will select factors based on your budget and risk. After selecting those factors, **consider giving your users the option to enroll in and use more secure factors**.

For example: Company A decided to support only Okta Verify with Push as a second factor due to financial constraints. The security administrator decided to allow users to use FIDO U2F keys at their own expense:



This type of policy allows security-minded users to better protect themselves and incentivizes a security culture in your company. However, when using this tactic, keep your default factor as mandatory – so users will have an MFA factor that's supported by the company always available.

Train users to deny suspicious events and alert security

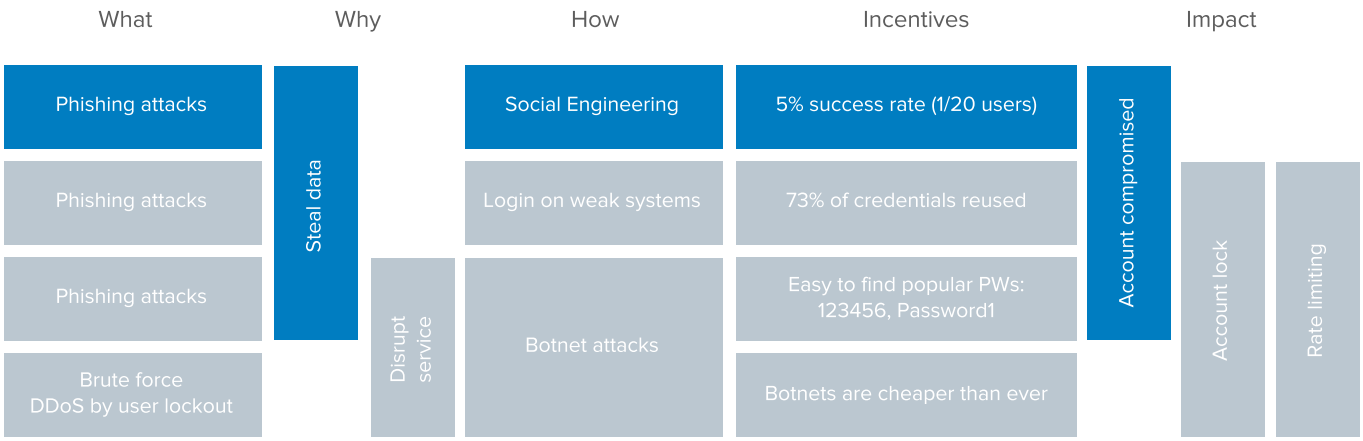
When training users, raise their awareness on how to read and respond to suspicious email notifications and Okta verify prompts. Training your users helps with identifying suspicious events and triggering security investigations.

Appendix A:

To focus on specific threats

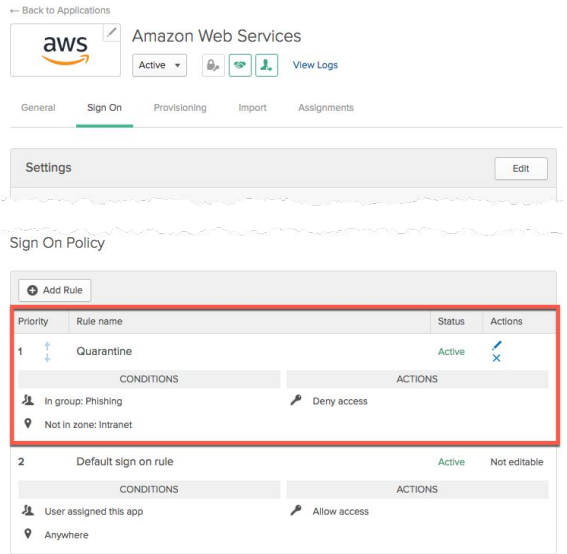
This document provides guidelines and best practices to configure your Okta org for mitigating four types of password attacks: Phishing, Credential Stuffing, Brute Force, and Password Spraying attacks. If you want to focus exclusively on a specific type of attack, you can start by focusing on a subset of our guidelines:

To focus exclusively on Phishing Attacks

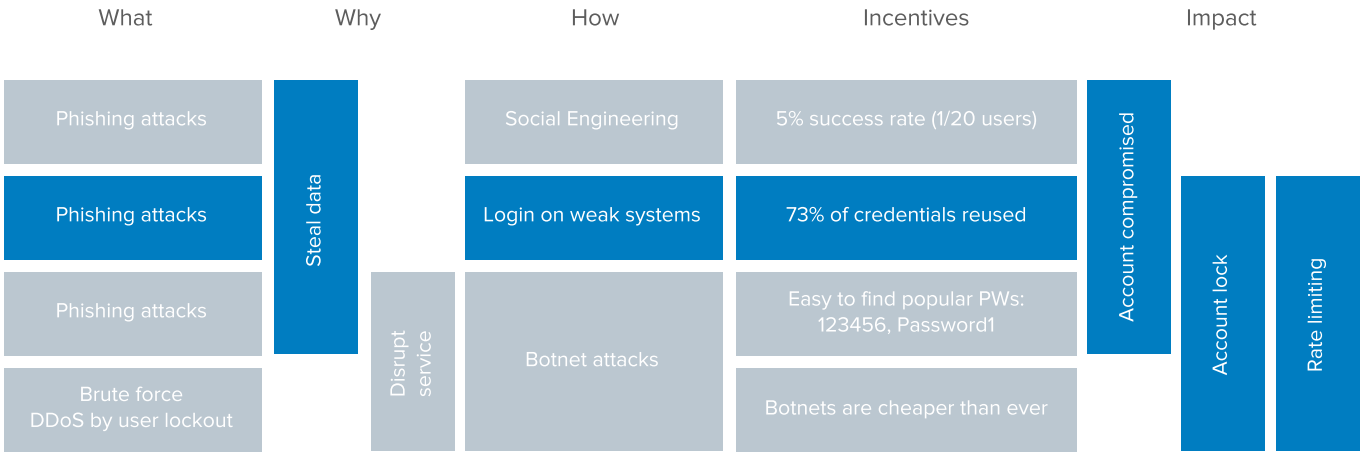


Start by implementing the recommendations from Improve Customer Awareness, Implement Multi-Factor Authentication, and Improve Password Policy. In addition, consider:

1. Reset passwords and track activity from customers targeted on the phishing campaign.
2. Extend the use of Okta Verify with Push or FIDO U2F tokens for all users.
3. Create a group in Okta for the targeted users and implement quarantine rules and policies for users in the group. For example, you can deny access to sensitive apps for users in the quarantine until they are safe:
4. Emulate a phishing campaign to test your user base using tools such as getgophish.com.



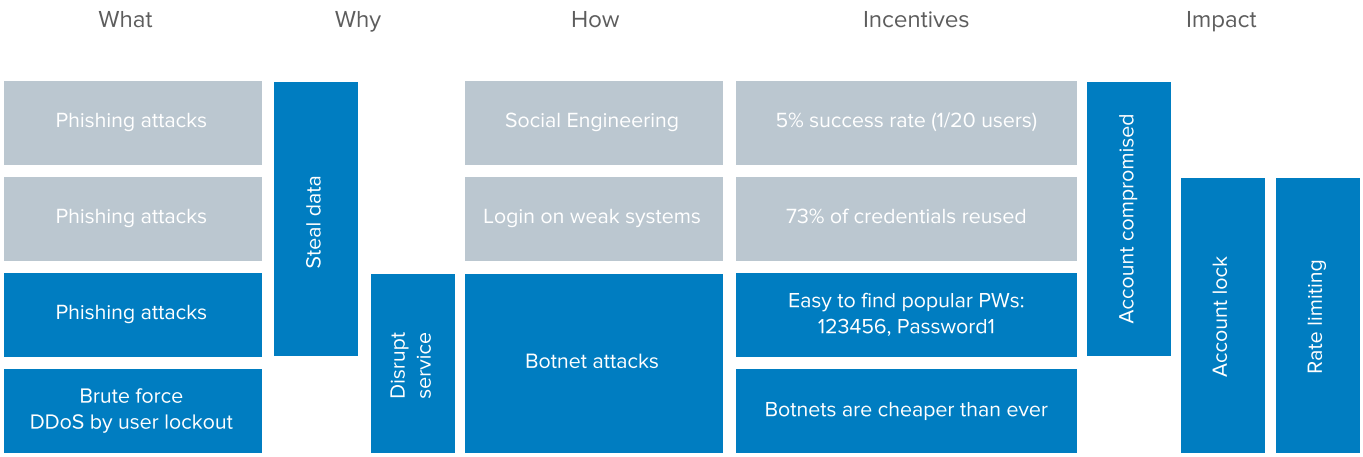
To focus exclusively on Credential Stuffing



Start by implementing the recommendations from Improve Password Policy and Implement Multi-Factor Authentication with special emphasis on a password campaign. In addition, consider:

1. Improve password requirements, reduce the time for resetting passwords, and reset passwords of all the current users.
2. Educate your users about haveibeenpwned.com and the importance of using different passwords per system.
3. Protect partners with MFA on top of inbound federation.
4. Once available, implement factor sequencing and passwordless.

To focus exclusively on Botnet attacks (including Brute Force and Password Spraying)



Start by implementing the recommendations from Implement Multi-Factor Authentication with special focus on closing legacy authentication on Office 365 (according to our support, 70% of the botnet attacks we see are targeted at legacy Office protocols: IMAP and POP).

Then, implement recommendations from Configure Network Zones and Improve Password Policy to further mitigate botnet attacks.

In addition, consider:

1. Implement new product features like the Okta Pre-Auth Policy Evaluation, Factor sequencing (with password as the last factor), and Okta ThreatInsight.
2. Review and tweak policies on your security analytics system tools to detect botnet attacks on other resources.
3. If you use Active Directory, double-check your password policies to ensure you're not blocking Desktop Authentication.
4. Ask your users to notify security in case of any suspicious email notification.

Appendix B:

Guidelines for detecting and monitoring threats in flight

This section provides guidelines on how to identify and monitor common identity threats using Okta System Logs.

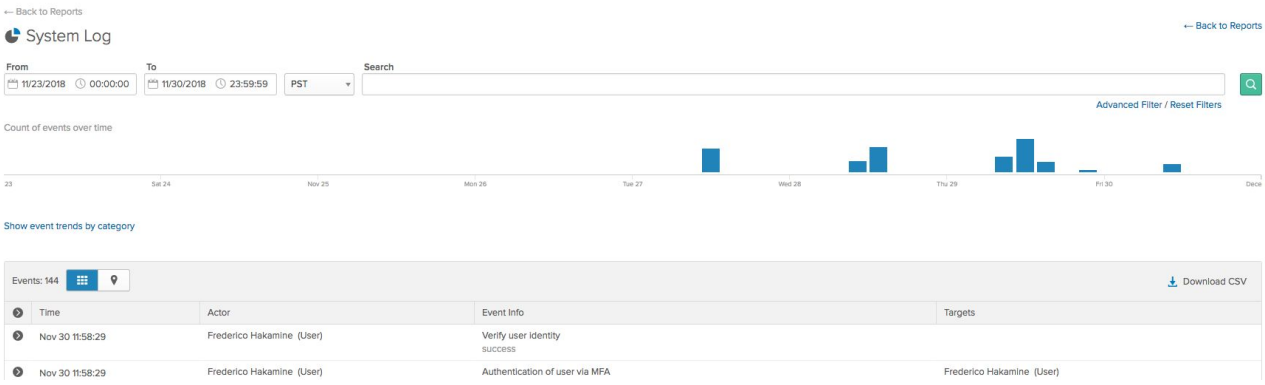
Tips

- The Okta System Logs monitor events that happen on the Okta UI and APIs.
- If you already have a Security Analytics System–i.e.: SIEM or a CASB – integrate this system with Okta and leverage its features to automate the threat detection and response (you can use the examples from this appendix for guidance on what to look for).
- If you want to filter the system logs results using Terminal commands (like grep and awk) or using Excel, export the Okta System Log results to CSV:

Download CSV

Access System Logs

To access the system logs, login to your Okta org as administrator. In the Admin console, go to **Reports > System Logs**.



Okta System Logs

The System Log page contains:

- **The search fields** – located on the top of the page – can be used to filter events. You can filter events occurring in specific time frames or using a search criteria.
- **The event count diagram** – located under the search fields – displays how many events happened over time. You can click the diagram bars to filter the events displayed.
- **The Show event trends by category link** – shows the event count diagram per specific applications (targets), users (actor), and event type.
- **The events table** – shows the results for your searches. Observe that each row can be expanded – to display details about the event – or clicked – to use information in the event as search criteria.

Search queries

The following search queries can be used to identify basic events and be combined to gather valuable insights:

Users

Events for a unique user

```
actor.alternateId eq "user@emaildomain.com"
```

Events for multiple users with the same email domain

```
actor.alternateId co "@emaildomain.com"
```

Geo locations

Events from a city

```
client.geographicalContext.city eq "San Francisco"
```

Events from a state

```
client.geographicalContext.state eq "California"
```

Events from a country

```
client.geographicalContext.country eq "United States"
```

User agents

Events from a specific browser

```
client.userAgent.browser eq "CHROME"
```

Events from a specific operating system

```
client.userAgent.os eq "Windows 10"
```

Rate limit alerts

Rate limit warning reached (triggered when the org is at 60% of its limit):

```
eventType eq "system.org.rate_limit.warning"
```

Rate limit violation (triggered when the org exceeded the rate limit)

```
eventType eq "system.org.rate_limit.violation"
```

Account Lockouts

Lockouts on legacy Office 365 authentication

```
outcome.result eq "FAILURE" and and outcome.reason eq "LOCKED_OUT"
and debugContext.debugData.requestUri co "sso/wsfed"
```

Lockouts on modern authentication:

```
outcome.result eq "FAILURE" and and outcome.reason eq "LOCKED_OUT"
and debugContext.debugData.requestUri co "api/v1/authn"
```

Access and login attempts

Requests blocked by blacklist rule

```
eventType sw "security.request.blocked"
```

Login attempts

```
eventType sw "user.session.start"
```

Successful login attempts

```
eventType sw "user.session.start" and outcome.result eq "SUCCESS"
```

Failed login attempts

```
eventType sw "user.session.start" and outcome.result eq "FAILURE"
```

Failed login attempts due to incorrect password

```
eventType sw "user.session.start" and outcome.result eq "FAILURE"
and outcome.reason eq "INVALID_CREDENTIALS"
```

Failed login attempts due to account lockout

```
eventType sw "user.session.start" and outcome.result eq "FAILURE"
and outcome.reason eq "LOCKED_OUT"
```

Policy evaluated during login attempts

```
eventType sw "policy.evaluate_sign_on"
```

Access after successful login

Access to Okta's admin console

```
eventType eq "user.session.access_admin_app"
```

Access to application with SSO provided by Okta

```
eventType eq "user.authentication.sso"
```

Audit trail specific sessions

```
authenticationContext.externalSessionId eq "<SESSION_ID>"
```

Changes in Configuration

Changes in user data

```
eventType sw "user.lifecycle"
```

Changes in group membership

```
eventType sw "group.user_membership"
```

Changes in application configuration

```
eventType sw "application"
```

Changes in security policies lifecycle

```
eventType sw "policy"
```

Using queries to identify threats

Example 1: Is my org under password spraying or brute force attack?

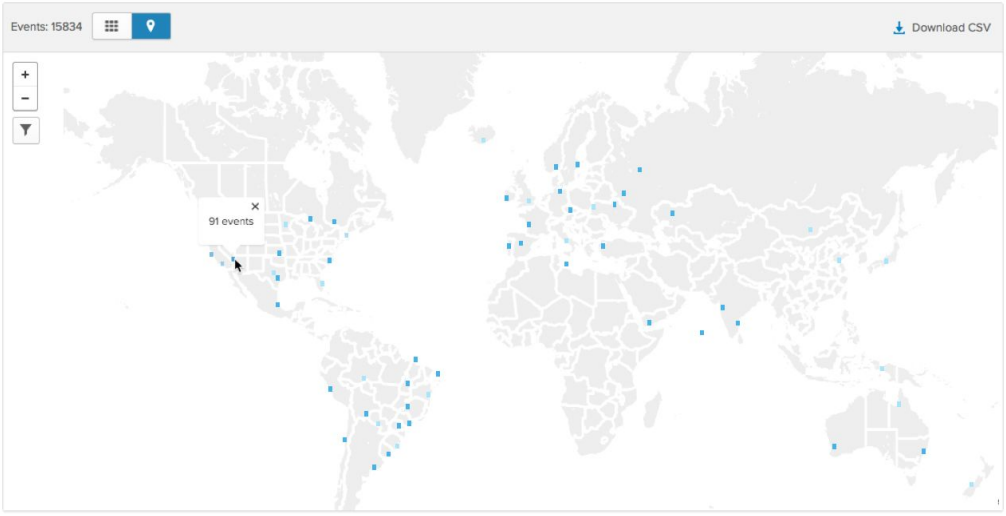
1. Search for login attempts.

```
eventType sw "user.session.start"
```

2. On the search results, look for signs of password spraying or brute force:

a. **Peak on number of login events.**

b. **Increase in login events from countries or regions you don't have business**. (i.e. This map shows a considerable number of login events originated in South America, Europe, and the US):



3. Search for login attempts from unknown agents.

```
eventType sw "user.session.start" and client.userAgent.os
eq "unknown"
```

4. On the search results, look for the same signs of password spraying or brute force listed in step 2.

5. Search for failed login attempts due to account lockouts.

```
eventType sw "user.session.start" and outcome.result eq
"FAILURE" and outcome.reason eq "LOCKED_OUT"
```

6. On the search results, look for the same signs of password spraying or brute force listed in step 2.

7. In addition, look for the user accounts locked and the number of login attempts after the account was locked out.

Example 2: Is someone in my org under a credential stuffing attack?

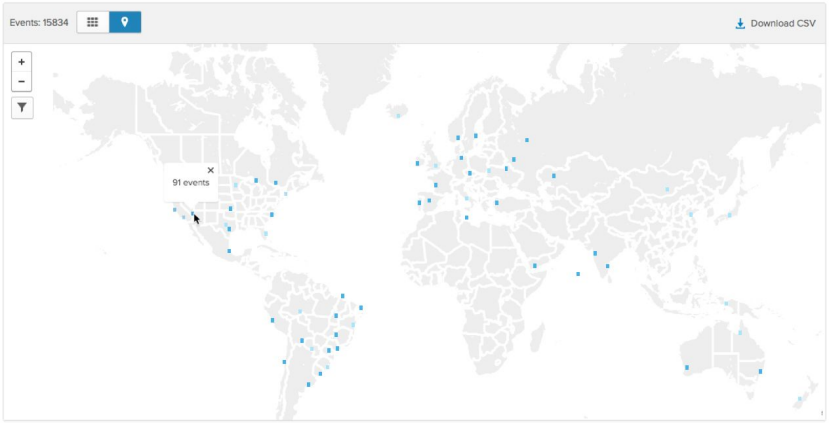
1. Search for login attempts from a specific user.

```
actor.alternateId eq "user@emaildomain.com" and eventType sw
"user.session.start"
```

2. On the search results, look for signs of multiple login attempts for the same account.

3. In addition, look for geographically distributed login attempts in the last 24 hours.

   Tip: To check requests in the last 24 hours, use the From and To fields.



4. Search for login attempts from unknown agents.

```
actor.alternateId eq "user@emaildomain.com" and eventType sw
"user.session.start" and client.userAgent.os eq "unknown"
```

5. On the search results, look for the same signs of password spraying listed in steps 2 and 3.

Example 3: Is someone in my org phished? Is an account compromised?

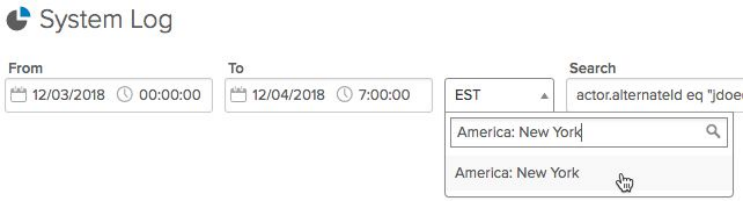
1. Search for successful login attempts (you can search by a specific user or the entire population).

```
actor.alternateId eq "user@emaildomain.com" and eventType sw
"user.session.start" and outcome.result eq "SUCCESS"
```

2. From the search results, look for successful login attempts from:

   a. Places the user is not working from (you can use the map feature to view the access per location).

b. Times when the user is not expected to log into your system (you can use the from/to and the timezone fields to filter the results.



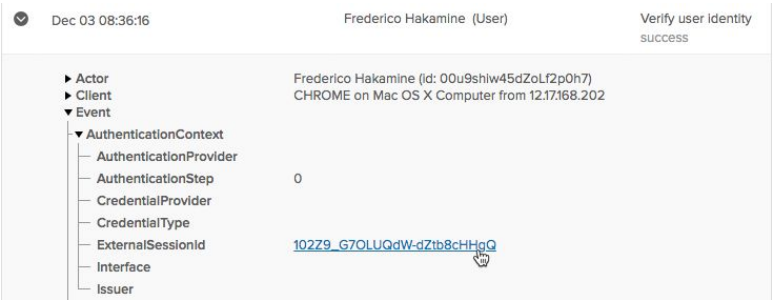
3. If you find a suspicious login, contact your user to confirm his login activity.

Example 4: An account got compromised. What factor(s) is/are compromised and what happened in the breached session?

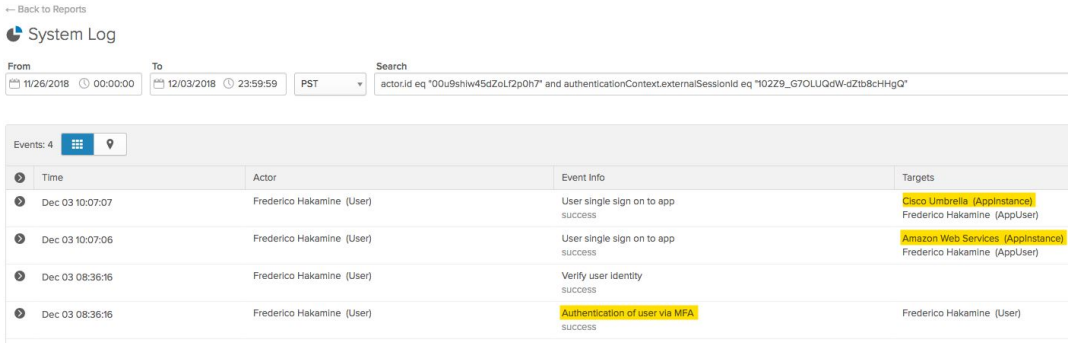
1. Use steps from Example 3 to detect an account compromise and isolate the sessions started by the attacker.

2. For each session compromised, expand the log entry > Event > Authentication Context.

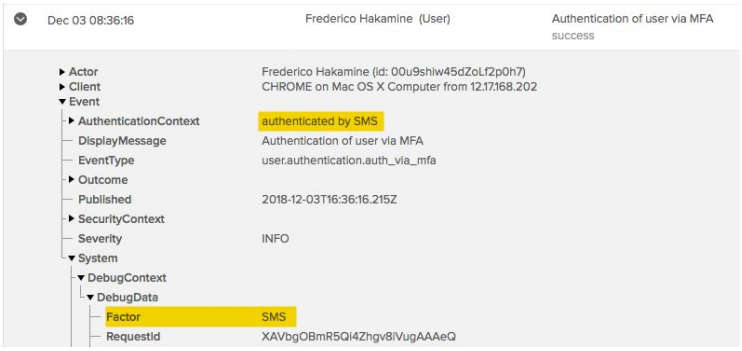
3. Click the ExternalSessionId.



4. The results will show which actions were performed by the attacker in the user console and how the attacker logged into Okta.



5. If you had a login with MFA, you can expand the MFA authentication to discover which MFA factor was compromised.



6. If the account compromised is an admin account in Okta, execute the following search to investigate an access to the admin console (use the same timeframe as the account compromise to narrow down the results):

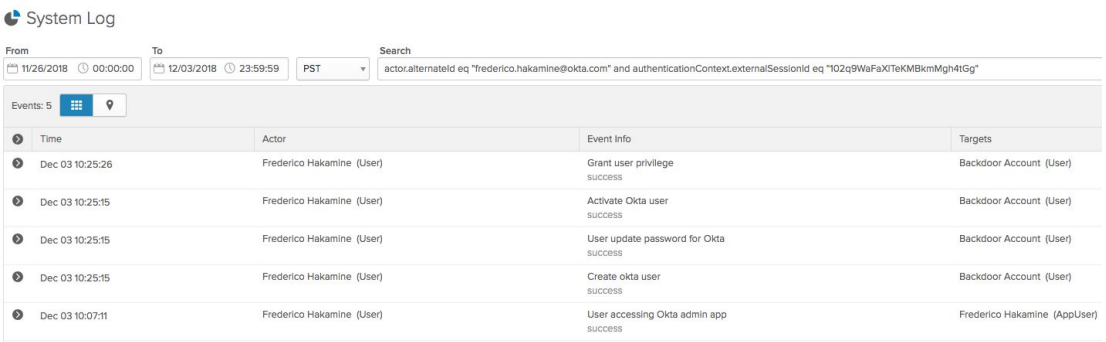
```
actor.alternateId eq "user@emaildomain.com" and eventType sw
"user.session.access_admin_app"
```

7. Expand the log entry > Event > Authentication Context and click the ExternalSessionId.

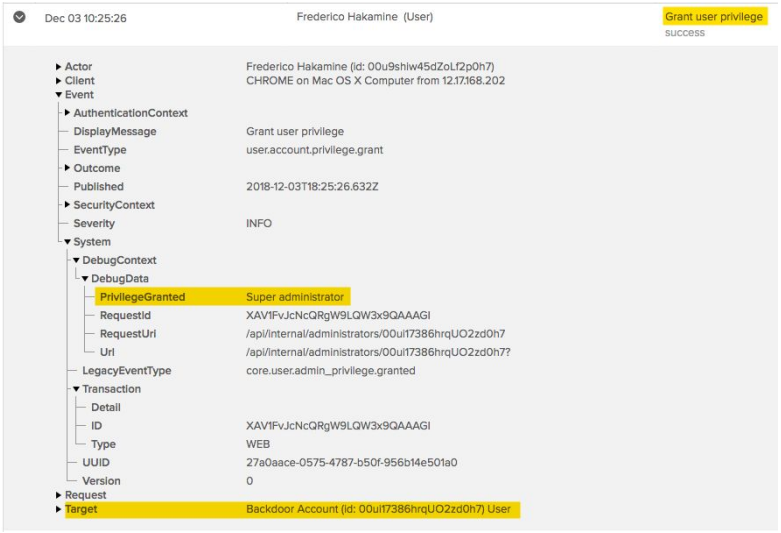
8. Confirm that the search criteria is updated to:

```
actor.alternateId eq "user@emaildomain.com" and
authenticationContext.externalSessionId eq
"1026zh97bHDRhG0HKdVuMGgIA"
```

9. The results will show all the administrative tasks executed in the compromised admin session: *(In this example, the attacker created a backdoor account and assigned admin privileges for the account)*:



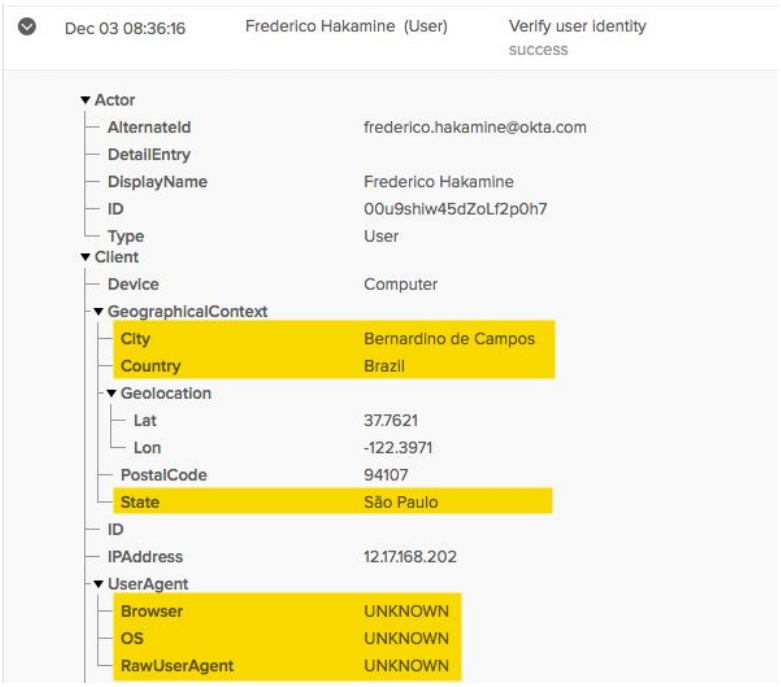
10. For details about each event, expand the syslog entry:



Example 5: Do we have other at-risk or compromised user accounts?

1. Use steps from examples 1 and 3 to detect threats or account compromises.

2. Expand a request identified as a threat and identify login anomalies (locations, agent, login time, etc).



3. Use the anomalies identified to search for other login attempts. For example:

   All activities originated from an unknown operating system

   ```
   client.userAgent.os eq "unknown"
   ```

   Successful logins from an unknown operating system

   ```
   eventType sw "user.session.start" and outcome.result eq
   "SUCCESS" and client.userAgent.os eq "unknown"
   ```

   Failed login attempts due to account lockout from an unknown operating system

   ```
   eventType sw "user.session.start" and outcome.result eq
   "FAILURE" and outcome.reason eq "LOCKED_OUT" and
   client.userAgent.os eq "unknown"
   ```

   Failed login attempts due to incorrect credentials from an unknown operating system

   ```
   eventType sw "user.session.start" and outcome.result eq
   "SUCCESS" and client.userAgent.os eq "unknown"
   ```

   To isolate a login attempt from a specific country, append the following to any request

   ```
   and client.geographicalContext.country eq "Brazil"
   ```

Example 6: Is my blacklist rule working?

1. Search for requests blocked with the blacklist rule:

   ```
   eventType sw "security.request.blocked"
   ```

2. From the results, you will see which requests are currently blocked.

3. Use steps from Example 1 to verify if you still have ongoing threats and then update your network zones.