



Integrating Okta and Preempt

Detecting and Preventing Threats With Greater Visibility and Proactive Enforcement

The Challenge: Smarter Attackers and Dissolving Perimeters

Modern enterprises are simultaneously confronting an unprecedented amount of change both in the threat landscape as well as in the fundamental architecture of their networks and applications. As cyberattacks have become more common and sophisticated, security teams have struggled to find practical ways to protect the organization without disrupting the business or overloading analysts.

At the same time the enterprise itself has rapidly evolved. The mobility of end users and the migration of applications to the cloud has steadily undermined the traditional perimeter approach to network security. This has created a challenging environment where security teams must address new threats and adapt to new architectures while keeping the business and its users productive.

The Solution: Extended Visibility + Adaptive Response

By integrating Preempt and Okta, security teams can extend their visibility to all applications regardless of whether are deployed locally or in the cloud, and automatically protect them from attacks and insider threats without disrupting valid users.

The Preempt solution continuously monitors and learns the behavior of every account and device in the network to identify risky behavior and threats such as compromised accounts, malware infection, lateral movement or malicious insiders. However these detections are just the first step. By integrating with both Okta OTP as well as Okta Verify Push, the Preempt Policy Engine can create an MFA challenge based on

Okta SSO

- Unified visibility into user behavior both on site and in the cloud
- Track application usage per user and challenge suspicious behavior
- Find risky usage of service accounts in the cloud

Okta MFA (Verify Push and OTP)

- Automatically challenge devices or accounts compromised by attackers
- Distinguish malware from human behavior
- Automatically protect, resolve incidents, and reduce alerts without manual effort
- Valid users stay empowered and productive

virtually any context. Then, based on the result, the policy engine can either approve and auto-resolve the event or take a different action such as block or demote the user.



Next, integration between Preempt and Okta’s Single Sign-On (SSO) allows organizations to extend these same threat detection and adaptive response capabilities to their web and cloud-based applications. The Okta SSO connector allows Preempt to track and learn user behavior on any application that uses Okta’s SSO. This provides staff with a unified view of a user’s behavior both when they are on site as well as when connected to cloud applications.

The screenshot shows the Preempt user interface for Kimberly Dickerson. The 'Activity' tab is selected, displaying a map of login history and a table of recent activities.

Login History Table:

Type	Origin	Device Type	IP Address	Time T
Domain Login	KDICKERSON_DT	Workstation (Windows)	172.16.32.140	16 hours ago
Domain Login	KDICKERSON_LAPT	Workstation (Windows)	10.52.10.218	2 days ago

For example, when analyzing a potentially compromised user, staff can quickly determine if the user has cloud access or not to better judge the risk. Likewise, Preempt can identify abnormal usage of a cloud-based application, and challenge the user with a second factor of authentication via Okta Push or Okta OTP to ensure the user is not compromised by an attacker. With the integration of Preempt and Okta, staff can remove blind spots and ensure a complete picture of any user’s behavior.

Extending Multi-Factor Authentication to Any App

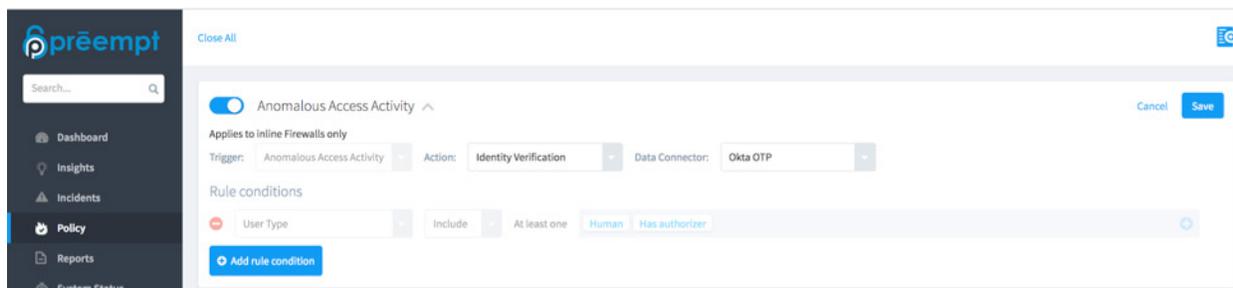
Given Preempt acts as a seamless LDAP proxy, staff can use Preempt to integrate multi-factor authentication into virtually any application. This can be particularly helpful for protecting legacy applications as well as any internally developed or custom applications. By using Preempt, organizations can easily add protections to these applications without requiring any changes or customization to the applications themselves. Protection is as simple as applying an MFA control to the appropriate security policy.

How The Integration Works

Integrating Okta into the Preempt solution is a quick and simple process. The integration is done by creating an Okta connector within Preempt. Separate connectors are available for Okta SSO, Okta Verify, and Okta OTP. In the case of Okta SSO, the Preempt solution will automatically ingest data from Okta and begins displaying cloud-based information in the user interface as soon as the connector is added.

For Okta MFA integration, staff will also need to apply the appropriate connector (Okta Verify or OTP) to a security policy. Policies are based on behavior, user, user risk score, target, role, and other factors, and can adapt over time as new information is collected. The policy can trigger iterative actions that can collect more information or enforce controls based on the situation.

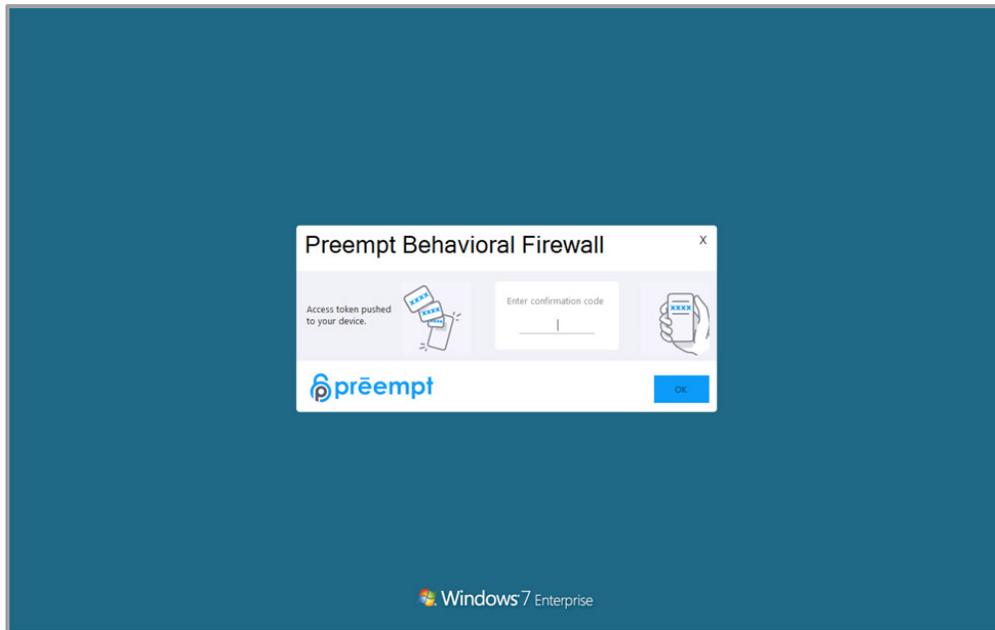
The image below shows an example of a Preempt policy. This policy invokes Okta OTP to verify a user's identity in response to anomalous behavior such as a user connecting from an endpoint they normally don't use.



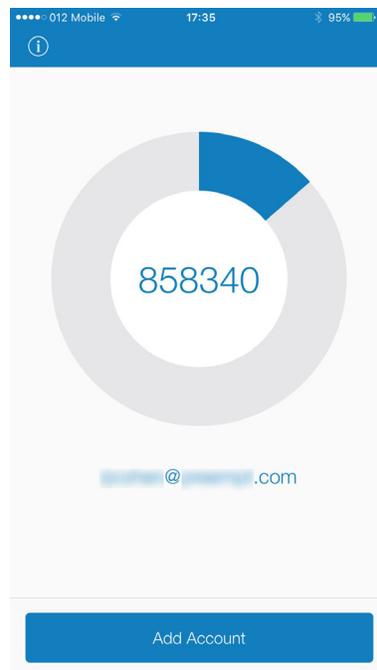
The User Experience

When the above policy is triggered, Okta will send a challenge to the user. The user process will vary slightly based on whether Okta OTP or Okta Verify is in use.

In the case of Verify OTP, the user will receive a one-time code on his enrolled device. The suspect device will be presented with a challenge page where the code can be entered.



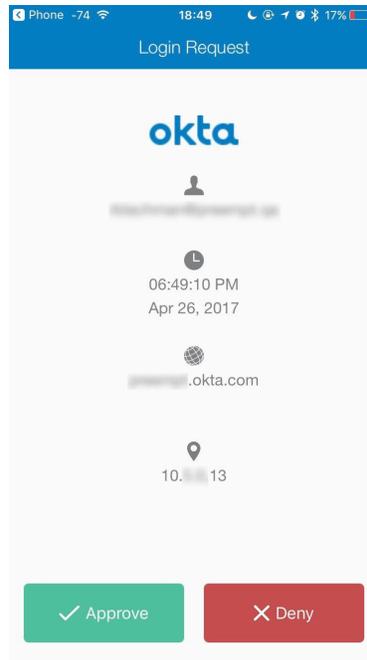
Notification to the suspect device



Verify OTP challenge code sent to the user's mobile device

As soon as the end user enters a code the OK button enables, the code is then verified and the user is granted access. If the user verification code is valid, the Preempt Behavioral Firewall logs the transaction but does not create an Incident, eliminating the need for unnecessary security analyst work. If the end user fails to enter the correct code or closes the dialog it will be logged as an incident, the severity raised and escalated based on policy.

The process is virtually the same for Verify Push, however instead of a one-time code, the user receives a simple "Approve" or "Deny" challenge to the enrolled device.



Verify Push challenge sent to the user's mobile device

Integration Details

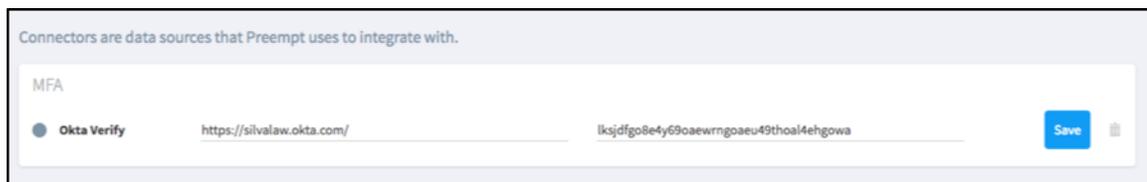
This sections walks through the steps to integrate Okta SSO, Okta Verify OTP and OKta Verify Push with Preempt. This will cover the information you will need to collect, and a step-by-step walkthrough of setting up the connector. Note that the integration will require an Okta Administrator Token in order to create the connector.

Key Steps

	Task	Description
1	Create a new Okta connector	In the Preempt User Interface, go to Configuration/ Connectors and choose the Okta SSO, Okta Verify, or Okta OTP option from the drop down menu and click "Add".
2	Enter the domain of the Okta Portal	Configure the connector with URL of the company's Okta portal. E.g. company.okta.com.
3	Enter the Okta API Administrator Token	The Okta API Token is available from the Okta UI. Details on creating and obtaining this Token are available here .
4	Add the connector	Once the domain and token are entered correctly, click "Save"
5	Enroll End Users (Only for MFA Integration)	Make sure Users are enrolled to OKTA MFA. Instructions are available here .
6	Apply control to security rule (Only for MFA integration)	Use the newly created connector to apply a control to a Preempt policy.
7	Test the integration	For MFA integration, trigger activity that violates the selected Security Rule. For SSO Integration, create a custom Insights with cloud-enabled as an attribute to view stats.

Configure Data Connector

1. Connect to Preempt user interface. Go to Configuration/Connectors. Select the appropriate Okta connector from the dropdown list and click on Add. The Data Connector is now added.
2. Collect and enter following information into the connector configuration page:
 - a. URL of the company's Okta Portal
 - b. The Okta Administrator API Token. More information about this token is available here: http://developer.okta.com/docs/api/getting_started/getting_a_token.html

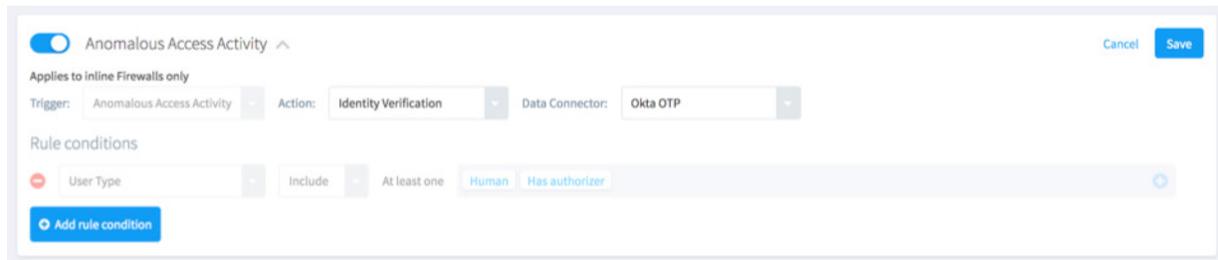


3. Click SAVE when done. The indicator will turn green within a minute, indicating the connection was successfully established. If this is not the case try the following:
 - a. Refresh the page
 - b. Verify the Hostname is accessible
 - c. It might be that one of the parameters was wrongly entered. Enter again and click Save.
4. Configuration of the Data Connector is now completed.

Apply Control to Security Rule

This step is only required for integrations with Okta MFA

1. In Preempt UI, select Policy from the main menu.
2. Select the policy or policies you want to control with Okta Verify and then click Edit. Select the action and Data Connector as shown in the screenshot below.



3. Toggle the policy on. Click Save and then Apply all changes.

Note: alternatively you can add conditions to force the policy on specific users based on membership in OU, Site, Group or Department as well as specific names or other attributes as needed.

Test the Integration

1. Choose a user who is enrolled to Okta MFA.

2. Logon to a workstation that not associated with the user.

Note: A list of associated endpoints can be found on the user page in Preempt, simply type the username in the search bar.

3. On screen notification presented to the user on the machine they used.

About Preempt

Preempt turns behavioral analytics into real-time action that stops security breaches and insider threats without impacting your business. The solution scores the risk of every user, account, and device in the network, then delivers adaptive actions to verify and eliminate threats—all without manual intervention from your security team.

About Okta

Okta is the foundation for secure connections between people and technology. Our IT products uniquely use identity information to grant people access to applications on any device at any time, while still enforcing strong security protections. Our platform securely connects companies to their customers and partners. Today, thousands of organizations trust Okta to help them fulfill their missions as quickly as possible.