Prisma Access Browser (PAB)

**POC Test Plan**

**For**

****

**Table of Contents**

[**Overview 4**](#_w759lop3c69i)

[POC Request Information 4](#_umngivekrlub)

[**Contact Details 5**](#_uk5kysd4dsyn)

[Client Contact Information 5](#_rlxaoifogji2)

[Palo Alto Sales Engineer Details 5](#_3cq3jvkxba70)

[Palo Alto Account Team Details 5](#_jnkfkq8klz2v)

[**Getting Started with a PoC 6**](#_gswsmfo9eau8)

[Describe the customers use Cases - and the Business and Technical Problem Prisma Access Browser Solves: 6](#_8x072f1fdb91)

[**POC Checklist 6**](#_m4csm7x3y6ew)

[**Discovery 8**](#_1pu4ym1ik91k)

[**Onboarding Users to PAB 11**](#_6xhf6z7va5mg)

[**Check if PAB is enabled on the POC tenant? 12**](#_ksuaxfqg5qpa)

[**Test cases 14**](#_t1q9n8ypqo47)

[Conditional Access - Authentication from PAB only 14](#_di9soka3iy35)

[Prerequisite: 14](#_m2ooxd3vfxxv)

[Execution: 14](#_bf7dq0t5m884)

[**Test cases: 16**](#_seoy5sfxbgb5)

[Conditional Access 16](#_djnu33x894v5)

[Success Criteria for Conditional Access: 16](#_xtxzn3afvk90)

[**Test cases 16**](#_1l5129n3isei)

[Customize the browser environment 16](#_atleia8nej0m)

[Prerequisite: 16](#_tsg2neg9ffv4)

[Success Criteria for customizing the browser environment: 17](#_7f4xlervzcy9)

[**Test cases 17**](#_tngatt1bns2g)

[Unmanaged contractor device access to SaaS applications 17](#_xybibddo9ws9)

[Success Criteria for unmanaged device access to SaaS applications: 18](#_61hadoefs6pg)

[**Test cases 19**](#_npf9hs271eq9)

[Employee BYOD device access to Internal applications 19](#_6kslaz6jovet)

[Prerequisite: 19](#_rkbddhc4ifm8)

[Success Criteria for BYOD device access to Internal applications: 20](#_6wii4acr47wf)

[**Test cases 21**](#_xicry6mryski)

[Harden the browser using Browser Security rules 21](#_ukizmg76lgz6)

[Success Criteria for hardening the browser environment: 21](#_7k44r0uhib2d)

# 

# Overview

This test plan will be used to drive the PRisma Access Browser (PAB) POC evaluation. The POC sales engineer will use this document to scope and determine all test related activities and timelines.

| POC Request Information | | |
| --- | --- | --- |
| **POC ID** |  | |
| **Client Tenant ID** |  | |
| **Client Name** |  | |
| **Start Date** |  | |
| **End Date** |  | |

# 

# Contact Details

| **Client Contact Information** | | |
| --- | --- | --- |
| **Client Name** | **Mohit Rustgi** | |
| **Client Email** | **Mohit.Rustgi@startek.com** | |
| **Client Number** | **+91 98184 82225** | |

## 

| **Palo Alto Sales Engineer Details** | | |
| --- | --- | --- |
| **Core Sales Engineer Name** | **Puneet Pahuja** | |
| **Core Sales Engineer Email** | **ppahuja@paloaltonetworks.com** | |
| **Core Sales Engineer Number** |  | |
| **Prisma Access Engineer Name** | **Brijesh Paramel Pattathil** | |
| **Prisma Access Engineer Email** | [Brijesh Paramel Pattathil](mailto:bparamelpatt@paloaltonetworks.com) | |
| **Prisma Access Engineer Number** | **+919972484558** | |

| **Palo Alto Account Team Details** | | |
| --- | --- | --- |
| **Account Rep Name** | **Rajakani** | |
| **Account Rep Email** | [Rajakani K](mailto:rajk@paloaltonetworks.com) | |
| **Account Rep Number** |  | |

# Getting Started with a PoC

The first step is to fill out the form below and send it back to your sales team. We will then build a tenant for your organization and schedule a kick-off call based on your availability. PoCs typically run for 30 days (about 4 and a half weeks), but we can modify the schedule to meet your needs.

## Describe the customers use Cases - and the Business and Technical Problem Prisma Access Browser Solves:

| Managed primary use case | {ZTNA, Browser protection, Elevated users, Visibility and Shadow IT, Insider risks, Advanced DLP} |
| --- | --- |
| Unmanaged primary use case | {Contractors, VDI Alternatives, BYOD (Personal devices, Mobile), 3rd party, M&A, Secure Access to Critical Applications} |

# 

# POC Checklist

| **PAB POC Checklist - PA Tenant Readiness** | | |
| --- | --- | --- |
| Description | Requirements | |
| * Enable PAB on the Prisma Access tenant to be used for the POC |  | |
| * Config Selection Criteria  (Panorama) | Yes/No | |
| * Config Selection Criteria  (Cloud Managed) | Yes/No | |
| * Cloud Services Plugin | Verifies meets min version/image requirement | |
| * Panorama Version | Verifies meets min version/image requirement | |
| * Dataplane version | Verifies meets min version/image requirement | |
| * Envoy / Explicit Proxy | Verifies meets min version/image requirement | |
| * Target user personas | See User onboarding | |
| * List of applications to be tested | See Discovery | |
| * Daily cadence emails/calls setup with client | A daily cadence email/call to sync up on the progress of the evaluation. | |
| * Eval License Expiry Date | Eval License can be extended | |

## 

# 

# Discovery

Please list out the top 10 SaaS and internal applications that PAB users will require access to using PAB.

| **Applications** | | |
| --- | --- | --- |
| **Website (incl. path)** | **SAAS** | **Private/Internal** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Please identify the following integration points for the Prisma Access Browser. The items with an asterisk (\*) are critical.

| Security |  |
| --- | --- |
| Identity Provider (IDP)\* | {Okta, AAD, PingID, etc.} |
| SIEM | {SYSLOG, S3, Splunk, LogScale, Sentinel, etc.} |
| EDR | {Cortex, CrowdStrike, Defender, etc.} |
| File Reconstruction | {OPSWAT, etc.} |
| Cloud |  |
| Cloud computing | {AWS, Azure, GCP} |
| Network |  |
| VPN | {GP, Pulse} |
| Palo Alto products deployed | {Prisma Access, Cortex, GP, SD-WAN, etc.} |
| DLP | {MPIP/AIP/MIP, Symantec, Forcepoint DLP} |
| Workflow |  |
| IT Support Automation | {ServiceNow, etc.} |
| Orchestration Tools | {Davinci, etc.} |
| Critical Apps |  |
| SaaS Apps (mention internal or external) | {Excel, SAP} |
| Desktop Apps (mention internal or external) | {Workday, Salesforce, etc.} |
| Productivity Suite | {Office365, GSuite, etc.} |
| File Sharing | {Box, G-Drive, etc.} |
| Extensions approved/deployed/declined | {LastPass, MS Proxy, etc.} |
| MDM | {Intune, MDM} |
| RBI | {Fireglass, Ericom, Menlo, Garrison} |
| Other security tools | {xxx} |
| Quantity of test users | {x} |

## 

# 

# Onboarding Users to PAB

CIE is required for Prisma Access Browser (PAB) to authenticate users. CIE must be integrated with the customer’s Identity management provider via a SAML and Directory Sync profile. Local user accounts are not supported in the current release.

For each use case implemented for the POC , identify the users and user-groups to onboard to PAB for the POC. The identified users and user-groups should have different job roles. HAving different job roles will be used to demonstrate how the PAB rules can be applied to allow ZTNA access by user, device and application.

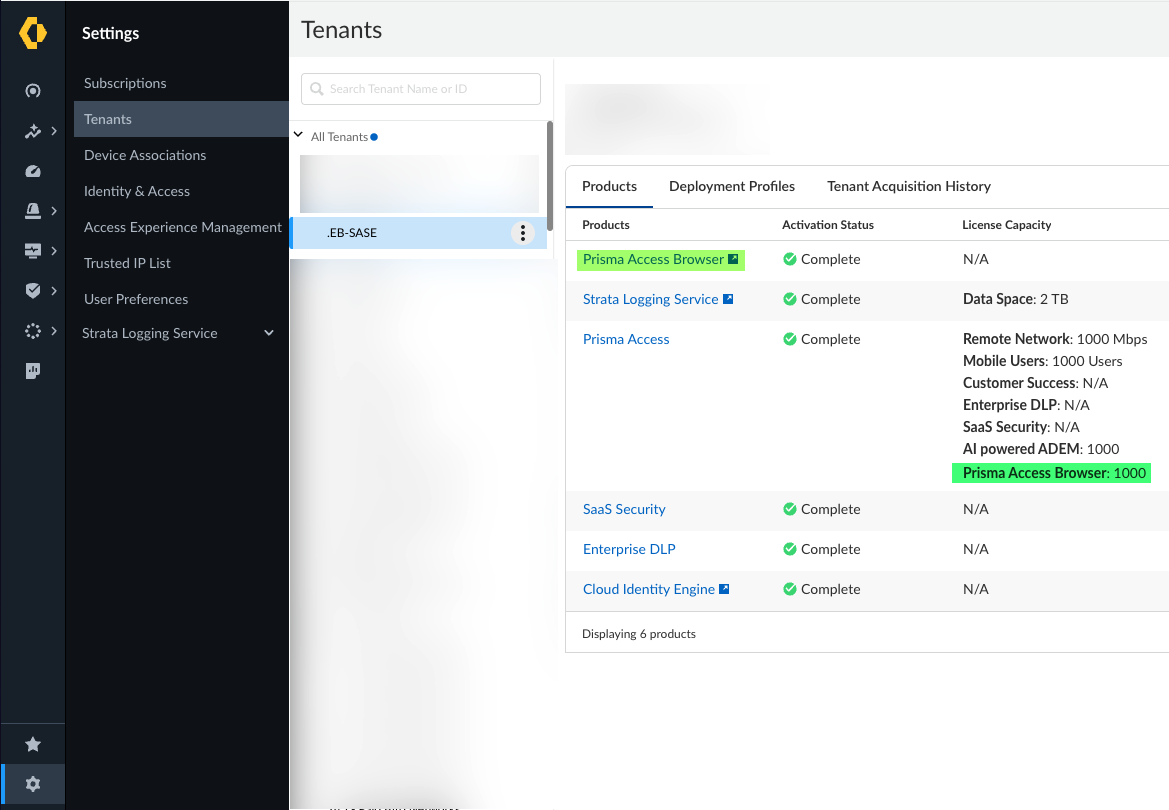
| **User Groups** |
| --- |
| Identify the users and user-groups to onboard to PAB for the POC use cases. |
|  |

# Check if PAB is enabled on the POC tenant?

Prior to starting a PAB POC, PAB must be licensed and enabled on the tenant.

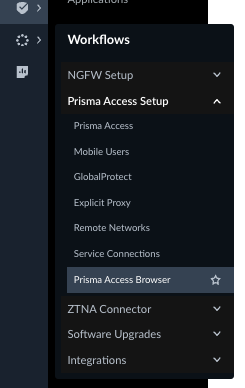
For information on the steps to submit an evaluation license please review this doc *<insert link to the SE license activation document>*

If the PAB add-on has been enabled on the tenant, verify the licenses are tied to the correct tenant and show up under the Tenants Tab.



Another way to check is , PAB tabs showing up under configure and manage options in SCM if the tenant is running correct versions.

Go to Workflows → Prisma Access Setup → Prisma Access Browser

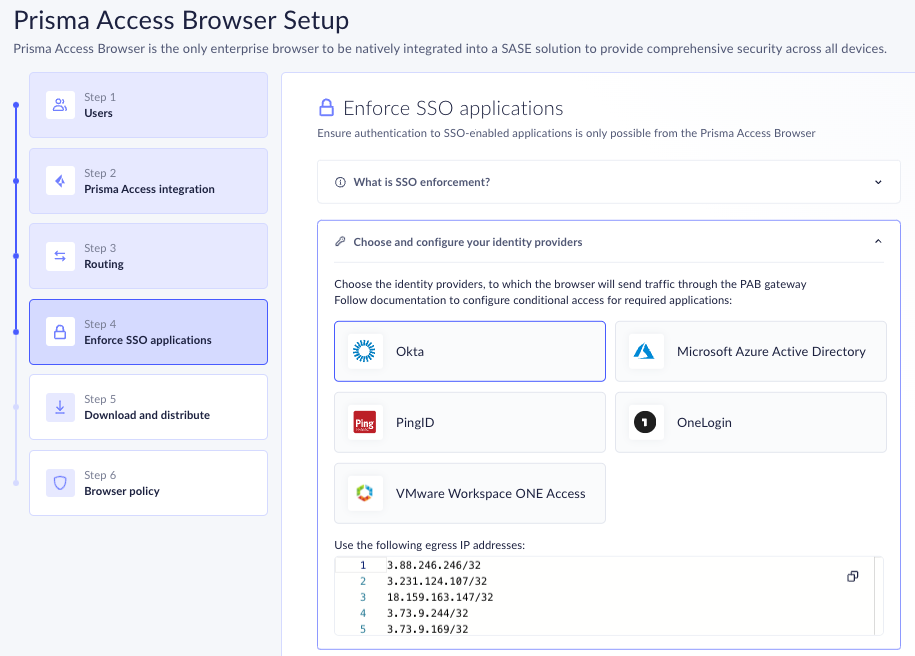


# Test cases

## **Conditional Access - Authentication from PAB only**

#### Prerequisite:

* SSO must be enabled
* The Identity Provider (IdP) need to be configured to whitelist only the IP addresses of the PAB Identity Proxies

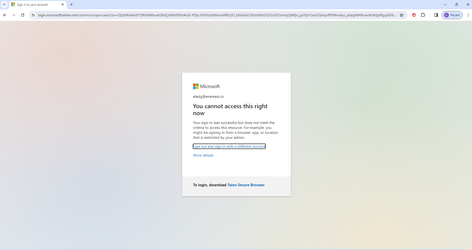


Identity the application to test and verify the conditional access rules only allow authenticated access from PAB.

For customers using O365, integrate SSO and add the Prisma Access egress IP’s to the IP whitelisting settings in the customers Azure AD service.

#### Execution:

1. Conditional Access / Auth Proxy - Navigate to [office.com](http://office.com) using Chrome
2. 2. Open PAB, complete the user authentication



The login prompt will fail to enable access to the application for the users.

Demonstrate the same user account used on Chrome is now enabling access.

# Test cases:

## **Conditional Access**

#### Success Criteria for Conditional Access:

| **Conditional Access Test** | **Pass/Fail** | **Notes** |
| --- | --- | --- |
| **SSO** |  |  |
| Demonstrate SSO and how only PAB allows authenticated access to office.com and Chrome fails to allow access |  |  |
| **Device Posture** |  |  |
| Sign-in Rules: Add device posture rules using sign-in rules and device groups |  |  |
| Sign-In Rules: Review the device posture meets the posture criteria for the device used for the POC |  |  |
| Check - Block access when Serial Number is not matched |  |  |

# Test cases

## **Customize the browser environment**

Goals to demonstrate for this use case:

* Enable the Browser Customization rules to improve the user experience by customizing the Prisma Access Browser to create a company branded secure workspace
* Demonstrate how the secure workspace can be customized by Forcing installation of an extension adding Managed Shortcuts, and Managing the Upgrade schedule

#### Prerequisite:

* Company Logo Downloaded
  + Recommended File Format: PNG or SVG
  + Recommended Pixel: 600PX
  + Max up to 1MB
  + Background should be Transparent for logo
* Gather URLs for applications that should show up as Shortcut on Homepage and be bookmarked
  + Private application URLs
  + SaaS Application URls
  + Optionally you can upload logos if needed for these applications
* Find the Extension that you want to force Install
  + Open the Chrome Web Store. Find and select the app or extension you want. Look at the URL. The ID is the long string of characters at the end of the URL.

#### Success Criteria for customizing the browser environment:

| **Browser Customization** | **Pass/Fail** | **Notes** |
| --- | --- | --- |
| Add company name and company logo |  |  |
| Managed Shortcuts |  |  |
| Maintenance for Browser Upgrade |  |  |

# Test cases

## **Unmanaged contractor device access to SaaS applications**

For this use case, you are the IT Admin, and your company has decided to outsource its call center to a firm where agents are working with multiple clients. Call center agents will need access to only 2 apps: webmail and your CRM (*e.g.,* Salesforce) but it contains sensitive information which the call center agents do not need to access. They simply need to enter details of the call in the CRM and use email.

This use case will build upon the Sgn-in rules configured at the start of POC guide to enforce device posture as an enforcement point.

Goals to demonstrate for this use case:

* Enable the DLP controls for the SaaS applications selected by the customer
* Demonstrate how the controls are applied to enforce secure access as required by application permissions required for the job roles of the user and how to apply least privileged access based on the scope of the rules.

In this Use Case we will:

1. Provide access to Corporate CRM
2. Ensure that agents cannot utilize credentials from personal accounts (to access the same CRM application)
3. Hide confidential data from being seen by the call center agents
4. Ensure that all downloads are blocked
5. Add a watermark to CRM pages
6. Block users from printing
7. Block users from sharing their screen

Maintain the Browser customization and Device group posture settings configured from the previous test use case configurations.

#### Success Criteria for unmanaged device access to SaaS applications:

| **DLP Feature to test** | **Pass/Fail** | **Notes** |
| --- | --- | --- |
| **DLP** |  |  |
| Block Downloads |  |  |
| Block Printing |  |  |
| Block Screenshare / Screen Capture Controls |  |  |
| Watermarking |  |  |
| Masking / Redaction / Unmasking |  |  |
| **User Workflows / Scalability** |  |  |
| Prompt |  |  |
| MFA (Optional) |  |  |
| **Event logs** |  |  |
| Recording of DLP events |  |  |
| Review event logs |  |  |

# Test cases

## **Employee BYOD device access to Internal applications**

Employees need access to internal applications, based on their job role, that are hosted in the customers private network or managed data center.

This use case will build upon the Sgn-in rules configured at the start of POC guide to enforce device posture as an enforcement point.

#### Prerequisite:

* Make sure SC is setup with Private Apps accessible in the datacenter
* Internal DNS Servers Configured for the private applications/Internal Domains
* Security Policy Configured on Prisma Access to Allow this traffic
* List of Private Applications configured under Manage → Prisma Access Browser → Applications
  + Under Private Applications Tab add your Private Applications

Goals to demonstrate for this use case:

* Enable private app access without Global Protect or any VPN client
* Enforce the the same levels of DLP and ZTNA controls applied to SaaS application as applied to internal applications

Important features for BYOD device access use cases include:

* Browser Enforcement
* Access Control
* Device Posture
* Granular DLP controls
* Admin Approval
* File Encryption
* Watermarking

For this use case, you are an IT Admin, and your company has decided to allow users to allow personal devices to access web content. In this use case, employees can browse to wherever they would like but business data will be isolated to only business websites. Additionally, harmful and inappropriate websites will be blocked, and file sharing sites will require admin approval.

#### Success Criteria for BYOD device access to Internal applications:

| **DLP feature to test** | **Pass/Fail** | **Notes** |
| --- | --- | --- |
| **DLP** |  |  |
| Cut/Copy/Paste Controls |  |  |
| Restrict Printing |  |  |
| Screenshare / Screen Capture Controls |  |  |
| Watermarking |  |  |
| Typing Guard |  |  |
| Masking / Redaction / Unmasking |  |  |
| **Malicious File protection** |  |  |
| Enable AWF for malicious file protection |  |  |
| **User Workflows / Scalability** |  |  |
| User Bypass |  |  |
| Admin Approval |  |  |
| **Upload / Download** |  |  |
| Encryption / Decrypt / Intra-site movement |  |  |
| Upload/Download Controls |  |  |
| **Event logs** |  |  |
| Recording of DLP events |  |  |
| Review event logs |  |  |

# 

# Test cases

## **Harden the browser using Browser Security rules**

Goals to demonstrate for this use case:

* Create the Browser Security rules to harden the Prisma Access Browser
* Apply Browser Security rules applied to the scope of the rule. Users that are classified as contractors may apply more strict browser hardening rules to reduce the attack surface of the browser.

#### 

#### Success Criteria for hardening the browser environment:

| **Browser Security** | **Pass/Fail** | **Notes** |
| --- | --- | --- |
| Browser idle lock |  |  |
| Flush browser data |  |  |
| **Browser Hardening** |  |  |
| Block developer tools |  |  |
| Block password saving |  |  |
| Block popups |  |  |
| **Extension management** |  |  |
| Block extension installation by permission |  |  |
| **Privacy** |  |  |
| Block 3rd party cookies |  |  |