



portnox™ CLEAR

Okta Integration

# Deployment Guide

October 17, 2018

## Why integrate Portnox CLEAR with Okta?

The Okta-Portnox CLEAR integrated solution offers all the benefits of SSO for cloud application access (SaaS), enhanced with extra layers of user and device authentication

The solution not only provides agile and user-friendly access, suitable for the cloud-empowered enterprise, but enhances security with always-on device risk assessment, multi-factor authentication, and network data enrichment that can be used to create specific, tailored security policies

## Introduction

The Okta-Portnox CLEAR integrated solution offers all the benefits of SSO for cloud application access (SaaS), enhanced with extra layers of user and device authentication. By tying the user to their device, as well as applications accessed, it's possible for IT departments to significantly decrease their overhead and create smarter access policies that directly address the specific security needs of their organization. Offering various options for augmenting the authentication process for SSO access, the Okta-Portnox CLEAR solution is ideal for enterprises keen on obtaining complete visibility and risk-based authorization cloud application access. The solution not only provides agile and user-friendly access, suitable for the cloud-empowered enterprise, but enhances security with always-on device risk assessment, multi-factor authentication, and network data enrichment that can be used to create specific, tailored security policies.

The benefits include:

- Risk-based authorization for SaaS applications
- Multi-factor authentication
- Expanded onboarding options to avoid access from none-sanctioned devices
- Efficient security-policy management

## Prerequisite

As a prerequisite to integrating Portnox CLEAR with Okta, you must deploy Portnox AgentP on all user devices eligible for cloud service access. Refer to the relevant Portnox documentation.

## Performing Integration

### In the CLEAR Portnox Portal

This section describes the actions you must perform in the Portnox CLEAR portal to prepare for integration with Okta.

#### A. Add the Okta service

1. In the CLEAR portal, navigate to **Settings** -> **Integration Services** -> **CLEAR Okta Service**. Click **Create new CLEAR RADIUS instance**, select a **Location** and click **Create**.
2. Note the **Cloud RADIUS IP**, **Okta Port**, and **Shared Secret** values. You will need them when configuring integration with CLEAR, in the Okta Developer Console

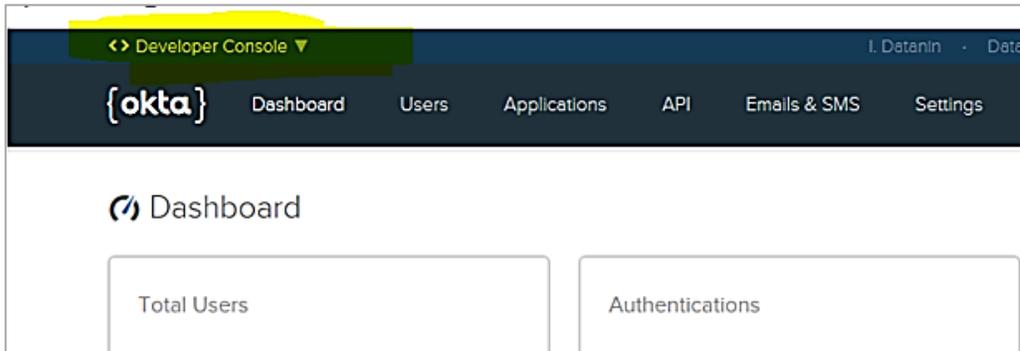
#### B. Enable Okta for user groups

1. In the CLEAR portal, navigate to **Settings** > **Groups**.
2. Click **Edit** to edit an existing group, or click **New** to create a new group for Okta authorization.
3. Select **Group Settings** > **OKTA Access** and check the **Enable OKTA access for devices in this group** checkbox.

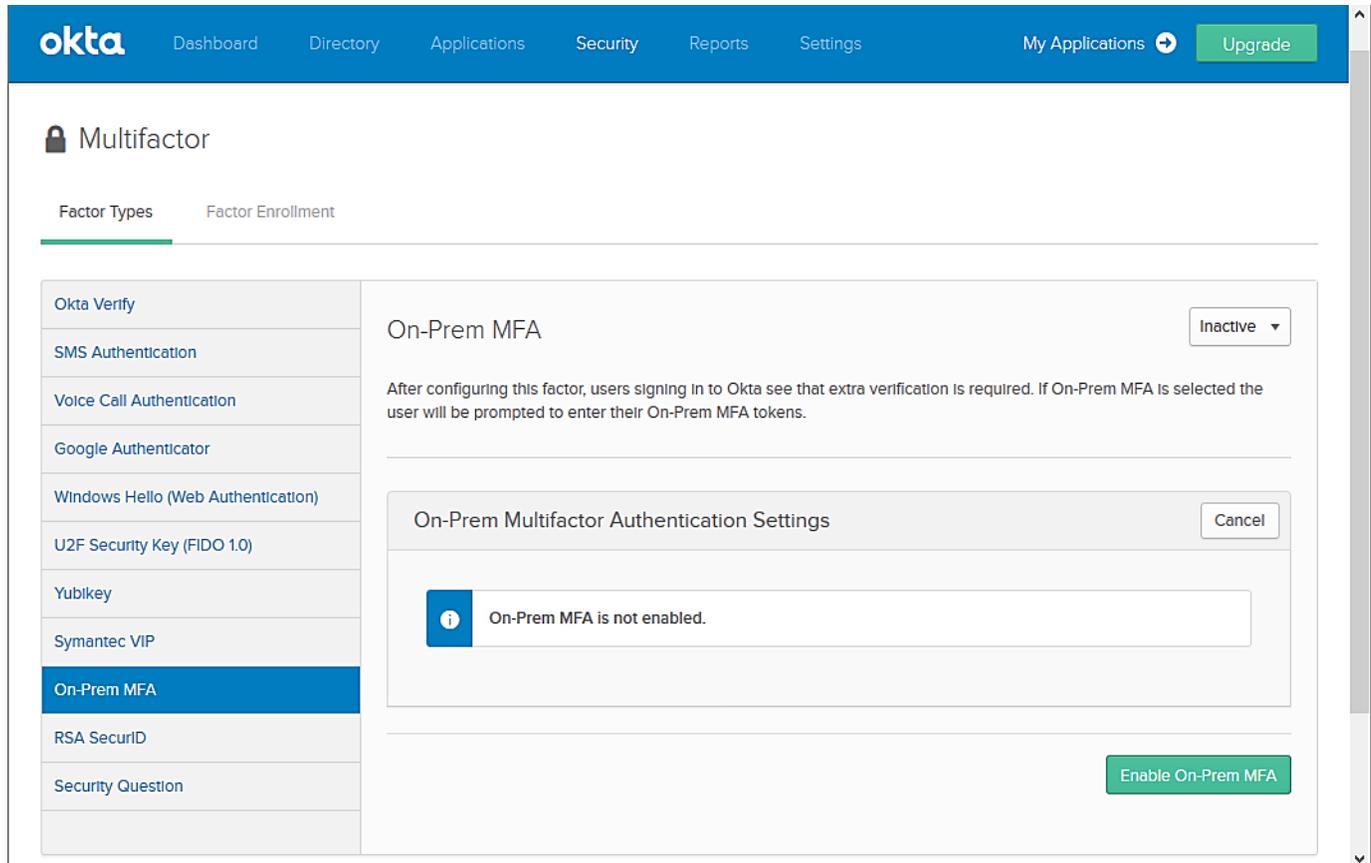
## In the Okta Console

The following actions need to be performed in the Okta Developer Console.

1. Create an Okta developer environment, or use an existing one, as follows:
  - a. To create an Okta developer environment, go to <https://developer.okta.com/signup/>
  - b. Follow the instructions in the activation email to access the environment.
  - c. Switch over to the Classic UI, using the drop-down list in the upper left corner of the screen.



2. Configure the Okta environment for general MFA setup as follows:
  - a. Select **Security > Multifactor > On-Prem MFA > Edit > Enable On-Prem MFA**.



b. Enter the following information, and then click **Save**:

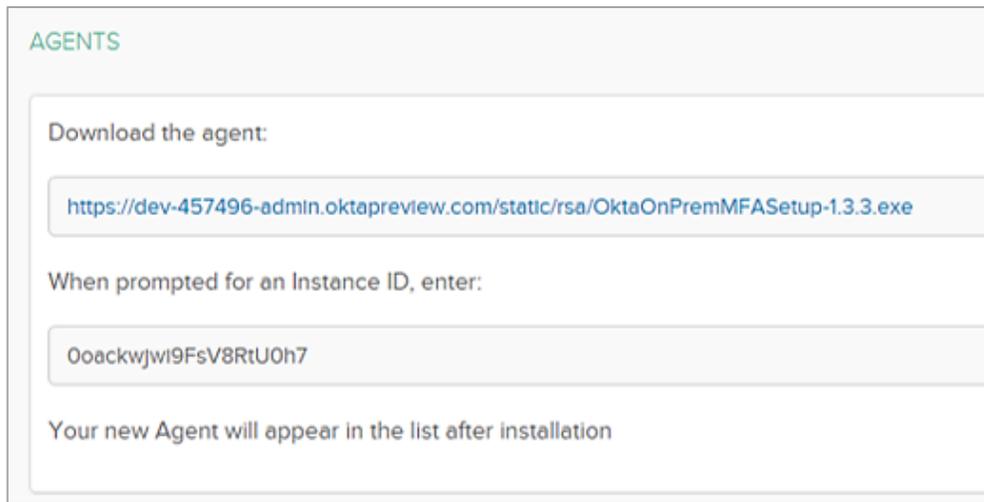
- **Provider name** – any name.
- **Provider username format** – Select **Okta username**.
- **Hostname** – the **Cloud RADIUS IP** value of the CLEAR Okta Service, noted in [Step A \(2\)](#).
- **Authentication port** – the **Okta Port** value of the CLEAR Okta Service, noted in [Step A \(2\)](#).
- **Shared secret** – the **Shared Secret** value of the CLEAR Okta Service, noted in [Step A \(2\)](#).  
Note that whenever you click **Edit** to edit the On-Prem MFA, you must re-enter the **Shared Secret** value from the CLEAR Okta Service.

The screenshot displays the Okta administration interface for configuring On-Prem MFA. On the left, a sidebar lists authentication methods: Okta Verify, SMS Authentication, Voice Call Authentication, Google Authenticator, Windows Hello (Web Authentication), U2F Security Key (FIDO 1.0), Yubikey, Symantec VIP, **On-Prem MFA** (selected and active), RSA SecurID, and Security Question. The main content area is titled 'On-Prem MFA' and includes an 'Active' status dropdown. A descriptive note states: 'After configuring this factor, users signing in to Okta see that extra verification is required. If On-Prem MFA is selected the user will be prompted to enter their On-Prem MFA tokens.' Below this is a 'Cancel' button and a section for 'On-Prem Multifactor Authentication Settings'. This section contains the following fields: 'Provider name' (text input: On-Prem MFA), 'Provider username format' (dropdown: Okta username), 'Hostname' (text input: 10.10.10.10), 'Authentication port' (text input: 1234), and 'Shared secret' (password field: masked with dots). An 'AGENTS' section features a green 'Add New Agent' button. At the bottom of the configuration area, there are 'Disable On-Prem MFA' and 'Save' buttons.

3. Install an MFA agent for the specific CLEAR+Okta environment, as follows. Note that the MFA agent can be installed anywhere (not necessarily on-premises):

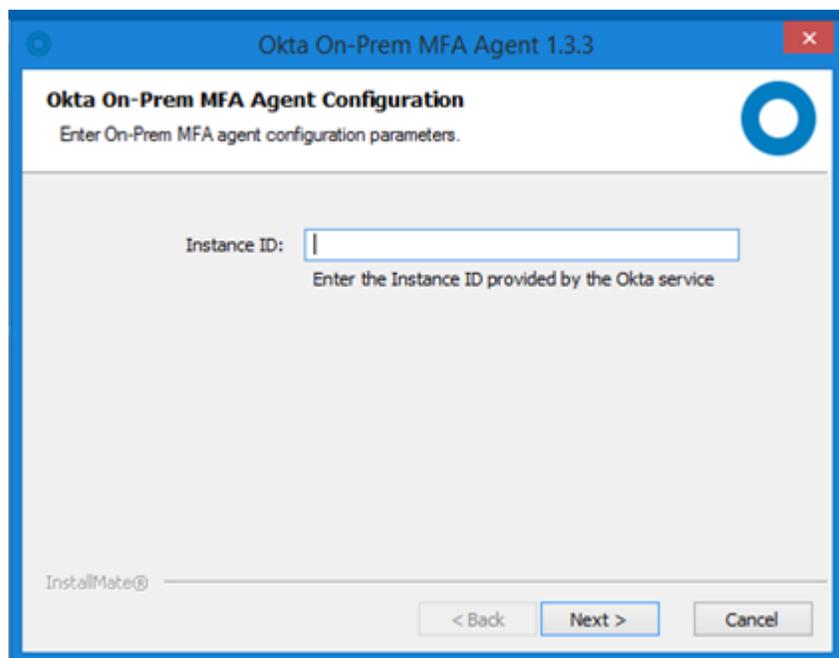
a. In the On-Prem MFA screen (shown above), click **Add New Agent**.

- b. In the **Agents** area that appears, click the link to download the agent, and note the instance ID displayed onscreen.



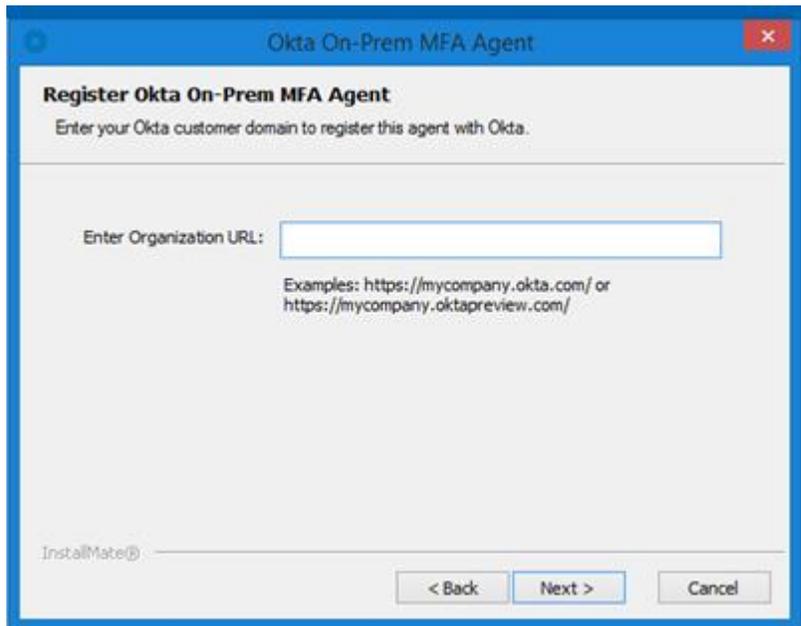
The screenshot shows a web interface with a header labeled "AGENTS". Below the header, there is a section titled "Download the agent:" with a text box containing the URL: <https://dev-457496-admin.oktapreview.com/static/rsa/OktaOnPremMFASetup-1.3.3.exe>. Below this, there is a section titled "When prompted for an Instance ID, enter:" with a text box containing the Instance ID: "0oackwjwI9FsV8RtUOh7". At the bottom of the section, there is a message: "Your new Agent will appear in the list after installation".

- c. When prompted for an **Instance ID**, enter the Instance ID you had noted in the previous step.

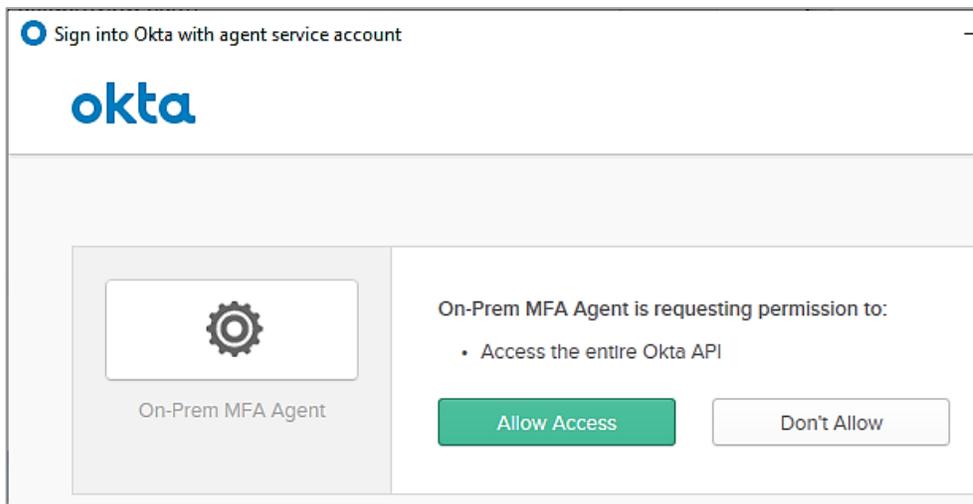


The screenshot shows a Windows-style dialog box titled "Okta On-Prem MFA Agent 1.3.3". The main title is "Okta On-Prem MFA Agent Configuration" and the subtitle is "Enter On-Prem MFA agent configuration parameters." Below the subtitle, there is a text box labeled "Instance ID:" with the text "Enter the Instance ID provided by the Okta service" below it. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted. The bottom left corner of the dialog contains the text "InstallMate®".

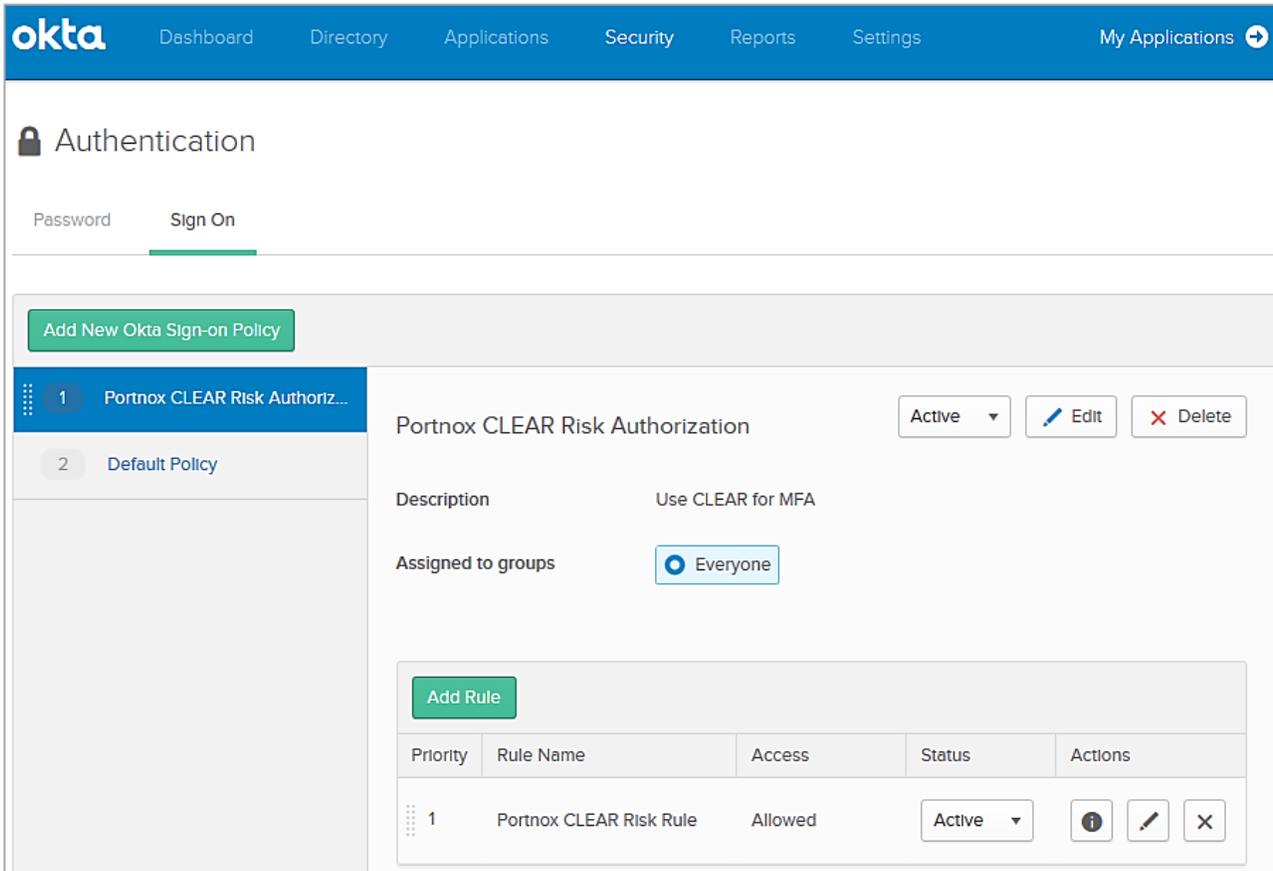
- d. When prompted for an **Organization URL**, enter your organization URL.



4. Log into Okta with admin credentials, and click **Allow Access** for the agent you configured.



5. Configure in Okta a sign-on policy requiring MFA access, for a specific user or in general, as follows:
  - a. Make sure you created at least another user in your Okta environment that does NOT require MFA, to avoid being locked out of your own environment.
  - b. Select **Security > Authentication > Sign On**.



- c. Configure a rule that requires MFA authentication (Prompt for Factor), but make sure to exclude at least one user from this rule, to avoid being locked out of the system.

**Authentication**

Password Sign On

Add New Okta Sign-on Policy

1 Portnox CLEAR Risk Auth

2 Default Policy

### Edit Rule

**Rule Name**  
Portnox CLEAR Risk Rule

**Exclude Users**  
Exclude Users

**IF** User's IP is Anywhere  
Manage configuration for [Networks](#)

**AND** Authenticates via Any

**THEN** Access is Allowed

Prompt for Factor  
Manage configurations for [Multifactor Authentication](#)

Per Device  
 Every Time  
 Per Session

**Session expires after** 4 Hours

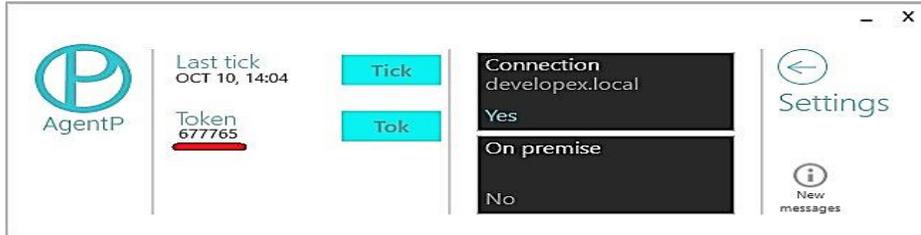
© 2018 Okta, Inc. Privacy Vers

Update Rule Cancel

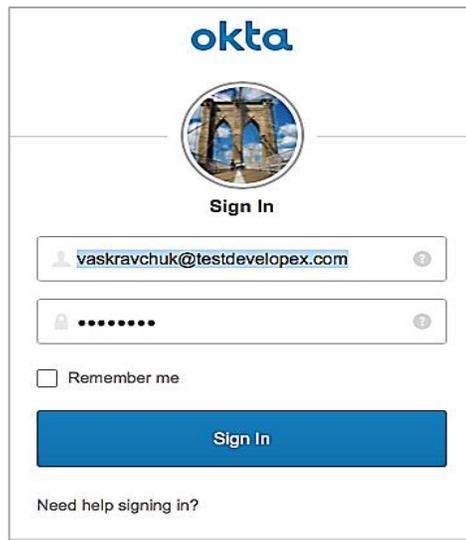
## End-user usage

Following Okta integration with Portnox CLEAR, the end-user must perform the following two-step authentication in order to access a Cloud application from his/her device.

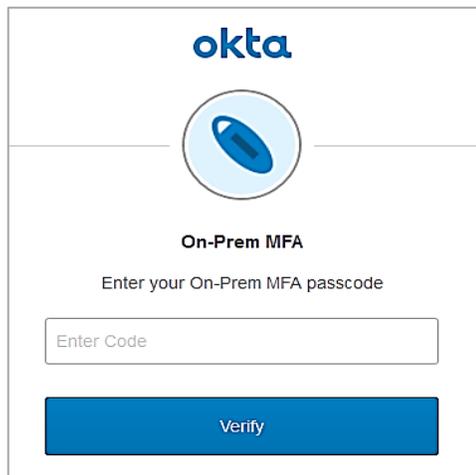
1. Login to your Portnox AgentP, click **Tok**, and note the token you receive.



2. Login to your organizational Okta portal, and enter your Okta credentials.



3. Following credential validation, you are prompted for your MFA passcode. Enter the token you noted in (1).



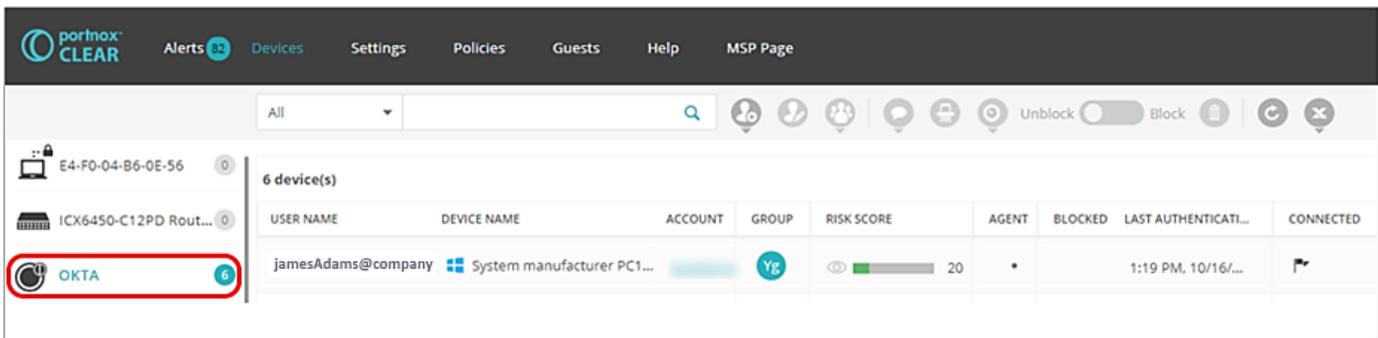
You can now access, from the Okta portal, the applications configured for you,

# Ongoing Monitoring

## Monitoring in the CLEAR Portnox Portal

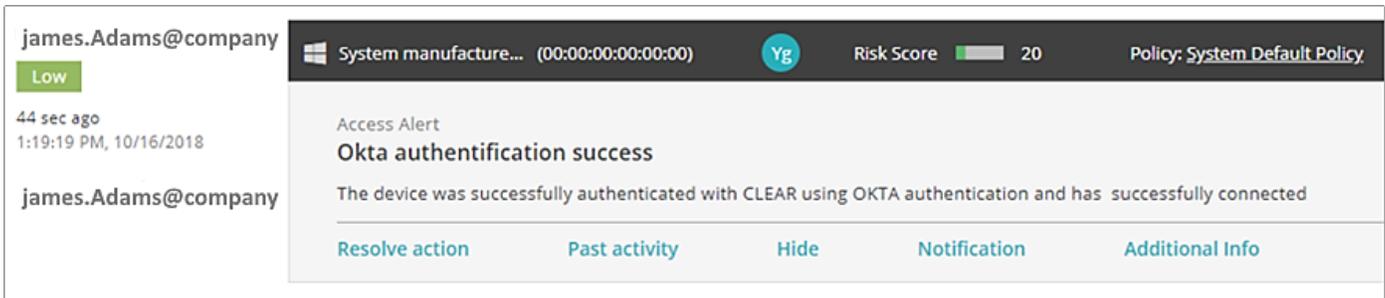
### Network page

Following successful integration, the Okta MFA Agent, indicated by the Okta icon, appears in the CLEAR portal's **Devices > Network** page, as shown in the left pane of the following figure. The right pane displays all the organizational devices that successfully connected to a cloud application after being successfully authenticated with CLEAR using Okta authentication.



### Alerts page

Okta-related alerts appear in the CLEAR portal's **Alerts** page. Successful connection to a cloud app following successful Okta + CLEAR authentication is indicated by a green icon (shown below). For unsuccessful attempts, the alert description provides details about the reason for failure.



## Monitoring in the Okta Admin Console

In the Okta console, you can monitor all events by navigating to **Reports > System log**, as shown in the following example.

← Back to Reports

### System Log

From: 10/10/2018 00:00:00 To: 10/17/2018 23:59:59 EEST Search

Count of events over time

110 Thu 11 Fri 12 Sat 13

Show event trends by category

Events: 491

Time	Actor	Event Info	Targets
Oct 17 15:25:53	James Adams (User)	Authentication of user via MFA success	James Adams (User)
Oct 17 15:25:52	James Adams (User)	Evaluation of sign-on policy challenge	Portnox CLEAR Risk Authorization (PolicyEntity) Portnox CLEAR Risk Rule (PolicyRule)
Oct 17 15:25:31	James Adams (User)	Evaluation of sign-on policy challenge	Portnox CLEAR Risk Authorization (PolicyEntity) Portnox CLEAR Risk Rule (PolicyRule)
Oct 17 15:25:31	James Adams (User)	User login to Okta success	



For further information please contact [info@portnox.com](mailto:info@portnox.com) or visit us at: [portnox.com](http://portnox.com)