SLASHNEXT

SLASHNEXT

CMS GUIDE

Version 1.1.0

SLASHNEXT

TABLE OF CONTENTS

TABLE OF CONTENTS

1 INTRODUCTION

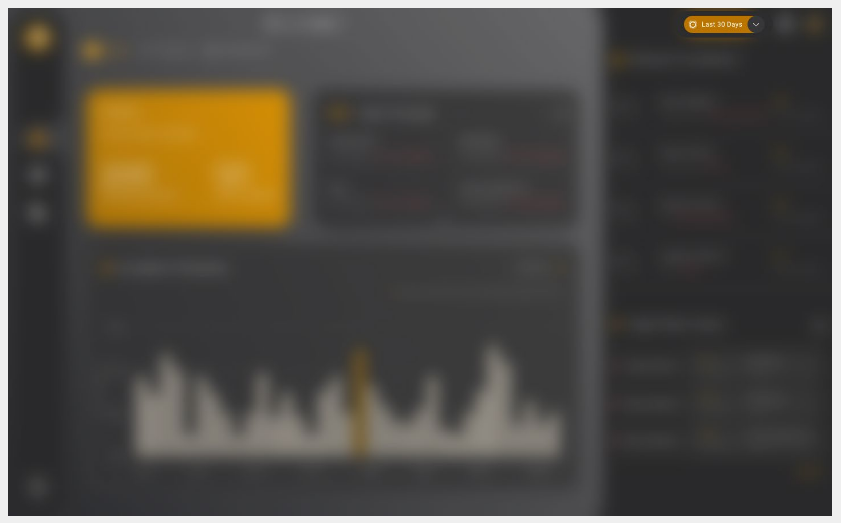
SlashNext CMS is a Web Console built for enterprise network team members (IT and security administrators) that allows them to provision, deploy and manage various mobile and browser versions of our Mobile and Browser Phishing Protection products.
CMS provides real-time information, displaying the latest deployments, activations, and licensing status of the product in real-time for the organization's entire user base.

2 CMS DASHBAORD

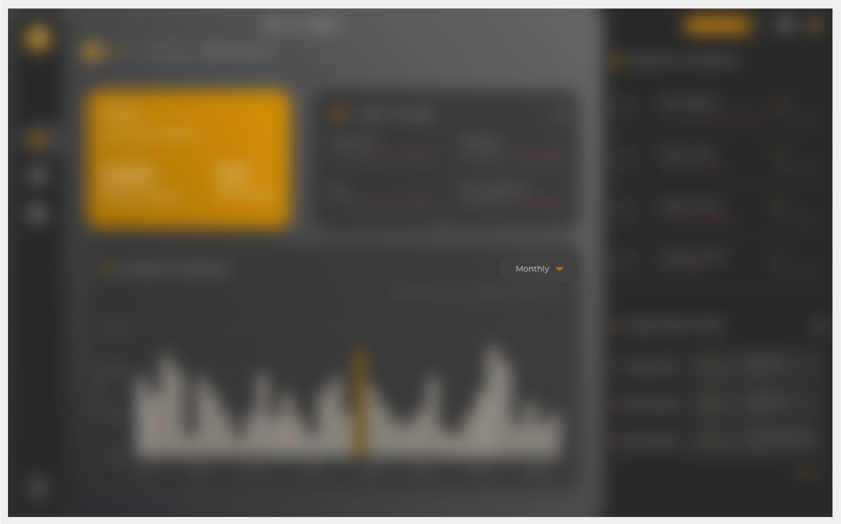
CMS Dashboard consists of three main tabs Users, Threats and Endpoints. You can switch between tabs to collect the information on the users in your organization such as the total number of phishing attacks with total number of users affected.

3 HOW TO GET STARTED WITH THE DASHBOARD?

You can optimize the dashboard according to your need by setting up the time filter values by Last 120 Days, Last 30 Days, Last 14 Days, Last 7 Days, Today and No Time Filter from the top right corner. The stats are displayed based on the time zone of the logged in user.



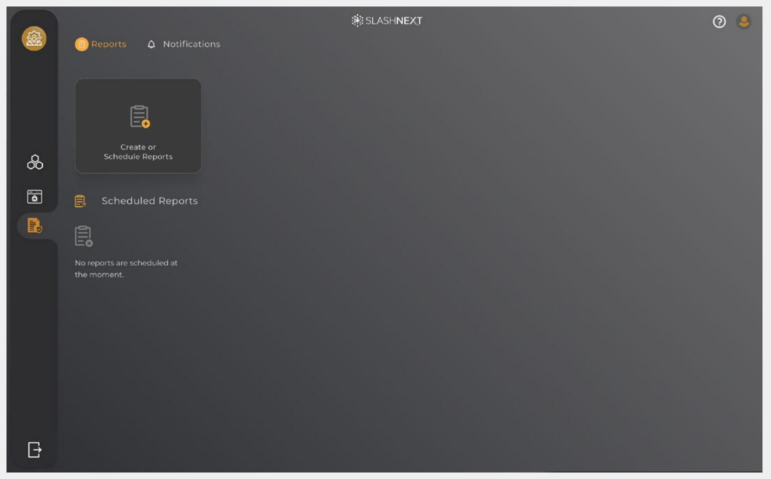
You can further drill down the values on the chart by applying the time filter on the charts. The filtered data may differ based on the global time filter selected.



4 HOW TO CREATE / SCHEDULE REPORTS?

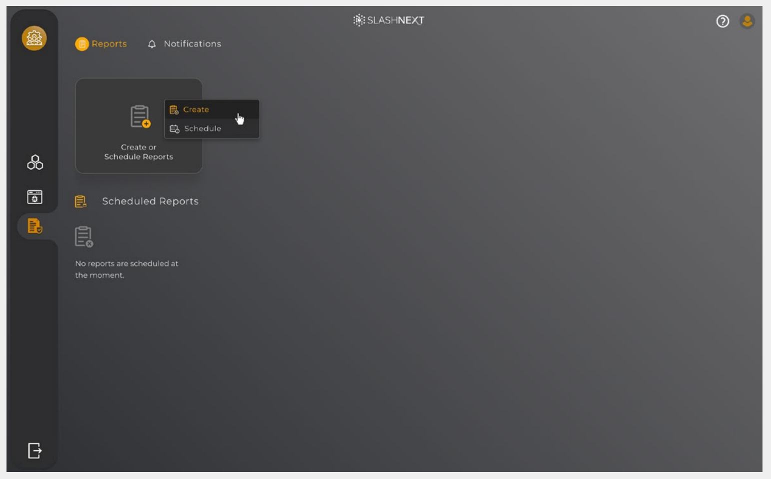
4.1 HOW TO CREATE A REPORT?

Go to Reporting and Notifications and in Reports tab click on to “Create or Schedule Reports”



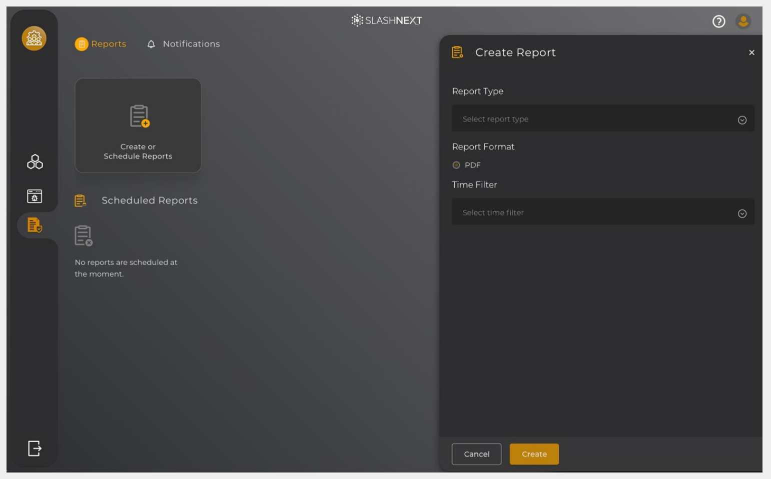
No reports are scheduled at the moment.

Select Create



No reports are scheduled at the moment.

Select Report type



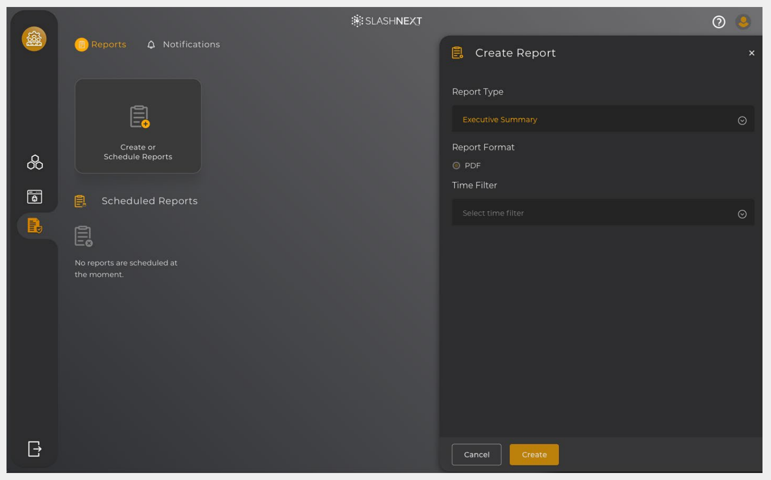
No reports are scheduled at the moment.

Report Type: Select report type

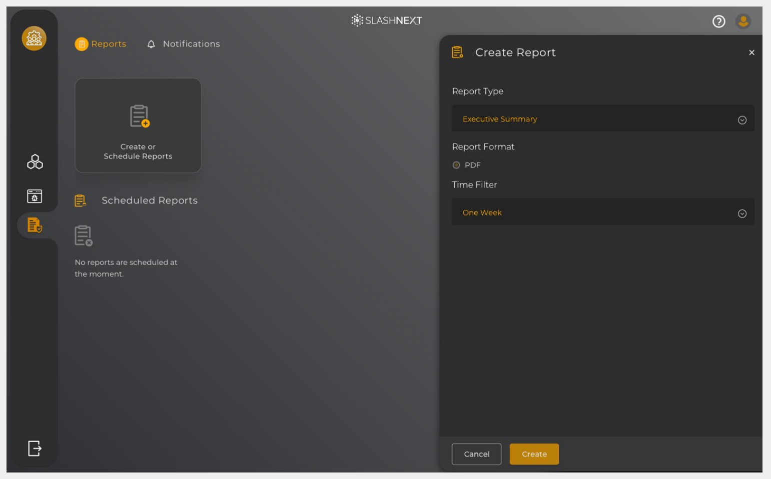
Report Format: ○ PDF

Time Filter: Select time filter

Select Time filter



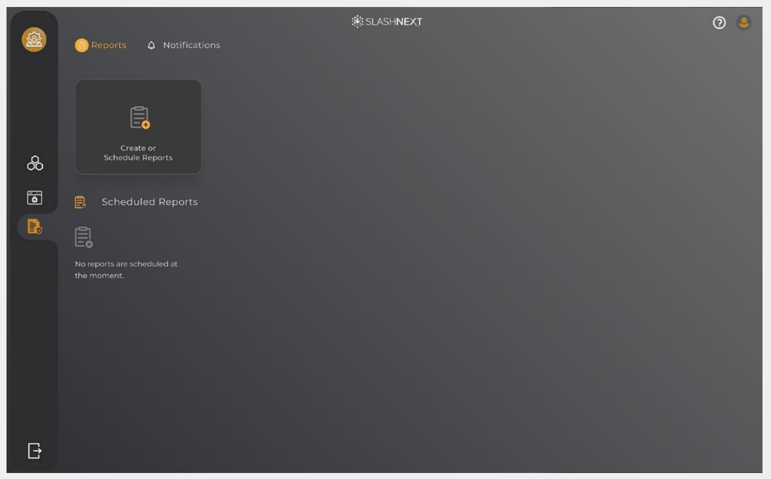
Click on Create, the report will be created and shown it to you



A new tab will open displaying the resultant report which you can download in PDF format

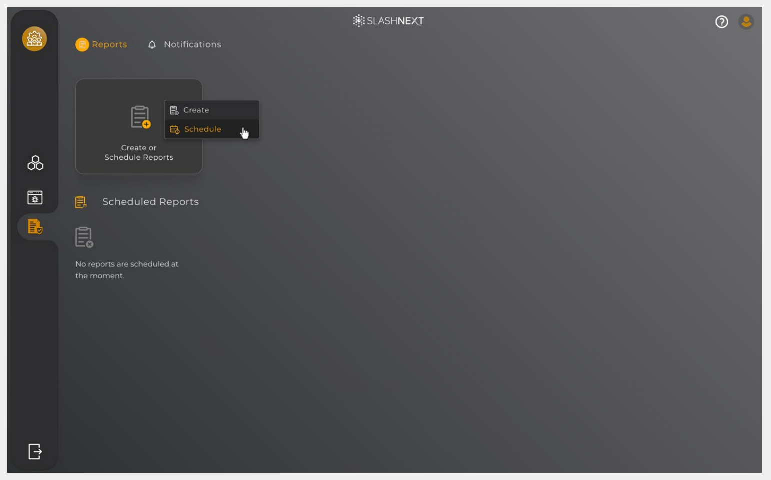
4.2 HOW TO SCHEDULE A REPORT?

Go to Reporting and click on to “Create or Schedule Reports”



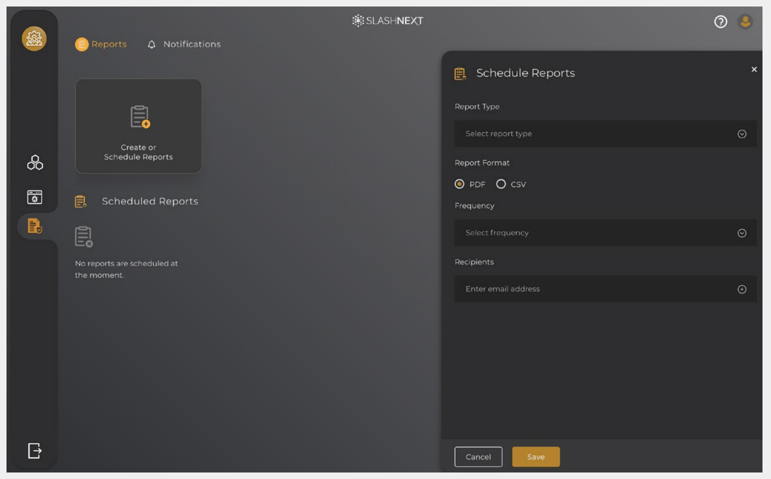
SLASHNEXT
Reports
Notifications
Create or Schedule Reports
Scheduled Reports
No reports are scheduled at the moment.

Select Schedule



No reports are scheduled at the moment.

Select Report type



No reports are scheduled at the moment.

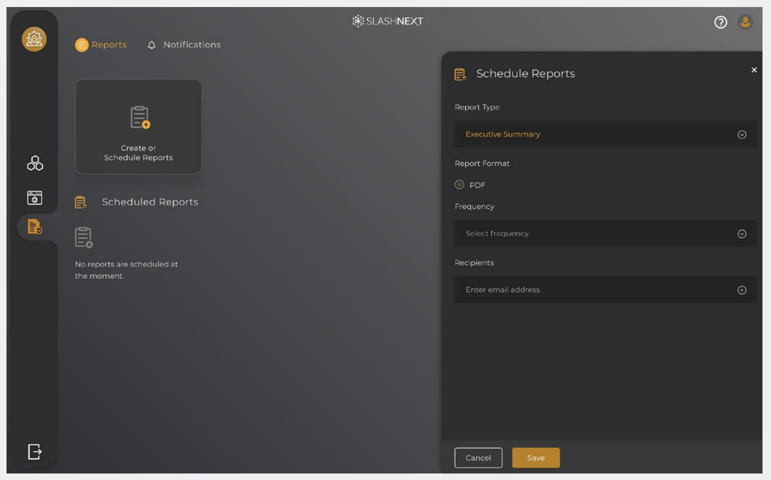
Report Type: Select report type

Report Format: ● PDF ○ CSV

Frequency: Select frequency

Recipients: Enter email address

Select Frequency



No reports are scheduled at the moment.

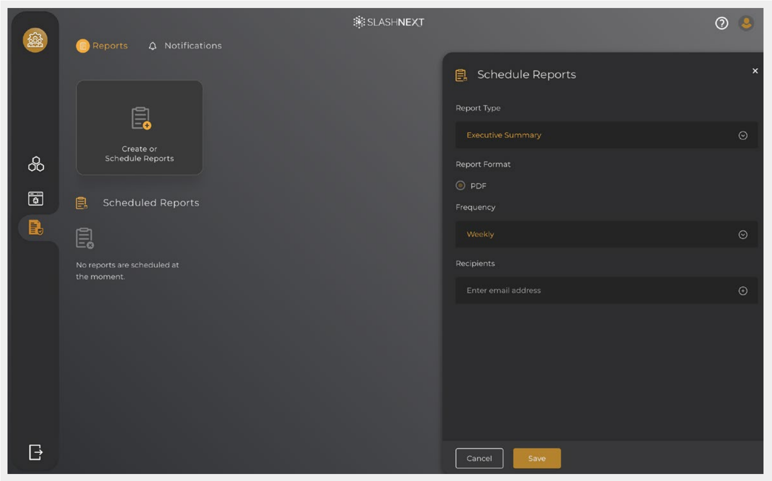
Report Type: Executive Summary

Report Format: ● PDF

Frequency: Select frequency

Recipients: Enter email address

Add Recipients



No reports are scheduled at the moment.

Schedule Reports

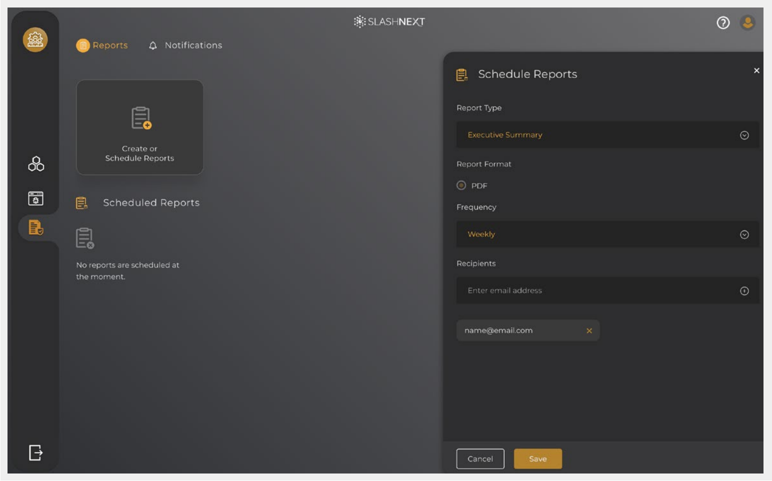
Report Type: Executive Summary

Report Format: ○ PDF

Frequency: Weekly

Recipients: Enter email address

Click on Save



No reports are scheduled at the moment.

Schedule Reports

Report Type: Executive Summary

Report Format: ○ PDF

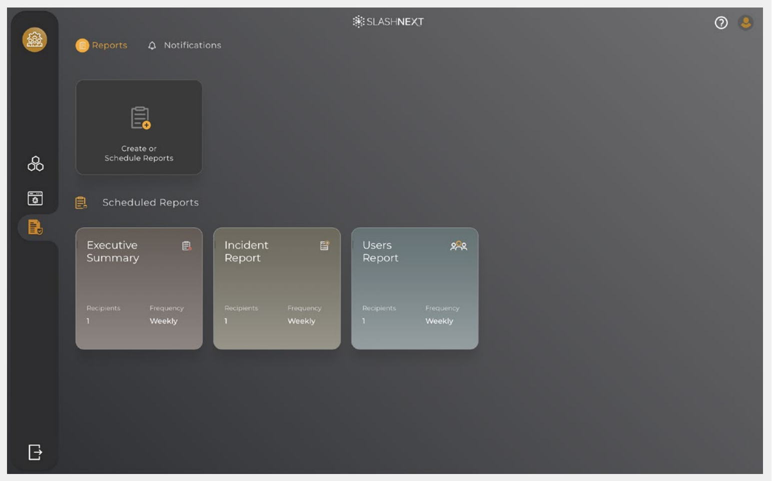
Frequency: Weekly

Recipients: Enter email address

name@email.com ×

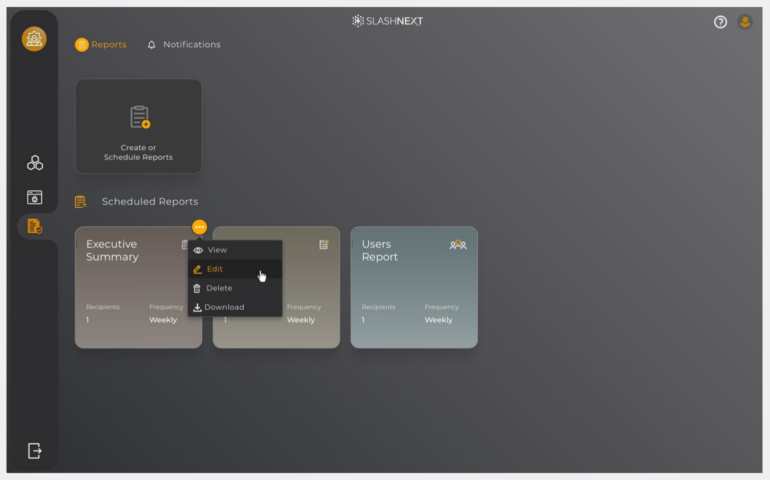
4.3 HOW TO EDIT A REPORT?

Go to Reporting and Notifications and in Reports tab click on ● icon over a scheduled report

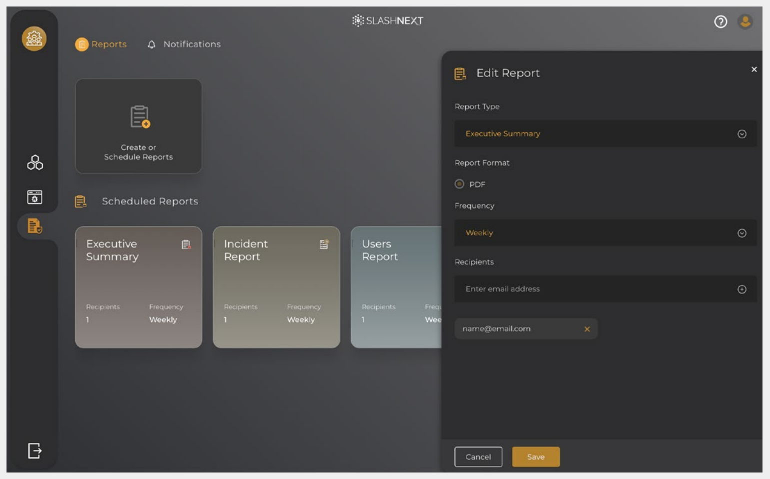


Report	Recipients	Frequency
Executive Summary	1	Weekly
Incident Report	1	Weekly
Users Report	1	Weekly

Click on Edit Report



You can edit Report type, Frequency or Recipients as well. After editing the report, you can click on save to save the edited report



Edit Report

Report Type: Executive Summary

Report Format: ○ PDF

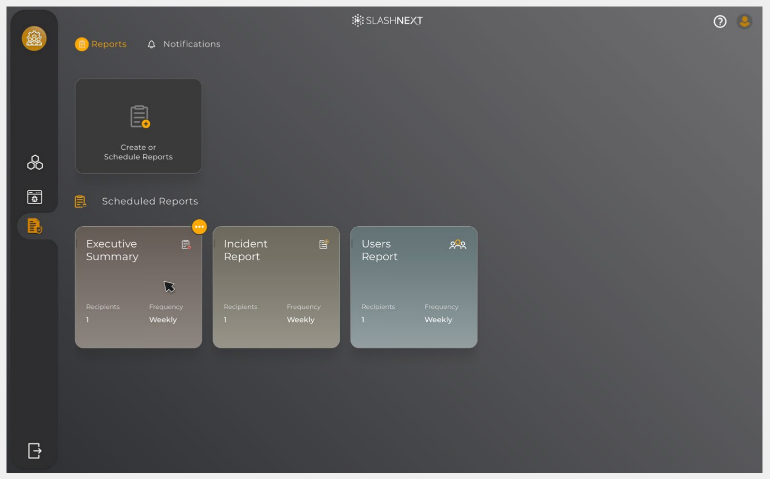
Frequency: Weekly

Recipients: Enter email address

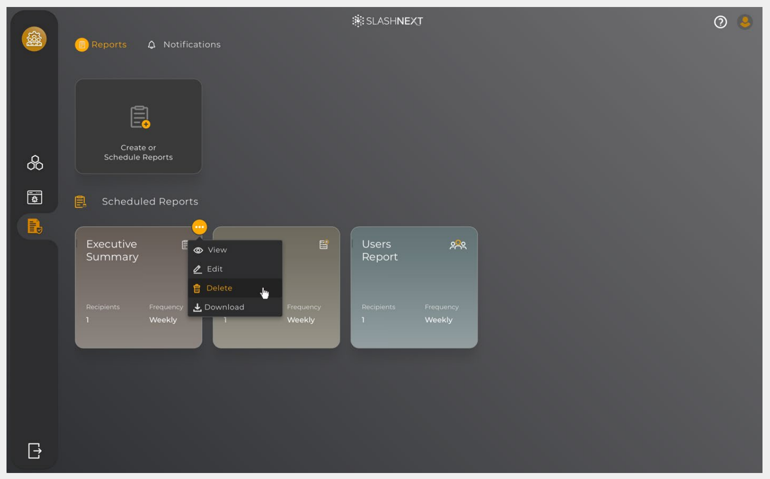
name@email.com ×

4.4 HOW TO DELETE A REPORT?

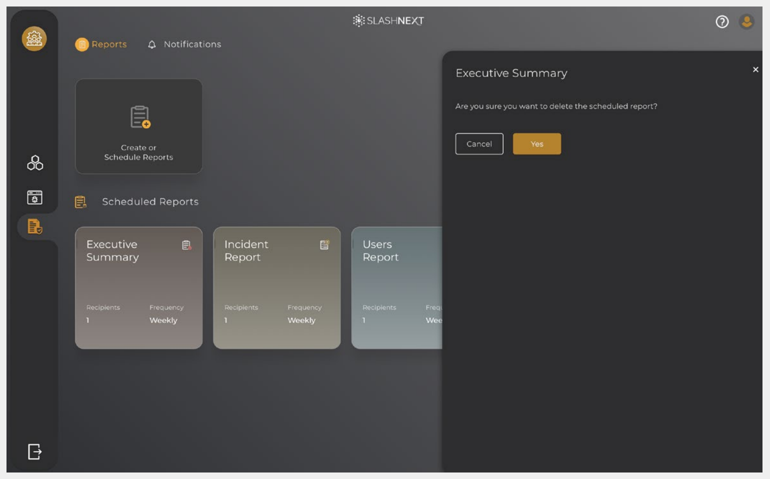
Go to Reporting and Notifications and in Reports tab click on ⋯ icon over a scheduled report



Click on Delete



Confirm the report to be deleted by clicking on to Yes.



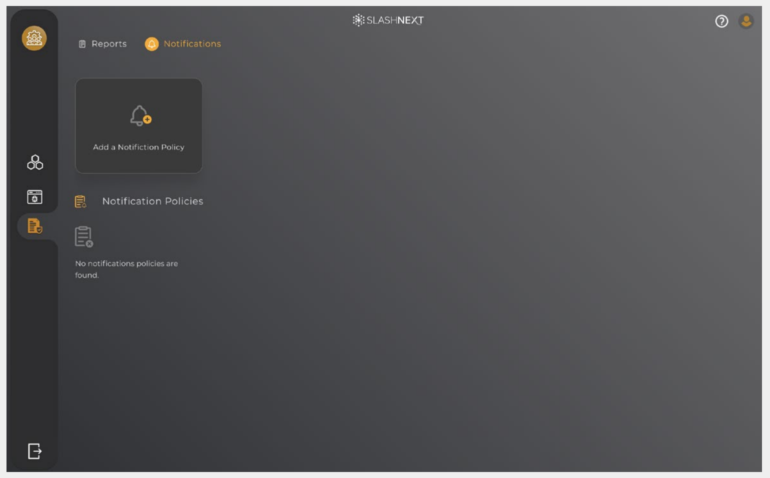
Executive Summary

Are you sure you want to delete the scheduled report?

5 HOW TO ADD, EDIT OR DELETE NOTIFICATION POLICY?

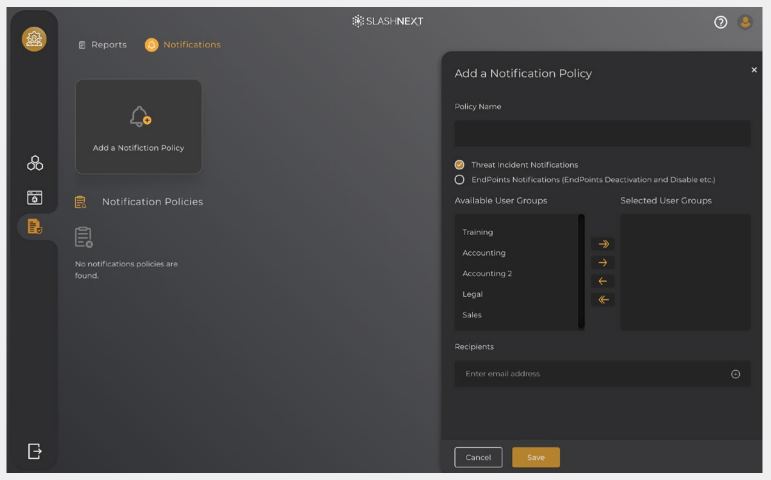
5.1 HOW TO ADD A NOTIFICATION POLICY?

Go to Reporting and Notifications and select Notifications tab click on to “Add a Notification Policy”

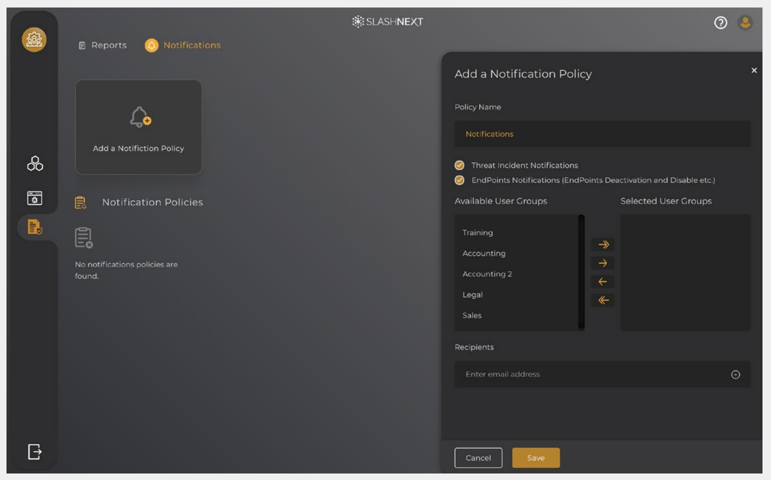


No notifications policies are found.

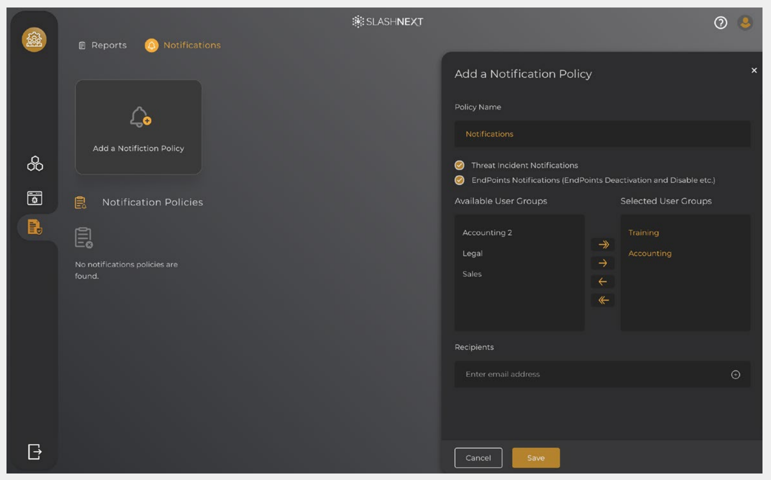
Add Policy Name



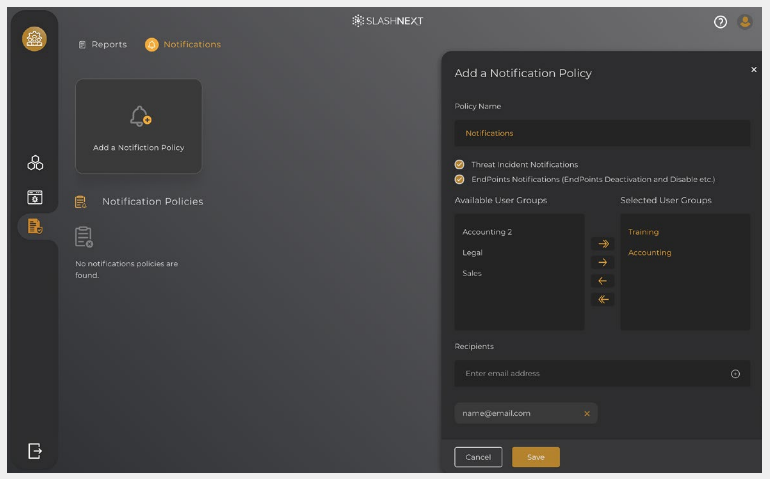
Select Threat Incident Notifications and Endpoints Notifications (Endpoints Deactivation and Disable etc.) you can select one of them or both



Add Groups to the Policy. In case if the group already exists in previously added Notification Policy it will not be available to be added into another Notification Policy



Add Recipients



Policy Name: Notifications

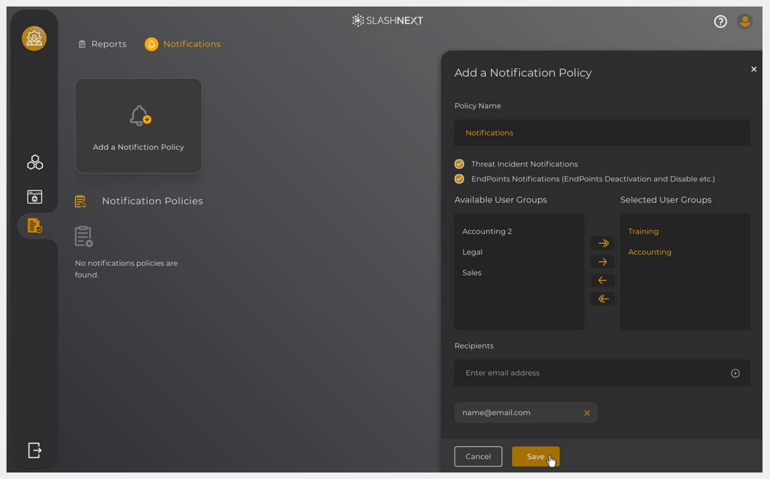
☑ Threat Incident Notifications
☑ EndPoints Notifications (EndPoints Deactivation and Disable etc.)

Available User Groups	Selected User Groups
Accounting 2	Training
Legal	Accounting
Sales	

Recipients: Enter email address

name@email.com ×

Click on Save



Policy Name: Notifications

☑ Threat Incident Notifications
☑ EndPoints Notifications (EndPoints Deactivation and Disable etc.)

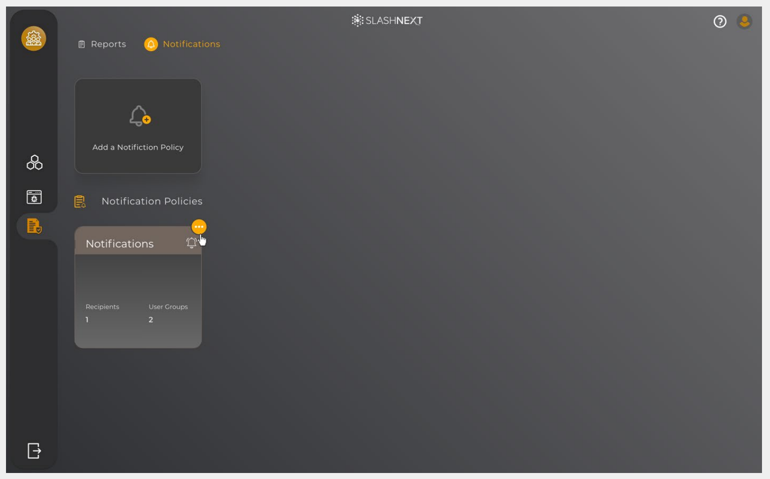
Available User Groups	Selected User Groups
Accounting 2	Training
Legal	Accounting
Sales	

Recipients: Enter email address

name@email.com ×

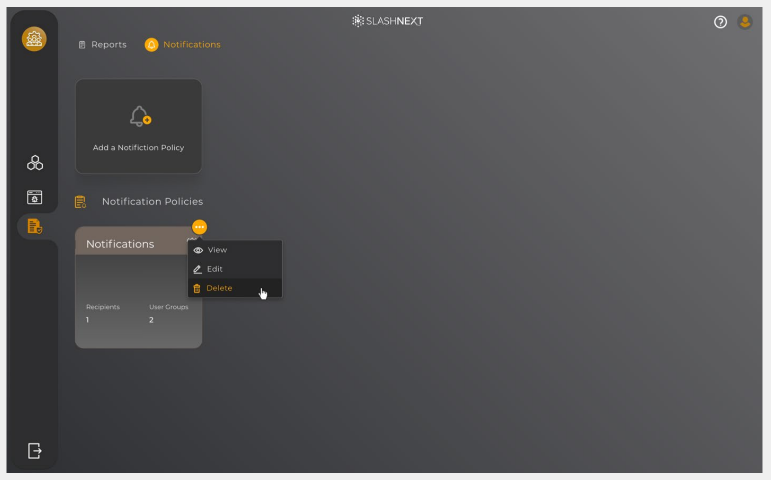
5.2 HOW TO DELETE A NOTIFICATION POLICY?

Go to Reporting and Notifications and in Notifications tab click on ⋯ icon over a Notifications Policy

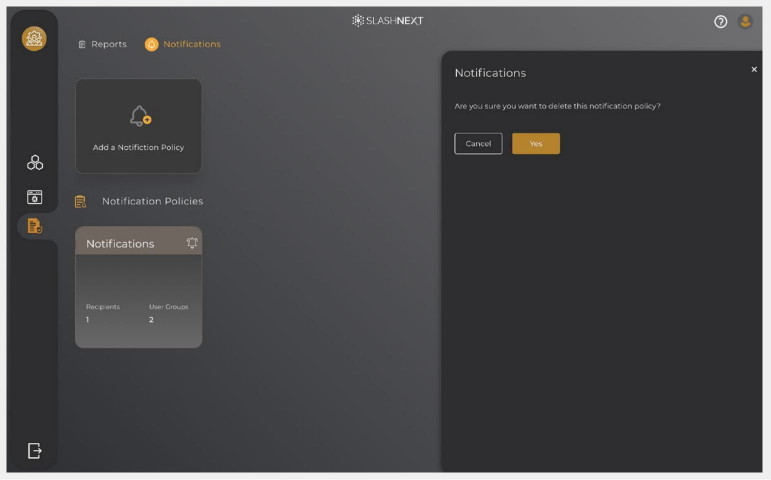


Recipients	User Groups
1	2

Click on Delete



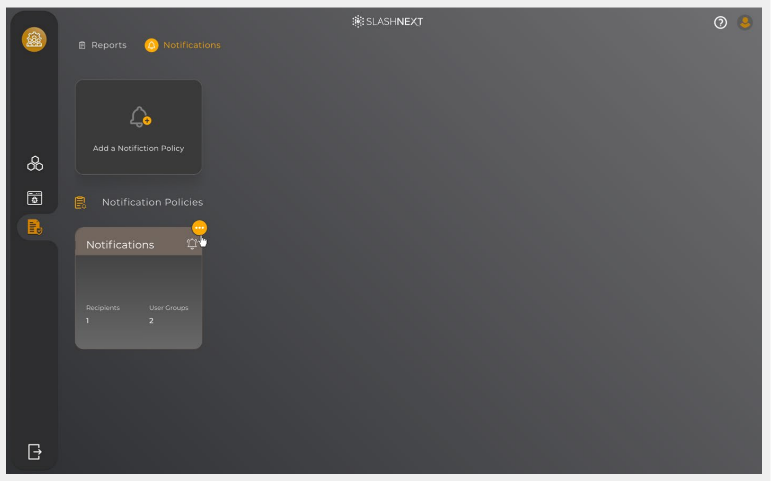
Confirm the report to be deleted by clicking on Yes



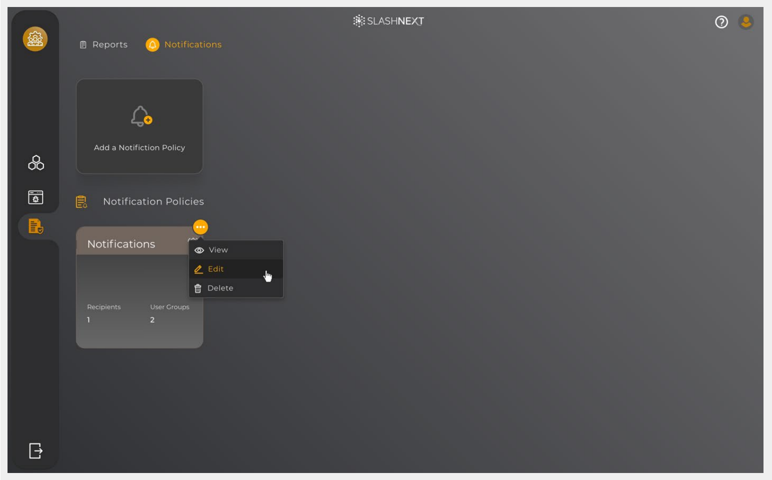
Are you sure you want to delete this notification policy?

5.3 HOW TO EDIT A NOTIFICATION POLICY?

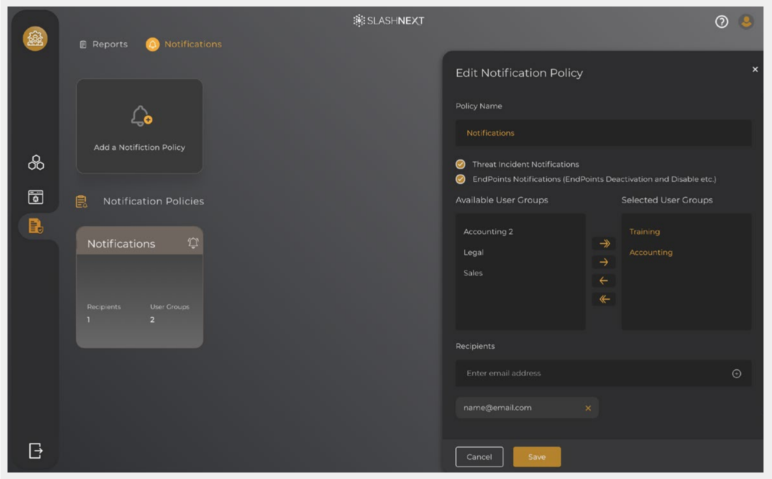
Go to Reporting and Notifications and in Notifications tab click on ⋯ icon over a Notifications Policy



Click on Edit



You can edit Policy options Threat Incident Notifications and Endpoints Notifications (Endpoint Deactivation and Disable etc.), Add or Remove from Selected User Groups. After editing the policy, you can click on save to save Policy



Edit Notification Policy

Policy Name: Notifications

☑ Threat Incident Notifications

☑ EndPoints Notifications (EndPoints Deactivation and Disable etc.)

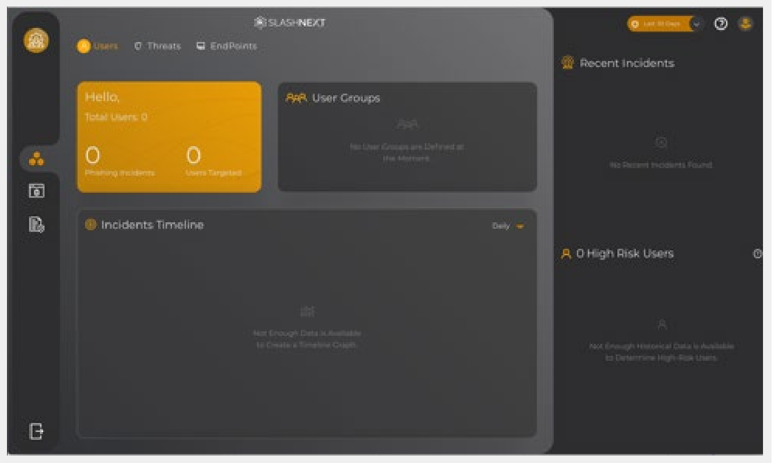
Available User Groups	Selected User Groups
Accounting 2	Training
Legal	Accounting
Sales	

Recipients: Enter email address

name@email.com

6 HOW TO GET STARTED WITH USER MANAGEMENT?

Sign-in to CMS



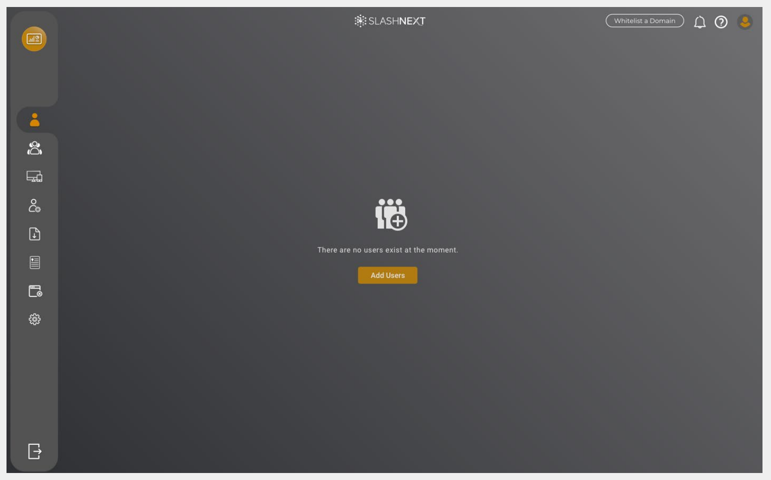
No User Groups are Defined at the Moment

Not Enough Data is Available to Create a Timeline Graph

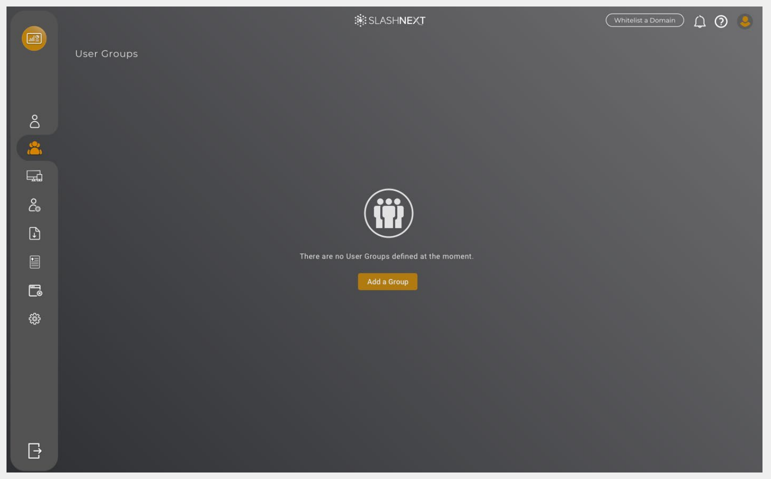
No Recent Incidents Found

Not Enough Historical Data is Available to Determine High-Risk Users

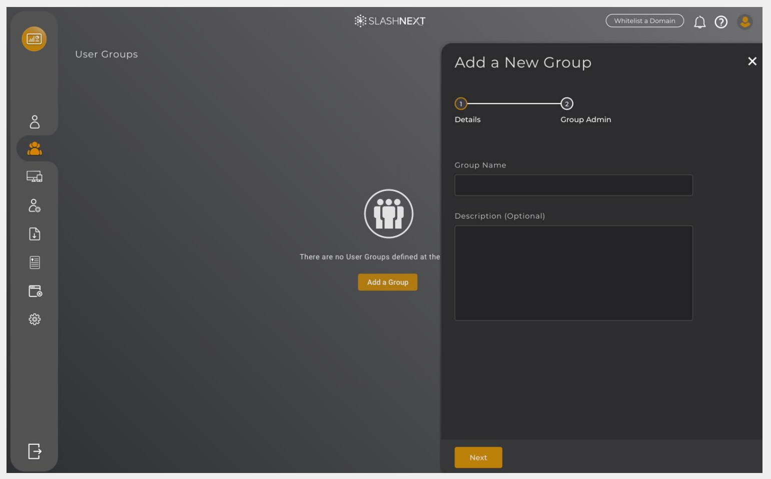
Go to Admin Area



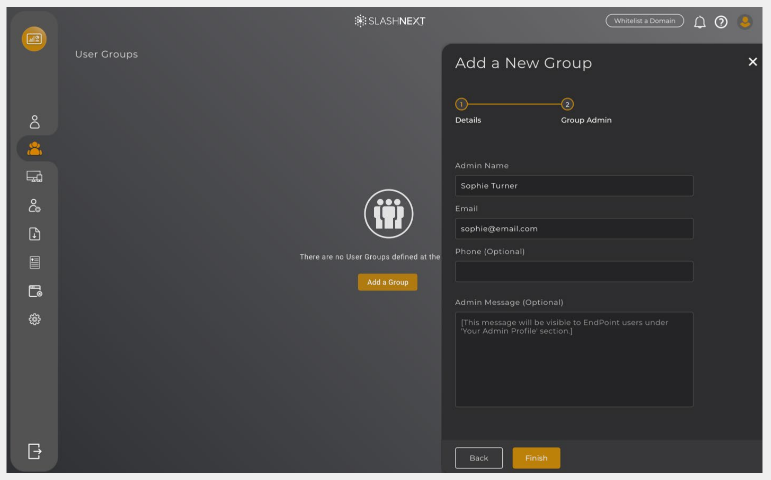
New user groups can be added by selecting "User Groups" on the left side panel



Click on Add a Group



For each new user group, add group admin details and click on Finish



Add a New Group

Admin Name: Sophie Turner

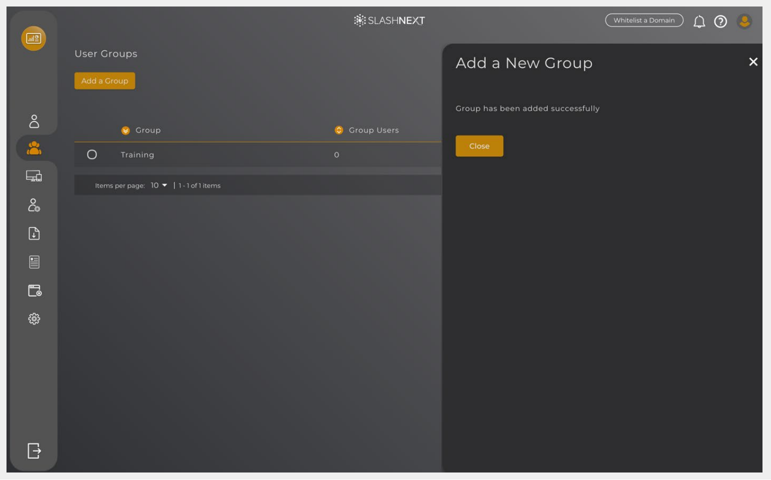
Email: sophie@email.com

Phone (Optional)

Admin Message (Optional): [This message will be visible to EndPoint users under 'Your Admin Profile' section.]

There are no User Groups defined at the

New User Group has been created, click on Close



Group	Group Users
Training	0

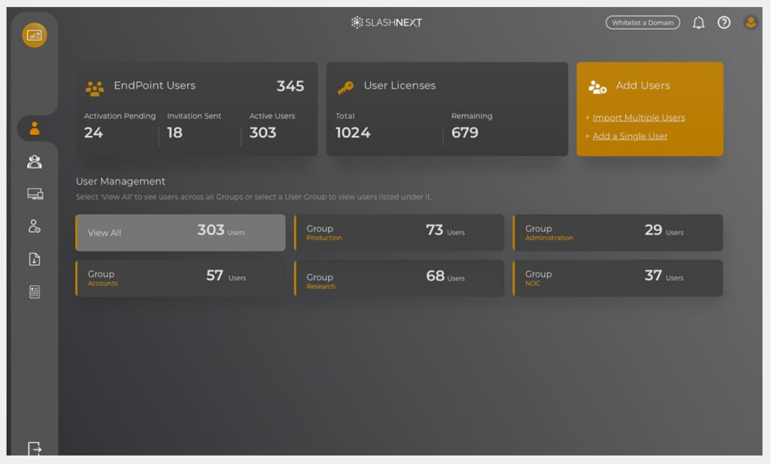
Items per page: 10 | 1 - 1 of 1 items

Add a New Group

Group has been added successfully

7 HOW TO ADD USERS?

To add users, go to "Admin Area" and then Users, you can directly import multiple users, or you can add a single user from the user's dashboard



EndPoint Users 345

Activation Pending	Invitation Sent	Active Users
24	18	303

User Licenses

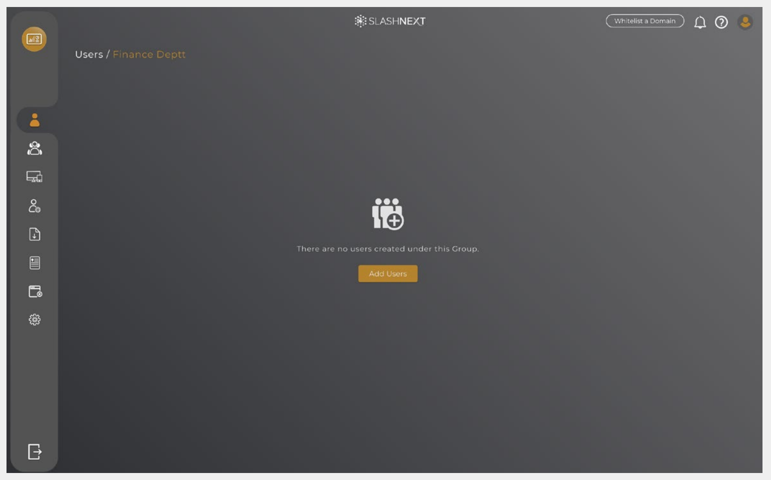
Total	Remaining
1024	679

User Management

Select 'View All' to see users across all Groups or select a User Group to view users listed under it.

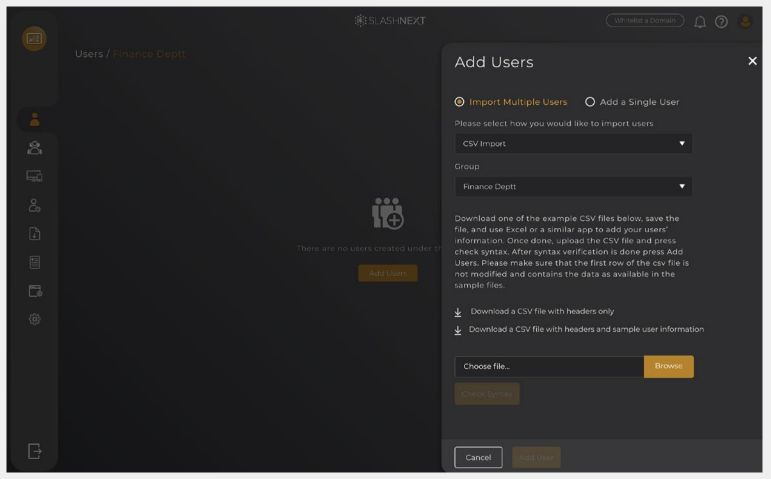
View All 303 Users	Group Production 73 Users	Group Administration 29 Users
Group Accounts 57 Users	Group Research 68 Users	Group NOC 37 Users

Or you can select a specific group where you would like to import/add users. Each user must be placed in an existing user group



There are no users created under this Group.

Multiple users can be added at one time through "Import Multiple Users" by picking a user group and uploading a CSV file with all users' information or you can use platforms like Okta, OneLogin and Azure Active Directory to import users and groups.



Add Users

● Import Multiple Users ○ Add a Single User

Please select how you would like to import users: CSV Import

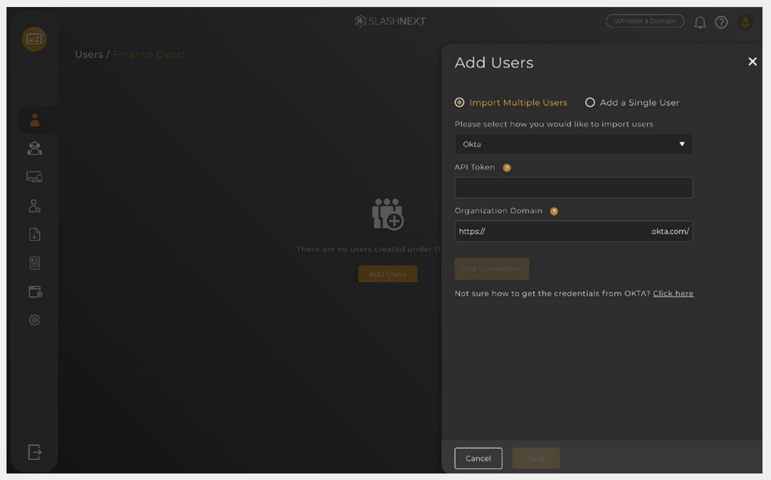
Group: Finance Deptt

Download one of the example CSV files below, save the file, and use Excel or a similar app to add your users' information. Once done, upload the CSV file and press check syntax. After syntax verification is done press Add Users. Please make sure that the first row of the csv file is not modified and contains the data as available in the sample files.

Download a CSV file with headers only

Download a CSV file with headers and sample user information

Choose file...



Add Users

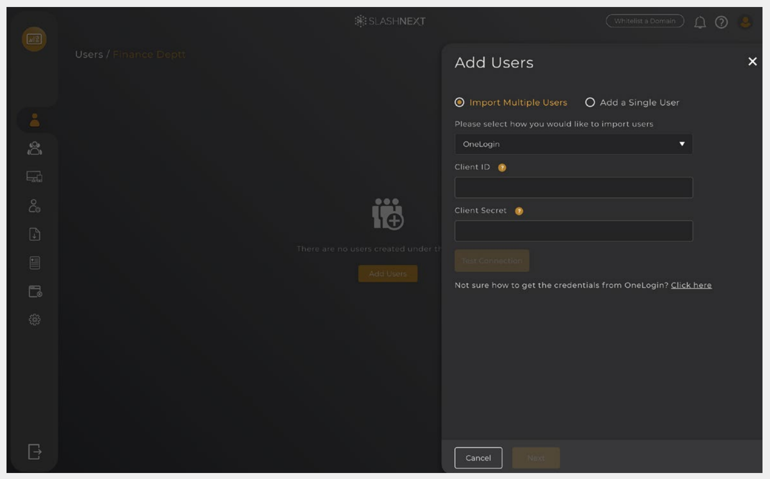
● Import Multiple Users ○ Add a Single User

Please select how you would like to import users: Okta

API Token

Organization Domain: https:// .okta.com/

Not sure how to get the credentials from OKTA? Click here



Add Users

◉ Import Multiple Users ○ Add a Single User

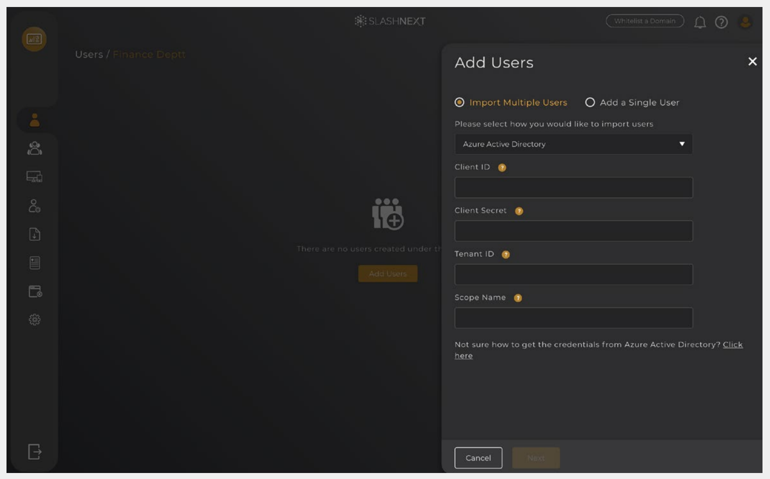
Please select how you would like to import users

OneLogin ▾

Client ID

Client Secret

Not sure how to get the credentials from OneLogin? Click here



Add Users

◉ Import Multiple Users ○ Add a Single User

Please select how you would like to import users

Azure Active Directory ▾

Client ID

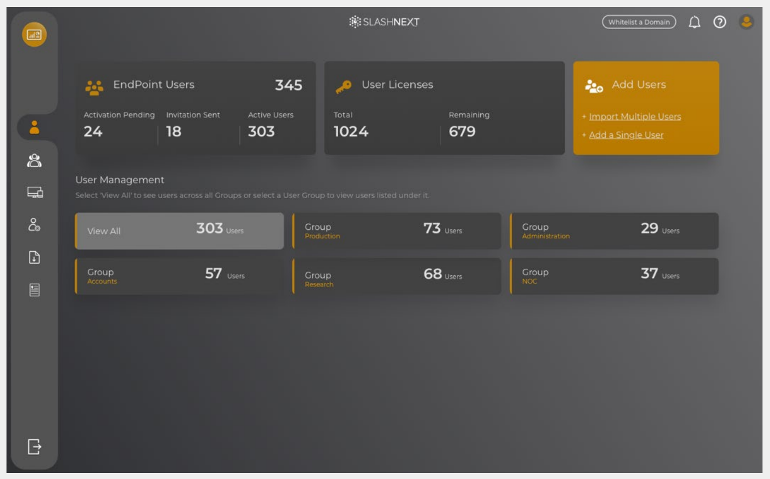
Client Secret

Tenant ID

Scope Name

Not sure how to get the credentials from Azure Active Directory? Click here

Main page of the Admin Area displays a summary of all endpoint deployments and the status of user licenses. From here specific User Groups can be viewed as well by going to "User Management" and selecting the group to view



EndPoint Users 345

Activation Pending	Invitation Sent	Active Users
24	18	303

User Licenses

Total	Remaining
1024	679

User Management

Select 'View All' to see users across all Groups or select a User Group to view users listed under it.

View All 303 Users	Group Production 73 Users	Group Administration 29 Users
Group Accounts 57 Users	Group Research 68 Users	Group NOC 37 Users

If you need further information or have any questions, please contact support@slashnext.com

8 CMS ACCOUNT

Any organization that purchases SlashNext Mobile and Browser Phishing protection products will have access to the Web Console and a dedicated CMS account. These can be used by IT and security administrators to manage endpoint products throughout their user base.

Details of this account can be viewed under the "Account" section available on the left side bar. It shows the basic contact information as well subscription details for the account including license status, number of users, and number of devices per user allowed under the license.

9 USERS

CMS supports three types of User

1. CMS administrators
2. Group administrators
3. Endpoint users

9.1 WHAT IS A CMS ADMINISTRATOR?

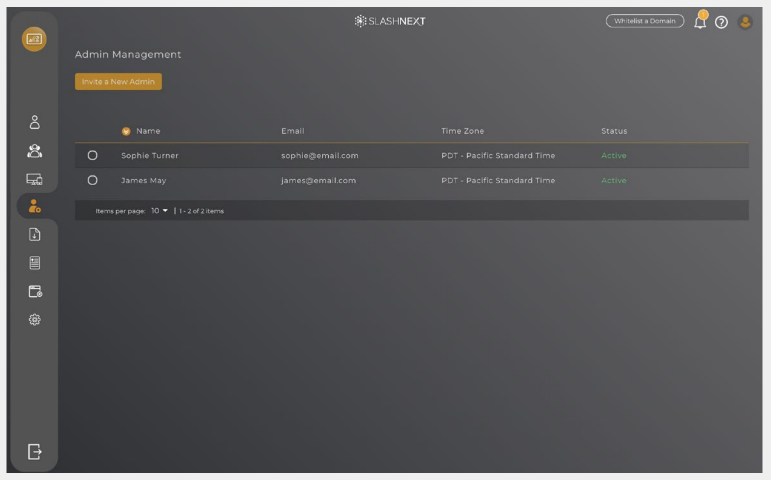
CMS administrators are responsible for managing the overall system. They can create user groups, group policies, provision endpoint users, view deployment statistics, and much more.

CMS administrators are also responsible for ongoing maintenance. For example, modifying and deletion of endpoint user profiles, deactivations, change in group policies, etc.

SlashNext will create a default administrative account at the time of account provisioning. The default administrator can further create multiple other administrative accounts by going to "Invite a New Admin" under "Admin Management" on the left pane.

9.1.1 HOW TO INVITE A NEW ADMIN?

Go to Admin Area and click on to Admin Accounts

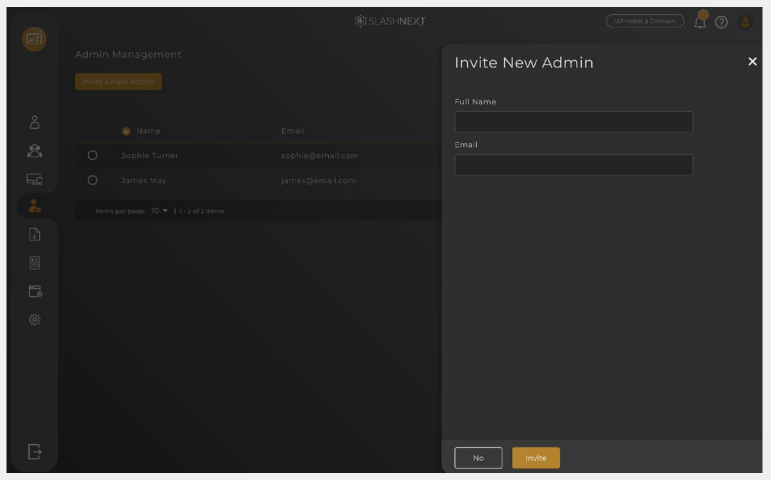


Admin Management

	Name	Email	Time Zone	Status
○	Sophie Turner	sophie@email.com	PDT - Pacific Standard Time	Active
○	James May	james@email.com	PDT - Pacific Standard Time	Active

Items per page: 10 | 1 - 2 of 2 items

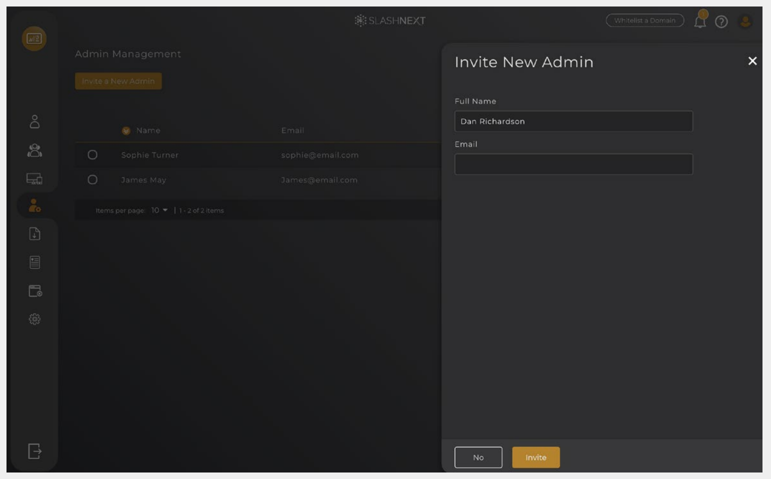
Click on Invite a New Admin



Name	Email
Sophie Turner	sophie@email.com
James May	james@email.com

Items per page: 10 | 1 - 2 of 2 items

Add Full Name



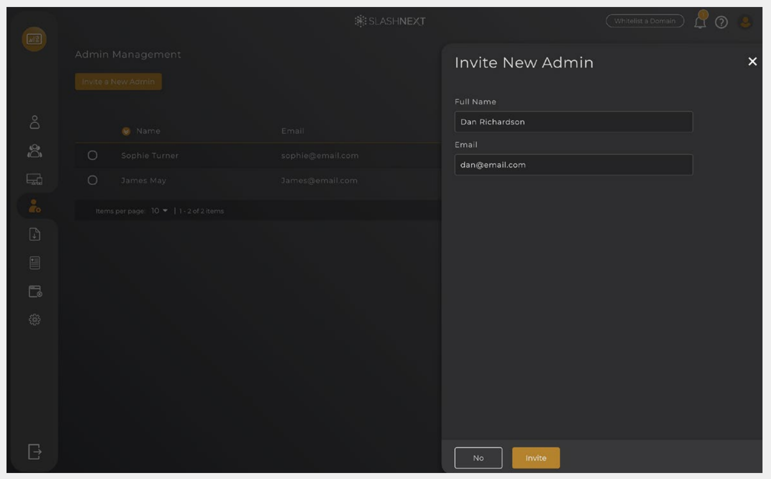
Name	Email
Sophie Turner	sophie@email.com
James May	James@email.com

Items per page: 10 | 1 - 2 of 2 items

Full Name: Dan Richardson

Email:

Add Email Address



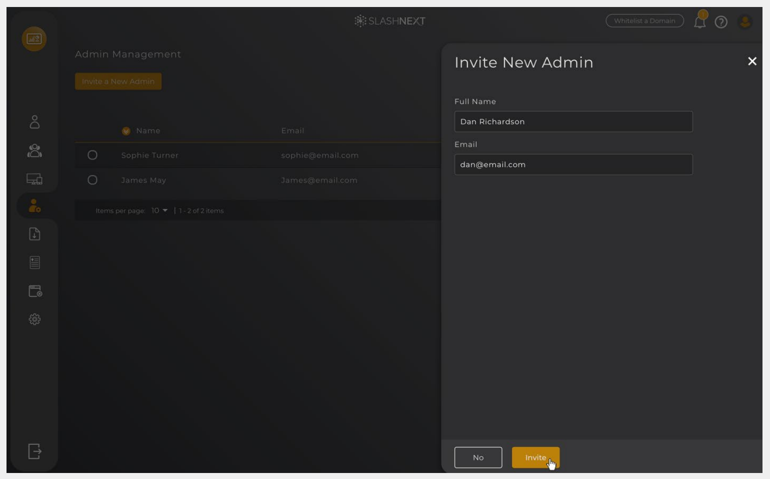
Name	Email
Sophie Turner	sophie@email.com
James May	James@email.com

Items per page: 10 | 1 - 2 of 2 items

Full Name: Dan Richardson

Email: dan@email.com

Click on Invite

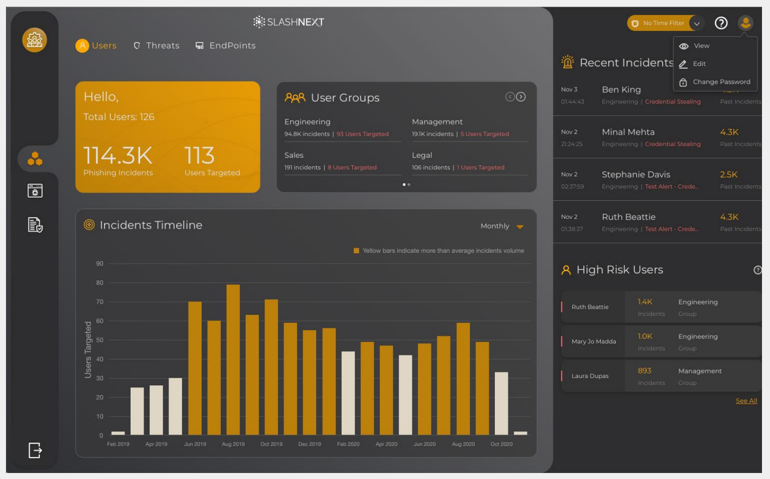


Full Name: Dan Richardson

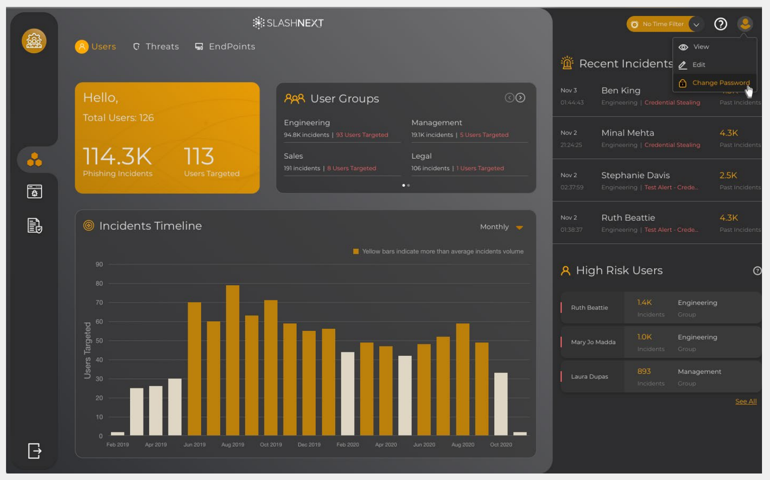
Email: dan@email.com

9.1.2 HOW TO CHANGE ADMIN PASSWORD?

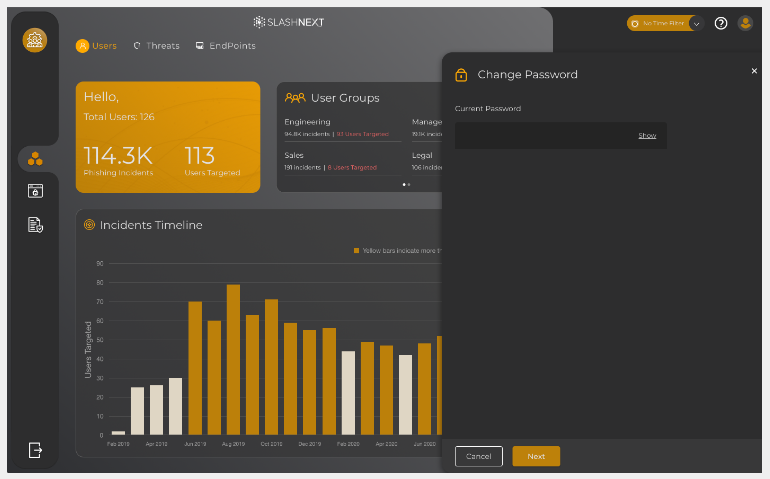
Click on Profile icon


SLASHNEXT
Users
Threats
EndPoints
No Time Filter
View
Edit
Change Password
Hello,
Total Users: 126
114.3K
Phishing Incidents
113
Users Targeted
User Groups
Engineering
94.8K incidents | 93 Users Targeted
Management
19.1K incidents | 5 Users Targeted
Sales
191 incidents | 8 Users Targeted
Legal
106 incidents | 1 Users Targeted
Recent Incidents
Nov 3 01:44:43 Ben King Engineering | Credential Stealing Past Incidents
Nov 2 21:24:25 Minal Mehta Engineering | Credential Stealing 4.3K Past Incidents
Nov 2 02:37:59 Stephanie Davis Engineering | Test Alert - Crede... 2.5K Past Incidents
Nov 2 01:38:37 Ruth Beattie Engineering | Test Alert - Crede... 4.3K Past Incidents
Incidents Timeline
Monthly
Yellow bars indicate more than average incidents volume
Users Targeted
90
80
70
60
50
40
30
20
10
0
Feb 2019
Apr 2019
Jun 2019
Aug 2019
Oct 2019
Dec 2019
Feb 2020
Apr 2020
Jun 2020
Aug 2020
Oct 2020
High Risk Users
Ruth Beattie 1.4K Incidents Engineering Group
Mary Jo Madda 1.0K Incidents Engineering Group
Laura Dupas 893 Incidents Management Group
See All

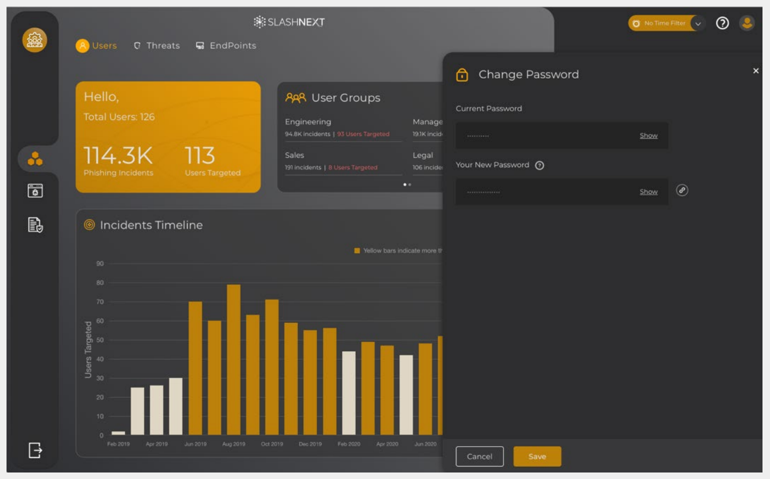
Click on Change Password


SLASHNEXT
Users
Threats
EndPoints
No Time Filter
View
Edit
Change Password
Hello,
Total Users: 126
114.3K
Phishing Incidents
113
Users Targeted
User Groups
Engineering
94.8K incidents | 93 Users Targeted
Management
19.1K incidents | 5 Users Targeted
Sales
191 incidents | 8 Users Targeted
Legal
106 incidents | 1 Users Targeted
Recent Incidents
Nov 3 01:44:43 Ben King Engineering | Credential Stealing Past Incidents
Nov 2 21:24:25 Minal Mehta Engineering | Credential Stealing 4.3K Past Incidents
Nov 2 02:37:59 Stephanie Davis Engineering | Test Alert - Crede... 2.5K Past Incidents
Nov 2 01:38:37 Ruth Beattie Engineering | Test Alert - Crede... 4.3K Past Incidents
Incidents Timeline
Monthly
Yellow bars indicate more than average incidents volume
Users Targeted
90
80
70
60
50
40
30
20
10
0
Feb 2019
Apr 2019
Jun 2019
Aug 2019
Oct 2019
Dec 2019
Feb 2020
Apr 2020
Jun 2020
Aug 2020
Oct 2020
High Risk Users
Ruth Beattie 1.4K Incidents Engineering Group
Mary Jo Madda 1.0K Incidents Engineering Group
Laura Dupas 893 Incidents Management Group
See All

Type in Current Password and click Next

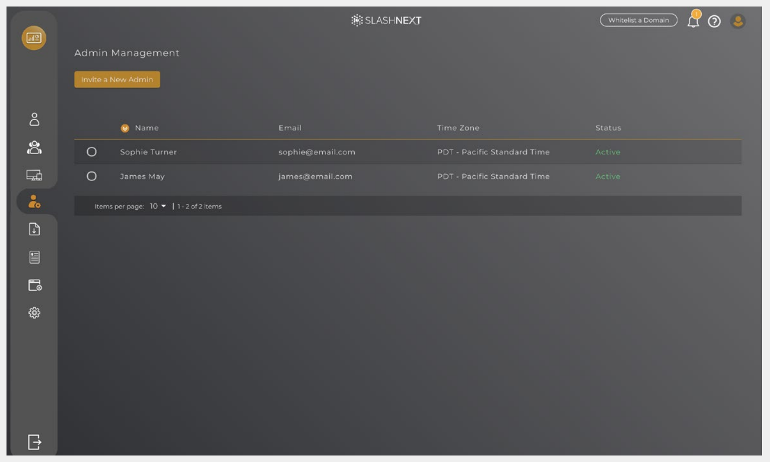


New Password is generated, you can copy the new password and click on Save to save the new password



9.1.3 HOW TO SUSPEND AN ADMIN?

Go to Admin Area and click on to Admin Accounts

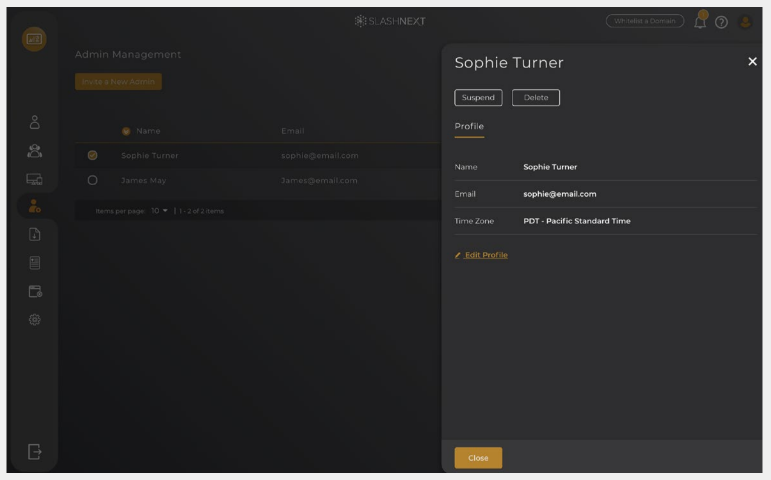


Admin Management

	Name	Email	Time Zone	Status
○	Sophie Turner	sophie@email.com	PDT - Pacific Standard Time	Active
○	James May	james@email.com	PDT - Pacific Standard Time	Active

Items per page: 10 | 1 - 2 of 2 items

Select the Admin you would like to suspend and click the Suspend button



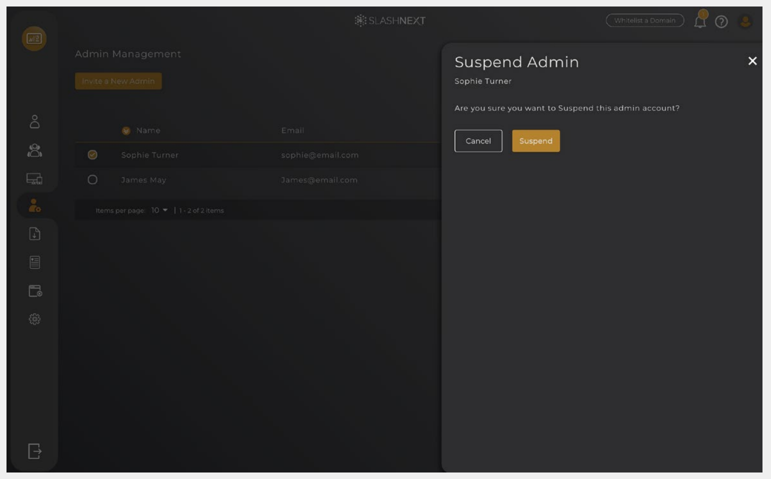
Name	Email
Sophie Turner	sophie@email.com
James May	James@email.com

Items per page: 10 | 1 - 2 of 2 items

Sophie Turner

Name	Sophie Turner
Email	sophie@email.com
Time Zone	PDT - Pacific Standard Time

Confirm the Admin to be suspended by Clicking on Suspend



Name	Email
Sophie Turner	sophie@email.com
James May	James@email.com

Items per page: 10 | 1 - 2 of 2 items

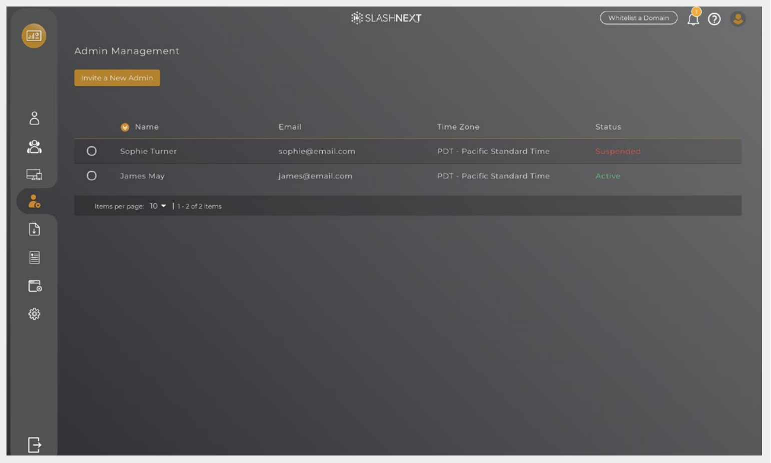
Suspend Admin

Sophie Turner

Are you sure you want to Suspend this admin account?

9.1.4 HOW TO REACTIVATE AN ADMIN?

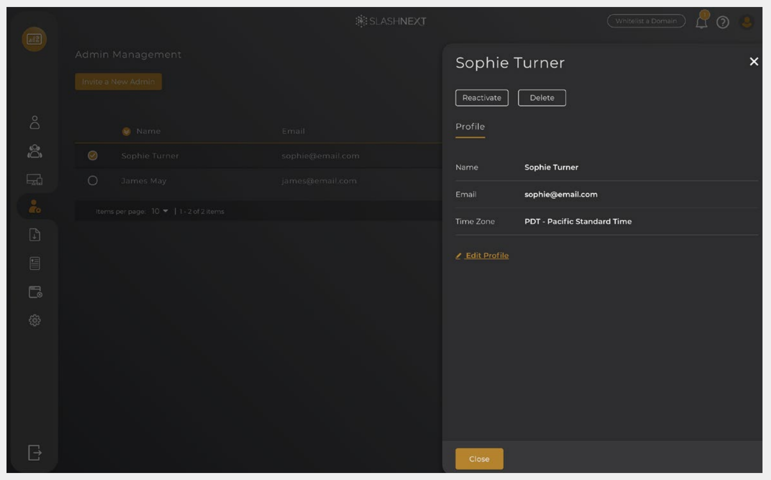
Go to Admin Area and click on to Admin Accounts



Name	Email	Time Zone	Status
Sophie Turner	sophie@email.com	PDT - Pacific Standard Time	Suspended
James May	james@email.com	PDT - Pacific Standard Time	Active

Items per page: 10 | 1 - 2 of 2 items

Select the Admin you would like to suspend and click the Reactivate button



Admin Management

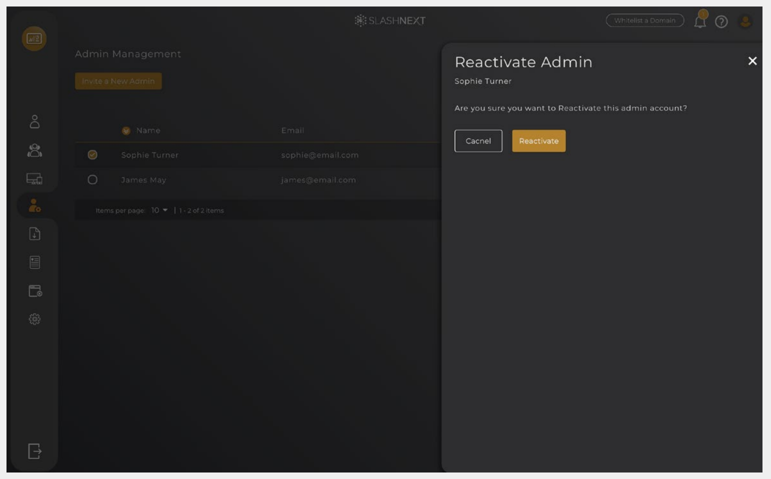
	Name	Email
●	Sophie Turner	sophie@email.com
○	James May	james@email.com

Items per page: 10 | 1 - 2 of 2 items

Sophie Turner

Name	Sophie Turner
Email	sophie@email.com
Time Zone	PDT - Pacific Standard Time

Confirm the Admin to be reactivated by Clicking on Reactivate



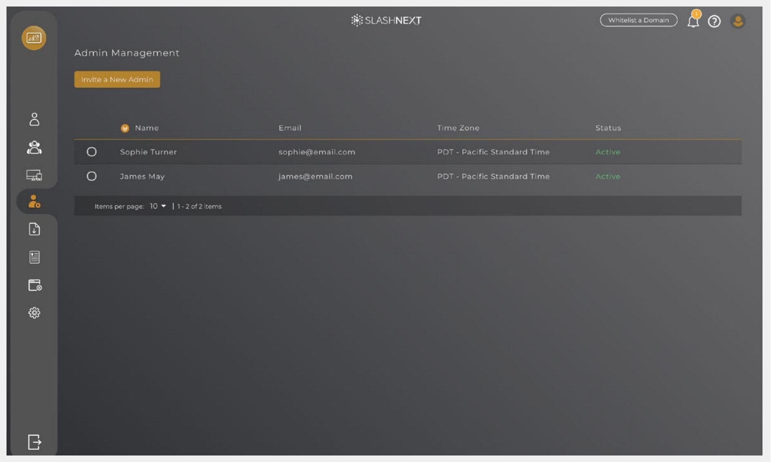
Reactivate Admin

Sophie Turner

Are you sure you want to Reactivate this admin account?

9.1.5 HOW TO EDIT AN ADMIN?

Go to Admin Area and click on to Admin Accounts

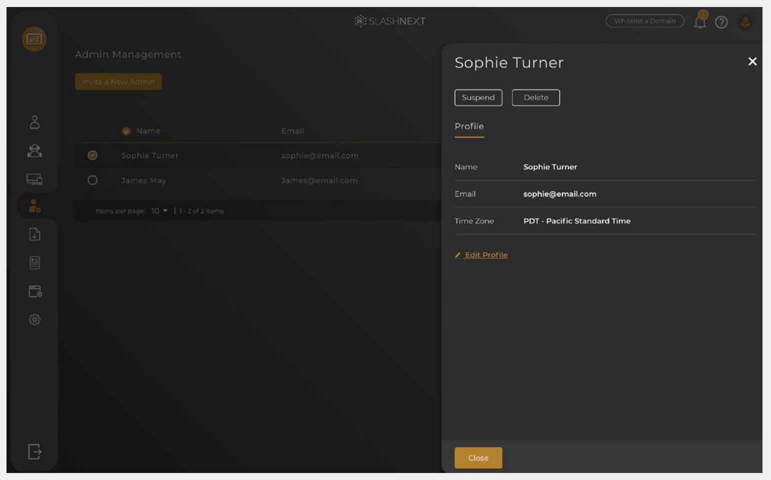


Admin Management

	Name	Email	Time Zone	Status
○	Sophie Turner	sophie@email.com	PDT - Pacific Standard Time	Active
○	James May	james@email.com	PDT - Pacific Standard Time	Active

Items per page: 10 | 1 - 2 of 2 items

Select the Admin you would like to Edit and click on Edit Profile



Admin Management

Name	Email
Sophie Turner	sophie@email.com
James May	James@email.com

Items per page: 10 | 1 - 2 of 2 items

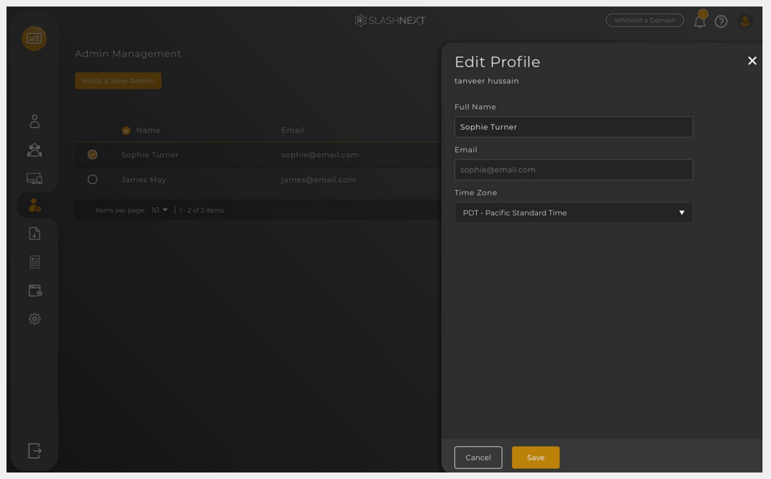
Sophie Turner

Name Sophie Turner

Email sophie@email.com

Time Zone PDT - Pacific Standard Time

You can Edit Full Name and Time Zone of an Admin. After editing click on Save to save the Admin profile



Admin Management

Name	Email
Sophie Turner	sophie@email.com
James May	james@email.com

Items per page: 10 | 1 - 2 of 2 items

Edit Profile

tanveer hussain

Full Name: Sophie Turner

Email: sophie@email.com

Time Zone: PDT - Pacific Standard Time

9.2 WHAT ARE GROUP ADMINISTRATORS?

Every endpoint user must have one administrator assigned to it called a group admin. This person is the recipient of endpoints disable and deactivate notifications. The group admin is also a support contact for all endpoint users under their group. Endpoint users can view their administrative profile from the endpoint About Section.

9.3 WHAT IS AN ENDPOINT USER?

Endpoint user is the person who has the SlashNext Remote Mobile or Browser Phishing endpoint product installed on their device(s). All users would have their profile created by the CMS administrator. Each endpoint user will get assigned a unique endpoint activation key. In case a user is installing EndPoints from an online store (App Store. Google Play etc.), the key can be used to activate multiple endpoints up to the designated allocation. In case of MDM/EMM based distribution, user may activate Endpoints using his/her email or via Single Sign-On services.

10 GROUPS

10.1 WHAT IS A GROUP?

The concept behind a group is almost the same as a branch office. Groups are categories that allow CMS administrators to form groups of users (based on geography, department, roles, etc.). CMS administrators can create as many groups as they like and divide the endpoint users across such groups for easy management.

Each group is assigned a dedicated group admin. A group admin is the recipient of endpoints disable and deactivate notifications. The group admin is also a support contact for all endpoint users in their group.

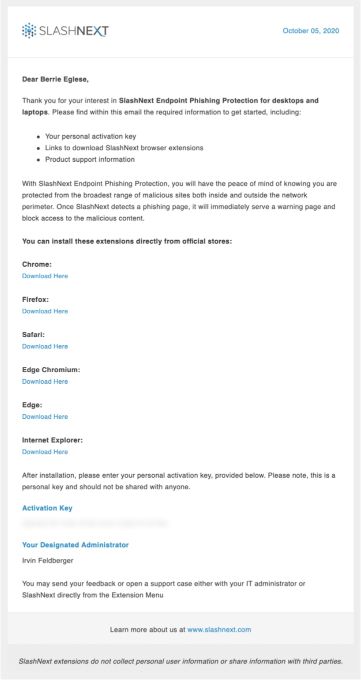
CMS administrator can also create group policies and assign it to a particular user group. Once a policy is assigned to a group, all user that exists under that group will be governed by that policy.

One endpoint user cannot belong to two groups at the same time. However, every user must belong to at least one user group.

11 ENDPOINT INVITES

Once users are added and assigned to groups, Admin can send them invites to download and install browser extensions and mobile based anti-phishing solutions – either individually or in bulk.

Users are sent an email with all the information on how to download, install and activate endpoints.



October 05, 2020

Dear Berrie Eglese,

Thank you for your interest in **SlashNext Endpoint Phishing Protection for desktops and laptops**. Please find within this email the required information to get started, including:

- Your personal activation key
- Links to download SlashNext browser extensions
- Product support information

With SlashNext Endpoint Phishing Protection, you will have the peace of mind of knowing you are protected from the broadest range of malicious sites both inside and outside the network perimeter. Once SlashNext detects a phishing page, it will immediately serve a warning page and block access to the malicious content.

You can install these extensions directly from official stores:

Chrome:
Download Here

Firefox:
Download Here

Safari:
Download Here

Edge Chromium:
Download Here

Edge:
Download Here

Internet Explorer:
Download Here

After installation, please enter your personal activation key, provided below. Please note, this is a personal key and should not be shared with anyone.

Activation Key

[redacted]

Your Designated Administrator

Irvin Feldberger

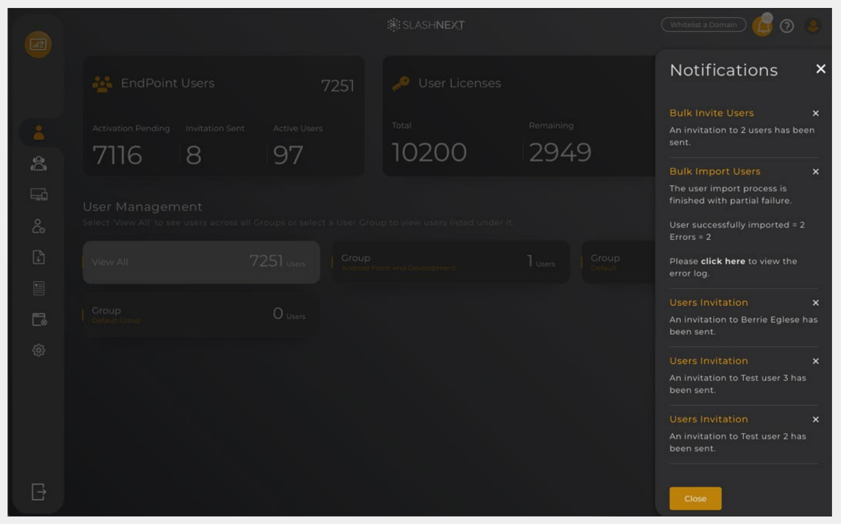
You may send your feedback or open a support case either with your IT administrator or SlashNext directly from the Extension Menu

Learn more about us at www.slashnext.com

SlashNext extensions do not collect personal user information or share information with third parties.

12 EMS NOTIFICATIONS

Users can check any Admin Area notifications by clicking on the bell icon on the top right of any page on the Admin Area. Most recent events and updates are displayed there in chronological order – with the most recent at the top. Invitation sent and bulk import process are all displayed here.



Notifications ×

Bulk Invite Users ×
An invitation to 2 users has been sent.

Bulk Import Users ×
The user import process is finished with partial failure.

User successfully imported = 2
Errors = 2

Please **click here** to view the error log.

Users Invitation ×
An invitation to Berrie Eglese has been sent.

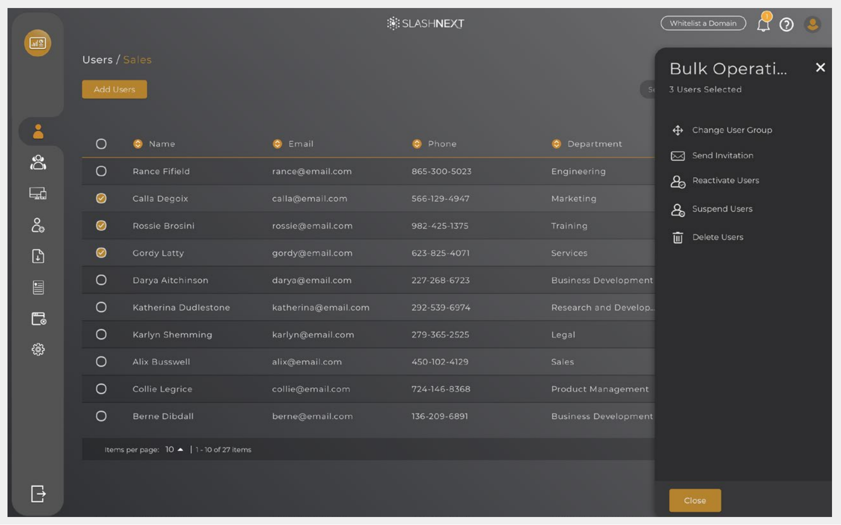
Users Invitation ×
An invitation to Test user 3 has been sent.

Users Invitation ×
An invitation to Test user 2 has been sent.

Close

13 BULK OPERATIONS

CMS Admin Area is a powerful tool allowing administrators to act on multiple users at a time. From the user's tab, pick a user group to display all the users assigned to it.



○	Name	Email	Phone	Department
○	Rance Fifield	rance@email.com	865-300-5023	Engineering
✓	Calla Degoix	calla@email.com	566-129-4947	Marketing
✓	Rossie Brosini	rossie@email.com	982-425-1375	Training
✓	Gordy Latty	gordy@email.com	623-825-4071	Services
○	Darya Aitchinson	darya@email.com	227-268-6723	Business Development
○	Katherina Dudlestone	katherina@email.com	292-539-6974	Research and Develop...
○	Karlyn Shemming	karlyn@email.com	279-365-2525	Legal
○	Alix Busswell	alix@email.com	450-102-4129	Sales
○	Collie Legrice	collie@email.com	724-146-8368	Product Management
○	Berne Dibdall	berne@email.com	136-209-6891	Business Development

Items per page: 10 | 1 - 10 of 27 items

Bulk Operati... ×
3 Users Selected

14 WHITELISTING DOMAINS

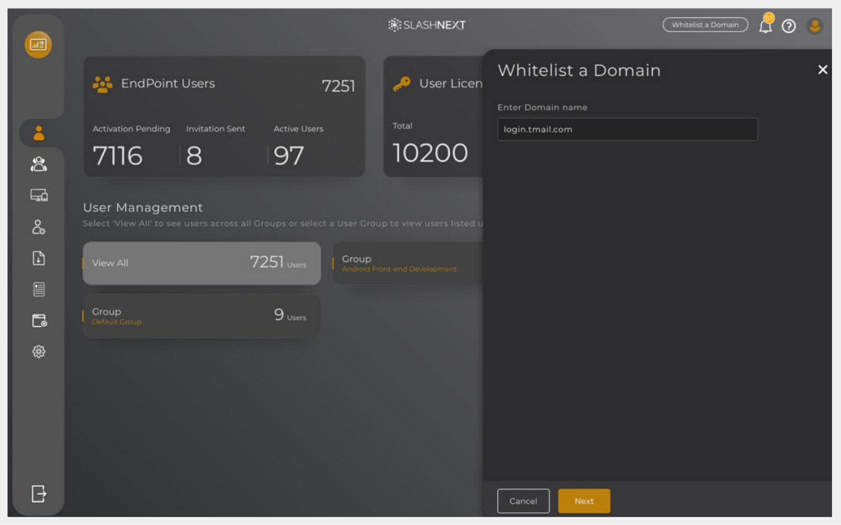
In order to give organizations greater control over what they consider malicious activity, CMS allows enterprise customers to whitelist specific domains as safe. Once the domain is whitelisted in the Web console, SlashNext Phishing Protection endpoint products will allow employees access to it without any restrictions.

How to specify which domains to whitelist?

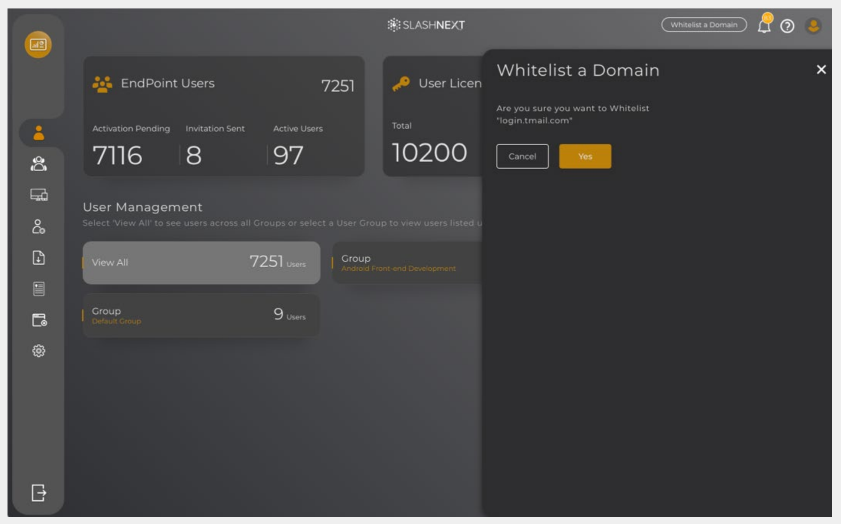
In order to give organizations greater control over what they consider malicious activity, CMS allows enterprise customers to whitelist specific domains as safe. Once the domain is whitelisted in the Web console, SlashNext Phishing Protection endpoint products will allow employees access to it without any restrictions.

How to specify which domains to whitelist?

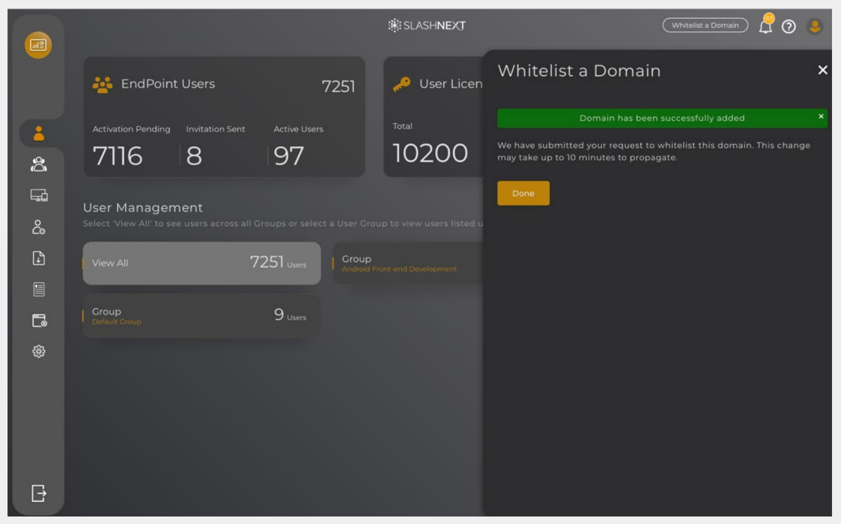
1. Once logged into CMS console, a "Whitelist a Domain" option will be availableGroup administrators
2. Type the domain name into that option (e.g. "login.tmail.com") and click "Next"
3. Then, after an "Are you sure" screen appears, a "Domain has been successfully added" message will confirm the whitelisted domain has been entered into CMS
4. The system will normally process these requests within 10 minutes



Enter Domain name: login.tmail.com



Are you sure you want to Whitelist "login.tmail.com"



Whitelist a Domain

Domain has been successfully added

We have submitted your request to whitelist this domain. This change may take up to 10 minutes to propagate.

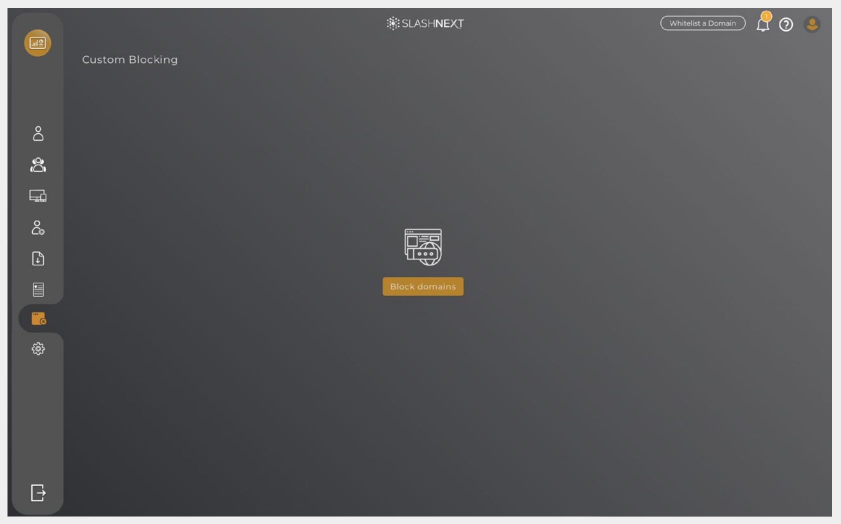
Done

Note

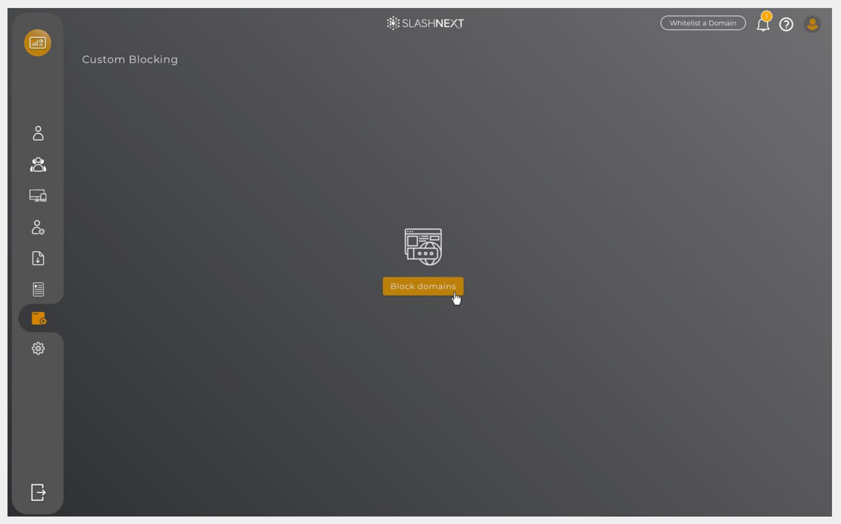
Once a domain has been successfully whitelisted, SlashNext support will need to be contacted directly support@slashnext.com in order to remove it from the whitelist.

15 HOW TO ADD DOMAINS TO CUSTOM BLOCKING?

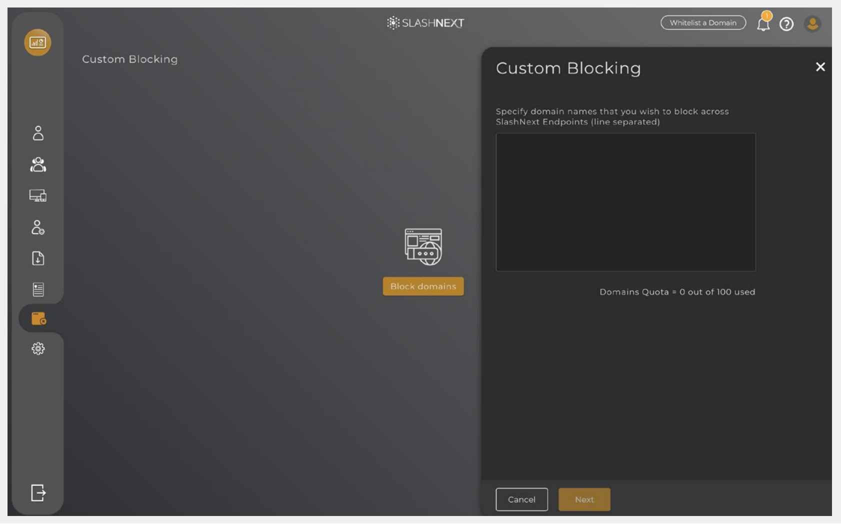
Go to Admin Area and click on to Custom Blocking



Click on to Block domains



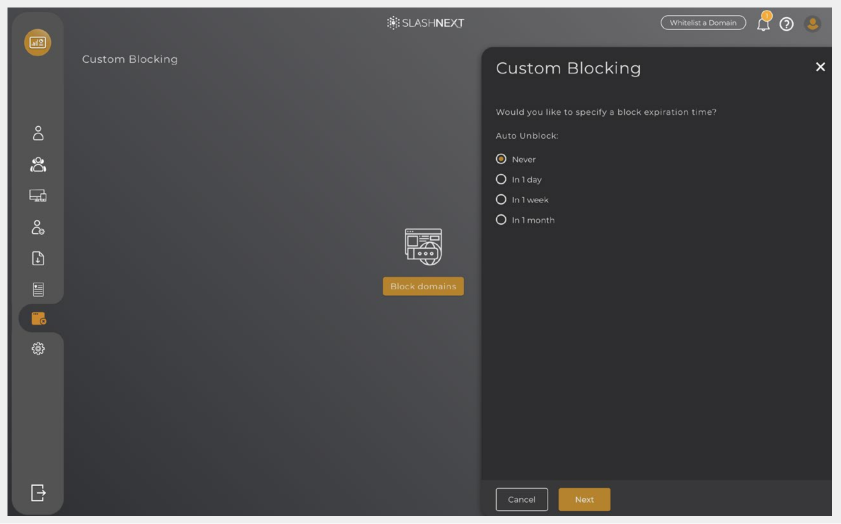
Add domain names that you wish to block



Specify domain names that you wish to block across SlashNext Endpoints (line separated)

Domains Quota = 0 out of 100 used

Specify block expiration time

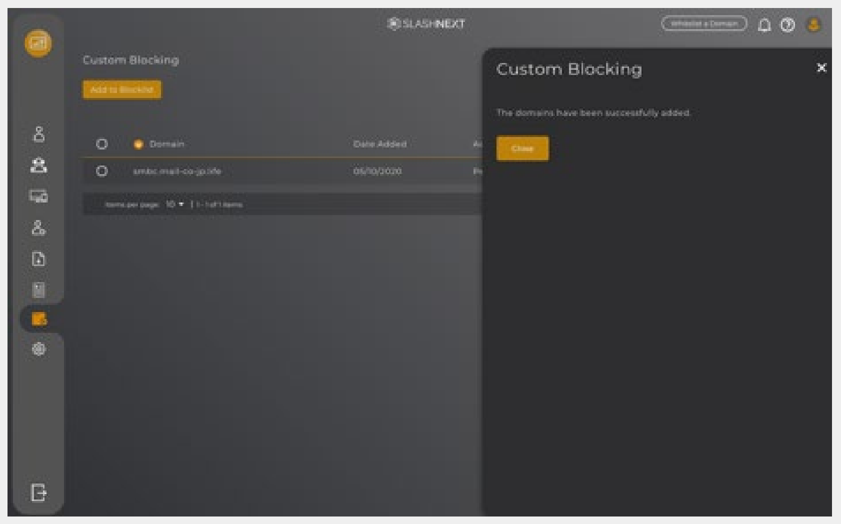


Would you like to specify a block expiration time?

Auto Unblock:

● Never
○ In 1 day
○ In 1 week
○ In 1 month

The domain has been successfully added to blocklist



Custom Blocking

Add to Blocklist

○	Domain	Date Added
○	smbc.mail-co-jp.life	05/10/2020

Items per page: 10 ▾ | 1 - 1 of 1 items

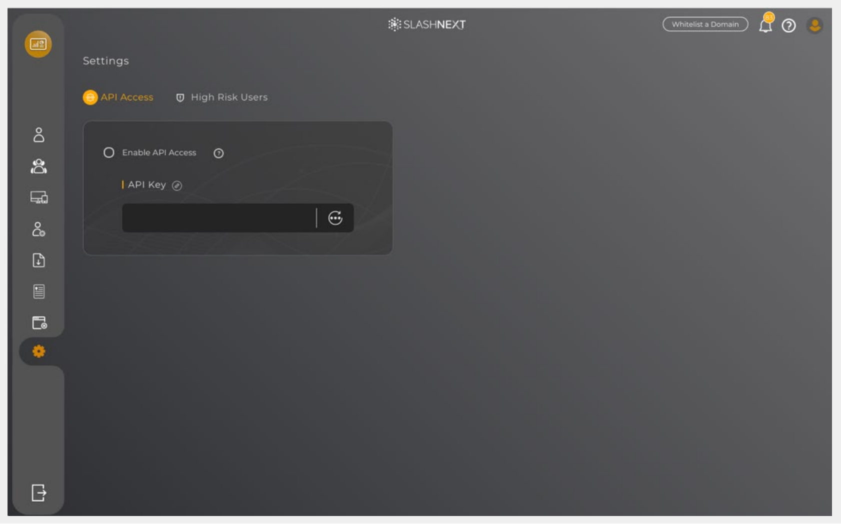
Custom Blocking ×

The domains have been successfully added.

Close

16 HOW TO ENABLE API ACCESS?

Go to Admin Area and click on to settings, select API Access



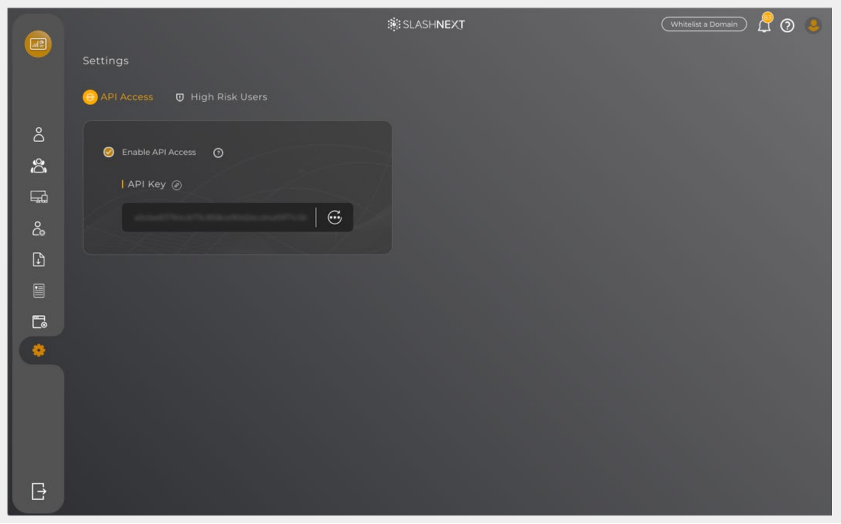
Settings

API Access | High Risk Users

○ Enable API Access

API Key

Click to Check Enable API Access it will generate API Key for you to use



Settings

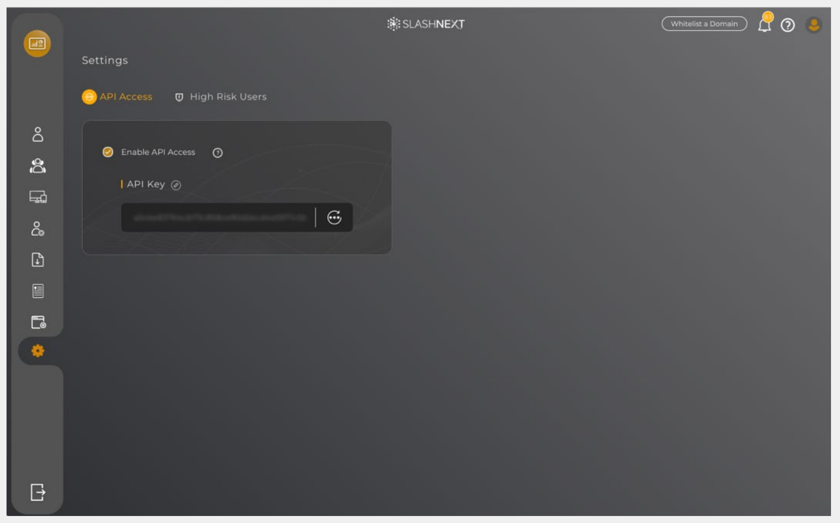
API Access | High Risk Users

☑ Enable API Access

API Key

16.1 HOW TO REGENERATE API ACCESS KEY?

Go to Admin Area and click on to settings, select API Access

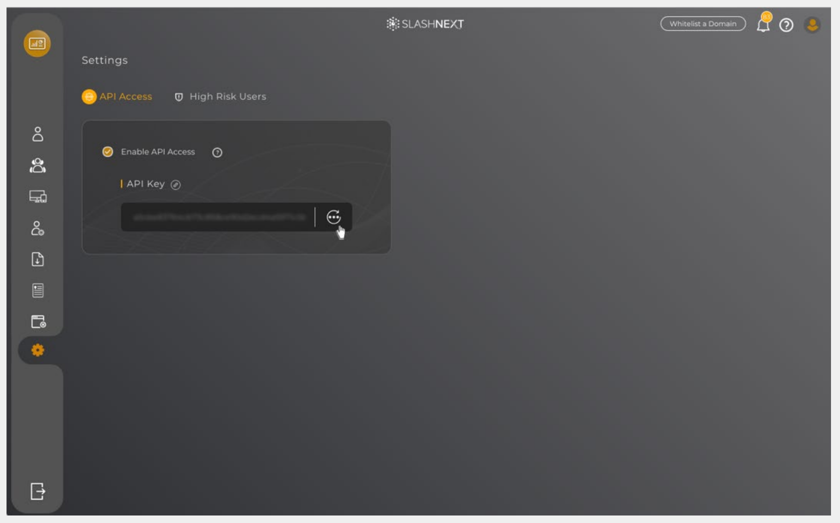


☑ Enable API Access

API Key

[redacted]

Click on to Regenerate API Access Key icon

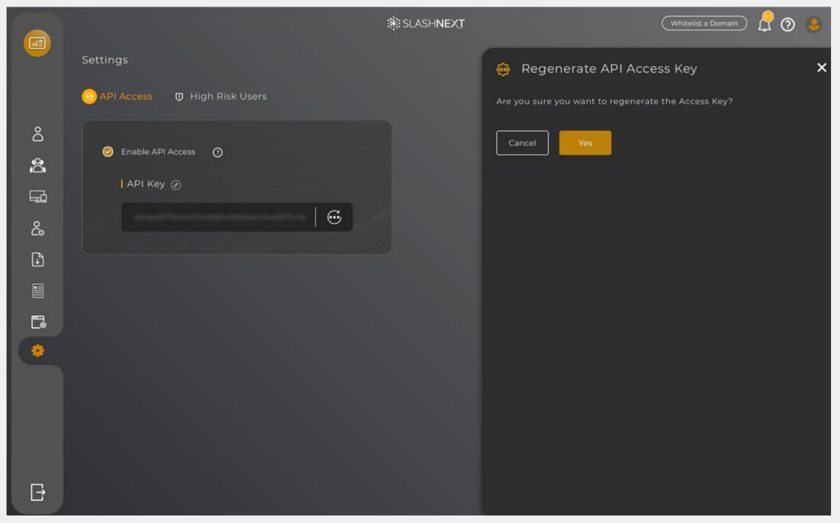


☑ Enable API Access

API Key

[redacted]

Confirm to Regenerate API Access Key by Clicking on to Yes. New API key will be generated, and it will disable the previous API Key.



☑ Enable API Access

API Key

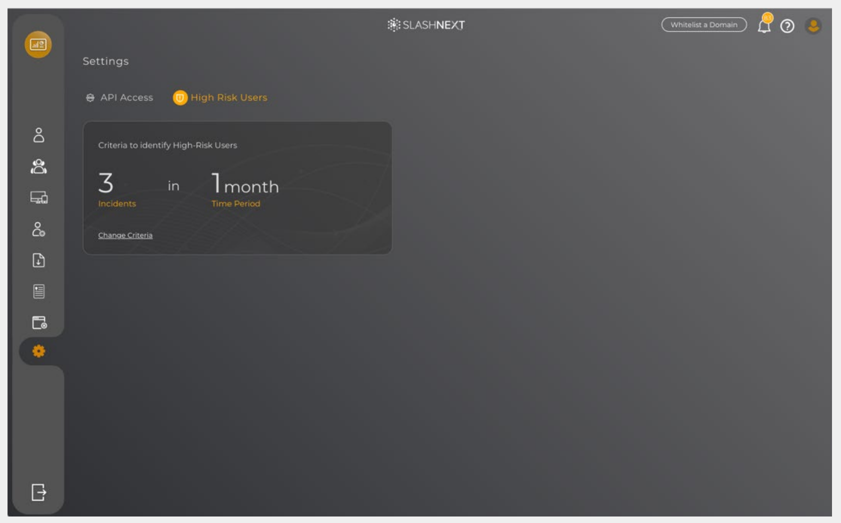
[redacted]

Regenerate API Access Key

Are you sure you want to regenerate the Access Key?

17 HOW TO RE-DEFINE HIGH RISK USER?

You can customize High Risk User Criteria to your own terms. If you would like to re-define High Risk User Criteria go to Admin Area and click on to settings, select High Risk User Criteria

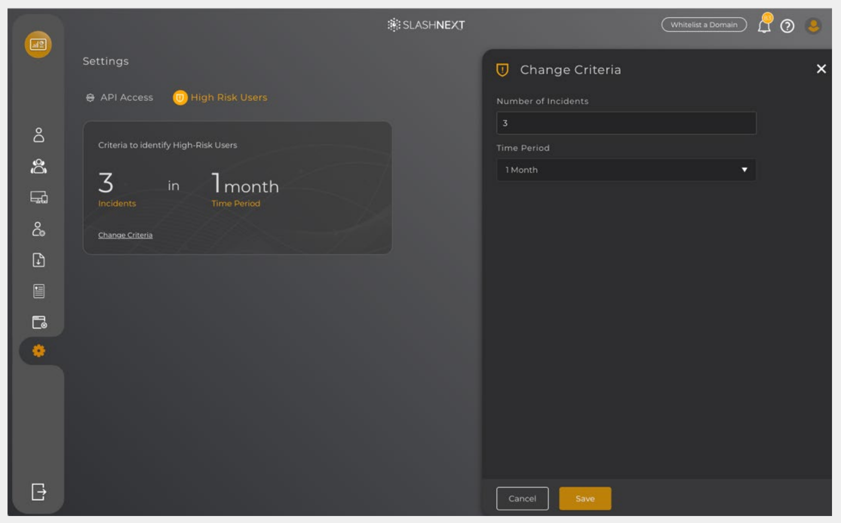


Criteria to identify High-Risk Users

3 in 1 month

Incidents Time Period

Click on to Re-define High Risk User Criteria



Criteria to identify High-Risk Users

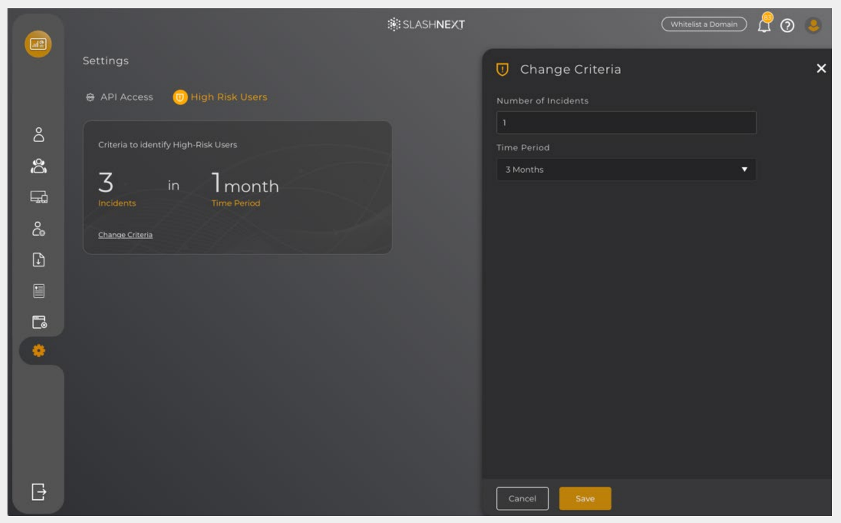
3 in 1 month

Incidents Time Period

Number of Incidents: 3

Time Period: 1 Month

Set or define your High Risk User Criteria and click on Save



Criteria to identify High-Risk Users

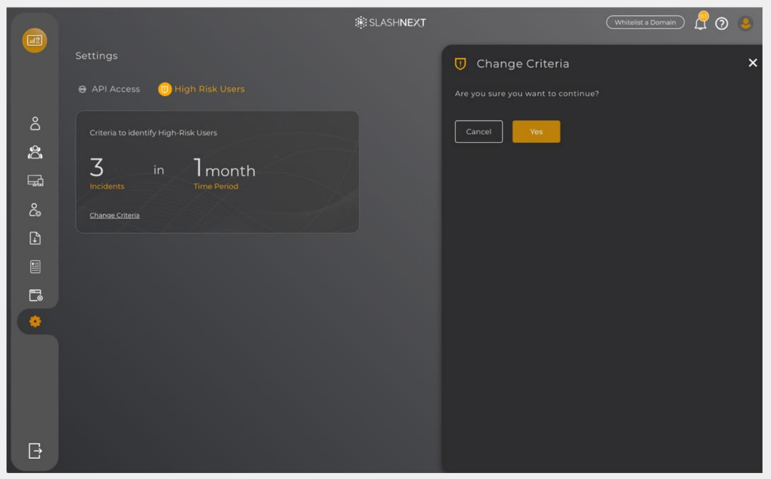
3 in 1 month

Incidents Time Period

Number of Incidents: 1

Time Period: 3 Months

Confirm it by click on to Yes



Criteria to identify High-Risk Users

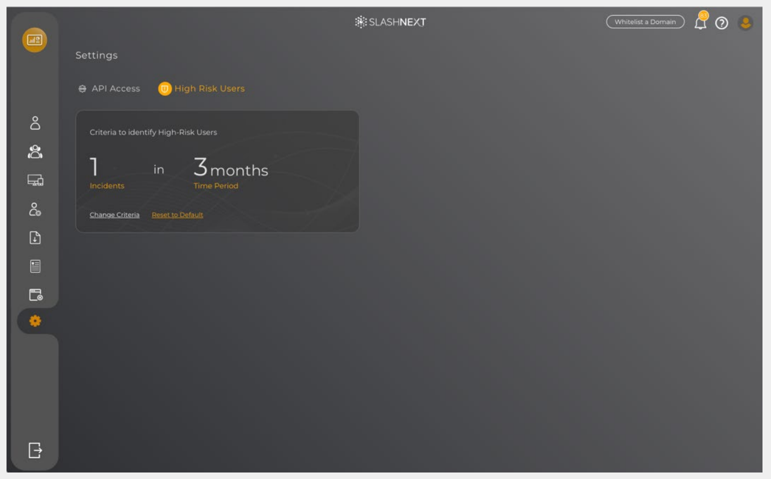
3 in 1 month

Incidents Time Period

Change Criteria

Are you sure you want to continue?

Once you have re-defined the High Risk User Criteria you can Reset it to default anytime by clicking on to Reset to Default



Criteria to identify High-Risk Users

1 in 3 months

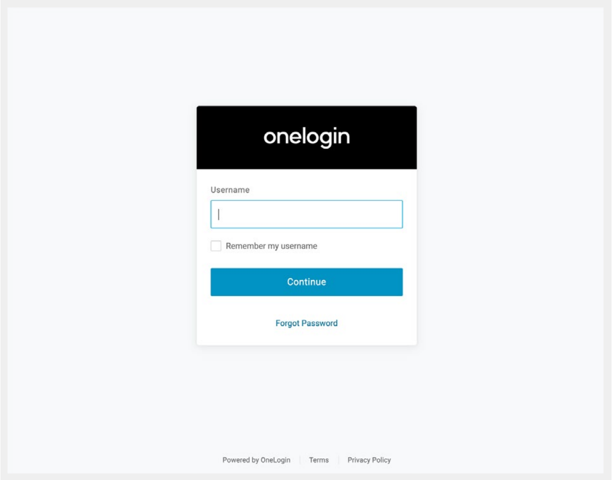
Incidents Time Period

18 ONELOGIN SSO INTEGRATION

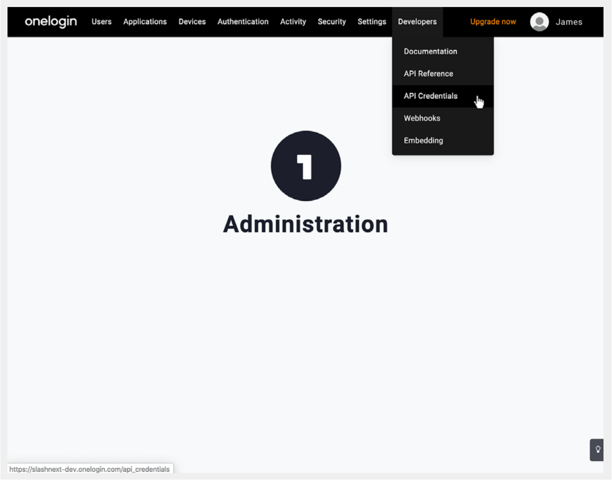
SlashNext CMS is a Web Console built for enterprise network team members (IT and security administrators) that allows them to provision, deploy and manage our Mobile Phishing Protection and Browser Phishing Protection endpoint products. CMS provides real-time information, displaying the latest deployments, activations, and licensing status of the products in real-time for the organization's entire user base.

Following are the steps for OneLogin SSO Integration being implemented in CMS

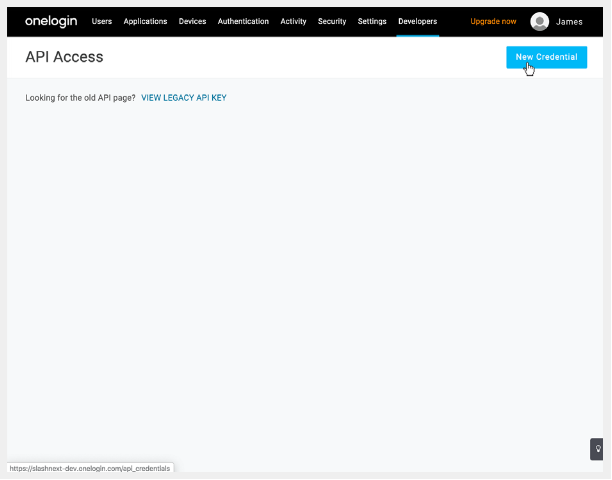
1. Login to OneLogin account.



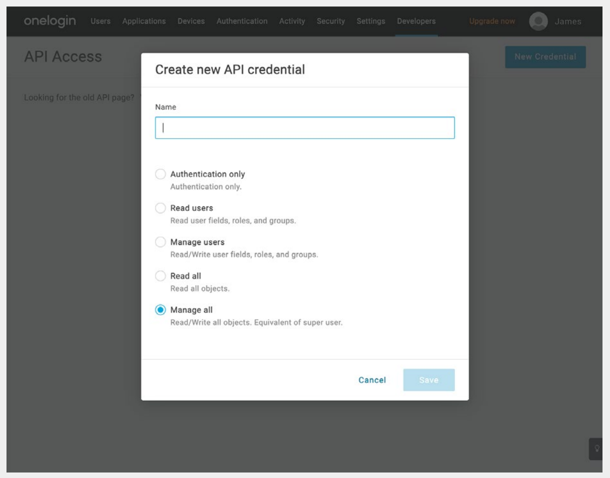
2. From the company's main dashboard page, click on **Developers → API** Credentials link from the Main Navigation bar.



3. Click the **New Credentials** button



4. Enter the name for new credentials in the form and select the **Manage All** option below. Click on **Save** button



Create new API credential

Name

○ Authentication only
Authentication only.

○ Read users
Read user fields, roles, and groups.

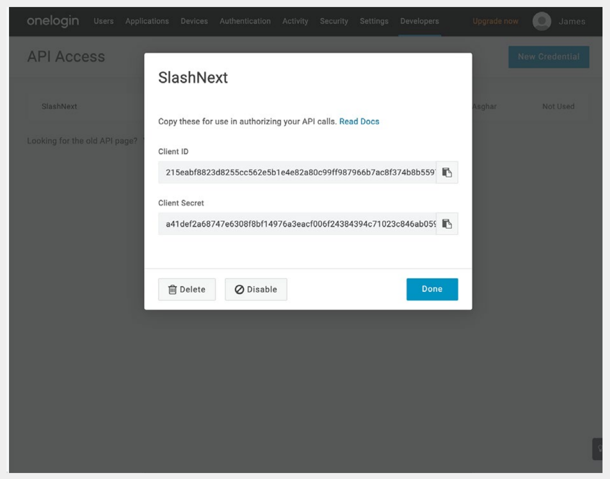
○ Manage users
Read/Write user fields, roles, and groups.

○ Read all
Read all objects.

● Manage all
Read/Write all objects. Equivalent of super user.

Cancel
Save

5. Form will display the **Client ID** and **Client Secret** to be used in OneLogin APIs



SlashNext

Copy these for use in authorizing your API calls. Read Docs

Client ID
215eabf8823d8255cc562e5b1e4e82a80c99ff987966b7ac8f374b8b559

Client Secret
a41def2a68747e6308f8bf14976a3eacf006f24384394c71023c846ab05

Delete
Disable
Done

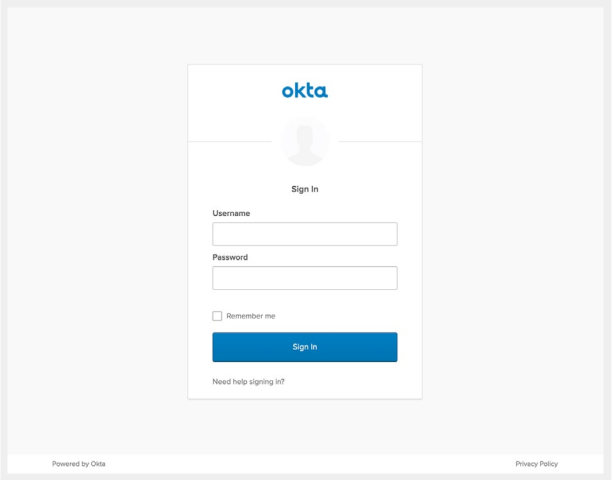
6. Click on **Done** button to finish

19 OKTA SSO INTEGRATION

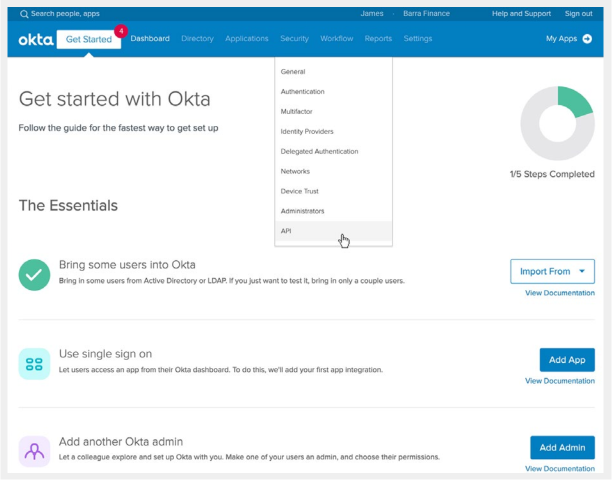
SlashNext CMS is a Web Console built for enterprise network team members (IT and security administrators) that allows them to provision, deploy and manage our Mobile Phishing Protection and Browser Phishing Protection endpoint products. CMS provides real-time information, displaying the latest deployments, activations, and licensing status of the products in real-time for the organization's entire user base.

Following are the steps for Okta SSO Integration being implemented in CMS

1. Login to OKTA account



2. From the top menu go to **Security → API**



Get started with Okta

Follow the guide for the fastest way to get set up

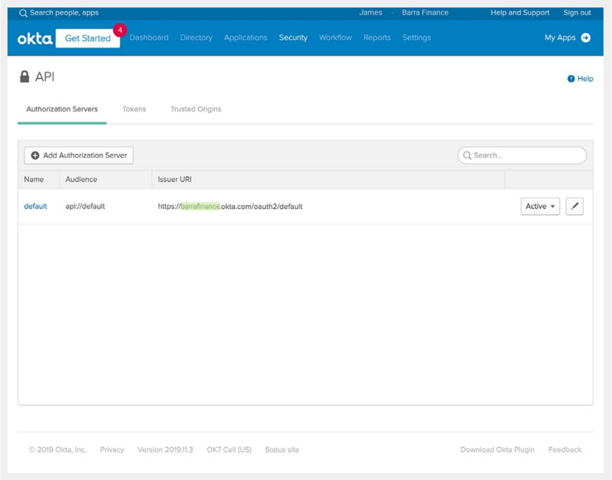
The Essentials

Bring some users into Okta
Bring in some users from Active Directory or LDAP. If you just want to test it, bring in only a couple users.

Use single sign on
Let users access an app from their Okta dashboard. To do this, we'll add your first app integration.

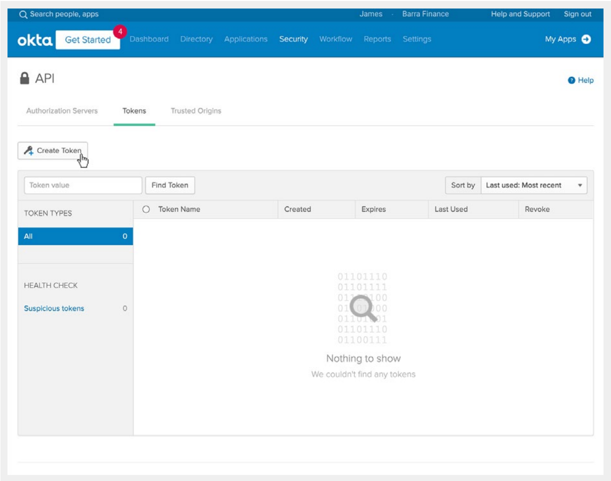
Add another Okta admin
Let a colleague explore and set up Okta with you. Make one of your users an admin, and choose their permissions.

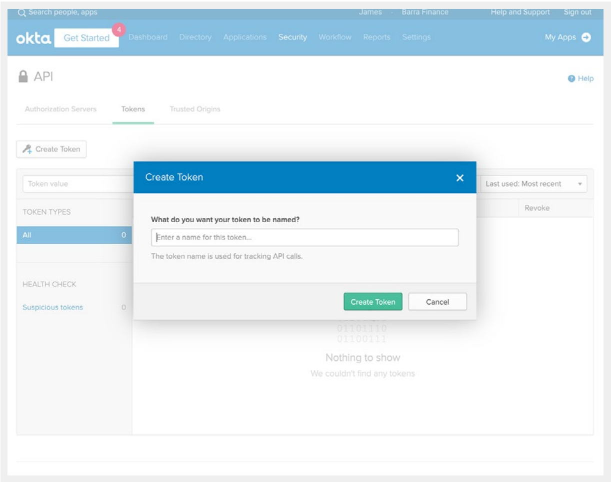
3. For the **Organization URL** go to the **"Authorization Servers"** tab and copy the Okta domain part mentioned under the column **"Issuer URI"**
e.g. https://youroktadomain.okta.com/oauth2/default.



Name	Audience	Issuer URI
default	api://default	https://barrafinance.okta.com/oauth2/default

4. For the **API Token** go to the **"Tokens"** tab and click **"Create Token"** button, you will be prompted to provide a name for the token. Enter a value e.g. "CMS Token" and click **"Create Token"**. Please make a note of this token and save it in a safe place as it will be the only time that you will be able to view it

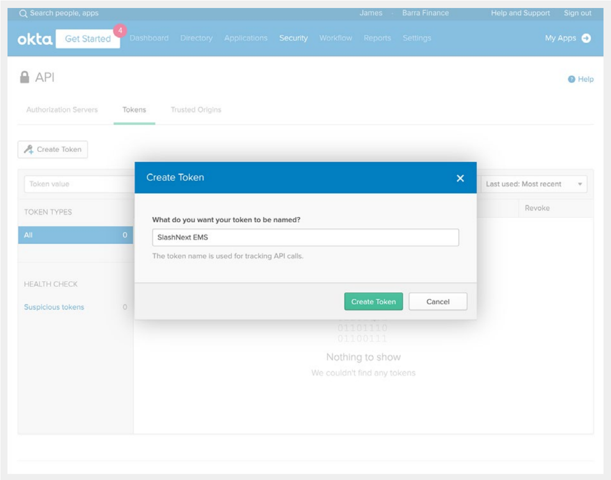




What do you want your token to be named?

Enter a name for this token...

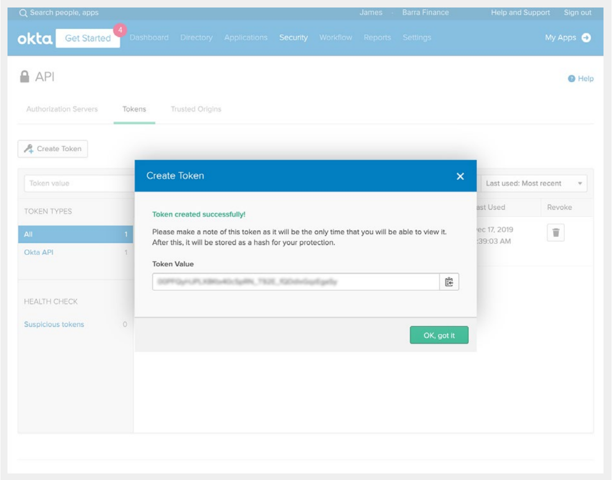
The token name is used for tracking API calls.



What do you want your token to be named?

SlashNext EMS

The token name is used for tracking API calls.



Token created successfully!

Please make a note of this token as it will be the only time that you will be able to view it. After this, it will be stored as a hash for your protection.

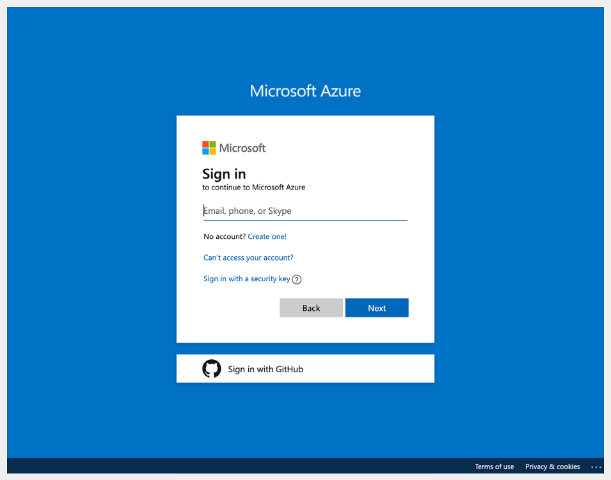
Token Value

20 AZURE ACTIVE DIRECTORY SSO INTEGRATION

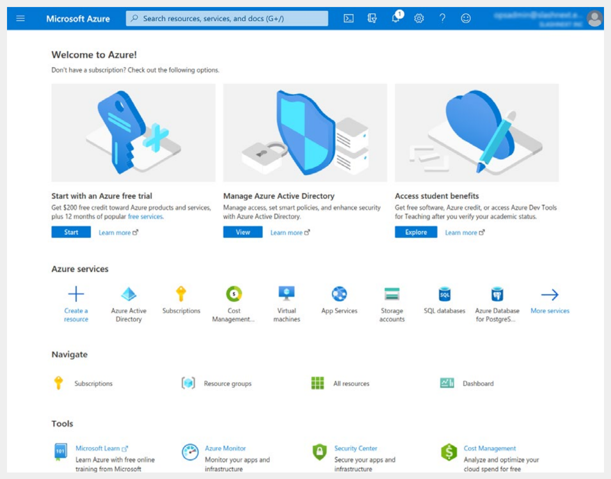
SlashNext CMS is a Web Console built for enterprise network team members (IT and security administrators) that allows them to provision, deploy and manage our Mobile Phishing Protection and Browser Phishing Protection endpoint products. CMS provides real-time information, displaying the latest deployments, activations, and licensing status of the products in real-time for the organization's entire user base.

Following are the steps for Azure Active Directory SSO Integration being implemented in CMS

1. Log into Microsoft Azure account



2. Go into **Azure Active Directory** dashboard through Azure services or searching resources



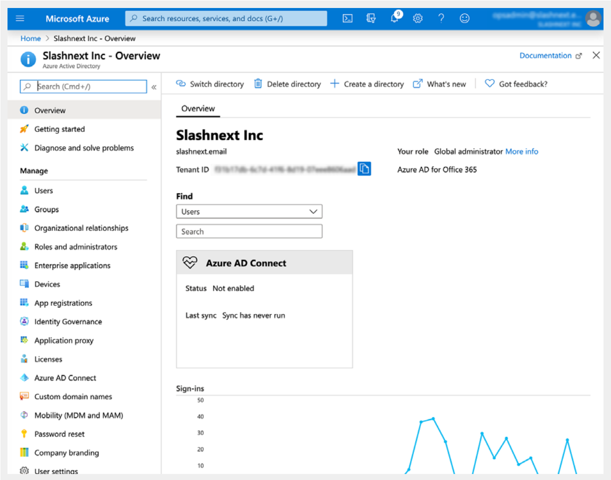
Welcome to Azure!

Don't have a subscription? Check out the following options.

Start with an Azure free trial
Get $200 free credit toward Azure products and services, plus 12 months of popular free services.

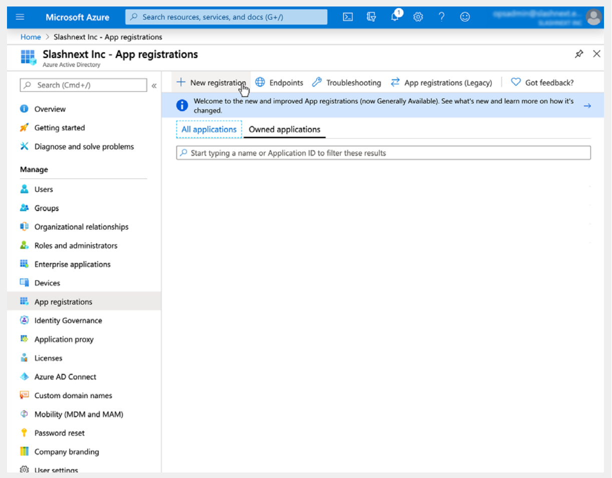
Manage Azure Active Directory
Manage access, set smart policies, and enhance security with Azure Active Directory.

Access student benefits
Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.



Slashnext Inc
slashnext.email
Tenant ID [redacted]
Your role Global administrator More info
Azure AD for Office 365
Find
Users
Search
Azure AD Connect
Status Not enabled
Last sync Sync has never run

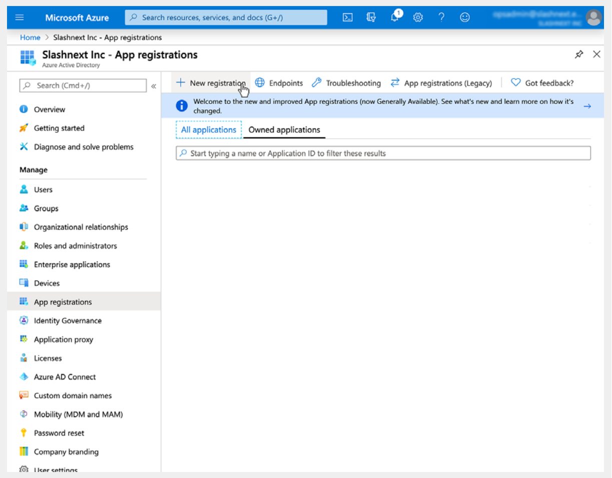
3. Go to **App Registrations** under the **Manage tab** in the left navigation folder



Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed.

Start typing a name or Application ID to filter these results

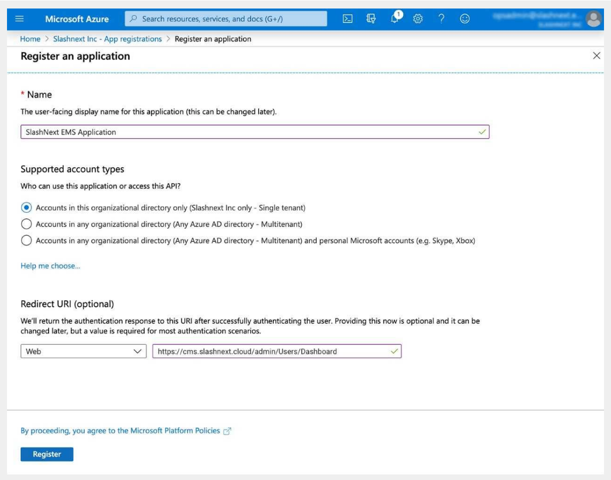
4. Click **New Registration** button to create a new application



Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed.

Start typing a name or Application ID to filter these results

5. Provide the following details and click **Register**. Azure will navigate to its main page.
    - Application Name e.g. SlashNextGroup administrators CMS Application.
    - Supported account type (use default selection).
    - Redirect URL (https://cms.slashnext.cloud/admin/Users/Dashboard)


Microsoft Azure
Search resources, services, and docs (G+/)
[redacted]
Home > Slashnext Inc - App registrations > Register an application

Register an application

* Name

The user-facing display name for this application (this can be changed later).

SlashNext EMS Application

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Slashnext Inc only - Single tenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Help me choose...

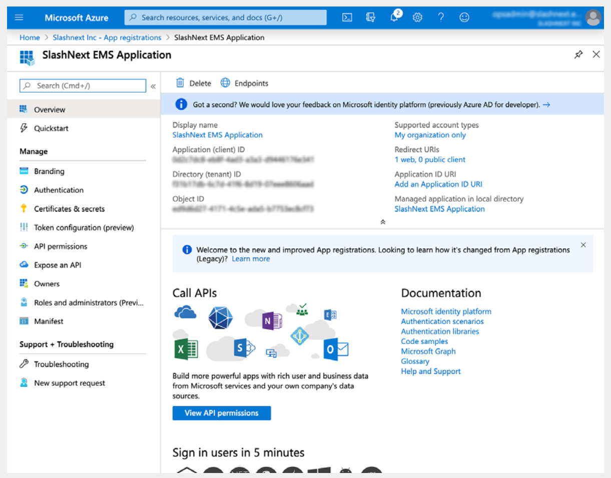
Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | https://cms.slashnext.cloud/admin/Users/Dashboard

By proceeding, you agree to the Microsoft Platform Policies

6. Note the **Application (Client) ID**, and **Directory (Tenant) ID** to be used in CMS


Microsoft Azure
Search resources, services, and docs (G+/)
[redacted]
Home > Slashnext Inc - App registrations > SlashNext EMS Application
Search (Cmd+/)
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
Token configuration (preview)
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Delete
Endpoints

SlashNext EMS Application

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name
SlashNext EMS Application

Application (client) ID
[redacted]

Directory (tenant) ID
[redacted]

Object ID
[redacted]

Supported account types
My organization only

Redirect URIs
1 web, 0 public client

Application ID URI
Add an Application ID URI

Managed application in local directory
SlashNext EMS Application

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Call APIs

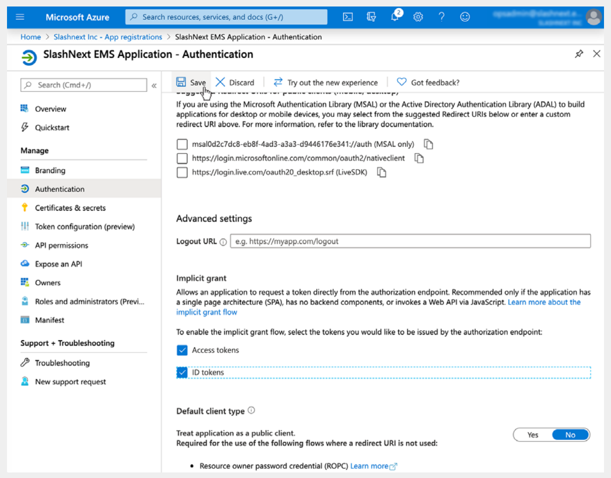
Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Documentation

Microsoft identity platform
Authentication scenarios
Authentication libraries
Code samples
Microsoft Graph
Glossary
Help and Support

Sign in users in 5 minutes

7. Go to **Authentication** link under Manage tab in left navigation bar and check the **Access Tokens** and **ID Tokens** under **Implicit Grant** and click **Save**


Microsoft Azure
Search resources, services, and docs (G+/)
[redacted]
Home > Slashnext Inc - App registrations > SlashNext EMS Application - Authentication
Search (Cmd+/)
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
Token configuration (preview)
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Save
Discard
Try out the new experience
Got feedback?

SlashNext EMS Application - Authentication

If you are using the Microsoft Authentication Library (MSAL) or the Active Directory Authentication Library (ADAL) to build applications for desktop or mobile devices, you may select from the suggested Redirect URIs below or enter a custom redirect URI above. For more information, refer to the library documentation.

□ msal0d2c7dc8-eb8f-4ad3-a3a3-d9446176e341://auth (MSAL only)
□ https://login.microsoftonline.com/common/oauth2/nativeclient
□ https://login.live.com/oauth20_desktop.srf (LiveSDK)

Advanced settings

Logout URL: e.g. https://myapp.com/logout

Implicit grant

Allows an application to request a token directly from the authorization endpoint. Recommended only if the application has a single page architecture (SPA), has no backend components, or invokes a Web API via JavaScript. Learn more about the implicit grant flow

To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:

☑ Access tokens
☑ ID tokens

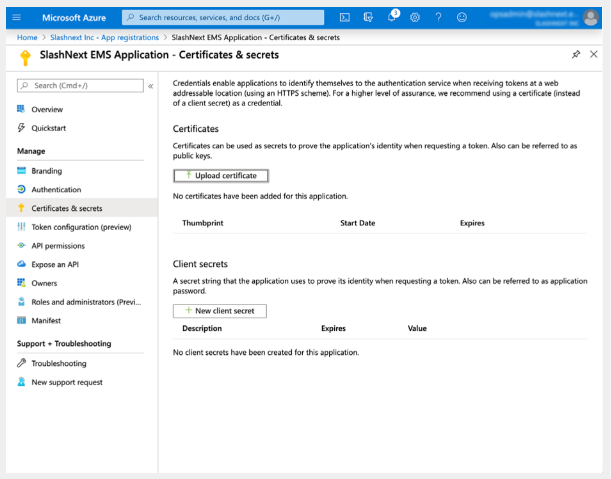
Default client type

Treat application as a public client.
Required for the use of the following flows where a redirect URI is not used:

Yes [✓ No]

- Resource owner password credential (ROPC) Learn more

8. Go to **Certificates & Secrets** link under Manage tab and click on **New Client Secret** button under **Client Secrets**


Microsoft Azure
Search resources, services, and docs (G+/)
3
[redacted]
Home > Slashnext Inc - App registrations > SlashNext EMS Application - Certificates & secrets
SlashNext EMS Application - Certificates & secrets
Search (Cmd+/)
«
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
Token configuration (preview)
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Upload certificate
New client secret

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

No certificates have been added for this application.

Thumbprint	Start Date	Expires

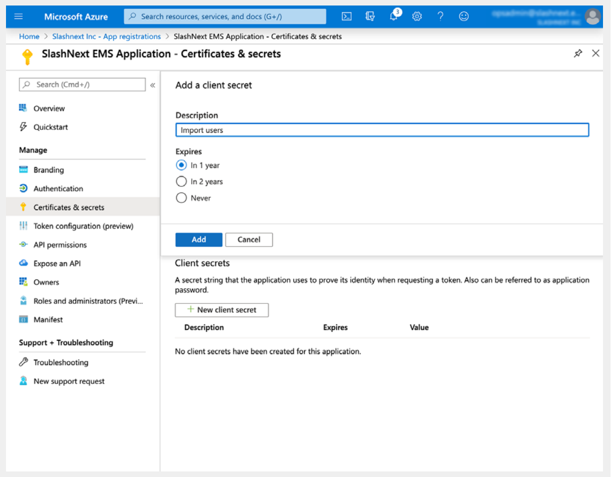
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value

No client secrets have been created for this application.

9. Add the client description with expiry time and click **Add** button


Microsoft Azure
Search resources, services, and docs (G+/)
3
[redacted]
Home > Slashnext Inc - App registrations > SlashNext EMS Application - Certificates & secrets
SlashNext EMS Application - Certificates & secrets
Search (Cmd+/)
«
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
Token configuration (preview)
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Add
Cancel
New client secret

Add a client secret

Description: Import users

Expires

● In 1 year

○ In 2 years

○ Never

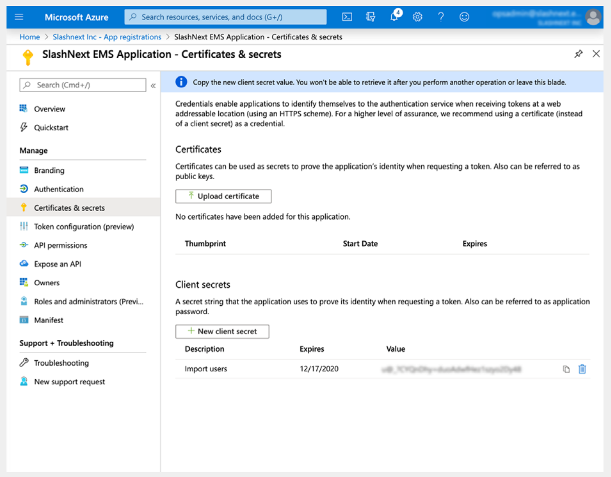
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value

No client secrets have been created for this application.

10. Note the **Client Secret** to be used in CMS


Microsoft Azure
Search resources, services, and docs (G+/)
4
[redacted]
Home > Slashnext Inc - App registrations > SlashNext EMS Application - Certificates & secrets
SlashNext EMS Application - Certificates & secrets
Search (Cmd+/)
«
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
Token configuration (preview)
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Upload certificate
New client secret

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

No certificates have been added for this application.

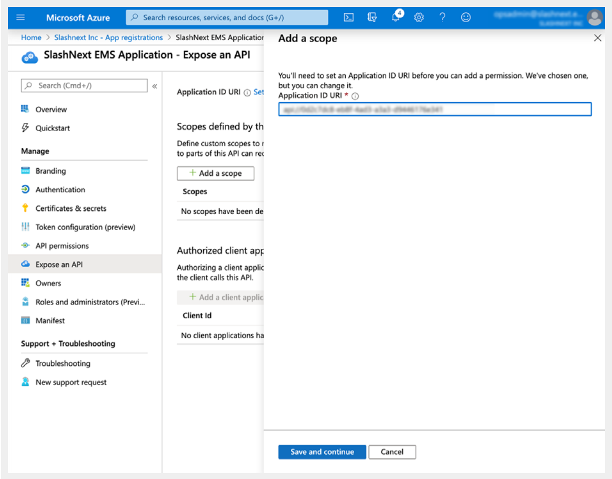
Thumbprint	Start Date	Expires

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value
Import users	12/17/2020	[redacted]

11. Go to **Expose an API** link under Manage tab and click on **Add a Scope** button

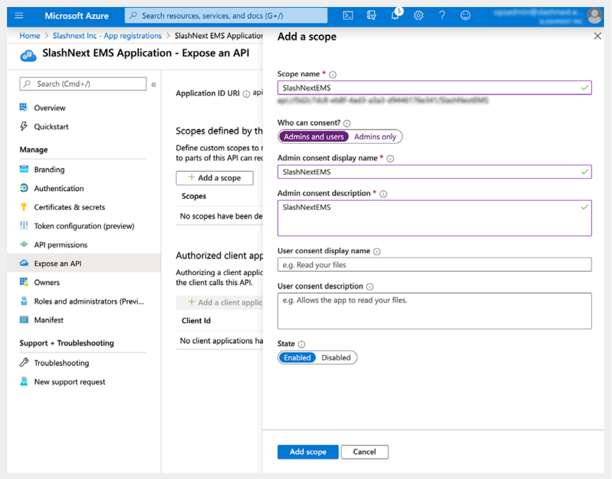


Add a scope

You'll need to set an Application ID URI before you can add a permission. We've chosen one, but you can change it.

Application ID URI * [redacted]

12. Click **Save and continue** button
    - Scope name = "SlashNextCMS".
    - Who can Consent? = select the "Admin and Users" option. c. Admin consent display name = "SlashNextCMS".
    - Description = "SlashNextCMS".


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Slashnext Inc - App registrations > SlashNext EMS Application
SlashNext EMS Application - Expose an API
Search (Cmd+/)
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
Token configuration (preview)
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Admins only
Disabled
Add scope
Cancel

Add a scope

Scope name * SlashNextEMS
[redacted]

Who can consent? Admins and users

Admin consent display name * SlashNextEMS

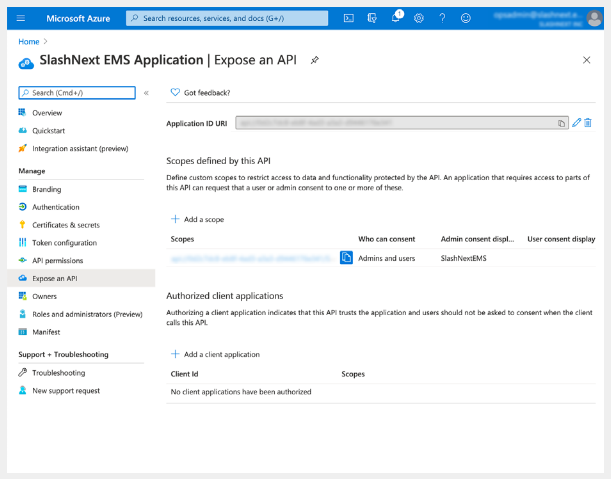
Admin consent description * SlashNextEMS

User consent display name: e.g. Read your files

User consent description: e.g. Allows the app to read your files.

State: Enabled

13. Once the scope is added successfully, it will be listed under the **Scopes** section. Click on the **copy** link next to the newly added scope and note it down to be used in CMS



Application ID URI [redacted]

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

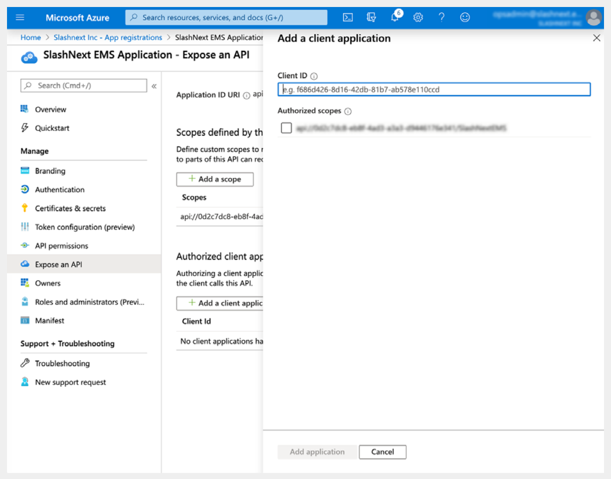
Scopes	Who can consent	Admin consent displ...	User consent display
[redacted]	Admins and users	SlashNextEMS	

Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

Client Id	Scopes
No client applications have been authorized	

14. Click the **Add a client application** button. Enter the **Client ID** noted before



Define custom scopes to r
to parts of this API can rec

api://0d2c7dc8-eb8f-4ad

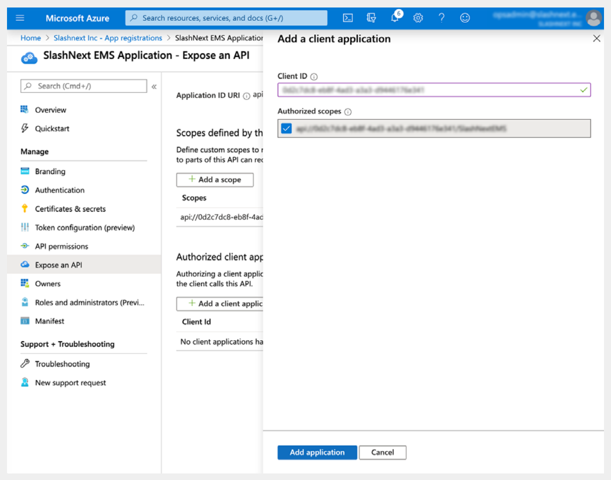
Authorizing a client applic
the client calls this API.

No client applications ha

Client ID: e.g. f686d426-8d16-42db-81b7-ab578e110ccd

Authorized scopes: □

15. Check the **Authorized Scopes** checkbox and click **Add Application** button



Define custom scopes to r
to parts of this API can rec

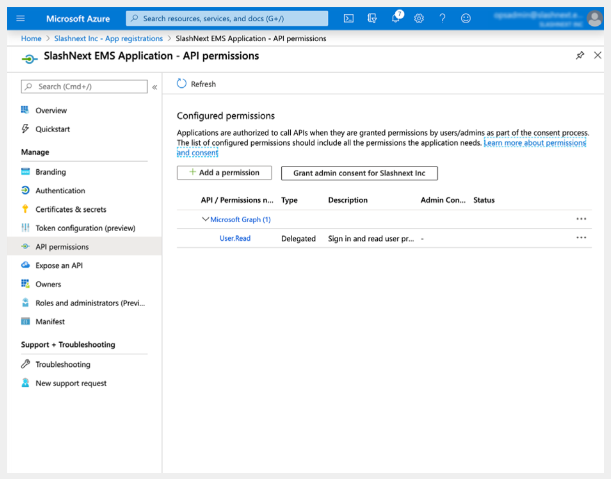
api://0d2c7dc8-eb8f-4ad

Authorizing a client applic
the client calls this API.

No client applications ha

Authorized scopes: ☑

16. Go to **API Permissions** link under the Manage tab in left navigation menu

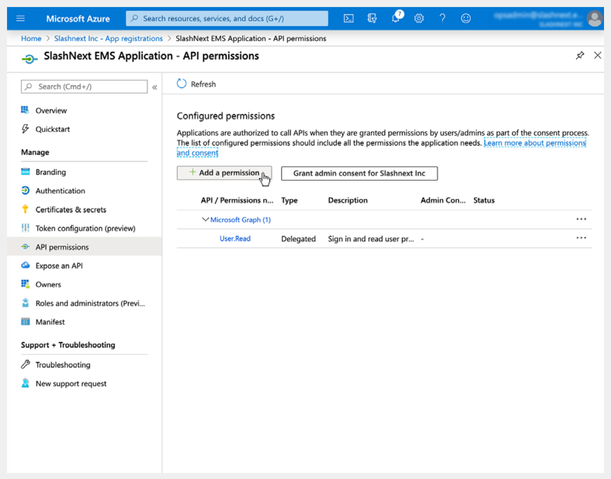

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Slashnext Inc - App registrations > SlashNext EMS Application - API permissions
SlashNext EMS Application - API permissions
Search (Cmd+/)
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
Token configuration (preview)
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Refresh
+ Add a permission
Grant admin consent for Slashnext Inc

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions n...	Type	Description	Admin Con...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user pr...	-	

17. Click on Add a **Permission** button

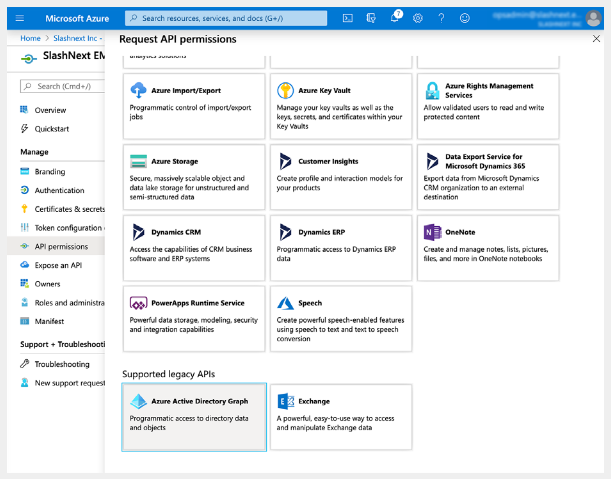

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Slashnext Inc - App registrations > SlashNext EMS Application - API permissions
SlashNext EMS Application - API permissions
Search (Cmd+/)
Refresh
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
Token configuration (preview)
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request
+ Add a permission
Grant admin consent for Slashnext Inc

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions n...	Type	Description	Admin Con...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user pr...	-	

18. Under **Supported Legacy APIs**, click **Azure Active Directory Graph**



Request API permissions

Azure Import/Export
Programmatic control of import/export jobs

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services
Allow validated users to read and write protected content

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights
Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

Dynamics CRM
Access the capabilities of CRM business software and ERP systems

Dynamics ERP
Programmatic access to Dynamics ERP data

OneNote
Create and manage notes, lists, pictures, files, and more in OneNote notebooks

PowerApps Runtime Service
Powerful data storage, modeling, security and integration capabilities

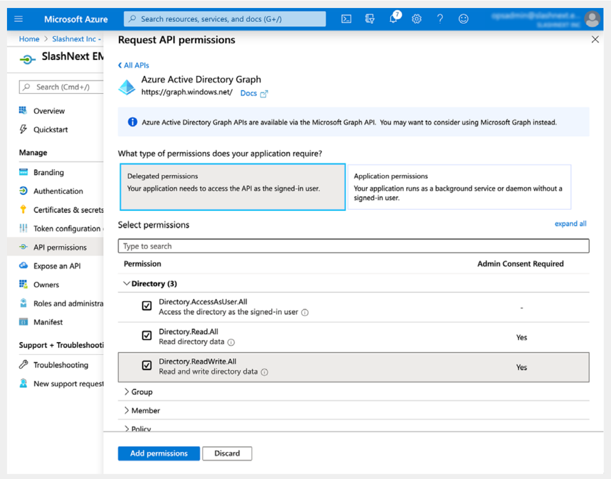
Speech
Create powerful speech-enabled features using speech to text and text to speech conversion

Supported legacy APIs

Azure Active Directory Graph
Programmatic access to directory data and objects

Exchange
A powerful, easy-to-use way to access and manipulate Exchange data

19. Click on **Delegated Permission** tab. Select all checkboxes under the **Directory**, **User** and **Group** options



Request API permissions

Azure Active Directory Graph
https://graph.windows.net/

Azure Active Directory Graph APIs are available via the Microsoft Graph API. You may want to consider using Microsoft Graph instead.

What type of permissions does your application require?

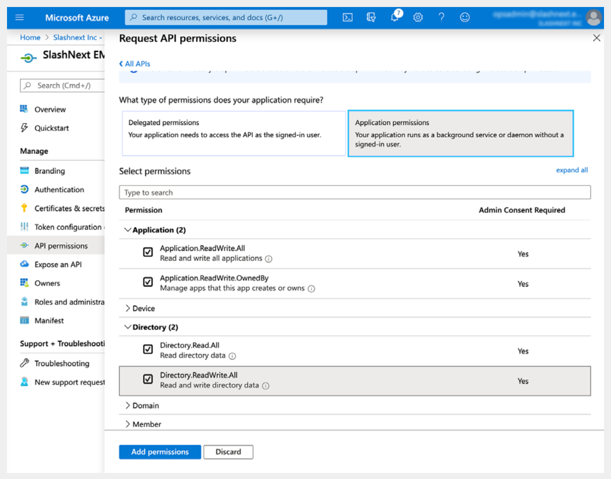
Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

Permission	Admin Consent Required
Directory (3)	
☑ Directory.AccessAsUser.All Access the directory as the signed-in user	-
☑ Directory.Read.All Read directory data	Yes
☑ Directory.ReadWrite.All Read and write directory data	Yes
> Group	
> Member	
> Policy	

20. Click on **Application Permissions** tab. Select all checkboxes under the **Application** and **Directory** options



Request API permissions

‹ All APIs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

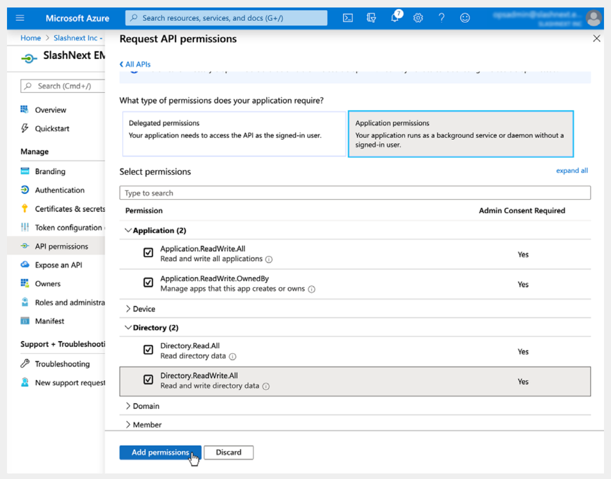
expand all

Type to search

Permission	Admin Consent Required
∨ Application (2)	
☑ Application.ReadWrite.All Read and write all applications ⓘ	Yes
☑ Application.ReadWrite.OwnedBy Manage apps that this app creates or owns ⓘ	Yes
› Device	
∨ Directory (2)	
☑ Directory.Read.All Read directory data ⓘ	Yes
☑ Directory.ReadWrite.All Read and write directory data ⓘ	Yes
› Domain	
› Member	

Add permissions | Discard

21. Click on **Add Permission** button



Request API permissions

‹ All APIs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

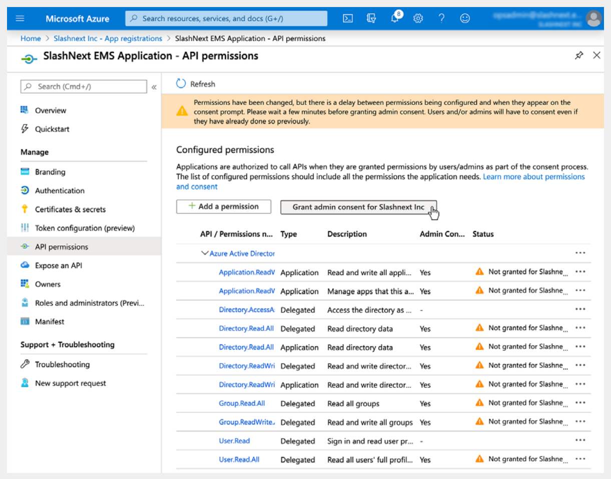
expand all

Type to search

Permission	Admin Consent Required
∨ Application (2)	
☑ Application.ReadWrite.All Read and write all applications ⓘ	Yes
☑ Application.ReadWrite.OwnedBy Manage apps that this app creates or owns ⓘ	Yes
› Device	
∨ Directory (2)	
☑ Directory.Read.All Read directory data ⓘ	Yes
☑ Directory.ReadWrite.All Read and write directory data ⓘ	Yes
› Domain	
› Member	

Add permissions | Discard

22. Click the **Grant Admin Consent** button


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Slashnext Inc - App registrations > SlashNext EMS Application - API permissions
Search (Cmd+/)
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
Token configuration (preview)
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request

SlashNext EMS Application - API permissions

Refresh

Permissions have been changed, but there is a delay between permissions being configured and when they appear on the consent prompt. Please wait a few minutes before granting admin consent. Users and/or admins will have to consent even if they have already done so previously.

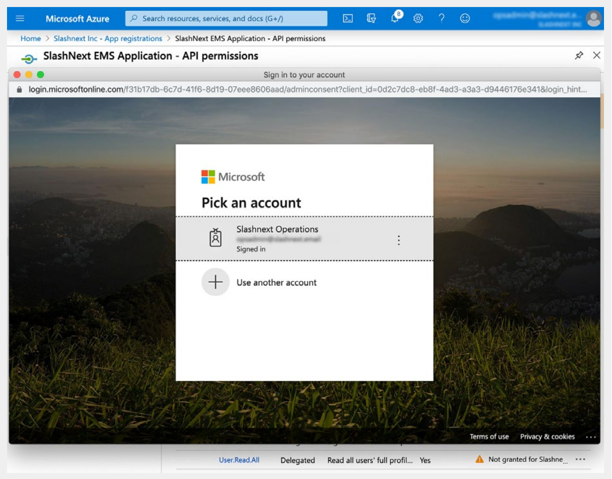
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission | Grant admin consent for Slashnext Inc

API / Permissions n...	Type	Description	Admin Con...	Status	
∨ Azure Active Director					•••
Application.ReadV	Application	Read and write all appli...	Yes	⚠ Not granted for Slashne...	•••
Application.ReadV	Application	Manage apps that this a...	Yes	⚠ Not granted for Slashne...	•••
Directory.AccessA	Delegated	Access the directory as ...	-		•••
Directory.Read.All	Delegated	Read directory data	Yes	⚠ Not granted for Slashne...	•••
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for Slashne...	•••
Directory.ReadWri	Delegated	Read and write director...	Yes	⚠ Not granted for Slashne...	•••
Directory.ReadWri	Application	Read and write director...	Yes	⚠ Not granted for Slashne...	•••
Group.Read.All	Delegated	Read all groups	Yes	⚠ Not granted for Slashne...	•••
Group.ReadWrite.	Delegated	Read and write all groups	Yes	⚠ Not granted for Slashne...	•••
User.Read	Delegated	Sign in and read user pr...	-		•••
User.Read.All	Delegated	Read all users' full profil...	Yes	⚠ Not granted for Slashne...	•••

23. Azure will ask you to provide the admin credentials again


Microsoft Azure
Search resources, services, and docs (G+/)
[redacted]
Home > Slashnext Inc - App registrations > SlashNext EMS Application - API permissions
SlashNext EMS Application - API permissions
Sign in to your account
Terms of use
Privacy & cookies
User.Read.All
Delegated
Read all users' full profil...
Yes
Not granted for Slashne...

login.microsoftonline.com/f31b17db-6c7d-41f6-8d19-07eee8606aad/adminconsent?client_id=0d2c7dc8-eb8f-4ad3-a3a3-d9446176e341&login_hint...

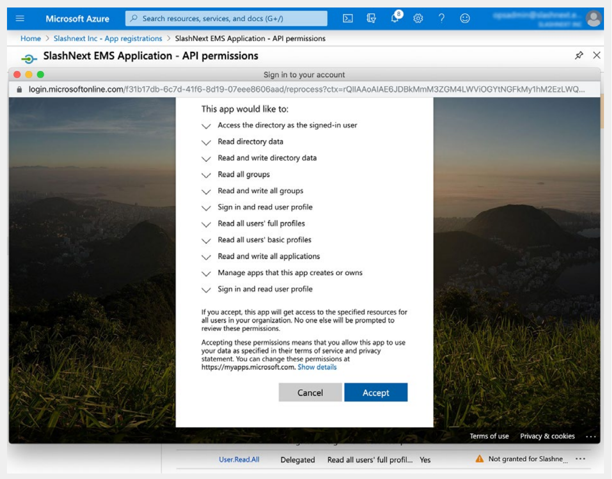
Microsoft

Pick an account

Slashnext Operations
[redacted]
Signed in

Use another account

24. Click on the **Accept** button when prompted to complete the setup


Microsoft Azure
Search resources, services, and docs (G+/)
[redacted]
Home > Slashnext Inc - App registrations > SlashNext EMS Application - API permissions
SlashNext EMS Application - API permissions
Sign in to your account
Terms of use
Privacy & cookies
User.Read.All
Delegated
Read all users' full profil...
Yes
Not granted for Slashne...

login.microsoftonline.com/f31b17db-6c7d-41f6-8d19-07eee8606aad/reprocess?ctx=rQIIAAoAIAE6JDBkMmM3ZGM4LWViOGYtNGFkMy1hM2EzLWQ...

This app would like to:

- Access the directory as the signed-in user
- Read directory data
- Read and write directory data
- Read all groups
- Read and write all groups
- Sign in and read user profile
- Read all users' full profiles
- Read all users' basic profiles
- Read and write all applications
- Manage apps that this app creates or owns
- Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Cancel Accept