

Netradyne IT Offboarding SOP

V2.1

Internal and Confidential

***Table of Contents***

1. [PURPOSE 3](#_bookmark0)
2. [SCOPE 3](#_bookmark1)
3. [ROLES AND RESPONSIBILITIES 3](#_bookmark2)
4. [PROCEDURE 3](#_bookmark3)
   1. [Definitions 3](#_bookmark4)
   2. [Employee Exit Workflow 4](#_bookmark5)
   3. [Roles and Responsibilities 4](#_bookmark6)
   4. [Offboarding Service Level 7](#_bookmark7)
   5. [Account Deactivation 7](#_bookmark8)
      1. [Following is the step-by-step offboarding procedure 8](#_bookmark9)
5. [CONDUCT 16](#_bookmark10)
6. [EXCEPTION 16](#_bookmark11)
7. [TERMS/ACRONYMS 17](#_bookmark12)
8. [REFERENCES................................................................................................................................................](#_TOC_250000)
9. [APPENDIX A: DOCUMENT RACI MATRIX 17](#_bookmark13)

**Document Control**

|  |  |
| --- | --- |
| **Document ID** | NDITP2023001 |
| **Document Name** | Netradyne IT-Offboarding SOP |
| **Document Status** | Released |
| **Document Released Date** | 26-Dec-2024 |
| **Document Author** | Priyesh Parashar |
| **Document Content Contributors** | Chethan Gangaraju |
| **Document Signatory** | Saravanan Sankaran |
| **Document Owner** | Priyesh Parashar |
| **Document Version** | V2.1 |
| **Information Classification** | Internal |

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised By** |
| v1.0 | 20-Mar-2023 | Initial Version Created | Ramesh Babu |
| V2.0 | 4-Oct-2024 | SOP for IT Offboarding for India & US employees | Priyesh Parashar |
| V2.1 | 20-Jun-2025 | Annual Revision | Priyesh Parashar |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Signatory Title** | **Comments** |
| 26-Dec-2024 | Saravanan Sankaran | Senior Director, Infosec & IT | Approved |
| 24-Jun-2025 | Saravanan Sankaran | VP, Infosec & IT | Approved |
|  |  |  |  |

**Distribution of Final Document**

|  |  |
| --- | --- |
| **Name** | **Organization/Title** |
| IT & Infosec | Netradyne |
|  |  |
|  |  |

# Purpose

The purpose of this SOP is to provide a standardized process for offboarding employees from the IT systems and infrastructure of Netradyne. This ensures company data security, sensitive information protection, and a smooth transition for departing employees. This document provides the standard procedure for IT offboarding when employees exit the company.

# Scope

This SOP applies to all employees, interns and contractors who are exiting the organization, whether through resignation, termination, or other means. It covers all the necessary steps and considerations for disabling accounts, retrieving company equipment, and managing access rights.

|  |  |
| --- | --- |
| **Intended Audience:** | IT Team & Infosec Team |
| **Owned By Department:** | IT |
| **Managed By Department:** | IT |
| **Control Implementer:** | IT |
| **Control Operator:** | IT & Infosec |
| **Control Governance:** | Infosec |
| **Offboarding Initiator:** | HR Team |
| **Access Deprovisioning Team:** | IT |

# Roles and Responsibilities

Roles and responsibilities specific to this document are included below:

|  |  |
| --- | --- |
| ***Role*** | ***Responsibilities*** |
| Owner | * Team or SME responsible for the process area needs to ensure this document is up to date and compliant with governing requirements. * Is the point of contact for the document. * Responsible for initiating and managing document review and the approval process from start to finish including gathering or delegating the collection of content including diagrams, formatting etc. as well as identifying stakeholders to participate in the peer review process. |
| Reviewers/Stakeholders | Representations from teams that can affect or be affected by the document under review (e.g., Operation, Security, Compliance, Quality) |
| Approvers | The Person(s) of authority to validate the document and sign-off on the latest version. Such Person include Document owner, Functional Team Lead, Security Lead, Product Delivery Lead. |
| Document Release | Document Owner/team to work with repository administrator to make release version available. |

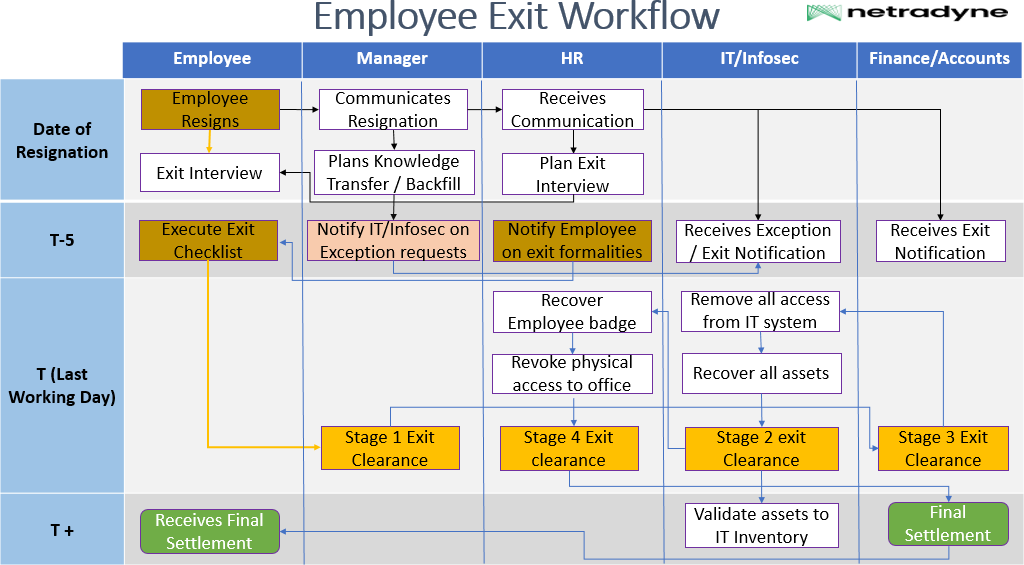
# Procedure

The offboarding process includes access deprovisioning like email accounts, network access, and software permissions. This procedure ensures that user hand over computers, phones, and other company devices back to the IT team during the offboarding process

### Definitions

* Offboarding: The process of employee exit from the organization.
* Access Control: Security measures that regulate the deactivation of access, ensuring that only authorized personnel can manage resources within the computing environment.
* IT Assets: The offboarding process ensures the secure return and management of hardware, software, and network resources owned by the organization, safeguarding company assets during the employee's departure.

### Employee Exit Workflow

****

### Roles and Responsibilities

This matrix helps clarify roles and responsibilities in the onboarding process, ensuring efficient coordination and accountability.

* **R** = Responsible: The person or role responsible for completing the task.
* **A** = Accountable: The person or role ultimately accountable for the task. This person has the final authority and responsibility.
* **C** = Consulted: The person or role consulted for input or feedback before the task is completed.
* **I** = Informed: The person or role who must be informed of the task's progress or completion.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Task/Team** | **HR**  **Team** | **Manager** | **IT**  **Team** | **Infosec Team** | **IT Asset Manager** | **Facility Team** |
| **Offboarding Request Creation** | R | A | I | I | I | I |
| **Access Revocation** | C | A | R | C | I | - |
| **CrowdStrike Removal** | I | A | R | C | I | - |
| **Endpoint Central Removal** | I | A | R | C | I | - |
| **Email Access/Forwarding** | A | A | R | C | I | - |
| **Data Backup/Transfer** | C | A | R | I | I |  |
| **Asset Recovery** | C | A | R | I | C | - |
| **Security Audit** | I | A | C | R | I | - |
| **ID Card Recovery** | I | I | - | - | - | R/A |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Completion Notification** | I | R/A | I | I | I | - |

### Offboarding Workflow (Detailed Steps)

* + - 1. **Initiation of Offboarding Request**
         * **Responsible Party**: HR Team
         * **Action**: HR creates an offboarding request in ServiceDesk+ (SD+), specifying the type of offboarding (Standard or Emergency) and email forwarding requirements. For any standard offboarding, an SD+ request must be raised at least 5 days prior to the offboarding date, while for emergency offboarding, the request can be raised on the same day.

## **Subject**: Offboarding ticket should follow below format

**Employee IT Offboarding: Employee Name (Offboarding Date)**

* + - * + **SLA:** IT must respond within 24 hours (standard) or 12 hours (emergency).
        + **ServiceDesk+ Template:** [Employee Exit Request](https://itservicedesk.netradyne.com/app/itdesk/ui/requests/add?reqTemplate=155142000001142157)
        + **Manager Offboarding:** If a manager is being offboarded, the HR team is required to provide the details of the new manager who will be mapped in the system to ensure a smooth transition.

### Access Revocation

* + - * + **Responsible Party**: IT Team
        + **Action**: IT revokes access to all systems, including:

**Accounts Disabled**: Email, VPN, ERP, CRM, financial software, and third-party applications.

* + - * + **SLA**: Must be completed within 12 hours (emergency) or 5 days (standard).
        + **Password Reset:** All passwords related to departing employee’s accounts, including shared and privileged credentials, will be reset or revoked to ensure security and prevent unauthorized access.
        + **Application List:** [Netradyne IT User Profiling](https://netorg726775.sharepoint.com/sites/netradynenet/IT%20Policies/Forms/AllItems.aspx?id=%2Fsites%2Fnetradynenet%2FIT%20Policies%2FNetradyne%20IT%20User%20Profiling%2Epdf&parent=%2Fsites%2Fnetradynenet%2FIT%20Policies)

### CrowdStrike Removal

* + - * + **Responsible Party**: IT Team
        + **Action**: Remove CrowdStrike from the employee's devices (once IT team has received the device) and validate the removal in the CrowdStrike portal to ensure all security endpoints are properly cleared.
        + **Note** - Please ensure that laptops for exit employees are either formatted or, if the manager/HR has requested to retain the laptop, Endpoint Central should be manually removed from the device.

### Endpoint Central Removal

* + - * + **Responsible Party**: IT Team
        + **Action**: Remove Endpoint Central from the employee’s devices (once IT team has received the device) and validate the status in the Endpoint Central portal.
        + **Validation**: IT Asset Manager must validate the status of the device in SD+ for accurate record-keeping.
        + **Note** - Please ensure that laptops for exit employees are either formatted or, if the manager/HR has requested to retain the laptop, Endpoint Central should be manually removed from the device.

### Email Access/Forwarding Setup

* + - * + **Responsible Party**: IT Team
        + **Action**: For any mailbox forwarding or access, the manager must submit a mailbox request. This request will first be reviewed and approved by the HR Manager, and then sent to the Infosec team for final approval.
        + **IT Team:** To setup the reminder in SD+ to revoke email forwarding or mailbox access post completion to the given duration. Also, please ensure that all meeting invites scheduled by the exiting employee are cancelled, and if the mailbox remains active, set up an out-of-office message to inform senders.

**Note:** Thank you for your email. Please note that this mailbox is no longer being monitored. For any urgent matters or assistance, kindly reach out to “**manager email** [**ID@netradyne.com**](mailto:ID@netradyne.com)***”***

* + - * + **ServiceDesk+ Template:** [Request for Mailbox Delegation](https://itservicedesk.netradyne.com/app/itdesk/ui/requests/add?reqTemplate=155142000001536009)

**Note** – Ensure that the '**Office Location**' and '**Manager**' fields are cleared for any O365 user account that has been disabled but has email forwarding enabled.

* + - * + **Account Deletion:** The O365 account will be retained for two working weeks post-offboarding. If the HR or manager misses submitting an email forwarding request during the offboarding process, the request can still be raised within this two-week retention period. If the IT team does not receive any notification within this timeframe, the account will be permanently deleted.

**Note** – Follow the steps below for email forwarding.

### Email Forwarding Setup

* + HR/Manager raises a request; IT sets up email forwarding to the appropriate manager for 30 days.

### Forwarding Review

* + HR contacts the manager at the end of the forwarding period to decide next steps:
    - **If continued access is required**: HR requests, IT to extend forwarding for an additional 30 days.
    - **If not required**: HR requests, IT to create a PST file.

### PST File Creation

* + IT generates the PST file and saves it in the **HR Confidential** folder, provided by HR.

### PST File Retention

* + PST files are retained in the HR Confidential folder for **five years**.
  + After five years, HR approves secure deletion of the files.

### Folder Management

* + HR maintains the **HR Confidential** folder with proper access and security measures.

### Data Backup and Transfer

* + - * + **Responsible Party**: IT Team
        + **Action**: Before deactivating employee accounts, all critical data and files will be securely backed up and transferred to ensure business continuity and prevent any potential data loss if it is requested by HR or employee’s manager.

### Asset Recovery

* + - * + **Responsible Party**: IT Support / Asset Management Team
        + **Action**: The IT department will collaborate with HR to manage the return process and ensure that all company assets are accounted for and properly returned. Recover all company assets (laptops, phones, tokens) and ensure devices are wiped and reconfigured. IT Asset Manager must validate the recovery in SD+.

### Security and Audit Check

* + - * + **Responsible Party**: Infosec Team
        + **Action**: Audit the employee’s accounts and access logs, ensuring complete

access revocation.

### Completion Notification

* + - * + **Responsible Party**: Manager
        + **Action**: After all steps are completed, notify HR and Department Head and ensure proper documentation in SD+.

### Offboarding Service Level

* + 1. **Standard Offboarding**

This applies to regular resignations or planned exits, where IT has 24 hours to respond and 5 days to complete the offboarding process.

|  |  |
| --- | --- |
| **Standard Offboarding SLA Type** | **SLA Duration** |
| Response | 24 business hours |
| Resolution | 5 business days |

### Emergency Offboarding

This applies to terminations or urgent situations requiring immediate access revocation. IT must respond within 12 hours and complete offboarding within 24 hours.

|  |  |
| --- | --- |
| **Emergency Offboarding SLA Type** | **SLA Duration** |
| Response | 12 business hours |
| Resolution | 24 business hours |

### Account Deactivation

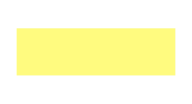
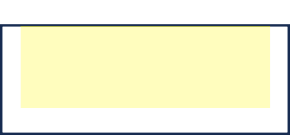
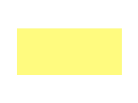
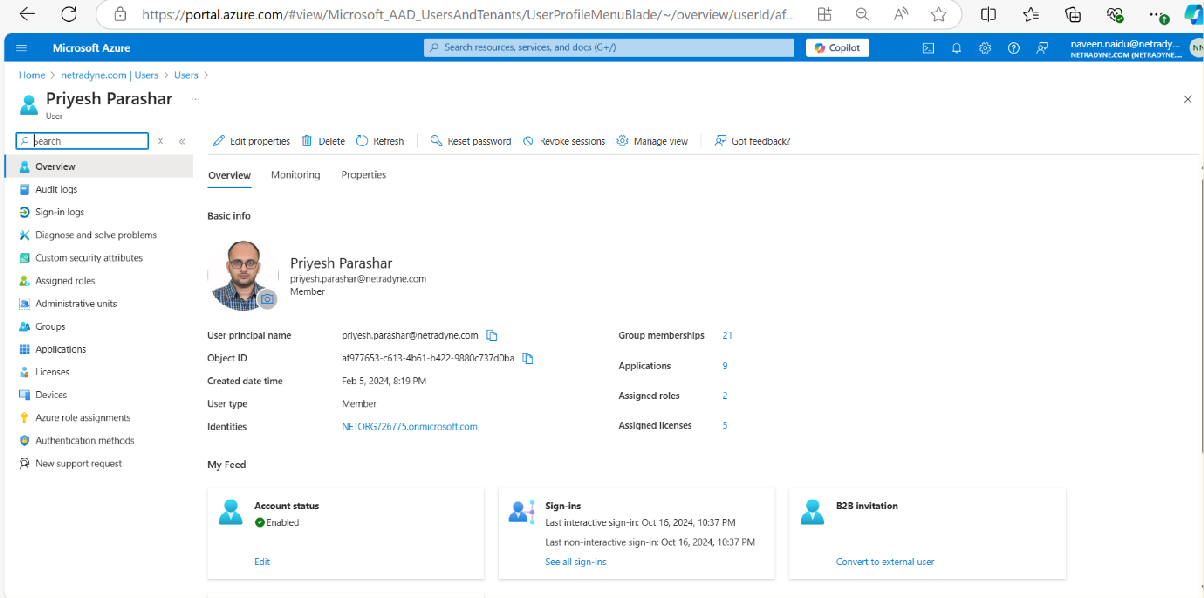
Upon receiving SD+ ticket from HR, the IT department will promptly deactivate the departing employee's user accounts, including email, network access, system logins, and any other relevant accounts.

### Following is the step-by-step offboarding procedure.

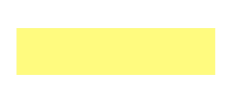
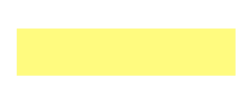
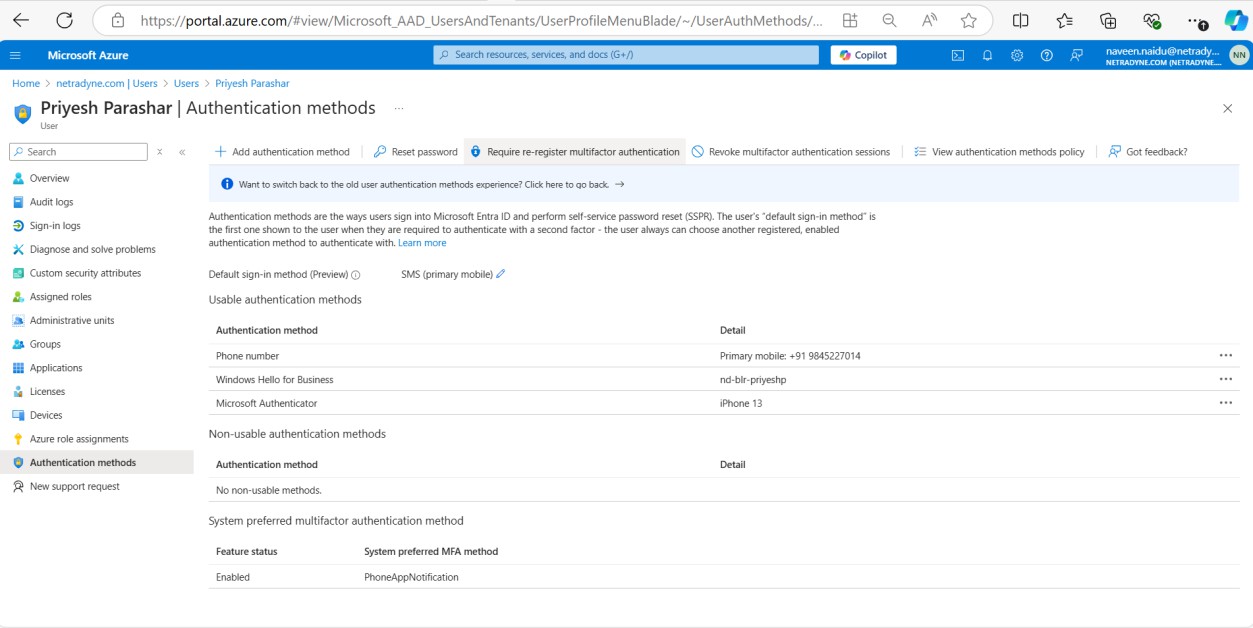
*Azure ID Deactivation:*

## Login - [Azure - Users](https://portal.azure.com/%23view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/~/AllUsers)

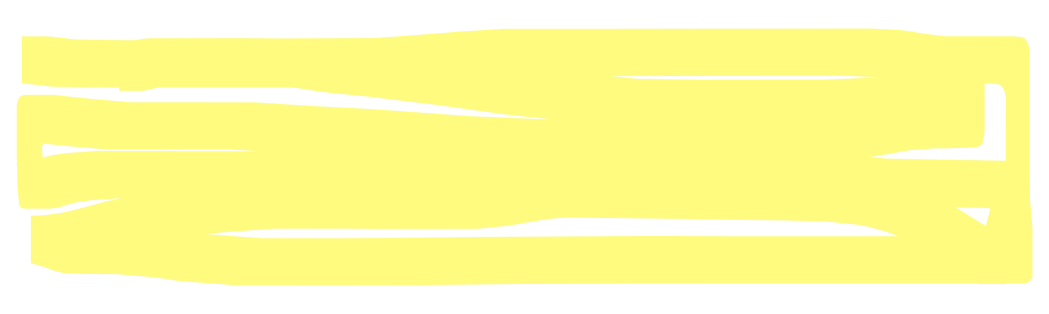
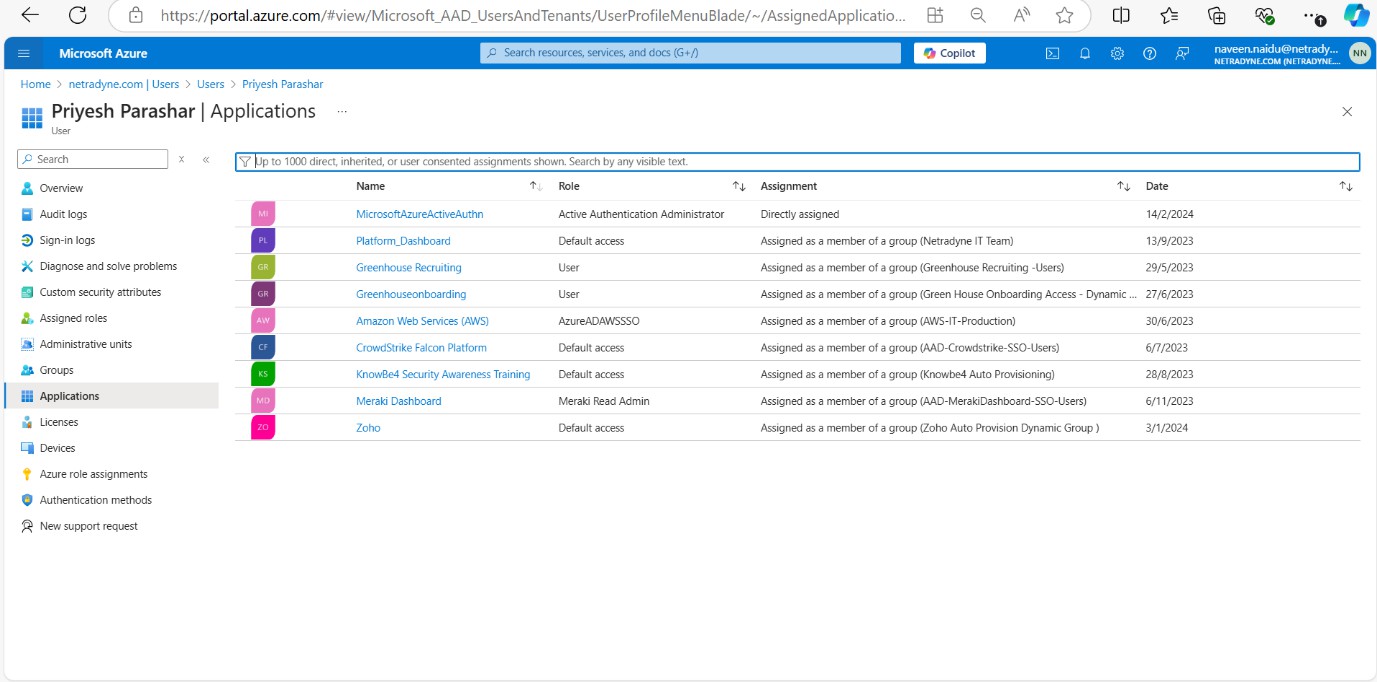
* + - 1. Search User in the tab
      2. Revoke all sessions
      3. Disable account status
      4. Remove manager while disabling the account



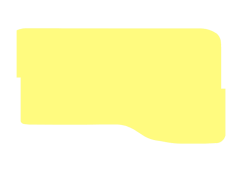
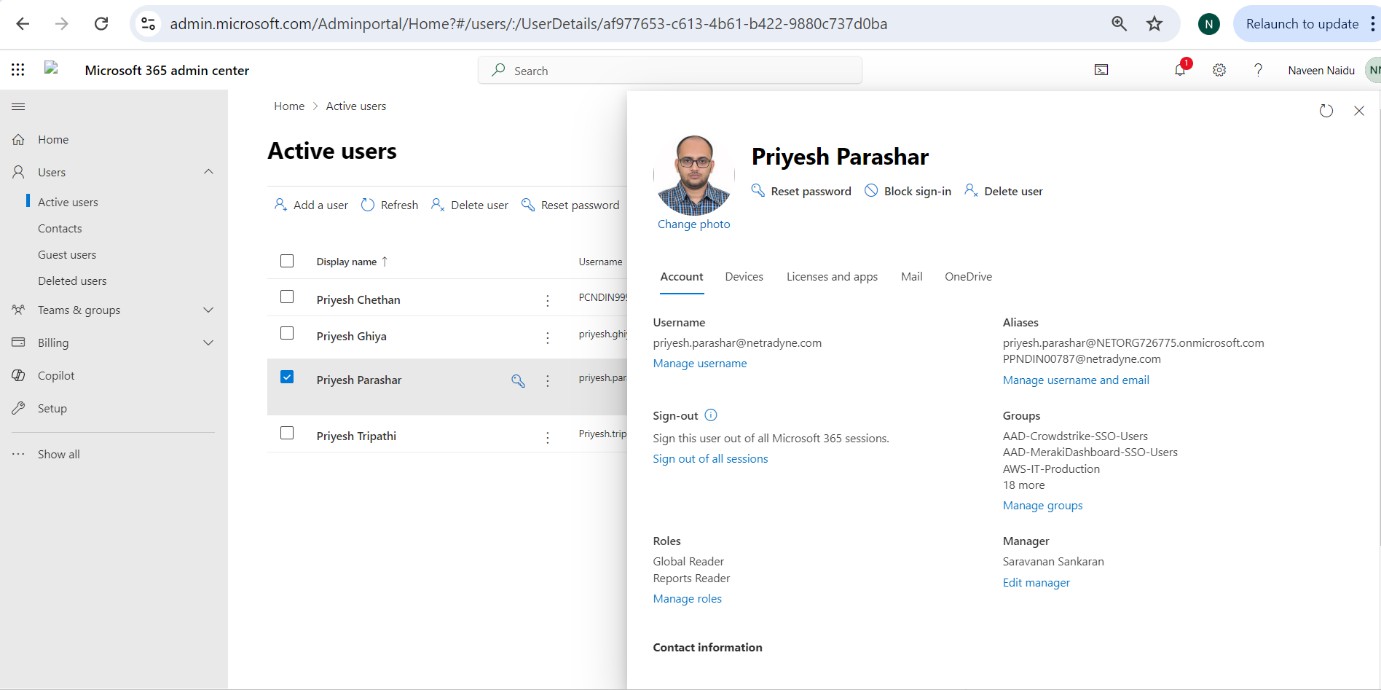
* + - 1. Go to “Authentication methods” and “revoke multifactor authentication sessions”



* + - 1. Remove application access

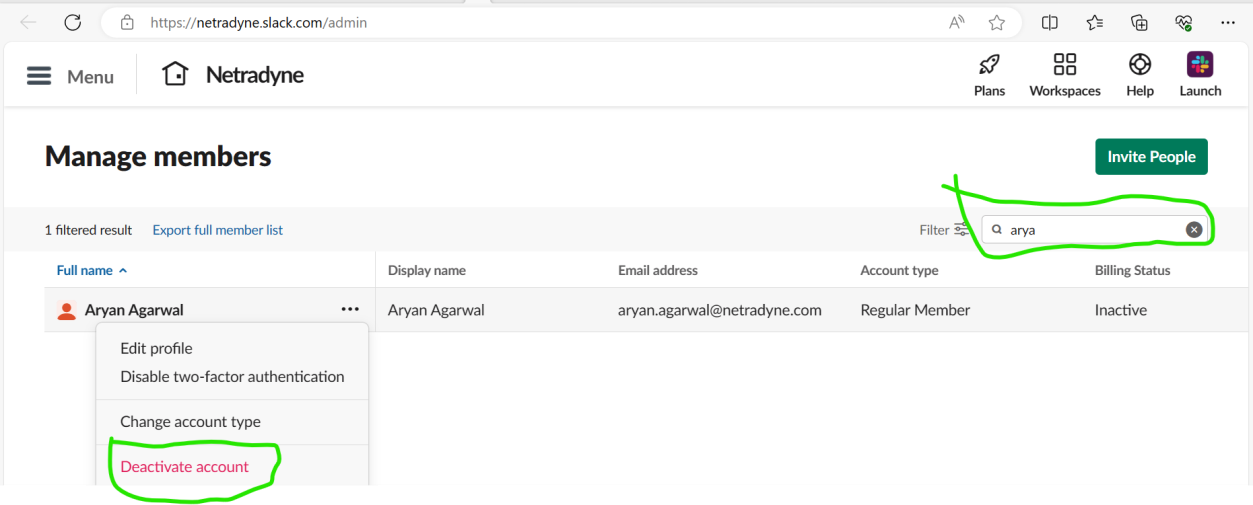


* + - 1. Go to Admin portal - [https://admin.microsoft.com/Adminportal/Home?#/users](https://admin.microsoft.com/Adminportal/Home?&/users)
      2. Search User in the tab
      3. Go to “Manage groups”
      4. Select all groups and click on “Remove”



*Slack Deactivation:*

Login to slack [https://netradyne.slack.com](https://netradyne.slack.com/) and select Manage Members and filter by exit username and click the deactivate.



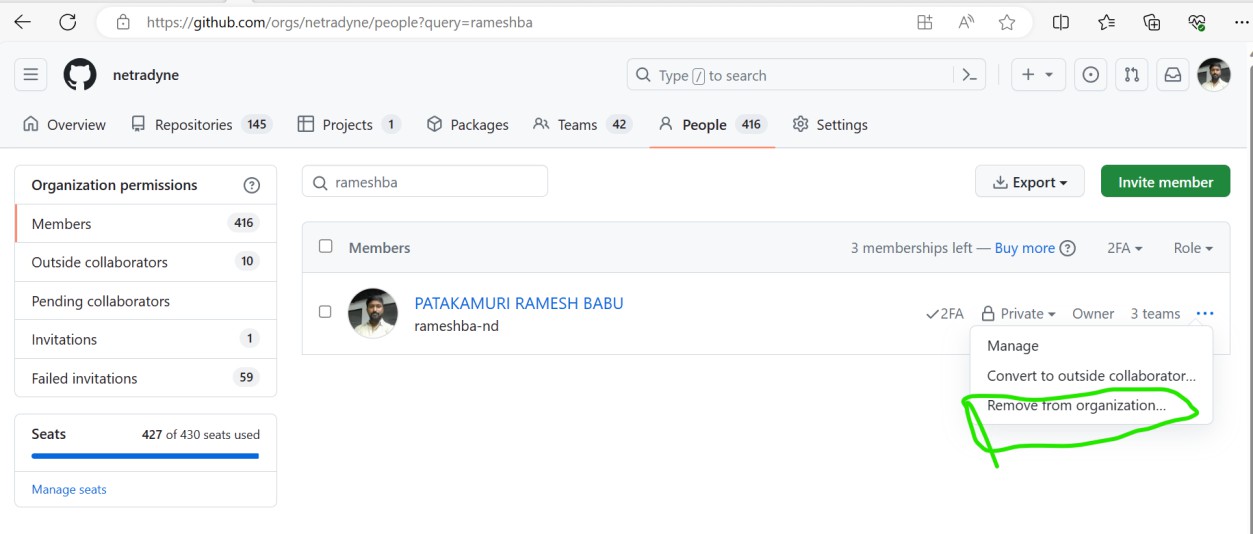
*Jira Access Deactivation:*

Login to Jira [https://admin.atlassian.com](https://admin.atlassian.com/). Under user management select the users and filter by exit employee name. Remove the license and user from organization.



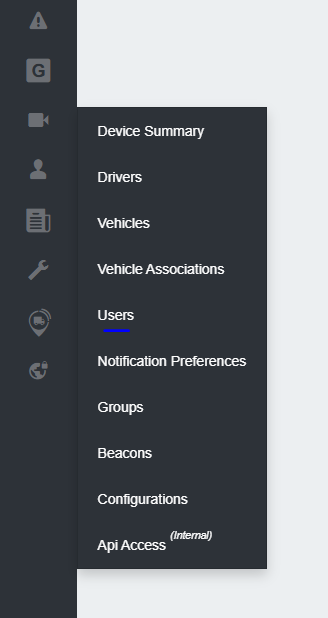
*GitHub Deactivation:*

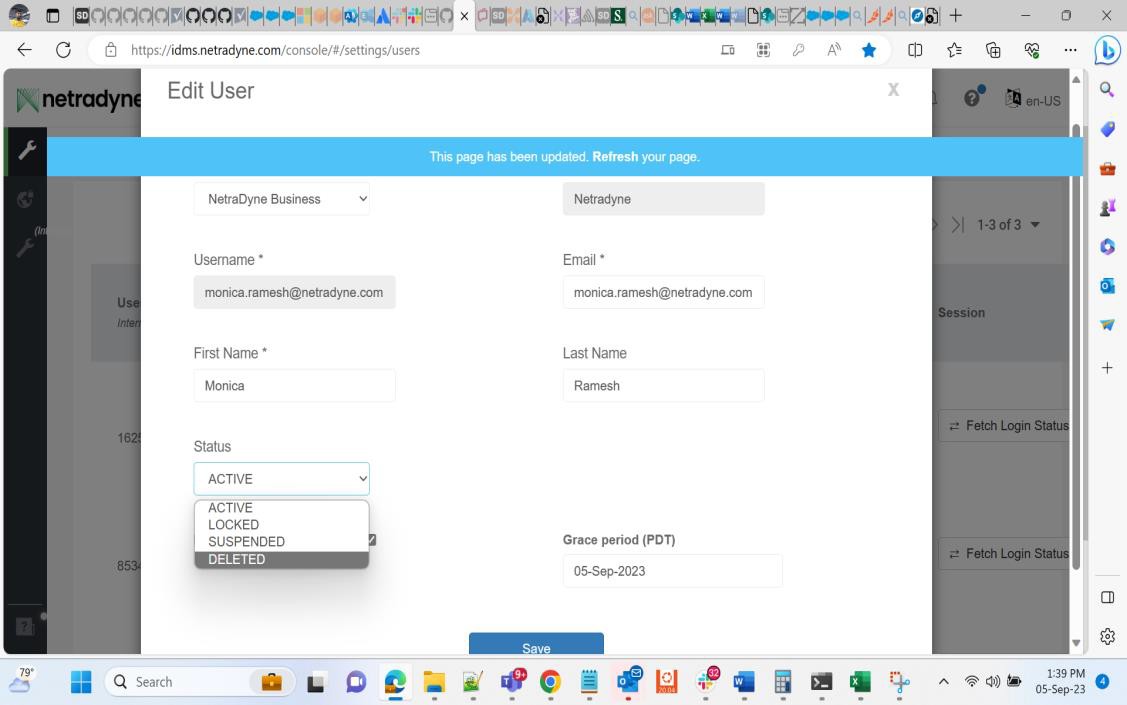
Login to GitHub [NetraDyne (github.com)](https://github.com/netradyne). Select people and filter by exit employee name and click on remove from organization.



*IDMS PROD & Stagging Access delete:*

1. Login to IDMS Prod & Stagging [Netradyne Driveri™](https://idms.netradyne.com/console/%23/settings/users) & [idms-testing.netradyne.com](https://idms-testing.netradyne.com/console/%23/resetpassword?token=0f1fc1e2-9279-4497-a553-3205b7b1bd7e).
2. Click on settings icon.
3. Search for the exit employee's name.
4. In the "Status" column, click the dropdown menu and select "Delete."



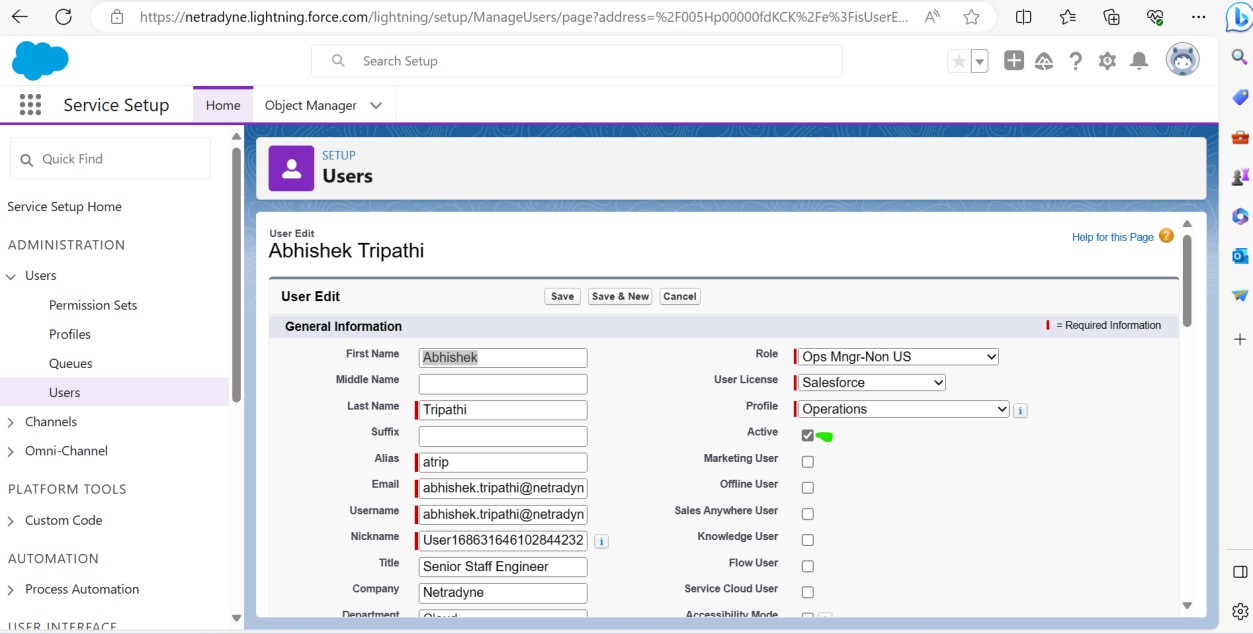


*AWS Access Delete:*

The AWS access is integrated with Single Sign-On (SSO), so once we remove access to Office 365, the exit employee will no longer be able to access it.

*Salesforce Access Deactivation:*

1. Login to salesforce [https://netradyne.lightning.force.com](https://netradyne.lightning.force.com/)
2. Navigate to "Users" and locate the user by their username.
3. Click on "Edit," and uncheck the "Active" icon to deactivate the user's access.



Note – Please follow below steps for any termination.

### Automate Role Setting on Termination:

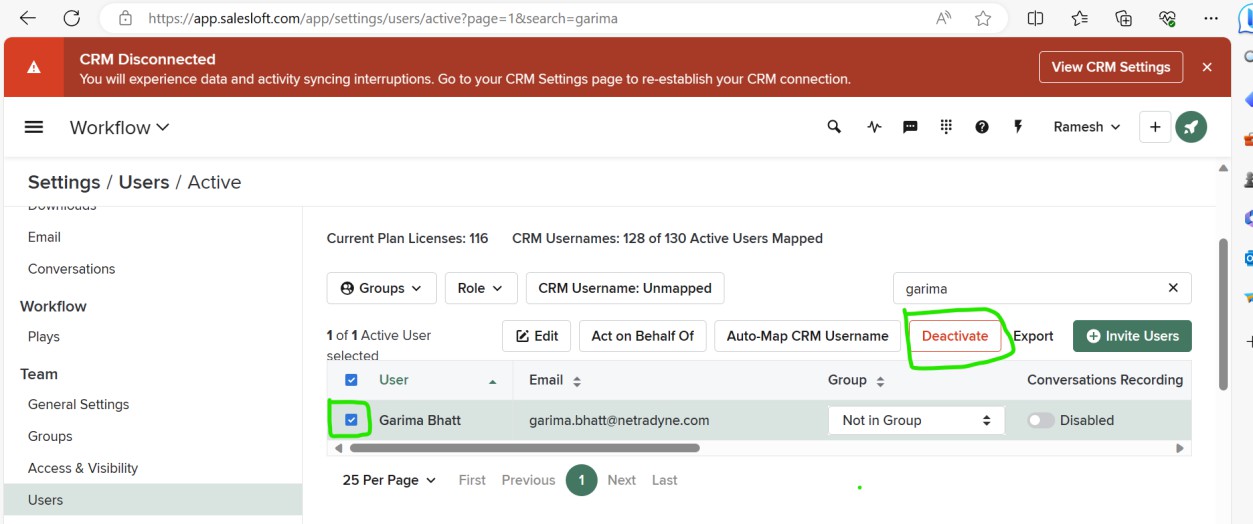
* + When users are terminated or leave, their Role should be set to "Inactive."
  + This will ensure that if they return as active users, they must update their Role.

### Expected Outcome:

* + All deactivated users should have their Role set to "Inactive," before they are marked inactive.

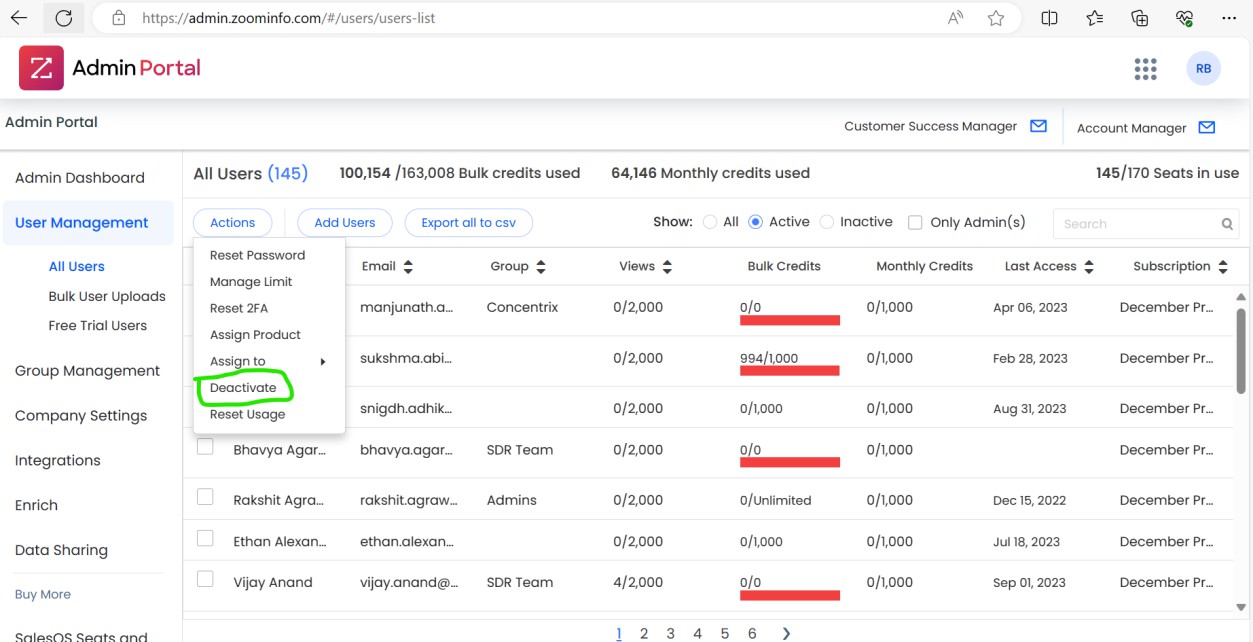
*SalesLoft Deactivation:*

1. Login to SalesLoft [https://app.salesloft.com](https://app.salesloft.com/)
2. Navigate to "Users" and locate the user by their username.
3. Select the user and click on “Deactivate”.



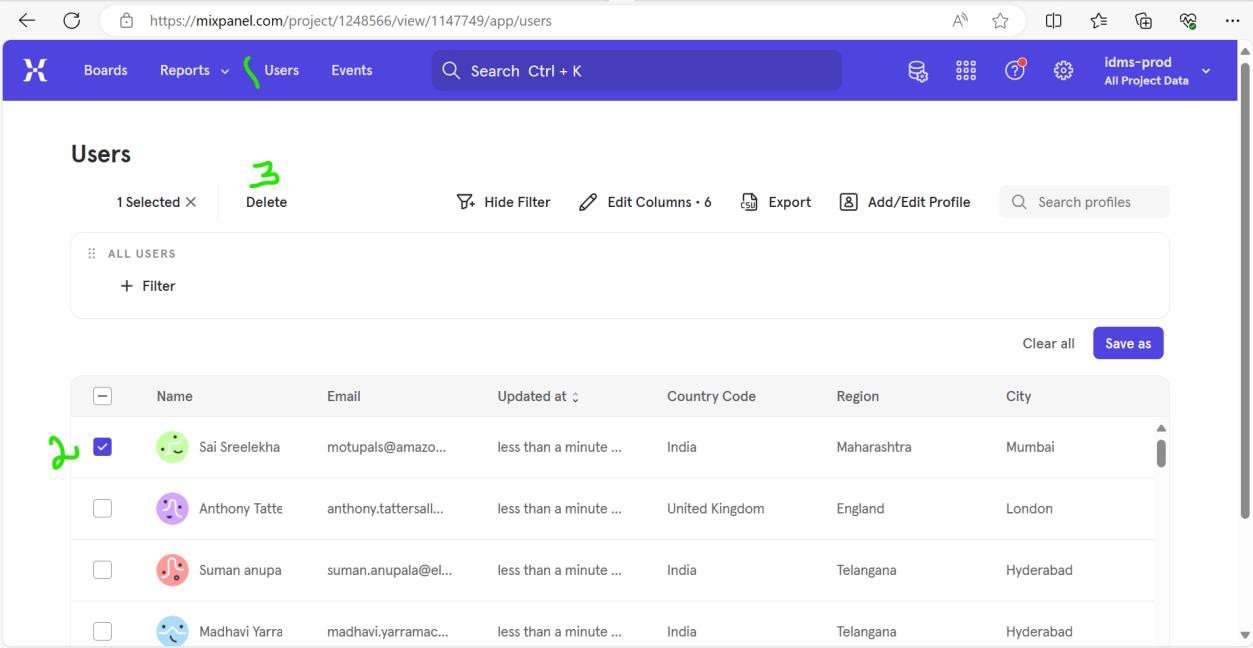
*ZoomInfo Deactivation:*

1. Login to Z admin portal [https://admin.zoominfo.com](https://admin.zoominfo.com/).
2. Navigate to user management and select “All users”
3. Select the user and click on “Actions” and select “Deactivate”.



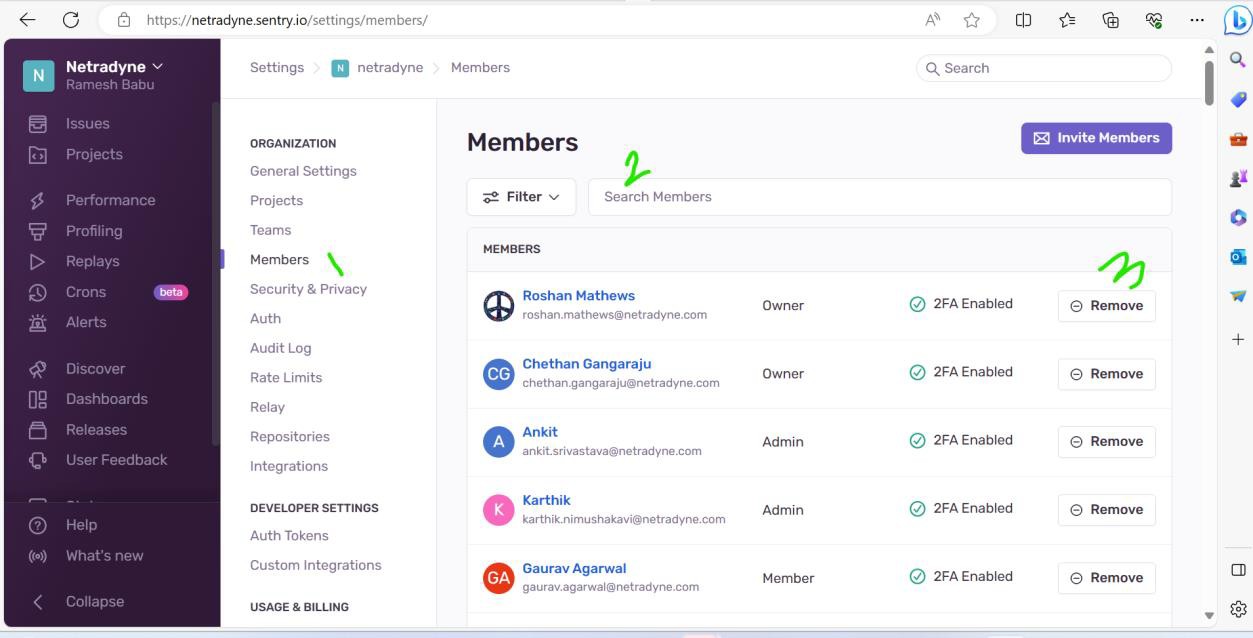
*Mixpanel Deactivation:*

1. Login to [https://mixpanel.com](https://mixpanel.com/)
2. Navigate to "Users" and locate the user by their username.
3. Click on Delete.



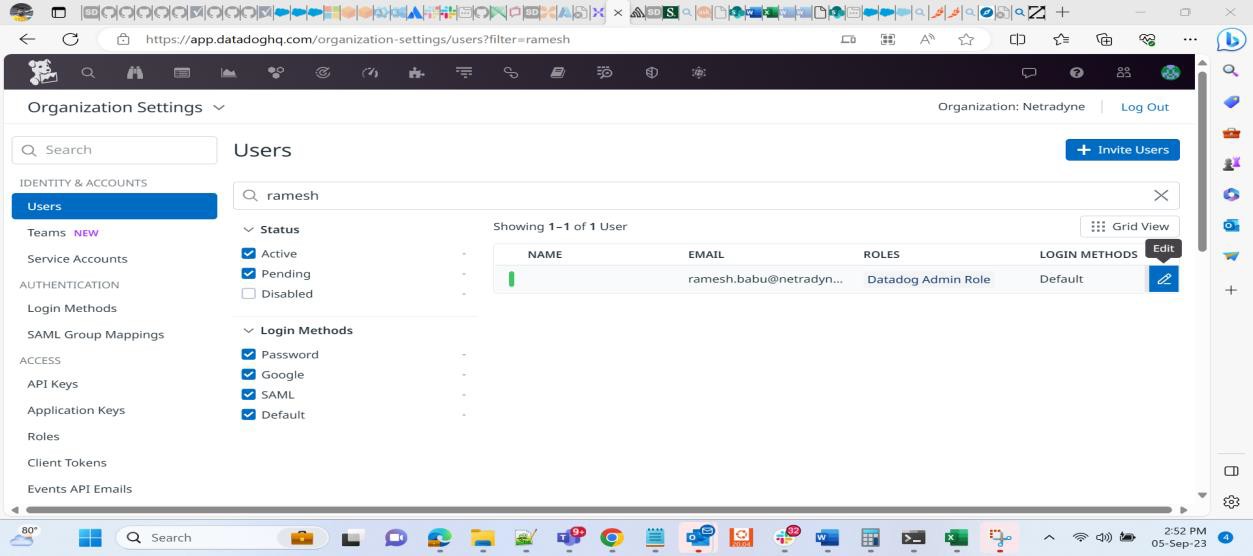
*Sentry Access Deactivation:*

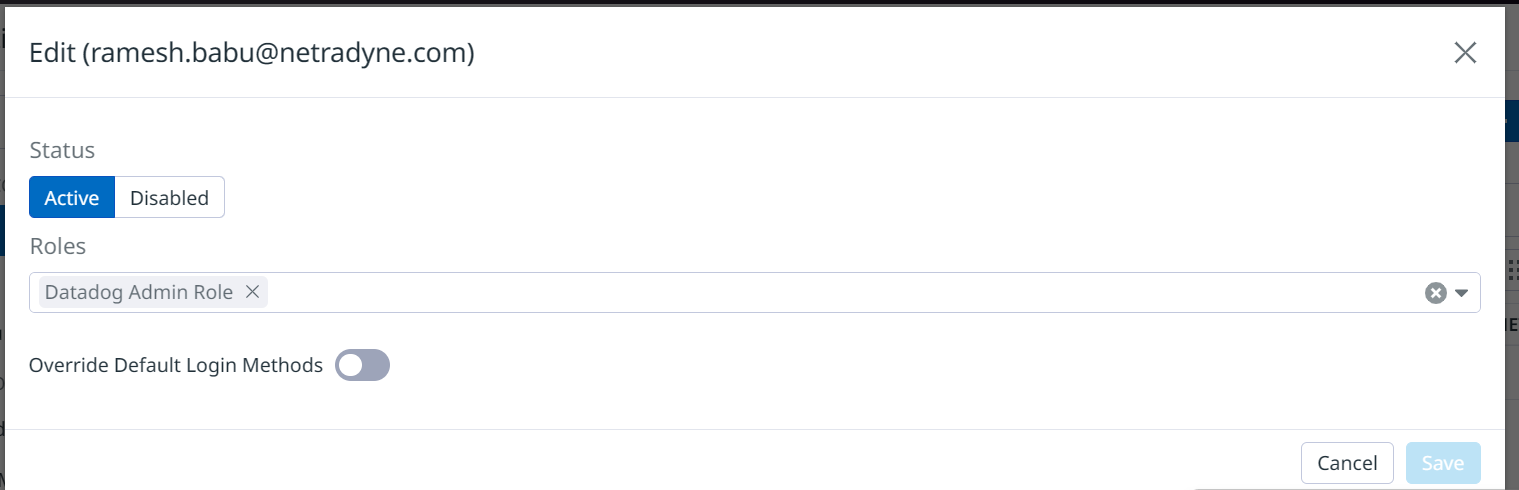
1. Login to sentry https://netradyne.sentry.io
2. Navigate to Members and search by username.
3. Click on “Remove”.



*Datadog Access Deactivation:*

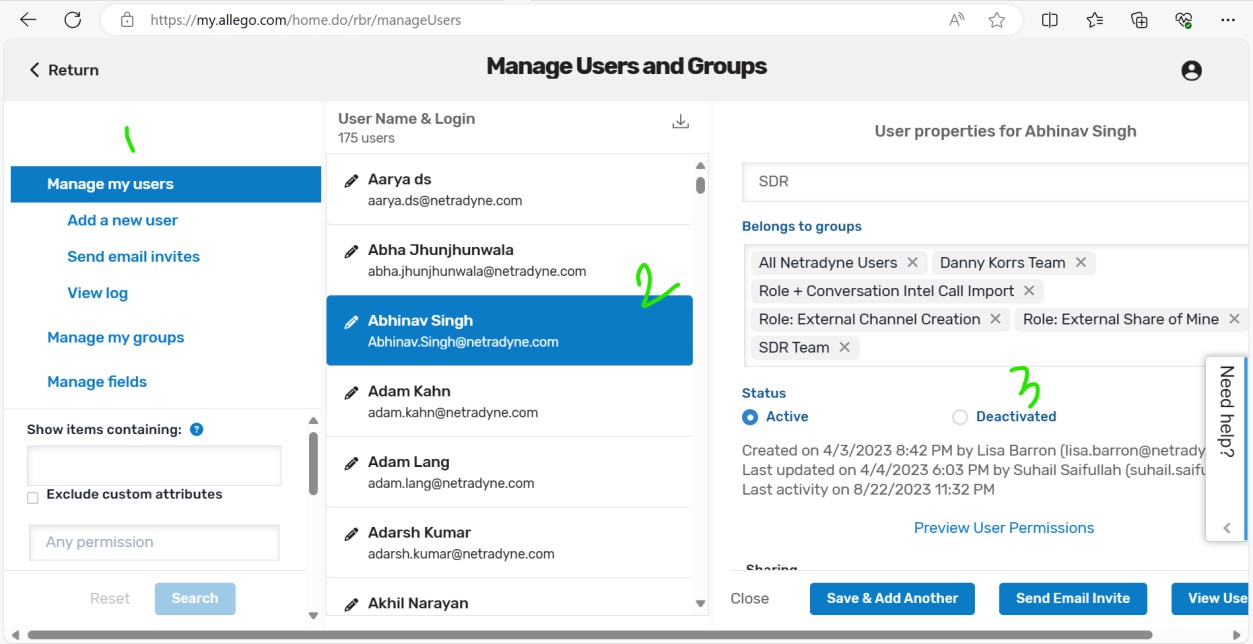
1. Login to Datadog [https://app.datadoghq.com](https://app.datadoghq.com/)
2. Navigate to "Users" and search the user by their username.
3. Click on edit and select the Disable.





*Allego Access Deactivation:*

1. Login to Allego [https://my.allego.com](https://my.allego.com/)
2. Navigate to Manage my user and select the username.
3. Click on “Deactivated”.



*Cisco AnyConnect*

The Cisco AnyConnect is integrated with Single Sign-On (SSO), so once we remove access to Office 365 and groups, the exit employee will no longer be able to access it.

*Knowbe4*

The Knowbe4 is integrated with Single Sign-On (SSO), so once we remove access to Office 365 and groups, the exit employee will no longer be able to access it.

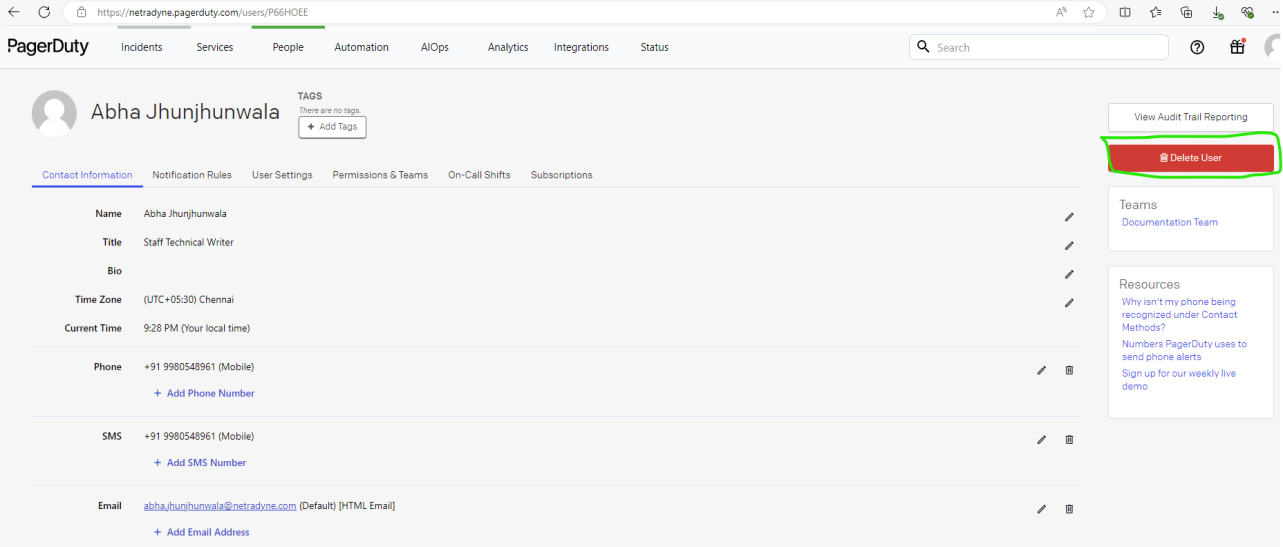
*Zoho*

The Zoho is integrated with Single Sign-On (SSO), so once we remove access to Office 365 and groups, the exit employee will no longer be able to access it.

*PagerDuty*

The PagerDuty access needs to be removed.

1. Log in to PagerDuty at [https://netradyne.pagerduty.com](https://netradyne.pagerduty.com/) or via [My Apps](https://myapplications.microsoft.com/).
2. Once logged in, click on People in the navigation menu and select the users.
3. Click on the exiting employee's name to open their profile.
4. Select the Delete option to remove their account.
5. Verify the user has been successfully deleted.



# Conduct

Compliance Checks to this process to be performed through various methods, including but not limited to reports, internal/external audits, Awareness training/assessments and feedback to the process owner. Non-compliance will be escalated to the Netradyne leadership team.

# Exception

IT Team is authorized to grant exceptions to the requirements set forth in this document. Any exception granted will require a thorough review of the situation and the implementation of appropriate compensating controls followed by ND Information Security Exception process.

# Terms/Acronyms

|  |  |
| --- | --- |
| **Term/Acronym** | **Definition** |
| IT | Information & Technology |
| Infosec | Information Security |

# References

### Templates

*Netradyne IT User Profiling* [*Netradyne Asset Acknowledgement*](https://forms.office.com/Pages/ResponsePage.aspx?id=miFPuM0P-k2Edu3MlvMyTBgDbLh02jpGjnqJczL4a2VUNzhXUUFXVzFBVkVESTVIVEpGOEpXWVBDOC4u)[*Onboarding Assistance*](https://netorg726775.sharepoint.com/sites/IT/SitePages/Onboarding-Assistance-(Netradyne-Employees).aspx)

*Employee\_Offboarding\_workflow\_updated.pptx*

### Policies

*Netradyne Information Security Policy & Procedure.pdf Netradyne Information Security Exception Process.pdf IT Guidelines for Software Purchases.pdf*

*Netradyne Acceptable Usage Policy.pdf Netradyne Change Management.pdf Netradyne Incident Management.pdf*

*Netradyne Information Technology Policy and Procedure.pdf Netradyne IT Asset Policy.pdf*

*Netradyne IT Asset Policy.pdf Netradyne Problem Management.pdf NetradyneOpen-SourceSecurityPolicy.pdf*

### Process/Procedures

*NETRADYNE DISASTER RECOVERY PROCESS.pdf NETRADYNE BUSINESS CONTINUITY PLAN.pdf*

*Netradyne Vulnerability & Patch Management Process.pdf NetradyneSecurityIncidentResponsePlan.pdf*

*Netradyne-Access\_Control\_matrix.xlsx*

# Appendix A: Document RACI Matrix

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Role/Activity** | **Document**  **Owner/Functional Area Lead** | **Document Contributor** | **ND**  **Leadership** | **Functional**  **Area Team** | **InfoSec** | **All ND Member(s)** |
| **Ensure**  **document is kept current** | A | R | I, C | R, C | C | I |
| **Ensure stakeholders are kept informed** | A | R | - | R | C | - |
| **Ensure document contains all** | A | R | I, C | R, C | C | I |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **relevant information** | |  | |  |  |  |  |  |
| **Ensure document adheres to document governance**  **policy** | | A, R | | R | I | R, C | R, C | I |
| **Provide SME advice** | | I, R | | A, R | I | R, C | I, C | I |
| **Gathering and adding document contents** | | I | | A, R | I, C | R, C | C | I |
| **Document Approval** | | A | | R | I, R | I | I, R | I |
| *Key* | | | | | | | | |
| *R* | Responsible | |  | | | | | |
| *A* | Accountable | |
| *C* | Consulted | |
| *I* | Informed | |