

# NEMSIS OKTA Account Policy

---

## Date

December 18, 2020

June 30, 2022 (updated)

December 5, 2022 (updated)

March 16, 2023 (updated)

August 3, 2023 (updated)

April 22, 2024 (updated)

## Overview

The NEMSIS Technical Assistance Center (TAC) formerly used Active Directory (AD) User Accounts to provide EMS stakeholders secure access to data that has been restricted from the public in reports and dashboards. The NEMSIS system migrated to the AWS cloud in May 2023, and AD accounts were migrated to Okta accounts in compliance with new security standards.

Access to restricted data is closely monitored for security and to honor restriction requests from States/Territories and for business purposes of EMS Software Vendors.

Individuals that completed the setup for the Okta accounts, will have the appropriate access to the NEMSIS reports and resources.

Individuals that did not receive an email confirmation from Okta and previously had a user account will need to request a new Okta account by submitting a [helpdesk](#) ticket. Please see the [NEMSIS AWS User Guide – OKTA](#) for set up instructions.

## Types of User Accounts

NEMSIS Okta Accounts offer four types of access:

1. State/Territory Data Manager
2. State/Territory (Restricted User)
3. EMS Software Vendor
4. National

## State/Territory Data Manager Okta Accounts

The purpose of the State/Territory Okta Account is to provide state officials with access to informative and dynamic state-specific dashboards that have been restricted to the public. The state's EMS data are used to produce dashboards and reports which provide details about submissions, data quality, geographic identifiers, and responding agency information. This restriction is currently specified in Data Use Agreements with the States/Territories.

The NEMSIS TAC allows each State/Territory Office of EMS four Okta Accounts. The State Manager-level Okta Accounts are primarily designated for the EMS Data Manager, EMS Director, EMS Medical Director,

and EMSC Program Manager. The EMS Data Manager may request the creation of an account for alternate staff if the state has not utilized all the accounts reserved for state directors and managers.

There are occasions when an EMS Data Manager may need to request additional accounts for staff members to access the state-level data. The TAC will review and manage each request individually. These accounts may be created temporarily with the goal of securing the data and equitably managing the number of Okta Accounts per state.

## **EMS Software Vendor Okta & Service Accounts**

The TAC provides NEMSIS-compliant EMS Software Vendors four Okta Accounts. These accounts permit the user to view tools and reports specific to their customers' submission of data.

Software vendors also utilize Okta Service accounts which are used for compliance testing and data submission via web services.

Some vendors will only use their Okta accounts during compliance testing and may need to reset the account after periods of inactivity. *(See Inactive user Accounts below)*

## **National Okta Accounts**

The TAC provides access to all State/Territory and EMS Software Vendor data to the NEMSIS program sponsor, NHTSA's Office of EMS. NHTSA may also authorize restricted access to other Federal agencies on a case by case basis with clear instruction on which data are allowed to be published and which are restricted for official use only.

## **Requesting an Okta Account**

Stakeholders may request access to restricted data by completing the form here: <https://nemsis.org/request-a-nemsis-account/> or by submitting a help desk ticket here: <https://nemsis.atlassian.net/servicedesk/customer/portals>.

The TAC will validate if the requestor is authorized to access data by the State/Territory Office of EMS or the primary vendor account representative, whichever is applicable to the request.

## **Management of Okta Accounts**

If a State/Territory has more than four active Okta Accounts, a list of all active accounts will be provided to the EMS Data Manager to confirm which accounts should remain open.

The TAC is proactive in managing the accounts, but it is the responsibility of the State/Territory Data Manager or EMS Software Vendor to notify the TAC when an Okta Account needs to be deactivated due to staffing changes.

## Inactive Okta Accounts

As a security measure all Okta Accounts which have not had a log in within a 6-month period are disabled.

### +6 months of inactivity

If the Okta Account is inactive for more than six months, the account will be deactivated *without notification* and the password reset link will not work for the account. The account can be reactivated by submitting a help desk ticket here: <https://nemsis.atlassian.net/servicedesk/customer/portals>. Select General NEMSIS Questions.

## Password Reset

All Okta Account Users will have to reset their passwords every 60 days. If the Okta Account has been active within the last six months, the User can reset their password here: <https://login.nemsis.org>

If the Okta Account has not been accessed within six months the password reset option will no longer work and the User will need to contact the TAC. If the email address with which the account was created has changed please submit a help desk ticket here: <https://nemsis.atlassian.net/servicedesk/customer/portals>. Select General NEMSIS Questions.

## Password Reset Instructions

Please see the Okta password reset instructions in step A, and then the dual authentication in step B. Once you complete these steps, you should have access to the NEMSIS dashboards.

### **Step A. Reset your password on your computer:**

1. Opening <https://login.nemsis.org>
2. Entering the state-issued or business email address as the username, e.g., (John.doe@state.agency.gov)
3. Press the "Forgot password?" button
4. Then press "Send me an email."

### **Step B. Open the Okta Verify App on your cell phone and complete the dual authentication:**

1. You will see login.nemsis.
2. And see your email address.
3. Then, you will see six shaded boxes. Click on the eyeball to get the code. You may need to authenticate with your fingerprint or face recognition.

Please note there is a 24-hour wait period from the last attempted password reset.

Please do not hesitate to contact the NEMSIS TAC with questions.