

Education Identity & Access Management (EDIAM) Security Introduction

David Reeg | IT Software Development Supervisor

8/7/2019



Topic

User Training

1. What is EDIAM, and when is it coming?
2. How do I use EDIAM security?
3. How does access expiration, revocation, and reauthorization happen in EDIAM?

IOwA Training

4. How are IOwAs set up in EDIAM?
5. How do IOwAs grant and reauthorize user access using EDIAM?



User Training

What is Identity & Access Management?

From the **MNIT Services Enterprise Identity and Access Management Standard**:

The State must establish, maintain and control authentication and access for users, systems, applications and networks. Access controls protect State data by only granting access to systems and data that is necessary for an individual's job responsibilities.

The **Identity Management Standard** describes the requirements for managing user account security including unique user IDs and strong passwords.

The **Access Management Standard** describes the requirements for managing user access authorization to state data systems.

Scope of Education Identity & Access Management

- The current Identity & Access Management system used by MDE is called MIDMS.
- MIDMS manages user access to state data systems with a user role on behalf of an organization (e.g. school, district, or state agency) in MDE-ORG.
- MIDMS manages user access to state data systems for MDE and PELSB and to SLEDS Secure Reports for MDE, OHE, and DEED. These data systems span 16 distinct agency division / unit organizations.
- MIDMS manages user access to over 50 web applications and over 200 secure reports (including both WebFOCUS and Crystal Reports).
- MIDMS manages user access for over 11,000 distinct user accounts with 236 distinct user roles.

EDIAM (Education Identity & Access Management) is a brand new single sign-on security system which will replace MIDMS. While there are some significant differences, the EDIAM security system should be mostly familiar to current MIDMS users.

Major Changes from MIDMS to EDIAM:

1. Delegated User Access Authorization
2. All User Access Has an Expiration Date

Change #1: Delegated User Access Authorization

- The current three-step Request/Preauthorize/Approve Access process is replaced by a single Authorize Access action by the Identified Official with Authority (IOwA).
- **The IOwA is appointed by the organization as responsible for assigning job duties.** The IOwA role was rolled out to LEAs to authorize external access for all MIDMS-secured applications in Spring 2015. At LEAs, we recommend assigning the IOwA role to the superintendent or executive director.
- Since there is no longer an Approve Access step at the agency, the IOwA role in EDIAM replaces the Admin role in MIDMS.
- IOwAs can now delegate their authority to authorize user access on behalf of their organization to an IOwA Proxy user role. The IOwA Proxy is NOT allowed to delegate.

Change #2: All User Access Has an Expiration Date

- Currently in MIDMS, once a user role is granted, it persists until it is revoked. There is no way to automatically “expire” access in MIDMS, which makes it difficult to enforce Minnesota IT Enterprise Security Policy & Standards.
- In EDIAM, all user access is granted with an expiration date. By default, all user roles will expire after 365 days of being granted.
- The user will receive two notification emails: first two weeks prior to expiration, and second after their access has been revoked. However, once the IOwA reauthorizes the user’s access, then notification emails will no longer be sent.
- The IOwA and IOwA Proxy(s) will receive monthly notification emails listing users with access on behalf of their organization which will expire within the next 45 days if not reauthorized and including a link to the EDIAM Authorization system.

EDIAM 2019 Project Schedule

Month	Deliverable
May 2019	EDIAM Production deployment #1: pilot rollout to production with internal-only applications and secured reports (Supporting 7 internal-only systems in May and 5 more in June)
June 2019	Complete EDIAM security requirements analysis for all MIDMS-secured web applications and secure reports.
July 2019	Implement EDIAM security configuration in development environment for all MIDMS-secured web applications and secure reports.
Aug. 2019	Update to EDIAM security all MIDMS-secured web applications and secure reports in development and test in staging environment.
Sept. 2019	EDIAM Production deployment #2: most MIDMS-secured applications and reports.
Oct. 2019	EDIAM Production deployment #3: more MIDMS-secured applications and reports.
Nov. 2019	EDIAM Production deployment #4: all remaining MIDMS-secured applications and reports.
Dec. 2019	Prepare for shutdown of old MIDMS security system.

How do I use EDIAM security?

Direct EDIAM Link: <https://secure.education.mn.gov/EDIAMProfile/>

- In August we will add an EDIAM launch page to the MDE Data Submissions website, the PELSB website, and other website portals as needed.
- When you login to EDIAM, you will land on the EDIAM User Profile page.
- The Create Account link launches the process to create a new user account. This is similar to the current MIDMS Create Account process.

The screenshot shows the Minnesota Department of Education website. The header includes the logo and navigation links: Home, About, Students and Families, Licensing, and Districts, Schools and Educators. The main content area is titled "Data Submissions" and contains several sections: "0-4 Census Data Reporting", "Access to Career Technical Education for Students with a Disability (ACTE-SPED)", "ADM Web Estimates (ADMWE)", "Assessment Secure Reports", "Assurance of Compliance and Mandated Reporting", "Athletics Data Reporting", "Career and Technical Education Levy Web-Based Reporting System", "Carl Perkins", "CLICS Program Administration", "Compulsory Instruction Compliance Data Reporting", "Continuing Education Clock Hour Reporting", "Disciplinary Incident Reporting System", and "District and School Site Verification". A sidebar on the left lists these categories under "Data Submissions".

The screenshot shows the "Education User Account Login" page. It features the Minnesota Department of Education logo and a lock icon. Below the logo is a "Username:" field and a "Password:" field. A green "LOGIN" button is positioned below the password field. Below the login fields, there are two links: "Don't have an account? [Create Account](#)" and "Can't access your account? [Get Login Help](#)". The "Create Account" link is circled in red. At the bottom, there is a disclaimer: "The system you are attempting to use is for authorized users only. This system is monitored for unauthorized access and use. Use of this system is expressed consent to such monitoring and recording. Any illegal or unauthorized use could be subject to federal, civil, criminal sanctions/penalties, disciplinary action, and/or other appropriate action."

EDIAM Create Account Process

- First, you must review and agree to the Acceptable Use Agreement.
- Second, you must fill out the form with your name, email address, phone, user ID, password, and security question.
- Each EDIAM user account must have a unique email address.



Education User Account - DEVSQL

Acceptable Use Agreement

Prior to accepting this agreement, please read the following information:

EDIAM System Acceptable Use Agreement

I agree to restrict access to my authorized application(s) to myself. I will not enter or enter required data for state reporting, communication exchange or other requirements.

I agree to abide by the provisions of Minnesota Statutes Chapter 13 and any other applicable statutes and regulations on confidentiality of data. This agreement shall be duplicated, used, or disseminated except as otherwise permitted in writing.

I agree to abide by the security standards prescribed by the Minnesota Department of Education at the protocol level as incorporated by the Minnesota Department of Education Information Security Force (IETF) and the IP (IPSec) Working Group. This will ensure the security of data protected under the Data Practices Act and FERPA.

I agree and understand that any sign-on or password instructions is being delegated to others. I further agree to maintain procedures within my control and unattended while it is logged onto the Minnesota Department of Education system.

I agree that my continued access to the Minnesota Department of Education system is contingent on the policies outlined in this agreement.

I agree that failure to abide by this agreement will result in my access to the system being terminated.

You must accept to be granted access.

Create User Account

Please complete your user account information.

Fields with an "*" are required

* First Name

Middle Name

* Last Name

* Full Name

* Email

* Confirm Email

* Phone
Example phone number: 6515828200 or 651-582-8200 or 651.582.8200.

* User ID
Please review 'User Id' errors above.

* Password
Must contain at least one of each of these: an upper and lower case character, number and a special character from this set !#\$*%&)(.:=?@+_-

* Re-enter Password

* Security Question

* Security Answer

EDIAM User Profile Page

- The EDIAM User Profile Page is the single launch page to all EDIAM-secured web applications and secured reports to which you have access. In the **Authorized Applications** section:
 - The [Application Link](#) launches that application. (For secured reports, the report group name is displayed in this table and the secure reports in the report group are listed in a separate **Authorized Secure Reports** section below.)
 - [View Access Details](#) shows each of your user account roles and days until expiration. You can remove your own role access.
- The Actions menu allows you to update your personal info (name, email, phone number), change your password, or update your challenge question.
- The Instructions menu is for EDIAM user documentation links.

mi MINNESOTA [Skip navigation](#)

Home ▾ Actions ▾ Instructions ▾ daviduser ▾

EDIAM User Profile - DEVSQL

Announcements

No Current announcements

Authorized Applications:

Application Link	User Actions	Description	More Information
ABE	View Access Details	Adult Basic Education Entitlement System	
Data Center Utilities	View Access Details	MDE Internal IBI/Data Center Utilities	
Maltreatment of Minors (MOMA)	View Access Details	Maltreatment of Minors (MOMA)	

Authorized Secure Reports:

WebFOCUS Team Reports

[MIDMS Users Mapped to Reports](#)

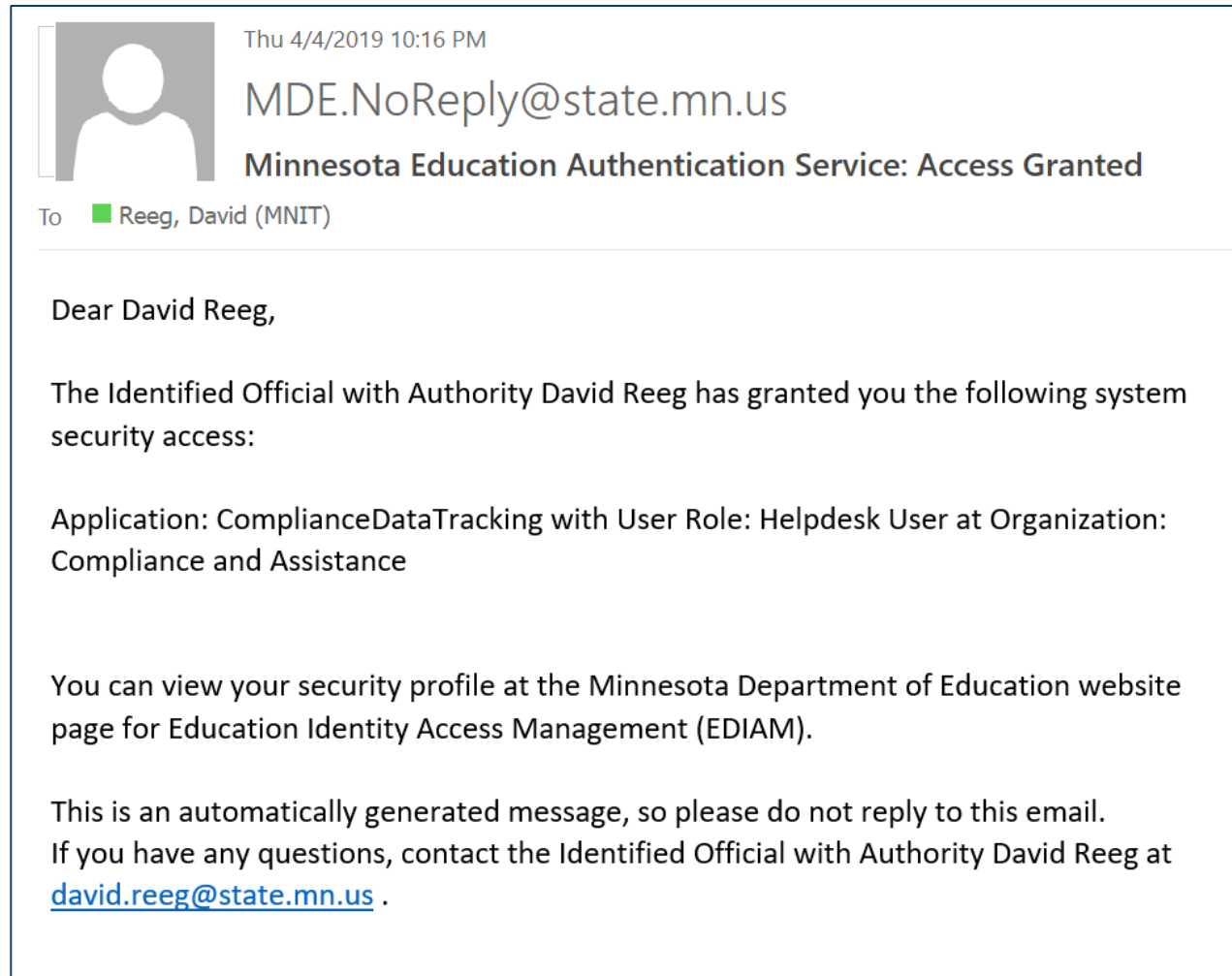
[Reports and MIDMS Roles](#)

How to get access to a secure application using EDIAM

- You get access to a secure application using EDIAM when the IOwA for your organization grants access to your user ID.
- There is no waiting period: as soon as the IOwA grants access to your user ID, you have that access.
- To grant access to you, the IOwA will need to know either your EDIAM user ID or the email address associated with your EDIAM user ID.
- **Unlike MIDMS, there is no way to “request access” within the EDIAM system.** Since the definition of Identified Official with Authority (IOwA) is the person responsible for assigning job duties, the IOwA (and their assigned IOwA Proxies, if applicable) is expected to know who needs access to State of Minnesota Education secure applications on behalf of their organization.
- If you do need to inform the IOwA that you need access to a secure application, you may use any form of communication appropriate for your organization (e.g. phone, email, helpdesk, etc.)

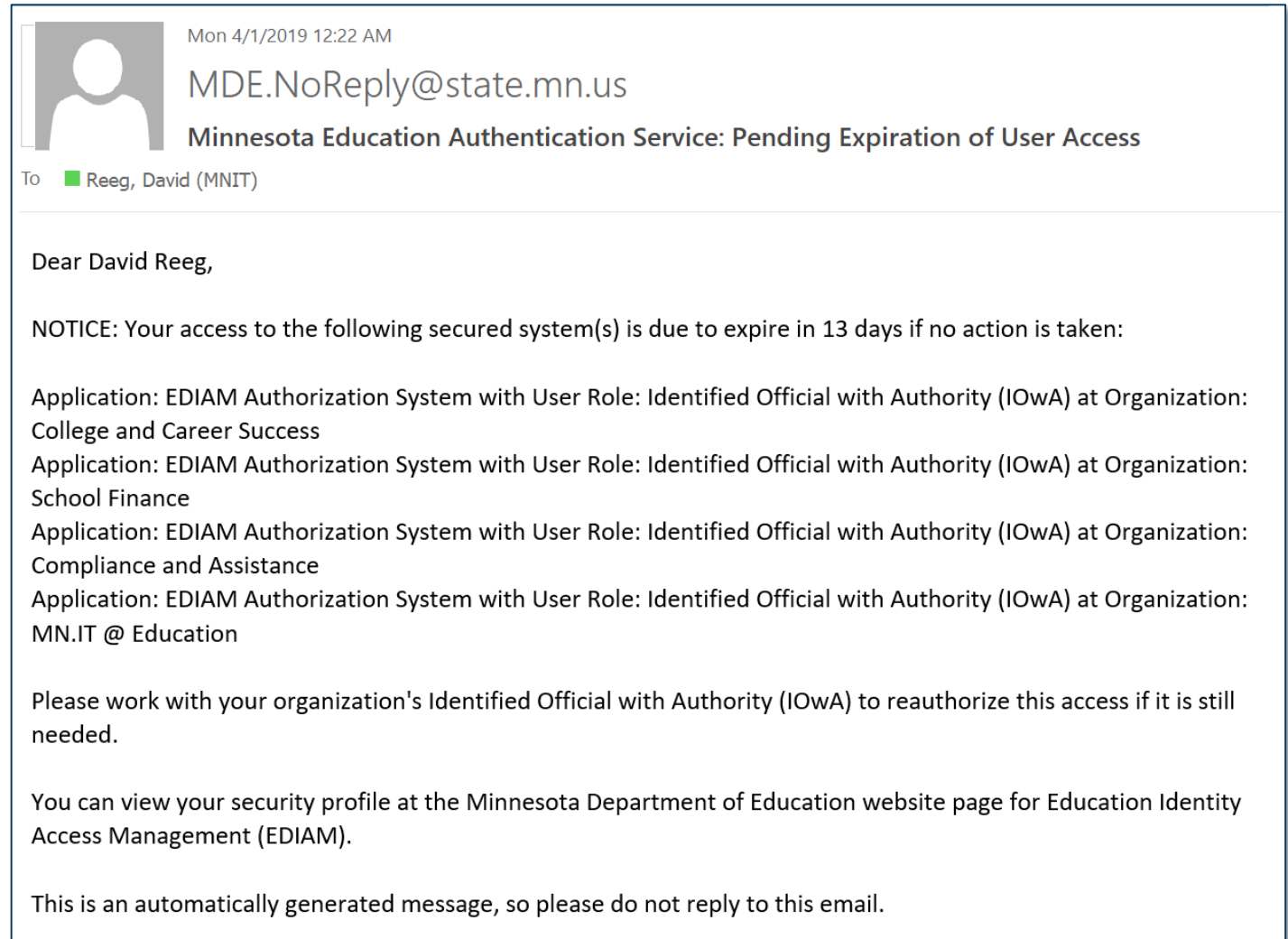
EDIAM Access Granted/Revoked: Email Notifications

- EDIAM sends an automated email notification informing you of the user role(s) you have been granted.
- The email notification provides you with contact information for the Identified Official with Authority (IOwA) who granted the access.
- A similar email notification is sent to the user when the IOwA revokes their access.





Access Expiration: Email Notifications

- EDIAM Authorization sends an automated email notification to you two weeks before your access is scheduled to expire.
- A similar automated email notification is sent when your access has expired and is automatically revoked.
- Because access expiration is automated, there is no Identified Official with Authority contact specified. Instead, then email directs you to the designated IOwA for your organization for any questions.



Mon 4/1/2019 12:22 AM

 MDE.NoReply@state.mn.us
Minnesota Education Authentication Service: Pending Expiration of User Access

To:  Reeg, David (MNIT)

Dear David Reeg,

NOTICE: Your access to the following secured system(s) is due to expire in 13 days if no action is taken:

Application: EDIAM Authorization System with User Role: Identified Official with Authority (IOwA) at Organization: College and Career Success
Application: EDIAM Authorization System with User Role: Identified Official with Authority (IOwA) at Organization: School Finance
Application: EDIAM Authorization System with User Role: Identified Official with Authority (IOwA) at Organization: Compliance and Assistance
Application: EDIAM Authorization System with User Role: Identified Official with Authority (IOwA) at Organization: MN.IT @ Education

Please work with your organization's Identified Official with Authority (IOwA) to reauthorize this access if it is still needed.

You can view your security profile at the Minnesota Department of Education website page for Education Identity Access Management (EDIAM).

This is an automatically generated message, so please do not reply to this email.



IOwA Training

EDIAM IOwA Authorizer Role

- EDIAM has a new IOwA Authorizer role. The IOwA Authorizer is a special type of Identified Official with Authority who can grant access to other Identified Officials with Authority (IOwAs) for both internal and external organizations.
- Unlike the IOwA, the IOwA Authorizer is NOT responsible for assigning job duties. The IOwA Authorizer is responsible for security system administration and support.
- To grant IOwA access, the IOwA Authorizer must have an **Authorization Document** which designates that person as the IOwA for that organization. This document is uploaded to EDIAM as a step in the process of granting access. The IOwA Authorizer must reauthorize this access annually, per the Enterprise Identity and Access Management Standard v1.1.
- For LEAs: the Authorization Document to designate the IOwA is the school board meeting minutes.
 - *NOTE: If the LEA already has school board meeting minutes designating the IOwA for MIDMS for the current year, those minutes can be resent to useraccess.mde@state.mn.us along with the designee's EDIAM user ID or email address associated with their user ID.*

LEA IOwA Setup Process

- **Step 1:** The IOwA designee must create a user account in EDIAM if they don't already have one.
- **Step 2:** The meeting agenda of your school board or equivalent governing board should include an agenda item to designate the Identified Official with Authority (IOwA) to authorize user access to State of Minnesota Education secured websites for your local education agency or organization. The board meeting minutes must clearly specify the name and EDIAM user ID (or email address) of the IOwA designee as well as the name of the local education agency and organization number for which that individual has the responsibility of assigning job duties.
- **Step 3:** Send an email to the EDIAM Helpdesk (useraccess.mde@state.mn.us) with the name of the designated Identified Official with Authority and the associated board meeting minutes attached.

Please include the following language in your meeting minutes:

Designation of an Identified Official with Authority for Education Identity Access Management

The Minnesota Department of Education (MDE), Professional Educator Licensing Standards Board (PELSB), and Office of Higher Education (OHE) require annual designation of an Identified Official with Authority (IOwA) for each local education agency that uses the Education Identity Access Management (EDIAM) system. The IOwA is responsible for authorizing, reviewing, and recertifying user access for their local education agency in accordance with the State of Minnesota Enterprise Identity and Access Management Standard, which states that all user access rights to Minnesota state systems must be reviewed and recertified at least annually. The Identified Official with Authority will authorize user access to State of Minnesota Education secure systems in accordance with the user's assigned job duties, and will revoke that user's access when it is no longer needed to perform their job duties. The Director recommends the Board authorize **add person's name and user ID** to act as the Identified Official with Authority (IOwA) for **add LEA name and organization number**.

Preparation for Conversion to EDIAM

- All users of MIDMS-secured web applications and secure reports will need to create new EDIAM user accounts.
- No MIDMS user accounts or user roles will be migrated to EDIAM.
 - There is obsolete security data in MIDMS that we don't want to migrate to a new security system.
 - Many MIDMS-secured web applications and secured reports are dropping obsolete user roles and making other changes which would also complicate migration.
- IOwAs therefore must grant all required user access using the EDIAM system. However, this process is much faster in EDIAM and includes user notifications.

How to Create an Initial User Access List for EDIAM

Signed in as: jmljajmlja with role: IdentifiedOfficialWithAuthority for 0011-01 Anoka-Hennepin Public School District [Log Out](#)

User Access Recertification - STAGING

UserAccessRecertification

[Home](#)

[Anoka-Hennepin Public School District - Change](#)

[Add Pre-Authorizations](#)

[Review Authorizations - User](#)

[Review Authorizations - Application](#)

[Export Authorizations csv](#)

MDE Authorization Review

[User Pre Authorization List](#)

[Organization Pre Authorization List](#)

Reference

[Applications and Roles](#)

Users for Anoka-Hennepin Public School District

Users with access on behalf of your local education agency.

Action	Name
Review Required	Admin Test
Review Required	Affinity Solutions
Review Required	All At Once
Review Required	Anne Danielson
Review Required	Anne Sheridan
Review Required	Anoka Hennepin
Review Required	Anu Sonti
Review Required	asdfas asdfasd
Review Required	Authorizer User
Review Required	Batch Tester
Review Required	BatchDiane Ba
Review Required	Beth Ann Toml

	A	B	C	D	E	F
	Authorization					
1	Status	Name	Application	Role	Organization	School
2	Has Access	Admin Test	CTE Budget	DistAdmin	Anoka-Hennepin Public School District	All Schools
3	Has Access	Affinity Solutions	Early Education Student	StudentCoordinator	Anoka-Hennepin Public School District	All Schools
4	Has Access	All At Once	TestWES	SchoolUserReadWrite	Anoka-Hennepin Public School District	Anoka High School
5	Has Access	All At Once	TestWES	SchoolUserReadWrite	Anoka-Hennepin Public School District	Anoka Middle School For The Arts
6	Has Access	All At Once	TestWES	SchoolUserReadWrite	Anoka-Hennepin Public School District	Anoka-Hennepin Regional High School
7	Has Access	All At Once	TestWES	SchoolUserReadWrite	Anoka-Hennepin Public School District	Champlin Park High School
8	Has Access	Anne Danielson	CTE Budget	DistUser	Anoka-Hennepin Public School District	All Schools
			Graduation Requirement			
9	Has Access	Anne Sheridan	System	SERVS Student Coordinator	Anoka-Hennepin Public School District	All Schools
10	Has Access	Anne Sheridan	TestWES	District UserRead Write	Anoka-Hennepin Public School District	All Schools
			Early Learning Scholarship			
11	Has Access	Anoka Hennepin	Award System	Scholarship Administrator	Anoka-Hennepin Public School District	All Schools
12	Has Access	anu sonti	MDE Secure Reports	District User	Anoka-Hennepin Public School District	All Schools
13	Has Access	anu sonti	MDE Secure Reports	School User	Anoka-Hennepin Public School District	Anoka-Hennepin Regional High School
14	Has Access	anu sonti	MDE Secure Reports	School User	Anoka-Hennepin Public School District	Secondary Technical Education Program
15	Has Access	Anu Sonti	SLEDSK12	DistrictUser	Anoka-Hennepin Public School District	All Schools
16	Has Access	Anu Sonti	Student ID System	Maintainer	Anoka-Hennepin Public School District	All Schools
			Student Support Data			
17	Has Access	Anu Sonti	Collection	Coordinator	Anoka-Hennepin Public School District	All Schools
18	Has Access	asdfas asdfasf	DisciplinaryIncident	Principal	Anoka-Hennepin Public School District	Anoka Middle School For The Arts
19	Has Access	Authorizer User	TestWES	AuthorizerReadWrite	Anoka-Hennepin Public School District	All Schools
20	Has Access	Batch Tester	DisciplinaryIncident	BatchDataEntry	Anoka-Hennepin Public School District	Anoka High School

Launching the EDIAM Authorization System

The IOwA launches the EDIAM Authorization System.

The screenshot shows the user interface for the EDIAM Authorization System. At the top left is the logo for the Minnesota Department of Education. The top right has a "Skip navigation" link. Below the logo is a navigation bar with "Home", "Actions", and "Instructions" menus, and a user profile for "david Iowa". The main heading is "EDIAM User Profile - DEVSQL". Below this is an "Announcements" section. The "Authorized Applications:" section contains a table with one entry for the "EDIAM Authorization System", which is circled in red.

DEPARTMENT OF EDUCATION

[Skip navigation](#)

Home ▾ Actions ▾ Instructions ▾ david Iowa ▾

EDIAM User Profile - DEVSQL

Announcements

Authorized Applications:

Application Link	User Actions	Description	More Information
EDIAM Authorization System	View Access Details	This system is used to grant user access to EDIAM-secured applications.	

Consenting to the Education Security Policy

Each user of the EDIAM Authorization System must consent to communicate the **Education Secured Website User Access Agreements and Acknowledgements** to each person who they grant access to EDIAM-secured systems.

mi MINNESOTA [Skip navigation](#)

Home Review User Search david Iowa

EDIAM Authorization - DEVSQL

Security Policy Review

Welcome to the Education User Access Authorization System. Only the organization's Identified Official with Authority (e.g. Superintendent, Executive Director or Board Chair) and their proxies are allowed to authorize access to State of Minnesota Education secured websites. By using this system, you are asserting that you are the Identified Official with legal Authority to authorize persons to access State of Minnesota Education secured websites for the organizations that you represent.

You must agree to communicate the Education Secured Website User Access Agreements and Acknowledgements with each person who you authorize to access Education Secured Websites.

[View the Education Secured Website User Access Agreements and Acknowledgements](#)

Yes consent to communicate these policies with each person who I authorize to access Education Secured Websites.

No do not consent. I understand that I will be logged out of the Education User Access Authorization System.

EDIAM Authorization - User Search

The IOwA can search for the user by either EDIAM User ID or Email Address. The IOwA must know the exact User ID or Email Address; no partial search is allowed.

The screenshot shows the EDIAM Authorization - User Search interface. The navigation bar includes 'Home', 'Review', and 'User Search'. The 'User Search' dropdown menu is open, showing 'User by Id' (highlighted with a red circle) and 'User by Email'. The main content area is titled 'EDIAM Authorization - DEVSQL' and contains a search form with the label 'Enter complete User Id of User' and a 'Search' button. Below the search form, it states '(Exact User Id only search done for security reasons)'. The page also includes sections for 'Overview', 'Authorization', and 'Review and Reauthorization'.

Overview

Welcome to the State of Minnesota. The State Security Standards require all user access authorization to be reauthorized annually.

Authorization

The Identified Official with Authority has the ability to authorize user access to Education secure systems for their authorized organization.

Review and Reauthorization

Once a user's access authorization is assigned, it must be reauthorized annually by the Identified Official with Authority. Reports will be sent by email monthly to the Identified Official with Authority showing the reauthorization status of all users with external access to one or more Education secure systems for their local education agency. The Identified Official with Authority can use this System at any time to review, update, and reauthorize external user access to State of Minnesota Education secure systems.

EDIAM Authorization - Add User Role

The IOWA reviews the User ID, First Name, Last Name, and Email Address to verify that they have selected the correct user. If so, the IOWA selects the Add User Role action.

The screenshot shows the IOWA Department of Education interface. At the top left is the logo and name 'DEPARTMENT OF EDUCATION'. At the top right is a link for 'Skip navigation'. Below this is a dark blue navigation bar with 'Home', 'Review', and 'User Search' menus, and a user profile 'david Iowa'. The main content area is titled 'EDIAM Authorization - DEVSQL'. It features a search form with the label 'Enter complete User Id of User', a text input containing 'daviduser', and a 'Search' button. Below the search form is a note: '(Exact User Id only search done for security reasons)'. The search results are displayed as a table with the heading 'User found for User Id provided'. The table has columns for 'Actions', 'User Id', 'First Name', 'Last Name', and 'Email'. One result is shown for 'daviduser', 'David', 'Reeg', and 'david.reeg@state.mn.us'. The 'Add User Role' link in the 'Actions' column is highlighted with a red circle.

Actions	User Id	First Name	Last Name	Email
Add User Role Review	daviduser	David	Reeg	david.reeg@state.mn.us

EDIAM Authorization - Select Authorizing Organization

An individual who is IOwA for more than one organization must first select which organization on behalf of which they are granting access (also known as the “Authorizing Organization”).

DEPARTMENT OF EDUCATION [Skip navigation](#)

Home Review User Search david Iowa

EDIAM Authorization - DEVSQ

Add User Role: Select Authorizing Organization

You are authorized to assign user roles for more than one organization, please select authorizing organization.

Selected	Organization Name	Formatted Id	State Organization Id
<input type="radio"/>	College and Career Success	0002-99	990002000000
<input type="radio"/>	School Finance	0006-99	990006000000
<input type="radio"/>	Compliance and Assistance	0010-99	990010000000
<input type="radio"/>	MN.IT @ Education	0015-99	990015000000

Add User Role for David Reeg (daviduser)

Authorizing User: David Reeg

Selecting Authorizing Organization

Select Authorizing Organization Cancel

EDIAM Authorization - Select Application

The IOwA selects which application to grant access to this user.

mn MINNESOTA [Skip navigation](#)

Home ▾ Review ▾ User Search ▾ dauidiowa ▾

EDIAM Authorization - DEVSQL

Add User Role: Select Application

List of Allowed Applications

Selected	Application Name	More Information
<input type="radio"/>	AOC Admin	
<input type="radio"/>	Compliance Data Tracking	
<input checked="" type="radio"/>	EDIAM Authorization System	
<input type="radio"/>	Maltreatment of Minors (MOMA)	

Select Application Previous Cancel

Add User Role for David Reeg (dauidiowa)

Authorizing User: David Reeg

Authorizing Organization: Compliance and Assistance (0010-99)

Selecting Application

EDIAM Authorization Example #1 - Select Application Role

After selecting the application, the IOWA selects which application role to grant access to this user. Hovering the mouse over the role name will display the role description. The Authorize Role action completes the process.


EDIAM Authorization - DEVSQL

Add User Role: Select Application

List of Allowed Applications

Selected	Application Name
<input type="radio"/>	AOC Admin
<input checked="" type="radio"/>	Compliance Data Tracking
<input type="radio"/>	EDIAM Authorization System
<input type="radio"/>	Maltreatment of Minors (MOMA)

[Skip navigation](#)



Home Review User Search
david Iowa

EDIAM Authorization - DEVSQL

Add User Role: Select Role

Action	Role Name	Authorization Length In Days
<input type="radio"/>	CDT Administrator	365
<input type="radio"/>	CDT Complaint Investigator	365
<input type="radio"/>	CDT Hearings Admin Complaint Investigator	365
<input type="radio"/>	CDT Mediations FIEP Admin	365
<input checked="" type="radio"/>	Helpdesk User	365

Add User Role for David Reeg (daviduser)

Authorizing User: David Reeg

Authorizing Organization: Compliance and Assistance (0010-99)

Application: ComplianceDataTracking (CDT)

Selecting Role

EDIAM Authorization Example #2 - Select IOWA Proxy Role

To grant a user the **IOWA Proxy** role, the IOWA will select the EDIAM Authorization System application. The IOWA Proxy role has equivalent access to the IOWA and is useful for assigning one or more backup IOWA users.


EDIAM Authorization - DEVSQL

Add User Role: Select Application

List of Allowed Applications

Selected	Application Name
<input type="radio"/>	AOC Admin
<input type="radio"/>	Compliance Data Tracking
<input checked="" type="radio"/>	EDIAM Authorization System
<input type="radio"/>	Maltreatment of Minors (MOMA)

Select Application **Previous**


Skip navigation

Home
Review
User Search
david Iowa

EDIAM Authorization - DEVSQL

Add User Role: Select Role

Action	Role Name	Authorization Length In Days
<input checked="" type="radio"/>	Identified Official with Authority (IOWA Proxy)	365

Authorize Role
Previous
Cancel

Add User Role for David Reeg (david Iowa)

Authorizing User: David Reeg


Authorizing Organization: Compliance and Assistance (0010-99)

Application: EDIAM Authorization System (ORGAUTH)

Selecting Role

EDIAM Authorization - User List

When the Add User Role action is completed, EDIAM Authorization displays a list of authorized users. The IOwA can then add another user role to the same user or another user.


[Skip navigation](#)

Home ▾
Review ▾
User Search ▾
dauidiowa ▾

EDIAM Authorization - DEVSQL

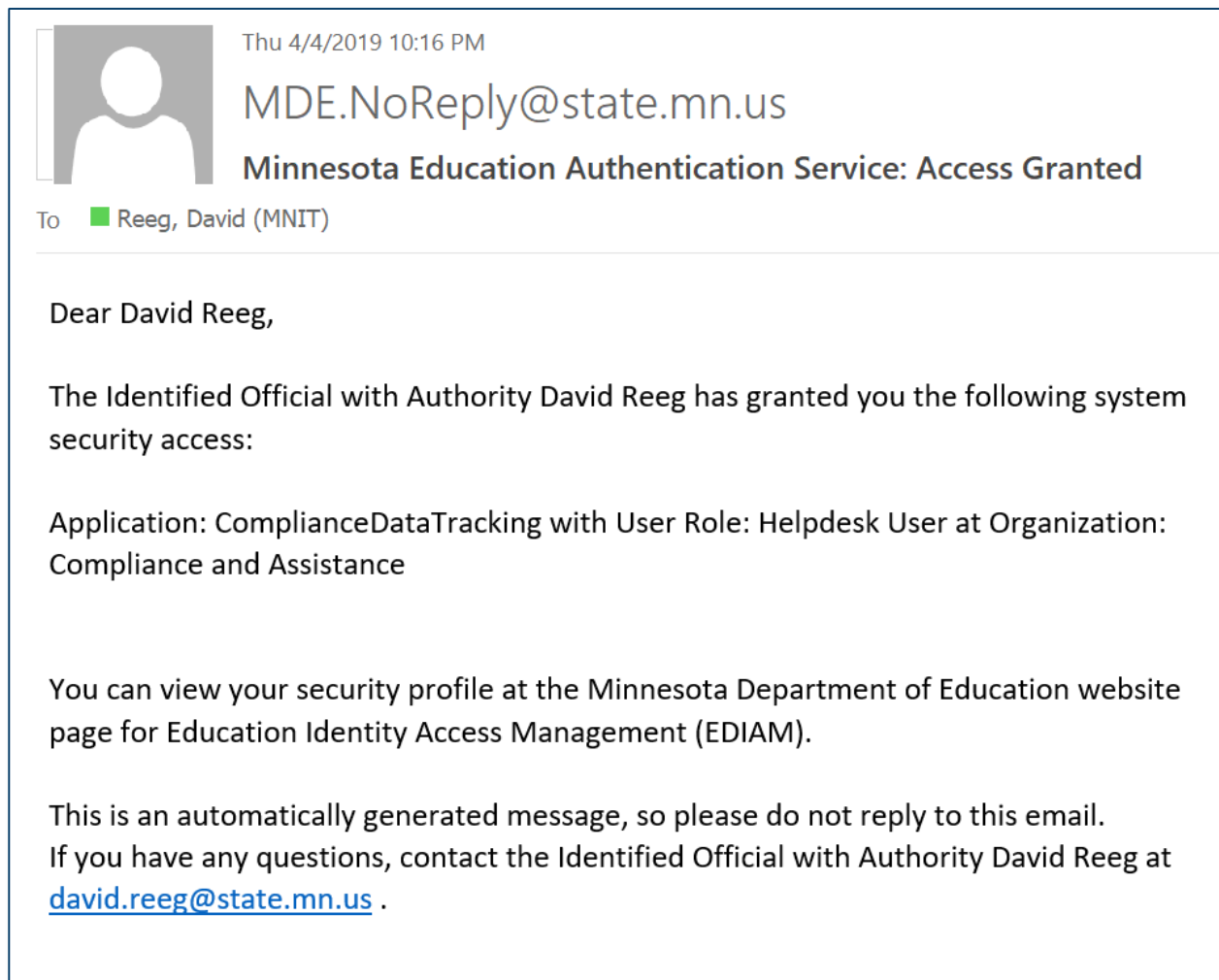
Authorization Assignment Completed.
[close](#)

List of Authorized Users

Actions	User Id	Full Name	Email Address	First Name	Last Name
Add User Role Review	daviduser	David Reeg	david.reeg@state.mn.us	David	Reeg

EDIAM Authorization - Access Granted Email Notification

- EDIAM Authorization sends an automated email notification to the user informing them of the user role(s) they have been granted.
- The email notification provides the user with contact information for the Identified Official with Authority (IOwA) who granted the access.



Access Revocation and Reauthorization: Review Access

- After searching for a user, the IOwA or IOwA Authorizer can select Review Access for access revocation and reauthorization on behalf of their organization.
- IOwAs can ONLY review access for role authorizations that they are permitted to add. If the selected user has none, EDIAM will inform the IOwA that this user has no authorizations for their review.

The screenshot shows the EDIAM Authorization - DEVSQL interface. At the top, there is a navigation bar with the Minnesota Department of Education logo and a 'Skip navigation' link. Below the navigation bar, there are menu items for 'Home', 'Review', and 'User Search', along with a user profile 'davidiowa'. The main content area is titled 'EDIAM Authorization - DEVSQL'. It features a search input field with the text 'Enter complete User Id of User' and a 'Search' button. The input field contains 'daviduser'. Below the search field, a note states '(Exact User Id only search done for security reasons)'. The search results are displayed as a table with the following data:


Actions	User Id	First Name	Last Name	Email
Add User Role Review	daviduser	David	Reeg	david.reeg@state.mn.us

The 'Review' link in the table is circled in red.

Access Revocation and Reauthorization Confirmation

On the Review Access Page:

- Select Reauthorize for all the user's roles to be reauthorized (resetting the days until expiration).
- Select Skip to take no action on the role at this time.
- Select Revoke for any role which should be revoked.
- Select Confirm to complete all of the selected actions for this user.


[Skip navigation](#)

Home ▾
Review ▾
User Search ▾
dauidiowa ▾

EDIAM Authorization - DEVSQL

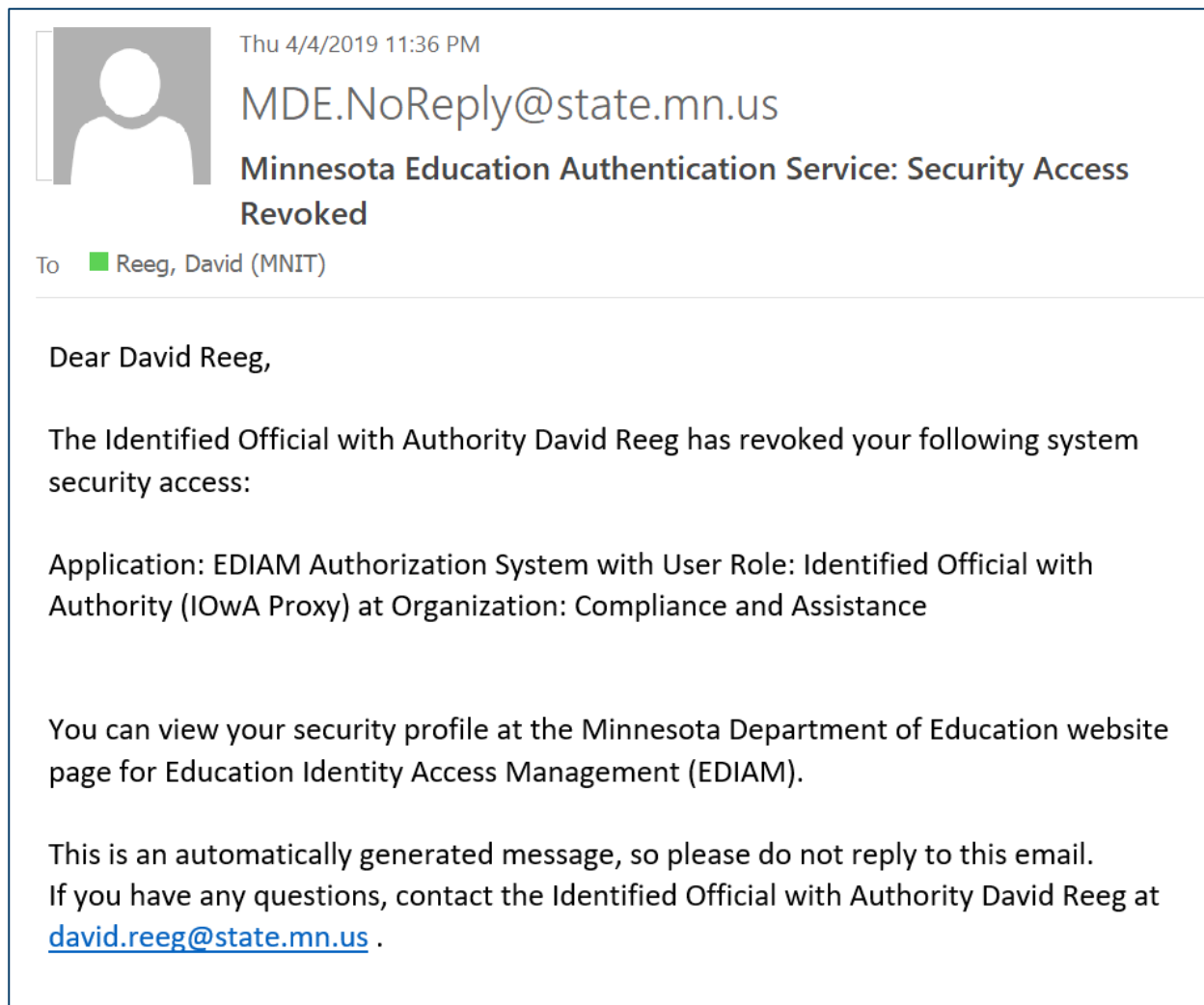
David Reeg (daviduser)

Authorize	Application	Role	Organization	Days Until Expiration	Notes
<input checked="" type="radio"/> Reauthorize <input type="radio"/> Skip <input type="radio"/> Revoke	ComplianceDataTracking	Helpdesk User	0010-99 Compliance and Assistance	20	
<input checked="" type="radio"/> Reauthorize <input type="radio"/> Skip <input type="radio"/> Revoke	Maltreatment of Minors (MOMA)	Help	0010-99 Compliance and Assistance	20	

Confirm
Cancel

Access Revoked Email Notification

- EDIAM Authorization sends an automated email notification to the user informing them when they have had user role(s) revoked.
- The email notification provides the user with contact information for the Identified Official with Authority (IOwA) who revoked the access.



Thank You!

David Reeg

MNIT Services partnering with Minnesota Dept. of Education

david.reeg@state.mn.us