<table>
<thead>
<tr>
<th>Topic</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Training</strong></td>
<td>1. What is EDIAM, and when is it coming?</td>
</tr>
<tr>
<td></td>
<td>2. How do I use EDIAM security?</td>
</tr>
<tr>
<td></td>
<td>3. How does access expiration, revocation, and reauthorization happen in EDIAM?</td>
</tr>
<tr>
<td><strong>IOwA Training</strong></td>
<td>4. How are IOwAs set up in EDIAM?</td>
</tr>
<tr>
<td></td>
<td>5. How do IOwAs grant and reauthorize user access using EDIAM?</td>
</tr>
</tbody>
</table>
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.
• 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.
<table>
<thead>
<tr>
<th>Month</th>
<th>Deliverable</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2019</td>
<td>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)</td>
</tr>
<tr>
<td>June 2019</td>
<td>Complete EDIAM security requirements analysis for all MIDMS-secured web applications and secure reports.</td>
</tr>
<tr>
<td>July 2019</td>
<td>Implement EDIAM security configuration in development environment for all MIDMS-secured web applications and secure reports.</td>
</tr>
<tr>
<td>Aug. 2019</td>
<td>Update to EDIAM security all MIDMS-secured web applications and secure reports in development and test in staging environment.</td>
</tr>
<tr>
<td>Sept. 2019</td>
<td>EDIAM Production deployment #2: most MIDMS-secured applications and reports.</td>
</tr>
<tr>
<td>Oct. 2019</td>
<td>EDIAM Production deployment #3: more MIDMS-secured applications and reports.</td>
</tr>
<tr>
<td>Nov. 2019</td>
<td>EDIAM Production deployment #4: all remaining MIDMS-secured applications and reports.</td>
</tr>
<tr>
<td>Dec. 2019</td>
<td>Prepare for shutdown of old MIDMS security system.</td>
</tr>
</tbody>
</table>
How do I use EDIAM security?
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.

Direct EDIAM Link: [https://secure.education.mn.gov/EDIAMProfile/](https://secure.education.mn.gov/EDIAMProfile/)
• 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.
• 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.
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.

---

Thu 4/4/2019 10:16 PM
MDE.NoReply@state.mn.us

Minnesota Education Authentication Service: Access Granted

Dear David Reeg,

The Identified Official with Authority David Reeg has granted you the following system security access:

Application: ComplianceDataTracking with User Role: Helpdesk User at Organization: Compliance and Assistance

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. If you have any questions, contact the Identified Official with Authority David Reeg at david.reeg@state.mn.us.
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, the email directs you to the designated IOwA for your organization for any questions.

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 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
The IOwA launches the EDIAM Authorization System.

Authorized Applications:

<table>
<thead>
<tr>
<th>Application Link</th>
<th>User Actions</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDIAM Authorization System</td>
<td>View Access Details</td>
<td>This system is used to grant user access to EDIAM-secured applications.</td>
<td></td>
</tr>
</tbody>
</table>

Skip navigation
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.
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 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.
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”).

<table>
<thead>
<tr>
<th>Selected</th>
<th>Organization Name</th>
<th>Formatted Id</th>
<th>State Organization Id</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>College and Career Success</td>
<td>0002-99</td>
<td>99000020000000</td>
</tr>
<tr>
<td></td>
<td>School Finance</td>
<td>0006-99</td>
<td>99000060000000</td>
</tr>
<tr>
<td></td>
<td>Compliance and Assistance</td>
<td>0010-99</td>
<td>99000100000000</td>
</tr>
<tr>
<td></td>
<td>MN.IT @ Education</td>
<td>0015-99</td>
<td>99000150000000</td>
</tr>
</tbody>
</table>

Add User Role: Select Authorizing Organization

You are authorized to assign user roles for more than one organization, please select authorizing organization.
The IOwA selects which application to grant access to this user.
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.
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.
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.
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.

Dear David Reeg,

The Identified Official with Authority David Reeg has granted you the following system security access:

Application: ComplianceDataTracking with User Role: Helpdesk User at Organization: Compliance and Assistance

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. If you have any questions, contact the Identified Official with Authority David Reeg at david.reeg@state.mn.us.
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.
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.

### EDIAM Authorization - DEVSQL

<table>
<thead>
<tr>
<th>Authorize</th>
<th>Application</th>
<th>Role</th>
<th>Organization</th>
<th>Days Until Expiration</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reauthorize</td>
<td>ComplianceDataTracking</td>
<td>Helpdesk User</td>
<td>0010-99 Compliance and Assistance</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Skip</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revoke</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reauthorize</td>
<td>Maltreatment of Minors (MOMA)</td>
<td>Help</td>
<td>0010-99 Compliance and Assistance</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Skip</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revoke</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IOwA

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.

Dear David Reeg,

The Identified Official with Authority David Reeg has revoked your following system security access:

Application: EDIAM Authorization System with User Role: Identified Official with Authority (IOwA Proxy) at Organization: Compliance and Assistance

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.
If you have any questions, contact the Identified Official with Authority David Reeg at david.reeg@state.mn.us.
Thank You!

David Reeg
MNIT Services partnering with Minnesota Dept. of Education

david.reeg@state.mn.us