



TSDS Upgrade Project

Security Management in the DMC

KEY TERMS

Application
Application Programming Interface (API)
Claim Set
Claim Set Resources
Data Management Center (DMC)
Individual Operational Data Store (IODS)
Key and Secret
Publish

You can find the definitions to these key terms and more here:

[Link to Key Terms Document](#)

LEARNING OBJECTIVES

By the end of this course, the users will be able to explain:

- The TEA Login (TEAL) role and privilege needed to manage security in the Data Management Center (DMC).
- What a claim set is and how it is assigned.
- How to generate a key and secret in the DMC.

WHY IS THIS COURSE IMPORTANT

- To understand how to access the DMC and generate the key and secret necessary for source system vendors to effectively publish data into the Individual Operational Data Store (IODS) for TSDS reporting and optionally for local use by the LEA.

COURSE AGENDA

GETTING STARTED

Apply for DMC LEA Technical Role

Key Concepts

Application, Claim Set, Key & Secret

Training Activity

Demo, Practice, Troubleshooting, Knowledge Checks

WRAP-UP

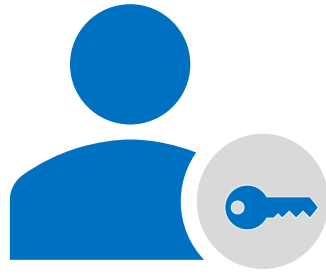
Key Takeaways, Resources, and Next Steps





GETTING STARTED

Apply for DMC LEA Technical Role



LEA TEAL ROLE

- LEA Technical Administrator:
 - DMC LEA Technical



KEY FUNCTIONS

- Administrator Functionality:
 - Manage Claim Sets
 - Manage Applications, Keys, and Secrets

REQUESTING TEAL ACCESS

Please refer to the LEA TEAL Roles and Privileges training material if you need more information on:

1. Requesting Access to the TSDS Portal
2. Applying for the TEAL Roles.

APPLY FOR DMC LEA TECHNICAL ROLE

STEP 1:

Enter your **Employing Organization** and select the **DMC LEA Technical** role.

The screenshot shows the 'Application access details' form. At the top, there are tabs for 'Applications' and 'Edit Account'. Below the tabs is the title 'Application access details' and a section titled 'Steps for adding access' with five numbered instructions. The 'Employing Organization' section has a red arrow pointing to the '* Organization:' field. Below this is the 'Roles & Parameters' section, which contains a list of roles. The 'DMC LEA Technical' role is selected, indicated by a red box around the checkbox and its label.

Applications Edit Account x

Application access details

Steps for adding access

1. Enter your Employing Organization (name or organization number).
2. Click the checkbox/radio button for the role(s) that you are applying for.
3. If there are parameters for the role(s) selected, enter that information.
4. Click the "Done" button to **queue** your request. This does not submit your request to TEAL.
5. Click the "Save Changes" button. This will then submit your access request to TEAL.

Employing Organization

* Organization: Who do you work for? In other words, what organization employs you (e.g. district, ESC, charter school)?

Roles & Parameters

- DMC LEA Admin Configurator
- DMC LEA Data Monitor
- DMC LEA L2 Validations
- DMC LEA Technical

STEP 2:

Enter the **Requested Organization** in the *Requested Organization ID* field and click **Done**. Click **Save Changes**.

The screenshot shows the configuration for the 'DMC LEA Technical' role. The role is checked at the top. Below it is the 'Description' field with the text 'DMC LEA Technical'. The '* Requested Organization ID:' field has a red arrow pointing to it. Below this is the 'Privileges' section, which is highlighted with a red box and contains the 'DMC Manage Key/Secret' privilege selected.

DMC LEA Technical

Description:
DMC LEA Technical

* Requested Organization ID:
(Requested Organization ID)

Privileges:
 DMC Manage Key/Secret



KEY CONCEPTS

Application, Claim Set, Key & Secret

SETUP STEPS IN THE DMC

1

Add an Application for each Source System Vendor and/or Vendor Product as necessary.

2

Choose the Appropriate Claim Set for each Vendor Application and/or Vendor Product as necessary.

3

Generate the Key & Secret for each Application.

4

Communicate Key & Secret Information with each Vendor.

- A **claim set** defines the access to which the source system has to the LEA's data in the IODS.
- Access may include:
 - **Create**
 - **Read**
 - **Update**
 - **Delete**

TEA Pre-Defined Claim Sets:

- SIS Vendor
- HR Vendor
- Finance Vendor
- HR/Finance Vendor
- SIS/HR/Finance Vendor
- Assessment Vendor
- Read-Only All Resources
(e.g., Third Party Vendors)

- A **key** and **secret** are the credentials used by the source system vendor to access the API.
 - The key and secret are like a username and password and should be handled in a secured manner and follow local security policy when applicable.
- The key and secret are **generated in the DMC** and are necessary for source system vendors to publish and read data.
 - The key and secret can be regenerated at any time. When regenerated, the previous key and secret are no longer valid.

GENERATE KEY & SECRET

Steps 1 & 2

ADD APPLICATION & CLAIM SET

1. Enter a unique and descriptive application name for each source system vendor and/or vendor product as necessary.
2. Assign the appropriate claim set. Click **Add Application.**

The screenshot shows a web interface for managing applications. At the top, there are navigation links for 'Monitor Validations' and 'Admin'. Below that, a breadcrumb trail reads 'Home >> Manage Applications, Keys, and Secrets'. The main heading is 'Add/Edit Application'. There are two input fields: 'Application Name' with the value 'My SIS Product Name' and 'Claim Set Name' with a dropdown menu set to 'SIS Vendor'. Both fields have a help icon (question mark) to their right. At the bottom, there are two buttons: 'Add Application' and 'Cancel'.

Steps 3 & 4

GENERATE KEY & SECRET

3. Generate the key & secret for the application.
4. Provide information to the vendor for **authentication** to the API. Click **Acknowledged.**

The screenshot shows the 'Key and Secret' page. At the top, there is a heading 'Key and Secret' and a key icon. Below the icon, the generated information is displayed: 'Application Name: My SIS Product Name (701603)', 'Key: UB3LJ1BzEDW9', 'Secret: YxGUIM7M7Z4ROOZN6hFlaSVY', and 'API URL: <https://odsprod.tea.texas.gov/odsedfiapi2024>'. A red 'Note' states: 'For security purposes, this key and secret cannot be viewed again after you leave this page. You must communicate this key and secret to your vendor for them to be able to access your IODS.' At the bottom right, there is an 'Acknowledged' button.

MANAGE CLAIM SETS

- The Manage Claim Sets UI in the DMC allows users to see the claim sets they have assigned.
- Clicking on the Claim Set Name will allow users to see the access granted to each resource within the claim set.

[Home](#) >> Manage Claim Sets

Admin

Manage Claim Sets

[Export Claim Set](#)
[Import Claim Set](#)
[Add Claim Set](#)

Creator	Claim Set Name ↑	Applications in Use ↑	Last Updated ↑	Action
	Assessment Vendor	0	09/18/2023	
	Ed-Fi Sandbox	0	07/28/2023	
	Finance Vendor	0	09/18/2023	
	HR Vendor	0	09/18/2023	
	HR/Finance Vendor	0	09/18/2023	
	Read-Only All Resources	0	09/18/2023	
	SIS Vendor	1	09/18/2023	
	SIS/HR/Finance Vendor	0	09/18/2023	

VIEW CLAIM SETS

- Upon the selection of a specific claim set, the appropriate access is shown for each resource.

🏠 [Home](#) >> Manage Claim Sets

Admin

View Claim Set

Claim Set Name: SIS Vendor

Application Name: My SIS Product Name

Resources	Read	Create	Update	Delete
AcademicWeek	✓	✓	✓	✓
AccountabilityRating	✓	✓	✓	✓
AssessmentMetadata	✓			
BasicReportingPeriodAttendance	✓	✓	✓	✓
BellSchedule	✓	✓	✓	✓
BilingualESLProgramReportingPeriodAttendance	✓	✓	✓	✓
Calendar	✓	✓	✓	✓



TRAINING ACTIVITIES

Demo, Practice, Troubleshooting, Knowledge Checks

DEMONSTRATION

1. Log into a TSDS Portal.
2. Navigate to DMC.
3. Hover over Admin tab and click Manage Applications, Keys, and Secrets.
4. Select Add Application, enter Application Name, and select the Claim Set. Click Add Application and then Save.
5. Review Claim Sets and Resources for the Claim Set.
6. Edit Claim Set.
7. Regenerate key and secret.

Note: The Reference Guide is a resource that provides step-by-step instructions for Managing Applications, Keys, and Secrets.

[Link to Security Management Reference Guide](#)

PRACTICE EXERCISE

Task 1: Set up vendor application in the DMC and assign the appropriate access to the IODS.

Task 2: Change the IODS access for the current vendor product (update name as needed).

Task 3: Regenerate the key and secret (as needed).

Ready

Set

Go

Scenario 1: Key and Secret information was not captured.

Manage Applications, Keys, and Secrets

[Add Application](#)

Application Name: My SIS Product Name ✎ 🗑️

Claim Set: SIS Vendor

Key and Secret: You cannot view an existing key and secret. If you need a key and secret for this application, you must regenerate.

Date Generated: 01/15/2024

Generated by: John Doe

[Regenerate](#)

Regenerate Key and Secret? ✕

Are you sure you want to regenerate the key and secret for **My SIS Product Name**?

- The current key and secret will be invalidated.
- You'll need to update your external application configuration with the new key and secret.
- This action cannot be undone.

[Regenerate Key and Secret](#) [Cancel](#)

Application Name:	My SIS Product Name (701603)
Key:	0u4KdJSRkLeB
Secret:	uTadv1W1ngQieTZVGWpLIjY
API URL:	https://odsprod.tea.texas.gov/odsedfiapi2024

Note: For security purposes, this key and secret cannot be viewed again after you leave this page. You must communicate this key and secret to your vendor for them to be able to access your IODS.

[Acknowledged](#)

Resolution Steps:

- Login to TEAL, then TSDS Production Portal, and navigate to the DMC. Hover over the Admin tab and select Manage Applications, Keys, and Secrets.
- Click **Regenerate** on the appropriate Application.
 - The previous key and secret will no longer be valid.
- Read the information in the pop-up dialog box.
- Click **Regenerate key and secret**.
- The key and secret dialog box will provide the new credentials to provide to the vendor. Once provided, click **Acknowledged**.

Scenario 2: User gets a Level 1 API error.

Level 1 API Error might read something like: “Provided Username and Secret Key is either incorrect or has expired.”

Manage Applications, Keys, and Secrets

Application Name: My SIS Product Name

Claim Set: SIS Vendor

Key and Secret: You cannot view an existing key and secret. If you need a key and secret for this application, you must regenerate.

Date Generated: 01/15/2024

Generated by: John Doe

Regenerate

Resolution Steps:

- Vendor is using an invalid key and secret.
- Note the date the key and secret was generated and by whom to help in determining if a new Key/Secret has been generated but was not communicated to the Vendor.
- Determine which individuals at the LEA have the DMC LEA Technical TEAL role and decide if further restrictions or guidelines should be initiated.
- **Regenerate the key and secret and communicate the new key and secret to Vendor.**
- Instruct LEA staff who have the DMC LEA Technical Role on the importance of communication and verifying whether the Vendor already has an Application and key and secret.

Scenario 3: Assigned Wrong Claim Set to Application in DMC.

Resolution Steps:

Manage Applications, Keys, and Secrets

Add Application

Application Name My SIS Product Name

Claim Set SIS Vendor

Monitor Validations Admin

Home >> Manage Applications, Keys, and Secrets

Add/Edit Application

Application Name: My SIS Product Name

Claim Set Name: SIS Vendor

Select Claim Set

- SIS Vendor
- Read-Only All Resources
- Assessment Vendor
- Finance Vendor
- HR Vendor
- SIS/HR/Finance Vendor

Save Changes Cancel

- Log into TEAL, then TSDS Production Portal, and navigate to DMC. Select Manage Applications, Keys, and Secrets.
- Click the pencil icon to edit this Application.
- Update the Application Name, if necessary.
- Click on the dropdown arrow on Claim Set Name, select the appropriate claim set.
- Click **Save Changes**.
- The key and secret originally assigned will continue to be valid but the access to resources will be updated.**

KNOWLEDGE CHECK

1. Which of the following TEAL roles is needed to manage claim sets or generate a key and secret?
 - A. DMC LEA Admin Configurator
 - B. DMC LEA Data Monitor
 - C. DMC LEA Technical
 - D. All of the above

Note: An LEA should limit the access to this role to only those responsible for configuring the IODS.

- 2. For TSDS reporting purposes, an LEA is not required to create a custom claim set.**
 - A. True
 - B. False

Note: In most cases, the LEA would select a TEA pre-defined claim set when generating a key and secret for their vendor.

KNOWLEDGE CHECK

3. The following information is displayed in the DMC upon generating a key and secret.
- A. Application Name
 - B. Key and Secret
 - C. API URL
 - D. All of the above

Note: Once **Acknowledged** is clicked, the LEA will no longer be able to view the key and secret.

KNOWLEDGE CHECK

4. Which of the following is not a reason to regenerate the key and secret for an application?
- A. When **Acknowledged** is clicked without capturing the information
 - B. When Level 1 errors prevent the Vendor from connecting to your IODS
 - C. When the LEA is performing periodic security cleanup
 - D. When changing the claim set currently assigned to a Vendor

Note: Changing the claim set assigned on an Application for a Vendor does **not** require that the key and secret be regenerated.



WRAP UP

Key Takeaways, Resources, and Next Steps

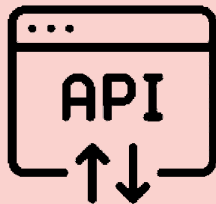
KEY TAKEAWAYS



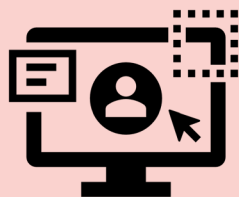
The **DMC LEA Technical** role is required to manage an application, claim set, and key and secret in the DMC.



Access to the management of the key and secret should be **limited** and handled in a **secure** manner.



Source system vendors will utilize the key and secret to **access the IODS via the API**.



The application, claim set, and key and secret can be updated in the **DMC application**.

TRAINING RESOURCES



- Key Terms and Definitions



- Security Management Reference Guide

NEXT STEPS

Apply for the DMC LEA Technical role

- Utilize the training materials available for step-by-step instructions in the Reference Guide.
- Apply under the Texas Student Data System Portal Application.
- Monitor the approval process and follow up with the designated TEAL approver as needed.

Generate the key and secret

- Assign the appropriate claim set.
- Generate the key and secret necessary for each source system vendor product.
- Confirm that data is being published to the IODS as expected.

In this training we talked about:

- The DMC LEA Technical role needed to manage security in the DMC application.
- The key concepts and definition of an application, claim set and key and secret.
- How to effectively add an application, assign a claim set, and generate a key and secret in the DMC application.

QUESTIONS

