SPECTRIM Guide

Texas.gov Digital Identity Solution (TDIS)

Access Management

Updated April 2022

Table of Contents

Introduction

SPECTRIM

To help tie together the overall state security program, DIR has implemented a governance, risk, and compliance software tool available to all state agencies and institutions of higher education. The SPECTRIM portal provides tools for managing and reporting security incidents, conducting risk assessments, storing, and managing organizational policies, performing assessment and authorization (A&A) on information systems, templates for agency security planning activities, and more.

Eligible Entities

The SPECTRIM portal is free for all Texas state agencies, public institutions of higher education, and public community colleges. There is no limit to the number of users each organization can have.

To request an account, ask your agency's Information Security Officer (ISO) to open a support request in the portal or email GRC@dir.texas.gov.

Texas.gov Digital Identify Solution with SPECTRIM

Texas.gov Digital Identity Solution (TDIS) allows authorized Texas government employees to access services and systems. TDIS utilizes multi-factor authentication (MFA), the requirement of more than one authentication factor for successful authentication. Logging in to SPECTRIM, through TDIS, leverages MFA to gain access.

Roles

Access Types

There are different levels of access for TDIS and SPECTRIM. TDIS access allows users to perform different functions within the TDIS application, while SPECTRIM access allows users to perform different functions within the SPECTRIM application. The information provided in this guide is for TDIS access. The table below is a basic description between the common types of access.

Application	Access Level Name	Description	Capabilities
TDIS	EndUser	General user role.	• View own Profile and Access
TDIS	Helpdesk	Helpdesk administrator role. Level 1 Organization Administrator	• View User Profile and Access • Send Enrollment Link • Password Reset • Account Unlock
TDIS	Application	Application administrator role. Level 2 Organization Administrator	• View User Profile and Access • Send New Enrollment Link • View, Enable, and Disable User App Access • Password Reset • Account Unlock • Manage Helpdesk (Level 1) Admins

Figure 1. Access Types Table

General Information

There are different levels of TDIS Delegated Administrators. TDIS Delegated Administrators are TDIS accounts with an administrator role who have the ability to manage other TDIS accounts assigned their organization. See Figure 1. Access Types Table for details.

Accessing the Delegated Administration Console

To manage access, administrators will login to the Delegated Administration Console.

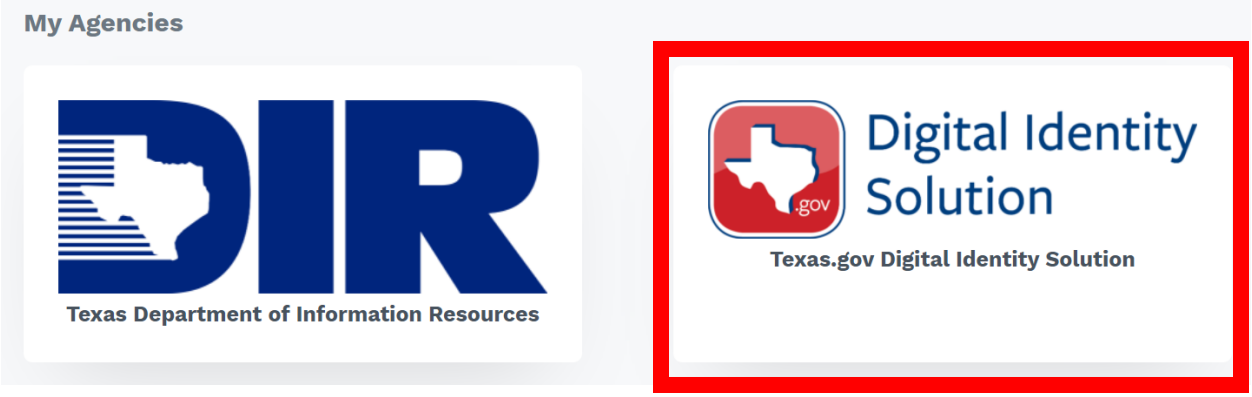
1. Login to TDIS
2. Navigate to the TDIS application
3. 

Figure 2. Applications in TDIS console

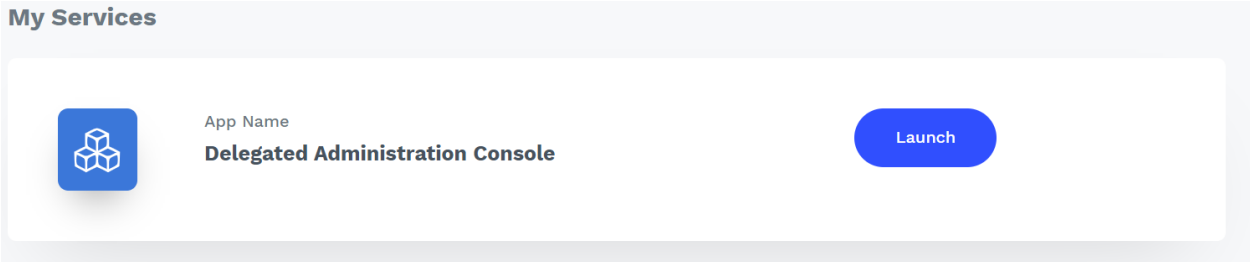
4. Launch the Delegated Administrator Console
5. 

Figure 3. Delegated Administrator's Console

Administrator Console Functions

Search Tips

When searching for a user, you will have the option to filter users by Agency User ID, Email Address, First Name, and Last Name. You can perform a wildcard search by including the percentage sign (%) before your search criteria, (i.e., %Alex), which will generate all user profiles

that contain the specified word or phrase. You will be able to view their Status, Email Address, Organization UserID (referred to as Agency User ID), DA Access Level, and more. This page may be used to view profile information and decode potential user issues. For example, the field Locked by OTP (One-Time Passcode) and Account Locked Time may provide insight into current user issues. If you would like to navigate between individual User Profiles and the User List, simply click the main back or forward arrows in the URL bar on the top of your screen.

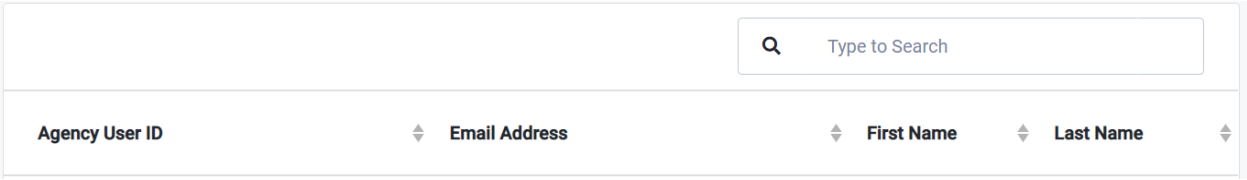


Figure 4. Delegated Administrator's Console search field

User Fields

Status - This field refers to if the user is disabled (inactive) or enabled (active). A disabled user cannot log into the TDIS Portal or their organization's application(s). Reminder: do not manually edit this field. The Status field is correlated to the Actions dropdown menu and must remain editable for the actions in the Actions dropdown menu to function properly. To edit a user's account status, please click Enable or Disable (depending on user attributes) from the Actions dropdown menu.

Organization (Agency) User ID - This is the user's organization-specific identification.

DA Access Level - The DA Access Level provides information into the specific user level. The user may be an End User, Helpdesk Administrator (Level 1), or Application Administrator (Level 2).

Sending Enrollment Information

Sending Enrollment Information

If the user does not know if they have an account already, you can help them check. Please instruct the user to:

1. Go to the Texas.gov Digital Identity Solution Portal login page and attempt to sign in. If they are not able to sign in because of an invalid email, ask them to confirm their work email. If their email is not the issue, please send the user a new tokenized link via email to enroll their account.

2. The user can also click Forgot Password and enter their work email. If there's an account associated with their email, they'll be prompted to verify their account. If there's not an

account associated with their email, you can send the user a new tokenized link via email.

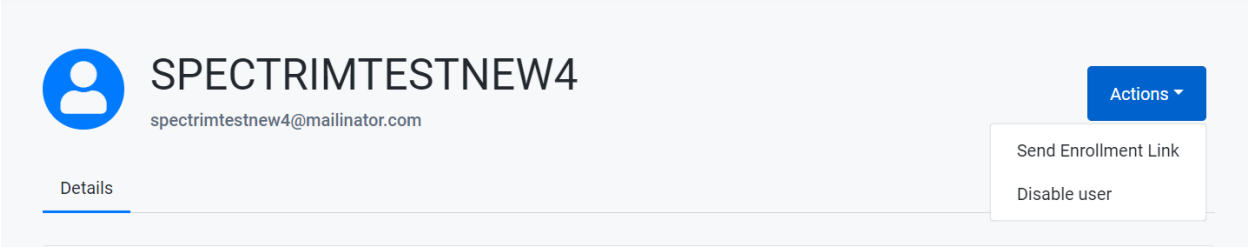
3. As an Admin, you can also search for the user in the Delegated Admin console and inform the user if their account is enrolled. If their account has not yet been enrolled, please send the user a new tokenized link to enroll their account.
4. 

Figure 5. Send Enrollment Link available in Actions

NOTE: If the user has not received their enrollment email or accidentally deleted the email:

- Please ask them to check their spam, junk, or Recently Deleted folder.
- If they cannot locate the enrollment email, please send them a new enrollment link via email.
- A work email is required to create a user's account.

Updating TDIS Attributes

Requesting TDIS Access

SPECTRIM users will have general TDIS user access. However, TDIS Delegated Administrator access can be appointed with authorization from the Organization's Security Office.

To request for a new SPECTRIM account submit a SPECTRIM portal Support Request or email GRC@dir.texas.gov for further assistance.

Password Adjustment

A user's TDIS password will be the same password used through the Single Sign-On process for SPECTRIM. The password expiration timeframe is 60 days. Users will receive a notification via email from no-reply@myaccess.dir.texas.gov to reset their password one week before password expiration and will also be notified on the TDIS Portal login page with an error message when their password has expired.

Resetting a Password

1. To reset a password on behalf of a user, navigate to the TDIS Delegated Admin Console

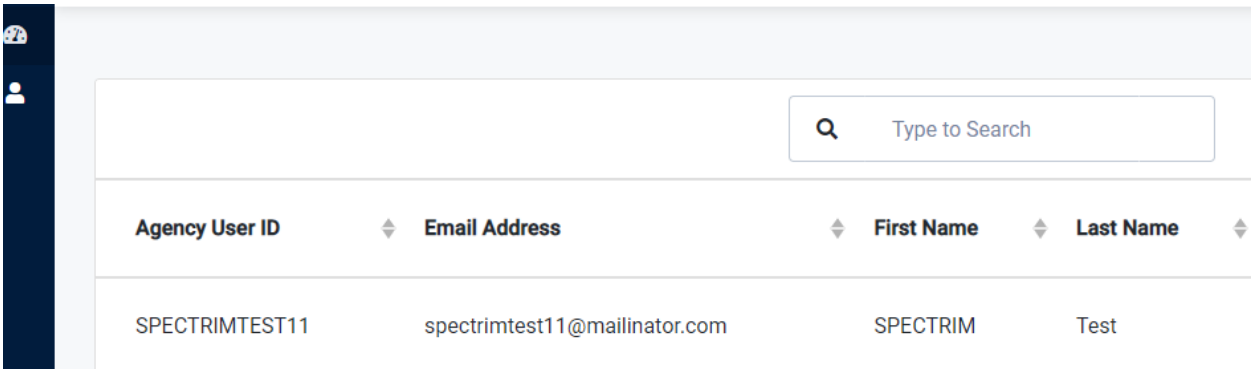
2. 

Figure 6. Example of a user from the Delegated Admin Console

3. Select the user
4. Expand Actions
5. Select Reset password

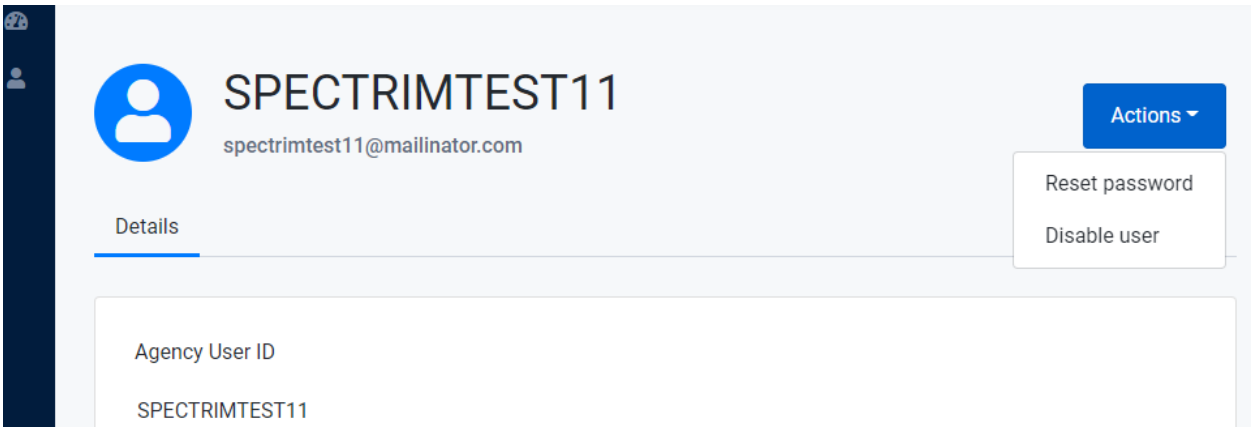
6. 

Figure 7. Reset password feature available in Actions

7. A pop-up will appear to confirm resetting of password, click Send

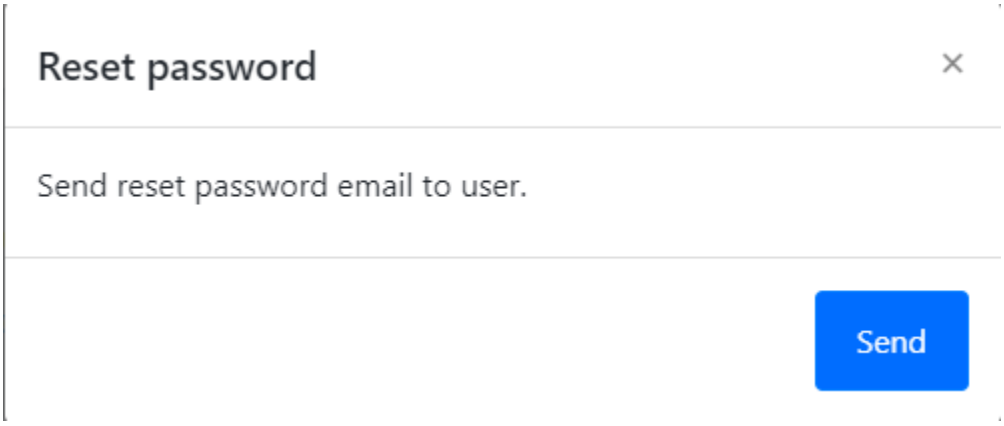
8. 

Figure 8. Complete password reset by clicking Send

9. User will then be sent a password reset email

Note: Users can make the following User Profile changes for their account:

- Forgot Password on the Texas.gov Digital Identity Solution Portal Login page.
- Change Password in Texas.gov Digital Identity Solution Portal Account Settings.
- Profile credentials (mobile phone number and security questions) in Texas.gov Digital Identity Solution Portal Account Settings.

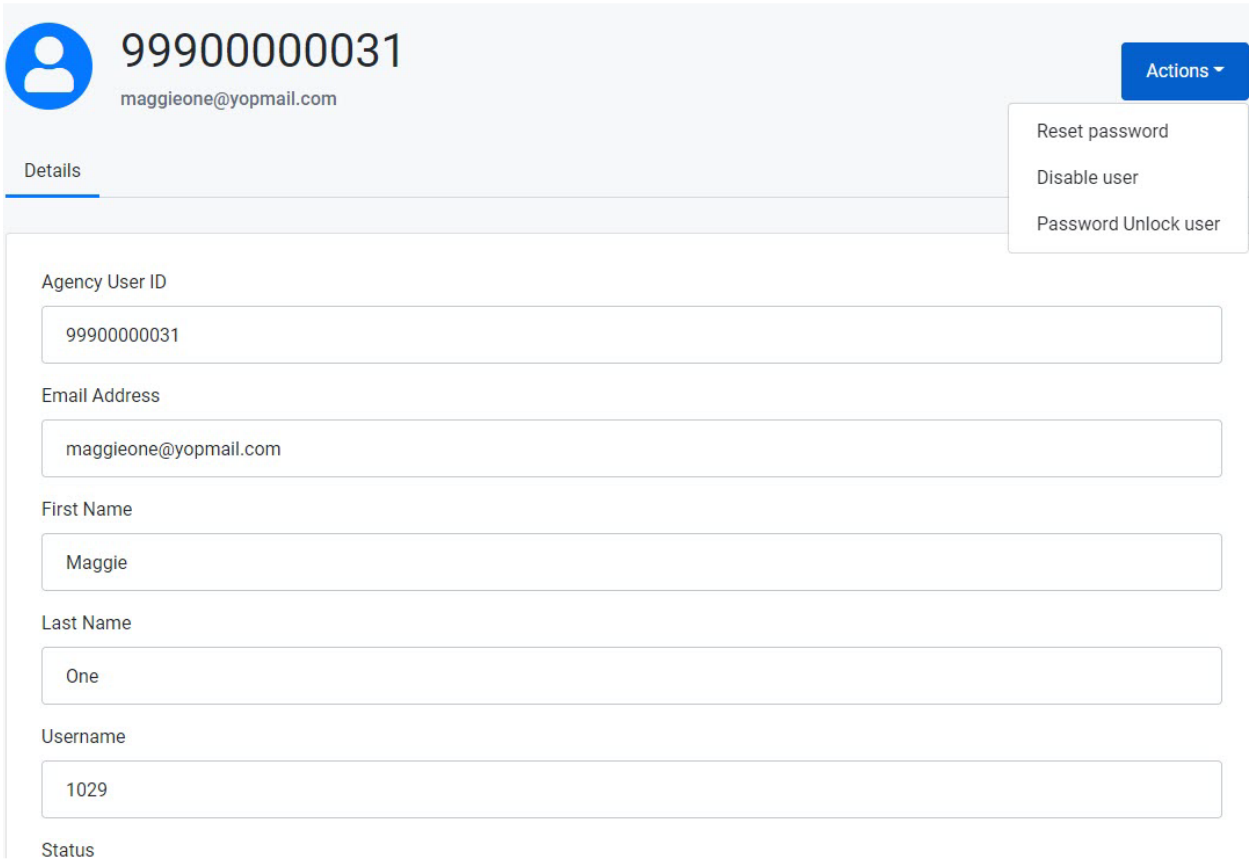
Unlocking an account

If a user is locked out of the Texas.gov Digital Identity Solution, they will be unable to access their account. There are two reasons that a user's account could be locked:

a) too many failed password attempts (5)

b) too many failed One-Time Passcode (OTP) attempts (3)

1. Verify the user's identity
2. Navigate to the Actions dropdown in their profile
3. Depending on what type of account lock scenario the user is experiencing, you may unlock the user's account by clicking Password Unlock user or OTP Unlock user



4.

Figure 9. Password Unlock available in Actions

5.

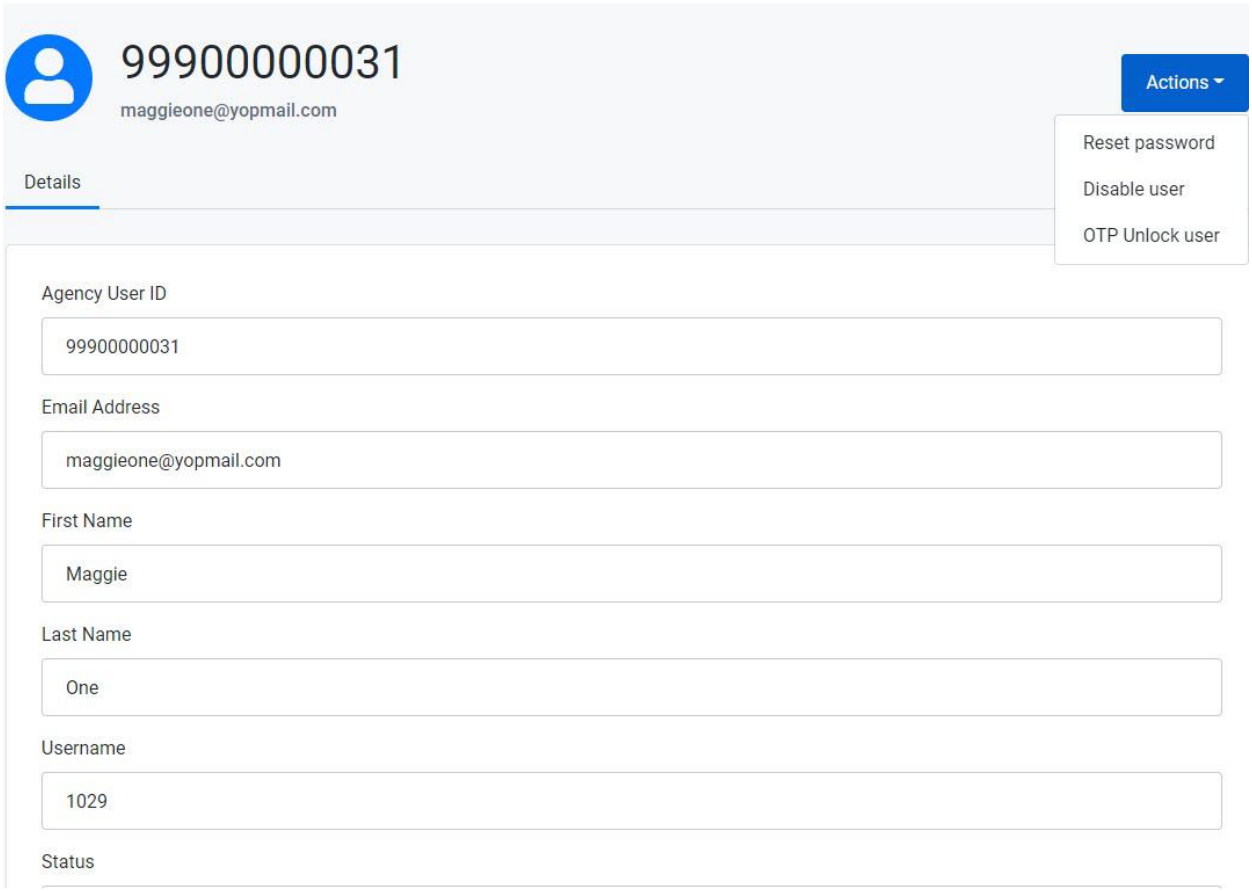


Figure 10. OTP Unlock available in Actions

6. Before completing the action, you will be prompted with a notification to confirm
7. After confirming, the user will be sent an automatic email notifying them of the completed action.

Updating TDIS User Access

1. An authorized Delegated Administrator will login to TDIS
2. Launch the Delegated Administrator Console
3. Navigate to the User tab to view a list of the users in your organization

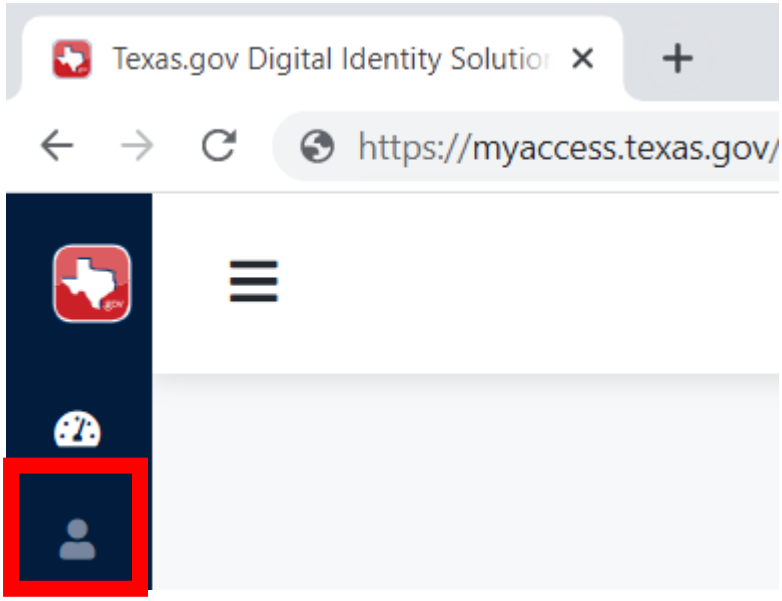
4. 

Figure 11. User tab

5. Search for the user
6. Update the DA Access Level field with the appropriate level of requested access to 313007_[role name]_[Agency Division number]. See table for examples of access that may be assigned.

Access Level Name	DA Access Level Field
Helpdesk	313007_Helpdesk_###
Application	313007_Application_###

Figure 12. Delegated Administrator Access Level Field Names Table

7. If user has an account with other applications with TDIS, append field using a | (pipe) to separate.

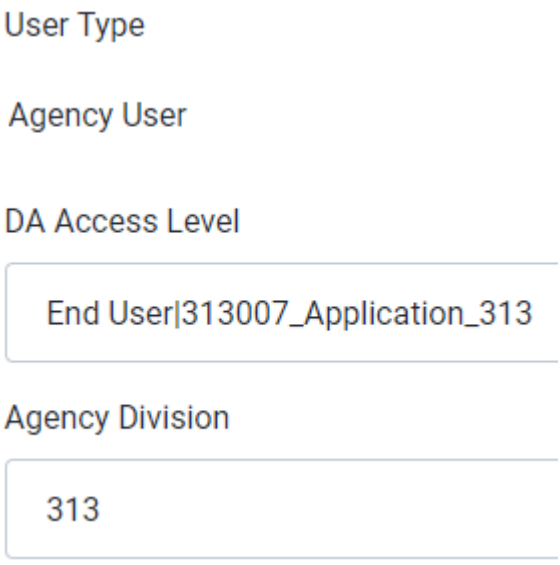
8. 

Figure 13. DA Access Level field contains two roles, with a | (pipe) separating the roles

9. Save to complete changes.

Enable/Disable an Account (Application Administrators only)

Enable User

Enable Application Access

Enabling and disabling application access allows or prevents a user from accessing their organization's application(s). They may have access to more than one application, or all access may be removed. Please note, that if a user has Admin access, the DA-Console role will appear in the User Roles field.

1. Navigate to the User's profile
2. Edit the User Roles field by adding "313007_SPECTRIM"

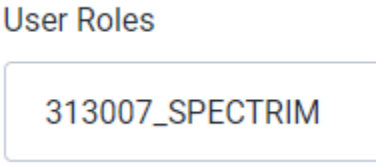
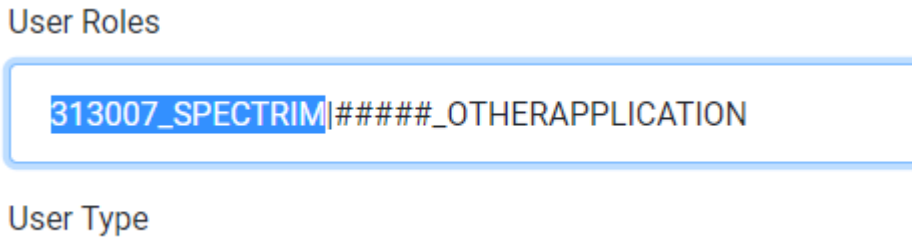
3. 

Figure 14. Enabling Application Access in User Roles field



4.

Figure 15. Enabling Application Access in User Roles field, when there are multiple applications listed

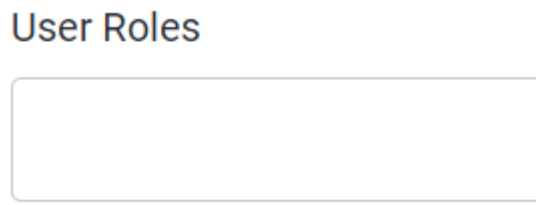
5. Click Save on the User Profile to complete

Disable User

Disable Application Access

Enabling and disabling application access allows or prevents a user from accessing their organization's application(s). Disabling a user's application access is helpful if the account needs to be disabled for a temporary amount of time (such as being on leave/vacation or if access needs to be disabled immediately). Please note, that if a user has Admin access, the DA-Console role will appear in the User Roles field.

1. Notify GRC@dir.texas.gov or submit a SPECTRIM Support Request (Request Type: Account Deactivation) to disable an account. If access must to be disabled temporarily or immediately, proceed to next steps.
2. Edit the User Roles field by removing "313007_SPECTRIM"



3.

Figure 16. Disabling Application Access in User Roles field (empty)

4. Click Save on the User Profile to complete

Resources

Texas.gov Digital Identity Solution Portal Login

https://myaccess.texas.gov/portal/

SPECTRIM Portal Login

https://dir.archer.rsa.com/

Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM) Webpage

https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting/statewide-portal-enterprise?id=136

DSTS Portal (ServiceNow) – Report an Incident

https://dirsharedservices.service-now.com/sp?id=sc_category&catalog_id=e0d08b13c3330100c8b837659bba8fb4

TDIS: User Guides (DSTS Portal)

https://dirsharedservices.service-now.com/sp?id=managed_docsv1&path=13539c551be02c90e933cbff1d4bcb25

TDIS: Admin Guides (DSTS Portal)

https://dirsharedservices.service-now.com/sp?id=managed_docsv1&path=13539c551be02c90e933cbff1d4bcb25

Support

Archer Support Requests

For SPECTRIM technical assistance submit a Support Request within the SPECTRIM portal or contact GRC@dir.texas.gov.

TDIS Support

If you experience a technical issue and are unable to resolve the issue, please contact the Shared Technology Services (STS) Help Desk, who will route the issue to the Level 4 Texas.gov Admin.

If it is a critical or high priority issue (P1 or P2), you should call the STS Help Desk immediately: (1-877-767-0656).

If the issue is non-critical or non-high priority (P3 or P4), you should contact the STS Help Desk via submitting an incident on the STS ServiceNow Portal Report an Incident page, use the chat feature on the STS ServiceNow Portal website, or send an incident report by email.

STS Helpdesk Contact Methods	Contact Information
Phone	1-877-767-0656 (for P1 or P2 issues)
Chat	Visit the STS ServiceNow Portal website.

Figure 17. STS Contact Table

Table of Figures

Version History

Version	Publish Date	Comments
1.0	2022-04-28	First publication

Figure 18. Version History Table