UNIVERSITY OF OREGON

Duo Admin Console Access procedure

Office: Information Service
Procedure Contact: Identity Management Engineer

A. Purpose

This procedure seeks to provide a mechanism for independent departments to request access to the Duo Admin Console with the Help Desk role.

Background

Duo was rolled out to all employees and students in the Spring of 2021. As part of the project the rolled out this new service, it was decided that the USS Tech Desk would support Level 1 and Level 2 support for users of the service. This was approved by Patrick Chinn, head of USS and Leo Howell, CISO.

The USS Tech Desk provides this support by logging into a tool called the Duo Admin Console. The Security team also uses this tool to troubleshoot security incidents. The tool has user roles, which dictate the authorization level of admin users. The roles used by the Tech Desk and Security are the following:

Group	Role	Description	More on current staff with Role
USS Tech Desk (Level 1)	Help Desk	Help Desk administrators can create, update, and delete user phones, tokens, and bypass codes; use directory sync to create or update a single end-user; send enrollment emails to users; modify full names, email addresses, and notes; change user status from "Locked Out" to "Active"; and can send Duo Mobile activations to users. Help Desk admins cannot manually create or delete users, modify usernames or user aliases; use bulk enrollment; or run a full directory sync. You can restrict Help Desk admins' ability to create bypass codes for users or send enrollment emails in Help desk settings. Help Desk administrators can view the Authentication Log, Telephony Log, Administrator Actions, and Policy Impact reports.	~20 student employees reporting to Katie Harsh. ~10 USS Directors reporting to Gary Sullivan.
USS Tech Desk (Level 2)	User Manager	The User Manager can create, update, and delete users, phones,	Account Services and Sara Stub's

		tokens, and bypass codes. The User Manager can also configure and run user directory synchronization. You can restrict User Manager admins' ability to apply bypass status to users in User manager settings. User managers can view the Authentication Log, Telephony Log, Administrator Actions, and Policy Impact reports.	direct reports. ~5 employees reporting up to Sara Stubbs
Security Team	Read Only	Admins assigned the Read-only role may view (but not modify) basic information about users, groups, phones, tokens, and applications, as well as view Trust Monitor security events and all reports. Read-only administrators may not access the Billing and Directory Sync pages.	~5 employees and ~5 student employees reporting to the CISO

More information can be found here: https://duo.com/docs/admin-roles

Data Security Risk

All roles can read the following types of Employee and Student data, making access controls a necessity:

- Cellphone numbers (as well has additional phone numbers added by user which can include Home and Work phone numbers)
- Cellular Device (model), device data, and cellular provider data
- First name, last name, and email address
- 2FA Token serial number information
- Activity data - when did users log into a service, from what IP address(es), and for what service(s)

This data is easily exportable from the system as CSV or PDF documents. While changes to data are logged in the audit records of the tool, there is no way to detect when a user copies, photos, or extracts the user data.

Quarterly Audits

Every three months, as each new term begins, Chris Bernard sends and email to the supervisors of those users with Duo Admin Console accounts. The email lists out the current users with access and asks the supervisor to respond with “approved” for the users to retain their access for the next three months. If during the term, the supervisor wishes to remove access from a departing resource or add access for a new resource, those change requests are tracked via email.

What Has Changed

The University has gone for a couple years with the above in place. This section will try to capture what has changed, resulting in the need for a new Procedure document.

In March of 2023, there have been three requests to have users from independent departments provided with access to the Duo Admin Console with the Help Desk role. After a couple of years of reaching out to USS for Duo changes to be made, these independent departments have decided they can provide better, faster service for their users if they fully avoid reliance on the USS team and access the Duo Admin Console directly.

The decision process around providing Duo Admin Access to independent departments is the classic "Usability versus Security" dilemma. Providing this access to these independent department staff will increase the usability of the service and produce faster resolution times for the employees and students in those independent departments. However, it will also allow more users access to all the Duo user databases, increasing the odds of the Duo data being wrongly distributed, shared, or utilized for non-approved reasons. The independent department staff with Duo Admin Console access would be able to see/modify/export ALL user data in the Duo system, not just the users of their own departments.

B. Definitions

Independent Departments - These are departments across campus which are not fully supported by USS. These include Housing, Athletics, PSI, and likely others. These units have their own IT staff helping employees and students and they do not rely on the Information Services USS organization for support in the same way as the rest of campus.

C. Procedure

When independent departments reach out requesting access to the Duo Admin Console, these are the steps to take:

1) Ensure the request is sponsored by the Directory/Manager of the unit and have them submit the request on behalf of their resource. Chris creates a TDx ticket to track the request and notifies Patrick Chinn and Jose Dominguez via TDx and Email.
2) Patrick Chinn (or USS delegate) reviews and approves the business need. Essentially, agreeing that the independent department staff can better serve their students and employees by having direct Duo Admin Console access instead of working with (and waiting for) the USS team to provide the same support.
3) Jose Dominguez, CISO, reviews the ask and approves the security risk. Essentially, agreeing that the person requesting the access should be trusted with the Duo data.
4) Chris Bernard, upon receiving approvals from Patrick and Jose creates the Duo Admin Console account for the user. In addition, Chris sends an email to the new user and their approving supervisor (key email content in below section). In addition, Chris provides Duo Admin Console user training for the user if requested by the supervisor.

Key email content to be included in the fourth step above includes:

> *It's important to call out that while the tool allows you to export this confidential data (save it off as a PDF or excel file), that is not an approved action. Please ensure the data is never exported out of the tool. We never want to deal with student name and cellular data being exported out of Duo*

> *onto a CSV and then shared on a cloud server where it can be accessed/seen by others, leading to a FERPA violation.*
>
> *Also want to note that the IS Security team asks that all actions taken within Duo have a corresponding ticket (tracked history in whatever ticketing system Matt uses), such that the action can be tied back to a ticket in the event of a security investigation.*
>
> *Quarterly, I'll be sending an email your way collecting your approval for this privileged level of data access.*

A copy of the above sent email and copies of the approvals from Patrick and Jose will be attached to a TDx ticket created by Chris Bernard in step one to track the provisioning of access.

Notes

We may want to include the Data Stewards in the process as well – or at least review this Procedure document with them and have them approve the Procedure.

This procedure may be revised at any time without notice. All revisions supersede prior procedures and are effective immediately upon approval.

D. Appendix

Revision History

Revision Number:	**Change:**	**Date:**
001	The initial procedure	7/6/2023