WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

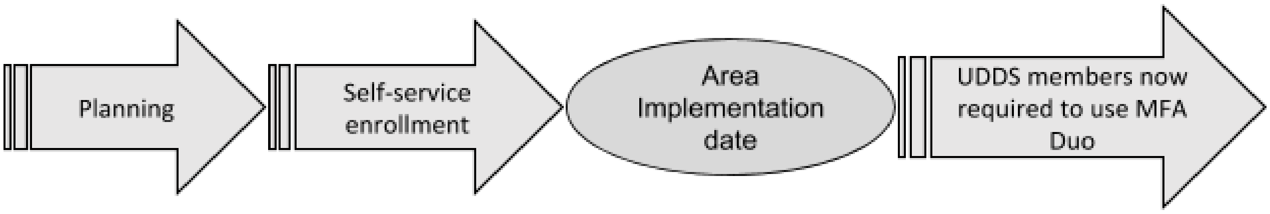
Area Onboarding Guide

Multi-Factor Authentication - Duo
Area: [x]
Implementation Partner: [x]
On Boarding Coordinator: [X]

This document is intended to be used to prepare for the implementation of Multi-Factor Authentication - Duo (MFA Duo) for NetID Login for an area or department.

This guide includes:

Process for onboarding groups for MFA Duo



Planning phase

During this phase, the **Onboarding Coordinator**[1] works closely with the area's **Implementation Partner**[2] to gather user implementation needs and plan the rollout.

[1] The Onboarding Coordinator is a member of the MFA Team responsible for working with Implementation Partner through the implementation of MFA Duo for their area.

[2] The Implementation Partner is a member of the area being onboarded for MFA Duo. Ideally this person is in a leadership position within the group and can make decisions about the onboarding for their area.

- The **Onboarding Coordinator** will make contact with the **Implementation Partner** to review this Group Onboarding Plan.
- The **Implementation Partner** answers the Pre-Implementation Questions, with guidance from the **Onboarding Coordinator**.
- The **Implementation Partner** selects an implementation date.
- The Onboarding Coordinator will explain to the Implementation Partner how to require MFA for users on the implementation date.
- The **Implementation Partner** will invoke the Communications Plan to alert users to self-enroll for MFA Duo.
- The **Onboarding Coordinator** will remain available to the **Implementation Partner** throughout the onboarding process to answer questions and help plan the rollout.

Self-service enrollment phase

During this phase, users will self-enroll for MFA Duo prior to the area's chosen Implementation date. After the implementation date, all employees in the UDDS will be required to use MFA Duo, unless otherwise exempt from enrollment.

- The **Implementation Partner** communicates to users about multi-factor authentication, self-enrollment, and known accessibility issues with the mobile application and tokens. See Communications Plan. The **Implementation Partner** lets their users know that additional support will be provided if use of the mobile app or token proves to be an access barrier to them before, during, or after implementation.
- The **Implementation Partner** assists users to self-enroll as needed. This includes those experiencing access and usability barriers. For more information, see the How to support employees who experience access or usability barriers section below.
- The **Implementation Partner** will use the MFA Implementation dashboard to monitor the self-enrollment process for their area.
    - Based on self-enrollment progress, we recommend that the **Implementation Partner** follow up with users who have not self-enrolled iteratively prior to the implementation date approaches.
    - If the Implementation Partner needs assistance in supporting users with access or usability barriers, they should reach out to their Onboarding Coordinator for additional guidance.
- The **Implementation Partner** will notify the **Onboarding Coordinator** if there are any members in the UDDS that should be excluded from using MFA Duo.
    - The following are examples of temporary exemption cases:
        - Employees who will be leaving the University prior to the University-wide implementation
        - Employees on temporary leave (maternity, FMLA, sabbatical, etc.)
        - Employees who are in the process of receiving more accessible support options (see the How to support employees who experience access or usability barriers section below).
- The **Implementation Partner** will distribute tokens to users that have requested them. Please be aware of known accessibility issues associated with the Duo token. While the

MFA team is investigating more accessible token options, employees who are in the process of receiving more accessible support options may be temporarily exempt. For more information, see the How to support employees who experience access or usability barriers section below).

Implementation

- Five business days prior to the implementation date, the **Onboarding Coordinator** will confirm with the **Implementation Partner** the following:
    a. Implementation date/time
    b. Area UDDS(s)
    c. Exclusions (if needed)
- On the selected implementation date and time, the **Implementation Partner** will add the appropriate UDDS(s) to the Manifest group. All members (less anyone who was excluded) will be required to start using MFA Duo for applications using NetID Login for authentication.

How to support employees who experience access or usability barriers

Employees navigating multi-factor authentication may encounter a barrier related to accessibility or usability. Some employees will identify that they are experiencing a problem immediately; others may not realize until they've used MFA for an extended period.

Users must be able to get assistance whether they identify as having a disability or not. We want to avoid a situation where people feel they need to disclose a disability in order to receive accessibility assistance. Employees should let their Implementation Partner know they are experiencing a barrier, and the Implementation Partner can contact their Onboarding Coordinator for additional guidance.

How to sensitively discuss barriers

When facilitating the identification of a barrier, be sure to focus on *what* the technical symptoms are that cause the barrier, rather than the reasons *why* the user might be having difficulty.

For example, focus on what barrier exists.

> **User**: “I’m having a hard time with MFA.”
> **Implementation Partner**: “Oh, let me help you then. What are you finding difficult?”
> **User**: “I can’t read my token code on this key fob, and the button is hard to press.”
> **Implementation Partner**: “I’m sorry that the key fob isn’t working well for you. Would you prefer to use the mobile app or a different device?
> **User**: “I don’t want to use my personal cell phone.”
> **Implementation Partner**: ”Then let’s get you a security key.” [Test security key with the user to ensure they are comfortable with it and no longer experience a barrier.]

Avoid pressing the user on reasons *why* the user might be having difficulty. Avoid using language that may cause the user to defend why they are experiencing the issue. This can lead to a self-disclosure of a disability, which can be an Americans With Disabilities Act (ADA) compliance violation.

Example of a non-compliant way of discussing a barrier.

> **User:** “I’m having a hard time with MFA.”
> **Implementation Partner**: “Oh, what’s going on?”
> **User:** “I can’t read my token code on this key fob, and the button is hard to press.”
> **Implementation Partner**: “Huh, that’s odd. Why is it hard to read? Can you show me?”
> **User:** “I can’t read my token code because I have partial blindness in my right eye and I just can’t see this code!”

It’s not uncommon for people to worry that they are unable to do something that they perceive others can. As a result, it’s easy for someone to inadvertently feel pressured to offer reasons why they are struggling. We want to help users feel comfortable and confident in their abilities so we don’t inadvertently pressure an employee to self-disclose a disability.

Duo MFA pre-implementation questions to answer

The following questions need to be answered by the Implementation Partner prior to MFA Duo implementation for a group.

1. What is the desired Duo MFA implementation date and time? We recommend a date prior to March 31, 2019 (UW–Madison deadline)
    a. Answer:

2. Duo MFA is implemented on a per UDDS basis, this means all employees who are members of the UDDS, unless otherwise exempt, will be required to use MFA Duo. What is/are your group’s UDDS(s)?
    a. Answer:

3. Are there members of your UDDS that should be exempt from the requirement to use Duo MFA? If yes, why and for how long? (e.g., upcoming retirements, employees transferring to another UDDS on campus, difficulty using the Duo token or app). Note: When exempting users due to accessibility, focus on the technical barriers being experienced by your users. See How to Support Employees Who Experience Access or Usability Barriers section above for details.
    a. Answer:

4. Do you expect your users will use a smart device for Duo MFA or will they need tokens?
    a. If tokens will be needed, approximately how many?
        i. Answer:
    b. If accessible tokens are needed, approximately how many?

i. Answer:

5. If a portion of users in your group need to pilot MFA prior to allowing the rest of the area to self-enroll, please supply their NetIDs and we will add them to an MFA manifest group.
    a. NetIDs:

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

MFA Duo Group Onboarding Communications Plan

This email communications plan is intended to be carried out by the **Implementation Partner** to notify their group of the upcoming MFA Duo implementation. We recommend also using in-person or other communication platforms to ensure all members of the UDDS are fully aware of the upcoming implementation.

Please feel free to modify the email templates to suit your area's specific needs.

Additionally at the end, we have shared with you the language that DoIT has adopted for use in our **letters of offer to job applicants**. We have included some context before and after the MFA paragraph to help you find the correct placement for your letters of offer. Pass this language on to your HR department to start using as soon as you have finished your implementation.

EMAIL #1- Send 2-4 weeks before implementation
FROM: Leadership of group/department
TO: Email list for departments/divisions moving to MFA Duo
SUBJECT: Changes to the NetID login process for improved security

Staff,

To better protect your personal identity and intellectual property, and to enhance the security of our digital assets, UW–Madison is adding a second verification step to the NetID login process. This process, called multi-factor authentication, is provided to campus by Duo Security and offers a second layer of protection to your digital identity. You may have seen a similar process in use at your bank, credit union or credit card company.

Implementing multi-factor authentication adds a new step to the NetID login process. The first step for UW–Madison login will remain the same, you'll enter your NetID and password. The second step uses your smartphone, tablet, or token (also called a fob) to verify your identity. Requiring two different types of authentication helps prevent anyone but you from logging in to your account, even if they have your password. The enrollment process is easy, using the free Duo app or token is simple, and results in added protection for your identity, intellectual property and UW–Madison assets. Learn more at: Guide: How to Use Multi-factor Authentication with Duo.

{Area/department name} employees will be required to use MFA Duo for access to applications using NetID Login for authentication on {Implementation date} at {Implementation time}. If you have questions about MFA Duo accessibility, see the MFA Duo - Accessibility Information KB or talk to {Implementation Partner} for additional resources.

What should I do now?
You can start using MFA Duo now, ahead of this date, by completing the MFA Duo Enrollment. If you do not have a smartphone or tablet (or choose not to use it) for MFA Duo, you can use a token. See MFA Duo - Accessibility Information KB for information about accessible MFA token options. If you need a token, contact {Implementation Partner}.

What if I already use Symantec OTP for access to HRS, SFS, OIM, PSVC/Phire, and UWBI systems?
Multi-factor authentication from Duo will replace the need for Symantec VIP for UW–Madison staff and faculty on February 28, 2019 for users who have migrated to MFA Duo. This impacts Human Resource System (HRS), Shared Financial Systems (SFS), Oracle Identity Manager (OIM), PeopleSoft Version Control/Phire (PSVC/Phire), and UW Business Intelligence (UWBI) at UW–Madison. Users who have enrolled in MFA-Duo will authenticate solely through their MFA-Duo device. Employees moving to MFA-Duo should keep their Symantec tokens until they receive further instructions.
For more information, including how to use MFA Duo, training videos, and FAQs, please visit the Multi-factor Authentication Project site. If you have any questions about the rollout, please contact {Implementation Partner}. If you have problems using MFA Duo, contact the DoIT Help Desk. If you have questions about MFA Duo accessibility, reference the MFA Duo - Accessibility Information KB and please contact {Implementation Partner} for additional support. If you'd like to share your thoughts, please use our Feedback Form.

Thank you,

{Sender Name}

EMAIL #2- Reminder for individuals who have not registered or completed their MFA Duo enrollment. We recommend that you send these reminders as needed. Be sure to exclude individuals who are exempt from enrollment at this time.

FROM: Leadership of group/department
TO: Email list that includes all staff in UDDS who are NOT using MFA Duo
SUBJECT: Set up your account for Multi-Factor Authentication-Duo (MFA Duo)

Staff,

On {Date email #1 sent}, I sent a message notifying you that you will be required to use Multi-Factor Authentication from Duo (MFA Duo) for accessing any applications using NetID Login for authentication starting on {Implementation Date}.

{Area/department name} employees will be required to use MFA Duo for access to applications using NetID Login for authentication on {Implementation date} at {Implementation time}

Our records indicate that you have not yet enrolled for MFA Duo. Please proceed with completing the MFA Duo Enrollment. If you do not have a smartphone or tablet (or choose not to use it) for MFA Duo, contact {Implementation Partner} to obtain a token.

For more information, including how to use MFA Duo, training videos, and FAQs, please visit the Multi-factor Authentication Project site.

If you have any questions, please contact the DoIT Help Desk. If you encounter access or usability barriers, see MFA Duo - Accessibility Information for known issues and workarounds, and please contact {Implementation Partner} for additional support.

Thanks,
{Sender name}

Tell us how we're doing: Use the Feedback Form.

Letters of Offer Language

NetID Activation email:
In order for you to have access to University email, calendaring and a number of other systems when you arrive, you will need to set up your UW–Madison NetID. Please do this as soon as possible. To do this, log into NetID Activation. It will ask for your Activation Key (xxxx-xxxx-xxxx-xxxx) and your date of birth. Then follow the rest of the activation steps.

You will then need to set up your multi-factor authentication account with Duo. Duo is UW–Madison's multi-factor authentication service, which adds a second step to your NetID login to verify your identity and prevents others from accessing your account. Visit our help document to get started. You can register with a smartphone, tablet or token. If you experience access or usability barriers, see the MFA Duo - Accessibility Information KB for information. Once you register your smartphone, tablet and/or token, you will be enrolled in using Multi-Factor Authentication (Duo) starting on your first day of employment.

After you set up your NetID and multi-factor authentication, set up your preferred primary email address. (...)

Manifest Group Management

Requiring individuals to start using MFA (performed by implementation partners):

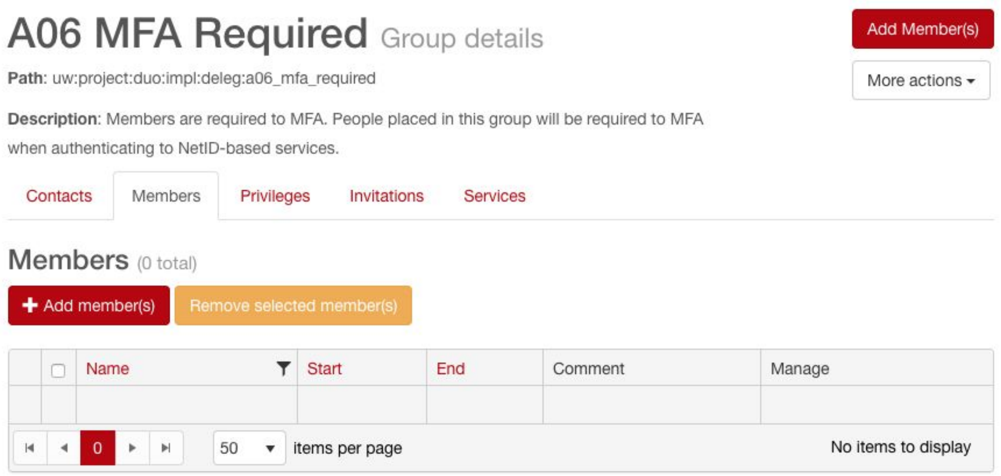
Note: Adding people to the MFA_Required group will require them to start using MFA at their next login. Be sure that your individuals are ready to start using MFA before adding them to this group.

Also Note: The MFA_Required group for a division is restricted to only take effect for individuals within that UDDS. Individuals outside of that UDDS may be added, but will be filtered out and MFA will not be enforced for them.

1. Log in to https://manifest.services.wisc.edu

2. Under "Groups I Manage' find the MFA_Required group for their division's UDDS. It will take the form of:
    'uw:project:duo:impl:deleg:a06_mfa_required'
   Where 'a06' is the UDDS of your division. (Example)
   You can also paste the above path into the 'Quick Launch' box on the left.

3. On the Group Details page, select the 'Group Members' tab:



A06 MFA Required Group details

Path: uw:project:duo:impl:deleg:a06_mfa_required

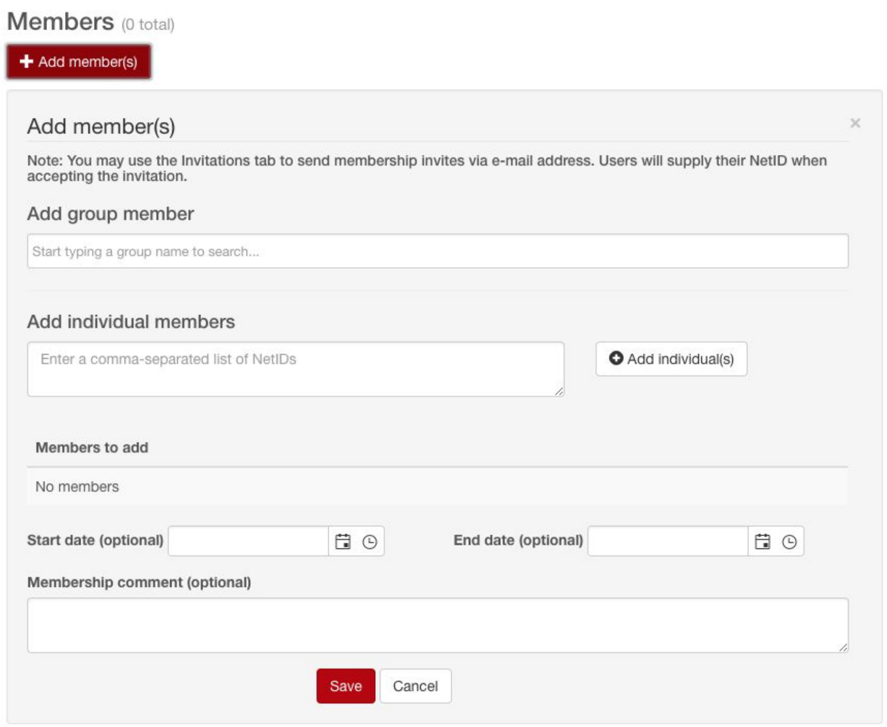
Description: Members are required to MFA. People placed in this group will be required to MFA when authenticating to NetID-based services.

Members (0 total)

No items to display

Figure 1: A06 MFA Required Screenshot
Screenshot showing the group details of an example "MFA Required" manifest group.

4. Select 'Add Members'. You will see the following:



Members (0 total)

+ Add member(s)

Add member(s)

Note: You may use the Invitations tab to send membership invites via e-mail address. Users will supply their NetID when accepting the invitation.

Add group member

Start typing a group name to search...

Add individual members

Enter a comma-separated list of NetIDs

Add individual(s)

Members to add

No members

Start date (optional)

End date (optional)

Membership comment (optional)

Save Cancel

Figure 2: Add Members Screenshot
Screenshot showing how to add members in an example “MFA Required” manifest group.

a. To add individual members, enter their netids into the box labeled ‘Add individual members’.

b. To add groups, enter the group name into the box labeled ‘Add group member’
    i. If you already have Manifest groups you’d like to enable for MFA enrollment (pilot groups, etc), they can be added here.
    ii. If you would like to add groups by UDDS, you may enter them here as well. These groups should take the following form:
        ‘uw:ref:hr_system:udds:A067140’
    where A067140 is the UDDS you would like to require to MFA.

c. Select ‘SAVE’. The group member(s) you’ve added will be prompted for MFA. Please note that there may be a delay of up to 15 minutes while group memberships are updated before the individual starts to be prompted.

Implementation Partner Dashboard Reporting on Enrollment

Your Onboarding Coordinator will give you access to the Implementation Partner Dashboard where you can track the progress of your UDDS group(s) as it relates to the DUO implementation.

MFA Duo Online Resources

MFA Duo Project Website
MFA Duo Training Website
MFA Duo - Accessibility Information KB
How to use MFA Duo
MFA Duo Frequently Asked Questions
MFA KnowledgeBase