Departmental Duo Integrations

Requests and Fulfillment

Requests for Duo integration with departmental systems and applications should be sent to help@uw.edu with a subject line of “Duo integration consult.” This will create a UW Connect request for the Identity and Access Management (IAM) team. An IAM Specialist will initiate a consultation with the requestor to determine if Duo is a good fit.

User Eligibility

Requestors should be aware of current Duo eligibility policy so they can assess whether the intended population for an integration is covered. Current eligibility policy is posted at https://itconnect.uw.edu/security/uw-netids/2fa/faq/. Contact IAM via help@uw.edu if you have questions about user eligibility.

User Enrollment

Although some Duo integrations support a user interface for enrolling users, this feature is disabled by policy. All users must enroll in Duo via https://identity.uw.edu/2fa.

UW NetID Namespace

Duo provides a second authentication factor based on the UW NetID namespace. In general, Duo integrations require that the departmental system or application use UW NetID for primary (password) authentication. In some circumstances, a Duo integration may be feasible for systems and applications that don’t use UW NetID for primary (password) authentication, if the local account namespace is synchronized with the UW NetID namespace.

Integration Contacts

One or more departmental contacts will be recorded for each integration. These contacts will be used for notifications concerning changes to the service that could impact integrations. It is the responsibility of the department to notify IAM about changes to contacts. Use of a team email list is recommended to ensure continuity of communication when staffing changes.

Integration Credentials

A departmental system or application must authenticate to initiate Duo 2FA for its users. Duo integrations use an assigned application key and secret key to authenticate. These credentials are scoped to a single integration type and a single domain of administrative control. The departmental contacts may use the same integration credentials on any of their systems or applications with the same integration type.

Credential Protection

Integration credentials (application key and secret key) must be protected from disclosure to any individuals outside the departmental IT team. If there is evidence or suspicion that the credentials have been compromised, contact IAM via help@uw.edu so old credentials can be revoked and new ones issued.

Service Reliability

Duo’s service operates in the cloud and is designed for high availability and geographic redundancy across multiple data centers. Duo’s SLA (https://duo.com/legal/sla) specifies 99.9% uptime. Current Duo operational status is always available at https://status.duo.com/, where the UW’s Deployment ID is Duo40. Components of the 2FA service operated by UW-IT are covered under UW-IT’s Geographic Resiliency Program and are also designed for high availability and geographic redundancy across data centers.

Outages

Any service can experience occasional outages. It is strongly recommended that departmental contacts subscribe to Duo’s incident notification service to receive the most timely and detailed updates on outages. Sign up at https://status.duo.com/. Details of past outages are available at https://status.duo.com/history. Departmental contacts should report Duo outages to help@uw.edu. Status information for significant Duo outages will be published to the UW community via the UW eOutage service (https://eoutage.uw.edu/).

Fail Open Option

Many Duo integrations provide an option to fail open or fail closed in the event of a Duo outage. When an integration fails open, Duo 2FA will be skipped and users will gain access to the system or application using only primary (password) authentication. When an integration fails closed, users will not be able to access the system or application until Duo service is restored. Configuration of this option resides on the client side and departmental contacts should make a choice based on their own unique security requirements. It is best to think through this before an outage occurs.

2FA Vendor Commitment

Duo is the UW's third 2FA vendor. As the 2FA marketplace evolves and matures in the future, other solutions may become more compelling than Duo. Should the UW decide to add new solutions or replace Duo, reasonable notice will be provided to departmental contacts so they can plan accordingly. Keep in mind that there is no guarantee any particular Duo integration type will be supported by all solutions and other vendors.