Gradient StealthMFA™

Service Description

EXECUTIVE SUMMARY

Gradient StealthMFA prevents identities from being compromised by cyber attackers. When deployed to a SAML or OIDC-based IDP, it becomes the authentication for user identities in the IDP such that only the actual user from their trusted system(s) is able to authenticate to the IDP and any third party applications federated with that IDP. Theft of digital credentials becomes infeasible with Gradient StealthMFA.

SERVICE DELIVERY TEAMS

- Customer Deployment Team (CDT): The CDT is a team of Gradient Engineers responsible for providing onboarding support to customers during the deployment of Stealth MFA within their environments. StealthMFA CDT will not interact with customer owned systems (such as the native IDP) but will perform configuration on the Gradient-side SaaS systems to facilitate deployment to the customer environment.

- Customer Success Manager (CSM): The CSM is the primary point of contact responsible for facilitating onboarding, conducting business performance reviews, and addressing ad-hoc requests such as policy adjustments, rule creation, and integrations.

- Gradient Engineering (Eng): The Engineering team works behind the scenes to support the service, ensure compliance with SLAs, and perform feature enhancements, bug fixes, and R&D for new integrations and products. Eng does not operate in a customer-facing capacity unless by request for a specific use-case agreed to by both the customer and CSM.

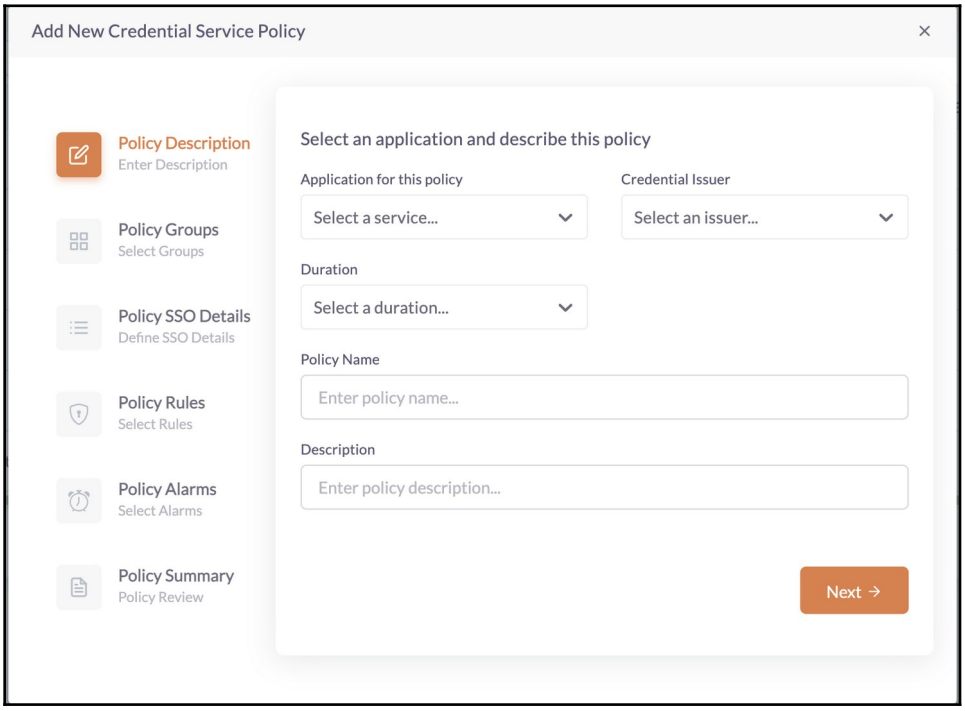
SERVICE DELIVERY

StealthMFA Manager Console (SMM): The Console is a web-based user interface that provides real-time visibility of all devices to which Gradient is deployed, all users, registration (aka association) of devices with users, and the credentials in place to access applications using StealthMFA.

- Credentials: The SMM Console includes a Credentials tab where all credential and access related information and configuration capability can be accessed and used by a Console Administrator. There are three sections related to credentials
    - *Applications*: This tab shows all applications that are integrated with Gradient. By default, customers are deployed with two integrations: 1) Their IdP (e.g., Okta, Ping, etc.) via SAML or OIDC and the SMM. Please contact your customer success manager to discuss additional applications and best practices for integration with Gradient.

    - *Policies*: Policies is where the SMM Administrator can take a high level access policy and create a Gradient policy to enforce it at the technical level. Policies are created on a per

application basis. Admins can then specify which credential should be used to enforce access for this policy (e.g., for an application that is federated with Okta, the admin can specify that the default Okta IDP credential is used OR that a Gradient credential is used). The admin can then configure the lifetime of that credential (how often it should be rotated/renewed to continue access).



Admins can then configure the policy to apply to specific groups of users (where groups are inherited from the native IdP).

○ *Rules*: Rules are the technical enforcement mechanisms for Policies. In the context of SMM, Rules are logical conditions that an underlying device must meet in order to allow policy to issue and renew credentials for access. Rules are written in GoLang and require deep knowledge of the underlying device to ensure proper operation. Customer Success should be contacted before modifying any out of the box rules in your environment.

- Endpoints: The Gradient Console allows admins to view all Endpoints within the environment. Note that Gradient defines an endpoint as the combination of a user and a device, so when viewing the endpoints tab, administrators will see a username along with a device name and a state describing whether or not that endpoint is active (able to receive and renew credentials) with the Gradient backend. Administrators can also see groups of endpoints in a separate tab, and take action on any of these tabs to change the state of the endpoint.

- Users: The Gradient Console's Users tab allows the Administrator to see information on the directory (or directories) that are the source of truth for user information and group membership within the customer organization. Gradient is designed to work with your existing Identity Provider and Directory/Group structure by inheriting it and then apply Gradient policies at the device level. Gradient is not intended to be used to create new groups of users that exist outside of your source of truth for user information and group membership.

  Within the OTP (One-Time Password) Registration (aka Associations) tab, an administrator can push an OTP to any user within the system that a user can use to register an endpoint to their identity.

- Settings: The Gradient Customer Portal provides a settings tab for configuration by system administrators.

Gradient API: The Gradient Application Programming Interface (API) provides access to the data elements visible in the console, enabling integration with ticketing systems, Security Orchestration and Automated Response (SOAR) tools, security information and event management (SIEM) systems, and other platforms where appropriate.

Self Service Portal (SSP) Add-On: Customers may choose to purchase a Self Service Portal (SSP) as an add-on to the Gradient StealthMFA Service. The SSP is a web portal hosted at <customerID>.gradient.tech that is designed to integrate as a Service Provider (SP) with the customer's SSO. End-Users are able to use the customer's existing SSO authentication methods to authenticate to the SSP. Once authenticated the end user will be able to download the Gradient StealthMFA client application to their device, then return to the SSP to click an Activate button which uses their SSO session with the SSP to register their device with their SSO account. Customers may also build their own integrations that allow the Activate button to change a custom attribute for the user inside the SSO that then switches the SSO authentication method to Gradient StealthMFA. NOTE: such modification of attributes within the Customer's SSO is outside the scope of Gradient services and performed by the Customer.

Workforce Kiosk StealthMFA (Sold Separately): Gradient Workforce Kiosk StealthMFA (WFK) is an alternative version of the StealthMFA product (sold separately) that is designed for MSFT Windows Kiosks. This version allows multiple SSO users to authenticate from the same kiosk device using a four (4) digit Personal Identification Number (PIN) to differentiate between users of the device. Users' SSO

identities are still anchored to the device using ephemeral credentials as defined below. Workforce Kiosk Stealth MFA supports up to 2200 users of the same Windows Kiosk device. WFK integrates seamlessly with the StealthMFA SMM portal and runs side by side with standard StealthMFA deployments within the same SMM console. WFK Endpoints are clearly differentiated in the SMM portal by operating system type and by the number of users to which the device is registered.

KEY FEATURES

Seamless Access: Gradient StealthMFA integrates with your existing identity providers using Single Sign On (SSO) and Federated Application Access to provide a seamless and secure authentication experience to these systems. Instead of a user typing a username and password into a form and then waiting to confirm via second authentication factor (such as a text message, prompt from an app, or touching a physical device), the user simply selects the application they wish to access, confirms their username, and is seamlessly granted access.

Access to applications for a given user is determined by the customer's existing Identity Provider (e.g., Azure Active Directory, Okta, etc.). The customer configures their identity provider, using Gradient onboarding documentation, to delegate the authentication of users and groups of users to Gradient. Specifically, customers may onboard Gradient such that only select users and groups use Gradient as the form of authentication.

Credential Rotation: Gradient's primary security feature is the automated rotation of credentials. In particular, for SAML or OIDC based IDPs with SSO (e.g., Azure AD, Okta, etc.), Gradient establishes a Gradient Credential (anchored to the device as described below). This credential then forms the basis of a secure connection to the Gradient hosted IDP Service, which then interacts with the Customer's IDP to perform Authentication flows for the User's session with the Customer's IDP. The Gradient Credential can be rotated at a configurable interval to ensure the continued security of the connection with the Gradient IDP. The customer can then configure their native IDP (e.g., Okta, Azure AD) to rotate sessions at the same frequency as the Gradient credential.

Credential Anchoring: On systems that contain a hardware root of trust that contains at least one keypair and identifier unique to the device, Gradient can use these elements to bind credentials to the device such that credential removal from the device will make them inoperable. In particular, Gradient binds the Gradient credential (issued to ensure a secure connection between the device and the Gradient Service) so that the Customer's authentication via Gradient to their native IDP (e.g., Azure AD, Okta, etc.) can only happen from the user's device.

Device Attestation: Gradient collects various measurements from the device that describe its state. Gradient uses these measurements to identify and verify the device.

X.509 Certificate Issuance (PKCS#11 and CNG): Gradient issues and device-anchors X.509 certificates and exposes them through the operating system's native cryptographic interfaces — PKCS#11 on Linux and

Cryptography API: Next Generation (CNG) on Windows 11. This enables standards-based use of Gradient-anchored key material for browser client certificates, Policy Enforcement Point (PEP) consumption, Certificate-Based Authentication (CBA), and mutual TLS (mTLS), without changes to the consuming application. As with all Gradient credentials, these certificates are bound to the device's hardware root of trust and are subject to Gradient credential rotation and anchoring.

Attestation-Only Mode (Entra ID): For Microsoft Entra ID customers, Gradient can be deployed in an attestation-only configuration in which Gradient does not issue or rotate credentials. Gradient attests device state approximately every ten (10) minutes using TPM Platform Configuration Register (PCR) measurements; when a monitored PCR changes, Gradient revokes the affected user's Entra sessions across all of that user's devices, with revocation taking effect in accordance with Microsoft Entra's session-revocation SLA. This capability is available only for Entra ID customers.

COMMUNICATION AND CUSTOMER ENGAGEMENT

The following standard methods are available to the Customer in order to successfully deliver the service:

- Gradient Customer Console (SMM): The Gradient Console is the primary method by which Customers can stay informed of the security posture of their environment.

- Email: Customers can initiate support requests via email to their CSM. Support Services are described below and on our public support page.

CUSTOMER ONBOARDING

The Customer's engagement and responsiveness will drive the onboarding process. The detailed description of the onboarding process can be found on the Gradient Customer Support portal.

Point of Contact: The Customer will provide email and phone contact information for the "primary escalation point-of-contact" as well as the primary owner of the Customer's Identity and Access Management program.

Rate of Onboarding: Gradient requires one business day to initiate onboarding and instantiate a SaaS instance of the SMM Console and endpoint deployment packages. Once the endpoint packages are ready, Gradient's endpoint software can be onboarded as quickly as allowed by the Customer's Desktop support (e.g., Endpoint Engineering) processes and technology allow. Customers then may choose the rate at which they both deploy Gradient software, convert users to Gradient authentication, and perform user-device registration (aka association) via OTP, API, or manually in SMM.

Addition or Removal of Net New Endpoints and Users: There are multiple scenarios in which a Customer may wish to add a new user, a new device, or remove one or both of those object types:

- Onboarding of a new user, or onboarding of a new Group via Merger or Acquisition

- Removal of a user or group due to termination, divestiture, or downsizing
- Provisioning of access for a user via a temporary device (e.g., a “loaner” laptop)
- Upgrading a user to a new device (device management lifecycle)

SMM enables an administrator to perform each of the above through the user and device pages. Note: Gradient is a credential-issuance based system. When access for a target user or group is “removed” via the Gradient console, SMM stops the provisioning of credentials for the target. Any credential that has been issued prior to “removing” access will continue to provide access until that credential expires, where the expiration time is determined by policy configuration in the Policy tab of SMM. Because Gradient facilitates seamless credential renewal, we recommend configuring credential renewals/rotation to the minimum possible setting allowed by the environment (e.g., 10 minutes for SAML 2.0+ applications).

SERVICE LEVEL AGREEMENTS, MAINTENANCE and SUPPORT

This Service Level Agreement sets forth the policies and procedures with respect to services provided by Ares Technologies, Inc. DBA Gradient Technologies ("Gradient") to a customer ("Customer") pursuant to a Master Services Agreement between Gradient and Customer (a "Customer Agreement").

Service Level Agreement Table

Definition	**Service Level Agreement**	**Notification Method**
Platform Availability: Availability of the SaaS platform to provide services that enable authentication and continual credential renewals	Gradient will use commercially reasonable efforts to: 1. Maintain 99.9% Platform Availability during Scheduled Availability Time, as measured throughout the calendar year (the "Uptime Guarantee"); 2. Notify Customer within one (1) hour of identification by Gradient of an outage and provide hourly updates until such outage is resolved.	1. Email

"Scheduled Availability Time" is defined as twenty-four (24) hours a day, seven (7) days a week, excluding: (i) scheduled maintenance, upgrades and repairs; (ii) downtime during an Emergency Maintenance Window (as defined below); (iii) downtime due to acts of Customer or any third party connections, systems, utilities, or equipment; and (iv) downtime related to any other forces beyond the reasonable control of Gradient (such as internet outages or outages with respect to the Customer's network or internet access); and (v) downtime caused by force majeure events, including without limitation: acts of God, natural disasters, war, terrorism, civil unrest, embargoes, labor disputes or strikes (other than those involving Gradient employees), epidemics or pandemics, governmental actions or restrictions, or failure of third-party infrastructure (including but not limited to power, telecommunications, or hosting providers) outside of Gradient's reasonable control. All scheduled maintenance will be conducted between the hours of 12:00 am EST and 5:00 am EST, provided that Gradient may, in its sole discretion, plan additional scheduled maintenance, which will be communicated to the Customer (by email) at least 24 hours in advance. Gradient will use commercially reasonable efforts to minimize any disruption, inaccessibility and/or inoperability of the Service in connection with outages, whether scheduled or not.

SLA Credits: Customer will be eligible for an "SLA Credit" for any failure by Gradient to meet the Uptime Guarantee. Customer must request an SLA Credit within thirty (30) days after the relevant failure and must be in compliance with all of its obligations under the Customer Agreement to receive an SLA

Credit. Gradient will research the request and respond to the Customer within thirty (30) days from the date of the request, and if in Gradient's reasonable determination Customer is entitled to an SLA Credit, such credit will be applied to the Customer's next billing cycle and calculated as set forth below against the monthly service fees due during such billing cycle. The SLA Credit shall be the Customer's exclusive remedy, and Gradient's sole liability, for failure to meet the Uptime Guarantee.

Actual Services Uptime Percentage	**SLA Credit Percentage**
≥ 95.0% but < 99.9%	5% of Monthly Fees
≥ 90.0% but < 95.0%	10% of Monthly Fees
< 90.0%	15% of Monthly Fees

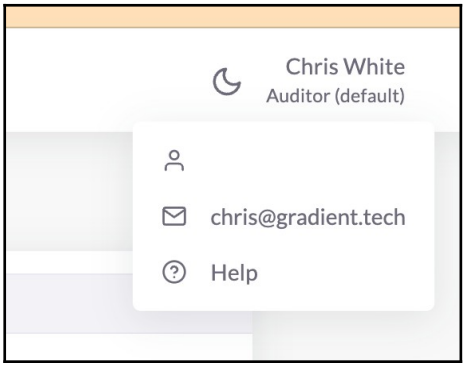
Emergency Maintenance: When immediate changes are required, Gradient may initiate an "Emergency Maintenance Window." When this situation occurs, Gradient will use commercially reasonable efforts to provide notice and minimize the impact to Customers. Emergency Maintenance Windows are not included in Scheduled Availability Time, and any corresponding interruption in service will not be eligible for an SLA Credit.

ENTERPRISE SUPPORT SERVICES ("SUPPORT")

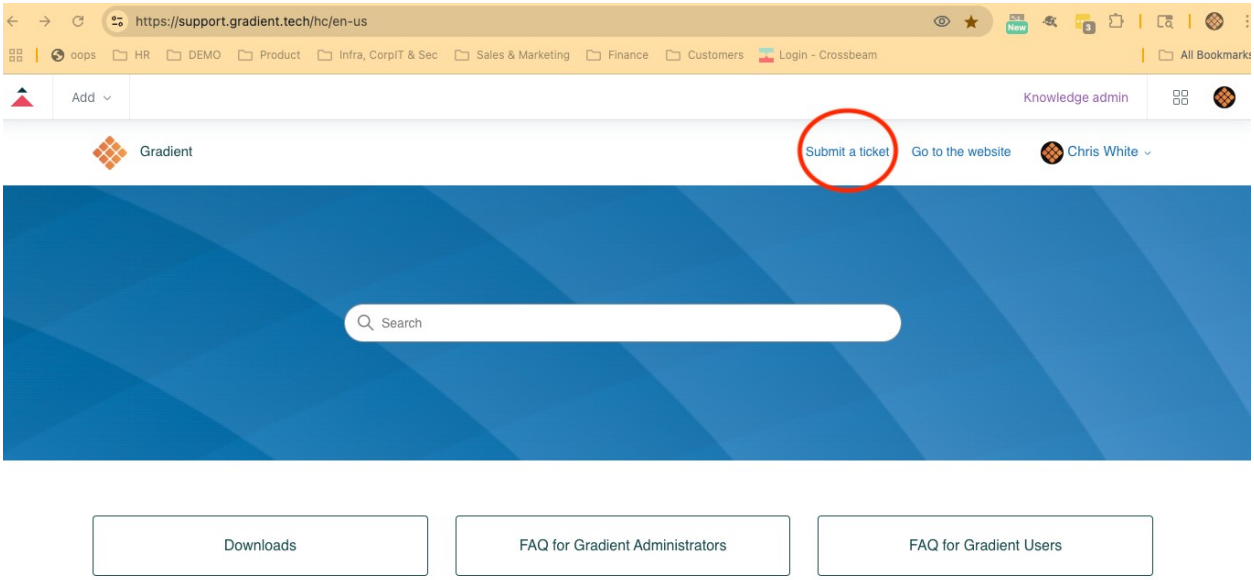
Gradient is designed to be frictionless and intuitive to use for both end users and administrators alike. Explanation of Console features for administrators is explained above, and also via pop-up windows whenever an administrator hovers their mouse cursor over most labels within the Console. However, support requests may come up in several circumstances:

1. Troubleshooting Customer deployments of agents on devices OR assistance with IDP integration
2. Customers request assistance to modify Console Applications, Rules or Policies
3. Feature requests
4. Bug fixes
5. Other

Feature Requests and Bug Fixes (items 3 and 4) are integrated directly into the Console. Admins can submit a Feature request or bug fix via the Help section under the user's account:



Followed by clicking the “Submit a Ticket” link in the upper right of the support.gradient.tech page:



Support requests may be submitted via email either to your Customer Support Manager or via support@gradient.tech for items 1,2 and 5 above.

If your Service Subscription Includes **Enterprise Support (per user)**, users may submit logs and support tickets directly through the agent desktop icon in their system tray by clicking “Report a Problem.” This feature helps the user collect logs locally from their machine and email them to the Gradient case management system, where a ticket will be opened on their behalf. Customers ***may choose*** to automatically CC one of their own IT Administrators for inclusion on the end user’s ticket.

Support tickets can be submitted in any language, but will be responded to via English, Spanish, French, Italian, Portuguese, Indonesian, Arabic, German, Chinese (simplified), Korean, Japanese, Hindi, and Bengali.

While Gradient has achieved a <15 minute average acknowledgement time on End User Tickets, Service Level Agreements for Support Services and Scenarios are formally described via the following table:

Support Service Level Agreement Table

Customer Service Request	**Acknowledgement**	**Resolution**
Troubleshooting Device Deployments/IDP integration	Gradient support will use commercially reasonable efforts to respond within one (1) business day to acknowledge the support request and begin support	Gradient will use commercially reasonable efforts to troubleshoot and resolve the issue within 5 business days of Acknowledgement
Assistance with modifying		Gradient will use commercially

rules		reasonable efforts to resolve the issue within 10 business days of Acknowledgement
Other		N/A

NOTE: Gradient will not honor support requests nor provide support services unless the customer has taken best efforts to provably determine that Gradient technology is causing a business disruption, and includes a summary diagnostic with the request.

OUT OF SCOPE

This Service does NOT include capability relating to:

- Securing (Rotating, Anchoring, etc.) any other form of Credentials such as SSH, Web Tokens, Cookies or any others not explicitly mentioned above.