Gradient Cybersecurity Mesh: Zero Trust Access for SSO

Service Description

EXECUTIVE SUMMARY

Gradient Cybersecurity Mesh (GCM): Zero Trust Access (ZTA) for SSO prevents SSO identities from being compromised by cyber attackers. When deployed to a SAML-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 GCM: ZTA for SSO.

SERVICE DELIVERY TEAMS

- Customer Deployment Team: The CDT is a team of Gradient Engineers who provide onboarding support to customers during deployment of GCM within their environment. GCM 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, ensuring compliance with SLAs, performing 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.

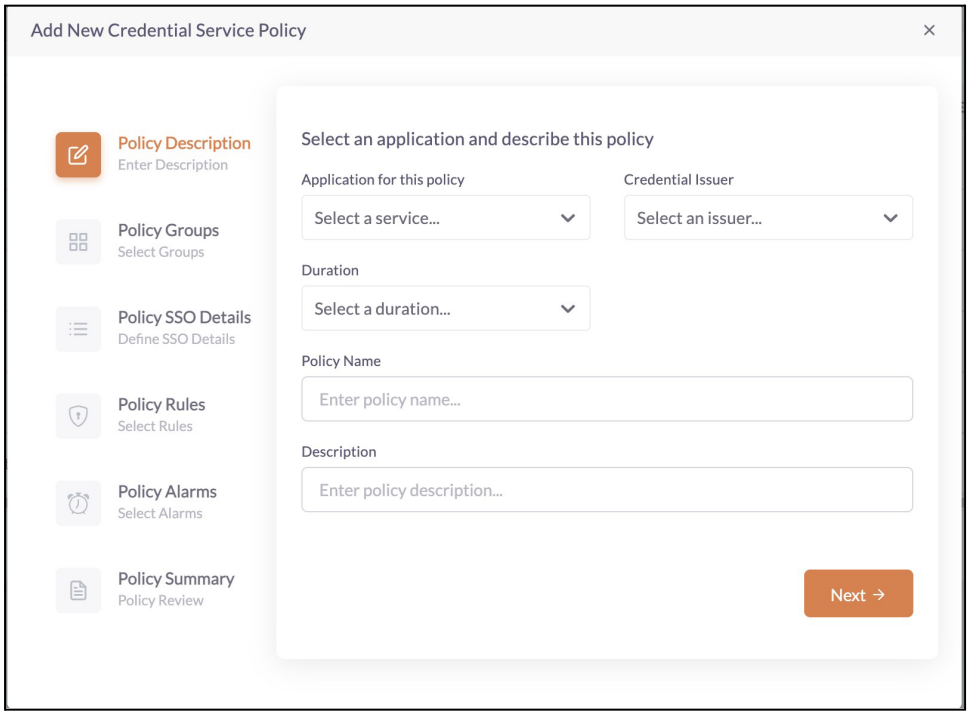
SERVICE DELIVERY

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

- Credentials: The GCMM 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 SAML IdP (e.g., Okta, Ping, etc.) and

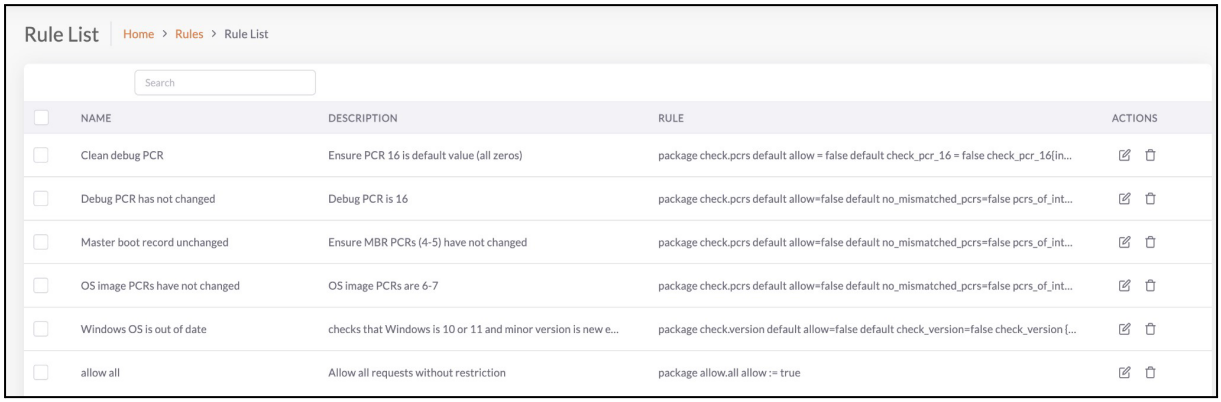
the GCMM (currently referred to as SMM in the Console). Please contact your customer success manager to discuss additional applications and best practices for integration with Gradient.

○ *Policies*: Policies is where the GCMM 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 Policy. In the context of GCMM, 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) Associations tab, an administrator can push an OTP to any user or group within the system. This is particularly useful when adding new endpoints in bulk using groups from your existing identity provider.

- 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) system, and other platforms where appropriate.

GRADIENT

KEY FEATURES

Seamless Access: Gradient 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 user-name, 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 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 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 then continually (at an interval configurable via Policy) validates that these measurements have not changed. If measurements have changed, Gradient will not allow credentials to be renewed to the device.

COMMUNICATION AND CUSTOMER ENGAGEMENT

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

- Gradient Customer Console (GCMM): 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.

CUSTOMER ONBOARDING

The Customer's engagement and responsiveness will drive the onboarding process. The detailed description of the onboarding process is here.

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 GCMM 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 association via OTP.

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)

GCMM 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, GCMM stops the provisioning of credentials for the target. Any credential that has been issued prior to "removing" access will continue to have access until that credential expires, where the expiration time is determined by policy configuration in the Policy tab of GCMM. 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).

GRADIENT

SERVICE LEVEL AGREEMENTS AND MAINTENANCE

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 IDP services and 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 2. Gradient Console

"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, 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). 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. Customer 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.

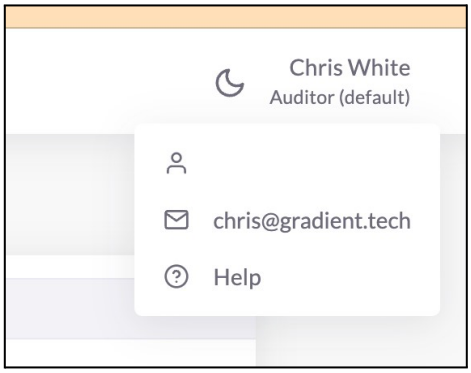
GRADIENT

SUPPORT SERVICES

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 rules for attestation and other conditions for credential issuance
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:



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. Service Level Agreements for Support Services are 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 2 business days to acknowledge	Gradient will use commercially reasonable efforts to troubleshoot and resolve the issue within 5 business days of Acknowledgement

Assistance with modifying rules	the support request and begin support	Gradient will use commercially 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 within 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, x.509 Certificates, Web Tokens, Cookies or any others not explicitly mentioned above. Each such credential is covered by a separate service description available at gradient.tech/contracts.