
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

PRT015

SPONSORED BY ERMETIC

JIT privileged access management for cloud infrastructure

Lior Zatlavi

Sr. Cloud Security Architect
Ermetic

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ermetic's cloud security platform



Identity

- Visibility to identities and entitlements
- Misconfigurations
- Privileged identities
- Excessive privileges and least privilege
- Provisioning and JIT access



Network

- Visibility to network components
- Misconfigurations
- Reachability analysis
- Visualization
- Segmentation
- Anomaly network access detection
- Unusual network access management (IAM)



Data

- Discovery
- Map sensitive data
- Misconfigurations
- External exposure
- Excessive privileges and least privilege recommendations
- Unusual data access



Compute

- Misconfigurations
- Kubernetes best practices, compliance, and RBAC
- Application identity privileges (analyze area of impact)
- Excessive privileges and least privilege recommendations
- Network exposure
- Anomaly detection



Runtime

- Vulnerability assessment for VMs and containers
- Secrets
- Malware scanning
- Network configuration
- SSH keys



Secrets

- Hidden in cleartext
- External exposure
- Excessive privileges and least privilege recommendations
- Unusual secret access

This talk is here

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Service vs. human identities

Service identities

- Consistent, predicted behavior
- Suited for right-sizing based on logged activity
- Permissions requirements seldom change

Human identities

- Unpredicted (by design)
- Very hard to right-size properly to specific resources and/or actions
- Elevation is sometimes required

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Humans are (also) vulnerable

Mismanage static access keys

Prone to social engineering

- Phishing (MFA doesn’t fix this!)
- Corruption

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

JIT access

Out-of-bound permissions; limited time, specific purpose

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

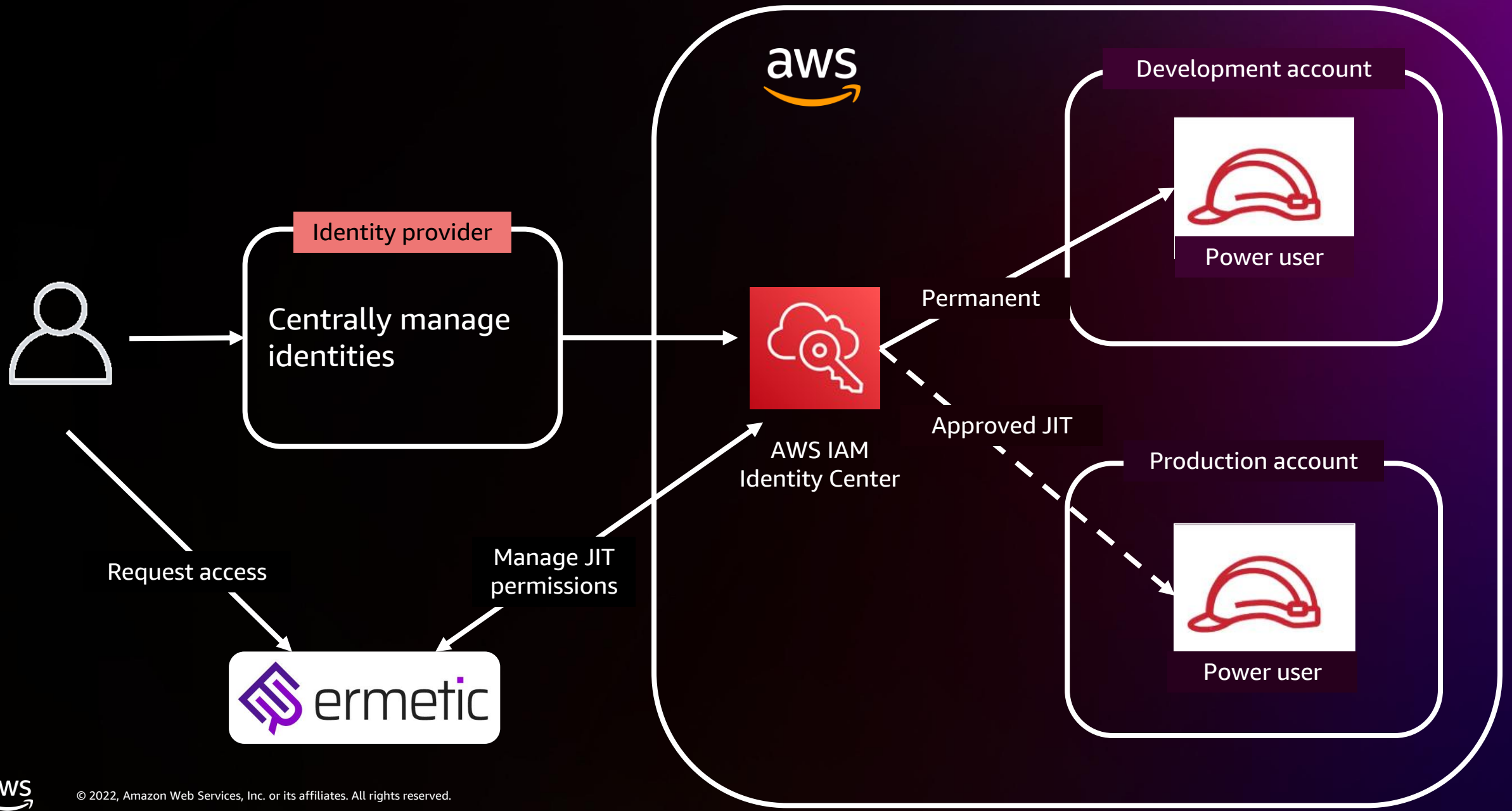
Zero standing trust

THE MISSING PIECE OF CLOUD ENTITLEMENT MANAGEMENT

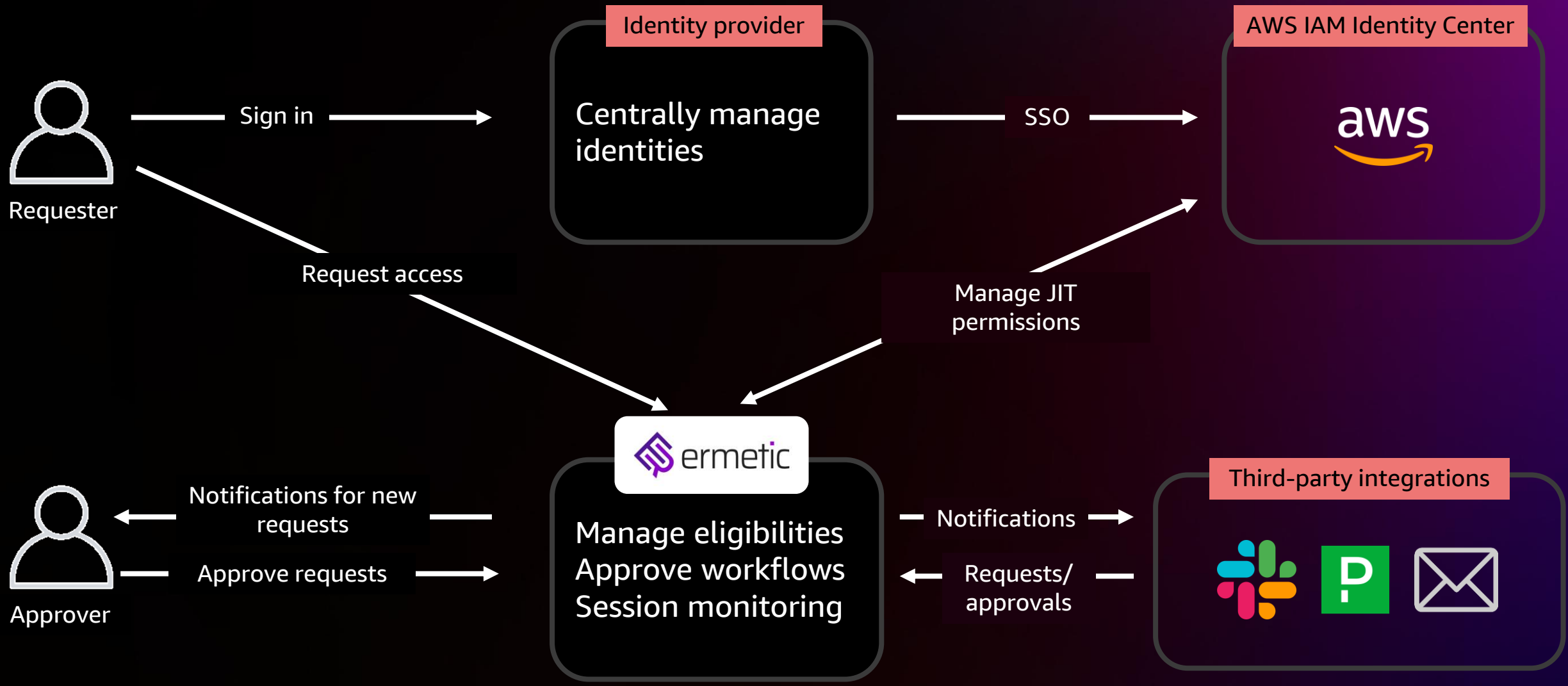
- Minimal/no permanent (“standing”) permissions
- User may be made “eligible” to receive additional one-time permissions
- When needed, requests can be made based on a business justification
- Approval can be granted for specific duration and then revoked

aws

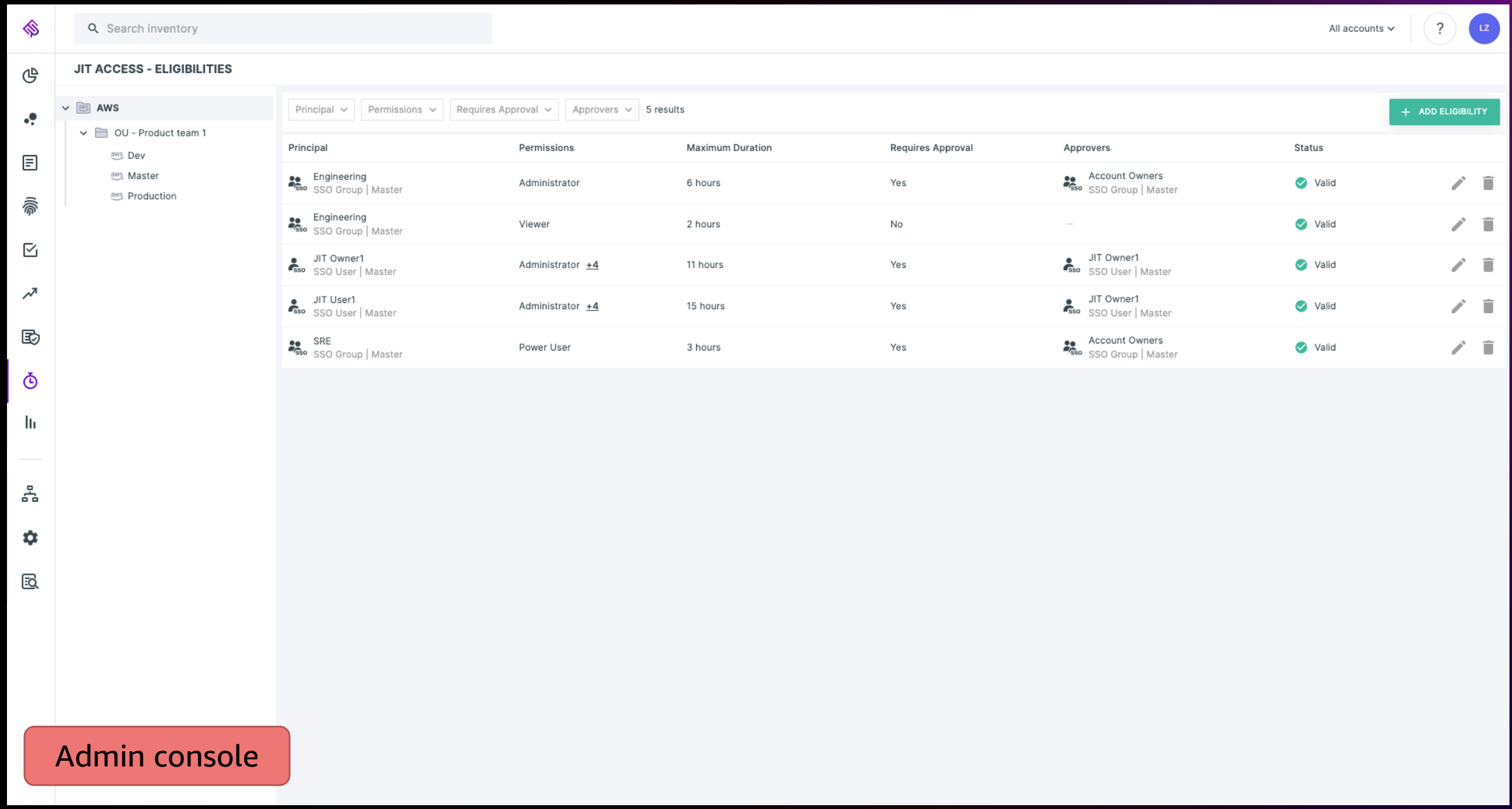
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

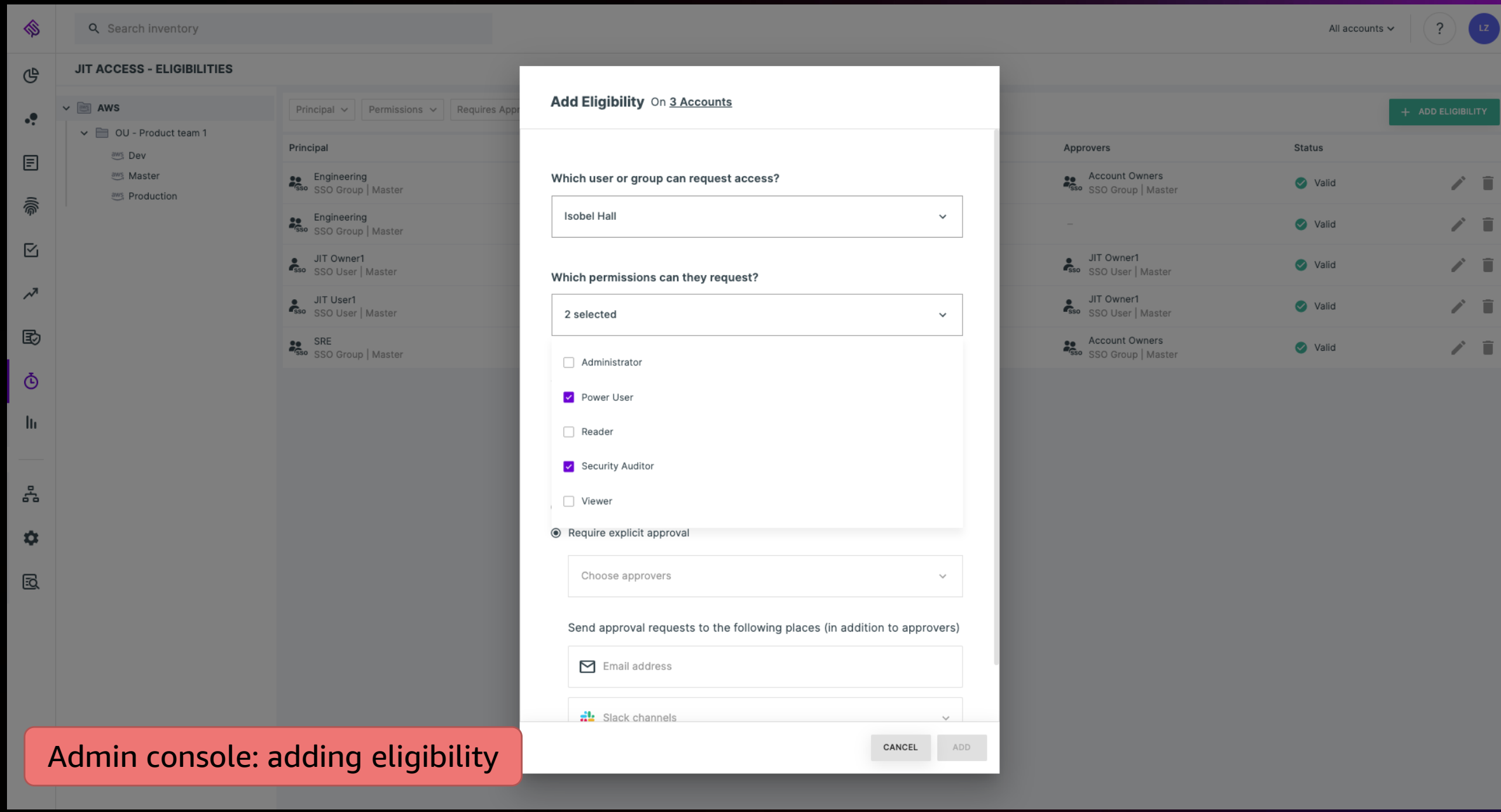


aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



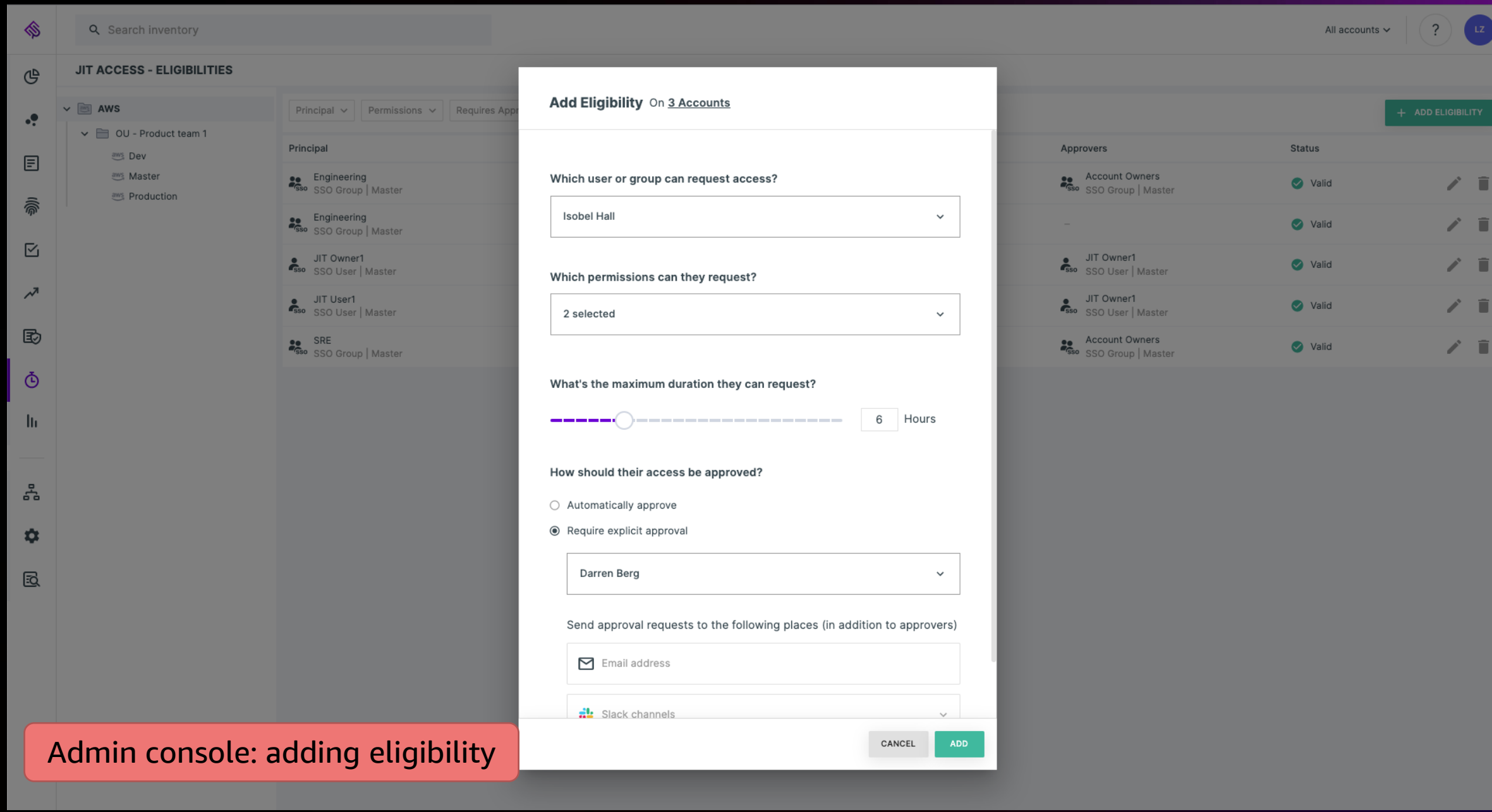
Admin console

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



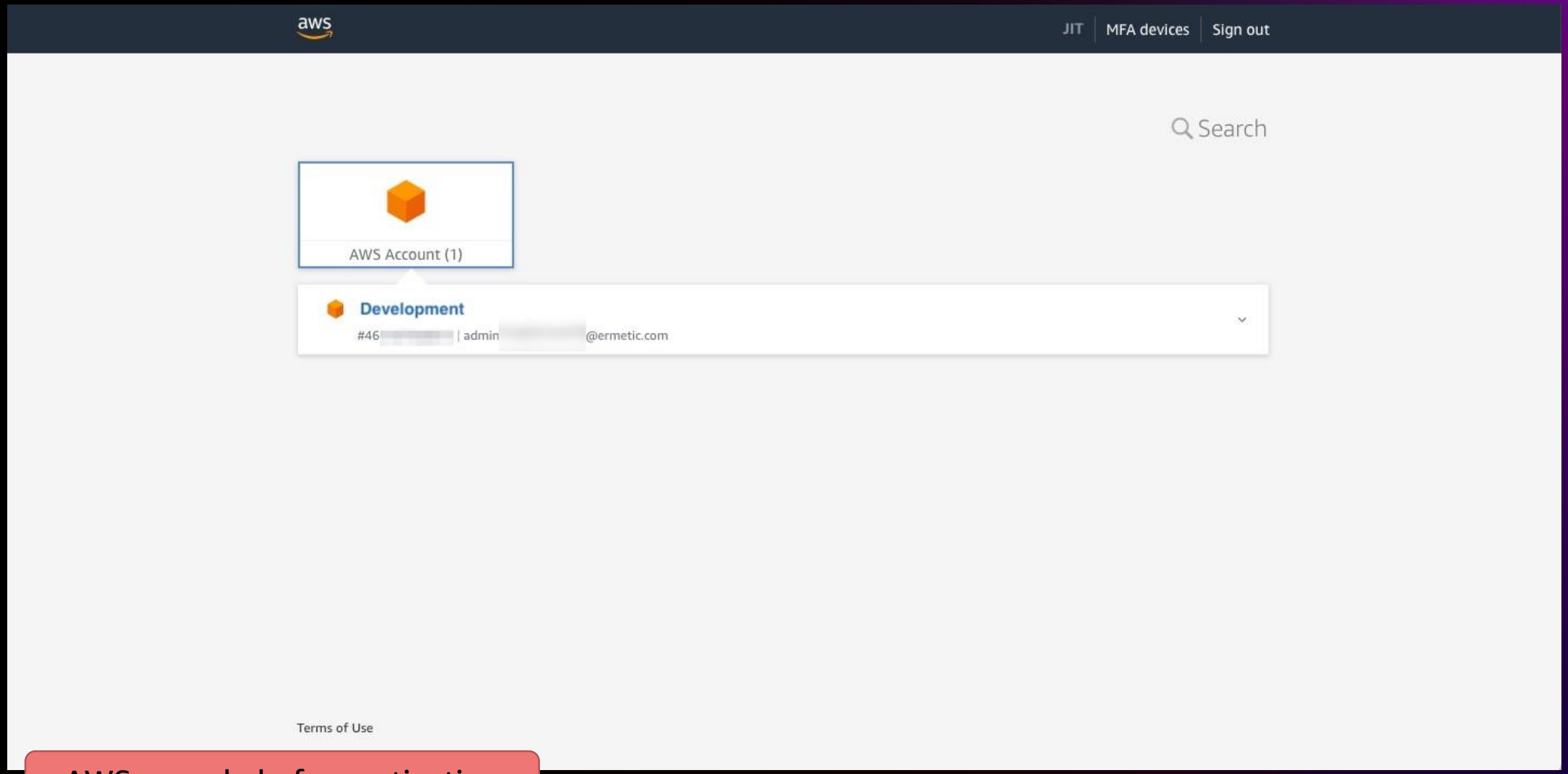
Admin console: adding eligibility

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



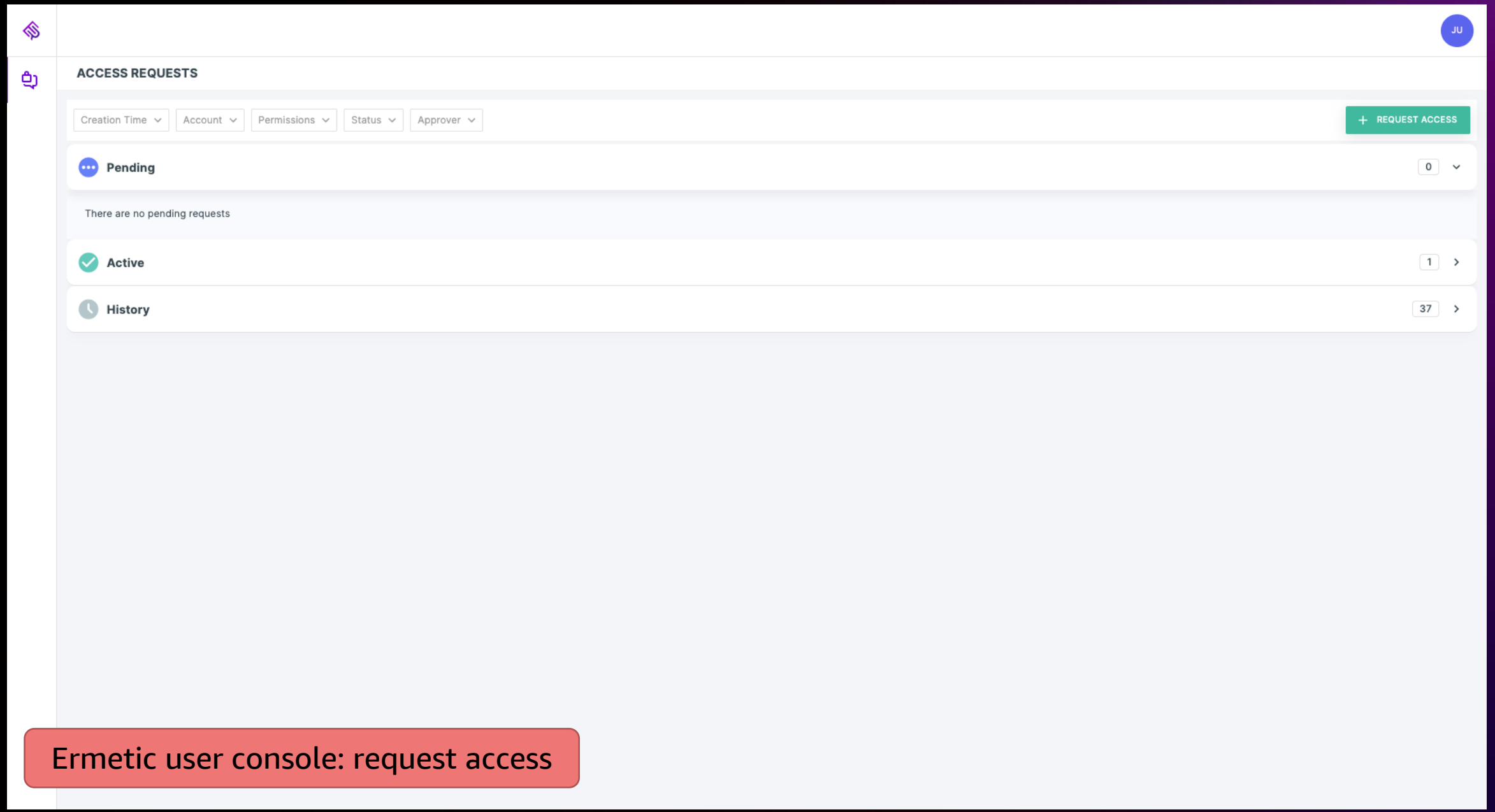
Admin console: adding eligibility

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



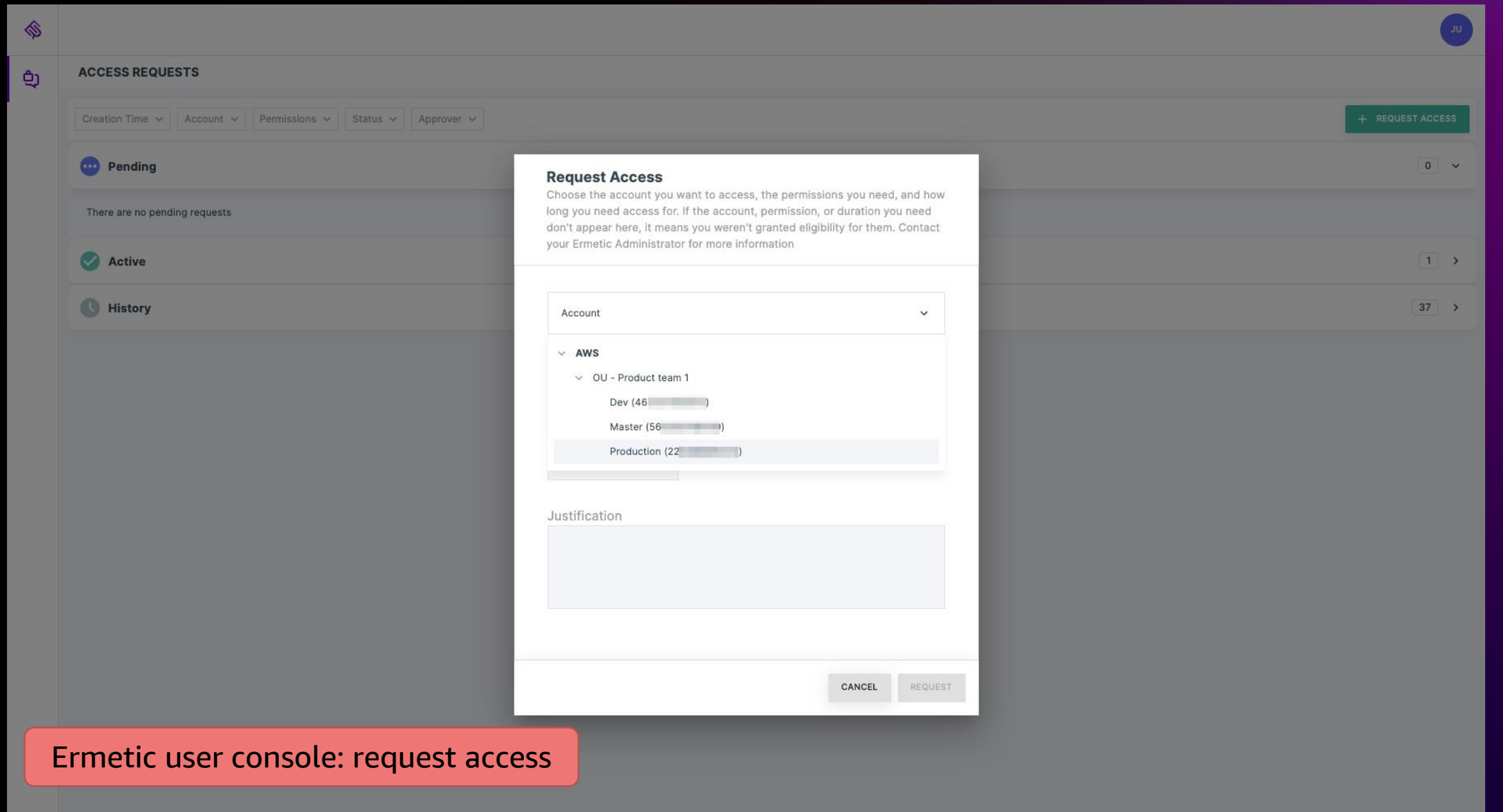
AWS console before activation

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



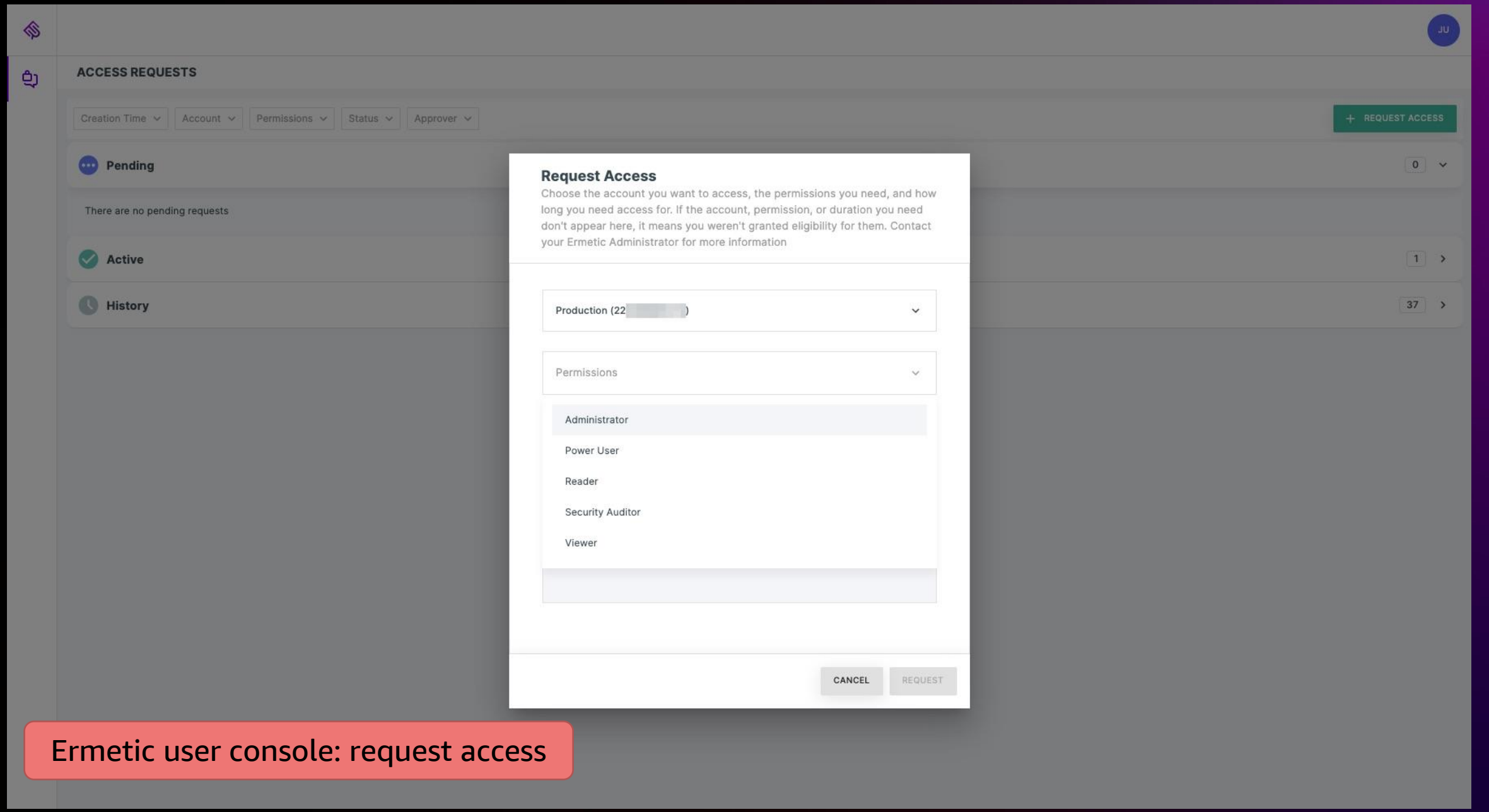
Ermetic user console: request access

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



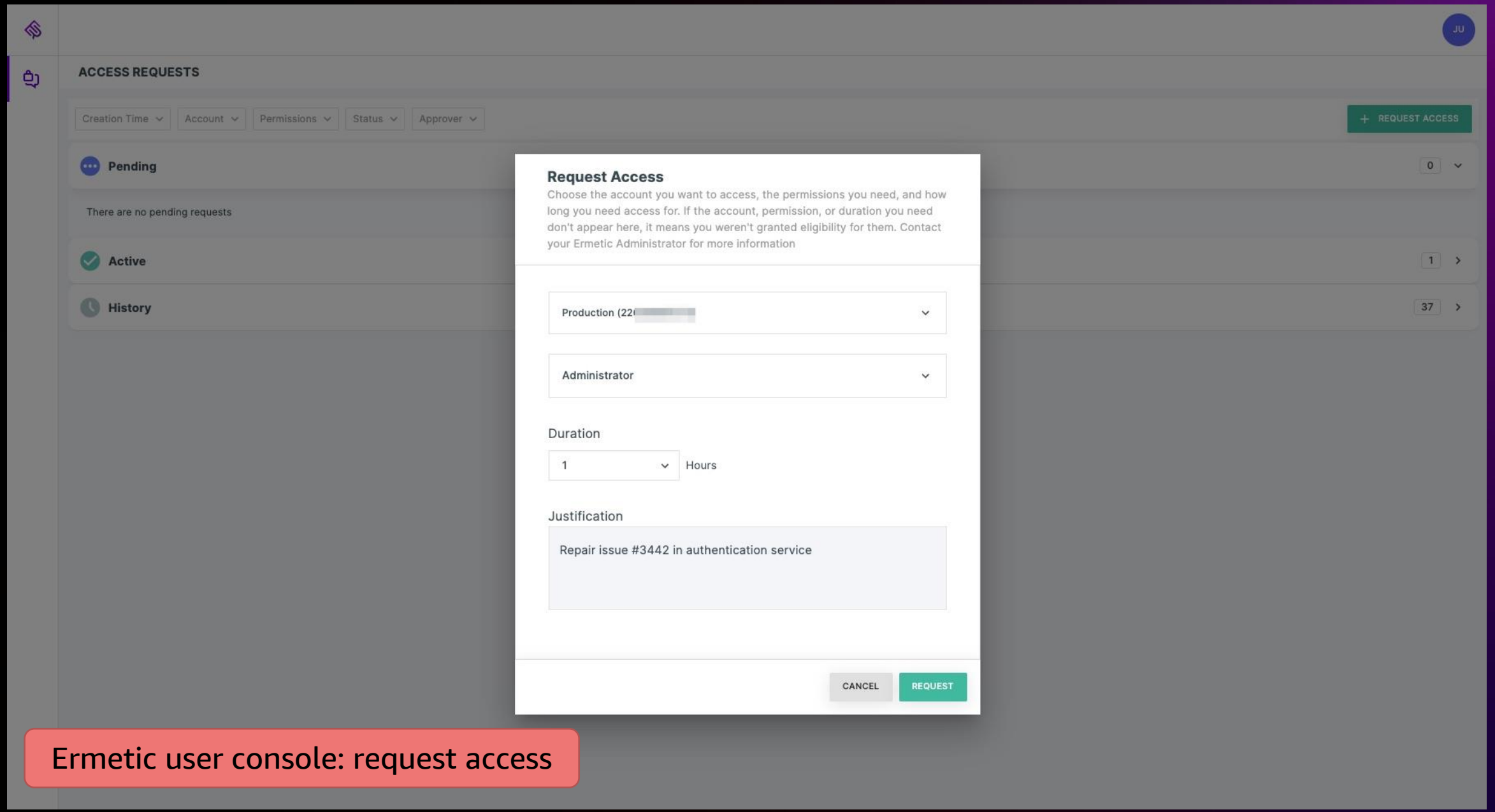
Ermetic user console: request access

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



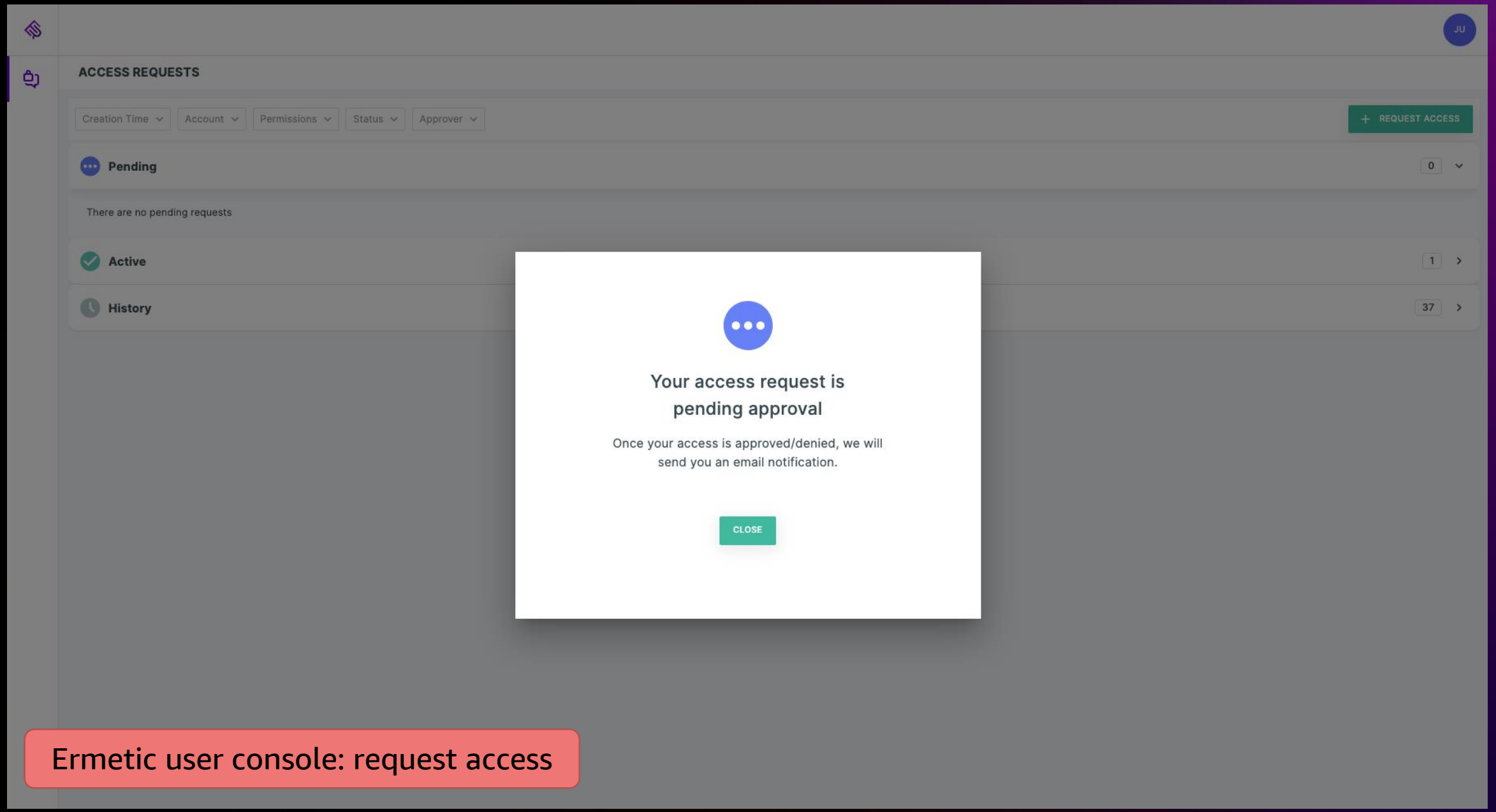
Ermetic user console: request access

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



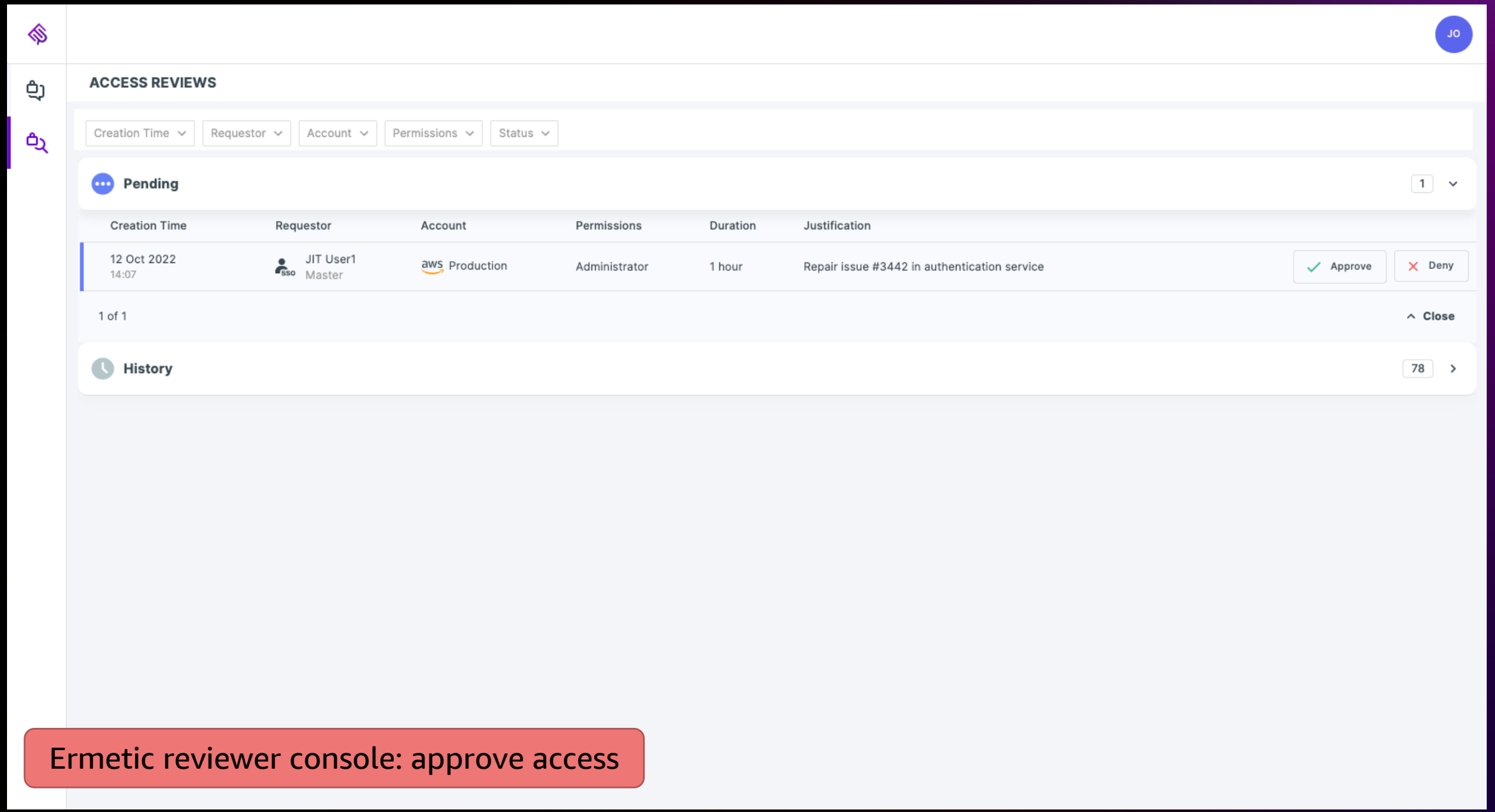
Ermetic user console: request access

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



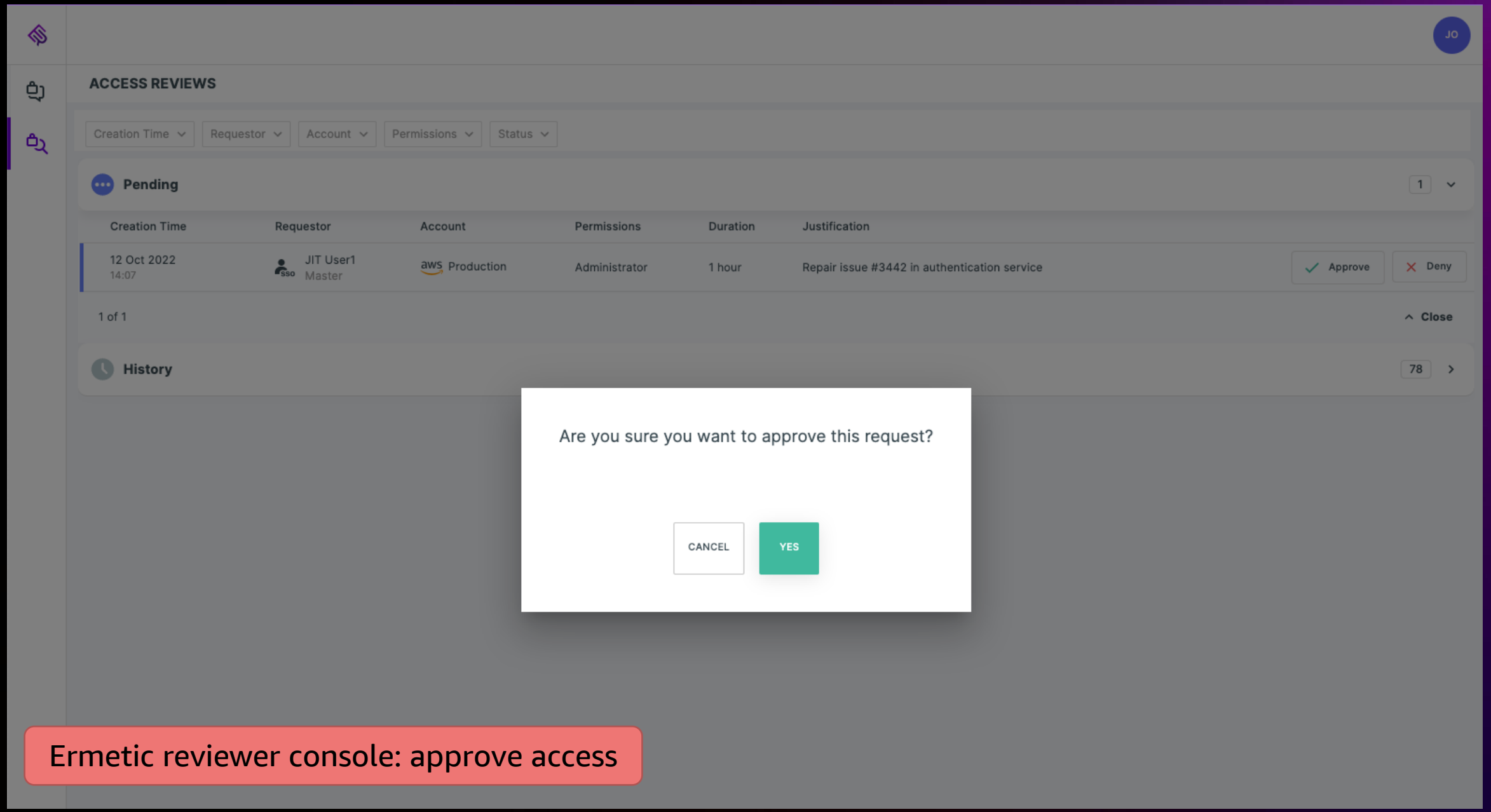
Ermetic user console: request access

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



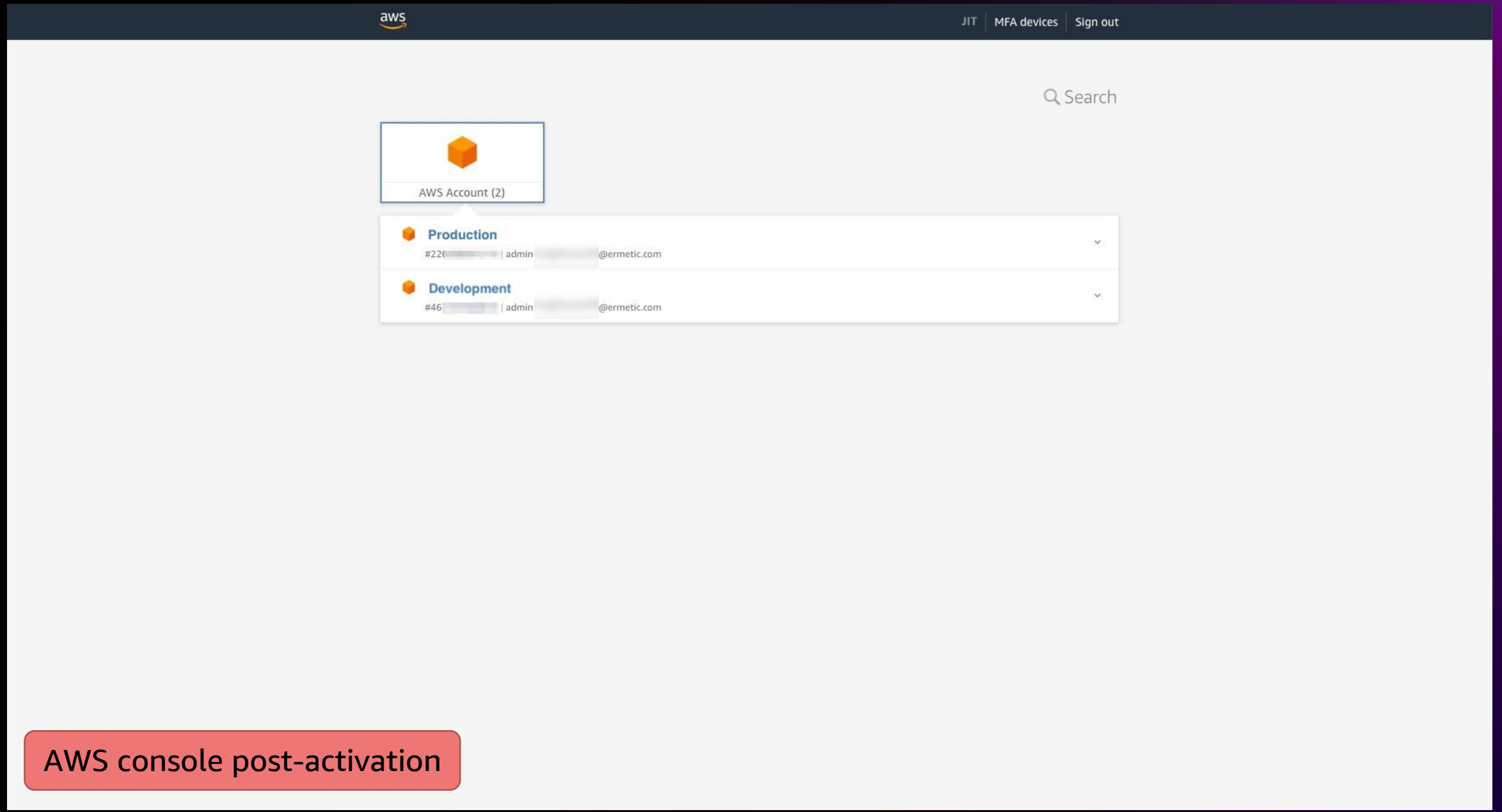
Ermetic reviewer console: approve access

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



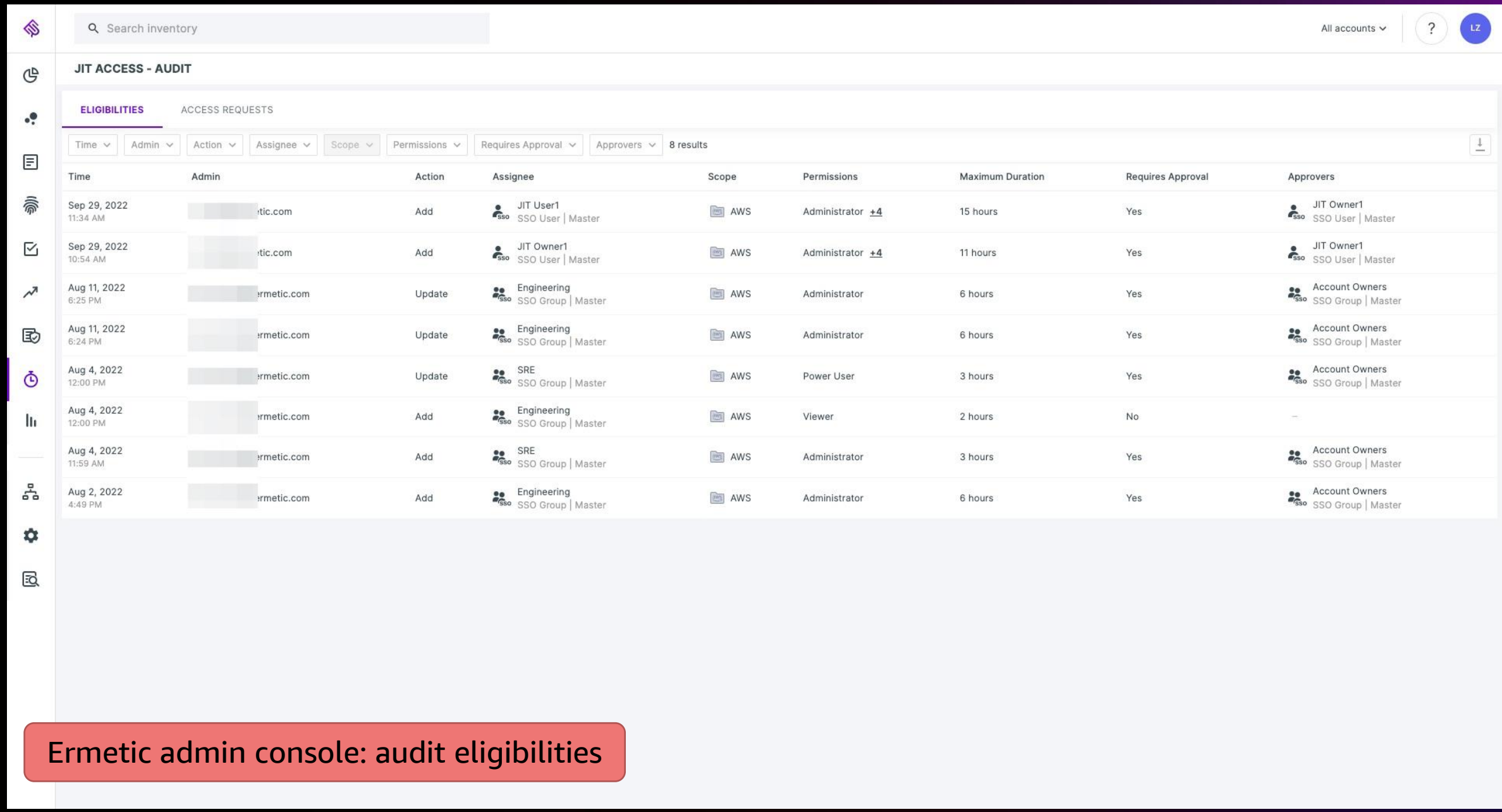
Ermetic reviewer console: approve access

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



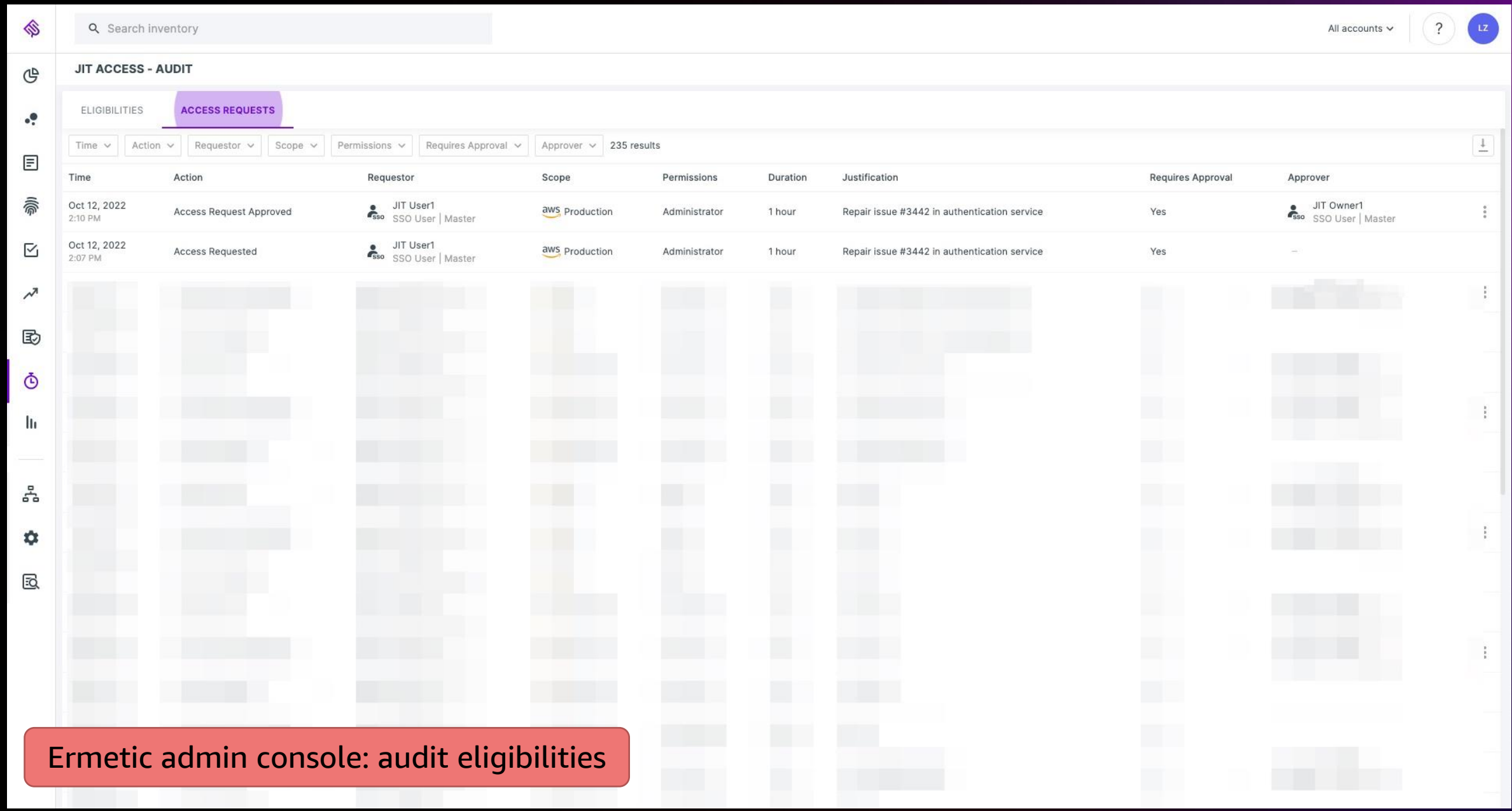
AWS console post-activation

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



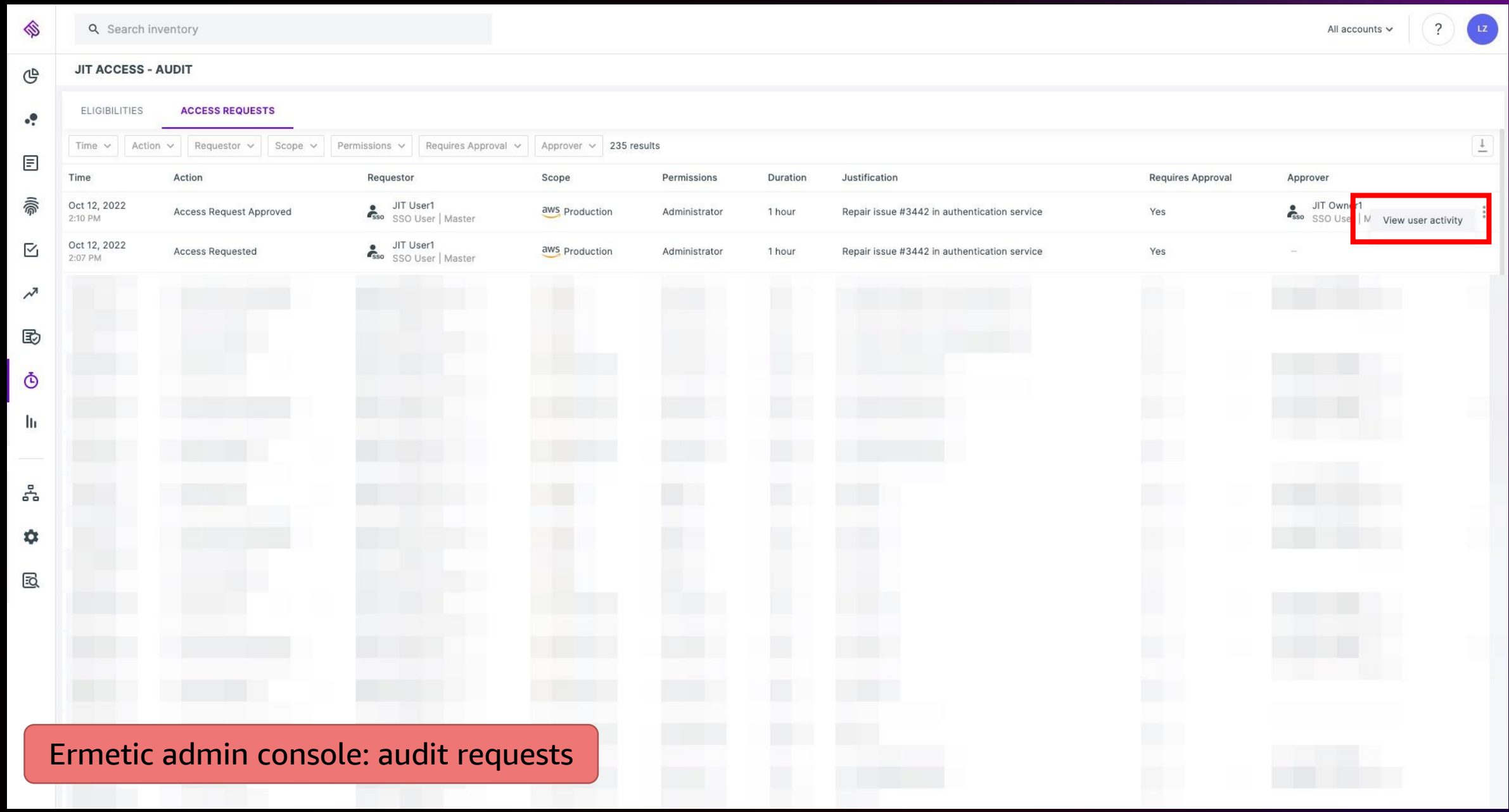
Ermetic admin console: audit eligibilities

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



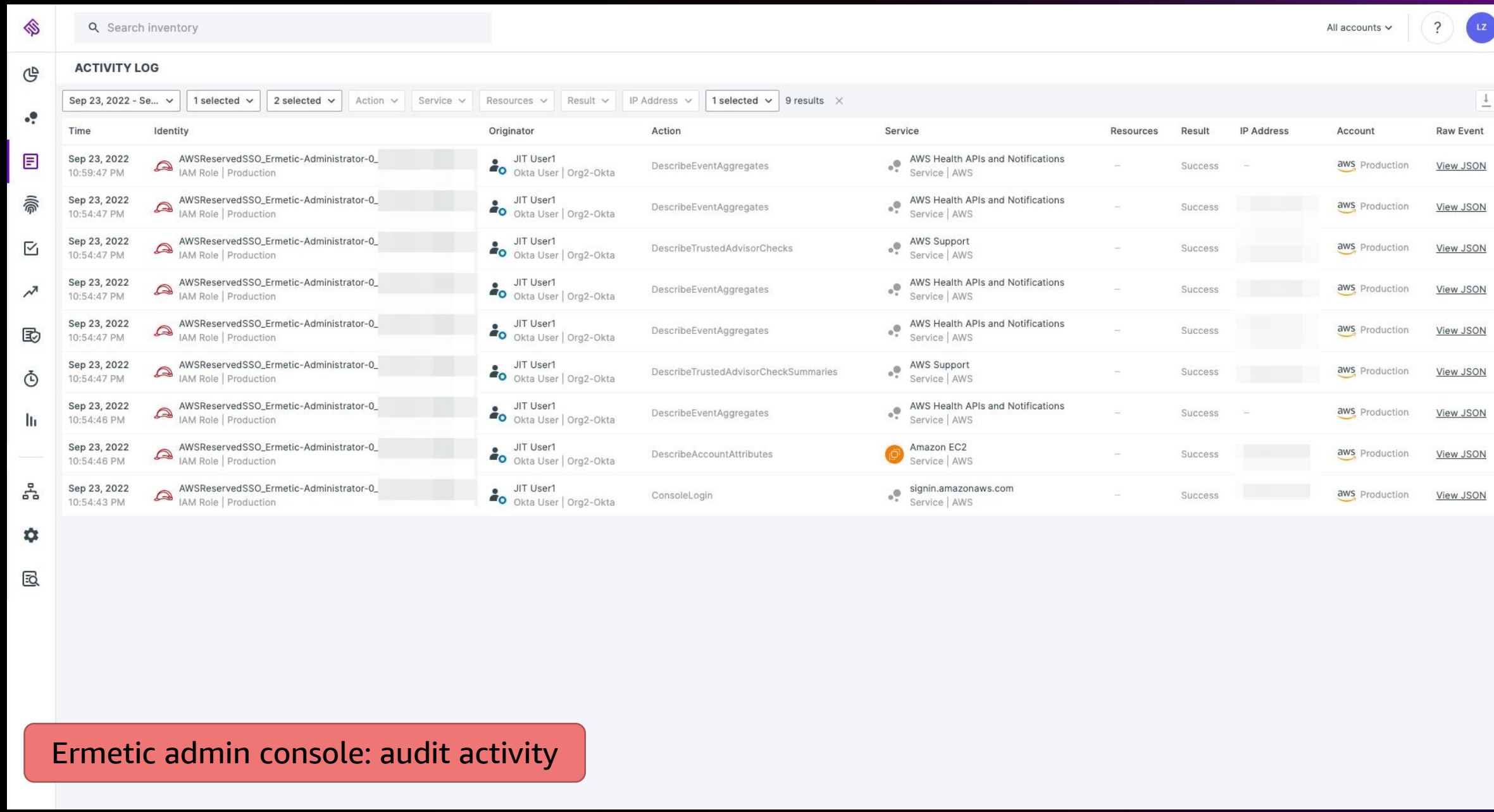
Ermetic admin console: audit eligibilities

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Ermetic admin console: audit requests

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

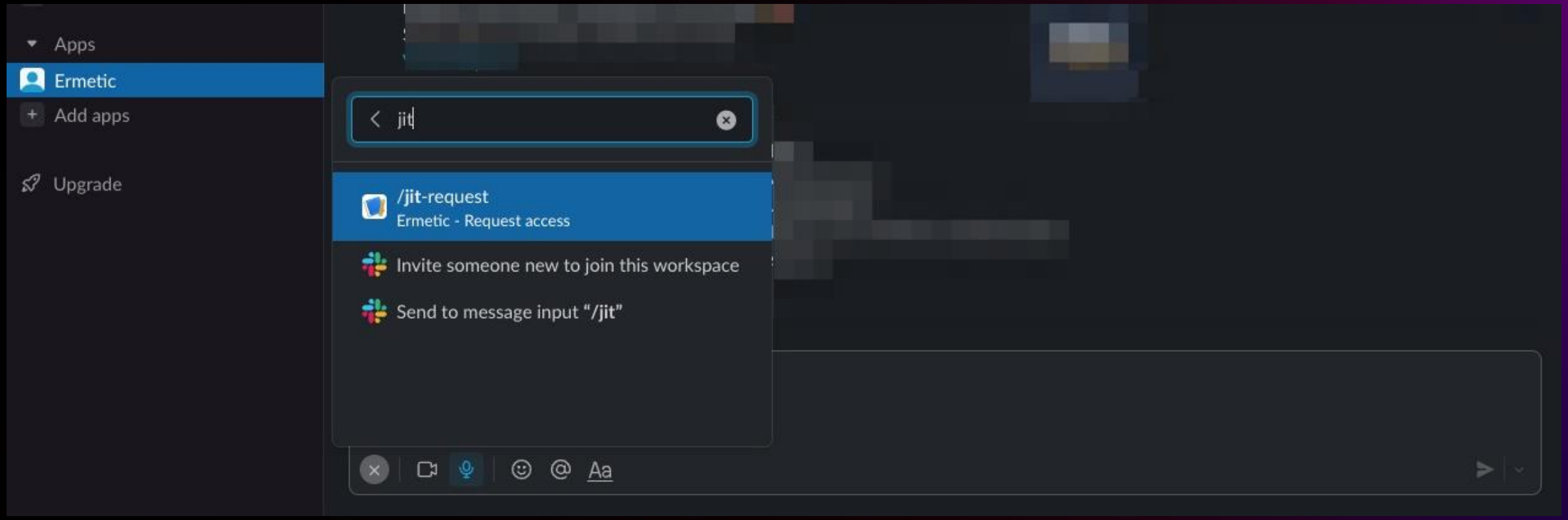


Ermetic admin console: audit activity

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

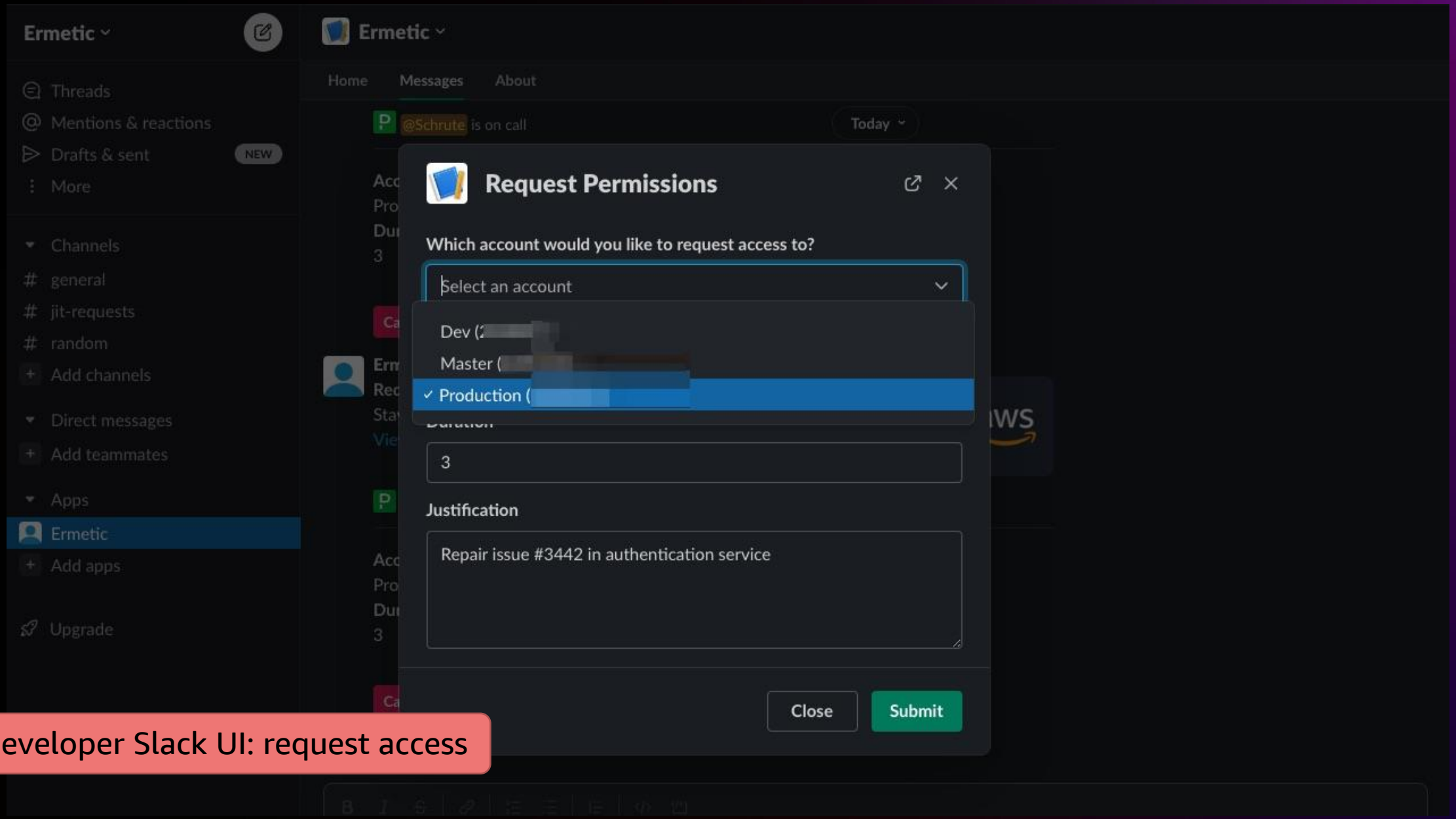
Slack and PagerDuty integration

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



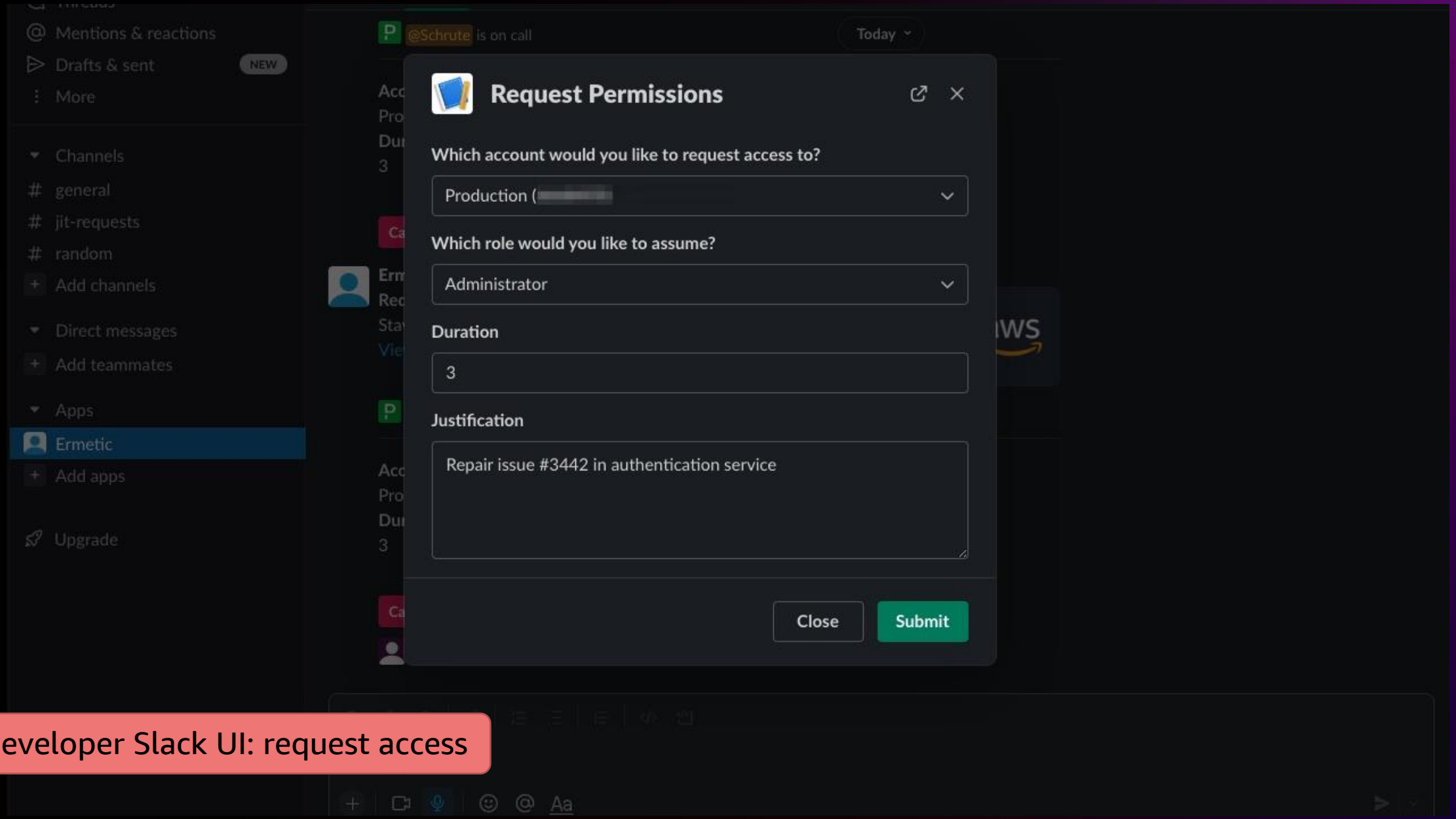
Developer Slack UI: request access

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



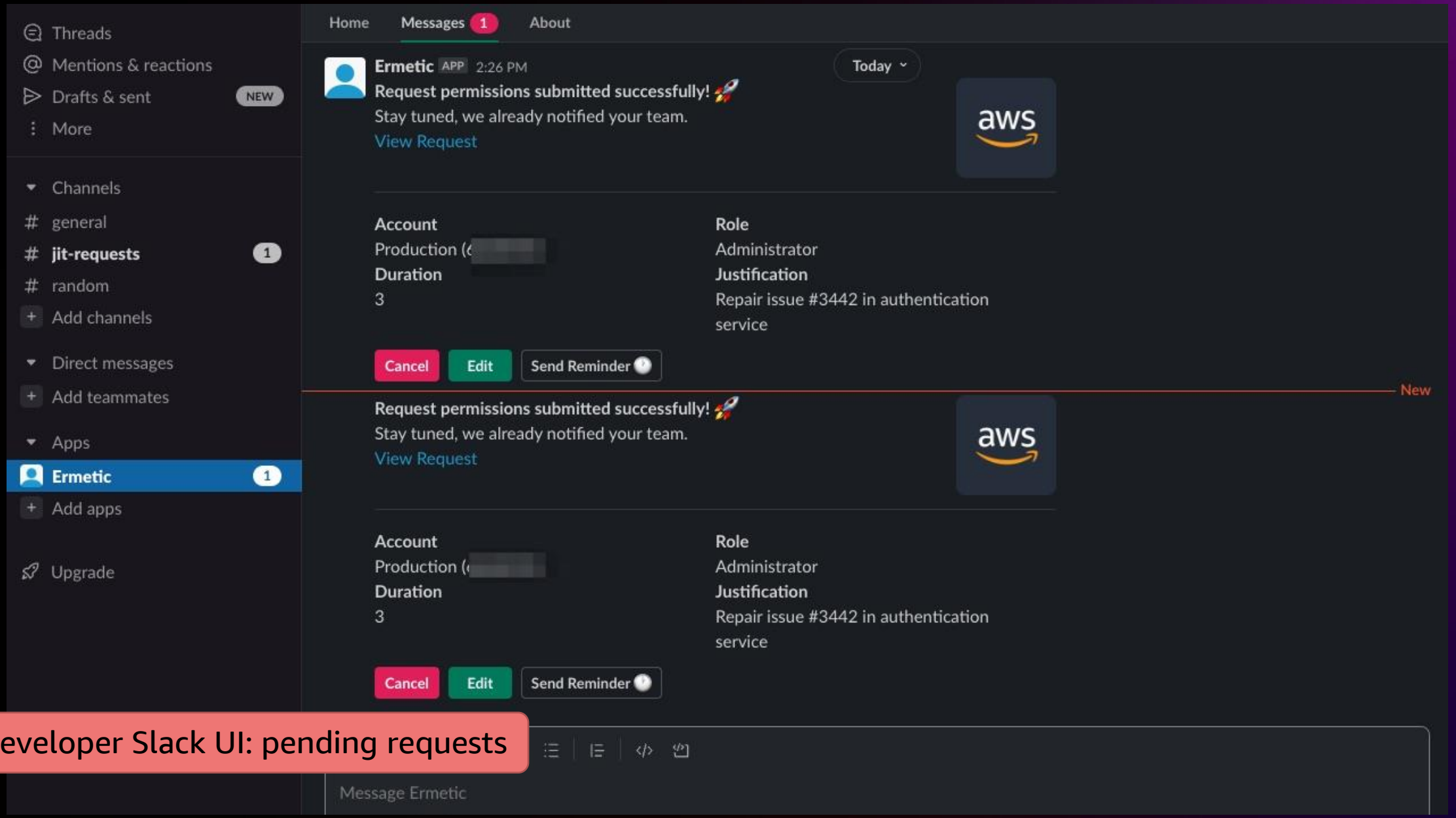
Developer Slack UI: request access

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



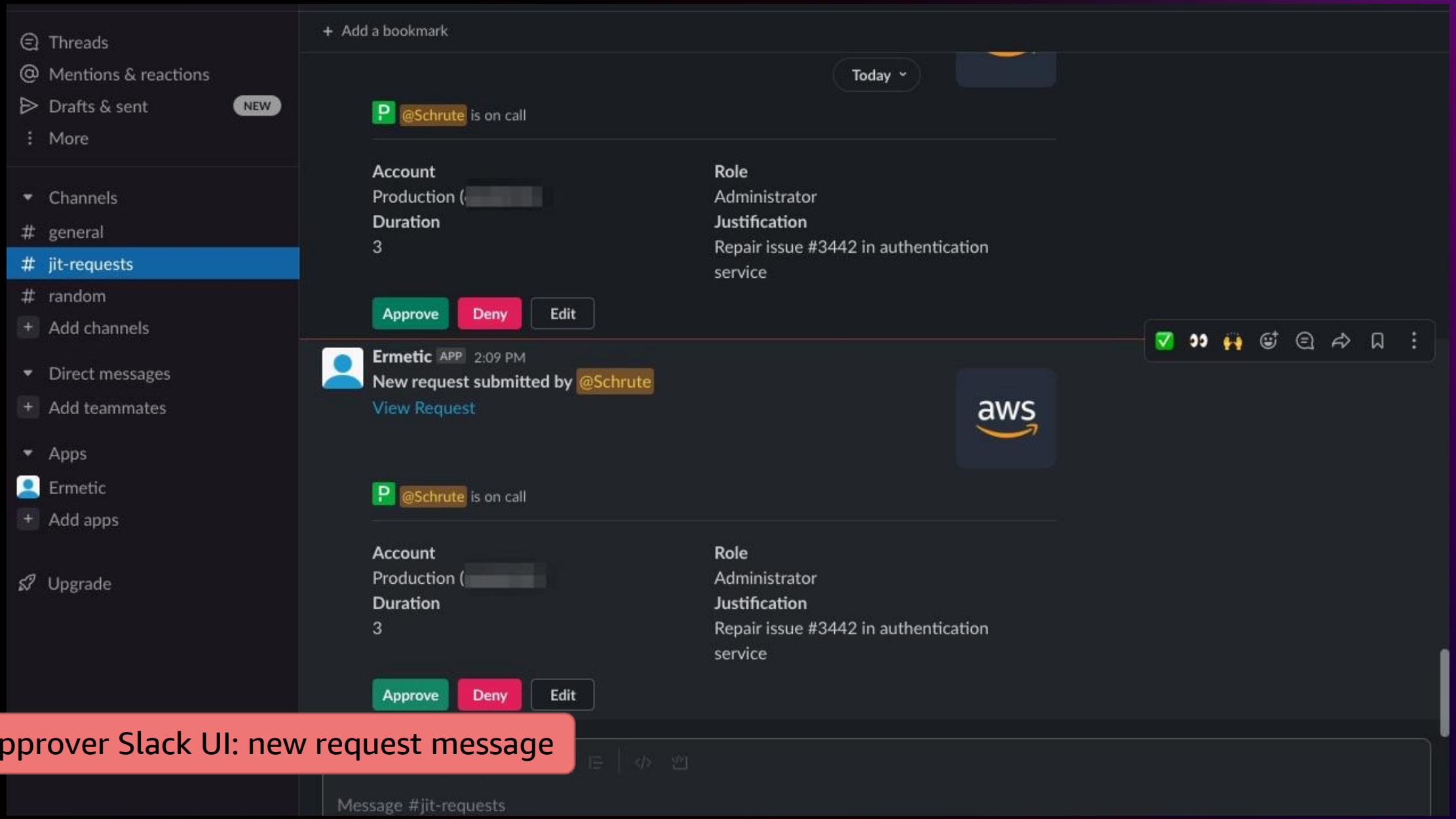
Developer Slack UI: request access

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Developer Slack UI: pending requests

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Approver Slack UI: new request message

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Benefits of the JIT approach

- It limits area of impact for security events **and** scope of operational mistakes
- Enables session monitoring
- Allows for focused auditing/investigating

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Lior Zatlavi
@CloudLior
liorzat@ermetic.com
www.ermetic.com



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.