VENDOR NAME: TriVir LLC

BUYER: Larry D McDonnell

SOLICITATION NO.: CRFP 0947 ERP2400000002

BID OPENING DATE: April 4th, 2024

BID OPENING TIME: 1:30PM Eastern

FAX NUMBER: N/A

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Proposals
Info Technology

Proc Folder: 1376334

Doc Description: Identity Management Single Sign-On Solution

Proc Type: Central Master Agreement

Reason for Modification:

Date Issued	Solicitation Closes	Solicitation No	Version
2024-02-23	2024-03-12 13:30	CRFP 0947 ERP2400000002	1

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code: TBD

Vendor Name : TriVir LLC

Address : 5860 Trinity Parkway, Suite 130

Street :

City : Centreville

State : Virginia **Country :** USA **Zip :** 20120

Principal Contact : Robert Walter

Vendor Contact Phone: 703-375-9690 **Extension:**

FOR INFORMATION CONTACT THE BUYER
Larry D McDonnell
304-558-2063
larry.d.mcdonnell@wv.gov

Vendor Signature X RWalter **FEIN#** 38-3675879 **DATE** 28 March 2024

All offers subject to all terms and conditions contained in this solicitation

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) Robert Walter, COO

(Address) 5860 Trinity Parkway, Suite 130, Centreville, VA 20120

(Phone Number) / (Fax Number) 703-375-9690

(email address) bwalter@trivir.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through *wv*OASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

TriVir LLC
(Company)

RWalter
(Signature of Authorized Representative)

Robert Walter, COO 28 March 2024
(Printed Name and Title of Authorized Representative) (Date)

703-375-9690
(Phone Number) (Fax Number)

bwalter@trivir.com
(Email Address)

4.4.Mandatory Qualification/Experience Requirements – The following mandatory qualification/experience requirements must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it meets the mandatory requirements and include any areas where it exceeds the mandatory requirements. Failure to comply with mandatory requirements will lead to disqualification, but areas where the mandatory requirements are exceeded will be included in technical scores where appropriate. The mandatory qualifications/experience requirements are listed below.

4.4.1.1. Vendor must provide SSAE No. 18 SOC 1 Type 2 report results yearly to satisfy overall State of WV SOC1 requirements.

SECTION 5: VENDOR PROPOSAL

5.1. Economy of Preparation: Proposals should be prepared simply and economically providing a concise description of the items requested in Section 4. Emphasis should be placed on completeness and clarity of the content.

5.2. Incurring Cost: Neither the State nor any of its employees or officers shall be held liable for any expenses incurred by any Vendor responding to this RFP, including but not limited to preparation, delivery, or travel.

5.3. Proposal Format: Vendors should provide responses in the format listed below:

5.3.1. Two-Part Submission: Vendors must submit proposals in two distinct parts: technical and cost. Technical proposals must not contain any cost information relating to the project. Cost proposal must contain all cost information and must be sealed in a separate envelope from the technical proposal to facilitate a secondary cost proposal opening.

5.3.2. Title Page: State the RFP subject, number, Vendor's name, business address, telephone number, fax number, name of contact person, e-mail address, and Vendor signature and date.

5.3.3. Table of Contents: Clearly identify the material by section and page number.

5.3.4. Response Reference: Vendor's response should clearly reference how the information provided applies to the RFP request. For example, listing the RFP number and restating the RFP request as a header in the proposal would be considered a clear reference.

Proposal Submission: All proposals (both technical and cost) must be submitted to the Purchasing Division **prior** to the date and time listed in Section 2, Instructions to Vendors Submitting Bids as the bid opening date and time.

SECTION 6: EVALUATION AND AWARD

6.1. Evaluation Process: Proposals will be evaluated in two parts by a committee of three (3) or more individuals. The first evaluation will be of the technical proposal and the second is an evaluation of the cost proposal. The Vendor who demonstrates that it meets all of the mandatory specifications required, attains the minimum acceptable score and attains the highest overall point score of all Vendors shall be awarded the contract.

6.2. Evaluation Criteria: Proposals will be evaluated based on criteria set forth in the solicitation and information contained in the proposals submitted in response to the solicitation. The technical evaluation will be based upon the point allocations designated below for a total of 70 of the 100 points. Cost represents 30 of the 100 total points.

Evaluation Point Allocation:

The evaluation questions in Section 4.3 have been divided into three levels (High, Medium, and Low).

High Requirement Level (42 responses):	15 Points Maximum (each)
Medium Requirement Level (24 responses):	10 Points Maximum (each)
Low Requirement Level (8 responses):	5 Points Maximum (each)

A total of 910 points can be earned from responses to these evaluation questions.

Total Technical Score:	910 Points Possible
Total Cost Score:	390 Points Possible

Total Proposal Score: 1300 Points Possible

6.3. Technical Bid Opening: At the technical bid opening, the Purchasing Division will open and announce the technical proposals received prior to the bid opening deadline. Once opened, the technical proposals will be provided to the Agency evaluation committee for technical evaluation.

6.4. Technical Evaluation: The Agency evaluation committee will review the technical proposals, assign points where appropriate, and make a final written recommendation to the Purchasing Division.

6.5. Proposal Disqualification:

6.5.1. **Minimum Acceptable Score ("MAS"):** Vendors must score a minimum of 70% (49 points) of the total technical points possible in order to move past the technical evaluation and have their cost proposal evaluated. All vendor proposals not attaining the MAS will be disqualified.

6.5.2. **Failure to Meet Mandatory Requirement:** Vendors must meet or exceed all mandatory requirements in order to move past the technical evaluation and have their cost proposals evaluated. Proposals failing to meet one or more mandatory requirements of the RFP will be disqualified.

6.6. Cost Bid Opening: The Purchasing Division will schedule a date and time to publicly open and announce cost proposals after technical evaluation has been completed and the Purchasing Division has approved the technical recommendation of the evaluation committee. All cost bids received will be opened. Cost bids for disqualified proposals will be opened for record keeping purposes only and will not be evaluated or considered. Once opened, the cost proposals will be provided to the Agency evaluation committee for cost evaluation.

The Purchasing Division reserves the right to disqualify a proposal based upon deficiencies in the technical proposal even after the cost evaluation.

We are requesting an initial contract term of three years, with the option to renew for three additional one-year periods. Please complete the pricing page for all six years.

6.7. Cost Evaluation: The Agency evaluation committee will review the cost proposals, assign points in accordance with the cost evaluation formula contained herein and make a final recommendation to the Purchasing Division.

Cost Evaluation Formula: Each cost proposal will have points assigned using the following formula for all Vendors not disqualified during the technical evaluation. The lowest cost of all proposals is divided by the cost of the proposal being evaluated to generate a cost score percentage. That percentage is then multiplied by the points attributable to the cost proposal to determine the number of points allocated to the cost proposal being evaluated.

Step 1: Lowest Cost of All Proposals / Cost of Proposal Being Evaluated = Cost Score Percentage

Step 2: Cost Score Percentage X Points Allocated to Cost Proposal = **Total Cost Score**

Example:

Proposal 1 Cost is $1,000,000
Proposal 2 Cost is $1,100,000

Points Allocated to Cost Proposal is 30

Proposal 1: Step 1 – $1,000,000 / $1,000,000 = Cost Score Percentage of 1 (100%)
Step 2 – 1 X 30 = Total Cost Score of 30

Proposal 2: Step 1– $1,000,000 / $1,100,000 = Cost Score Percentage of 0.909091 (90.9091%)
Step 2 – 0.909091 X 30 = Total Cost Score of 27.27273

6.8. Availability of Information: Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code §5A-3-11(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3.d.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

TriVir LLC
(Company)

Robert Walter, COO RWalter
(Representative Name, Title)

703-375-9690
(Contact Phone/Fax Number)

28 March 2024
(Date)

TriVir

Technical Proposal for Identity Management Single Sign-On Solution

In Response To:

ITN Number: CRFP 0947 ERP2400000002

TriVir
IDENTITY MANAGEMENT SOLUTIONS

Identity Management Solutions
5860 Trinity Parkway, Suite 130
Centreville, VA 20120

Title Page

For: State of West Virginia

Vendor Name: TriVir LLC

Business Address:5860 Trinity Parkway Ste 130

Centreville, VA 20120

Phone Number: 703-375-9690

Contact Person: Bob Walter

Email: bwalter@trivir.com

Signature: RWalter

Date: 28 March 2024

Buyer: Larry D McDonnell

Solicitation No: CRFP 0947 ERP2400000002

Fax Number: 304-558-3970

Table of Contents

Executive Summary

Department of Administration
Purchasing Division
2019 Washington Street E
Charleston, WV 25305

ATTN: Bid Clerk/ Larry D McDonnell

Re: CRFP 0947 ERP2400000002

Dear West Virginia Team:

TriVir is pleased to submit a response to the above-referenced solicitation.

Requested Services - The State of West Virginia desires to modernize its identity and access management solution to provide secure and appropriate access to State resources and applications. The State wants to standardize the login process for the various internal applications such as WVOASIS, CGI Advantage, UKG, Deighton, and others designated by the ERP Planning Board.

State employees must have access to a password self-service solution, single-portal access to entitlement-assigned digital resources, and an account and access request system for State staff. Account and access requests can be automatic or approved by multiple approval levels and/or approvers. As users transition through their professional careers with the State, access to systems and applications must be changed appropriately.

TriVir proposes implementing the Ping Advanced Identity Cloud platform, a Software-as-a-Service (SaaS) solution built on a single code base for speed and an excellent end-user experience.

Role and Qualifications - As a technical IAM expert with prior State workforce experience, TriVir will help identify and realize the State's IAM vision to modernize existing systems.

TriVir has experience with Ping Identity and familiarity with moving government organizations to Ping Identity, making us uniquely qualified to provide services and expertise to meet the solicitation requirements. TriVir also has relationships with many identity and access management solutions–Ping Identity, Okta, Microsoft, and OpenText–so we can recommend the proper solution for a client and help augment vendor engineering teams. For example, TriVir has access to Ping Identity source code and regularly submits enhancements and bug fixes for the product. TriVir also provides technical feedback to the cloud team to steer capabilities to meet the emerging needs of TriVir government clients. Because of this relationship with Ping Identity, TriVir can assist the State of West Virginia in tackling any stated task or business outcome confidently, with the ability to overcome any challenges.

TriVir implements all features with automated testing and a robust engineering methodology to ensure the solution remains agile. The automated tests then evolve with the solution to meet evolving requirements for user experience, compliance, privacy, and security.

SOW Achievement Challenges - The TriVir team will coordinate with State of West Virginia staff and Ping Identity support engineers to identify and resolve all project issues as they arise. Examples of the challenges TriVir has resolved in the past for state governments include:

- Change management can be challenging but essential in identity system modernization programs. TriVir utilizes a methodology that solicits regular, detailed feedback in regular iterations supported by automated testing. The process starts with driving right to the pain point or objective, describing it in data-driven terms, and implementing the new feature quickly to put it back into the hands of the stakeholders for feedback. This process is repeated until feature acceptance is achieved.
- Performance can be bottlenecked not just at the cloud SaaS level but also with any required on-prem components. TriVir leverages a test-first approach and performance tests all solution components to ensure they meet or exceed expectations.
- The definition of "done" is sometimes vague and difficult to articulate. With TriVir's data-driven approach to design, the State of West Virginia will regularly reach defined states of completion in a testable way.

Points of Clarification - The State will need to review and accept the Ping Advanced Identity Cloud (Ping AIC) subscription Agreements prior to the use of the offered solution. It is recommended that Article 26 of the State's contract terms and conditions be amended to account for the addition of the Ping AIC Agreements. In addition, TriVir assumes that the State will negotiate the conditions of our offer in good faith. If, for some reason, an agreement can not be reached, the discontinuation of negotiations by TriVir will not constitute a unilateral withdrawal of our offer. Finally, TriVir will register with the State's Procurement Office as required upon contract award notification.

We look forward to working with the State of West Virginia team on this project and creating a long-standing partnership of trusted cybersecurity and digital modernization advisory services.

Sincerely,

Glen Knutti
President
TriVir, LLC

Proposed Approach and Methodology

With the State of West Virginia ecosystem information and the desire to enhance the IAM framework and SSO, TriVir recommends moving to **Ping Advanced Identity Cloud Software-as-a-Service (SaaS).** The move to this IAM SaaS platform provides a single vendor that meets or exceeds all technical and business requirements outlined in this solicitation.

The move to **Ping Advanced Identity Cloud** achieves the following key State of WV objectives:

- **Remove the need for management** of full IAM stack on-premises (i.e., servers, software, custom developed modules, etc.)
- **Alleviate regular upgrades** and patching to stay current and supported
- **Enable State of WV IAM staff** to spend more time enabling application owners and business stakeholders rather than managing an IAM system product
- Delegate the burden of **enhancing the solution for evolving data privacy** requirements
- **Outsource the hardening** of the solution, regular vulnerability scanning, penetration testing, and cybersecurity controls for the IAM system
- **Accelerate** the provisioning and management of State of WV identities with cloud-native provisioning capabilities as State of WV moves to the cloud/SaaS IT model
- **Reduce cost** of regular 3rd party attestations and certifications, which are required for cyber risk management, cyber insurance policies, and other data privacy requirements
- **Enable State of WV business stakeholders** to do more with less staff during periods of extreme market competition for IT and IAM talent
- Deliver modern **Zero Trust and Continuous Adaptive Risk and Trust Assessment** (CARTA) capabilities without time-consuming or costly upgrades to the existing State of WV IAM system
- Provide **a single State of WV authority** of identity for authentication, authorization, federation, provisioning, group, and role automation
- Deliver a fully IAM SaaS integrated **User Experience (UX) no-code/low-code orchestration** platform, which allows State of WV admins the ability to customize workflows simply and quickly

As a solely focused IAM solution implementation partner, an Accredited Delivery Partner (ADP) of Ping Identity, TriVir is uniquely positioned to reimagine how State of WV IAM features and requirements could best be implemented in the modern cloud/SaaS model.

Scope of Work

TriVir will work with State of West Virginia to deploy an IAM solution that will:

a. Provide a state-wide solution for ERP integration and Single Sign-On (SSO) of applications.
b. Deliver a complete SSO cloud-based solution that will provide robust security solutions to include encryption, logging, and industry-standard SSO solutions.

The TriVir delivery team will achieve the fastest and most reasonable project velocity. TriVir will perform the following high-level tasks in short, iterative sprints in this initial Ping Advanced Identity Cloud SaaS IAM implementation phase. The TriVir Project Manager will take steps to provide Quality Assurance, issue tracking, and resolution.

Refer to the Project Methodology and Technical Approach section after the tasks and milestones described for the first few phases.

The following is a sample approach based on the requirements put forth by the State. Once priorities have been identified in the initial requirements analysis, the ordering of the approach will be updated to meet those business needs. Thus, the approach below is notional and will be updated per the priorities and needs of State of West Virginia stakeholders.

Proposed SaaS Solution: Advanced Ping Identity Cloud

TriVir proposes **Ping Advanced Identity Cloud Software-as-a-Service (SaaS)**. The migration to this IAM SaaS platform provides a single vendor that meets or exceeds all technical specifications and functional requirements outlined in this State of West Virginia solicitation. Since this single SaaS service includes all of the IDM capabilities requested by the State of West Virginia in a single offering, the overall complexity is significantly reduced. Ping Advanced Identity Cloud is the only SaaS IAM platform that includes all of the following capability pillars under one isolated tenant:

- Identity Lifecycle Management
- Access Management
- User Journey Orchestration
- Identity Governance and Administration
- Privileged Identity Management

Ping Advanced Identity Cloud also uniquely meets the on-prem requirements of the State of West Virginia to provide:

- An on-premise LDAP directory for legacy applications
- A reverse-proxy Identity Gateway to facilitate modern MFA and authentication experiences on legacy State of West Virginia applications that are otherwise not able to utilize modern federation protocols
- Low-code/No-code configuration that simplifies the definition of user journeys and experiences without having to be a software developer

This singular SaaS Platform will specifically facilitate the State of West Virginia requirements around:

- Access Management (SSO) with Standard Federations and Integrations like SAML/SAML2, OAuth/OAuth2, WS-FED, OIDC, and Others
- Strong and flexible Multi-Factor Authentication (MFA)
    - Options for strong identity proofing at enrollment and also at token reset/self-service
    - Strong identity proofing before calls with the helpdesk
- Support for modern and legacy applications
- Account Lifecycle Management
- Application Roles, Access, and Authorization Management
    - Support for:
        - Roles-Based Access Control (RBAC)
        - Attribute-Based Access Control (ABAC)
        - Policy-Based Access Control (PBAC)
- Approval Workflows and Resource Access/Requests and Approvals
- Password Management, Seeding, Self-Service, and Passwordless Options
- Identity Governance and Administration
- Simplified Integration with the State of West Virginia HR/HCM systems and other authoritative sources

- Simplified Integration with Downstream Systems like Active Directory and other critical systems on-premises at State of West Virginia

The move to **Ping Advanced Identity Cloud achieves the following** key client objectives:

- **Remove the need for State of West Virginia management** of full IAM/SSO stack on-premises models (i.e., servers, software, custom-developed modules, etc.), thus retiring the existing, custom-developed solution.
- Reduce complexity by introducing native **low-code/no-code** configuration options for user orchestration, allowing for customized experiences for each State of West Virginia user personas (e.g., staff, faculty, employees, parents, non-employee workers, volunteers, etc.) without needing custom development.
- **Alleviate regular upgrades** and patching to stay current and supported.
- **Enable State of West Virginia IAM staff** to spend more time enabling application owners and business stakeholders rather than managing an IAM system product.
- Delegate the burden of **enhancing the solution for evolving data privacy** requirements.
- **Outsource the hardening** of the solution, regular vulnerability scanning, penetration testing, and cybersecurity controls for the IAM system.
- **Accelerate** the provisioning and management of **State of West Virginia's** identity into and Microsoft Azure AD with cloud-native provisioning capabilities as **State of West Virginia** moves to the cloud/SaaS model for IT.
- **Reduce the cost** of regular third-party attestations and certifications, which are required for cyber risk management, cyber insurance policies, and other data privacy requirements.
- **Enable State of West Virginia business stakeholders** to do more with less staff during periods of extreme market competition for IT and IAM talent.
- Deliver modern **Zero Trust and Continuous Adaptive Risk and Trust Assessment** (CARTA) capabilities without time-consuming or costly upgrades to the existing IAM system.
- Provide **a single State of West Virginia authority** of identity for authentication, authorization, federation, provisioning, group, and role automation.
- Deliver a fully IAM SaaS integrated **User Experience (UX) no-code/low-code orchestration** platform, allowing **State of West Virginia** admins to customize workflows simply and quickly.
- Improve security by ensuring all data and communication are protected by the latest cryptography standards with support for SSL/TLS and NIST FIPS standards.

As a longtime partner and IAM provider, an Accredited Delivery Partner (ADP) of Ping Identity, and a longtime world leader in Ping Identity IAM solution delivery, TriVir is uniquely positioned to reimagine how **State of West Virginia** IAM features and requirements could best be implemented in the modern cloud/SaaS model. TriVir has the experience and knowledge specific to migrating legacy customers to Ping Identity at scale for internal-facing and external IAM features at federal, state, and local governments.

Suggested Initial Phase

- **Discovery**
  - **Milestone:** Conduct detailed, data-driven Requirements Assessment (RA) workshop, focusing on connecting authoritative sources for State of West Virginia identity to include:
    - Employees

        - External Contractors
        - other identified parties
- **Planning–**
    - After the Discovery sessions with the State of WV team, the resultant outcomes from the direction both parties agree upon, the next step is to determine resources and timelines that will lead to the desired outcome. Due to our engagement with other States, TriVir will deploy best practices learned and suggest prioritizing certain aspects of the project in the planning process.
    - Workshop process for IAM DevOps in Ping Advanced Identity Cloud SaaS; provide system overview with:
        - Business unit representatives
        - Developers
        - Application owners and administrators
        - Other key stakeholders of the new identity solution
- **Design**
    - **Milestone:** Document design, testable business use cases, or **Acceptance Criteria** (ACs) for each major solution function are delivered through the IAM SaaS platform in this Initial Phase.
        - Business rules and features will be informed by those present in the current IAM system.
        - Where feasible, TriVir SMEs will guide IAM team members through best practices to consider how to accomplish similar business outcomes with less or no customization as business processes are re-imagined for sustainable operation in IAM SaaS.
    - **Milestone:** Deliver design document (ACs) and architecture documentation for State of West Virginia approval
        - Review and update ACs with stakeholders; incorporate feedback
        - Include budgeting costs and updated calculations based on the new design and architecture, including any new ongoing costs.
        - If existing code will be reused or enhanced, a security review will take place
- **Operations**
    - TriVir will engage with the State in financial analysis around operating expenditures and have State tracking available to hours worked on by TriVir consultants. TriVir preferes to engage with the State in a Time and Materials type engagement. This will allow the State full transparency to TriVir's billing and engagement process.

Install and configure SSO and IAM solutions

- **Milestone:** Provisioning of customer Ping Advanced Identity Cloud SaaS tenant with Dev, Test, and Production environments once contracts are signed
- Workshop process for IAM DevOps in Identity Cloud SaaS; provide system overview with:
    - Business unit representatives
    - Developers
    - Application administrators
- Other key stakeholders of the new identity solution
- **Milestone:** Conduct detailed, data-driven Requirements Assessment (RA) workshop, focusing on connecting authoritative sources for State of West Virginia identity to include:

    - Employees
    - Non-employees (i.e., contract professionals, volunteers, etc.)
- **Milestone:** Document design, testable business use cases, or Acceptance Criteria (ACs) for each major solution function are delivered through the IAM SaaS platform in this Initial Phase.
    - Business rules and features will be informed by those present in the current IAM system.
- Where feasible, TriVir SMEs will guide IAM team members through best practices to consider how to accomplish similar business outcomes with less or no customization as business processes are re-imagined for sustainable operation in IAM SaaS.
- **Milestone:** Deliver design document (ACs) and architecture documentation for State of West Virginia approval
    - Review and update ACs with stakeholders; incorporate feedback
    - Include budgeting costs and updated calculations based on the new design and architecture, including any new ongoing costs.
- If existing code will be reused or enhanced, a security review will take place
- **Milestone:** Configure IAM SaaS tenant administrators, in cooperation with the service desk, PAM policies, and security requirements
- **Milestone:** Configure Realms for operation; establish the required footprint of the customer subdomain for Ping Advanced Identity Cloud services
- **Milestone:** Establish the new SaaS identity repository in Ping Advanced Identity Cloud SaaS Directory Services (DS) Dev environment
- Connect authoritative sources by implementing Identity Management (IDM) Connectors
    - Map in existing UserIDs and passwords (as well as relevant group/role memberships to seed the system to facilitate transparent service transfer to Ping Advanced Identity Cloud for experiences within existing applications)
    - **Milestone:** Authoritative source connected (for each target source system)
- **Milestone:** Conduct Initial Program Load (IPL) through the IDM connectors connected to authoritative sources for in-scope user types (Dev tenant)
- **Milestone:** Prepare and test Access Management (AM) configuration to close out customer requirements for IdP, SSO, MFA, etc., to consume and leverage the DS identities in Dev
    - **Milestone:** Bring over at least one application of each desired integration model for this sprint (i.e., SAML, OIDC, OAUTH, WS-Fed, etc.) and begin to deliver AM-integration cookbooks specific to customer applications
    - **Milestone:** Design seamless transition from existing AM experiences onto the new platform, with minimal service disruption or friction to end users through the delivery of no-code user journeys (authentication trees) for each supported user type on this AM target application
    - **Milestone:** Configure Self-Service portal (user profile, privacy, MFA/credentials), leveraging user journeys and no-code orchestration
- **Milestone:** State of West Virginia Team Enablement: customer staff to perform AM integrations on their own, based on our cookbooks and Ping Advanced Identity Cloud best practices (teach staff how to fish and support their successful angling with the new tools)
    - Test Dev applications against new AM paradigm and SaaS IAM solution
- **Milestone:** Configure on-demand provisioning/administration of identities (i.e., non-employees, Non-Person Entities, etc.) where required

Build the Initial Test System

- **Milestone:** Conduct IPL against Test tenant (Staging)
- Conduct automated testing/manual testing against Staging with at least one application

- **Milestone:** Conduct UAT testing in the Staging environment
- **Milestone:** Conduct IPL against Production tenant
    - Invoke process to migrate Staging environment static and dynamic configuration to Production environment (leveraging the same tools and Ping Identity promotion model)
    - Conduct automated testing/manual testing against Production

Comprehensive Functional Testing

- **Milestone:** Performance and Load testing per specified use cases in the ACs
- **Milestone:** Conduct UAT testing in the Production environment
- **Milestone:** Connect and instrument operational components
    - IDMMonitor (verifies SaaS and feature integrity to push issue detection up the stack)
    - SIEM integration where required
    - Dashboarding and monitoring for key solution aspects as requested

Training and Technical Services

Detailed training plan and user acceptance

- **Milestone:** Sprint retrospective; document learnings for the next sprint
    - Knowledge transfer to State of West Virginia developer and IDM support teams
    - Provide seeds for admin and user guides as described in the ACs
    - End user training materials constructed and distributed to State resources
- **Post-Deployment Milestone:** Post initial deployment support Month 1
- **Post-Deployment Milestone:** Post initial deployment support Month 2
- **Post-Deployment Milestone:** Post initial deployment support Month 3
- **Post-Deployment Milestone:** Post initial deployment support Month 4
- **Post-Deployment Milestone:** Post initial deployment support Month 5
- **Post-Deployment Milestone:** Post initial deployment support Month 6

Post Initial Phase

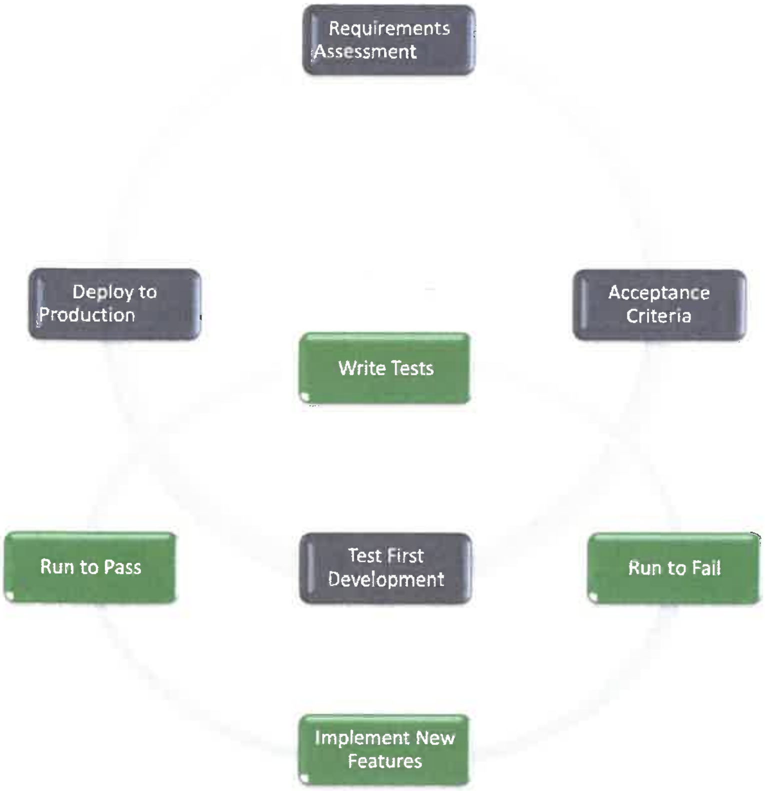
Lessons learned development and solution acceptance

- Move into repeatable sprint iterations:
    - Assist IAM staff with the integration of additional AM federations per the cookbooks, along with associated user journeys and orchestration
    - Configure Ping Advanced Identity Cloud to replace existing/legacy IDM connectors
        - Deliver recommendations on simplifying current business logic to reduce customization and streamline customer operations (for example, leverage Bring Your Own Identity (BYOI) and remove complicated IDM drivers and workflows for identity management).
        - Configure and deliver the Ping Advanced Identity Cloud connectors to meet the simplified/streamlined business logic for connected customer applications.
        - Generate an associated cookbook for IDM/AM integration of this type of system (i.e., REST, SCIM, etc.) and acquaint the IAM team with the approach.
    - Follow Ping Advanced Identity Cloud DevOps for promotion, testing, and full service
- Repeat sprint iterations to integrate the following AM targets:
    - Contractor portal
        - Integration with existing databases; simplify existing process
    - Self-service experiences

    - User orchestration journeys
    - Others
- Repeat sprint iterations to integrate the additional integration targets while hours remain
- Repeat sprint iterations to add other essential business logic, such as:
    - Delegated group administration and associated workflows
    - Delegated role administration and associated workflows
    - Others

Project Methodology and Technical Approach

It is essential to realize that any identity management project must be delivered following a consistent approach to yield consistent results. Having implemented many Identity Management systems for numerous organizations, TriVir has coalesced best practices and lessons learned in order to streamline and simplify the implementation process. This methodology, as described and depicted below (see Figure TriVir Methodology), includes a requirements assessment, established acceptance criteria, iterative development, automated testing using IdMUnit (an open-sourced tool designed, developed, and maintained by TriVir), and measured progress towards testable and documented project outcomes.



TriVir Methodology

- **<u>Requirements Assessment</u>** – The Requirements Assessment (RA) begins with a series of meetings to review the organization's objectives and goals and determine the project scope. Meetings with stakeholders and system owners are held in order to understand current and future needs. Communication with system owners and stakeholders is critical in an identity management implementation to increase the likelihood of implementing the appropriate solution through the proper interface with the best processes.

TriVir creates an Acceptance Criteria (AC) document for each project containing testable business use cases that collectively define the requirements for a successful project. Each AC use case includes a description, preconditions, specific action, expected result(s), and example data to clarify format and syntax requirements. The AC document includes the detailed project and business requirements to be designed, configured, and deployed by TriVir consultants. These precise requirements are refined through additional conversations with stakeholders, and TriVir consultants build on what they learned during the Requirements Assessment. The final AC document provides a specific description of each use case the solution must support. For project success, AC documents must be thoroughly understood, reviewed, and accepted by stakeholders, as the requirements drive the developed solution.

Once client stakeholders have accepted the AC document, the TriVir consultants estimate the time necessary to configure and develop the solution. The estimates for all AC use cases will comprise the total estimated time for development and testing efforts for the project. At this point, it is critical to reconvene and review the project estimates based on the specific use cases identified in the AC document in order to establish and set proper delivery expectations.

- **Development and Testing** – With use cases defined in the AC document, configuration and development work is divided into iterative releases (weekly or bi-monthly). This process allows for incremental solution testing to start before the development phase is complete and developmental checkpoints along the way to support keeping the project aligned with the documented plan.

  Testing the developed solution is an integral part of the TriVir process. We use automated tests to facilitate our test-first approach. Automatically testing use cases before deploying and regression testing of the entire solution provides a higher confidence level when deploying to a production environment.

- **Deployment** – With regular, iterative testing of releases, deployment to testing and production environments is relatively seamless. Once the configuration is moved to the test or staging environment, the automated tests are executed to validate that the deployment operates as expected. Once validated, the configuration is promoted to production, where the automated tests are rerun to ensure that the entire identity system works as designed.

Throughout the process defined above, TriVir management provides weekly status reports detailing work completed, planned activities, and risks, issues, or concerns. TriVir makes generated documentation and project-related assets available on a shared volume accessible by customer technical resources and management. This project management value-add provides the ability to adjust design and system specifications to comply with constantly evolving guidance, regulatory policy, and the current needs of the IAM team and its stakeholders.

TriVir has supported customers for over two decades using our proven process when designing, developing, and implementing these IAM solutions. TriVir will continue to adhere to this approach as new work and support requirements are identified and developed for the State of West Virginia.

Project Plan

A roadmap and project plan specific to the customer will be developed and presented after the Requirements Assessment phase of the project.

Project Management

In addition to TriVir's technical abilities, TriVir also provides project management support to its consultants and related projects. This ensures that each client engagement can benefit from a well-defined, proven, and standard approach to implementing IAM and SSO SaaS solutions.

TriVir's Program and Project Managers (PM) oversee and control the resources and activities associated with this proposal. Specifically, the PMP-certified TriVir Project Manager utilizes best practices defined by the Project Management Institute (PMI). They have standard procedures and templates to address the following tasks effectively.

- Provide management and leadership for project team members and act as primary liaison and escalation point.
- Develop and maintain the Project Management Plan (PMP) detailing goals, milestones, resources, and adherence to customer standards, regulations, and policies.
- Maintain project scope as defined in the Statement of Work (SOW) to ensure the project stays on schedule and within budget.
- Develop project plans from pre-engagement to kick-off meetings through design, engineering, test, and validation cycles, continuing until deployment.
- Deliver weekly status reports and facilitate status meetings scheduled based on the project's needs (i.e., bi-weekly, weekly, or daily) or the needs of individual project phases.
- Identify risks and mitigation plans, identify and address issues to reduce their impacts, and provide tracking and frequent status updates for each.
- Conduct close-out activities to ensure a smooth transition of the solution and next steps for the customer.

Additional Project Management Responsibilities:

- Schedule consultants and other resources to meet the defined project schedule.
- Manage and coordinate all activities against the project schedule to meet timelines.
- Maintain quality control on provided services, solutions, documentation, and deliverables.
- Work with the customer Project Manager to ensure the change control processes are defined, change requests are submitted and approved, and changes are made within the customer environment before the date specified in the agreed-upon project schedule.
- Maintain the SOW, change requests, and identify issues and their resolutions.

Integration and Configuration Services

The TriVir Methodology outlines the development process TriVir uses to ensure the resulting solution meets the requirements specified for the system.

TriVir uses several automated testing tools to stress-test the solutions to verify that they perform as desired. Using these tools, we put the system under loads comparable to the average and peak loads expected. The tests use data representative of the data in production.

Hardware and Infrastructure Recommendations

The Ping Advanced Identity Cloud solution will be provided as a SaaS service; therefore, no hardware or infrastructure recommendations are required for those components. The only exceptions would be to facilitate integration with legacy and on-prem systems promoted through Ping Advanced Identity Cloud Edge.

System Testing

TriVir uses several automated testing tools, including IdMUnit, to verify that the solution functions according to business rules and specifications. With these tools, functional testing can be completed for the entire IDM solution in seconds rather than weeks. TriVir is the only firm in the identity management implementation marketplace that offers this level of automated testing, IAM system regression testing, and verification of identity management connections. IdMUnit and the process defined above will continue to be used to test the entire IAM system. Additionally, because the system is delivered using Test-Driven Development (TDD), the features and functionality offered are far more straightforward for customer IAM staff to receive, own, and evolve. Through this automation-supported delivery approach, the customer IAM team naturally becomes a part of the TriVir IAM DevOps culture. It can wash, rinse, and repeat these best practices in TriVir's absence post-engagement.

Performance and Security Testing

Within the Ping Advanced Identity Cloud platform, three categories of functionality need to be tested: authentication, self-service, and synchronization. The approach to verify the performance of each class of functionality involves a different set of tools to simulate the average and peak loads handled by the system. Additionally, because Ping Identity Access Manager (AM) and Ping Identity Manager (IDM) share the same user repository, Ping Identity Directory Server (DS), the testing needs to account for the load that may happen concurrently from the different categories of functionality.

Authentication and Self-Service Performance and Functional Testing

TriVir uses a combination of Gatling, jMeter, and Selenium for performance testing of authentication and self-service functionality. The features in these categories are implemented with a user interface as a single-page application. This means all of the requests made by the user interface can be simulated without a browser. Because of this, we can generate more load on the servers with fewer computers.

Typically, authentication use cases are more susceptible to significant peaks in the number of requests, so generating a substantial load with little coordination or delay is vital.

Because there will be different authentication journeys for different types of users, they can have other performance characteristics. The tests will simulate different types of users authenticating to match real-world traffic as closely as possible.

The TriVir approach to testing these components, coupled with the tools mentioned above, enables the automated testing of the Ping Advanced Identity Cloud IAM SaaS system and customer systems tied into the IAM framework. This facilitates complete end-to-end unit testing and user UX testing across the enterprise, which is critical for the initial success of this IAM modernization effort and the continued evolution of the customer's journey to modernize and move to the cloud.

Synchronization Performance and Functional Testing

The Ping Identity system supports three types of synchronization: implicit sync, live sync, and reconciliation. Each type of synchronization will need to be tested based on the standard expected load. Additionally, we will perform bulk loading of users to quantify the performance characteristics related to this operation.

TriVir utilizes our IDM testing tool, IdMUnit, to test implicit and live sync use cases. With IdMUnit, we can generate changes in the authoritative system and verify that they are adequately synchronized with the other connected systems.

User Acceptance Testing

The TriVir approach to User Acceptance Testing (UAT) is data-driven. It enables State IAM team members and customer business and application stakeholders to leverage critical features and provide feedback. It also offers the opportunity to measure progress and guide the focus and deliverables of upcoming sprints. At a high level, UAT testing involves the following:

- Description of testable business use cases in-scope for this testing (data-driven, where possible)
- Creation of UAT steps or scripts by user and role type
- Brief, simplified training to manage expectations and help business participants understand what is being tested
- Overview of what constitutes pass or fail (based on the initial Acceptance Criteria driving the sprint)
- Conducting test steps and scripts together to record findings and gather feedback
- Consolidation of all results into a summary report delivered to the customer IAM Team
- Incorporation of findings into upcoming sprint objectives, adding incident tracking (along with associated severity) for any issues or defects discovered

Deployment Plan

Since the Ping Advanced Identity Cloud platform is a SaaS offering, the configuration process differs from that of an on-premises solution. Ping Identity manages the base configuration and integration of the individual components.

As part of the Ping Advanced Identity Cloud offering, they provide customers with development and test environments in addition to their production environment. Ping Identity provides a mechanism to promote configuration from a lower environment to a higher environment as it is completed in the development environment.

TriVir develops automated tests for the system's use cases as part of our development process. When a configuration is promoted to a higher environment, the automated test can be used to verify that the system functions as intended. TriVir also provides IAM SaaS DevOps tools to remove human or manual steps relating to asset/artifact revision control and code promotion to reduce risk at deployment intervals.

The initial production deployment of the system will require coordination with the existing system and applications. TriVir will develop a detailed plan for the steps, timeline, and responsible party for each part of the initial deployment. Refer to Tab 5 for a high-level overview of the unique approach to the initialization of the IAM SaaS system. It should include 100% adoption of existing customer-managed identities on day one, along with their existing passwords and other critical business attributes and memberships.

Training

Refer to the attachment included with this response entitled, "Ping Identity University Overview " for a description of the training approach provided with Ping Advanced Identity Cloud. Pricing scope has been added to train multiple State of West Virginia team members on the product components that will be leveraged for this implementation.

In addition to product-specific training by Ping Identity, TriVir will work as requested with the customer team to create specialized training plans to meet defined objectives using one or more of the defined training formats. The training materials will be constructed for the State and distributed with branding provided by the State. The goal with the training for end-users–employees, staff, external contractors, etc. is specific training to ensure adoption of the new system is seamless.

Services

TriVir can provide services on an hourly or SOW fixed-price basis for services beyond the scope of the initial implementation and for customization services. In summary, the TriVir service approach includes the following:

1. The TriVir Project Manager (PM) and Customer Manager remain in contact, at least weekly, to determine the state of current initiatives and future plans.
2. The TriVir PM communicates to the TriVir Management team any needs for the subsequent week for new, continued, or increased/decreased engineering support.
   a. Requests for new or increased support are reviewed by the TriVir Management Team each Friday, who then assign qualified consultants to the project on the consultant's next availability. Note: TriVir assigns staff to projects on a first-in, first-staffed basis. "First in" means a funded contract with a defined set of activities and a commitment from the client's representative that the project or work is ready to commence.
   b. Once an assignment has been identified and communicated to the applicable consultants, the TriVir PM will provide the name of the proposed consultant(s) and a potential start date to the customer Project Manager.

This process, adhered to every week, allows TriVir to plan for and address the evolving nature of the customer IAM/SSO business requirements as soon and effectively as possible. The key to this process is maintaining an open dialogue between the customer IAM Team and the TriVir PM to forecast future needs as soon as possible in order to obtain the desired engineering support on or near the time a project is intended to start.

The process above defines TriVir's approach to project-based, hourly consulting. Should customers have an operational issue and need TriVir's assistance to address a system outage or critical system issue, a customer representative should reach out to the TriVir PM and seek expedited support. The PM will immediately discuss the concern with qualified consultants and coordinate the work to provide the needed help.

Post Implementation Support

As described below, both Ping Identity (vendor) and TriVir (contractor) will provide maintenance and support.

Ping Identity Service Account Management

This recommended premium support offering provides customers with an identified (by name) Senior Customer Success Outcome Manager (CSOM) to act as a customer advocate with the Ping Identity support staff. Availability of web, phone support, and phone escalation is 24/7/365.

The SAM provides the following services critical to obtaining **product-specific** assistance:

- Verifies all incidents are logged, prioritized, and completed appropriately
- Coordinates with support engineers and management to facilitate the critical issues' shortest possible resolution times
- Serves as the main point of contact for issue escalation
- Provides product training and conducts regular reviews of the customer service history to and with IAM team members

- Makes recommendations to leverage new product features and health checks to help improve the effectiveness of the IDM
- Records and surfaces customer-generated ideas for product improvements to development teams
- Provides pulse cadence twice a month, executive business reviews, and Innovation & Roadmap Sessions twice a year

In addition, this premium support provides customer IAM team access to the Ping Identity knowledgebase, technical documentation, and support forums.

Ping Identity provides an option to log medium/low severity issues through their online Customer Center. For high-severity issues, customers may call the defined CSOM directly.

Premium response times for incidents are as follows (listed by Priority/Severity):

P1: 1-hour response

P2: 2-hour response

P3: 4-hour response

P4: 24-hour response

Please refer to the attached guide for additional support details, "Ping Identity Success Packages" and refer to the Premium Tier, which is bundled with this proposal for the State of West Virginia.

TriVir Support

As IAM experts, TriVir provides and coordinates Tier II-IV level support for the production IAM SaaS solution. This goes beyond password reset or basic troubleshooting typically managed by a Tier I or frontline support technician. Tier II-IV support focuses on component or system outages, assessing and troubleshooting system anomalies, working with the Ping Identity SAM and/or backline engineers (Tier IV), and implementing solutions and patches in an organized, tested, and controlled format. Should system adjustments be necessary, TriVir will follow our standard methodology to include complete documentation, readme files, and other aids to record the details of the deployed remedy correctly.

TriVir has a long and deep partnership with Ping Identity engineering, the Ping Advanced Identity Cloud team, and backline support. Over many years, TriVir has delivered Ping Identity IDM connectors, AM feature enhancements, and defect resolutions. It is critical to the success of the customer IAM SaaS program that the services provider have an excellent relationship with the engineering and support teams of the IAM vendor in order to troubleshoot issues and resolve problems quickly and effectively.

To request solution support from TriVir consultants, please call (USA) 703-375-9690.

Warranty Period

During the period that Ping Identity makes the Ping Advanced Identity Cloud available to customers pursuant to this contract, Ping Identity shall provide IAM SaaS SLA subject to the service level terms prescribed in "Ping Advanced Identity Cloud Support Services Terms and Conditions.pdf". Suppose Ping Identity does not fulfill its SLA obligations. In that case, the customer, as its sole and exclusive remedy, may be entitled to service credits, as defined in the same terms and conditions document. This warranty applies to the customer production tenant environment.

Service Level Commitments

Ping Identity warrants that during the contracted service period, they will target to respond to service interruptions and other incident reports based on the Service Priority defined in the premium services agreement and in accordance with the prescribed working hours. The customer is responsible for ensuring that Support Contacts are available during working hours to provide diagnostic and technical context for the reported issues.

Escalation

Suppose an Authorized Support Contact experiences issues with Ping Identity Support Services, such as difficulty in raising tickets, exceeding Support SLA initial response times, or not receiving the expected support level. In that case, the Authorized Support Contact can escalate their issue via the ticket. A Ping Identity representative will report back with a response and action plan (when appropriate) to address the Support Contact's escalation points. The TriVir PM may also assist with issue escalation, troubleshooting, and management.

For additional warranty and SLA details, refer to the attached "Ping Advanced Identity Cloud Support Services Terms and Conditions.pdf".

Mandatory Project Requirements (Section 4 of RFP)

Please note: *Ping Advanced Identity Cloud, *__formerly known as the "ForgeRock Identity Cloud,"__ is undergoing a product rebrand. As we transition our informational materials to align with "Ping Identity," there may be occasional instances where the previous ForgeRock name is temporarily visible or used interchangeably.*

Requirement:	Meets Req?	Proposer Response:
4.2.2.1 The solution must be able integrate with our existing identity sources including Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and Ultimate Kronos Group (UKG)	Yes	Ping Advanced Identity Cloud integrates with LDAP directories such as Ping Directory Services or Active Directory. Ultimate Kronos Group can be used as an identity source via the SOAP and REST APIs.
4.2.2.2 The solution must provide a seamless migration path for users from our existing identity infrastructure.	Yes	Due to the often complex and critical nature of identity migrations, the Ping Identity Platform simplifies the approach for handling migrations. The Ping platform supports a number of migration approaches and hybrids of each. These include just-in-time (JIT) and pre-emptive or bulk approaches. • Just-in-Time (JIT): This approach provides for co-existence with existing systems until the migration is deemed complete. When a user authenticates, the credentials used, identity details, and context are assessed and a decision is made on how to manage the migration on the fly. Subsequent authentication attempts occur against the migrated account. This avoids 'big bang' migrations and scenarios where passwords may be stored in an irreversible hash. It also allows for identity details to be updated at the time of migration (e.g. ask users to update their phone number or address during migration). • Pre-Emptive/Bulk: Identities at rest are migrated in batches or all at once, using predefined logic to handle the individual scenario of each identity. This approach allows the migration to be handled in one day / weekend / during downtime, reducing the risk of impact to customers. It enables fast decommissioning of legacy systems, and allows for extensive staging and testing of the new system. These scenarios are not mutually exclusive and can be used in conjunction with one another. Modernize IAM Accelerators To help customers migrate from legacy IAM systems to Ping faster and with less expense, Ping has developed a pluggable framework that can be extended to specific legacy systems. Modernized IAM Accelerator kits are available for

Requirement:	Meets Req?	Proposer Response:
		coexistence or phased migration to Ping from all major platforms. The Accelerators include three toolkits: Bidirectional Coexist (Core), Bidirectional Coexist (Edge), and Bulk User Migration. Customers can choose the optimal toolkit (or combination of toolkits) based on their migration strategy. The pluggable system, plug-ins, reference architectures, code, and configuration provided as part of the Modernize IAM Accelerators have been designed to achieve a greater than 25% acceleration in the migration from legacy vendors to Ping.
4.2.2.3 Authentication methods must include SAML2.0, SP(Service Provider) and IDP (Identity Provider) methods of authentication.	Yes	Ping Advanced Identity Cloud supports federation authentication methods such as SAML 2.0 IDP and SP, as well as SAML 2.0 SSO and SLO, Federation with ADFS, SAML 2.0 attribute and advanced profiles, OpenID Connect, and OAuth 2.0, WS-FED, as well as other standards.
4.2.2.4 The solution presented must be cloud-based.	Yes	Ping Advanced Identity Cloud environment is hosted in FedRAMP authorized Google Cloud Platform services.

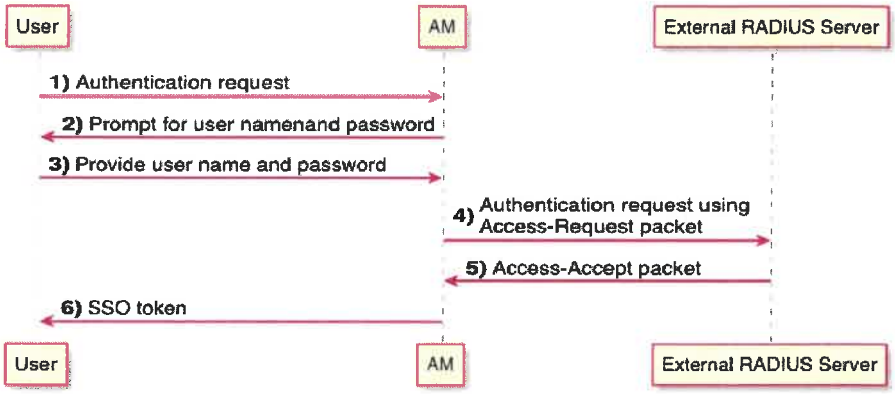
Requirement:	Meets Req?	Proposer Response:
4.3. Qualifications and Experience: Vendor should provide information and documentation regarding its qualifications and experience in providing services or solving problems similar to those requested in this RFP. Information and documentation should include, but is not limited to, copies of any staff certifications or degrees applicable to this project, proposed staffing plans, descriptions of past projects completed (descriptions should include the location of the project, project manager name and contact information, type of project, and what the project goals and objectives where and how they were met.), references for prior projects, and any other information that vendor deems relevant to the items identified as desirable or mandatory below.		Refer to the "Experience and Qualifications" section of this document for a summary of TriVir and Ping experience and qualifications.

Requirement:	Meets Req?	Proposer Response:
4.3.1.1. Can apps integrate directly with the solution's Application Programming Interface (API) to perform restful Application Programming Interface calls such as reading user information, or making changes to user objects, group membership.	Yes	Ping Advanced Identity Cloud's services-based architecture facilitates an easy-to-use RESTful web API framework. The REST API is intended for common use across all Ping components and for invoking underlying services across the platform. It includes a set of easy to remember REST calls to Create, Read, Update, Delete, Patch, Action, and Query (CRUDPAQ) identity objects and services. The simplicity of this common API makes it easy for implementers and deployers of the Ping platform to solve business-critical identity management-related problems quickly. REST APIs are mainly protected for internal use only. If you wish to expose these externally, Ping Identity Gateway can be used for more advanced protection (e.g. OAuth 2.0, and authorization engine). Additionally, various standards are supported for easy integration, including WS-Federation, SAML2, OAuth 2.0, OpenID Connect, and UMA. The Ping Identity Platform includes an online REST API reference, which is an implementation of the Open API Initiative Specification, also known as Swagger. The API Explorer provides useful reference information for developers to create client applications to access Ping's services. This allows developers to easily interact with, test, and explore all API services. The API Explorer can also be used to auto-generate sample code for our platform in any programming language. APIs are available to configure services including but not limited to authentication (journeys, nodes), authorization (creating policies, conditions, rules), OAuth2/OIDC (client registration/management), SAML2 (entity creation and management), identities (creation/management/lifecycle). Instantiation of services via REST APIs is also possible for services, including but not limited to authentication (logging in, passwordless, OTP, MFA), authorization (evaluating user-to-resource access), token exchange services, and federation.

Requirement:	Meets Req?	Proposer Response:
4.3.1.2. Indicate if the proposed solution provides the ability to create custom Application Programming Interface access policies and/or authorized servers. Provide details.	Yes	The Ping Identity Platform facilitates API access management. It includes multiple security elements to finely control who (or which application/service) has which type of access (read, write, query) over which fields. At the lowest level, the REST API uses authorization roles to define access rights. In addition, the delegated administration feature allows the definition of internal roles associated with privileges (typical CRUD operations) on a given subset of managed data. A user assigned such an internal role can manage the defined data from their end-user dashboard without accessing the solution's administration console. Depending on the use case, other access control features can also be leveraged. For example, OAuth 2.0 scope-based access control, where access to data is governed by OAuth 2.0 scopes defined by an administrator. Granting the relevant scope(s) in such a case depends on the business logic and rules that have been configured. Scope values and mapping to real identity attributes are highly flexible through scripting or Java development to add further fineness to the access rules. In Ping Advanced Identity Cloud, customers have complete control over the construction and enforcement of granular security access controls to their tenant environments. Customers can deploy their own security keys for application use cases.
4.3.1.3. Indicate if your service/solution offers Application Programming Interface token management and creation. If the solution offers this capability, provide details on API token management and creation capabilities.	Yes	The Ping Advanced Identity Cloud platform allows for the complete management of token lifecycle via APIs. Additionally, these tokens may be leveraged in no-code/low-code access journeys. Here is an example: https://backstage.forgerock.com/knowledge/kb/article/a20028489 This platform is used at scale by many large and complex enterprise organizations, often with users numbering 10's or 100's of millions, resulting in security tokens (for example, session tokens or OAuth access tokens) numbering several hundred million and above. As well as storing tokens at scale, the service must also handle the necessary rates of scale for operations (e.g., API requests) on tokens, such as validation, introspection, and revocation. Internally, the Ping platform implements a high-scale, highly resilient Core Token Service (CTS) often distributed and replicated over many instances to maintain high-availability and resilience. Externally, a Secure Token Service (STS) is available for applications and APIs to manage and convert their tokens between different token types (e.g., SAML <-> OpenID Connect). Often, this service helps organizations integrate legacy systems which may have specific security token requirements. Ping supports a number of different security token types, and some of these can be configured as "stateful" or "stateless", each of which has different characteristics and use cases. Similarly, for many standards-based tokens, such

Requirement:	Meets Req?	Proposer Response:
		as OAuth access tokens, and OpenID Connect identity tokens, Ping allows for token contents to be modified to suit different use cases. Some examples of this might include modifying the scopes or expiry times of access tokens or including custom claims in OpenID Connect tokens.
4.3.1.4. Describe the Application Programming Interface capabilities your solution offers for integration with custom applications and workflows.	Yes	Workflows are exposed through REST APIs which are secured using OAuth and can be invoked using the workflow APIs. They can also be configured through the low-code/no-code interface called "Orchestrations". External clients, event hooks and Governance events can trigger workflows. In addition to workflow capabilities, Ping Advanced Identity Cloud provides Event Hooks where administrators can incorporate scripts to meet business requirements. For example, an event hook could be used to query an external system and verify a new username or email address is unique, before assigning it to a user. The APIs exposed by the Ping Identity Platform generally fall into the following categories: Standards-Based For standards-based APIs, the modifications permitted fall within the boundaries that apply to the given standard. For example, enabling OAuth/OIDC results in those endpoints being created. Claims handling for OIDC is then easily modifiable through a script stored as part of the configuration. Extensions to the SAML protocol can be handled by the development of a custom SAML adaptor which is enabled through configuration. OAuth 2.0 scope handling can be extended through a custom plugin. Data Management Any managed object created in the Ping solution results in the automatic creation of a new CRUD (Create, Read, Update, Delete) APIs. These are documented in the API Explorer. Many areas of Ping's identity management functionality can be adapted or extended through the use of simple scripts. Default or custom REST endpoints can also be created to perform a wide variety of tasks, such as custom registration flows or account validation. Data management APIs are adaptive to the configuration. For example, when using the API to create a new user the data validation policies applied to the object configuration will be automatically invoked when the API is called. Additional APIs for data management can be created. Custom endpoints are easily created through the development of a script that is deployed as part of the platform configuration. The script has access to the object model and can implement any logic that is necessary. Additionally, Ping Identity Gateway can be used to expose arbitrary endpoints that may call other services and apply business logic as appropriate. The logic may be a simple configuration of Identity Gateway filters and handlers, as well as more complex scripting deployed as part of the configuration.

Requirement:	Meets Req?	Proposer Response:
4.3.1.5. How do you ensure the security and privacy of data transmitted through your Application Programming Interfaces?		All communication is communicated over encrypted channels, and encrypted at rest. PKI-based (or other strong) MFA is required to access interfaces and APIs. API security is typically achieved using the OAuth and OIDC standards and the issuance of bearer tokens. In this context the Ping Identity Platform can provide a fully compliant OAuth 2.0 and OIDC authorization server (AS) that can be used to issue such tokens to TPPs and ensure that SCA has been achieved and consent registered from the PSU before doing so. Payment and account APIs can be made available securely through the use of the Ping Identity Gateway, which can protect APIs by exposing them as an OAuth 2.0 Resource Server. Identity Gateway can be rapidly integrated with the Ping OAuth 2.0 authorization server; however, integrating with a third-party API management solution, such as Apigee, is extremely achievable.
4.3.1.6. Can your solution support standards like Open Authorization (OAuth) 2.0 and OpenID Connect for secure Application Programming Interface access?	Yes	Ping Identity supports standards such as OAuth 2.0 and OpenID Connect for secure API access.
4.3.1.7. Detail the scalability of your Application Programming Interface infrastructure to support high volumes of authentication and authorization requests.		The Ping Identity platform meets enterprise-grade requirements for high performance. We deliver high performance, such as a high volume of authentication transactions per second (tps) STANDARD in our cloud. We place no limits on our customers' performance. Utilizing the flexibility of the Google Cloud framework, performance of the Ping platform is not limited to a particular server farm. If usage is increased, Google Cloud automatically provides a failover to other clusters and performance is not impacted. Because Advanced Identity Cloud is a single, isolated tenant, there is no metering or performance degradation at high-load. Additionally, pricing is simple to not penalize the IAM program for heavy use and load on the system. Specific stress testing performance metrics are available to the State upon entry into an NDA with Ping Identity.

Requirement:	Meets Req?	Proposer Response:
4.3.1.8. Does your solution provide Remote Authentication Dial-In User Service (RADIUS) support that does not require on-premise components?	Yes	RADIUS is supported using Ping Enterprise Connect add-on. Once the module is installed, it can communicate with the Ping Advanced Identity Cloud (AIC).  User AM External RADIUS Server 1) Authentication request 2) Prompt for user namenand password 3) Provide user name and password 4) Authentication request using Access-Request packet 5) Access-Accept packet 6) SSO token User AM External RADIUS Server
4.3.1.9. Indicate if the solution provides supported push notification. If so, what controls can be used to lower the risk of push fatigue attacks.	Yes	The Ping Identity Platform supports push notifications as part of the authentication process, allowing multi-factor authentication or passwordless login via a mobile device. There are several options that can be configured to help lower the risk of push fatigue. The simplest approach is to leverage Ping Protect to assess risk and reduce friction for the user, only forcing MFA when there is medium or high-risk. This reduces MFA Bombing and Fatigue related attack risk. Specific user experiences can be plotted via the no-code/low-code orchestration interface in order to regularly improve user experiences, without complicated customizations or programming. Push notifications work with both iPhone and Android devices. Multi-factor push authentication can be easily achieved with Ping Intelligent Access by configuring an authentication journey to receive push notifications and perform the authentication. If passwordless authentication is required, the authentication flow can be configured to ask the user to enter their User ID but not their password. A push notification is sent to the registered device to complete the authentication using the Ping Authenticator App. The Ping SDKs also support using push notifications within your mobile app as a second factor during authentication. The native push-based authentication mechanism also includes the concept of 'recovery codes' that allows users to authenticate if their device is not accessible or responsive. Ping provides a push notification service via SNS (provided by Amazon AWS). Ping customers can easily subscribe to this service, which sends out push messages from cloud-based and on-premises-based Ping installations. The SNS service delegates push messages to APNS (Apple Push Notification Service) for iOS devices and GCM (Google Cloud Messaging) for Android devices.

Requirement:	Meets Req?	Proposer Response:
4.3.1.10. List the Multi-factor methods supported.	Yes	The Ping Advanced Identity Cloud solution supports a broad range of MFA methods. Some of the methods are provided out-of-the-box and some require integration. The following protocols are supported for MFA out-of-the-box: - OATH, - Push, - OTP, - WebAuthN In addition to the out-of-the-box MFA features Ping Advanced Identity Cloud allows for easy, low-code integration with other MFA providers you might be interested in. Such integrations are usually created as part of Intelligent Access Journeys in the form of a JavaScript based Scripted Decision Node (one of the Journeys building blocks).
4.3.1.11. Does your service offer out of the box login flows that protect against bruteforce attacks?	Yes	Ping Advanced Identity Cloud (AIC) provides OOTB components to help protect against brute force attacks. This is provided through Ping Protect (a.k.a Autonomous Access).
4.3.1.12. Indicate if the proposed service offers out of the box login flows that protect against brute-force attacks and describe the protection against these attacks.	Yes	The Ping solution provides out of the box components to be used in flows that protect against brute-force attacks. These include: • Self-registration features such as email validation and CAPTCHA functionality, or strong identity proofing capability (i.e. live selfie compared to driver's license, out of band authentication). • Intelligent Access for frictionless login using an email address, username, or other modalities, together with push notification, the use of MFA solutions (including biometrics) and step-up authentication. • Contextual Authorization to ensure the authenticity of users, devices, things and services at all times, even during established sessions. • Transactional Authorization requires a user to perform additional authentication action(s) when trying to access a resource protected by an authorization policy. • Account Lockout capabilities. • Short-lived access tokens and refresh tokens where client applications are using OAuth or OIDC to access protected APIs. • Proof-of-possession to eliminate one of the main vulnerabilities of bearer tokens such as OAuth access tokens and OIDC JWT tokens. • Audit logs for tracking user and administrator activities.
4.3.1.13. Detail the		The Ping Identity Platform provides excellent support for authentication factors

Requirement:	Meets Req?	Proposer Response:
authentication methods supported by your platform (e.g., Email Multi-Factor Authentication (MFA), Short Message/Messaging Service (SMS) MFA, Biometric/Web Authentication API (WebAuthN), and define any other capabilities that the vendor offers.		through the wide range of built-in authentication nodes, and nodes that require scripted configuration to work with third-party providers who are not available out of the box Built-in MFA methods include one-time passcode (OTP) via email, SMS or authenticator apps, push notification, WebAuthn (FIDO2 support, Biometrics), and recovery codes. The authentication service is designed to be easily extended, so custom authentication nodes can be created using JavaScript. Ping also provides a native authentication app for iOS and Android devices, which supports both OTP and push notifications. In addition, the Ping SDKs (iOS, Android, and JavaScript) support different types of MFA, including time and counter-based OTP and push notifications. The following protocols are supported for MFA out-of-the-box: - OATH, - Push, - OTP, - WebAuthN **OATH** OATH support can be provided via for example: - Ping Authenticator mobile application which supports HMAC one-time password (HOTP) and time-based one-time password (TOTP) authentication as defined in the OATH standard protocols for HOTP (RFC 4226) and TOTP (RFC 6238). - third party OATH compatible application eg. Google Authenticator Recovery codes are also supported. **Push** Out of the box Push functionality is provided by the Ping Authenticator mobile application. **OTP** - via Email - via an email-to-SMS gateway provider - custom channel (requires low code approach) **WebAuthN including support for Passkeys/Passwordless** - via supported clients Ping Advanced Identity Cloud provides a growing list of certified integrations with Ping's partners through the Marketplace. Currently the following MFA integration options are provided: - Duo - Daon - OneSpan and others

Requirement:	Meets Req?	Proposer Response:
		In addition to the out-of-the-box MFA features Ping Advanced Identity Cloud allows for easy, low-code integration with other MFA providers you might be interested in. Such integrations are usually created as part of Intelligent Access Journeys in the form of a JavaScript based Scripted Decision Node (one of the Journeys building blocks).
4.3.1.14. How does your solution provide adaptive authentication based on risk assessment?	Yes	The Ping Identity Platform natively supports risk-based authentication (or adaptive authentication) through its Intelligent Access capabilities. You can configure Ping so that additional or more secure authentication is only requested when necessary, minimizing user friction while maintaining the appropriate security posture. With Ping Intelligent Access, an authentication journey is broadly composed of information-gathering nodes intended to pick up a wide range of digital "signals" and decision nodes that act upon those signals. Nodes can gather information about the user's authentication environment, i.e., the device they are using, their IP address, geolocation, and time of day; static information about the user, e.g., information already gathered from their profile or information held in other systems of record (contract information, billing systems, contact center interaction); and data available from external services, e.g., identity proofing agencies, threat analysis services, and risk engines. Smart login journeys can be configured to minimize friction and maximize security for legitimate users, while suspicious users could be denied access or redirected to a sandbox environment for further monitoring. The authentication level can be modified or decided on at any point in the authentication flow, therefore adapting the authentication flow depending on the accumulated risk score so far; for example, to allow access based on a low-risk score requires a step up in authentication if the risk score is above a configured threshold, or deny access if the risk score is too high. Multiple paths, each evaluating a digital signal, can be connected to intelligently adjust login journeys, providing a fast, secure login experience and minimizing the risk of data breaches and DDoS attacks. Intelligent Access nodes can receive digital risk signals from any source which exposes applicable data via an API. Selected technology providers deliver tightly integrated joint solutions ready to plug into the Ping platform, emphasizing the following areas: Strong Authentication, Fraud and Risk Management, Behavioral Biometrics, and Know Your Client (KYC) / Identity Proofing. It is also simple to introduce custom nodes supporting other risk sources. Our low-code orchestration nodes and native SDKs allow you to capture various inputs such as location, device integrity, device registration, IP address, and network information. The detection capabilities include any data that can be derived from the incoming HTTP request (e.g., IP address), geolocation, device information, CAPTCHA support, and biometrics (push, WebAuthn). You can find a variety of nodes on the Ping Marketplace, which our Trust Network Technology Partners offer. https://support.pingidentity.com/s/marketplace-integration-home-page#sort=relevancy

Requirement:	Meets Req?	Proposer Response:
4.3.1.15. Can your solution integrate with third-party identity providers for federated authentication?	Yes	The Ping Identity Platform supports all major federation and authorization standards, including SAML 2.0, WS-Federation, OAuth 2.0, OpenID Connect and User-Managed Access (UMA). For SAML 2.0, the Ping platform supports both service provider (SP) or identity provider (IdP) roles. Similarly, for OAuth 2.0, the platform functions either as a client (relying party) or an authorization service. Applications that have federation capabilities, both on-premises and cloud-hosted, should integrate seamlessly with Ping's access management component. Support for the SAML Enhanced Client or Proxy (ECP) profile allows creating a SAML hub that enables straightforward integration with multiple SPs or IdPs. Rather than sharing each entity's metadata with all other entities, metadata for each SP or IdP need only be shared with the hub. Adding and removing services or providers becomes relatively trivial. Additional components can be enabled or plugged in to customize the behavior of the hub, for example, applying logic to direct a user to an appropriate IdP for login, allowing a user to choose their preferred IdP for login, or enriching the user's profile attributes returned by the IdP with additional attributes from an attribute matching service.
4.3.1.16. Indicate which authentication protocols the proposed solution supports (e.g., Security Assertion Markup Language (SAML) 2.0, OpenID Connect (OIDC) , Remote Authentication Dial-In User Service (RADIUS). Identify any other authentication protocols the proposed solution offers.	Yes	The Ping Platform supports the following authentication protocols: SAML 2.0, WS-Federation, OAuth 2.0, OpenID Connect, User-Managed Access (UMA), OAuth 2.0 Device Flow and OAuth 2.0 Proof-of-Possession. FIDO2/WebAuthN, OATH, GSMA Mobile Connect and others. Together these standard protocols enable authentication, authorization and federation features such as advanced authentication flows for single-factor, multi-factor and risk-based authentication. RADIUS is supported using the Ping Enterprise Connect add-on.

Requirement:	Meets Req?	Proposer Response:
4.3.1.17. Explain how your solution adapts authentication methods based on contextual factors like location and device.		Ping applies contextual identity, fine-grained authentication, adaptive risk, and multi-factor authentication at the time of authentication as well as at any point during a digital session. Our continuous security approach ensures the authenticity of people, things, and services at all times and can mitigate risk whenever an anomaly is detected. Contextual authorization is implemented through Ping authentication nodes and authorization policies. With Ping Intelligent Access, signals such as context (e.g. IP address, operating system, browser, device, time of day), behavior (e.g. 'does the user log in at a particular hour', or 'is the location familiar'), and risk-based factors (such as 'is the user accessing sensitive data') can be considered. If an environmental or context attribute changes (e.g. the user's IP address), re-authentication or a stronger credential can be requested. Authorization policies define the rules upon which authorization decisions are made. Since policy decisions are made at the time of access rather than user authentication, contextual authorization enables continuous real-time authorization decisions based on live data. Predefined objects and methods are available to access the user's profile and session data, together with helper functions allowing access to external resources such as web services and REST services. Additionally, authorization policy scripts can be used to define more complex policy decisions locally or call out to external services for additional information upon which to make a decision.
4.3.1.18. How does your solution handle scenarios where a user has lost their primary authentication device?	Yes	Ping can enforce the standards of the State of WV for a number of different actions in this case, such as (but not limited to) the following: ● Disable/log-out/revoke the lost credential ● Allow for the re-enrollment of a new device and credential after strong identity proofing ● Advanced self-service to reduce load on help-desk
4.3.1.19. Can the solution block access based on blacklisted Internet Protocol (IP) addresses or Geography (GEO) location?	Yes	Through the low-code, no-code orchestration interface, such policies may be easily implemented, enforced and maintained over time. In addition to such blacklisting, other risk instrumentation may be leveraged, such as Open Source Intelligence (OSINT) and user and entity behavior analytics instrumentation.

Requirement:	Meets Req?	Proposer Response:
4.3.1.20. Does the service identify, detect, and block suspicious authentication activity?	Yes	Preventing malicious activity as early as possible is the best way to reduce the total cost of fraud. The Ping Identity Platform helps to achieve this in the following ways: • Account Verification: During registration, the platform allows for identity verification via email, or even biometrics or strong identity documents verification. • Sufficient Strength Authentication: Using sufficient strength authentication, continuous authorization, and step-up authentication, can all help prevent unauthorized access to sensitive data. • Risk-Based Authentication: Using Ping Intelligent Access you can pre-identify digital signals such as a user's location, IP address, device type, operating system, browser type, user profile attributes, device cookie, last login, request header, time of day and device fingerprint before a username is even collected. Multiple paths, each evaluating a digital signal, can be connected to intelligently adjust login journeys for suspicious users. • Bot-prevention: PingOne Protect (available in SaaS and on prem) is a cutting edge RBA solution leveraging both heuristics (credential attacks/bot detection) and UEBA (User and Entity Behavior Analytics) which is powered by AI and ML. It provides an increase in security posture while reducing friction where appropriate. • Technology Partners: The Trust Network provides access to the numerous 3rd party technologies to enhance authentication, identity proofing and threat intelligence capabilities that can be easily integrated into the risk engine to further extend the ability to detect fraud. Technologies such as Identity Document Validation, bot detection, and identity data analytics are essential to reduce the occurrence of fake accounts from being opened, while behavioral biometrics, user behavior analysis, transaction risk analysis and exposed credential analysis are instrumental in detecting account takeover and limiting fraudulent purchases. • Transactional Authorization: With transactional authorization, users can securely and conveniently approve high-risk transactions and events, for example via mobile device notifications. This approval mechanism is event-based, increases security, and reduces the threat window for malicious activity. • REST Calls to Report an Anomaly: At the end of the authentication process, it is possible to trigger a REST call to report an anomaly to a tool that can react accordingly. • Centralized Event Audit Logging: The Ping Identity Platform can be configured to generate a comprehensive audit trail, typically consumed by existing enterprise SIEM and analytics tools, such as FireEye®, or ArcSight, which can perform continuous threat detection and alert or block potentially suspect activity. This ensures that all access requests, provisioning activities, authentication, and failed attempts are logged in a centrally managed tamper-evident manner.

Requirement:	Meets Req?	Proposer Response:
4.3.1.21. Does the solution perform behavior detection during authentication? (Example: Impossible Travel, Device context, Network Context,)	Yes	Ping Advanced Identity Cloud provide several authentication nodes that can be used to incorporate geolocation, geofencing, and impossible travel logic in user journeys: • Autonomous Access signal node - Allows you to specify the heuristics and/or anomaly detection to be included in risk score generation during the AI/ML pipelines. The Impossible Traveler heuristic signal can be used to detect if a user is moving between two locations at an impossible speed. • Device Profile Collector node - Gathers metadata about the device used to authenticate. • Device Profile Location Match node - Compares any collected device location metadata with that stored in the user's profile. • Device Geofencing node - Compares any collected device location metadata with the trusted locations configured in the authentication node. • Scripted Decision Node: Runs a script during authentication. Can be used to apply custom logic beyond what is available via the out of the box nodes.
4.3.1.22. How does your platform detect and prevent unauthorized access?	Yes	Through the combination of risk instrumentation and no-code/low-code orchestration, Ping Advanced Identity Cloud detects and prevents unauthorized access, as described in the answers above.
4.3.1.23. Can your platform support attribute-based access control (ABAC) to dynamically adjust access based on user attributes?	Yes	The Ping Identity Platform supports authentication and authorization through a variety of standard mechanisms, implementing key features of NIST 800-162 "Guide to Attribute Based Access Control (ABAC) Definition and Considerations". This allows the State of WV to implement and enforce Policy Decision Points (PDPs), Policy Enforcement Points (PEPs) and other ABAC capabilities. Fine-grained authorization is even possible via Ping Authorize, leveraging the States identity attributes, where appropriate.
4.3.1.24. Can your solution integrate with external identity providers to extend authorization capabilities?	Yes	Ping Identity Platform integrates with external IdPs like Microsoft, Okta and others, and supports all major federation and authorization standards, including SAML 2.0, WS-Federation, OAuth 2.0, OpenID Connect and User-Managed Access (UMA). This extends the capabilities of the original IdP by adding no-code/low-code orchestration, Risk-based authentication and other complementary capabilities. For SAML 2.0, the Ping platform supports both service provider (SP) or identity provider (IdP) roles. Similarly, for OAuth 2.0, the platform functions either as a client (relying party) or an authorization service. Applications that have federation capabilities, both on-premises and cloud-hosted, should integrate seamlessly with Ping's access management component.

Requirement:	Meets Req?	Proposer Response:
4.3.1.25. Can your platform enforce access policies based on contextual factors such as, but not limited to time of day, location, and user behavior?	Yes	This is accomplished and configured through the no-code/low-code orchestration interface (User Journeys).
4.3.1.26. Describe your solution's approach to enforcing the principle of least privilege for user access.		Ping Advanced Identity Cloud is the only cloud SaaS IAM platform that has Identity Governance built-in. This allows application owners and managers to regularly review high-risk access, and remove privileges or system entitlements that are no longer needed, thereby reducing the footprint of privileges for a given user or service account. The Ping Identity Platform supports 'least privileged access'. Whether accessing resources through user interfaces or APIs, Ping delivers fine-grained authorization, a mechanism to distribute and assign strongly-typed scopes to applications, API endpoints, and other protected resources. Scopes are coupled with real-time context at policy-enforcing gates throughout the identity ecosystem. Scopes for fine-grained, actionable rules that can be used to make authorization decisions are also applied.

4.3.1.27. How does your platform support session termination and re-authentication based on inactivity or specific triggers?	Yes	The Ping Identity Platform ensures that user sessions are terminated after an administrative action, or when certain conditions occur. Session termination effectively logs the user out of all systems protected by the Ping platform. Sessions are terminated in the following situations: • User logout: When a user explicitly logs out • Idle timeout: When a user session remains idle for a configured amount of time, it can be automatically terminated by the server. • Lifetime timeout: An overall lifetime configured for sessions can be used to automatically terminate a session regardless of user activity. • Session quota: A user can be restricted to a certain number of concurrent sessions. • Administrative termination: An administrator can view and terminate sessions directly from the console. • REST termination: Sessions can be queried and terminated programmatically using REST APIs. When a session terminates, Ping's access management component responds by removing CTS-based sessions from the CTS store and from the server memory caches. With the user's session no longer in the CTS, Ping forces the user to re-authenticate on subsequent attempts to access protected resources. When a user explicitly logs out of Ping's access management component, the system also attempts to invalidate the iPlanetDirectoryPro cookie in the user's browsers by sending a Set-Cookie header with an invalid session ID and a cookie expiration time that is in the past. In the case of administrator session termination and session timeout, Ping cannot invalidate the iPlanetDirectoryPro cookie until the next time the user accesses Ping. Single Logout (SLO) Single logout (SLO) is typically provided either as a REST service or by exposing a SAML compliant single logout endpoint. Session Revocation The Ping Identity Platform can instantly revoke access for any user/group/service/app where stateful CTS-based sessions and tokens have been used. The Ping platform supports the endpoint defined in http://tools.ietf.org/html/rfc7009 - Token Revocation used to revoke both access and refresh tokens. Revoking a refresh token also revokes any other associated tokens that were issued with the same authorization grant. If a client has multiple access tokens for a single user that were obtained using different authorization grants, the client would need to make multiple calls to the revoke token endpoint to invalidate each token.

Requirement:	Meets Req?	Proposer Response:
		The Ping Identity Platform creates an authentication session to track the user's authentication progress through an authentication tree. Once the user has authenticated, a session is created to manage the user's or entity's access to resources. Session related services are stateless unless otherwise indicated; they do not hold any session information local to the Ping instances. Instead, they store session information either in the CTS token store or on the client. This architecture allows you to scale your Ping platform infrastructure horizontally since any server in the deployment can satisfy any session's request.
4.3.1.28. Does the solution have the ability to have isolated lower environments for the purposes of testing / development?	Yes	Ping Advanced Identity Cloud includes a dev environment, staging environment and production environment. Upon request, additional isolated, lower sandbox environments may be acquired.

4.3.1.29. Does your solution provide multiple environments for testing purposes?	Yes	Ping Advanced Identity Cloud comes with three separate tenant environments out of the box, where each has a different purpose: • Development • Staging • Production Using multiple environments ensures any changes you make are fully tested before they are made available to end users. You can promote configuration from Development to Staging or Staging to Production. You cannot promote configuration straight from Development to Production. Sandbox environments A Sandbox environment can also be added to your subscription if required; this is a completely separate environment from your tenant environments and configuration cannot be promoted from it. Development The Development environment is the place where you can develop and test out potentially breaking changes without impacting other environments or users. Once these changes have been fully tested and any bugs fixed, you can promote these changes to your Staging environment. You should note the following: • It is a mutable environment. This means you can customize it and build new authentication experiences, all through a cloud-based UI and API. • It is not scaled for high availability or performance, and should not be used for any performance or load testing. • The number of identities is limited to 10,000. Staging The Staging environment is intended for testing applications with realistic settings and data. It should mirror your Production environment as closely as possible. Once your changes have been promoted to Staging, you should test them thoroughly to ensure they work as expected in a realistic environment and also to performance/load test your changes to ensure they do not impact performance. Once you have completed your testing, you can promote these changes to your Production environment. You should note the following: • It is an immutable environment.

Requirement:	Meets Req?	Proposer Response:
		• It is scaled for high availability and performance to match your Production environment to facilitate realistic testing. Production The Production environment contains all your live data, and is intended for real applications and end users. No development or testing should take place in this environment. You should note the following: • It is an immutable environment. • It is scaled for high availability and performance. Understanding the promotion process When you want configuration promoted from one environment to another, you can promote the configuration yourself. The high-level process for promotion is as follows: 1. Promote configuration from your Development environment to Staging. 2. Confirm your Staging environment is working correctly after promotion. It is important you test your Staging environment thoroughly to ensure it is working as expected before proceeding. 3. Promote configuration from your Staging environment to Production. Please be aware of the following important points: • All static configuration in an environment is promoted. This means you cannot pick and choose what items are promoted, or only promote one realm but not the other. • When you promote configuration from one environment to another, you must lock the lower and upper environments to prevent any conflicts during the promotion period. • Automated backups are taken regularly and all configuration data is stored in Git repositories with the history preserved. TriVir provides IAM DevOps tools and automations to help manage configuration and CI/CD with automation. Additionally, automated testing is provided to help accelerate validation, post-promotion.
4.3.1.30. Does the solution allow automation of tasks through scripting or	Yes	Ping applies a common REST API format(referred to as Common REST or CREST) across the whole platform. Execution of platform REST endpoints can be automated to execute business logic or automate otherwise complex, manual tasks.

Requirement:	Meets Req?	Proposer Response:
Application Programming Interface calls?		
4.3.1.31. Do you offer flexible application integrations such as general Security Assertion Markup Language (SAML), OpenID Connect (OIDC) and Open Authorization (Oauth) connectors?	Yes	The Ping platform keeps simple things simple, and makes complicated integrations possible, leveraging standards such as Security Assertion Markup Language (SAML), WS-Federation and OpenID Connect (OIDC). Your enterprise applications can be integrated with the Ping Identity Platform for single sign-on using either policy agents, federation technologies, or REST APIs. This enables anyone authenticated by the Ping platform to access these applications with single sign-on. OOTB connectors exist for every major application integration standard.
4.3.1.32. Do you offer deployment assistance, documentation, or training to ensure a smooth transition to your platform?	Yes	TriVir offers this platform to the State, coupled with implementation and migration services. Please refer to the Methodology and Approach section of this document for additional details. Ping training subscription and enablement is also included in the pricing, for up to 6 individuals.
4.3.1.33. Can the solution leverage Active Directory as the Identity Provider? If so, do agents need to be installed on our systems to facilitate that communication? Additionally, is your solution capable of syncing that information in real time?	Yes	Ping Identity solution can leverage Active Directory as the authoritative identity source. An agent may be required based on requirements (i.e. if password sync is required from AD to the IAM solution). OOTB LDAP Connector for AD does not require an agent. Yes, near real-time synchronization is provided for AD and Entra ID (Azure). Specific attributes may be identified as “need to sync immediately” to achieve real-time sync where needed.
4.3.1.34. If an agent is required to facilitate a connection between		No agent is required for AD connectivity. All communication is communicated security over TLS.

Requirement:	Meets Req?	Proposer Response:
Active Directory and your service, please describe how that information is exchanged securely.		
Additionally, please describe how redundancy and failover can be configured to ensure there is a constant flow of information.	Yes	The Ping Advanced Identity Cloud is built on redundant, fault-tolerant infrastructure inside of Google Cloud Platform. Refer to "Ping Advanced Identity Cloud Architecture and Platform Capabilities" in this document for more information.
4.3.1.35. Does the solution support the ability to import password hashes from other Identity Providers (IDPs)? If so, describe what hashing algorithms are supported and how that process works.	Yes	Importing of hashed passwords from arbitrary sources is available in Ping Advanced Identity Cloud deployments, however this is discouraged. There are better methodologies around transitioning legacy account passwords to modern credentials. This will be discussed in greater detail during the initial Requirements Assessment.
4.3.1.36. Do you have an administrator dashboard User Interface (UI) to manage users? Can you enforce a specific multi-factor type for administrative access?	Yes	Ping Advanced Identity Cloud offers an administrative console to manage users, privileges, policies, and other services. Different types of MFA are enforced for any administrative role access.

Requirement:	Meets Req?	Proposer Response:
4.3.1.37. Does the solution support external federation? If so, how, and what Identity Providers (IdPs) are supported?	Yes	The Ping Identity Platform supports all major federation and authorization standards, including SAML 2.0, WS-Federation, OAuth 2.0, OpenID Connect and User-Managed Access (UMA). Common trusted Identity Providers include Apple, Google, Facebook, Microsoft Azure/Entra, Linkedin and many others. For SAML 2.0, the Ping platform supports both service provider (SP) or identity provider (IdP) roles. Similarly, for OAuth 2.0, the platform functions either as a client (relying party) or an authorization service. Applications that have federation capabilities, both on-premises and cloud-hosted, should integrate seamlessly with Ping's access management component. Support for the SAML Enhanced Client or Proxy (ECP) profile allows creating a SAML hub that enables straightforward integration with multiple SPs or IdPs. Rather than sharing each entity's metadata with all other entities, metadata for each SP or IdP need only be shared with the hub. Adding and removing services or providers becomes relatively trivial. Additional components can be enabled or plugged in to customize the behavior of the hub, for example, applying logic to direct a user to an appropriate IdP for login, allowing a user to choose their preferred IdP for login, or enriching the user's profile attributes returned by the IdP with additional attributes from an attribute matching service.
4.3.1.38. How does your solution streamline user onboarding and offboarding processes?		The Ping Identity Platform enables automated provisioning and deprovisioning of identities, user accounts, and entitlements like groups, roles, or other assignments of privileges in a connected system through its identity connectors and synchronization engine. The Ping identity synchronization engine can provision users in the Ping platform from an external source of truth (like AD, or like an HR/HCM system) or act as source of truth and provision users to connected systems. Synchronization can occur in either direction or in both directions. The administrator can configure provisioning, deprovisioning, and profile data synchronization behavior, thus fully or partially automating the onboarding, updating, and removal of user accounts. The Ping Identity Platform includes a number of specific application connectors for common business applications like SAP, Workday, Salesforce, Active Directory, etc. and generic connectors supporting standards like LDAP, SCIM, JDBC, REST, Groovy Script, Linux Shell Scripts, etc. allowing the integration of large numbers of application supporting any of those standards.

Requirement:	Meets Req?	Proposer Response:
4.3.1.39. How does your platform handle role-based access control and user provisioning?		Ping Advanced Identity Cloud performs user provisioning and lifecycle management based on data events in authoritative sources. These events may also be triggered as a result of an access request, access approval or other governance-related review, or certification. The Ping platform implements automated provisioning of accounts and entitlements based on roles. These components work together to enable the implementation of Role-Based Access Control (RBAC). Roles may be granted at provisioning time (birthright-access) or as a result of a request. The Ping platform handles RBAC natively and supports several approaches according to requirements and the capabilities of the particular service. Ping Identity Management can synchronize entitlements in connected systems based on business roles. This means that users granted a particular role might become a member of a specific Active Directory group. The applications relying on this group membership then enforce the policy the application is configured with. More generally, access control using roles, attributes and contextual information about the current request can be implemented using the Ping authorization engine. Note: The platform can leverage roles in existing source systems (e.g. an underlying LDAP directory) to provide RBAC.

4.3.1.40. What customization options are available for the user interface and branding?		The Ping End User and Login UIs have a default theme that includes the logos, colors of buttons and links, and so on. This default theme applies to the entire realm. You can add custom themes so that your end users are presented with screens specific to their authentication journey. Custom themes let you create a different look and feel for each brand that you support, including different profile page layouts, logos, headers, and footers. A theme is followed throughout an authentication journey. This means that if a user logs in through the Login UI with a specific theme, the remaining pages in the journey will have that same theme. Various aspects of the theme may be customized: • Styles lets you set the color of text, links, menus, buttons, and background pages. • Logos lets you set the logo on the login page, and other pages in the authentication journey, as well as the Favicon that is displayed for the Login and End User pages. Specify the URL to an image to set the Sign-in Logo and, optionally, the End User and End User Collapsed logos. Images are resized proportionally so that they are not distorted. You can resize individual logos according to where they appear in the journey. If you specify a Sign-in Logo and do not specify any of the optional logos, the Sign-in Logo is used throughout. • Layout lets you customize the components and layout of end-user pages: • For Journey pages, specify whether objects are centered, left-aligned, or right-aligned on the page, and set custom headers and footers. Headers and footers can take HTML or inline CSS to insert links, classes, and so on. Scripting is not currently supported in headers and footers. • For Account pages, specify which fields should be displayed for end user accounts. Use this page, for example, to let users edit their passwords, trusted devices, and so on. The footer on this page is separate from the footer that is displayed on the Journey page. This lets you set up different buttons, links, and so on, that are displayed to a user once they have logged in. Identity Cloud hosts default web pages you can use in end-user journeys. The pages are designed to help you quickly create and test common user self-service operations. For example, the default login journey starts with a sign-in page for capturing username and password. The journey ends with the end-user's profile page. By deactivating the default end-user profile, you can still use the hosted end-user journey UI, while denying unauthorized access to end-user profiles. Your customers manage only their own profiles, or delegate administration, using your application. The Ping Identity Platform offers several levels for organizations to deliver custom UIs: • Minor theming of the OOTB UI. The supplied UIs are built using standard HTML, CSS and JSPs. Simple changes such as inserting a custom brand or logo to reflect your organization are achieved by modifying the HTML and CSS stylesheets. For minor changes to the Self-Service UI, the simplest approach is

Requirement:	Meets Req?	Proposer Response:
		to use realm theming. This allows basic branding of the end-user interface with colors and a logo image. A Theme node (available on the Ping Marketplace) allows you to easily customize the look and feel of any authentication or registration flow and optionally change the Login button text. • Restyling of the standard UI through Bootstrap theming. Further enhancements can be made using a responsive design framework such as AngularJS or Handlebars.js. • SDKs. Ping supports SDKs for mobile and web authentication, which can be fully customized and branded according to your requirements. Our SDKs interact directly with and adapt on the fly to any modification to user journeys, including authentication, registration and customer self-service. This means that end-user application changes are not required when updating user journeys; a major benefit when adding security measures to respond to an evolving threat landscape or when adding new features. The SDK team continually develops new capabilities to enable our customers' developers to quickly and easily create exciting yet secure experiences for their customers. • Rich customization using your choice of UI frameworks, calling REST APIs directly. Complete UI customization, or integration with your existing portals, can be achieved by invoking the same REST APIs as Ping's supplied UI. This allows new or existing apps and portals to integrate with the Ping platform by reusing the integration patterns and code used in the supplied UI. • Complete availability of the Ping UI as open source. Powered by Vue.js and available on GitHub, this capability allows you to easily build out and expand the supplied UI to evolve and grow to suit your changing requirements while providing a peerless end-user experience.
4.3.1.41. Are all Multi-Factor Authentication (MFA) factors available for use in authenticating a user prior to performing self-service password maintenance? (E.g., Forgot Password, Change Password, Account Unlock)	Yes	All factors that a user has enrolled for MFA can be configured as a required step prior to performing self-service password maintenance. Additionally, identity proofing and verification steps may be taken before performing self-service functions.

Requirement:	Meets Req?	Proposer Response:
4.3.1.42. During a password reset, does the solution compare the supplied new password against a public database of known-compromised credentials and block the use of compromised credentials?	Yes	Advanced Identity Cloud allows for the checking against OSINT repositories (via API) to check passwords against known-compromised data sets. Ping authentication nodes (including Have I Been Pwned and VeriClouds CredVerify) can securely test user-provided passwords against publicly available services. Ping additionally provides a variety of password validators: • Password History (the password must not have been used before in the last x resets) • Attribute Value (to ensure personal information from the digital identity is not included in the password) • Character Set (the password should include/exclude a subset of characters) • Dictionary • Length-Based Password Validator • Repeated Characters • Similarity-Based Password Validator • Unique Characters

Requirement:	Meets Req?	Proposer Response:
4.3.1.43. Describe the self-service features available to end-users for password resets and profile updates.		The Ping Identity Platform provides user self-service features that enable users to self-register, manage their profile and consent settings, securely reset forgotten passwords, and retrieve their usernames. The service is fully accessible over REST APIs and through the customizable Ping UI and SDKs. Supported features relating to self-service include: • Self-registration • Social account mapping • Forgotten password reset • Forgotten username support • Email validation • CAPTCHA (for use with reCAPTCHA v2 and hCaptcha v1) • Knowledge-based authentication (KBA) questions • Terms & Conditions • Customizable confirmation emails • Password policy configuration • Profile management • Identity proofing and validation Various user flows are supported and can be configured easily using a simple drag-and-drop journeys feature. Ping provides a range of self-service nodes, as well as pre-built flows (designed on best practices) that you can use as a base for configuring your own self-service flows. These include sample journeys for registration, login, progressive profiles, password reset, forgotten username, and password update. The Ping platform also includes a profile dashboard that enables users to manage all identity data about themselves in a single place, with self-service controls for editing personal information, opting-in or opting-out of data collection, regulating device pairing, authorizing app access with greater login and security options as well as managing privacy and consent features such as "right to be forgotten". Further onboarding and provisioning features are offered in Ping's Identity Management solution. Synchronization and workflow triggers can be used to extend self-service functionality to include functions such as identity proofing, access requests, approvals, identity de-duplication, and provisioning across multiple systems.
4.3.1.44. How does your platform handle de-provisioning of user access when an employee leaves the		The Ping Identity Platform enables automated provisioning and deprovisioning of identities, user accounts, and entitlements like groups, roles, or other assignments of privileges in a connected system through its identity connectors and synchronization engine.

Requirement:	Meets Req?	Proposer Response:
organization?		The Ping identity synchronization engine can provision users in the Ping platform from an external source of truth or act as source of truth and provision users to connected systems. Synchronization can occur in either direction or in both directions. The administrator can configure provisioning, deprovisioning, and profile data synchronization behavior, thus fully or partially automating the onboarding, updating, and removal of user accounts. The Ping Identity Platform includes a number of specific application connectors for common business applications like SAP, Workday, Salesforce, Active Directory, etc. and generic connectors supporting standards like LDAP, SCIM, JDBC, REST, Groovy Script, Linux Shell Scripts, etc. allowing the integration of large numbers of application supporting any of those standards.

Requirement:	Meets Req?	Proposer Response:
4.3.1.45. What mechanisms are in place to ensure that user access is granted or revoked promptly?		Since Ping Advanced Identity Cloud enforces changes sent from authoritative sources, timely terminations are enforced in the IAM platform and down-stream. When access is added, the system also initiates downstream automated fulfillment quickly so that the user may begin to leverage their new access in real-time. The system also allows for granular authorization through ABAC/RBAC services: Ping Advanced Identity Cloud acts as a Policy Decision Point (PDP) as well as Policy Administration Point (PAP) and enforces access by using Policy Enforcement Points (PEPs). A PEP can be a policy agent (typically installed in the same web server or container as the application being protected), Ping SDK, Ping Identity Gateway, or a third-party gateway. -> The PEP requests a policy decision from the PDP based on various factors, including requested resource, subject (user), token (if any), or environment (IP address, time of day, etc.). Ping Advanced Identity Cloud evaluates policies that apply to the requested resource. If multiple policies apply, they are applied in order until either all have been evaluated or a deny decision is reached. -> The response to the PEP is an entitlement that indicates the resource(s) to which it applies, the actions permitted/denied on the resource, and optionally response attributes and advice. Where the overall decision is to deny, the advice can be used by the PEP to take remedial action, for example, if access to a resource was denied because the authentication level was too low, the PEP can attempt to let the user re-authenticate using a stronger form of authentication. -> Developers of resource servers and other services wishing to implement their own policy enforcement capability can take advantage of Ping's authorization REST API. REST endpoints are available to request policy decisions, manage policies, resource types, application types, environment conditions, subject conditions, and import/export policies in eXtensible Access Control Markup Language (XACML) format. -> Ping Advanced Identity Cloud can also act as an authorization server in OAuth 2.0, OpenID Connect scenarios, therefore delivering and validating various types of tokens to clients accessing compliant resource servers. -> Ping Advanced Identity Cloud relies on policies to reach authorization decisions, such as whether to grant or to deny access to a resource or grant or deny an OAuth 2.0 scope. With dynamic OAuth 2.0 authorization, when Ping Advanced Identity Cloud receives a request for scopes, the authorization service grants or denies access scopes dynamically by evaluating authorization policies at runtime. -> Policies are stored in Ping Advanced Identity Cloud.

Requirement:	Meets Req?	Proposer Response:
4.3.1.46. Does your service integrate with third-party logging solutions? If so, what logging formats are supported (i.e. JavaScript Object Notation (JSON), Comma separated Variable (CSV), and define any other capabilities that the vendor offers. And are they sent in real-time?	Yes	Ping Advanced Identity Cloud implements a REST-based Audit Logging Service across all its components, which captures all auditing events critical for system security, troubleshooting, usage analytics, and regulatory compliance. Audit logs gather operational information about events occurring within a deployment to track processes and security data, including authentication mechanisms, system access, user and administrator activity, error messages, and configuration changes. Audit logs are commonly consumed by third-party SIEM and analytics solutions, such as FireEye, Guardian Analytics, Logstash, and Splunk. The data is held for 30 days and is available to be downloaded via a REST API. The Ping Advanced Identity Cloud audit log is accessed via a read-only API.The Ping Advanced Identity Cloud audit log is accessed via API keys. Your Identity Cloud tenant administrators manage the creation and deletion of the API keys and how they are distributed.
4.3.1.47. Does the solution provide reporting on authentication statistics (Single Sign On (SSO) attempts, Multi-Factor Authentication (MFA) enrollment, new user creation, lockouts, permission changes, password resets), and define any other capabilities that the vendor offers.	Yes	Ping Advanced Identity Cloud customers have access to a comprehensive REST API that includes detailed identity and system auditing event logs and monitoring information, which you can then use in whatever reporting/analytics systems you prefer (for example, Prometheus, PowerBI, Splunk, etc.).
4.3.1.48. How long are the logs maintained?		All log data is stored in Google Cloud Platform's logging infrastructure, which provides protection against deletion or change. By default, administrative log data is retained for 365 days, and data-access logs are retained for 30 days. We also forward infrastructure logs (i.e., not AM, IDM or DS logs) to an offsite log analysis system.

Requirement:	Meets Req?	Proposer Response:
4.3.1.49. Do you provide any ability to create or pull reports? Do you have any templates for executive type reports?	Yes	The Ping Identity Platform includes a basic reporting service but typically customers integrate with industry-leading reporting technologies. Our extensive audit logging allows audit logs to be consumed by well-known SIEM and analytics tools. Ping's identity management component includes a dashboard in which standard third-party reporting widgets, such as Kibana (based on the Elastic Stack), can be embedded. Reports generated by the Ping solution can be modified by creating a workflow where authorized users can select, for example, the type of report and content of their choice. Reports generated outside our solution depend on the tool used to create them. Reports can be scheduled to run on a regular basis by an administrator, or by end-users with simple customization. In addition to the fine-grained scheduling facility, a scheduled batch scan can be performed for a specified date, and a task automatically runs when this date is reached. The basic reporting service enables you to generate reports on specific sets of data within a resource collection. While this reporting service does not replace a comprehensive data analysis platform, it can avoid the need for third-party data analysis tools in simple use cases. Admin dashboard widgets enable you to audit events and monitor system capabilities such as logins and registrations, system health, and resource usage. The Ping platform also includes a metrics endpoint for gathering and processing monitoring data in Prometheus. If deeper analytics are required tools such as Grafana can be used to create customized charts and graphs based on the information collected by Prometheus.

4.3.1.50. Please provide the full list of security events and descriptions captured by your service.		The audit service logs information related to the following events: ● System access ● System activity ● Authentication operations ● Configuration changes ● Reconciliations ● Synchronizations Default Audit Event Topics The audit service logs the following event topics by default: Access Events IDM writes messages at system boundaries, that is REST endpoints and the invocation of scheduled tasks in this log. In short, it includes who, what, and output for every access request. Default file: openidm/audit/access.audit.json Activity Events IDM logs operations on internal (managed) and external (system) objects to this log. Entries in the activity log contain identifiers, both for the action that triggered the activity, and for the original caller and the relationships between related actions, on internal and external objects. Default file: openidm/audit/activity.audit.json Authentication Events IDM logs the results of authentication operations to this log, including situations and the actions taken on each object, including when and how a user authenticated and related events. The activity log contains additional detail about each authentication action. Default file: openidm/audit/authentication.audit.json Configuration Events IDM logs the changes to the configuration in this log. The configuration log includes the "before" and "after" settings for each configuration item, with timestamps. Default file: openidm/audit/config.audit.json Reconciliation Events

IDM logs the results of reconciliation runs to this log (including situations and the resulting actions taken). The activity log contains details about the actions, where log entries display parent activity identifiers, recon/reconID, links, and policy events by data store.

Default file: openidm/audit/recon.audit.json

Synchronization Events

IDM logs the results of automatic synchronization operations (liveSync and implicit synchronization) to this log, including situations and the actions taken on each object, by account. The activity log contains additional detail about each action.

Default file: openidm/audit/sync.audit.json

For detailed information about each audit event topic, see Audit Event Handler Configuration.

Custom Audit Event Topics

You can create custom event topics to collect audit information for customizations, such as scripts. Creating a new event topic has a few additional requirements:

You must specify a schema for your custom topic. The schema determines the structure and type of information stored in audit logs.

Your script needs to call the new audit event topic (for example audit/example), providing the values you specified in your topic schema.

Create custom event topics directly in audit.json, or using the Admin UI. The following example, from an audit.json file, has been modified to include a custom audit event topic named example:

```
"eventTopics": {
 "authentication": {},
 "access": {},
 ...
 "example": {
  "schema": {
   "$schema": "http://json-schema.org/draft-04/schema#",
   "id": "/",
   "type": "object",
   "properties": {
    "_id": {
     "id": "_id",
     "type": "string"
    },
        "transactionId": {
          "id": "transactionId",
          "type": "string"
        },
        "timestamp": {
          "id": "timestamp",
          "type": "string"
        },
        "status": {
          "id": "status",
          "type": "string"
        },
        "message": {
          "id": "message",
          "type": "string"
        }
      },
      "filter": {
        "actions": []
      }
    }
  }
}
```

When your topic has been created, add it to an event handler such as the JsonAuditEventHandler, in order to output the audit logs in your desired format. New audit events can be sent by calling the audit topic endpoint (in this example, audit/example). For example, the following REST call will add a new audit event for the example topic:

```
curl \
 --header "X-OpenIDM-Username: [redacted]" \
 --header "X-OpenIDM-Password: [redacted]" \
 --header "Accept-API-Version: resource=1.0" \
 --header "Content-Type: application/json" \
 --request POST \
 --data '{
   "transactionId": "779d3cda-dab3-4e54-9ab1-e0ca4c7ae6df-699",
   "timestamp": "2019-02-12T01:11:02.675Z",
   "status": "SUCCESS",
   "message": "Script has run successfully."
 }' \
"http://localhost:8080/openidm/audit/example"
{
  "_id": "2091c3f2-7a22-47bf-a618-b2af4c322e46-1192",
  "transactionId": "779d3cda-dab3-4e54-9ab1-e0ca4c7ae6df-699",
  "timestamp": "2019-02-12T01:11:02.675Z",
  "status": "SUCCESS",
```

Requirement:	Meets Req?	Proposer Response:
		"message": "Script has run successfully." }
4.3.1.51. Explain the logging mechanisms in place to capture identity-related events and activities.		Ping Advanced Identity Cloud implements a REST-based Audit Logging Service across all its components, which captures all auditing events critical for system security, troubleshooting, usage analytics, and regulatory compliance. Audit logs gather operational information about events occurring within a deployment to track processes and security data, including authentication mechanisms, system access, user and administrator activity, error messages, and configuration changes. Audit logs are commonly consumed by third-party SIEM and analytics solutions, such as FireEye, Guardian Analytics, Logstash, and Splunk. The data is held for 30 days and is available to be downloaded via a REST API. The Ping Advanced Identity Cloud audit log is accessed via a read-only API.The Ping Advanced Identity Cloud audit log is accessed via API keys. Your Identity Cloud tenant administrators manage the creation and deletion of the API keys and how they are distributed.
4.3.1.52. How does your solution provide real-time alerts for security incidents and policy violations?	Yes	From a platform perspective, Ping follows strict SLAs that guide security governance, real-time alerts and notifications. These are described in the Customer Success Package, which will be made available to the State of WV upon entering into an NDA. For users managed in the platform, Ping includes a Policy feature that allows the creation of policy rules that define combinations of user details, roles or assignments, which constitute policy violations. Policies can be defined using the Ping supplied UI. When a scan is performed against a policy, violations will be created for users based on the rules of the policy. The violation details the policy violated, the user in violation, and the specific rules violated. Policy violations detected during a certification are added to workflow for approval. The owner of the violation may choose to remove the violation via remediation or grant an exception to the user and allow the violation to exist for a defined period of time. Policies can be configured with risk thresholds. When specified change events occur a certification can be triggered that evaluates these policies and associated workflow can trigger actions. An overall user risk score is the maximum of the risks associated with each policy violation.

Requirement:	Meets Req?	Proposer Response:
4.3.1.53. Can your solution meet compliance requirements by generating audit trails and activity reports?	Yes	Ping Advanced Identity Cloud implements a REST-based Audit Logging Service across all its components, which captures all auditing events critical for system security, troubleshooting, usage analytics, and regulatory compliance. Audit logs gather operational information about events occurring within a deployment to track processes and security data, including authentication mechanisms, system access, user and administrator activity, error messages, and configuration changes. Audit logs are commonly consumed by third-party SIEM and analytics solutions, such as FireEye, Guardian Analytics, Logstash, and Splunk. The data is held for 30 days and is available to be downloaded via a REST API. The Ping Advanced Identity Cloud audit log is accessed via a read-only API.The Ping Advanced Identity Cloud audit log is accessed via API keys. Your Identity Cloud tenant administrators manage the creation and deletion of the API keys and how they are distributed.
4.3.1.54. What options are available for exporting logs and reports to external systems or Security information and event management (SIEM) solutions?		As mentioned above, all logs are available to the State of WV SIEM to pull and leverage, in real-time.
4.3.1.55. Indicate and identify any countries where you provide services to clients outside of the United States (and US territories).		Ping Identity is a global company and has offices/customers worldwide.
4.3.1.56. Have there been any significant security breaches in the past 24 months? If so please provide documentation of how this breach occurred, how many accounts	No	No known security breaches in the past 24 months.

Requirement:	Meets Req?	Proposer Response:
were involved, and the remedy/solution for the breach.		
4.3.1.57. Provide information on how clients are informed of maintenance and patch releases.		Ping will provide notification of any change that may impact the service via an alert notice posted to Ping Backstage, RSS feed and via your Ping Customer Success Manager (CSM). Our goal is to provide notification of impacting changes up to 90 days in advance. New or changed functionality will be detailed in accompanying release notes. Ping events such as Identity Live and the Customer Advisory Board are also opportunities to learn about new and upcoming functionality.
4.3.1.58. Where does the solution reside?		Ping Advanced Identity Cloud is deployed in Google Cloud Platform services. Regional clusters provide protection by distributing Kubernetes resources across multiple zones within a region. More specifics found here: https://www.forgerock.com/platform/identity-cloud/regions
4.3.1.59. Describe how your service is compliant with Americans with Disabilities Act (ADA) standards and how you support screen readers and descriptive technology.		The Ping Advanced Identity Cloud is Section 508 and WCAG compliant. VPATs are currently being updated for the Ping Advanced Identity Cloud and will be fully supported through Ping. The UI is primarily a React interface, allowing the majority of accessibility standards to be compliant through inheritance from the browser platform. There are no UIs outside of a browser or mobile device application.
4.3.1.60. Describe how your service provides failover and redundancy.		Ping Advanced Identity Cloud is deployed in Google Cloud Platform services. Regional clusters provide protection by distributing Kubernetes resources across multiple zones within a region. We use regional clusters to increase the availability of both a cluster's control plane (master) and its nodes by replicating them across multiple zones in a region. This provides the advantages of multi-zonal clusters, with additional benefits. If one or more (but not all) zones in a region experience an outage, the cluster's control plane remains accessible as long as one replica of the control plane is available. Also, during cluster maintenance such as a cluster upgrade, only one replica of the control plane is unavailable at a time, and the cluster is still operational.

Requirement:	Meets Req?	Proposer Response:
4.3.1.61. What controls does your service have in place to prevent automated attacks?		Account Verification: During registration, the platform allows for email verification or identity proofing/verification. You can also utilize integrations to third parties to carry out identity verification (proofing) or simple tools such as Google reCAPTCHA to prevent automated attacks.
4.3.1.62. How does your solution ensure high availability and resilience in the face of unexpected outages or disasters?		Regional clusters provide protection by distributing Kubernetes resources across multiple zones within a region. We use regional clusters to increase the availability of both a cluster's control plane (master) and its nodes by replicating them across multiple zones in a region. This provides the advantages of multi-zonal clusters, with additional benefits. If one or more (but not all) zones in a region experience an outage, the cluster's control plane remains accessible as long as one replica of the control plane is available. Also, during cluster maintenance such as a cluster upgrade, only one replica of the control plane is unavailable at a time, and the cluster is still operational.

Requirement:	Meets Req?	Proposer Response:
4.3.1.63. Provide your data backup and recovery strategies to safeguard against data loss?		Customers are not responsible for restoring data from backup media. Ping handles any restore operations for Ping Advanced Identity Cloud. We automatically delete log data after 30 days and we delete environments and log data after the contract has ended via scripts. We test restore from a backup about once a quarter. We also run through incident scenarios (known as "Katas") once a month to test our reactions to production issues, which sometimes include executing recovery procedures. Ping Advanced Identity Cloud maintains complete tenant isolation with no data being co-located within a data store with other customer data. When deploying a cloud environment you can choose where the tenant and tenant data will reside. Your data will be maintained in this location at all times. For backup copies, data will be stored in a backup format in another location within your region to maintain DR and BC best practices. Backups are stored in multiple zones within the region and are separated by significant physical distance .We currently run backups every 2 hours (RPO) and we can restore from backup in 1 hour (RTO) within the region. We also have backups between regions from the same geo. Inter-regions RPO is 2 hours and RTO is 8 hours. All critical data is automatically backed up. This not only includes service infrastructure data such as DNS records but also customer-specific information. The backup process signs and verifies the integrity of backups and encrypts backup files, therefore providing integrity, confidentiality, and data availability with respect to disaster recovery. The process encrypts the keys used for signing and encryption with the shared master key and, for portability, stores the encrypted keys in the backup files. For additional backup options, Ping Advanced Identity Cloud allows you to stream logs out to a cloud storage system of your choice and identity data can be synced via our Synchronization or Remote Connector Server (RCS) capability.
4.3.1.64. Describe your approach to continuous monitoring and threat detection within your identity infrastructure.		As described in https://cloud.google.com/security/infrastructure/design, Google has implemented file integrity monitoring at the physical server level. Ping implements file integrity monitoring at the Kubernetes level through its use of Google Compute Engine Shielded VMs as Kubernetes nodes. Additional monitoring and threat detection details are available in the Customer Success Package, available upon entering into NDA with Ping.

Requirement:	Meets Req?	Proposer Response:
4.3.1.65. Can your solution provide insights into user behavior anomalies that might indicate compromised accounts?	Yes	When detecting fraud and threat signals before a user authenticates, Ping facilitates integration with existing threat detection and monitoring solutions, using a common audit log service that is commonly consumed by third-party SIEM and analytics solutions such as FireEye, Guardian Analytics, and Logstash. Additionally the Trust Network provides access to more than 75 vendors that provide authentication, identity proofing and threat intelligence capabilities that can be easily integrated into the risk engine to further extend the ability to detect fraud. Technologies such as Identity Document Validation, bot detection, and identity data analytics are essential to reduce the occurrence of fake accounts from being opened, while behavioral biometrics, user behavior analysis, transaction risk analysis and exposed credential analysis are instrumental in detecting account takeover and limiting fraudulent purchases. Data from these threat detection sources can be used to alter the authentication level which in turn governs the access to resources. Ping Autonomous Access utilizes artificial intelligence (AI) and machine learning (ML) techniques to examine threat signals and detect abnormal behavioral patterns. It offers an advanced threat detection solution powered by AI to safeguard against account takeover and fraudulent activities at the identity perimeter. By expediting and streamlining access decisions, Autonomous Access enables your organization to effectively block threats while providing personalized user experiences that enhance digital interactions for legitimate users. In addition, Autonomous Access aims to provide insights based on the following queries: Is the user's online behavior unusual compared to their typical behavior? If the user typically exhibits similar behavior to a specific group (for example, a department), is their current behavior deviating from the norm in this context? Does the user's behavior differ from any other patterns observed on the platform? Ping implements Autonomous Access within your new or existing tenants (development, staging, and production), ensuring that your users' data and personally identifiable information (PII) remain exclusively within the tenant's boundaries.

Requirement:	Meets Req?	Proposer Response:
4.3.1.66. How does your platform ensure data integrity and protection against unauthorized modifications of user attributes?	•	Only authorized role holders are able to access and perform CRUD operations against user attributes. At a lower level, Ping Advanced Identity Cloud is hosted in Google Kubernetes Engine (GKE), which provides verifiable integrity via Shielded GKE nodes. Shielded GKE nodes are built on top of Compute Engine Shielded VMs. For further information, see https://cloud.google.com/kubernetes-engine/docs/how-to/shielded-gke-nodes
4.3.1.67. Can sessions be configured to timeout? If so, what are the configurable parameters?	Yes	The Ping Identity Platform can be configured to restrict session times, globally, per realm, or per user. You can define: • Maximum Session Time - the maximum number of minutes that a session can remain active before a user is required to re-authenticate • Maximum Idle Time - the maximum number of minutes that a session can remain idle before a user is required to re-authenticate Different session timeouts for different contexts (devices, locations, time of day, etc.) can be achieved with utility nodes that execute custom code following successful authentication which can modify session attributes such as expiry time. Environmental conditions can be applied to authorization policies to base authorization decisions on session properties or session times. The Ping platform also includes the ability to add Webhooks to events such as session termination. Webhooks can trigger a URL call to an external service. For example to notify a billing application that an SSO session has ended in order to close a billing session.
4.3.1.68. Are sessions cleared upon logging off?	Yes	Yes, when a session terminates, Ping's access management component responds by removing CTS-based sessions from the CTS store and from the server memory caches. With the user's session no longer in the CTS, Ping forces the user to re-authenticate on subsequent attempts to access protected resources. When a user explicitly logs out of Ping's access management component, the system also attempts to invalidate the iPlanetDirectoryPro cookie in the user's browsers by sending a Set-Cookie header with an invalid session ID and a cookie expiration time that is in the past. In the case of administrator session termination and session timeout, Ping cannot invalidate the iPlanetDirectoryPro cookie until the next time the user accesses Ping.

Requirement:	Meets Req?	Proposer Response:
4.3.1.69. Can active user sessions be forcibly terminated by administrators?	Yes	Yes, administrators can force session termination, which effectively logs the user out of all systems protected by the Ping platform.
4.3.1.70. Describe your approach to managing long-running sessions	Yes	This UX is typically paired with the incorporation of User Journey nodes for risk instrumentation, to force session/MFA/friction if a session has entered a higher-risk category. Long-lived sessions that persist across browser restarts (commonly used to implement "Remember Me" functionality) are typically achieved using persistent browser cookies. After successful authentication, a long-lived cookie is set in the user's browser, which is detected during subsequent logins. This mechanism has the benefit of regularly refreshing sessions (with updated session properties), but if needed, this happens transparently without interruption to the user. Ping customers have used this approach to implement passwordless login and very long-lived sessions successfully. Depending on the use case, different mechanisms are used to allow users to manage long-lived sessions. For applications that use the standards OAuth and OpenID Connect (OIDC), the standards define access tokens and refresh tokens. Access tokens are typically short-lived and may have lifetimes of only minutes. Refresh tokens may have a lifetime of days or months and are used to renew new access tokens. A user can revoke the tokens at any time, which ends the application's access rights. Ping provides an end-user dashboard to let users manage their consented applications, or the REST API can be used. For web-based applications, once a user has authenticated, a session is created, and a token issued to the browser to be stored in a cookie. The session can be ended by the user at any time via a logout button, or through a REST API call. An administrator can also invalidate (logout) as the user's session if desired via an admin console or API call.
4.3.1.71. How does your platform manage user sessions in scenarios where users access applications from various locations?		With Ping orchestration, workflow-like decision trees can be easily viewed, created, changed, and configured with drag-and-drop functionality for a user journey. The nodes within the tree can take account of context factors such as location, IP address, device type, network, or any other contextual information that is included in the request. Based on the outcome, nodes can be configured for risk calculations, modifications to authentication level, alteration of session properties, and more. Administrators can use digital signals to design a smart login journey that minimizes friction and maximizes security for legitimate users while suspicious users could be denied access or redirected to a sandbox environment for further monitoring.

Requirement:	Meets Req?	Proposer Response:
4.3.1.72. Explain how your solution assists administrators in remotely terminating active sessions when necessary.		Using Ping Autonomous Identity, an administrator can view and terminate sessions directly from the console. Sessions can be queried and terminated programmatically using REST APIs. When a session terminates, Ping's access management component responds by removing CTS-based sessions from the CTS store and from the server memory caches. With the user's session no longer in the CTS, Ping forces the user to re-authenticate on subsequent attempts to access protected resources. When a user explicitly logs out of Ping's access management component, the system also attempts to invalidate the iPlanetDirectoryPro cookie in the user's browsers by sending a Set-Cookie header with an invalid session ID and a cookie expiration time that is in the past. In the case of administrator session termination and session timeout, Ping cannot invalidate the iPlanetDirectoryPro cookie until the next time the user accesses Ping.
4.3.1.73. Does your solution integrate with Active Roles Server?	Yes	Ping Advanced Identity Cloud can govern access (i.e. access requests/approvals) with Active Roles Server, and leverage ARS for policy-related decisions.
4.3.1.74. Explain how your platform complies with industry standards and regulations related to data security and privacy.		Compliance certifications are found here: https://www.forgerock.com/security-compliance Ping Advanced Identity Cloud uses best practices from various security architecture frameworks that provide concrete requirements for security capabilities from a business perspective, as well as from a service and operations perspective. Our security model implements all the must-have tenants of a secure as-a-service platform such as those documented under the CSA Trusted Cloud Infrastructure (TCI) Reference Architecture. Specifically, the Ping Advanced Identity Cloud service protects customer data in two ways. At the service level, customer data is stored within the customer environment. It is never commingled with other customers' data and can be accessed only by the customer. At the physical level, the Google Cloud Platform (GCP) provides encryption of data at rest. All data is encrypted when written to storage, and decrypted when read.
4.3.1.75. Vendor must provide three references of clients with similar requirements and user base. Vendor must provide contact		References are available upon request from multiple state and federal agencies with equal or larger environments.

Requirement:	Meets Req?	Proposer Response:
information for each reference and current user count range. The estimated range should be greater than 30,000 users.		
4.4 Mandatory Qualification/Experience Requirements – The following mandatory qualification/experience requirements must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it meets the mandatory requirements and include any areas where it exceeds the mandatory requirements. Failure to comply with mandatory requirements will lead to disqualification, but areas where the mandatory requirements are exceeded will be included in technical scores where appropriate. The mandatory qualifications/experience requirements are listed below.		The Ping Advanced Identity Platform has full SOC compliance and supporting reports. These will be made available as part of the Customer Success Package provided after entering into NDA with Ping.
4.4.1.1. Vendor must provide SSAE No. 18 SOC 1 Type 2 report results yearly to satisfy overall State of WV SOC1		The Ping Advanced Identity Platform has full SOC compliance and supporting reports. These will be made available as part of the Customer Success Package provided after entering into NDA with Ping.

Requirement:	Meets Req?	Proposer Response:
requirements.		

Ping Advanced Identity Cloud Architecture and Platform Capabilities

Ping Advanced Identity Cloud delivers the speed, flexibility, and scale that the State of West Virginia requires. Moving to the cloud may raise security concerns in the face of ever-escalating cybersecurity threats and rampant online fraud. It presents a range of challenges for organizations like State of West Virginia that must meet strict privacy and data management regulations.

A major key to success in this IAM transformation journey lies in the architecture of the proposed cloud SaaS solution. This proposal of Ping Advanced Identity Cloud is the **only IAM SaaS offering** in the market that brings the cost savings of multi-tenant architecture while simultaneously delivering the security and scale required with full tenant isolation and data sovereignty.

Key Benefits

Deliver Exceptional Experiences

Leverage a cloud architecture purpose-built to provide frictionless digital services for consumers, workforces, and things.

Predictable Pricing and Performance

Experience consistently superior performance, even as needs and usage change, without fear of vendor surcharges or "throttling."

Accelerate Cloud Adoption

Eliminate security concerns. Rapidly move to the cloud with a service that delivers complete customer isolation via a modern multi-tenant architecture.

Features

Full Tenant Isolation

Gain speed and performance with dedicated, fully isolated resources that ensure full access to applications and data at all times.

Individual Backup Snapshots

Never worry about disaster recovery again with fully automated backup and recovery. Since no data is commingled, your environment can be rapidly restored in the event of a security breach.

Granular Data Sovereignty

Reduce the risk of compliance violations by ensuring data and backups are only stored in the region or country of your choice.

Three Dedicated Environments

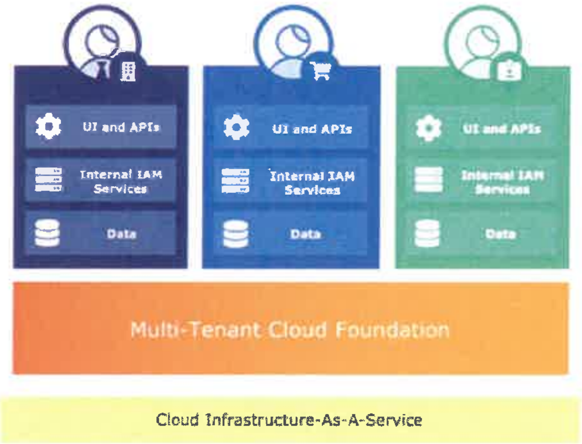
Reduce your infrastructure and maintenance costs with three dedicated environments (with the option to add more) and simplified DevOps with continuous integration and continuous deployment (CI/CD).

Our Approach: Full Tenant Isolation

ForgeRock Identity Cloud's architecture protects you from the "noisy neighbor effect" – interference caused by other cloud users.

With ForgeRock Identity Cloud, you can take advantage of your own full suite of IAM capabilities – from the user interface (UI) to the data store – as an isolated tenant. Your resources are never shared with other tenants.

The result: you can expect zero throttling as your usage ramps up. Instead, you receive a consistently high-performing, dedicated identity service that scales to meet your needs.



The ForgeRock Identity Cloud provides dedicated resources, from the data layer all the way through the endpoints.

Differentiators

True IAM Platform

Improve productivity and efficiency by leveraging a comprehensive true identity and access management platform (IAM) in the cloud.

Fine-Grained B2B2X Delegation

Extend Zero Trust security beyond your workforce to customers, vendors, partners, and contractors.

Low-Code/No-Code Orchestration

Focus on critical business demands by saving time with a no-code visual drag-and-drop orchestration engine.

Intelligent Routing for Coexistence

Seamlessly integrate, centralize, and manage identities across all cloud and on-premises solutions without creating identity silos.

Compliance and Certifications

AICPA SOC

ISO 27001 CERTIFIED schellman

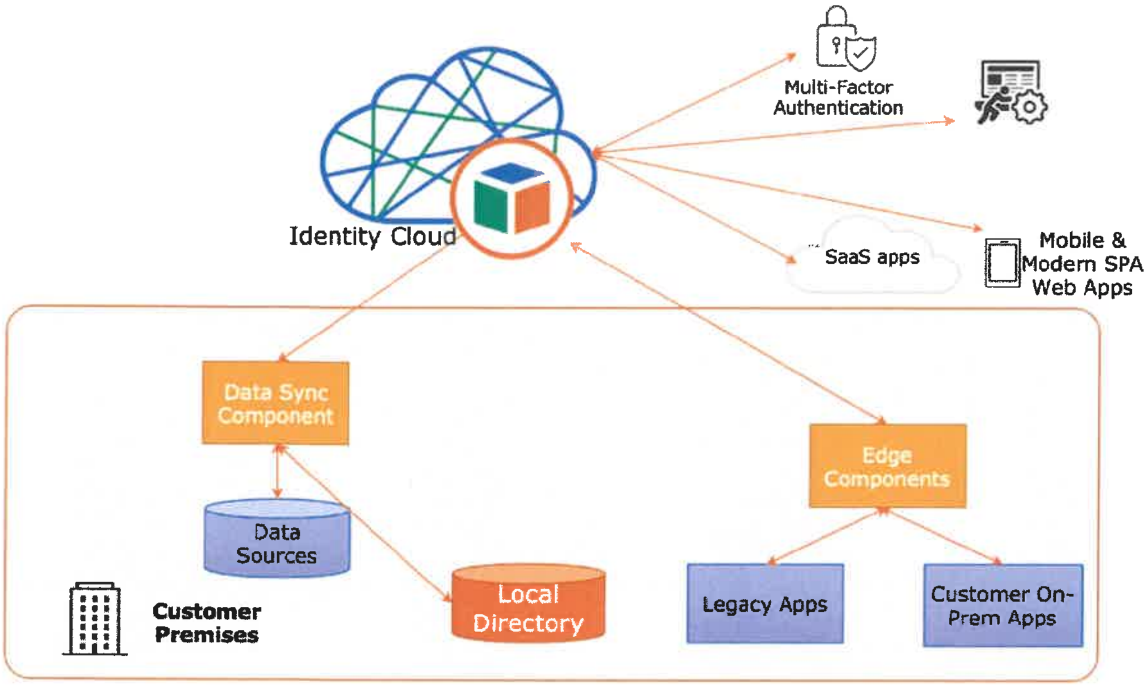
CYBER ESSENTIALS PLUS

CSA cloud security alliance

HIPAA COMPLIANT

5.1.a High-level Architecture

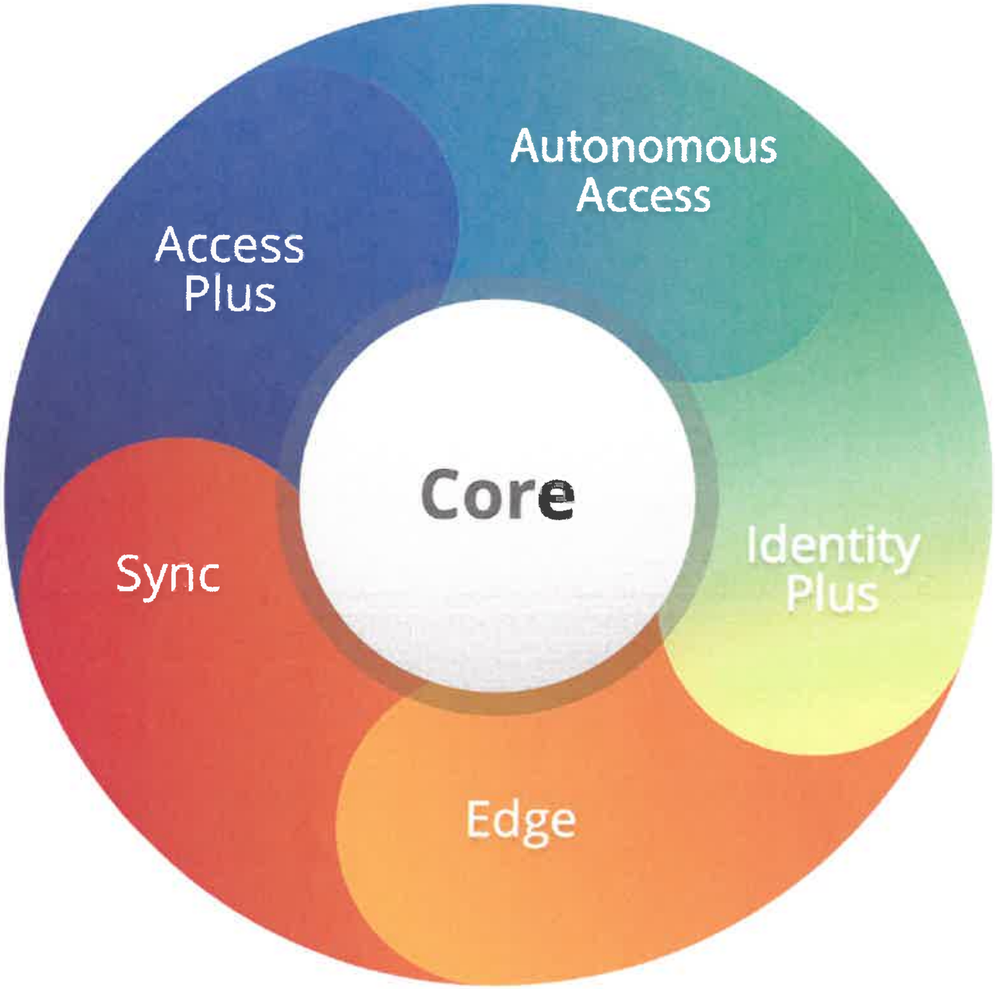
This TriVir-delivered Ping Advanced Identity Cloud solution provides a best-in-class, fully comprehensive IAM solution suite, including an available full IGA suite, full Identity Management Connectors, and logic required to replace homegrown **State of West Virginia** legacy IAM systems, a certified Identity Provider suite, and Privileged Access Management (PAM) components. The solution fully meets or exceeds all technical requirements. Additionally, it meets or exceeds the security and service requirements.



TriVir's unique approach brings 100% adoption of **State of West Virginia** identity into the new IAM cloud SaaS system quickly with all usernames, existing passwords, group and role memberships, and other important business attribute information to be useful for **State of West Virginia** applications (see Initial Phase of Scope of Work Section 6 of this volume). This approach applies authoritative sources of identity to the newly managed objects within the Ping Advanced Identity Cloud system while facilitating the fastest time-to-live for a cloud IAM SaaS platform.

5.1.b Product Names and Versions

The Ping Advanced Identity Cloud is the market's first comprehensive identity platform as a service. Built for organizations looking for a comprehensive, enterprise-grade identity platform that delivers usability, customizability, and operational cost savings, Ping Advanced Identity Cloud is packaged to meet your needs and align with your unique consumption model of the Ping Identity Identity Platform. Ping Identity secures, monitors, upgrades, and runs the software while providing the flexibility and extensibility to satisfy some of the industry's most complex identity and access management use cases. Ping Advanced Identity Cloud supports all major identity standards, including OAuth 2.0, OIDC, SAML, WebAuthN, and CIBA, and provides synchronization and storage. The Ping Advanced Identity Cloud can be supplemented with the Ping Identity Identity Gateway or Ping Identity Agents to provide policy enforcement and API management of legacy systems that do not support modern federation protocols. No third-party technologies or partnerships are required to fulfill this solicitation's requirements or the anticipated IAM requirements. The product proposed is Ping Advanced Identity Cloud. It consists of a Core platform as well as a few modules, which are included in our proposal and pricing.



The ForgeRock Identity Cloud Product Packages

Ping Advanced Identity Cloud Packages

Core

The Ping Advanced Identity Cloud Core package provides industry-leading technology essential to meet the demand for superior digital experiences. The Core package is designed to solve the majority of your Identity and Access Management (IAM) use cases with a single offering. This includes identity management, access management, single sign-on (SSO) and federated SSO, adaptive and multi-factor authentication (MFA), as well as strong authentication factors, including one-time passcode (OTP), email confirmation, Mobile Push, and Magic Link. Core also integrates seamlessly with Ping Identity's software development kits (SDK) for easy implementation with your applications.

The Ping Advanced Identity Cloud Core package can be customized to address additional requirements through the upgrade packages Access Plus, Autonomous Access, Identity Plus, Edge, and Sync.

Access Plus

The Ping Advanced Identity Cloud Access Plus package provides increased security while improving user experience with passwordless and username-less authentication capabilities and support for Zero Trust and CARTA strategies. Additionally, organizations requiring more contextual and fine-grained authorization enforcement components can leverage Access Plus to enforce continuous and contextual authorization for transactions. Access Plus also includes dynamic scopes and constant risk-monitoring capabilities.

Ping Protect/Autonomous Access

The Autonomous Access package leverages a unique combination of AI, machine learning (EUBA), advanced pattern recognition (heuristics), and big data to provide risk scores in order to help stop known bad actors, flag anomalous behavior, and learn about new and emerging cyber threats. Built into Ping Identity's Intelligent Access, it includes out-of-the-box threat protection nodes and drag-and-drop configuration, making it easy for your teams to create any number of personalized user access journeys based on identified risk scores.

Identity Plus

The Identity Plus package manages user identity data. It provides users with a privacy and consent dashboard that allows them to download, update, or delete personal information or give consent to use their data. Identity Plus also includes social identity registration and login, personalization, delegation, and user dashboards. Ping Identity Identity Plus supports all leading social identity providers out of the box, along with other identity providers supporting OAuth2 or OpenID Connect.

Edge

The Edge package extends the security capabilities of Ping Advanced Identity Cloud to legacy applications on-premises and modern microservices running in the cloud. Edge enables you to coexist Ping Advanced Identity Cloud with other legacy IAM solutions and augment legacy or home-grown applications with current IAM capabilities, giving you the time you need to execute your cloud migration and security strategy. Edge also includes Ping Identity Identity Gateway capabilities to create a secure perimeter for legacy applications and modern API traffic.

Sync

The Sync package consists of a full-featured outbound provisioning engine with complete bi-directional and translatable synchronization to various systems and applications. Sync discovers new, changed, deleted, or orphaned accounts to determine user access privileges and reconciles them seamlessly to ensure that user identity data, including passwords, are always accurate. It provides a stable hybrid environment where all identity data is consistent across all systems.

Cloud-Native Governance

We at Ping Identity have combined our unique cloud architecture and proprietary AI and machine learning (ML) with Google Cloud Platform (GCP) to deliver the hyperscale required by today's large enterprises. Ping Identity Identity Governance helps organizations make faster and more informed decisions and even automates low-risk decisions to reduce workloads for IT teams.

Ping Identity's approach creates the industry's most complete offering. It combines three primary components:

- Access certifications to accelerate access decision-making with AI-determined recommendations and confidence scores

- Access requests to provide users with a 24/7 self-service portal and automated application access

- Segregation of duties to ensure regulatory compliance when and where you need it

Physical Hardware and Dependencies for State of West Virginia

Because this solution is delivered as a SaaS offering, there are no requirements of the State **of West Virginia** for hardware or other on-prem dependencies, with a few minor exceptions. They include the following:

- Cloud Edge Remote Connectors for provisioning and lifecycle management of legacy systems
- Identity Gateway for the federation of legacy systems
- Web Agents for the federation of legacy web server platforms
- Password Plugins for bi-directional sync (replacement of legacy IDM between AD and other systems)
- Admin UI, a native management console for support of IDM and AM configuration in a hybrid environment

* Note that TriVir may advise **State of West Virginia** stakeholders for each system integration to minimize or obviate the use of these on-prem agents where possible, even in a phased approach per app, in order to accelerate the move to cloud/SaaS with the smallest on-premise footprint possible.

Object Limit

Ping Identity presently manages more than 4 billion identities worldwide. Many Ping Advanced Identity Cloud environments cover the world's largest employers and their suppliers, partners, and customers, equalling hundreds of millions of identities in a single tenant. Ping Advanced Identity Cloud can easily accommodate millions of managed objects.

Build-It-Once Architecture Based on Microservices

Ping Advanced Identity Cloud is implemented with microservices, which are consumed by the Administrative UI layer, the RESTful services and APIs exposed to app and system owners, and SDK users. Because of this, all delivered IAM functionality is the same, whether provided through a Ping Identity UI, a web service, or another interface.

Tenant Status and Redundancy

Ping Advanced Identity Cloud is the only IAM SaaS offering available today that is built as a multi-tenant solution but with full tenant isolation. This makes unique features possible, such as:

- Granular/rapid data backup/restoration
- Data sovereignty with granular placement within all major regions
- Sustained performance when one client tenant is experiencing a heavy load
- No intentional metering for busy workload in other non-related tenants
- Increase in security since data is encrypted micro-segmented, per Zero-Trust
- The guarantee that transactional cost of IAM transactions is predictable and constant, regardless of the load

Platform User Interface

The out-of-the-box Ping Advanced Identity Cloud Platform UI support everything from basic branding, themes, and layout to very sophisticated options:

- **Minor theming of the Out-of-the-box Platform UI**. The supplied UIs are built using standard HTML, CSS, and JSPs. Simple changes, such as inserting a custom brand or logo to reflect your organization, are achieved by modifying the HTML and CSS stylesheets. For minor changes to the Self-Service UI, the simplest approach is to use realm theming, which allows basic branding of the end-user interface with colors and a logo image. A Theme node (available on the Ping Identity Marketplace) allows you to easily customize the look and feel of any authentication or registration flow and optionally change the Login button text.

• **Restyling of the standard UI through Bootstrap theming**. Further enhancements can be made using a responsive design framework such as AngularJS or Handlebars.js.

• **Complete availability of the Ping Identity platform UI as open source**. Powered by Vue.js and available on GitHub, this capability allows you to easily build out and expand the supplied UI to evolve and grow to suit your changing requirements while providing a peerless end-user experience.

• **SDKs**. Ping Identity supports SDKs for mobile and web authentication, which can be fully customized and branded according to your requirements. Our SDKs interact directly with and adapt immediately to any modification to user journeys, including authentication, registration, and customer self-service. This means that end-user application changes are not required when updating user journeys– a significant benefit when adding security measures to respond to an evolving threat landscape or when adding new features. The SDK team continually develops new capabilities to enable our customers' developers to quickly and easily create exciting yet secure experiences for their customers.

• **Rich customization using your choice of UI frameworks, calling REST APIs directly**. Complete UI customization, or integration with your existing portals, can be achieved by invoking the same REST APIs as Ping Identity's supplied UI. This allows new or existing apps and portals to integrate with the Ping Identity platform by reusing the integration patterns and code used in the supplied UI.

Browser Support

Ping Advanced Identity Cloud supports all major browsers, such as Chrome, Edge, Safari, and mobile versions of each browser.

On-Premise Components

Through the comprehensive Ping Advanced Identity Cloud UI, its analytics dashboard, coupled with TriVir's IdMMonitor solution, every aspect of the system, from the SaaS side to the on-prem footprint components, may be viewed, monitored, and managed from a single dashboard from an administrative UX perspective.

Interface Consistency

All end-user UI pages supplied as part of the Ping Advanced Identity Cloud are device-agnostic and responsive and provide a consistent look and feel across all modules. Customers connecting via home PCs, smart TVs, tablets, smartphones, or public kiosks should be able to interact with the service in a consistent manner. The UI is rendered within a browser and is therefore not dependent on the underlying Operating System and will function correctly on browsers running with iOS, Android, Windows, Linux, and other OS.

The UI pages are fully brandable and customizable and can be adapted to include support for specific requirements, e.g., high-contrast mode for the visually impaired.

Internationalization support is built into the user interfaces, and language/locales automatically switch according to the user's browser locale settings. A translation framework is built to support locale-specific variations of all user interface elements (e.g., titles, field names, notification messages, etc.).

Interface Configuration

The UI is completely configurable. The Admin UI is dynamically configured typically through delegated administration. The interface is adjusted to expose only the capabilities the authenticated user has the right to see and leverage. Additionally, UX flows are configured via no-code visual flows that resemble MS Visio diagrams. Authentication journeys through these UIs may be configured (and defaulted) to have the least friction and not require re-authentication when moving between UIs.

Identity Administration

Automated Identity Lifecycle

The Ping Advanced Identity Cloud Sync package includes a full-featured outbound provisioning engine with complete bi-directional and translatable synchronization to various systems and applications. Sync discovers new, changed, deleted, or orphaned accounts to determine user access privileges and reconciles them seamlessly to ensure that user identity data, including passwords, are always accurate. It ensures a stable hybrid environment where all identity data is consistent across all systems on-prem and in the cloud.

Manually Initiated Identity Lifecycle

Ping Advanced Identity Cloud provides a consistent experience for maintaining all identities of every type in the system. Based on customer business policies, some accounts may be administered manually (like contractors) if they are outside the scope of data reconciliation with a more authoritative source. Who can request/approve new accounts is fully policy-protected (functionally limiting the ability through the UI or even through the RESTful APIs in the underlying microservices of Ping Identity.) The UIs and object models for managed identities are configurable.

Manually Initiated Identity Changes

Managers/requestor role holders can modify authorized records to update attributes, memberships, subscriptions, capabilities, identifiers, and credentials (passwords, MFA, etc.) through consistent UIs and RESTful APIs.

Non-employee Identity Recertification

The administrative UIs provide the ability to recertify assigned roles and groups for Non-employee identities. Non-employee access can be time-boxed at identity creation time (or subsequently for existing users). Upon expiration of the constraint, a workflow is triggered, requiring recertification. Otherwise, business rules will be triggered to then disable/de-provision the use or implement other customer processes to handle complex deprovisioning logic. This can be done at the identity level or the role/group level, automating the process of the customers moving closer to least-privileged access.

Non-employee Identity Provisioning

Privilege revocations and entitlements may be automatically added or removed based on customer business policy. TriVir has a DevOps process, outlined in Tab 6, for interpreting existing IDM logic to inform the necessary rules as we move IAM into the SaaS Ping Advanced Identity Cloud.

Attribute Data Mapping

Ping Advanced Identity Cloud can implement one-to-many and many-to-one relationships, state machines, and other concepts to facilitate layered, complex business logic. For speed of implementation and simplification of solution understanding/ownership, TriVir provides guidance during implementation to simplify some of these types of more complicated mapping scenarios to reduce complexity in the system. Rules like this can be an area of IAM that accumulates technical debt over time. This move to Ping Advanced Identity Cloud is an opportunity to remove some of the legacy IAM policy-based technical debt.

B2C Identity Support

Ping Advanced Identity Cloud specializes in support for B2C and B2B IAM. A key differentiator here is the ability to customize user journeys and authentication trees to provide exactly the right UX and the most appropriate/adaptive friction for each user. This is often challenging due to layered requirements on the external side of the solution. The no-code orchestration engine makes this easy for customer IAM staff to manage without scripting or coding.

Identity Proofing

Identity proofing can be achieved by adding a custom step in the user self-service configuration. This prompts the customer to enter details that can be validated against an existing database before continuing the registration flow. For new users, many user journey nodes can integrate with external identity-proofing services such as OneSpan, Intercede, Idemia, Transmit Security, Daon, Callsign, and many others. Alternatively, a custom user journey node may be leveraged to use customer applications, databases, or processes that assist person identification.

B2C Associations

Ping Advanced Identity Cloud maintains immutable, system-generated associations, or GUIDs, for each managed object in each realm. This can be accessed in the Ping Advanced Identity Cloud UI, CORE Directory Services (LDAP), or through REST.

International User and Character Support

Ping Advanced Identity Cloud provides user attributes that may contain international forms of identity data. Additionally, the Ping Advanced Identity Cloud team has innovated significantly to find ways to support varying formats while at the same time supporting effective indices and data categorization and normalization to make it more consistent between countries. Many Ping Identity customers have worldwide footprints of clientele with these needs.

Non-Person Entity Identity Support

The customer Ping Advanced Identity Cloud will facilitate request/approval workflows and identity lifecycle management for non-person entities (NPEs) following the Build it Once concept. The Ping Identity Identity Platform includes a Thing SDK, Intelligent Access nodes for Thing registration and authentication, and a Thing Gateway to support constrained and offline devices needing identity. These NPEs enjoy the same security, digital UX, lifecycle management, privacy controls, and automation that human identity objects enjoy.

Non-Person Entity Identity Sponsorship

Ping Advanced Identity Cloud provides for the sponsorship of an identity, whether it be an admin account, a service account, a parent/guardian account, etc. When the sponsoring identity is deprovisioned, associated (or owned) identities may either have ownership transferred via workflow or may also be deprovisioned based on customer business rules.

Non-Person Entity Identity Documentation

In Ping Advanced Identity Cloud, each identity can store any information required using custom attributes. TriVir will expose a data model for human identity with support for NPEs to allow for rapid expansion of the concept of identity in the customer environment, including lexically transparent documentation constrained upon each NPE object.

Non-Person Entity Identity Requests

Per 5.3.I above, Ping Advanced Identity Cloud supports requests/approvals for such identity account requests or may be linked to the customer service desk in order to leverage normalized business workflows and request/approval experiences.

Merging and Splitting

This Ping Advanced Ping Advanced Identity Cloud specializes in this capability. It is especially critical because, in workforce systems like this, a person may "wear multiple hats" and hold several different types of accounts. For this reason, Ping Advanced Identity Cloud allows for the merging and splitting of any identities (human and NPE) through automated reconciliation or even Access Management user journeys and business workflows.

Delegated Identity Administration

Ping Advanced Identity Cloud specializes in delegated identity administration; it is purpose-built to move the burden of identity administration closer to the business users closest to the data. With the Build It Once approach, experiences for delegated administrators are consistent in each UI and API access to underlying Ping Advanced Identity Cloud RESTful interfaces and microservices.

Delegation of Authority

The Ping Advanced Identity Cloud UI provides features to delegate administration to another group or individual via roles. These can be assigned temporarily (time-boxed) or permanently. They apply within Ping Advanced Identity Cloud UIs and at the API and microservices level, so this concept of delegation works regardless of the use context within the customer environment.

Limits of Delegation

Specific roles can limit all privileges for users in the Ping Advanced Identity Cloud. These roles can be limited to only approving access or only being able to access end-user information or any combination developed by super users. Ping Advanced Identity Cloud provides excellent documentation on delegated admin features, configuration, and possibilities.

Role Appropriate Data Access

Role-based data isolation of viewable or editable screens, workflows, attributes, functions, and data by a delegated administrator, helpdesk, and other end users are scoped and controlled through assigned roles. These constraints apply to the UI as well as REST API access.

Support for User-Entered Data

The Ping Identity platform also includes a profile dashboard that enables users to manage all identity data about themselves in a single place. It features self-service controls for editing personal information, opting in or opting out of data collection, regulating device pairing, authorizing app access with greater login and security options, as well as managing privacy and consent features such as the "right to be forgotten."

Universal Provisioning Capability

Ping Advanced Identity Cloud leads globally with connection support for any system for provisioning, deprovisioning, and managing the lifecycle. Out-of-the-box connectors included in Ping Advanced Identity Cloud as cloud-native within the SaaS environment include:

- MS GRAPH for Azure/O365
- SalesForce
- ServiceNow
- SuccessFactors
- Adobe Cloud
- Others

For customer systems that may not have pre-existing pure-SaaS integrations, these additional Ping Advanced Identity Cloud connectors are available out-of-the-box for Remote Connector Server (RCS)-delivered capabilities, such as:

- SCIM
- CSV
- SAP
- Workday
- Kerberos
- Scripted REST
- Database (requires third-party JDBC driver for the target database platform)
- LDAP
- Scripted SQL
- Groovy
- SSH
- Docusign
- Epic
- Google Apps/Workspace
- HubSpot
- MongoDB
- And many others
- More connectors and integrations are added to Ping Identity MarketPlace regularly.

Identity Provider

MFA Options

The Ping Advanced Identity Cloud system exposes every major type of MFA, coupled with its intelligent authentication engine, orchestration for simplified enrollment, and management of MFA tokens/credentials. Typical MFA methods utilized through Ping Advanced Identity Cloud include:

- **OATH (HOTP/TOTP):** The Ping Identity Authenticator app or another authenticator app (such as the Google app) must be installed on an out-of-band device to provide codes. The out-of-band device that generates the code does not need connectivity to the server, but the device being used to access an application by the end user does. TriVir may assist with creating a customer version of this app and push the mechanism as desired.
- **SMS OTP**: The user requires a mobile connection to receive an SMS message to an out-of-band device (phone). The device being used to access an application by the end user requires SMS connectivity.
- **Push Notification**: The out-of-band device and the device being used to access the application

both require connectivity. The Ping Identity Authenticator app or Ping Identity SDK must be used.

- **FIDO WebAuthn**: A FIDO2 device must be available (Touch ID, Windows Hello, Yubikey). The device being used to access the application and interact with the FIDO2 device requires connectivity. This method enables passwordless and username-less solutions.

Third parties on the Ping Identity Marketplace regularly develop and provide additional options. The MFA options also facilitate user account recovery and re-registration or resetting of MFA devices.

MFA Support of Zero Trust Principles

With native support for user journey orchestration, Ping Advanced Identity Cloud helps customer admins strike the right balance between security and convenience. Instrumented by the Ping Identity risk engine (as well as external risk instrumentation from the customer as necessary), authentication factors may easily be “stepped up” dynamically to manage the transaction’s related risk levels.

AuthN Context Scoping

Ping Advanced Identity Cloud allows for the simple scoping of MFA options and requirements based on assigned groups, roles, authentication trees/user journeys, or user attributes.

SSO Standards Support and Capability

The Ping Identity platform supports all major federation, authorization, and provisioning standards, including SAML 2.0, WS-Federation, OAuth 2.0, OpenID Connect (OIDC), User-Managed Access (UMA), LDAPS, and SCIM, among others. The platform also supports advanced OAuth 2.0 standards such as Device Flow and Proof-of-Possession.

Support for Complex Authentication Requirements

Ping Advanced Identity Cloud keeps simple user journeys simple while enabling IAM team members to configure complex authentication scenarios easily. The natively integrated user journey orchestration system facilitates this. Other IAM SaaS providers that market this capability have attempted to add and integrate orchestration by acquiring third-party products and platforms, which still require separate hosting, security requirements, and additional integration steps. Ping Identity brings this capability in the simplest way possible by building it from the ground up, native to Ping Advanced Identity Cloud, with no-code/low-code configuration options.

Support for Single Logout (SLO)

Ping Advanced Identity Cloud includes multiple options for configuring SLO and was one of the first IdPs in the world to support such behavior.

Passwordless Capability

The Ping Identity Identity Platform has extensive support for passwordless authentication methods, including mobile push, certificate, WebAuthn (based on FIDO2 standards), Face ID, and Touch ID. Multiple options exist for handling passwordless in different ways for different customer identities.

Prepopulation of Data

Ping Advanced Identity Cloud Connectors can pull authoritative source data as necessary to pre-populate the customer Identity Cloud Directory Services (DS) environment. TriVir provides a unique approach to pre-populating customer identity data within Ping Advanced Identity Cloud by linking in authoritative sources as well as existing identity stores (like the existing authentication system) to provide a seamless transition for existing user identities onto the new system.

As a unique differentiator, this TriVir-delivered **Ping Advanced Identity Cloud SaaS solution is the only IAM/SSO SaaS solution in the marketplace that can bring existing user passwords** into the new environment for 100% of customer identities on day one.

Support for Password Sync and Management

Ping Advanced Identity Cloud provides out-of-the-box support for all customer password-related requirements. Uniquely, it also provides a path toward minimizing usernames and passwords for modern customer on-prem and SaaS solutions, as well as legacy solutions that don't support current federation and authentication standards. Password management within Ping Advanced Identity Cloud supports:

- Bi-directional password synchronization
- Granular password policies to match enterprise directory requirements and facilitate specific requirements for customer environments
- Multiple password policies to support different customer constituencies
- Ability to manage the fact that down-stream systems may not support the same level of password complexity
- Password dictionary and attribute checks to ensure common words or specific details about oneself are not used within the password
- Password complexity scoring and simplified guidance for users
- Self-service password resets
- Assisted password resets via the service desk, manager, or a responsible party

MFA Re-registration and Lifecycle Management

Ping Advanced Identity Cloud allows MFA and related tokens to be re-enrolled and self-serviced effectively from the end user's perspective. Additionally, administrators may clear registered tokens and guide the user to re-enroll. Lastly, with the orchestration mentioned above of Ping Advanced Identity Cloud, MFA troubleshooting, re-registration, and lifecycle management may be naturally facilitated during user interactions, thereby reducing the administrative burden typically associated with password resets and MFA credential assistance.

ML/AI Enhanced Identity Protections

Ping Advanced Identity Cloud implements the concept of "autonomous identity." AI/ML nodes may be added to orchestrated user journeys as a drag-and-drop element. This allows for data to be gathered and for measurements of risky behavior to be processed against the Ping Identity intelligent authentication risk engine. Based on the associated risk found, the authentication journey may branch as suggested in this requirement and provide for additional friction as necessary.

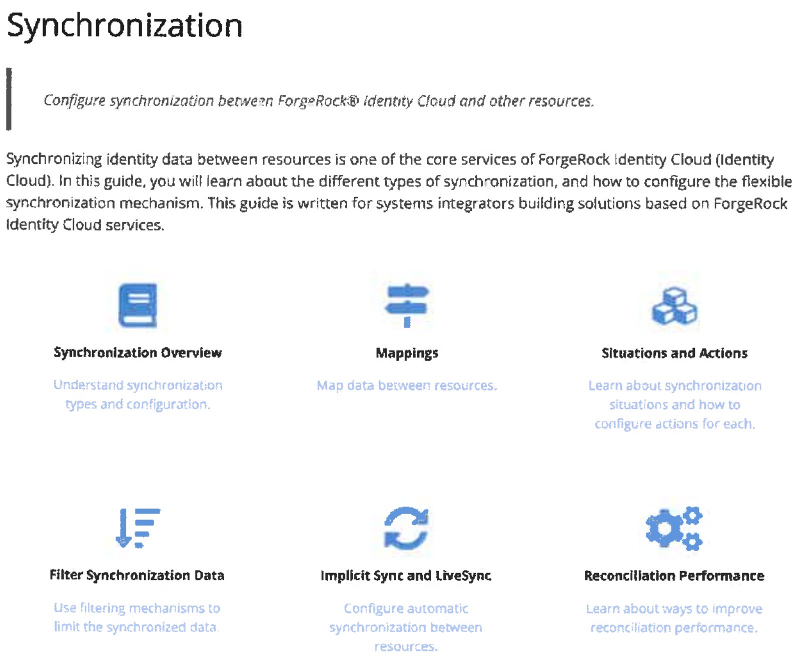
Provisioning

Data Synchronization

The Ping Advanced Identity Cloud offers comprehensive provisioning, reconciliation, and bi-directional synchronization functions, and functionality can be integrated with a range of typical enterprise data stores using multiple standard protocols such as LDAP, database, SOAP, JSON, XML, REST, and more. Ping Identity's identity management component can perform complex transformations to allow integration between different schemas and data models.

Event-based Provisioning and De-provisioning

Ping Advanced Identity Cloud facilitates event-based triggers to facilitate near-real-time synchronization between systems with LiveSync.



Synchronization

Configure synchronization between ForgeRock® Identity Cloud and other resources.

Synchronizing identity data between resources is one of the core services of ForgeRock Identity Cloud (Identity Cloud). In this guide, you will learn about the different types of synchronization, and how to configure the flexible synchronization mechanism. This guide is written for systems integrators building solutions based on ForgeRock Identity Cloud services.

Synchronization Overview

Understand synchronization types and configuration.

Mappings

Map data between resources.

Situations and Actions

Learn about synchronization situations and how to configure actions for each.

Filter Synchronization Data

Use filtering mechanisms to limit the synchronized data.

Implicit Sync and LiveSync

Configure automatic synchronization between resources.

Reconciliation Performance

Learn about ways to improve reconciliation performance.

*Note that these images show live-action guides, videos, sample projects, and practical enablement training at the press of a button, guiding IAM administrators in configuring provisioning and de-provisioning.

Event and State Monitoring

Ping Advanced Identity Cloud can identify discrepancies where something has been changed out of band. In this case, Ping Identity can "reconcile" differences, applying customer logic to either a) allow for the authoritative source data to overwrite or b) follow customer logic to determine whether to use another value for the authoritative source version for the attribute value. For high-risk or sensitive attributes, a notification may be sent to the SIEM system or directly to administrators or managers. This is handy logic for organizations that trigger IDM operations on a number of different attributes. In addition to reconciling attributes that are out of sync, Ping Advanced Identity Cloud can identify and report on orphaned accounts or other boundary conditions that are not typically apparent in other IAM solutions.

Support for SCIM and API Provisioning/De-provisioning

The Ping Advanced Identity Cloud includes a SCIM connector, which is based on the System for Cloud Identity Management (SCIM) protocol and enables you to manage user and group accounts on any SCIM-compliant resource provider, such as Zoom, Slack, or Facebook. The SCIM connector implements both 1.1 and 2.0 endpoints with all features. For all connected systems, Ping Advanced Identity Cloud supports out-of-the-box support for provisioning and deprovisioning via an application's APIs. Ping Identity identity lifecycle transactions and operations may also be invoked via the comprehensive RESTful APIs exposed through the Identity Cloud.

API Support and AMQP

Ping Advanced Identity Cloud provides direct integration capability with AMQP through the Edge component.

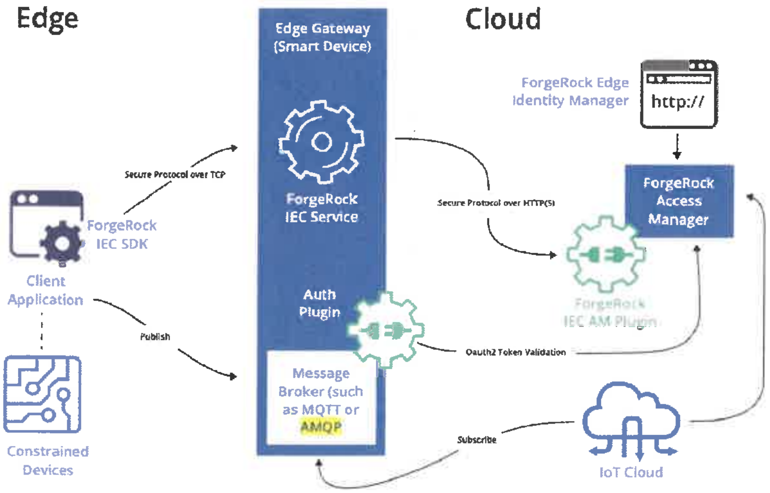


Figure 1: This image shows the high level architecture of ForgeRock's IoT Edge.

Platform-Specific Connectors for Provisioning/De-provisioning

Ping Advanced Identity Cloud has out-of-the-box connectors for all major IAM integration connection protocols and many native connectors for customer platforms. For example, the Ping Advanced Identity Cloud may provision, de-provision, and manage the Azure Active Directory environment directly without an on-prem footprint or dependency for this connector. Additionally, Ping Advanced Identity Cloud contains connectors for GCP and other major platforms/SaaS. During the initial requirement assessment phase, TriVir will recommend the best connectors and practices to integrate each in-scope system.

Notification of Required Action

Ping Advanced Identity Cloud provides out-of-the-box notification capabilities to inform admins, managers, approvers, and delegates of required/pending actions by email or other push notification methods.

Account Reconciliation

The Ping Advanced Identity Cloud reconciliation process ensures that correct values exist for all users and attributes. Any orphans are identified and reported to administrators. This is supported in modern systems with modern API interfaces and legacy systems. Ping Advanced Identity Cloud also may reduce the need for reconciliation within so many systems by bringing federation to more and more systems, thereby reducing the number of supported user identity stores.

Universal Provisioning

SCIM provisioning is a part of Ping Advanced Identity Cloud. This IAM SaaS solution will also facilitate the integration of other legacy systems that don't support SCIM. The Ping Advanced Identity Cloud environment will support integration with the existing systems currently integrated with legacy or in-house IAM solutions.

No-Code/Low-Code Orchestration

Ping Advanced Identity Cloud is the only IAM SaaS solution on the marketplace today with native no-code/low-code orchestration fully integrated and supported without a third-party integrated solution. It provides a simple no-code interface for facilitating all stated (and anticipated) user experiences and journeys. It also provides an excellent platform for scriptability, where IAM admins may need to facilitate more complicated scenarios.

Provisioning Controls

Ping Advanced Identity Cloud implements such control over identities and groups to limit provisioning with a consolidated policy engine. This enables the "Build it Once" approach to facilitate provisioning situations. Regardless of when and where the provisioning occurs, policies can evaluate existing data, attribute values, and customer business logic to provision only when desired.

Group Management

Delegated Group Management

The Ping Advanced Identity Cloud solution will expose a UI for the management of groups as well as the delegated administration of groups, their memberships, and their lifecycle. Reports will be available to measure utilization and efficacy.

Public and Private

Ping Advanced Identity Cloud facilitates granular access privileges to view, read, update, or delete group objects, their attributes, and memberships. Visibility is controllable with rights or role memberships in Ping Advanced Identity Cloud DS. For management of visibility in the Global Address Book or other downstream systems, a group can be marked as "hidden," wrapping the functionality available in Active Directory as well as Azure Active Directory.

Additional Mail Permissions and Settings

In terms of Exchange management (on-prem) or O365 identity, subscription, and rights management, the Ping Advanced Identity Cloud connector for Active Directory and the connector for Azure Active Directory may control every aspect of Exchange or O365 administration, rights, subscriptions, and visibility. Any operation that may be performed over PowerShell or GRAPH API is supported in the Ping Advanced Identity Cloud. For Google Workspace, all group management features that are available in the admin UI are also available to the Ping Advanced Identity Cloud connector through the Google Workspace directory and mail management APIs.

Group Lifecycle Management

Ping Advanced Identity Cloud can monitor and report group-related metrics to assist in group lifecycle management decisions. Many predetermined actions may be automated once the associated metrics indicate a need, such as de-provisioning a group.

Group Membership Management

Ping Advanced Identity Cloud natively provides for all requested group and group membership management features to include:

- Static and dynamic groups
- Granular control of groups and their memberships flowing down-stream to other IDM-connected systems

- Support for nesting of groups (including the ability to show members added via nesting, as simple membership where needed via Virtual Static Groups)

Group Update and Re-Evaluation Cycle

Group re-evaluation cycle happens in near-real-time within Ping Advanced Identity Cloud. For downstream systems, sync can also be done in near-real-time or in fast enough intervals to meet business requirements for each connected system.

Group Metadata Attributes

Ping Advanced Identity Cloud allows for the extension of metadata attributes via custom schema or the allocation of extended attributes that may be configured and extended. Various indexing strategies are applicable.

Role Management

Delegated Role Management

The Ping Advanced Identity Cloud provides a web interface to delegate administration to a separate service desk or business team. Typically, an administrator can define administrative or business roles, assign users to them statically or dynamically (based on configurable rules), and then define the privileges inherited by users assigned to each role.

Access and Role Modeling/Role Mining

Roles may be defined either through the Advanced Ping Advanced Identity Cloud UI or the RESTful interface. Role definition support and analytic augmentation (based on AI/ML) are available through the Ping Identity AutoID function.

Role Governance

Ping Ping Advanced Identity Cloud provides several ways for role requests to be reviewed prior to being created and promulgated to downstream systems. Additionally, AI/ML (through AutoID) can provide recommendations based on configured attributes, elements, and member assignments based on past learning and modeling within the customer environment. Ping Advanced Identity Cloud can facilitate the periodic review and attestation of roles and groups.

Nested Roles

Roles may be mapped to groups that support nesting and thereby facilitate nested role use cases.

Support for RBAC, ABAC, and PBAC

The Ping Advanced Ping Advanced Identity Cloud supports coarse and fine-grained contextual, continuous, and transactional authorization. The platform also supports all common forms of access control: Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Policy-Based Access Control (PBAC), Risk-Adaptable Access Controls (RAdAC), and Relationship-Based Access Control (RelBAC).

Ping Advanced Ping Advanced Identity Cloud meets the requirements of NIST 800-162.

Entitlement Access

Ping Ping Advanced Identity Cloud may assign birthright roles or auto-approve role requests for low to medium-risk roles, which will result in the automated provisioning of such entitlements. Downstream, the Ping Identity Identity Platform supports role-based access control by provisioning entitlements in connected systems according to the roles assigned to the identity. All standard forms of access control are supported, including Role-Based Access Control (RBAC), Policy-Based Access Control (PBAC), Attribute-Based Access Control (ABAC), Risk-Adaptable Access Controls (RAdAC), and Relationship-Based Access Control (RelBAC).

Direct Provisioning

Ping Identity Identity Governance capabilities include the feature to merge entitlements in key customer systems and applications to represent a mature service catalog. These entitlements may be mapped to workflows where their requests, approvals, and lifecycle management may be done in common language terms (not technical) and are completely manageable by lines of business.

Indirect Provisioning

In Ping Advanced Ping Advanced Identity Cloud, all provisioning actions can be initiated via API calls from UIs or the service-oriented architecture. This allows for complete automation of the request, approval, verification, and recertification process for provisioned access and its associated lifecycle.

Access Control

Adaptive Access Control Capabilities

Ping Advanced Ping Advanced Identity Cloud provides one of the most flexible adaptive access controls available in the marketplace as a SaaS offering. Ping Advanced Identity Cloud supports the following, based on integration with the Ping Identity Intelligent Access risk engine, in collaboration with any other SaaS risk sensory providers, such as:

- Allow
- Allow and Monitor
- Ask for more context
- Challenge for step-up
- Reduce access
- Block
- Deceive

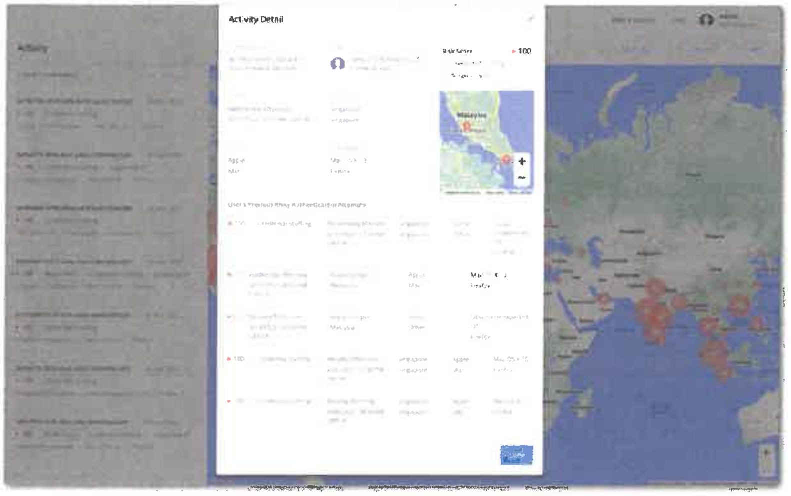
As mentioned in earlier sections, Ping Advanced Identity Cloud contains an intelligent access management orchestration system. Each action above is represented as a node in a flow tree or user journey. Many out-of-the-box nodes **cover all of the above**. There are also other helpful nodes, such as Intelligent Access nodes, which gather data and train the Ping Identity AI/ML engine to help make the actions above more effective over time as the customer organization improves the efficacy of the access process for all user types.

In the case of Deceive, which has not been mentioned earlier in this technical response, Ping Advanced Identity Cloud may drop the user into a honeypot of bad information or, in many cases, stop hitting back-end systems altogether while the attacker continues fruitlessly. Ping Advanced Identity Cloud user journeys can facilitate all customer-requested adaptive authentication scenarios while infusing fraud/bad-actor protection and adaptive behaviors.

Access Request Management

Reporting and dashboard capabilities allow users to review pending and completed requests. The user can see each approver's decision and final outcome for completed requests. For pending requests, the user can see the current approver(s) and due date. Additionally, the request/approval process can be tightly integrated with the service desk for a more integrated experience using the Ping Identity RESTful APIs presented by Ping Advanced Identity Cloud SaaS.

Figure 3: Activity detail page



Access Recertification

Ping Advanced Identity Cloud supports in-depth reporting on roles and groups to provide a clear picture of who has access to what. This facilitates regularly recurring reviews and certifications of access for internal and external audit processes and compliance.

Access Recertification for Non-Person Accounts

Ping Advanced Identity Cloud facilitates access recertification for non-person accounts. The object model can associate these accounts with human owners or groups so the system can kick off natural reviews/updates/secret rotation/etc. The reporting and review interface may consolidate all re-certification processes through the same interfaces and workflows in order to provide a consistent experience for review and recertification, where the Access Request and Access Approval modules are employed.

Access Recertification for Federated Identities

With Ping Advanced Identity Cloud Autonomous Identity, the access landscape of an organization can be modeled, and the results can be used to drive actionable insights and automation, including automated recertification. Team members can be automatically recertified based on discovered access patterns and confidence scores. This recertification support covers B2B, B2C, and even BYOI use cases, as well as enterprise use cases.

Access Recertification Interval Configurability

Re-certification intervals and workflows are configurable in the system and can be managed by app, role, team/group, or individual. Additionally, micro-certifications may be initiated when risk scoring exceeds a maximum threshold for an identity.

Privileged Access Management Capabilities

This concept of step-up requests/approvals to perform administrative tasks is uniquely implemented in

Ping Advanced Identity Cloud with configurable user journeys and trees. With this, you can implement incredible UX with no code. For example, a domain administrator may authenticate in the morning, request domain-admin access, and then have their credentials revoked at the shift's end. These flows are easily configured and managed for various types of elevated privileges used by administrators and business managers.

PAM capability in Ping Identity allows server administrative accounts to be used by authorized users for a predetermined period without the user knowing the full administrator credentials. Ping Advanced Identity Cloud can be configured to implement PAM features in the following ways:

- Customize an "account or password checkout process"
- Integrate with a third-party PAM product via an Identity Cloud connector
- Manage shared accounts (e.g., service accounts, admin accounts, etc.)

Scheduled PAM Capabilities

Administrative entitlement grants may take place for the life of the session, a day, a week, or any specified amount of time. At the end of the period, access entitlements can automatically be removed.

BYOI Support

Ping Advanced Identity Cloud allows for the support of identities coming in through other approved and federated IdPs. Additionally, we can limit the amount of PII shared in these transactions and assertions, protecting these identities and customer systems. Ping Advanced Identity Cloud also has instrumentation with Autonomous Access to enable fraud detection, measure risky user behavior, and prevent account spoofing, credential stuffing, session stealing, and other common access management attack vectors for B2B/federated identities. This facilitates Bring Your Own Identity (BYOI) support for various social identity providers, including Google, enabling account linking to already-established customer identities through social sign-in and social registration flows.

Default identity provider support includes:

- Amazon
- Apple
- Facebook
- Google
- Instagram
- itsme
- LinkedIn
- Microsoft
- Salesforce
- Twitter
- Vkontakte
- WeChat
- WordPress
- Yahoo
- Others; support for other providers is available using well-known standard APIs.

With the user journeys and authentication trees in Ping Advanced Identity Cloud, identity proofing can take place given support from back-end systems, as well as external services like LexisNexis, Experian, and others. Ping Advanced Identity Cloud Identity Manager will provide Identity Lifecycle management within the customer environment. This process manages the full identity lifecycle.

Access Portal

Portal Launch Page

The Ping Advanced Identity Cloud Platform UI includes a dashboard that provides the end user with an interface to access applications secured by Ping Identity. This consists of both cloud-based/SaaS applications and internal applications. The console may be configured to show authorized applications and areas where new applications may be requested/approved. The dashboard service uses single sign-on (SSO) to log in to the applications when the user clicks on the application icon.

IdP vs. SP Initiated Login Support

Ping Advanced Identity Cloud supports logon both as IdP-initiated as well as SP-initiated.

Portal Branding

Ping Advanced Identity Cloud has flexible support for customer branding without the need for custom UIs or custom code. It supports configurable icons, styles, URLs, localization, themes, and all other major UI/UX artifacts required for delivering a modern digital experience. Note that the powerful Ping Identity user journey feature may invoke different journey themes as needed by customer business use cases.

Portal Scoping

UI-available applications for a user are scoped to the adequate roles/groups/privileges associated with the user. Additionally, since Ping Identity facilitates authorization and authentication, features within an app may be added/removed automatically to take effect immediately in associated UIs and API interfaces.

Custom Portal Pages

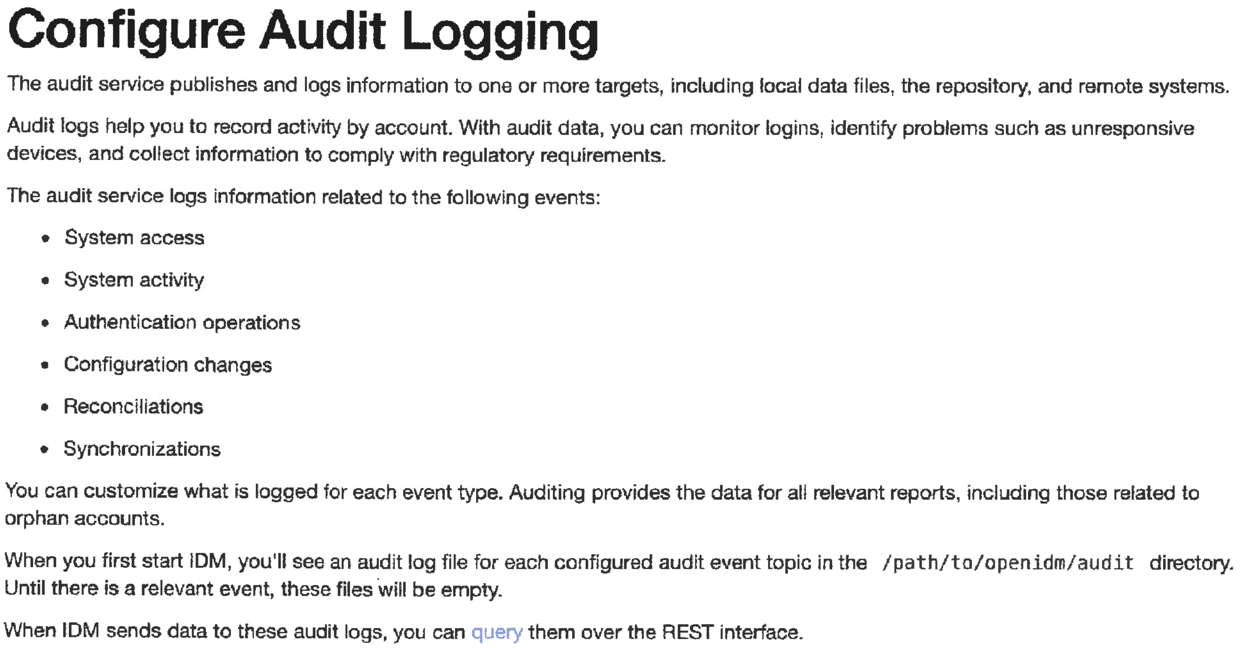
The Ping Advanced Identity Cloud customer can modify the provided UI or build and use their own customized UI by invoking the REST API. The Ping Identity UI pages are fully brandable and customizable and can be adapted to include support for specific requirements. Ping Advanced Identity Cloud facilitates cloud-hosted pages that are themed and configured for the customer while at the same time providing the ability to leverage customer-hosted UIs.

Audit, Logging, Reporting, and Other Administrative Concerns

AICPA SOC   ISO 27001 CERTIFIED by schellman   CYBER ESSENTIALS PLUS   CSA cloud security alliance   HIPAA COMPLIANT

Audit and Logging

Ping Advanced Identity Cloud leverages Prometheus for full auditing and logging for all actions taken and operations performed. This can be reported and reviewed directly, or logs/alerts may be sent to the customer's SIEM system.



Configure Audit Logging

The audit service publishes and logs information to one or more targets, including local data files, the repository, and remote systems.

Audit logs help you to record activity by account. With audit data, you can monitor logins, identify problems such as unresponsive devices, and collect information to comply with regulatory requirements.

The audit service logs information related to the following events:

- System access
- System activity
- Authentication operations
- Configuration changes
- Reconciliations
- Synchronizations

You can customize what is logged for each event type. Auditing provides the data for all relevant reports, including those related to orphan accounts.

When you first start IDM, you'll see an audit log file for each configured audit event topic in the `/path/to/openidm/audit` directory. Until there is a relevant event, these files will be empty.

When IDM sends data to these audit logs, you can query them over the REST interface.

Compliance and Operations Reporting

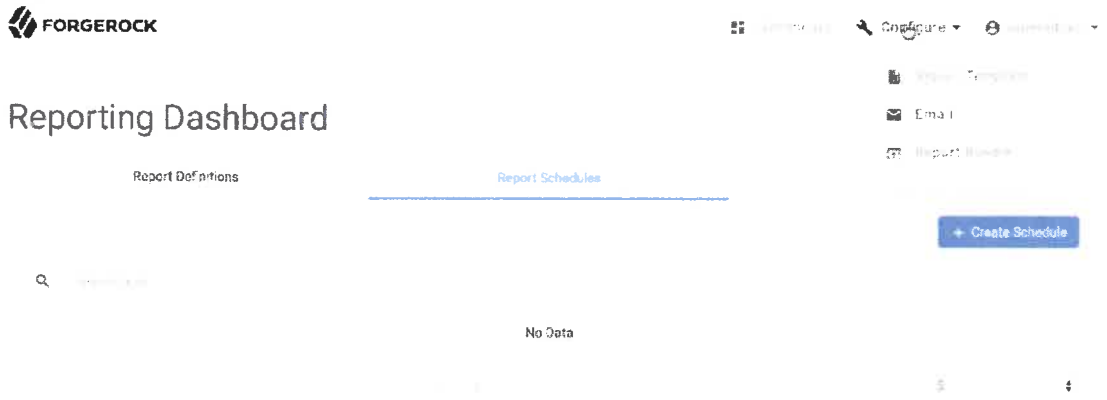
Ping Advanced Identity Cloud provides the ability to define reports that help to facilitate a regular review for regulatory compliance and operations management. Also, Ping Advanced Identity Cloud implements a REST-based Audit Logging Service across all its components, which captures all auditing events critical for system security, troubleshooting, usage analytics, and regulatory compliance. This makes it easier to conduct such reporting from other customer enterprise systems, like the service desk or SIEM system, as desired.

Ad-hoc Reporting Functionality

Ping Advanced Identity Cloud exposes a simple, powerful interface for the configuration of ad-hoc reporting. There are many out-of-the-box sample reports, and all manner of LDAP or database queries can facilitate simple to complex reporting.

Schedule and Push Reporting

Ping Advanced Identity Cloud can be scheduled to push reports as JSON files, SIEM data pushes, or even email messages with attachments to provide the necessary insights into the IAM system for operations or compliance purposes.



SIEM Integration

There are several ways in which the Ping Advanced Identity Cloud can typically integrate with SIEM products as a producer of information, a consumer, or both.

Producer

The Ping Advanced Identity Cloud can provide information to SIEM products using the Audit Logging Service. The platform implements a REST-based Audit Logging Service across all its components, which captures all auditing events critical for system security, troubleshooting, usage analytics, and regulatory compliance. Audit logs gather operational information about events occurring within a deployment to track processes and security data, including authentication mechanisms, system access, user and administrator activity, error messages, and configuration changes. Audit logs are commonly consumed by third-party SIEM and analytics solutions.

Consumer

The Ping Advanced Identity Cloud can consume the information generated by fraud detection tools and SIEM products and use this information for making access management decisions based on adaptive risk when these tools have APIs available for integration. Ping Identity Intelligent Access may use such information to direct the authentication journey, enforcing higher security authentication methods and then passing that risk information along to applications in the session context. Similarly, the authorization policy engine may use fraud detection tools and SIEM products as part of the decision-making process around granting or denying access to certain resources.

Alerts

The Ping Identity Identity Platform provides a variety of standard mechanisms for monitoring and alerting in its components. Ping Identity monitoring is designed to allow alerting on the availability and system characteristics of the various platform components and also on the performance and events that occur for specific functions.

Included Components

This solution proposal by TriVir is unique in that only one vendor is needed to meet the requirements and desired features articulated in this solicitation. Ping Advanced Identity Cloud meets or exceeds all requirements in this appendix and lays a foundation for continued digital transformation. The specific Ping Advanced Identity Cloud components included in this proposal are further outlined in the General Solution Architecture and Platform Capabilities section of this proposal.

ETL Support

Ping Identity supports ETL for initiation program load and subsequent uploads of authoritative or complementary data. The data is then processed using standard Ping Advanced Identity Cloud synchronization and reconciliation policies. Uniquely, Ping Advanced Identity Cloud can consume identities from the existing IAM/legacy environments, if desired, to assist with initial load procedures. ETL processes are typically minimal, as Ping Advanced Identity Cloud connectors automate much of the pulling, pushing, and reconciliation of identity data throughout the enterprise.

Fault-Tolerance and Data Controls

HA, DR Capabilities, and Procedures

Ping Advanced Identity Cloud provides high availability (HA) by deploying Google Kubernetes Engine (GKE) clusters across multiple availability zones (AZs) within a region to create regional redundancy. In the event of a physical hardware failure within a particular zone, workloads are **automatically** redistributed to other zones. Procedures are automated and also available via Ping Advanced Identity Cloud support requests.

Ping Identity provides disaster recovery (DR) by:

- Taking snapshots of the data stored within each region. Should data corruption occur, the images let you restore the datastore and associated configuration data. Because Ping Advanced Identity Cloud takes snapshots incrementally, you can perform a complete restore or restore data starting from the time at which a snapshot was taken.
- Backing up data to a different region. In case of a major outage in a particular region, Ping Identity can restore service by moving the workloads to a backup region.

TriVir has scoped out time in this initial engagement to document and test backup/restore procedures as needed.

Data Eradication

Ping Advanced Identity Cloud allows for partial or complete eradication of customer data via RESTful calls or scheduled coordination with Ping Identity. Ping Advanced Identity Cloud complies with compliance and privacy-related data management requirements, including eradication and purging.

Data Locale

IAM administrators may specify the exact data locale for live, replicated, and backup data per Google Cloud Platform options and data center regions.

Unique Differentiator: Ping Advanced Identity Cloud is the **only IAM SaaS solution** that provides this level of specificity for data locale and sovereignty. Other SaaS IAM offerings typically provide data locale control at the country level, at best.

Network Architecture

Because Ping Advanced Identity Cloud is built on GKE clusters across multiple availability zones within a region, there is regional redundancy. Additionally, workloads are automatically redistributed to other zones should there be an outage (i.e., hardware issue, weather emergency, etc.).

TriVir may go one step further by providing customers the option to have a replicated node for core Ping Advanced Identity Cloud services to run in a backup center at the edge/on-premises (if desired) to maintain operations in the event of complete loss of cloud access. See the attached “Ping Advanced Identity Cloud Security Whitepaper.pdf” for a deeper dive into the Ping Advanced Identity Cloud network architecture and security details.

Experience and Qualifications

TriVir's successful at-scale IAM implementation experience for state governments like the State of Utah, and federal agencies like the US Census Bureau qualifies the TriVir-Ping Identity single platform SaaS offer as a confident choice for State of West Virginia's Identity and Access Management Services and Single Sign-On Solution initiative. TriVir consistently delivers IAM and SSO programs through a repeatable engineering methodology described in a later section of this proposal entitled "Project Methodology and Technical Approach". This process includes automated code promotion, revision control, automated testing, quality assurance, issue tracking, knowledge transfer, and other familiar aspects of an agile program.

With experience delivering IAM programs for the federal government, TriVir staff have strong knowledge of applicable industry and security standards like NIST, ISO, FERPA, CPRA, FedRAMP, DHS CISA guidelines, and others. This knowledge helps to accelerate security reviews with State IAM teams to move functionality to production faster, with security and privacy built in from the beginning of each sprint.

TriVir specializes in large, at-scale IAM and SSO programs. The best example is the State of Utah, with tens of thousands of employees and millions of citizens. TriVir was instrumental in designing a path from legacy on-premises IDM technology to move the Ping Advanced Identity Cloud. Large public agencies that have a mixture of employees as well as external users (like citizens, parents, contractors, etc.) can run into complex situations at times. At State of Utah, an example of this complexity was the requirement to disambiguate employee IAM accounts from citizens accounts. Although most employees are also citizens, the context and situation an account may be used needs different access management policies applied for each situation. For large state governments, similar complexity exists. A staff member may also serve as a teacher. A teacher may also be a coach, or even a parent. TriVir has the experience needed to facilitate these types of potentially complicated relationships, at scale.

Additional details regarding TriVir's profile and capacity are found below. Ping Identity details are provided as well.

TriVir Profile

Number of years in business:

- Established in 2003, TriVir has been in business for over 20 years, focused solely on identity solutions.

Number of years involved in the services described in the request for proposal (RFP):

- TriVir has over 20 years of experience implementing IAM solutions, covering all business and technical aspects of the State of West Virginia RFP.
- TriVir is a partner of several leading IAM vendors in the analyst leadership quadrants and has unparalleled proficiency in the decomposition and documentation of critical business features that need attention during the shift from legacy to SaaS IAM.
- TriVir has served for many years at the highest level of Ping Identity partnership and has provided product features (with Ping Identity source-level access), patches, and new capabilities for the Ping Identity platform. Additionally, TriVir uses a Ping Identity IAM SaaS solution internally and is well-integrated with the Ping Identity IAM SaaS product team.

Total number of employees:

- TriVir currently has 46 employees.

Number of employees dedicated to the services described in the RFP:

- 41 employees. All but two employees (who provide administrative support) are engaged in providing the services defined in the solicitation.

Total number of clients to which you are providing similar services:

- TriVir has provided services and solutions similar to those requested in the RFP to more than 144 customers throughout our history.

Total number of clients of similar size to State of West Virginia:

- TriVir has provided IAM solutions to approximately 22 clients similar in size and scope to this contract. Of our active contracts, ten meet or exceed the size and complexity of the scope of the RFP.

Deliveries of IAM to State Governments:

- State of Utah
- State of New Hampshire
- State of Virginia (Fairfax County)
- State of Florida (Palm Beach/West Palm Beach)
- State of Montana

TriVir does not envision the need for or use of subcontractors in fulfilling the requirements of this solicitation. TriVir reduces friction for this contract by providing a single vendor, single implementor approach.

Ping Identity Profile

Number of years in business:

- Established in 2002, Ping Identity has been in business for over 22 years.

Number of years involved in the services described in the request for proposal (RFP):

- Ping Identity has focused exclusively on building identity and access management products and solutions.
- The state government market vertical has been important for Ping Identity since the firm's inception.
- Ping Identity platform provides IAM for State of Utah.institution:https://www.pingidentity.com/en/customer-stories/3954-state-utah.html (customer testimonial included).

Total number of employees:

- Ping Identity has more than 2,000 employees.

Dedicated services described in the RFP:

- Ping Identity hosts the world's leading IAM Platform-as-a-Service (PaaS) called Ping Advanced Identity Cloud, with leadership standing with each of the major industry research analysts:

  - https://www.pingidentity.com/en/resources.html
- Ping Identity maintains top security certifications:
  - https://www.PingIdentity.com/security-compliance

Total number of clients to which you are providing similar services:

- Ping Identity has thousands of customers in all major industry verticals.

TriVir Organizational and Staff Experience with Identity and Access Management and Single Sign-On System Modernization

TriVir is uniquely qualified to assist the State of West Virginia with modernization initiatives due to having designed the same kind of move for other similarly sized organizations like the State of Utah. Our unique position results from our leadership in the IAM field, depth of identity solution experience, understanding and ability to decompose the existing legacy identity management infrastructure, and expertise and thought leadership in providing on-premise and cloud-based identity solutions to States. Our established history of successful IAM projects includes the following:

- Global IAM rollouts with no-code/low-code user orchestration
- Risk-based friction and Multi-Factor Authentication (MFA) customized to each user and their existing context of use
- Automation of heavy testing for functional, performance, and business use cases to ensure forward project momentum while additional features are added, and more systems are integrated
- Integration with monitoring and identity-proofing systems to ensure suitability and high assurance that the correct person (or thing) is interacting in the IAM system
- Native integration with the industry's largest Credential Management Systems (CMS) for deep identity tie-in, enabling IT system access and building access with strong credentials
- Implement IdMMonitor, a TriVir tool that monitors all identity drivers/connectors, services, and certificates. This has dramatically reduced production outages.
- Implementation of passwordless and WebAuthN solutions to make authentication and authorization nearly invisible for many IAM use cases
- Governance for a movement toward least-privilege access, thereby reducing the cyber blast radius for compromised identities in the system
- Successful migrations from legacy IAM systems to Ping Identity using behind-the-scenes, transparent migration paths that occur at authentication time, enabling users to access the new system with low-to-no impact

With deep and broad Identity and Access Management backgrounds, TriVir consultants can implement solid solutions that consistently meet client-specific acceptance criteria.

TriVir Capabilities

TriVir provides robust and compliant identity and access management solutions. We offer the following service capabilities to multiple federal, state, and local organizations:

- Vendor-neutral recommendations and assistance on IAM-dependent solutions during platform evaluation and selection exercises
- Requirement Assessments (RA) and the creation of solution Acceptance Criteria (AC) documents
- Creation of project roadmaps for all phases, detailing how the Commercial-Off-The-Shelf (COTS) IAM solution may be configured and deployed based on organizational requirements
- IAM system and application-level assistance to enable controlled access management to state resources, SSO for web-based apps (Kerberos, SAML/SAML2, OAUTH/OAUTH2, OpenID, reverse proxy, WebAuthN/Passwordless), legacy apps, Linux/UNIX, and mainframe
- Generation and delivery of training documentation to major user audiences, including end users, helpdesk personnel, and administrators
- Deployment of access governance tools to help manage who has what credentials deployed, compared to what systems/roles they are accessing with those deployed credentials
- Automation of metrics data collection around the use of credentials for internal/external users, standard, and elevated privileges
- Project/Program management assistance to client organization leads
- Automated testing for functionality and business outcomes, Test-Driven Development (TDD), and solution self-regression testing to eliminate the most time-consuming components of testing IAM projects

With a strong history of deploying IAM solutions for States and other public agencies, TriVir is uniquely positioned to configure Ping Advanced Identity Cloud combined with existing technologies in place for the State of West Virginia.

TriVir-Proposed Personnel

TriVir will use a variety of expert IAM employees from our team to fulfill the requirements of the RFP. Consultants dedicated to the State of West Virginia will be supported by similarly qualified TriVir consultants on an as-needed, part-time basis to address the work required and ensure sufficient resources are available to meet delivery schedules that are mutually acceptable to the State of West Virginia and TriVir. TriVir proposes consultants who will meet or exceed the qualifications detailed in the resumes presented later in this document to address the technical needs defined for this project. Each TriVir consultant assigned to work and support this contract maintains up-to-date knowledge and/or certification in identity management and related technologies and has several years of experience working in the technical areas provided in the RFP. In addition, each is skilled in using TriVir's automated testing tool, IdMUnit, and TriVir's monitoring tool, IdMMonitor, and is intimately familiar with TriVir's delivery methodology and approach.

Complementing the consultants will be a skilled PMP/Scrum Master certified project manager. This engineering project manager will work closely with the State of West Virginia team to learn of pending requirements, help define and address critical project dependencies, and work to schedule TriVir consultants best suited to address the needs at their next availability.

The nature of the work called for in the RFP does not lend toward a dedicated staffing model or apportion how much time assigned consultants will provide the State of West Virginia throughout this engagement. Instead, TriVir will appoint consultants to be primarily responsible for responding to operational needs while working to identify and staff project-based work as the organization moves onto the Ping Advanced Identity Cloud platform. As mentioned earlier, once project-based work is defined and organized; the project manager will work to ensure qualified consultants are scheduled to start those tasks at their next availability.

In addition, each member of the TriVir team will have access to senior management, including TriVir's President, Glen Knutti, and TriVir's Chief Operations Officer, Bob Walter.

We look forward to engaging directly with the West Virginia team to display how Ping Advanced Identity Cloud will address the issues presented in this RFP, but also to collaborate with the State on future initiatives related to Identity and Access.