



Imprivata Product Roadmap: Recent Releases and Upcoming Innovation

Published: July 31, 2024



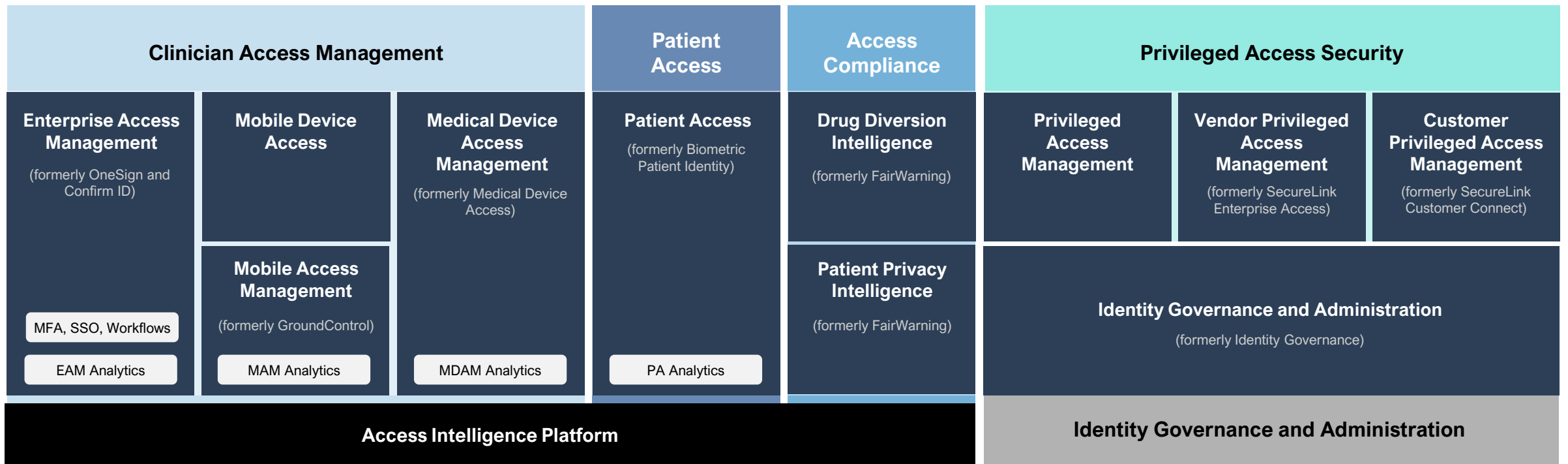


A Note Regarding Forward-Looking Statements

The following includes statements regarding planned or future development efforts for our existing or new products or services. These statements are not intended to be a promise or guarantee of future availability of products, services, or features and are not intended to indicate when or how particular features will be priced or packaged. These planned and future development efforts are based on factors known to us at the time of publication and may change without notice. Purchasing decisions should not be made based on reliance on these statements. We assume no obligation to update these forward-looking statements.”

Imprivata Access Management Portfolio

Made for all user categories including clinicians and other frontline workers, privileged IT admins, and third parties. Integrated across your ecosystem for a consistent user experience.



Enterprise Access Management

(formerly OneSign and Confirm ID)

Overview

Imprivata Enterprise Access Management (EAM) offers SSO and user authentication to enable fast, secure access to the devices, applications, and workflows that clinicians and front-line workers need to care for patients and boost productivity. Capabilities include:

- **SSO into legacy and standards-based applications**
- **Badge-tap access to shared workstations, connected medical devices, and virtual desktops**
- **Re-authentication for in-app workflows**
- **Fast user switching on shared workstations**
- **Complete EPCS compliance**
- **Flexible authentication methods**
- **Comprehensive access workflow analytics**

[Click here for more information](#)

[Return to Portfolio slide](#)

RECENTLY RELEASED

Windows Hello for Business supported for EAM SSO (July 2024)

Imprivata's application single sign-on can be used with Windows Hello for Business on single-user computers to support a passwordless Windows logon experience.

Enterprise Access Management Analytics (May 2024)

Visibility into SSO and user access workflows across your organization to identify and remediate potential security gaps, reduce operational burden and IT overhead, and more.

Number matching to mitigate MFA fatigue attack (October 2023)

Combats a common phishing scam, MFA fatigue attack, by minimizing the risk of users accepting MFA push notifications they did not initiate. When enabled, it requires users to type a code that matches the random number displayed on the application being accessed. Number matching is available for all Imprivata EAM remote access workflows.

Mobile EPCS with Epic Haiku and Canto (October 2023)

Imprivata Mobile EPCS is the industry's only solution that enables facial biometrics for user authentication to send EPCS orders directly from a provider's mobile iOS device via Epic Haiku and Canto. This offers a simpler, more efficient process for prescribing controlled substances from a mobile device while ensuring full DEA compliance.

MFA integration with Entra ID for Conditional Access (July 2023)

Microsoft Entra ID conditional access policies can be applied to Imprivata MFA to enable granular access policies, consolidate MFA authenticators, provide a simplified and more consistent user experience, and reduce security policy complexity.

Self-service renewal of virtual smartcards (NHS England) (June 2023)

Clinicians can self-renew their expiring virtual smartcards to meet the two-year renewal requirements without contacting registration administrators, saving time and reducing burden.

COMING INNOVATION

Support for Entra ID-only customers

Will allow customers who use only Microsoft Entra ID (formerly Azure AD) for their directory to use that as the stand-alone directory for EAM.

Enhanced self-service password reset

The Imprivata ID MFA mobile app will be integrated as a second factor of authentication for self-service password reset, providing a higher level of security.

Integration with Epic Monitor for fast access to digital whiteboards

Clinicians can tap their badge on the digital whiteboard to display a dashboard with critical information specific to the user and their role. Creates fast and secure access to patient information without the need to fully log into the Epic desktop application.

Integration with Microsoft Azure Virtual Desktops

Integrated badge-tap access to shared and private Azure Virtual Desktops.

Android support for Mobile EPCS for Epic Haiku and Canto

Extends the use of facial biometrics for EPCS signing from a mobile device (via Epic Haiku and Canto) to Android devices, giving providers more flexibility when prescribing controlled substances from a mobile device.

Virtual Smartcard Support for Care Identity Service Passcode (NHS England)

Optional feature that enables all newly created Virtual Smartcards to be encrypted using the CIS Passcode provided by the end user, which supports enhanced security standards for national authentication and access in the NHS England.

macOS support

Imprivata agent for Tap and Go and EPCS signing on private and shared macOS computers.

Epic SAML login support

SAML-based integrated authentication into Epic Hyperdrive for a higher level of application security.

Automated biometric consent for EPCS

Ensure compliance with state and federal regulations through biometric consent embedded into EPCS and other enrollment workflows.

Mobile Access Management

(formerly GroundControl)

Overview

Imprivata Mobile Access Management is a comprehensive, end-to-end mobility solution that helps organizations optimize their use of shared iOS and Android devices by delivering

- **Secure device checkout**
- **Simple access to mobile applications**
- **Personalized device experiences**
- **Visibility into device status and assignment**
- **Automated device management workflows**

RECENTLY RELEASED

Native Epic Rover Logout (May 2024)

Update a user's presence status in Epic when devices are checked in to eliminate irrelevant alerts sent to checked in devices.

Simplified device Check Out with Smart Hub LEDs configuration (May 2024)

Admins can now disable the blue (deployment in progress) LED in the check out workflow action.

Indicators for network connectivity loss (May 2024)

Monitors network connectivity on checked in devices with visual indication if the phone loses network connectivity.

Automatically launch an Android application at check out (May 2024)

Admins can now configure an app (ex. Microsoft Teams) to launch automatically after checkout to improve the user experience.

Quick and easy badge enrollment from a mobile device (February 2024)

Users can now easily enroll a new or replacement Imprivata badge directly from the Locker app at the time of check out.

Self Service SAML Setup (February 2024)

Admins can now configure identity federation with their enterprise identity provider.

Support for new Android applications, MDMs, and MDM Launchers (February 2024)

Recent highlights include Tiger Connect and Voalte One applications, SOTI and Samsung Knox MDMs and Microsoft Intune Managed Home Screen and VMware Workspace ONE Launcher for Locker Android.

Monitor device readiness and quickly remediate issues with Heartbeat (November 2023)

Monitor Locker app readiness and prioritize devices with an active heartbeat. Dashboard visibility and **Bulk Deployment** facilitate quick remediation for admins, from the cloud.

COMING INNOVATION

Simplified device refreshes, at scale

Support the bulk erasure and retiring of devices for faster time to value with device refreshes.

Streamlined and secure Check Out workflows

Align security requirements between Enterprise Access Management and Mobile Access Management to streamline check out and improve security, improve management of security.

Simplify Launchpad management and configurations

Develop organization specific, pre-configured Launchpad installations to remove the need for manual configuration.

Comprehensive analytics

Improve reporting and analytics for with more data, customizable dashboards and proactive issue detection.

Improved visibility of device status for department managers

Device management application to provide direct views into device check out status in real-time including who has been assigned each device and where it's been returned.

Faster Check Out experience for iOS devices

Improve the time it takes to check out a device for end users

Simplify deployment of new Launchpads and Smarthubs

Automatically configure badge readers with Enterprise Access Management to quickly enable check out workflows.

Simplify management across multiple organizations

Console Admins can support multiple organizations from one place.

Deliver consistent access experience across systems

Set Android device passcode to match Enterprise Access Management (Formerly OneSign) policies.

[Click here for more information](#)

[Return to Portfolio slide](#)

Mobile Device Access

Overview

Imprivata Mobile Device Access delivers on the promise of uncompromised security and efficiency by removing barriers to access share shared Android devices with

- **Secure, personalized access to Android devices**
- **Single sign-on for mobile applications**
- **Fast user switching with badge-tap on the device**

RECENTLY RELEASED

Enable secure access for more environments and use cases (May 2024)

Support for Android workstations and devices with external badge readers.

Mobile Device Access Analytics through EAM Analytics Platform (May 2024)

Robust analytics capabilities provide unparalleled visibility into user access workflows across your shared mobile devices environments to drive actionable insights, remediate security gaps, and reduce operational burden and IT overhead.

Faster care team collaboration with support for native dialer applications (March 2024)

Mobile Device Access now supports the use of Samsung and Zebra dialer applications to enable fast, secure access to phone calls and notifications on shared devices.

Improved diagnostics and troubleshooting (March 2024)

Users can quickly check Mobile Device Access app configuration and connectivity right from the lock screen and submit logs from the tool for troubleshooting.

Support for new Android applications (March 2024)

Recent highlights include integration with Tiger Connect, Dr. First, Microsoft Edge browser and more.

Simple sign-in and out of Cerner applications (September 2023)

Ensure clinical staff have fast & secure access to the tools they need.

Support for International Languages (February 2023)

Support for customers with devices running with the OS in the native language and support for the translation of strings to the country language.

COMING INNOVATION

Deliver consistent workflows regardless of connectivity

Support for "offline mode" to enable device access when there is no network connectivity.

[Click here for more information](#)

[Return to Portfolio slide](#)

Patient Access

(formerly Imprivata Biometric Patient Identity)

Overview

Designed with privacy in mind, Imprivata Patient Access is a facial recognition solution that enhances patient safety and experience by streamlining check-ins and accurately linking patients to their medical records with a single photo, helping to ensure efficient and error-free healthcare delivery.

- **Improved patient identification accuracy**
- **Enhanced patient safety and experience**
- **Streamlined registrar workflows**
- **Flexible hardware**
- **Seamlessly integrated with Epic**

[Click here for more information](#)

[Return to Portfolio slide](#)

RECENTLY RELEASED

Enhanced photo retake capability (May 2024)

Easily retake patient enrollment photos if the initial photo has issues, such as closed eyes. This flexibility helps improve the appearance of the patient photo.

Smart workflow management (April 2024)

Intelligently prompts the registrar with the appropriate action—either enroll or verify—based on the patient's status. This streamlines the enrollment and check-in processes.

Facial recognition for patient identification (February 2024)

Healthcare organizations can now enhance patient safety and experience by accurately linking patients to their record with a simple face photo through Imprivata Patient Access. Creating a one-to-one match between a patient and their record allows healthcare organizations to provide the best possible care and experience enhanced operational efficiency.

COMING INNOVATION

Integration with Existing Epic Photos

Streamline the enrollment process by leveraging already available patient photos from Epic. This capability eliminates the need for in-person enrollment, enabling instant access and significantly enhancing operational efficiency, thereby delivering faster time to value.

Self-Service Identification

With integration into Epic Welcome kiosks, patients can identify themselves, significantly easing the workload on registrars and speeding up the check-in process.

Duplicate Proofing

As an extra safeguard to help prevent misidentification errors, Imprivata Patient Access will help ensure that each face is enrolled only once. (Allows for the enrollment of identical twins.) This critical feature helps maintain a one-to-one match between a patient and their medical record.

Advanced Fraud Detection with Liveness Checks

Strengthen security measures with enhanced liveness and spoof detection capabilities, helping to ensure that the system is interacting with a real person and not a fraudulent representation.

Configurable Enrollment Age

Tailor the patient enrollment experience by setting a minimum age for eligibility in healthcare facilities, helping ensure compliance and patient care standards.

Reporting by Location

Gain insights with reporting features that allow organizations to understand usage and performance metrics specific to each location.

Image Refinement for Patient Privacy

Improve how images are displayed by cropping and blurring backgrounds, focusing solely on the patient to protect privacy and improve the clarity of identification photos.

PatientSecure

Overview

Imprivata PatientSecure uses palm vein biometric identification to accurately and securely identify patients, reducing identity errors, preventing fraud, and improving workflow efficiency across healthcare systems. This touchless authentication solution ensures positive patient identification at any point of care, enhancing patient safety and satisfaction.

- **Accurate Patient Identification**
- **Enhanced Patient Safety**
- **Fraud Prevention**
- **Workflow Optimization**

[Click here for more information](#)

[Return to Portfolio slide](#)

RECENTLY RELEASED

Azure Virtual Desktop single user session support (May 2024)

Allows PatientSecure to access remote machines using Remote Desktop Protocol (RDP).

COMING INNOVATION

Database Performance Enhancements

Reduces the number of SQL deadlocks and timeouts, reports will run significantly faster.

Display Patient's Preferred Name for Improved Patient Experience

Allows for a more personal patient check-in experience.

Improve Admin Console Experience

Admin console will display frequently performed actions front and center for quick access and streamlined workflows.

Parallel PatientSecure and Imprivata Patient Access

Epic customers will be able to run either PatientSecure (Palm Vein) or Imprivata Patient Access (Facial) at each point of registration.

Patient Privacy Intelligence

(formerly FairWarning)

Overview

Imprivata Patient Privacy Intelligence (PPI) helps protect patient privacy and deliver actionable insights for investigations, documentation, and reporting of privacy breaches. Equipped with artificial intelligence (AI), machine learning, and behavioral analytics, PPI provides healthcare organizations with the tools they need to comply with confidence, protect patient data, and prevent violations

- Proactive & reactive auditing
- Robust reporting
- Efficient investigations

RECENTLY RELEASED

First Access Reporting (July 2024)

Allows customers to build custom reports on First Access data with scores and explanations for enhanced auditing functionality.

Auto-Disabled End User Accounts (May 2024)

Application users accounts that have not been logged into within the previous 180 days will now be automatically disabled for extra security. User accounts will not be deleted, and audit history will not be affected. User accounts can be re-enabled at any time and timeframes for auto-disabling can be customized.

Custom Investigation Memorandums (April 2024)

Allows users to quickly document investigations and manager outreach within the platform. This new functionality also allow users to document investigations that are initiated outside the application for a streamlined investigation process.

2015 Edition Cures Update Certification (March 2024)

Certification of Imprivata PPI Version 24 to the 2015 Edition Cures Update to make it easier to leverage PPI for modular certification under set criteria. Find certification information at Imprivata [ONC Certification Disclosures](#).

Task Status Experience Updates (February 2024)

New, updated User Interface for Task Status screen with various updates to improve overall performance and navigation.

Improved Application Performance (January 2024)

Improved performance when navigating through the application, decreasing screen load times by as much as 60%. Speeding up workflows and creating a better overall experience.

Governance Report Timeframe Options (September 2023)

New additions to the Governance Report Builder to filter for longer periods when selecting the Within Timeframe comparators.

COMING INNOVATION

Internationalization of Machine Learning Closing Model

Availability of our full-feature set of machine learning to our international customers for optimized internal access auditing.

Dashboard Filtering and Library

Streamline users and analyst workflows with the ability to rank users with peer clustering to determine which users present the most risk.

Imprivata Cloud Portal (ICP) Integration

Streamline user experience by providing a holistic Imprivata Cloud Platform.

Unified Patient Privacy Intelligence Model

Streamline risk identification, advancing anomalous workflow model and establishing a foundation for UEBA model expansion.

[Click here for more information](#)

[Return to Portfolio slide](#)

Drug Diversion Intelligence

(formerly FairWarning)

Overview

Imprivata Drug Diversion Intelligence (DDI) helps organizations manage drug diversion to protect their patients, workforce, and organization while satisfying key regulatory requirements for managing controlled substances.

- Medication lifecycle auditing
- Use Case Monitoring
- Investigation management

RECENTLY RELEASED

Device Cluster Management (June 2024)

Discover trends within users and potential anomalies for diversion mitigation with the ability to set customer defined peer groups.

Auto-Disabled End User Accounts (May 2024)

Application users accounts that have not been logged into within the previous 180 days will now be automatically disabled for extra security. User accounts will not be deleted, and audit history will not be affected. User accounts can be re-enabled at any time and timeframes for auto-disabling can be customized.

Custom Investigation Memorandums (April 2024)

Allows users to quickly document investigations and manager outreach within the platform. This new functionality also allow users to document investigations that are initiated outside the application for a streamlined investigation process.

Task Status Experience Updates (February 2024)

New, updated User Interface for Task Status screen with various updates to improve overall performance and navigation.

Improved Application Performance (January 2024)

Improved performance when navigating through the application, decreasing screen load times by as much as 60%. Speeding up workflows and creating a better overall experience.

Governance Report Timeframe Options (September 2023)

New additions to the Governance Report Builder to filter for longer periods when selecting the Within Timeframe comparators.

Updates to UI for better user experience (July & August 2023)

Report page updates to perform bulk actions, and updates to the Governance page layout to be consistent with the Report page layout. Update to a single Enforced Policies screen for a better user experience and performance. Addition of a new screen in the Application Settings to show Application Version History, and "alerts by" dashboard update to better display Alerts by Owner.

COMING INNOVATION

User-Based Risk Model & AI Configuration

Streamline users and analyst workflows with the power of AI, providing the ability to rank users with peer clustering to determine which users present the most risk.

Dashboard Filtering and Library

Streamline users and analyst workflows with the ability to rank users with peer clustering to determine which users present the most risk.

Imprivata Cloud Portal (ICP) Integration

Streamline user experience by providing a holistic Imprivata Cloud Platform.

High Risk User Monitoring

Leveraging one ID technology and our UEBA anomaly detection, monitor your high-risk users on your dashboard and immediately investigate.

[Click here for more information](#)

[Return to Portfolio slide](#)

Privileged Access Management

Overview

Imprivata Privileged Access Management (PAM) is a comprehensive, easy-to-use privileged access management solution secures privileged accounts that from unauthorized access. It provides visibility and control over privileged internal access and secures privileged credentials to prevent a data breach or cyber attack.

- **Secure privileged accounts**
- **Privileged password management**
- **Monitor session activity**
- **Demonstrate compliance**
- **Verify privileged identities**
- **A modern architecture**

[Click here for more information](#)

[Return to Portfolio slide](#)

RECENTLY RELEASED

Dual account management (June 2024)

Ensures seamless connectivity to critical accounts for high load or business continuity scenarios by enabling PAM to manage more than one account that can be used with a single API call to always return valid credentials.

Azure token authentication for MSI account (June 2024)

Allows for native Azure tokens, associated to MSI accounts, to authenticate into PAM via API calls for a more seamless authentication experience for the user.

Multi-account management (May 2024)

Introduces high availability for privileged account rotation to meet the requirement for systems that need 100% authentication uptime.

SSH component updates (April 2024)

Updates to the underlying SSH component enables faster connectivity to sessions and password and key resets, access to modern keys and algorithms, and improved security.

Dynamic and pass-through credentials with PAM web extension (March 2024)

Users can quickly login to a website by dynamically injecting vault secured credentials through the PAM web extension.

New federated sign-in module (February 2024)

The new federated sign-in module introduces an improved login page experience, better performance, and backend security enhancements.

Instant video playback with session events overlay (December 2023)

Easily and quickly understand what a user did a in a session without having to navigate through several reports with an event timeline that displays user activities overlaid on the instant video playback.

MFA grace period (September 2023)

Define a configurable grace period for MFA enforcement to provide a more streamlined experience for users while using the product while maintaining security

COMING INNOVATION

Database account management

Provide support for additional database accounts including native password reset policies for MySQL accounts.

Kiosk account management

Enables PAM to manage and rotate accounts on kiosk systems.

Azure virtual desktop sessions

Provides secure session connectivity to Azure virtual desktops, including permission and workflow enforcement, session recording, and robust auditing.

Vendor Privileged Access Management

(formerly SecureLink Enterprise Access)

Overview

Imprivata Vendor Privileged Access Management (VPAM) is a remote access platform that enables organizations to manage and secure third-party privileged access and connectivity to their internal, critical assets.

- **Third-party identity management**
- **Vendor onboarding**
- **Enterprise-grade remote access**
- **Credential management**
- **Zero trust network access**
- **Session monitoring**

[Click here for more information](#)

[Return to Portfolio slide](#)

RECENTLY RELEASED

Pre-Connection Notifications (May 2024)

Provide timely notifications during the connection process with application-specific information that vendor users need to know before connecting to an application.

Custom Application Access Request Forms (April 2024)

Capture custom information about access that your administrators need to make an informed decision when granting or denying access; common examples include case number or who approved access.

New UI Beta (April 2024)

Experience and familiarize yourself with the brand-new UI in your sandbox environment; help shape future development with direct feedback to our Product Management team.

Gateway Pool Management (January 2024)

Update an instance in a Gateway pool to maintain the most secure, current version, without impacting existing user sessions or connectivity.

Admin Log Export (November 2023)

Quickly and easily export the specific information you need from the admin log to report on specific activity or events.

German Language Availability (May 2023)

Users with their default browser language set to German will automatically see the VPAM UI in German for a better user experience.

COMING INNOVATION

Full New UI Release

Experience a beautiful, modern UI and improved workflows that streamline navigation, processes and ensure information is easily and clearly available.

New Connection Manager

The next generation of the Connection Manager provides a more reliable and faster connection experience.

Containerized Network

Enable easy and streamlined access to users connecting to devices and thick clients with strict port requirements, such as PLCs, common in OT environments.

Improved Upgrade Process for Cloud

Experience a faster and streamlined upgrade process that minimizes downtime and provides quicker access to new functionality and features for customers deployed in the cloud

Credential Rotation

Improve the security around privileged credentials by automating password rotation based on certain events or time-based triggers.

Active User Sessions View

Improve visibility into user activity by showing active sessions by user, rather than by application.

Customer Privileged Access Management

(formerly SecureLink Customer Connect)

Overview

Imprivata Customer Privileged Access Management (CPAM) is a remote support platform that enables service providers and technology vendors to securely connect to their customers' environments.

- Comprehensive, anytime access
- Credential management
- Session recording
- Streamlined access
- Customer access controls
- Least privilege access

[Click here for more information](#)

[Return to Portfolio slide](#)

RECENTLY RELEASED

Access Request Reminder Notifications for Gatekeeper Admins (May 2024)

Automatically remind Gatekeeper Admins of pending requests on a configurable basis to reduce the need to reach out to remind customers and to facilitate quicker access approvals.

Gateway Pool Management (January 2024)

Update an instance in a Gateway pool to maintain the most secure, current version, without impacting existing user sessions or connectivity.

Custom Terms and Conditions for Quick Connect (December 2023)

Apply your own Terms and Conditions that must be accepted by any customers you may support with Quick Connect.

Admin Log Export (November 2023)

Quickly export the specific information you need from the admin log to report on specific activity or events.

Gatekeeper Host Information (July 2023)

Quickly find Gatekeeper host information you may need, such as version information and disk space, without having to connect to the Gatekeeper itself. Easily see the list of hosts a specific Gatekeeper may be installed on to identify duplicates.

SDK Credential Token Support (June 2023)

Improve the security of SDK connections by eliminating any exposure of encrypted credentials with the use of credential tokens for username and password injection.

COMING INNOVATION

New Connection Manager

The next generation of the Connection Manager provides a more reliable and faster connection experience.

Nexus Service and Status Sharing

Immediately review the services available at Nexus sites and their connectivity status, rather having to establish a connection to see this information.

Containerized Network

Enable easy and streamlined access to users connecting to devices and thick clients with strict port requirements, such as PLCs, common in OT environments.

Improved Upgrade Process for Cloud

Experience a faster and streamlined upgrade process that minimizes downtime and provides quicker access to new functionality and features for customers deployed in the cloud

New UI Release

Experience a beautiful, modern UI and improved workflows that streamline navigation, processes and ensure information is easily and clearly available.

Identity Governance and Administration

Overview

Imprivata Identity Governance and Administration (IGA) automates identity lifecycle management, enforces a least privileged environment and enables day-one role-based access.

- Governance of lifecycle
- Role-based access controls
- Same day access
- Least privilege enforcement
- Access monitoring
- Certification of active users

[Click here for more information](#)

[Return to Portfolio slide](#)

RECENTLY RELEASED

Localization enhancements (July 2024)

Localization for end user screens to support users in European countries

Imprivata Enterprise Access Management (formerly known as OneSign) enhancements (July 2024)

Allow for non-Active Directory EAM user management

Improved homepage and content management (July 2024)

Redesigned homepage and redesigned content management section to simplify the creation and update of charts, reports and scorecards

Improved experience in compliance tasks & system administration (December 2023)

Improved UI of system admin and compliance task screens. Compliance tasks can be assigned to the manager of the users with a single click.

Self Service Password Reset using Duo for additional authentication (December 2023)

Support for MFA through Duo when a user resets their password.

Workday integration enhancements (December 2023)

Enhancements include support for Workday identities in a single IGA identity and improves Leave of Absence, Rescinds and data syncing.

ServiceNow integration (Released September 2023)

Point and click ServiceNow integration to reduce errors and save time by eliminating the need to manually create help desk tickets.

Password-less onboarding (Released September 2023)

Provide end users with frictionless, secure and fast onboarding.

Import account data improvements (Released September 2023)

Point and click experience for importing application accounts.

Attestation improvements (Released September 2023)

Application and entitlement attestation now includes an expiration date, enhancing control and compliance over out-of-role access and its duration.

COMING INNOVATION

AI driven peer analysis

Real time AI driven peer analysis for access assignment. If your roles are not fully developed for a new application or population of users, access coordinators and managers can be permitted to review the access of their peers to make informed real-time decisions on what access their user needs.

Imprivata Enterprise Access Management (formerly known as OneSign) enhancements

Automates proximity card provisioning directly from IGA.

Multi-account support

Support for users who require separate accounts for varying roles in downstream applications (e.g. a user who has both a nurse account and a student account at the same organization).

Entitlement driven attestations

Allow for fine grained, out-of-role access controls to allow managers and access coordinators the ability to make very specific requests for their managed identities.

Expand support for Microsoft server 2022

Extending IGA support to include SQL 2022.

Dynamic configuration actions from any report

Enhancing GRC functionalities to facilitate direct actions from tasks and reports

Simplified application account detail view

A newly designed interface for viewing account entitlements without requiring modify permissions.

Identity Governance and Administration (DACH)

Overview

Imprivata Identity Governance and Administration (IGA) automates identity lifecycle management, enforces a least privileged environment and enables day-one role-based access.

- Governance of lifecycle
- Role-based access controls
- Same day access
- Least privilege enforcement
- Access monitoring
- Certification of active users

[Click here for more information](#)

[Return to Portfolio slide](#)

RECENTLY RELEASED

SAP Success Factors Interface (July 2024)

This integration ensures that your SAP Success Factors works harmoniously with our IGA Solution. By aligning with your organizational structure, it streamlines employee onboarding, role assignments, and access controls, all while maintaining compliance and boosting efficiency.

Multi Language (Released April 2024)

Support for multilingual functionality for all forms and emails, adapting to user settings. Available languages include English, German, French, Spanish, Italian, Dutch, and Portuguese. This ensures a seamless and personalized experience for users around the globe.

Improved Performance (April 2024)

Faster response times, smoother navigation, and more efficient workflows.

Bridge Integration (April 2024)

Leverage existing bridges, such as EPIC, directly within IGA. Connect seamlessly to your current systems to streamline access management and enhances interoperability, ensuring a cohesive and efficient identity management process across your healthcare applications and beyond.

Improved Identity & BOB Dashboard Reporting (November 2023)

Users can effortlessly select from a variety of pre-built reports or create custom reports tailored to their specific needs. This new functionality empowers you to gain deeper insights and maintain comprehensive oversight, ensuring your identity management processes are more efficient and transparent than ever before.

Improved SAP HCM Interface (December 2023)

This integration ensures that your SAP Human Capital Management (HCM) system works harmoniously with our IGA Solution. By aligning with your organizational structure, it streamlines employee onboarding, role assignments, and access controls, all while maintaining compliance and boosting efficiency.

Improved SAP User Administration Interface (December 2023)

This feature allows for a seamless and efficient management of user accounts across various SAP environments. By automating user provisioning, role assignments, and access controls, it ensures consistency and compliance throughout the entire user lifecycle.

COMING INNOVATION

HR Data Transformation Wizard – Visual Tool to integrate different HR sources via SQL, ODBC, CSV, XML into IGA and use for Life Cycle Service.

Reconciliation – Stay informed with real-time alerts and detailed reports whenever manual changes occur, ensuring full transparency and control. If an unauthorized or erroneous change is detected, you can quickly and easily revert to the previous state, maintaining the integrity of your system.

New Service Portal– Fully redeveloped service portal with responsive design and security features to be used as a public portal.

Multi-Contract-Support – Native support for multiple employee contracts for one Identity.

Imprivata PAM Integration – Managing administrative accounts within Imprivata PAM.

NIS 2 Event Registration – Use IGA Workflow to manage an NIS 2 event to be sure, that legal deadlines are maintained.

Password Reset as a Standard Service

Includes the ability to add customer changes in hookpoints.

Workflow Troubleshooting

Ability to pause and restart a specific workflow to support debugging, and avoid downtime of target systems.

Interface Improvements and Expansions

Support for multiple Orbis tenants and virtual facilities. AD Interface performance optimization in combination with new database structure. Adding user provisioning into EPIC.

Exchange On-Prem

Refreshing the interface and integrating them in the BOBs.

 **imprivata**[®]

