

Data Sheet | Avancer's Epic – IAM Provisioning Enterprise Application Connector

Overview

Epic's market focuses on providing large healthcare organizations with an integrated suite of healthcare software. The solutions are centered on a Caché database provided by InterSystems.

According to Epic, hospitals that use its software have 54% of patients' records in the USA. About 190 million patients have a current electronic record in Epic.

The range of Epic's applications support functions related to patient care, including registration and scheduling; clinical systems for doctors, nurses, emergency personnel, and other care providers; systems for lab technologists, pharmacists, and radiologists; and billing systems for insurers. It has evolved as an essential application support system within the healthcare industry.

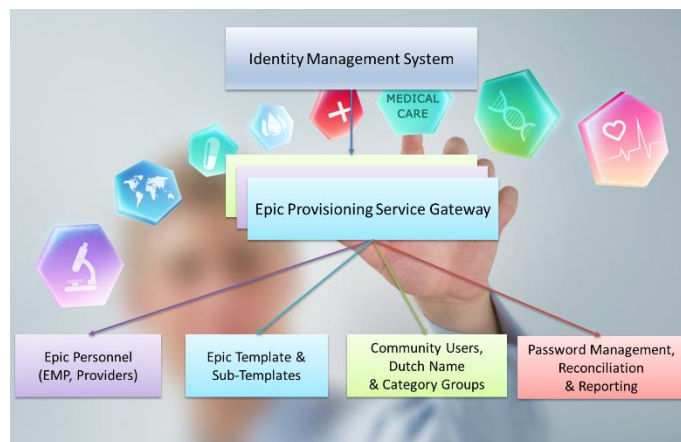


Figure 1 Interaction of Identity Management System with Epic Provisioning Service Gateway

Features of Avancer's EPIC IdM Connector

- 1. Rapid, Timely and Precise account provisioning**
 - Manage complete identity lifecycle for EPIC users
 - Ability to automate SER provider provisioning
 - Enable multiple accounts provisioning
 - Facilitate primary account provisioning with AD authentication
- 2. Supports latest security services Personnel management**
 - Support for internal and external ID
 - Supports training, SunRise/Sunset and advance use cases
 - Establishes relationship(linking) between EMP & Providers (SER)
 - Support for entering credentialing information
- 3. Provides standard interface for reconciliation & real-time identity synchronization for all connected accounts**
- 4. Supports multiple linkable templates (including sub-templates), employee demographics, & category report groupers, extensive reporting.**
- 5. Secures User access through recertification.**



Benefits for Administrators and End-Users

IdM Connectors are used to integrate IdM Solutions with external, identity-aware applications. Avancer's Epic Connector can be deployed quickly to enable IdM Solutions to automate access rights management, security, and provisioning of users on Epic System. For system administrators and end users, such integrations result in the following benefits:

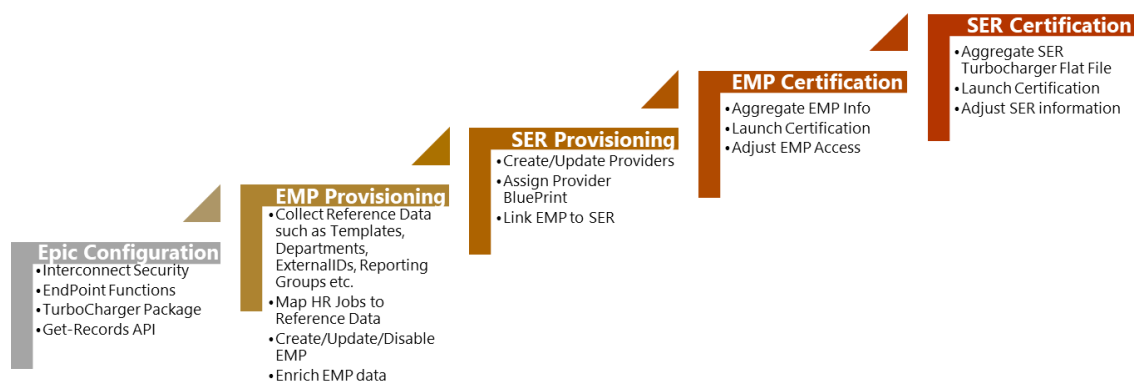
- **Minimizes Costs & Risk:** Stores Identity information in a single, external source, reducing maintenance & auditing requirements.
- **Brings down manual effort:** Automation of provisioning process that ties to existing provisioning systems resulting in accurate provisioning and is in sync with identity life cycle events.
- **Step-Up Enterprise Security:** Extensive reporting, certification to vet out access grants. Additionally, Epic connector grants temporal rights to ease out personnel administration and manual efforts.

Supported Functions of Avancer's Epic – IdM Provisioning Enterprise Application Connector

Avancer's Epic IdM Connector supports the latest Security Services Personnel Management interfaces and handles all identity life cycle events, including joiners, transfers & leavers' identity processes. Avancer's Epic connector also performs CRUD operations on employee identity, setting items like multiple linkable templates, employee demographics, and category report groupers during user creation. Each function can be performed singularly or, depending on the operation, in a batch mode.

Function	Details
Create User	Automated creation of a new user account(EMP and SER) on Epic.
Create SER User	Create (SR,1000) specification based SER user
Link SER-EMP records	Update EMP record with ProviderID and CustomeID Type
Enrich User Access	Set new items like multiple linkable templates, employee demographics and category report groupers during user creation.
Enable User	Activate a disabled user account on the Epic, update the record based on the linked template
Update User	Modify privileges or multiple linkable templates of users' accounts on the Epic.
Update Community User	Update access to EpicCare Link/Plan Link/Healthy Planet Link ("community user") items
Disable User	Temporarily in-activate a user account on the Epic Application.
Delete User	Revoke the access of a user's account on Epic Application.
Password Management	Manage/change passwords. Password propagation to Epic for users who uses Epic Native Authentication.
Reconciliation	Reconciliation of templates and groups. Reconciliation of Users based on the data sent by Epic on daily basis.
Reporting	Reports to view the user access such as the list of departments & their groups, list of locations & service areas.
Certifications	Undertake certification related actions for credentials & other information (Available through IAM system)

Overall Epic Integration Flow



Epic Configuration

1. Configure Epic Interconnect Security to accept EMP and SER data
2. Configure various endpoints to control what data is being sent
3. Configure Turbocharger package to aggregate SER data
4. Configure GetRecords API to aggregate EMP data

EMP and SER Provisioning

1. Establish IAM tool connection with Epic Interconnect
2. Prepare to onboard HR and Credentialing data
3. Prepare IAM tool to configure various LMS and AD use cases.
4. Configure HR Matrix for Job responsibilities vs (Templates/Sub-Templates/Departments/ExternalIDs/ReportGroups etc.) – Applicable to EMP

5. Configure HR Matrix for Job responsibilities vs Blueprints (templates for SER) – Applicable to SER
6. Provision EMP records (Create/Update/Disable Epic EMP accounts)
7. Assign Templates/Sub-Templates etc.
8. Provision SER records (Create/Update/Epic SER accounts)
9. Assign Provider Blueprints
10. Link EMP with SER records

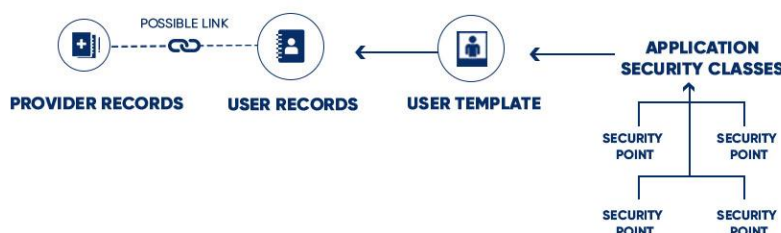
Epic EMP Access Re-Certifications

Post aggregating the Epic EMP data with IAM tool, the certification campaigns can be launched to certify the accesses provided to a user to various templates/sub-templates inside Epic system. Any additional access the user has can be reviewed by managers, Epic security team, and finally by Information Security departments, and accordingly can be certified or revoked. Further, any revocation action taken inside IAM tool can be propagated to the Epic system.

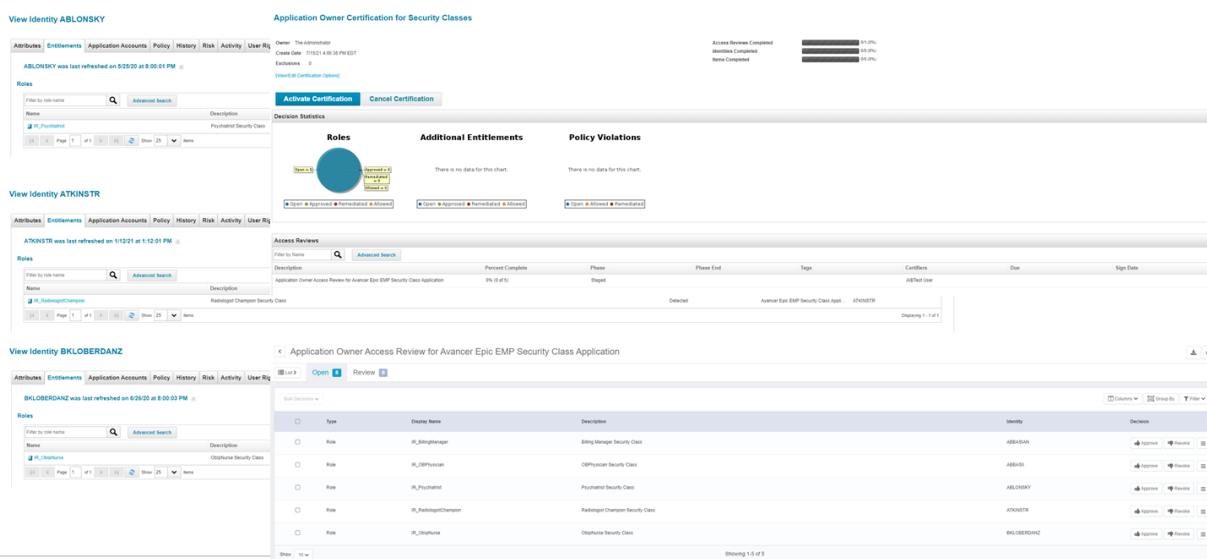
Epic SER Provider Blueprints Access Re-Certifications

Provider Blueprints offer a solution to time-consuming and often repetitive provider maintenance tasks. If the Epic admin/security team members are aware of the values required for a particular role, they can create a Blueprint with those values. Thereafter, the Blueprints information is fed into the IAM system and mapped against job responsibilities. In case of creating any new SER provider, one can simply provision Blueprint information, so that the provider records begin with expected values already entered, instead of beginning as a blank slate. Similarly, with the help of Turbocharger package, which contains a variety of provider/SER data, including the currently applied provider Blueprint, an access re-certification can be launched, on periodic basis, to evaluate if the provider has right information.

Epic Security Class Re-Certifications



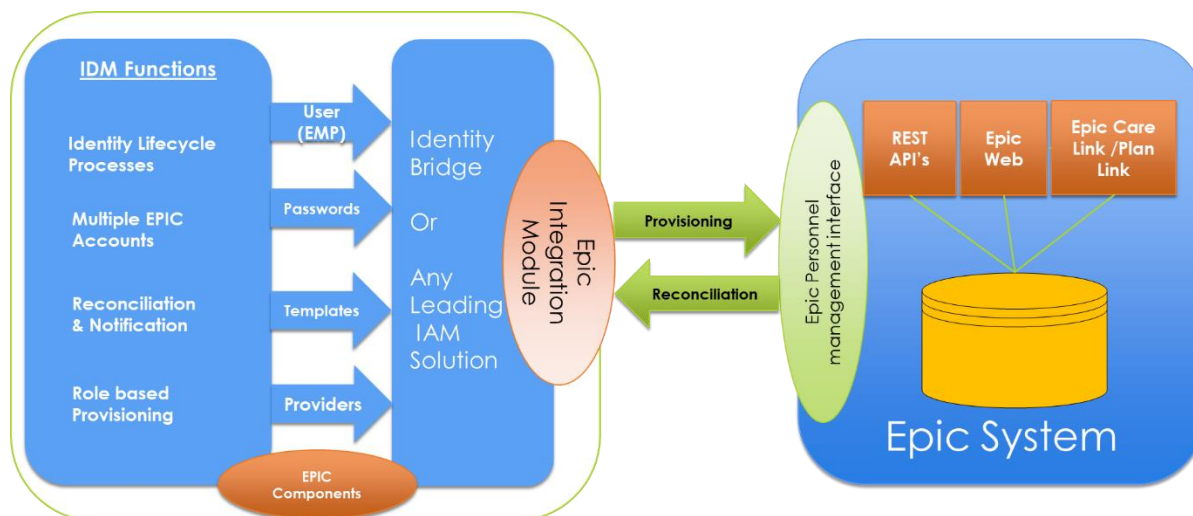
Examples of Security Class Re-Certifications on SailPoint Identity Management System



The screenshot displays three instances of the 'Application Owner Certification for Security Classes' interface in the SailPoint Identity Management System. Each instance is for a different user: ABLONSKY, ATKINSTR, and BKLOBERDANZ. The interface includes a sidebar with navigation tabs (Attributes, Entitlements, Application Accounts, Policy, History, Risk, Activity, User R) and a main content area with sections for Roles, Additional Entitlements, Policy Violations, and Access Reviews. The 'Access Reviews' section shows a table of security classes and their associated users, with columns for Type, Create Name, Description, Identity, and Decision.

Type	Create Name	Description	Identity	Decision
Role	HR_BillingManager	Billing Manager Security Class	ABLONSKY	Approve
Role	HR_OBPProvider	OBPProvider Security Class	ABLONSKY	Approve
Role	HR_Physician	Physician Security Class	ABLONSKY	Approve
Role	HR_RadiologyCharger	RadiologyCharger Security Class	ABLONSKY	Approve
Role	HR_Diagnostic	Diagnostic Security Class	BKLOBERDANZ	Approve

Architecture Diagram



System Requirements and Supported Platforms

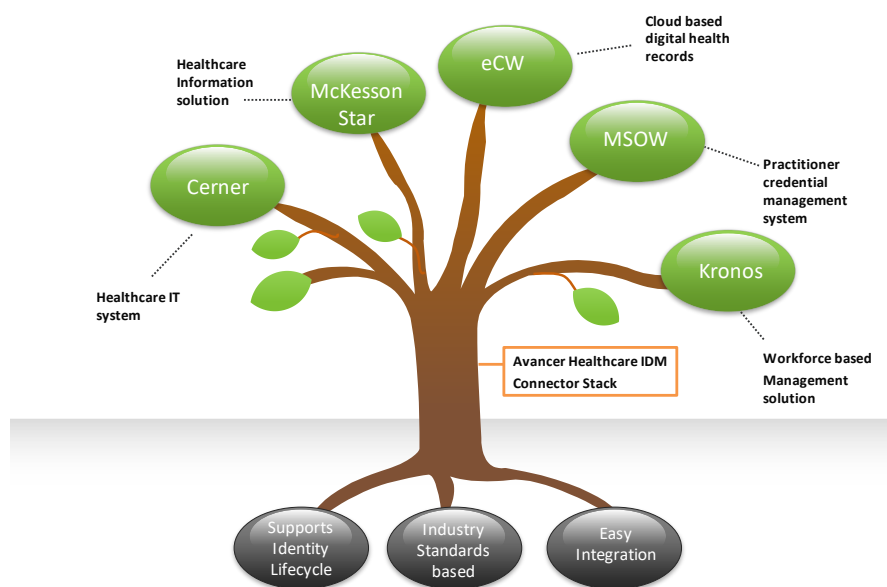
- Java JDK above version 1.6 (+), Connector Server
- SailPoint IIQ, ForgeRock Identity Management 4.5, Oracle Identity Management 11gr1 or 11gr2 (PS1+) or 12c
- Epic Personnel Management interface license (Available from Epic)

Other HealthCare Connectors from Avancer Development Lab

Avancer Corporation has developed healthcare industry-specific IDM connectors for various industry-specific applications to fully integrate IDM provisioning solutions.

Avancer's product and IT Security team come together to meet critical success factors, such as:

- Breadth and depth of industry knowledge and technical experience
- Ability to team with management, implementation professionals, and internal audit personnel
- Consistent, modular, and easy-to-use methodology
- Focus on learning, knowledge transfer, and training



Corporate Headquarters

30N Main Street,
suite 201
Cranbury, NJ 08512

Tel: 609 632 1285
Fax: (877) 843-8594

Email: info@avancercorp.com
<https://www.avancercorp.com>

About Avancer

Avancer Corporation is a multi-system integrator focusing on Identity and Access Management (IAM) Technology. Founded in 2004, it has over a decade's expertise in the field of Identity and Access Governance and IT Security. With a depth of experience in end-to-end IT Security Solutions, Avancer has evolved as a specialist in integrating enterprise IT security through a range of solutions, products, and services focused on IAM Technology. Our services range from full-term project life-cycle implementation to tailor-made short-haul projects, including software procurement, architectural advisement, design, and development through deployment, administration, and training.

For More Information, please visit <https://www.avancercorp.com>.

© 2022 Avancer Corporation. All rights reserved. Avancer, the Avancer logo, and all techniques are trademarks or registered by Avancer Corporation. in the U.S. and other countries.