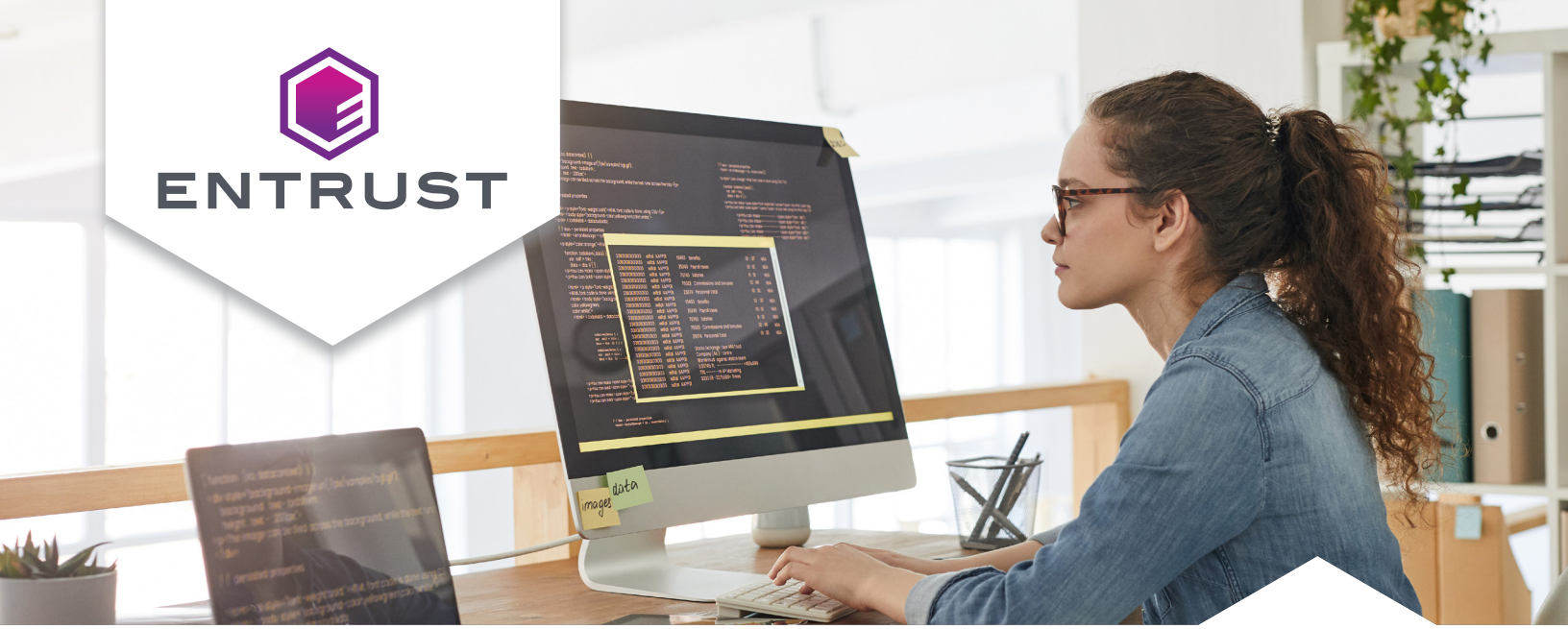


Automate Identity Lifecycle Management with System for Cross-Domain Identity Management (SCIM)

Onboard and offboard users with confidence to ensure only authorized and active users have access to resources.

Provisioning

User provisioning is an identity and access management (IAM) process that ensures employee/user accounts are created, updated, deleted, and given proper access across multiple applications and systems at the same time. Users who are provisioned and part of a group can be automatically assigned to specific applications or a group of applications. User information such as first name, last name, date of birth, address, group name, and other data are available through account and access management. User provisioning is usually triggered by events like onboarding, hiring, promotions, and transfers.

Create, update, delete

Learn more about Identity as a Service at entrust.com

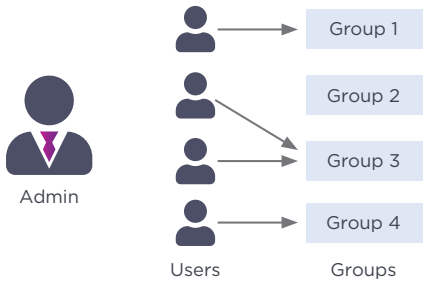
System for Cross-Domain Identity Management (SCIM)

Deprovisioning

User deprovisioning is the process of disabling or removing a user's access to an application or system. It involves revoking permissions, disabling the account, and removing a user from any role or group they are part of. It is usually done when an employee or user leaves an organization/offboarding or switches to a new role/department.

Role-based provisioning

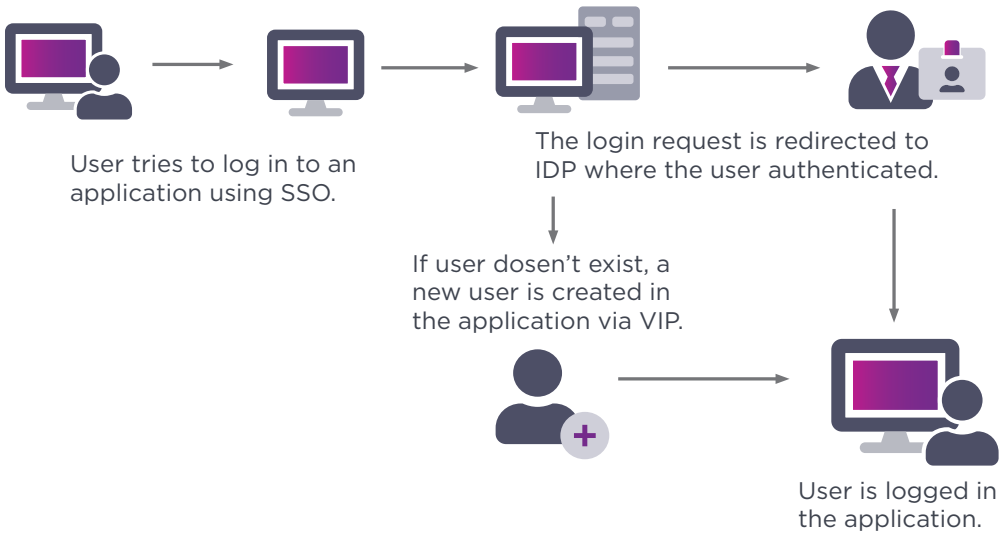
Role-based lifecycle management allows for the use of groups and roles to define access and permissions. It simplifies managing permissions and users by automating processes.



Just-in-time (JIT) provisioning

Provisioning using SAML assertions is commonly referred to as JIT provisioning. With JIT provisioning, user accounts are created when users sign on to an application for the very first time, provided they have necessary permissions. To enable JIT provisioning, administrators must first set up single sign-on (SSO) between the target service provider (SaaS application) and the identity provider (IdP) and confirm that the user attributes required by the application are included.

When a new user attempts to log in to the application for the very first time, they will instantly invoke the creation of their account, rather than requiring an admin to do it. SAML assertions provide the application with the information it requires from the identity provider.



Learn more about Identity as a Service at entrust.com

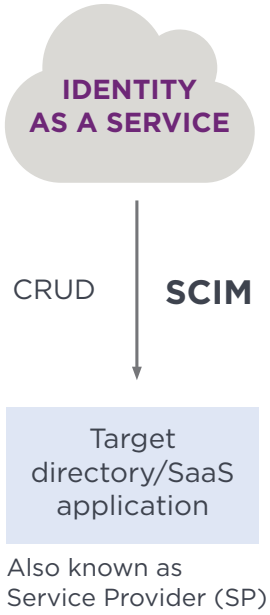
System for Cross-Domain Identity Management (SCIM)

What is SCIM?

System for Cross-Domain Identity Management is an open standard based on REST and JSON. With the SCIM protocol, user data is stored in a consistent way and can be shared with different applications. This allows for automated and orchestrated provisioning and deprovisioning of users across multiple applications and systems.

Outbound SCIM

The IdP is the SCIM client and is connected directly to the user directory and monitors for changes. When users are added, deleted, or updated, corresponding changes are pushed to the target directories (SaaS applications) through the SCIM protocol.



Also known as Service Provider (SP)

Inbound SCIM

The source directory containing the user information that is the source of truth is external to the SCIM client (IdP). The source directory can be partner systems, HRIS systems, etc. The source directory updates the SCIM client (IdP), which in turn will update other target directories (SaaS applications).

Learn more about Identity as a Service at entrust.com

System for Cross-Domain Identity Management (SCIM)

Benefits of SCIM

Improve UX - Users automatically get access to applications and systems needed without requiring individual requests to IT.

Enhance security - Ensures users can only access applications and systems they are authorized to use. Ensures users are deactivated instantly across applications and systems during offboarding.

Reduce cost - Better utilization of licenses and resources through just-in-time (JIT) provisioning. A user account isn't created until the first time the user accesses an application.

Eliminate overhead - Automated provisioning allows changes to be automatically synchronized to all applications instantly, reducing the need for manual intervention and streamlining user lifecycle management.

User and app provisioning with Entrust Identity as a Service (IDaaS)

IDaaS supports the SCIM protocol. Users can be provisioned outbound to various services and applications. Configuration includes URL of the service or application, OAuth credentials needed to authenticate into the service, mapping of IDaaS user attributes to the service attributes, and using groups to specify which users will be provisioned for a given service. Once configured, when IDaaS users are created, updated, or deleted those changes are sent to the service.

In addition, IDaaS also supports inbound provisioning with users from Azure AD synced into Entrust IDaaS with inbound provisioning for enhanced authentication and access management services. Both users and groups are synced from Azure AD into the IDaaS user directory.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223