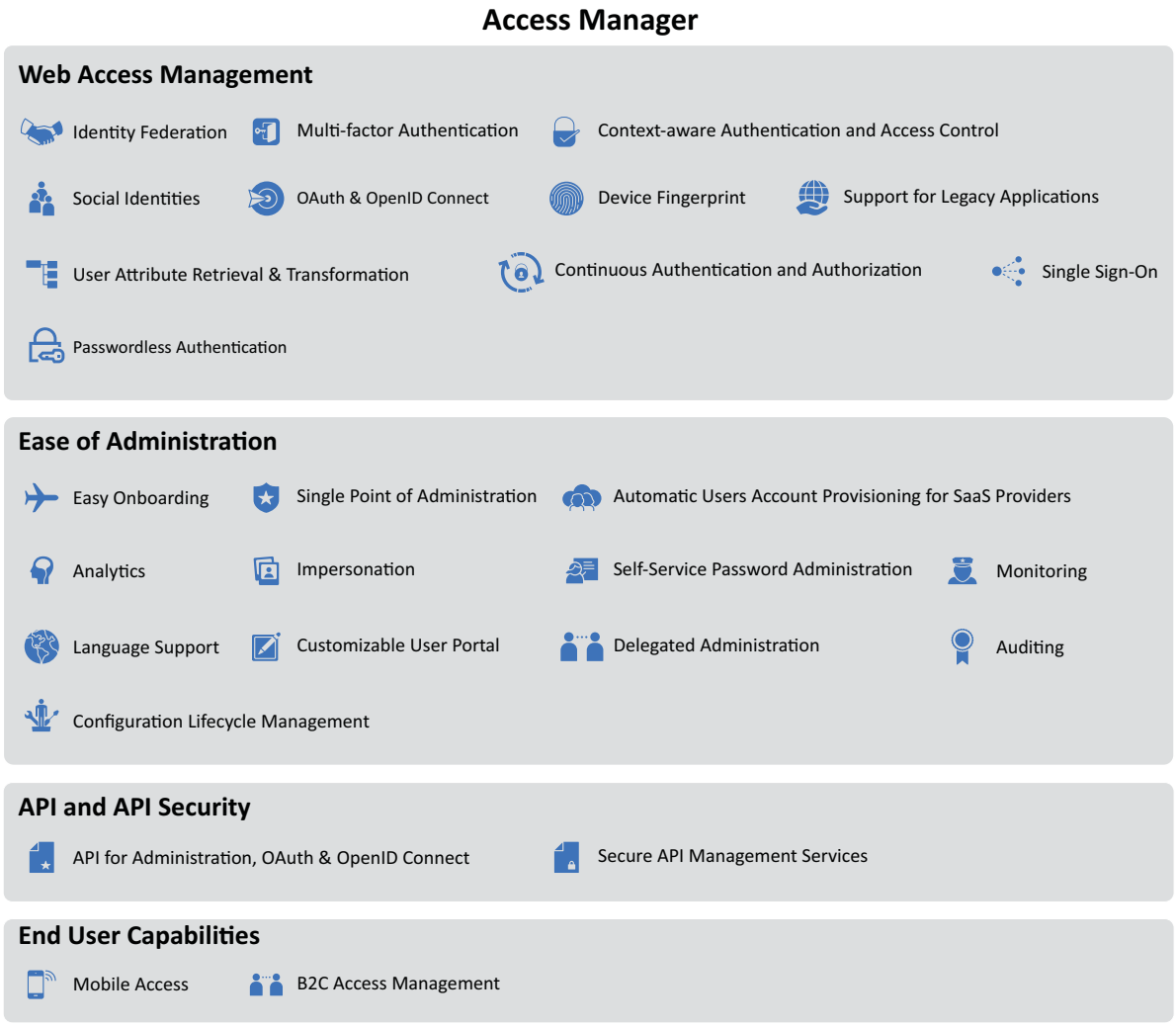
opentext™

Access Manager Overview

Access Manager is a comprehensive access management solution that provides single sign-on and secure access to web-based applications, SaaS services, and federated business-to-business interactions.

Access Manager provides authorized users with adaptive, context-aware, and secure access to Intranet and cloud applications from anywhere and from any device.

Access Manager uses industry standards, such as SAML, OAuth, OpenID Connect, and WS-Federation to deliver federated single sign-on and supports multi-factor authentication, role-based access control, and data encryption.



For more details about these features, see "Key Features" on page 3.

How Access Manager Solves Business Challenges

Access Manager focuses on simplifying secure access to web applications and devices for your employees and partners and on simplifying consumer management.

Access Manager lets you provide your employees, customers, and partners secure access to your applications from any type of device.

The following are the common use cases of Access Manager:

- **Secure Web Access Management**

  Provides a secure and seamless SSO for employees to on-premises, cloud, and SaaS applications. It enables organization to provide secure access to sensitive data by using context-aware multi-factor authentication and granular access control.

- **Effective Partner Collaboration**

  Provides delegated administration capability to manage secure access for partners. Enables restrictive access to only required applications instead of the entire network to partners. This helps in eliminating the risk of security breaches by any third-party partner.

- **Simple and Secure Consumer Access Management**

  Delivers robust access management including self-service on-boarding and SSO for your customers. It enables your customers to sign-up and set up their own accounts using social identities, such as Facebook, Google, Twitter, and LinkedIn.

  Access Manager enables self-service management of identity and profile data of your customers and control their access to applications and services. Access Manager ensures that consumers' identities, personal information, and privacy are protected.

Access Manager is a one-stop solution if your business requires any of the following identity-enabled access control capabilities:

- Providing SSO to employees to eliminate the need of managing multiple passwords.
- Enabling federation capabilities to share the information securely with business participants.
- Protecting resources by providing access to only authorized users.
- Ensuring that the authorized users can access resources regardless of users' location or the type of device they use.
- Ensuring that users have access only to the resources required for their jobs.
- Providing identity enabled access control to protect users' privacy and confidential information.
- Providing facility to access protected resources by using token-based protocols.
- Providing facility to users to use their existing credentials to access services from different service providers, such as Office 365 and Salesforce.
- Managing multiple SaaS accounts in your corporate environments.
- Determining and providing access depending on the context: who, what, when, where, history.

Key Features

Flexible Deployment

Access Manager offers flexible deployment as an all-in-one appliance, or globally distributed servers. The solution supports installing as a virtual server in your private data center, public cloud (Amazon Web Services (AWS) EC2 and Microsoft Azure), or a combination of both.

Access Manager comes with the following deployment options:

- Deploying individual components (Identity Server, Access Gateway, Analytics Server, and Administration Console). Each component can be installed and managed on separate servers. These can also be deployed as services on Amazon Web Services EC2 and Microsoft Azure.
- Deploying Access Manager components through a containerized mechanism. Access Manager uses Kubernetes for managing Docker containers. Access Manager components are delivered as Docker images.
- Deploying all components as an appliance. Access Manager Appliance is a soft appliance based on SUSE Linux Enterprise Server. It bundles pre-configured Identity Server, Access Gateway, and Administration Console in one server. Analytics Server is installed and managed on a separate server.

Secure Web Access Management

Access Manager delivers the appropriate level of access across your Intranet and cloud-based services for all your users. Access Manager delivers simple and secure access irrespective of whether it is for your employees or consumers, laptop or mobile.


Single Sign-On


Secure Identity Federation


Multi-Factor Authentication


Context-aware Authentication and Access Control


Passwordless Authentication


Broad Support for Social Identities


Device Fingerprinting


Continuous Authentication and Authorization


OAuth and OpenID Support


User Attribute Retrieval and Transformation


Support for Legacy Environments

Single Sign-On

Access Manager establishes authentication to applications and provides authorization for those applications. With Access Manager serving the front-end authentication, you can deploy standards- based single sign-on (SSO). With SSO, your employees, partners, and customers need to remember only one password or login routine to access all corporate and web-based applications they are authorized to use.

By simplifying password management, Access Manager helps you enhance users' experience, increase security, streamline business processes, and reduce system administration and support costs.

See Configuring Authentication.

Secure Identity Federation

In today's business environment, organizations need to share resources with trusted business partners in a secure manner. Access Manager provides federated identity management to enable users to authenticate seamlessly and securely across autonomous identity domains.

Access Manager also supports federated provisioning. New user accounts can be automatically created in your trusted partner's (or provider's) system. For example, a new employee in your organization can initiate the creation of an account in your business partner's system through Access Manager rather than relying on the business partner to provide the account. Customers or trusted business partners can automatically create accounts in your system.

Access Manager enables you to determine which business and personal information from your corporate directory to share with others. You can choose to share only the information required to establish the account at the service provider or trusted partner. Access Manager supports out-of-the-box integration and SSO to Microsoft SharePoint and Office 365.

See Configuring Authentication.

Multi-Factor Authentication

Used together with NetIQ Advanced Authentication, Access Manager supports multi-factor authentication to provide secure access from any device with minimal administration. Advanced Authentication delivers various authentication mechanisms that enable identity assurance and proofing apart from traditional username and password based authentication. You can authenticate on diverse platforms by using various authenticators such as Fingerprint, OTP, and Smartphone.

See Multi-Factor Authentication Using Advanced Authentication.

Context-aware Authentication and Access Control

Access Manager enables organizations to select the authentication methods that fit the context of access. It provides risk-based access control, authentication, and authorization of users based on the context, pattern, location, and various other attributes. Using the right authentication type provides high security for sensitive information while simplifying access for authorized users.

See Risk-based Authentication.

Passwordless Authentication

Passwordless authentication differs from traditional username and password-based login systems. Instead of requiring users to remember and input a password, it uses biometrics, one-time codes sent via SMS or email, or a physical security key.

Access Manager supports it through the following features:

- **Kerberos Authentication**
- **Certificate-based Authentication**
- **Integration with NetIQ Advanced Authentication**

  When integrated with NetIQ Advanced Authentication, Access Manager supports passwordless authentication through the Advanced Authentication methods.

See Access Manager Passwordless Authentication.

Device Fingerprinting

Users can log in to applications by using any device. The device can be a desktop, a laptop, or a mobile device. Each device has many characteristics, such as operating system, hardware, and browser characteristics. Access Manager uses device characteristics and user identity to create a unique fingerprint of the device. You can use this fingerprint to uniquely identify and associate a risk profile for the device.

See Device Fingerprinting.

Broad Support for Social Identities

Access Manager supports authentication through external OAuth providers, such as Facebook, Google+, Twitter, and LinkedIn. Social authentication simplifies login for users and does not require maintaining large user stores. Login using social identities provide a convenient way for users, improving customer satisfaction, and increased registration levels.

Social login allows business, universities, and government entities to leverage social identity providers to share select identity information for authentication via OAuth tokens. This information can then be used to provide protected online services ranging from customer-focused applications, university sites to state and local services and more.

See Social Authentication.

Continuous Authentication and Authorization

Access Manager provides the capability to reevaluate the risk associated with an active session at a regular interval. When a user's contextual parameters, such as IP address or location, get changed, Access Manager can perform any of the following actions:

- Prompts the user to re-authenticate
- Prompts the user to perform second-factor authentication
- Logs out the user

You can configure this capability through the following features of Access Manager:

- Risk-based authentication: See "Risk-based Authentication" in the *NetIQ Access Manager Appliance 24.2 (v5.1) Administration Guide*.
- Session Assurance: See "Setting Up Advanced Session Assurance" in the *NetIQ Access Manager Appliance 24.2 (v5.1) Administration Guide*.

OAuth and OpenID Support

Access Manager supports OAuth and OpenID Connect for secure token-based authorization. It enables users to allow third-party clients to access users' private resources. Users do not need to share their credentials. Third-party clients can be web applications, mobile phones, handheld devices, and desktop applications.

Access Manager uses OpenID Connect along with OAuth to implement a single sign-on protocol on top of the OAuth authorization process.

See OAuth and OpenID Connect.

User Attribute Retrieval and Transformation

The User Attribute Retrieval and Transformation feature enables you to retrieve attributes from an external data source (any database, REST web service, or LDAP repositories) and transform before sending it in an assertion. You can also transform a user's local attributes (LDAP attributes, Shared Secrets, and various profiles such as Personal Profile and Employee Profile).

See User Attribute Retrieval and Transformation.

Support for Legacy Environments

In the legacy environments where federation may not work, Access Manager can serve as a reverse proxy to protect your web resources.

See Protecting Web Resources Through Access Gateway.

Ease of Administration

 Single Point of Administration

 Delegated Administration

 Application Connectors for Easy On-boarding

 User Accounts Provisioning Using SaaS Account Management

 Customizable User Portal

 API Support

 API Security

 Access Manager Dashboard

 Configuration Lifecycle Management

 Self Service Password Administration

 Language Support

 Impersonation

 Auditing

 Monitoring

Single Point of Administration

The browser-based Administration Console provides a central location for your administrators to view, configure, and manage all installed components and policies. In addition, IT managers can monitor the real-time health of all network and automate the certificate distribution using this console.

See Configuring Administration Console.

Delegated Administration

You can delegate some of the administrative tasks to a user with limited administrator rights. For example, resetting users' passwords. This helps reduce the burden of administrators.

This capability also eliminates any risk of security breaches when collaborating with partners. You can provide your partners with restrictive access to only the required applications.

See Configuring Administration Console.

Application Connectors for Easy On-boarding

Access Manager provides a simplified way using connectors to give users secure SSO access to different web applications. Access Manager uses connectors to establish the connection between Access Manager and applications. When you configure a connector for an application, the system automatically creates an appmark for this application and adds it on the User Portal page.

Access Manager provides an Application Connector Catalog (https://catalog.netiq.com/ncarest/displayCatalog) containing the list of available application connectors that Access Manager supports for SSO.

Application Connector Catalog displays all available connectors and the browsers that are compatible with the connectors. The catalog can display the connectors by name or by connector type. The available connector types are SSO Assistant, SAML, SAML/Account Management, and WSFED.

See Access Manager Appliance CE 24.2 (v5.1) Applications Configuration Guide.

User Accounts Provisioning Using SaaS Account Management

SaaS Account Management (SAM) addresses several common problems with SaaS accounts in corporate environments, such as the proliferation of SaaS accounts, the need to have a user account in each SaaS system to enable user access, and the need to deprovision accounts when user roles are changed or users leave the company.

SAM in Access Manager enables you to provision user accounts automatically to your SaaS providers. After you link your user store and configure your SAM connectors, SAM performs the following actions:

- Automatically provision user accounts to supported SAML applications.
- Synchronize any changes you make in your user store.
- Automatically deprovision accounts for connected applications based on the following changes made in your user store:
  - When a user no longer needs access to the application.
  - When a user's responsibilities are changed.
  - When a user leaves the company.

To provision SAML accounts by using SAM, you must first purchase and deploy the SAM appliance and configure the appropriate SAM connector for the SAML application. For more information about deploying the SAM appliance and SAM connectors, see the NetIQ SaaS Account Management 1.0 Connectors Guide and the NetIQ SaaS Account Management 1.0 Installation Guide.

Customizable User Portal

Access Manager provides a customizable user portal. You can customize user interfaces, such as the optional login page and portal. With minimal effort, you can brand the login page with your own corporate logo and colors. Users also have the flexibility to choose favorites and the type of view they want to experience.

See Setting Up an Advanced Access Manager Configuration.

API Support

Access Manager includes administrative APIs and OAuth and OpenID Connect APIs. Administration APIs help to automate the common administrative tasks. OAuth and OpenID Connect APIs are for all OAuth functionalities, such as endpoints for registering clients and obtaining access tokens.

See Access Manager 5.0 Developer Resources Documentation.

API Security

Secure API Manager extends Access Manager’s capability to secure micro-services, REST-based web services, and legacy API systems. Secure API Manager offers API creation, lifecycle management, API traffic management, and analytics. Secure API Manager requires Access Manager as the Identity Provider. Access Manager provides authentication of API clients and authorization of APIs protected by Secure API Manager.

For information about Secure API Manager, see Secure API Manager Overview.

For information about using Access Manager with Secure API Manager, see Configuring Secure API Manager.

Access Manager Dashboard

Access Manager includes Access Manager Dashboard to provide visual analytics of access related data based on the usage, performance, and events of Access Manager. The events are captured and filtered through the Analytics Server component.

This dashboard helps in visualizing the access patterns, tuning the policies, and getting insights about the usage of Access Manager in your environment. You can also monitor the real-time data access patterns to decide further actions.

See Analytics Dashboard.

Configuration Lifecycle Management

The wizard-based code promotion utility allows you to bring up a new server, take a backup, or migrate your policies from one Access Manager environment to another Access Manager environment in a matter of minutes.

You can use Code Promotion to replicate configuration between two Access Manager systems that are in different networks, with a different number of devices, and with different user stores.

See Code Promotion.

To maintain the file-based advanced configuration, Access Manager provides the Advanced File Configurator feature.

See Advanced File Configurator.

Self Service Password Administration

Used together with NetIQ Self Service Password Reset, Access Manager enables users to reset their passwords or unlock their accounts without calling the help desk. Access Manager distributes password updates in real time across all your physical and virtual resources. That makes your environment password-maintenance free.

See Configuring Self Service Password Reset Server Details in Identity Server.

Language Support

The Access Manager installation software and Administration Console are not localized and are available only in English.

The User Portal and its help files are localized. This portal is available when users log in to Identity Server. Access Manager also supports localizing error messages and login prompts.

Access Manager supports localization in the following languages:

- German
- French
- Spanish
- Italian
- Japanese
- Portuguese
- Dutch
- Chinese (Simplified)
- Chinese (Traditional)
- Swedish

The language must be set in the client's browser to display a language other than English.

Impersonation

Access Manager enables a help desk user to perform certain actions on behalf of users without knowing their credentials. The help desk user gains access to the user's existing configuration and performs the necessary actions required for troubleshooting.

See Impersonation.

Auditing

Access Manager supports audit logging at the component level. You can configure Access Manager to use Sentinel, syslog server, or Analytics Server as the audit server.

The audit logs record the events occurred in the identity and access management system. The audit logs are intended primarily for auditing and compliance purposes.

See Auditing.

Monitoring

An alert is generated whenever the system detects a condition preventing it from performing normal system services. Access Manager components have been programmed to send alerts to various types of systems such as Sentinel server or syslog server. Therefore, the administrator is aware of any significant change that affects Access Manager performance.

See Monitoring Component Command Status, Monitoring Server Health, and Monitoring Alerts.

End User Capabilities

 MobileAccess  Business-to-Consumer Access Management Consent Management

MobileAccess

Access Manager enables you to extend your web-based applications to your mobile users. It supports the MobileAccess app to keep the applications secure and simple to access. Access Manager includes an SDK for iOS, OpenID Connect, or OAuth for organizations that deliver services through native mobile apps.

See Enabling Mobile Access.

Business-to-Consumer Access Management

Access Manager offers a solution that addresses a broad set of Business-to-Customer (B2C) use cases. The B2C solution enables you to securely identify and engage with your customers while providing a seamless experience on any device, app, or service they are using.

Access Manager, in combination with NetIQ Self Service Password Reset and NetIQ Advanced Authentication, delivers support for B2C use cases, such as user on-boarding, account validation, customizable web logins, portal integration, device registration and management, preference, profile, and privacy management. These are achieved through a broad set of APIs, customizable scripts, and a built-in portal.

It enables customers to set up end-consumer facing applications and portals, enabling better end-consumer interaction. It also provides tools to support privacy and security requirements outlined in regulations such as GDPR and PSD2.

See *Access Manager Business to Consumer Access Management*.

Consent Management

Access Manager allows end-users to choose which personal data they want to share with a business. For more information about how Access Manager handles user consent, see the following resources:

- **OAuth Consent using Scopes**: Scopes decide what resources client applications can access and what actions they can perform on the resources. It can include any user attribute from the user store or any custom claim.

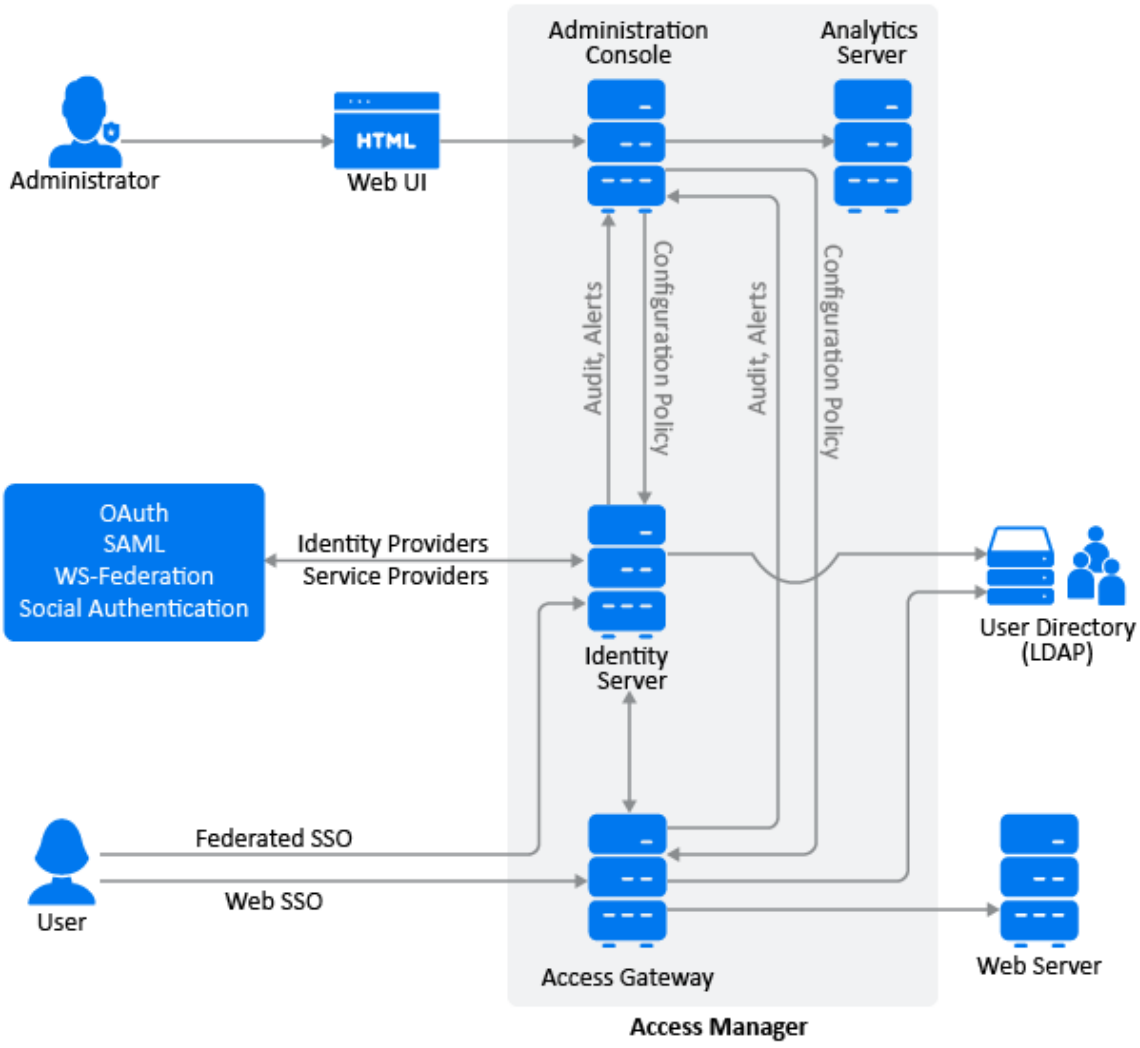
  Access Manager can issue only the defined scopes to the client application. See “Defining Scopes for a Resource Server” in Configuring OAuth and OpenID Connect.
- **Consent during Identity Federation**: Access Manager prompts end-users to confirm whether they want to federate their identities with the service provider. See “Verifying the Trust Relationship” in Establishing Trust between Providers.
- **Consent in the Business to Consumer Access Management scenario**: End-users can decide what personal information they want to share with applications. See Access Manager Business to Consumer Access Management.
- **Consent during Impersonation:** Impersonation enables a help desk administrator to perform actions on behalf of end-users without knowing their credentials. End-users can decide whether to share the session with the help desk administrator. See Impersonation Flow.

Architecture

Access Manager consists of the following components:

- Administration Console
- Identity Server
- Access Gateway
- Analytics Dashboard

The following diagram depicts the architecture and components of Access Manager:



Administration Console

Administration Console provides a unified console for configuring and managing all components of Access Manager.

Key features:

- Resource management, such as policies and certificates

- Health and statistics monitoring of individual components
- Policy administration
- Certificate management
- Delegated administration
- Persistent configuration store
- Granular auditing using syslog server

Identity Server

Typically, Identity Server functions as an identity provider. However, you can configure it as an identity consumer or service provider by using SAML or OAuth protocols.

Key features:

- Authentication using x509, RADIUS, Time-Based One-Time Password, social authentication using external OAuth providers, risk-based authentication, and so forth.
- Federated authentication using SAML, WS Federation, WS Trust, or OAuth.
- Authentication of user identities stored in multiple identity stores, such as eDirectory, Microsoft Active Directory, or Sun ONE Directory Server.
- Service provider account provisioning by creating user accounts automatically during a federation request.
- Single sign-on and logout.
- Authentication and identity services to Access Gateways that are configured to protect web servers.
- RBAC (role-based access control) management to associate roles and attributes with an authenticated user.

Access Gateway

Access Gateway provides secure access to existing HTTP-based web servers. It provides security services (authorization, single sign-on, and data encryption) integrated with the identity and policy services of Access Manager.

Key features:

- Single sign-on to protected web services (with Identity Server).
- Authorization to authenticated users.
- Single sign-on to legacy web servers through form-fill and identity injection. Identity injection is retrieving information from a LDAP directory and injecting the information into HTML headers, query strings, or basic authentication headers to send this information to the back-end web servers. Web servers use this info to personalize the content or for additional authorization decisions.
- Multi-homing that enables to use a single public IP address to protect multiple types of web resources.
- Caching to enhance the content delivery performance. When a user meets the authentication and authorization requirements, the user is sent the page from the cache rather than requesting it from the web server.

- URL Normalization or Rewriting to ensure the following conditions are met:
  - URL references contain the proper scheme (HTTP or HTTPS).
  - URL references containing private IP addresses or private DNS names are changed to the published DNS name of Access Gateway or hosts.

Embedded Service Provider

Access Gateway uses an Embedded Service Provider (ESP) to redirect authentication requests to Identity Server. ESP performs the following tasks:

- Redirects all authentication requests to Identity Server.
- Maintains a cache of the user data fetched from Identity Server.
- Evaluates policies by requesting additional data from Identity Server.

Analytics Dashboard

Analytics Dashboard analyses usage, performance, and events of Access Manager. It captures, filters, and analyzes the events that are generated by Access Gateway and Identity Server. The required events are displayed in the Dashboard.

You can view the analyzed information in the following ways:

- Dynamic graphs on Access Manager Dashboard
- Reports generated in different formats
- Raw auditing records

For information about Analytics Dashboard, see Analytics Dashboard in the NetIQ Access Manager Appliance 24.2 (v5.1) Administration Guide.

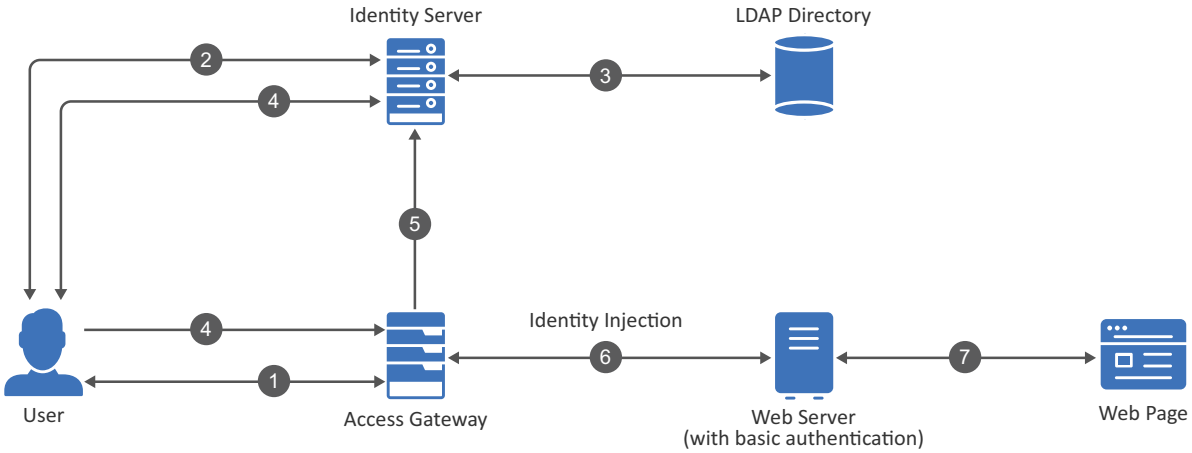
How Access Manager Works

The following are basic sample illustrations of how Access Manager works:

- “Protecting Web Resources” on page 15
- “Providing SSO through Identity Federation” on page 15

Protecting Web Resources

The following diagram illustrates the configuration for protecting resources using Access Gateway:



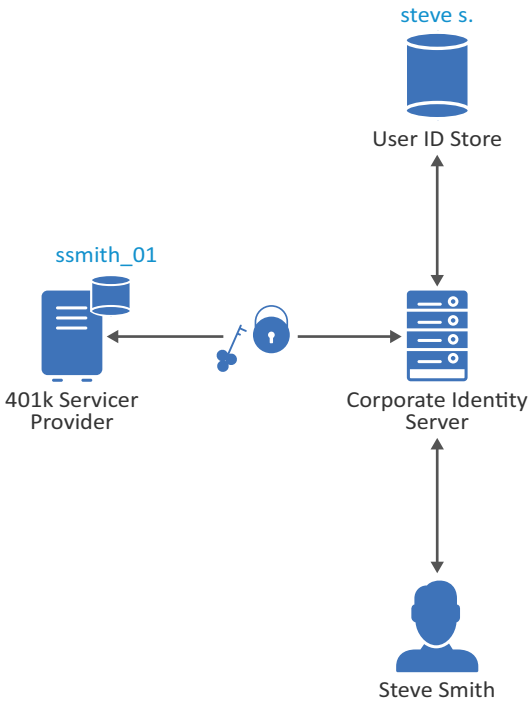
1. A user sends a request to Access Gateway for accessing a protected resource.
2. Access Gateway redirects the user to Identity Server, which prompts the user for credentials (username and password).
3. Identity Server verifies the credentials against the configured LDAP directory user store.
4. Identity Server returns an authentication artifact to Access Gateway through the browser in a query string.
5. Access Gateway retrieves the user's credentials from Identity Server through the SOAP channel in the form of a SOAP message.
6. Access Gateway injects the basic authentication information into the HTTP header.
7. The web server validates the authentication information and returns the requested web page.

Providing SSO through Identity Federation

Let us assume, an employee named Steve is known as steve s. at his corporate Identity Server. He has an account at a 401k service provider called, which has set up a trust relationship with his company. At 401k, he is known as ssmith_01. Figure 1 illustrates this scenario.

401k is configured to trust the authentication from the corporate Identity Server (Access Manager). Steve can enable single sign-on and single logout by federating or linking his two accounts. Steve authenticates to Identity Server (Access Manager) with his corporate username and password.

Figure 1 *Identity Federation*



The process involves the following sequence of actions:

1. Access Manager authenticates Steve against the username steve s. and associated password in the user store.
2. Steve accesses the user portal containing an appmark for the 401k application that he is entitled to use.
3. When Steve clicks the 401k appmark, Access Manager produces an authentication assertion or token for the 401k application (service provider) that contains the identity attributes needed for authentication.
4. The 401k application consumes the assertion or token to establish a security context for the user with Access Manager (identity provider).
5. The 401k application uses the assertion or token to validate that steve s. is ssmith_01 and authorizes the authentication (resource request).
6. The 401k application establishes a session with Steve.

Through this process, Steve entered his user name and password only once for the corporate Identity Server.

Legal Notice