**HRM CODE TUTORIAL COLLECTION**

**Collection By:** R&D Team

Contents

[Content Security Policy 2](#_Toc62813334)

# Active Directory Federation Service

Active Directory Federation Service (ADFS) cho phép Federated Identity và Access Management có thể chia sẽ Digital Identity và Entitlement (quyền lợi) một cách an toàn trải qua (across) Security và Enterprise Boundaries. ADFS mở rộng khả năng sử dụng chức năng Single Sign-on và available trong phạm vi một Single Security hoặc Enterprise Boundary tới Internet-facing Applications để cho phép Customers, Partners, và nâng cao trải nghiệm người dùng trong quá trình sử dụng một Web-based Application của một Organization

## What is ADFS

Active Directory Federation Services (ADFS) là một Single Sign-On (SSO) Solution được tạo ra bởi Microsoft. Nó là một phần của Windows Server OS, cho phép một người dùng đã được chứng thực truy cập tới một Application, việc mà không thực hiện được với Intergrated Windows Authentication (IWA) thông qua Active Directory (AD).

Được phát triển theo định hướng dễ mở rộng, ADFS mang lại cho các tổ chức khả năng quản lý nhân viên Account trong khi đơn giản hóa trải nghiệm người dùng: một nhân viên chỉ cần nhớ duy nhất một Credentials Set để có thể truy cập vào nhiều ứng dụng thông qua SSO.

## How does ADFS work?

ADFS quản lý Authentication thông qua một Proxy Service hosted giữa AD và một Target Application. Nó sử dụng một Federated Trust, liên kết ADFS và Target Application dể cung cấp quyền Access cho người dùng. Việc này cho phép người dùng khả năng đăng nhập vào một Federated Application thông qua SSO mà không cần chứng thực với Application một cách trực tiếp.

Quá trình chứng thực nhìn chung bao gồm 4 bước chính

1. Người dùng đi tới một URL được cung cấp bởi ADFS
2. ADFS Service sau đó chứng thực người dùng thông qua AD Service của Organization
3. Ngay sau khi chứng thực, ADFS Service sẽ cung cấp cho người dùng một Authentication Claim
4. Browser của người dùng sau đó sẽ gửi Claim này tới Application, và Application có thể Grant hoặc Deny Access dựa trên Federated Trust Service được tạo trước đó

## Why do Companies use ADFS

ADFS được tạo ra để phục vụ mục đích vượt qua được Authentication Challenge đượic tạo bởi AD trong một môi trường Online mà số lượng kết nối liên tục tăng. AD và IWA có một giới hạn khi đối diện với quá trình chứng thực hiện đại, và không thể chứng thực người dùng truy cập tới AD Intergrated Application từ bên ngoài. Việc này là một trở ngại trong môi trường làm việc hiện đại, nơi mà User thường xuyên cần truy cập Applications không thuộc quản lý của AD Organization.

ADFS có khả năng xử lý và đơn giản hóa quá trình chứng thực của một Third-party, nhưng việc này cũng đi kèm với những bất lợi và rủi ro của nó.

ADFS giải quyết vấn đề của người dùng có mong muốn truy cập tới AD Integrated Applications khi làm việc từ xa. Cung cấp các giải pháp một cách linh động nơi mà họ có thể chứng thực sử dụng Organization AD Credentials thông qua một Web Interface. Nó cho phép User từ một Organization truy cập một Application của một Organization khác vượt qua giới hạn AD Domain của họ.

## What are the risks and disadvantages?

ADFS có những bất lợi riêng của nó, điều làm nó không trở thành một giải pháp chứng thực thật sự lý tưởng. Những bất lợi đó nằm tại những Hidden Infrastructure và Maintenance Costs, cùng với Security Risks.

# More

ADFS là một giải pháp Single Sign-On của Microsoft cho Web-based Authentication

Nó vốn được sử dụng để cung cấp một Single Set of Credentials có thể sử dụng để truy cập những Site không có chung Domain.

LDAP

Giao tiếp thông qua TCP/UDP tại port 389 (hoặc port 636 cho LDAPS)

Có những Commands dùng cho việc seaching/retrieving/adding/deleting/modifying Users, Profiles và các Directory Entries khác

Không thể được thực hiện trực tiếp thông qua một Web Browser, tuy nhiên HTTP Authentication có thể được biên dịch sang LDAP thông qua kiểu như Apache’s mod\_authnz\_ldap

Khi sử dụng cho một Third-party Website Authentication, yêu cầu username và password được cung cấp bởi Third-party, việc này là không lý tưởng cho vấn đề bảo mật

Có nhiều Open Standard và có một cơ số triển khai trên Linux

ADFS

Được thiết kế cho Web để giao tiếp thông qua Standard HTTPS

Thực thi thông qua một tiến trình an toàn hơn giống với (không hoàn toàn giống) OAuth nơi mà Original username/password được cung cấp trực tiếp tới ADFS Server của Organization (hoặc một proxy, nhưng không phải một third-party), và nếu thông tin cung cấp hợp lệ ADFS Server có thể trả về một Unique Token có thể sử dụng để truy cập tới các Website của Third-party.

Mặc dù nó sử dụng một số Open Standards (HTTPS, SAML, etc…) tuy nhiên nó là của Microsoft và sẽ yêu cầu Internet Information Service (IIS) và chỉ chạy trên Windows Servers.

ADFS hoạt động theo kiểu giống như có một Single Site (Site A) host ADFS/ADFS proxy Server, nó có khả năng truy cập tới Credentials ( thông thường thông qua việc giao tiếp với một Active Directory Domain Controller). Và nó sau đó cung cấp một Trust giữa các Site khác (Sites B, C,… ) được yêu cầu chững thực thông qua ADFS

Khi một người dùng truy cập tới Site B tại Browser, Site B sẽ điều hướng người dùng tới ADFS-proxy Website (Site A) và yêu cầu username, password, thực hiện chứng thực, cuối cùng trả về một bộ Cookies sau đó điều hướng trở lại Site B cùng với một Access Token

Nếu người dùng lại tiếp tục muốn truy cập Site C, họ cũng sẽ được điều hướng tới Site A để thực hiện chứng thực từ ADFS-proxy Website. Nếu Cookies hợp lệ tồn tại (từ lần đăng nhập trước), User sẽ không bị yêu cầu nhập username, password lại mà được chuyển trực tiếp sang site C với một Token

ADFS có thể cấu hình những Claims cụ thể (hoặc Permission) cho người dùng cho mục đích Authorization.

Người dùng có thể mong muốn việc