



RADIANTONE

Federate Identity for Cloud-Based Applications and Provide SSO Across AD Domains & Other Identity Stores

A new, more flexible identity infrastructure is on the horizon. With the growing adoption of federation standards and protocols, such as SAML 2.0, OpenID, and WS-Trust, **both enterprises and end users will benefit from enhanced security, increased privacy, and a better experience.** While these technologies are designed to make it safer and easier to distribute authentication and authorization, they are not designed to go the “last mile” into each separate identity source. **This new system still requires a way to reach into disparate identity stores and unify, route, and authenticate against these scattered, siloed sources.**

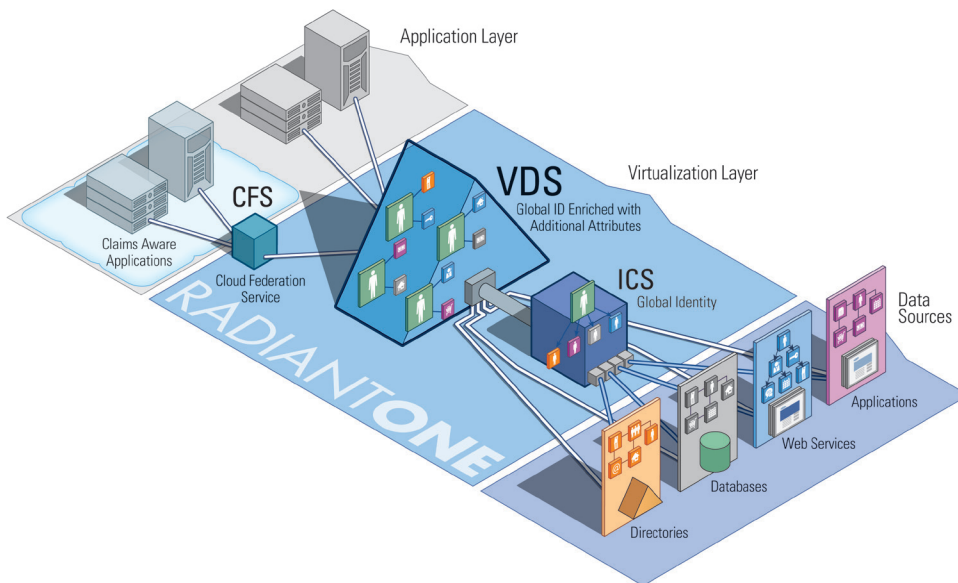
The Last Mile Challenge: Reaching Into Disparate Identity Endpoints

Today's enterprises have many sources of identity, often stored in different formats and enforcing their own specific forms of authentication. Once these identity resources are pooled in a federation or hooked into a cloud infrastructure, **the Identity Provider (IdP, or “IP” in Microsoft nomenclature) very quickly faces the issue of fragmented identification: how to identify users across heterogeneous data sources** and check credentials using different methods, such as passwords, tokens, and certificates. Each IdP needs a way to integrate identity and delegate credential checking to the diverse array of identity silos within the enterprise.

The Virtualization Solution: Integrating Identity Across Heterogeneous Sources

In a federated identity architecture, RadiantOne acts on behalf of the IdP or the Relying Party (RP, or “Federation Provider” in the Microsoft world), identifying and authenticating users and collecting attributes for authorization from an array of directory, database, or web-based applications. If your system has no IdP, **the new Cloud Federation Service (CFS) can step in, packaging the identity data it collects into claims** and sending them to Relying Parties. So users can be authenticated in one place, then receive personalized content and services in other locations—without logging in again or forcing applications to maintain personal information.

RadiantOne Global Architecture



Identity virtualization and identity federation go hand in hand, securely—and seamlessly—joining applications across the cloud. Deliver a single point of access from across a range of heterogeneous sources, for smarter authentication, finer-grained authorization, and customized views of siloed data

RadiantOne in Your Federated Infrastructure

- ▲ **Easier SSO across all sources:** Give applications a single source for identity data—without building customized connections to multiple AD domains/forests, LDAP directories, databases, or applications.
- ▲ **Better user experience:** With federated single sign-on, your users can sign in once, then access applications across the enterprise or on partner sites.
- ▲ **Enhanced security:** Credential checking stays local, so most passwords are not sent over the Internet and synchronization is reduced.
- ▲ **Expanded partnerships:** Extend services to business allies without having to store data about their users—or share data about yours.
- ▲ **Federated forests:** Aggregate across AD forests without managing multiple trust relationships.
- ▲ **Scalable infrastructure:** Enable your IdP to deliver federated identity or use the new CFS as a **complete Identity Provider** out of the box.



RADIANTONE

Traveling the Last Mile Into Endpoints: How RadiantOne Supports Your Identity Provider

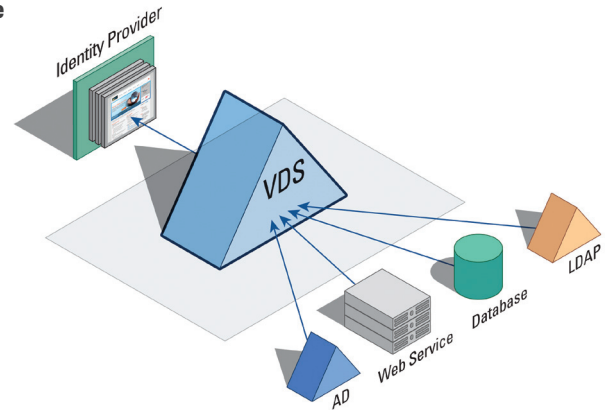
A claim is only as good as the identity data it transmits. RadiantOne's Identity and Context Virtualization suite strengthens claims with information pulled from all the **diverse identity stores within your enterprise**—including multiple Active Directory domains, SQL databases, LDAP directories, and applications accessed by web services.

With advanced data integration capabilities, the RadiantOne platform takes care of identifying users, no matter where—or how—they show up in your enterprise stores. RadiantOne's Virtual Directory Server (VDS) delegates the complicated task of authenticating against all your sources to one common virtual layer, creating **a central authentication service for the Identity Provider.**

VDS can also enhance authorization in the Relying Party by acting as an attribute server, securely gathering attributes from all backend sources. With user profiles enriched with attributes pulled from across your disparate infrastructure, a token can **transfer a 360-degree view of a user's identity and his/her profile to the consuming application**, providing the necessary attributes for enforcing fine-grained authorization policies.

These virtualized authentication and authorization services make VDS an essential tool in any federated infrastructure.

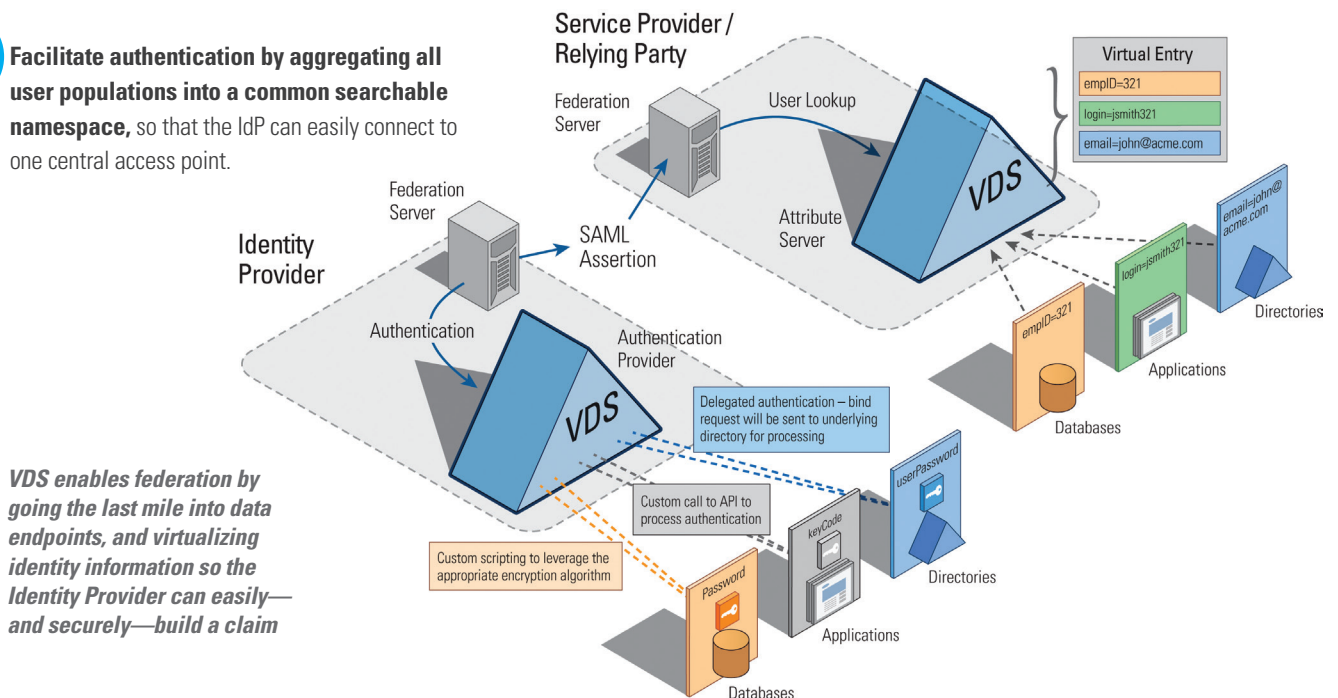
Inside an IdP: Federating Identity



RadiantOne's Virtual Directory Server delivers attributes from disparate identity sources to the identity provider, in a format it can understand

Identity and Context Virtualization at Work in Your Federated Architecture

- Step 1:** Identify your users across a fractured identity infrastructure, no matter how the user is represented, or how many times he or she appears in your sources. The RadiantOne platform can even correlate user accounts without a global identifier, using the Identity Correlation and Synchronization Server.
- Step 2:** Facilitate authentication by aggregating all user populations into a common searchable namespace, so that the IdP can easily connect to one central access point.



VDS enables federation by going the last mile into data endpoints, and virtualizing identity information so the Identity Provider can easily—and securely—build a claim



RADIANTONE

Step 3: Delegate credential checking to backend sources according to whichever method is expected. Credentials are sent to VDS as an LDAP bind, and VDS handles the different authentication mechanisms required by the various backends.

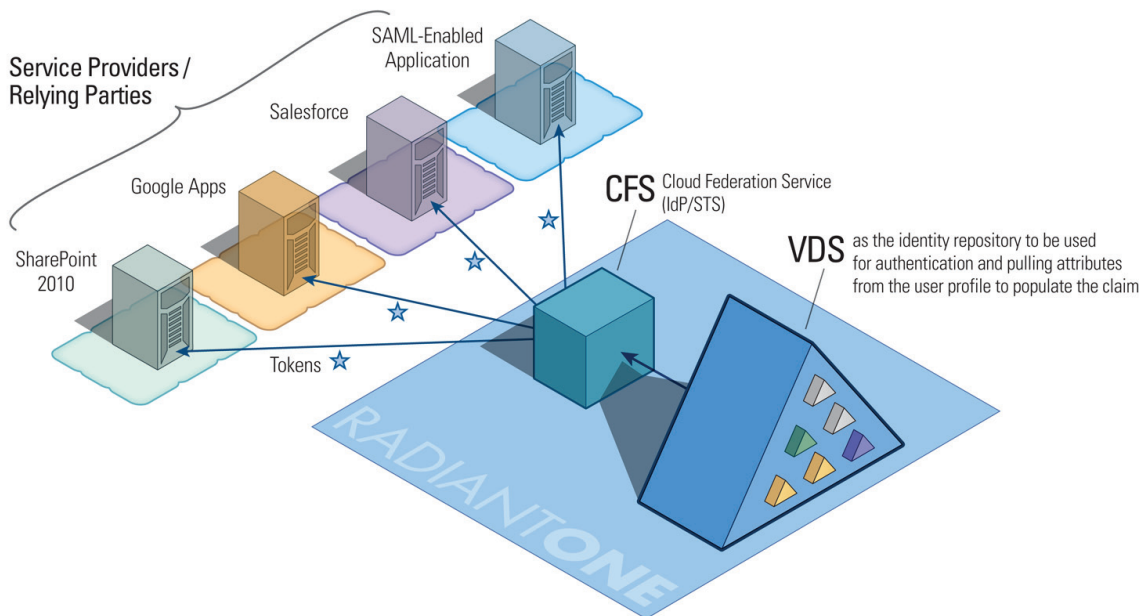
Step 4: Feed finer-grained authorization policies by gathering user attributes from diverse data stores, including LDAP directories, untrusted AD domains, SQL databases, and web services. VDS dynamically pulls in attributes to the virtual layer through “joins” and delivers the required attributes to the IdP or the RP. VDS can also receive queries from an RP and return profiles containing the attributes from all sources in which the user resides.

Step 5: Deliver the requested attributes so they can be packaged into claims. Whether you’re on the Identity Provider or the Relying Party side of the federation architecture, VDS plays a key role in gathering information from all backend sources.

RadiantOne Cloud Federation Service: A Complete “Configure and Forget It” IdP-in-a-Box

A new component within the RadiantOne suite, the **Cloud Federation Service (CFS)** includes both a complete **Identity Provider and Security Token Service (STS)**. Leveraging Windows Identity Foundation, CFS allows you to delegate the complicated task of securely authenticating against all your identity stores to one common virtual layer—shielding your applications from the complexity of your infrastructure.

Cloud Federation Service Acts As an IdP



When used together with the Virtual Directory Server, CFS enables a secure federated infrastructure by supporting claims generation for users residing in various endpoints. The result is stronger security and greater flexibility to transmit identities to external applications on the web. **It connects all the fragmented identities of an organization to the cloud—as a complete IdP, right out of the box.**

The Cloud Federation Service packages authentication results and additional attributes into secure tokens, then sends the encrypted tokens to the appropriate Relying Parties. CFS can securely deliver claims to many of today’s mission-critical applications, including **SharePoint 2010, Salesforce, Google Apps—or any other claims-aware application that supports your essential business operations.**



RADIANTONE

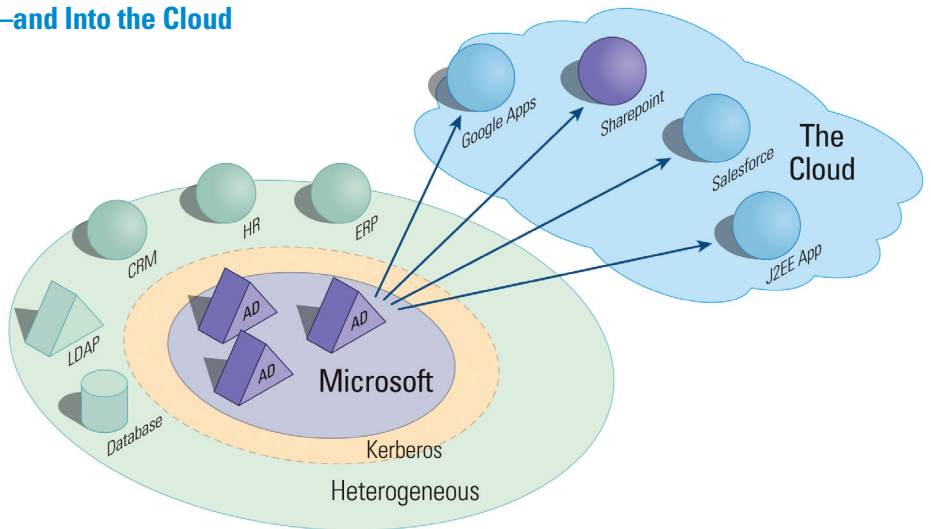
Bridging Identity Islands: Microsoft Meets the Rest of the World

Today's typical enterprise is built around a Microsoft-based internal Windows network, centered on Active Directory. It also has a heterogeneous world beyond Microsoft, such as CRM, Human Resources, or Accounting. Such applications provide services to identities within the Microsoft network, so users are often duplicated across these conflicting domains. And now, with the rise of the cloud, there's yet another realm where identities get siloed.

Getting all these domains to work together—integrating identity and sharing identity resources—is a major IT challenge.

Delivering SSO Across Multiple Forests—and Into the Cloud

Given these infrastructure challenges, there are a number of barriers to achieving single sign-on that gives your constituents access to enterprise and cloud-based applications. To achieve SSO for internal users, an enterprise could establish trust relationships between multiple AD domains, but managing all of those trusts can be difficult. Active Directory Federation Service (ADFS) could also be used to address this issue, but ADFS will only manage your Microsoft identity stores. **Although a critical part of the infrastructure, Microsoft doesn't always integrate well with the rest of the world.** Because many existing applications don't leverage Kerberos, and some customers and other non-employees are stored outside AD, they cannot use Windows Integrated Authentication (WIA)—or benefit from SSO. Such users have to re-enter their credentials every time they want to access SharePoint or other



An internal user's identity data is passed via Kerberos tickets, but the open world—where external users reside—uses SAML tokens. While ADFS translates from Kerberos to SAML, it only supports AD authentication

cloud applications. Now there's a better option: unlike ADFS, which is limited to Microsoft backends, **the Cloud Federation Service connects to any identity source, including AD, LDAP directories, databases, and web services—enabling SSO for all users, both internal and external.**

Making SSO Easier with the New RadiantOne Cloud Federation Service

Radiant's new Cloud Federation Service (CFS) enables users in any AD domain to be authenticated using Windows Integrated Authentication. CFS then translates the Kerberos token from AD into a SAML token and sends it to the appropriate Relying Party, securely enabling SSO to claims-aware applications. **So users can leverage their AD credentials to access non-Microsoft applications**—without the IT team synchronizing AD user accounts into another data source.

How RadiantOne Helps You Get More From Your Microsoft Infrastructure:

- ▲ **Complete solution:** With RadiantOne, you can tap into any identity store—AD, directory, database, or web service—and package that data as secure tokens.
- ▲ **Greater flexibility:** Authenticate users across multiple AD forests to a SharePoint 2007 or 2010 site, using either WIA or forms-based authentication (FBA).
- ▲ **Dynamic groups:** Define groups as you go, for finer-grained authorization policies. Dynamically create groups based on user attributes, not static roles.
- ▲ **Seamless user experience:** Hide the complexity of IdP authentication: users login once and are properly authenticated for enterprise and cloud-based applications, including SharePoint.