RadiantOne Cloud Federation Service

One Hub to Securely Link Cloud Applications with All Authentication Sources, Including Multiple AD Domains and Forests

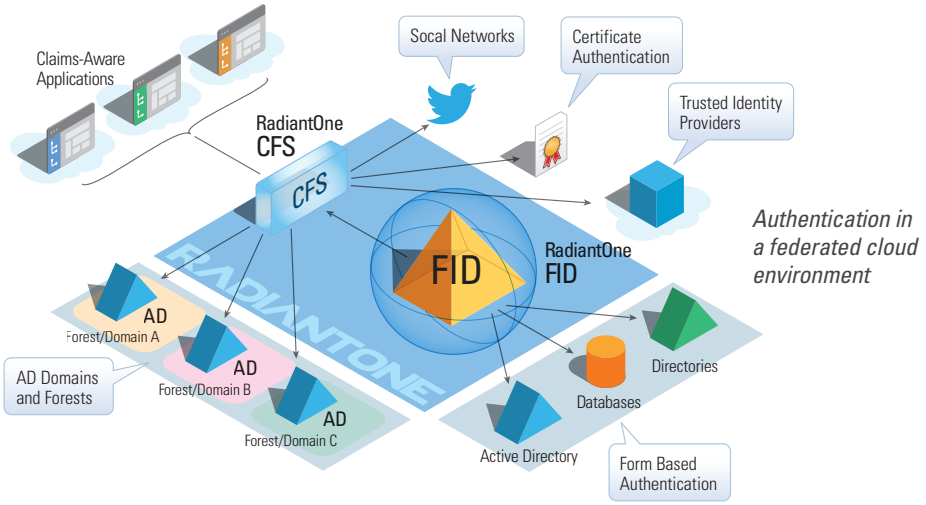
It's tough to secure access to cloud-based applications or federated environments when your identities are scattered across disparate authentication sources, including multiple Active Directory domains and forests, databases, and internal applications. With a variety of protocols, authentication methods, and authorization requirements, it's a challenge to provide security, manage identities, or check credentials, while also offering your users the ease of use that comes from single or simplified sign-on. ***So how do you securely connect multiple internal identity sources and connect authentication systems with a growing set of cloud applications?***

The Identity Provider (IdP) Challenge

The best cloud applications support modern security and authentication protocols such as SAML and WS-Federation/WS-Trust. These applications expect that authentication will be provided by identity providers—in this case, your enterprise or organization. This division of work makes sense for security because it delegates the management of users and credentials to the IdP, so authentication stays closer to the source of the information itself. However, the task becomes more complicated when you're dealing with multiple identity sources, and users are organized in different groups or roles for authorization. In this case, **the identity provider needs to authenticate against a variety of sources**, and gather additional attributes for authorization or services as requested by the cloud application.

The Token Mapping (STS) Challenge

The task of an identity provider doesn't stop with the IdP challenge. Once a user is authenticated, the identification information and other attributes need to be remapped and packaged into a secure token, in a form recognized by the cloud application. Since each cloud application expects certain attributes in a specific format (even if it uses a standard such as SAML 2.0), remapping requirements are different for each application.



The Solution: One Secure Connector to Bridge Your Identities with the Cloud

The RadiantOne Cloud Federation Service (CFS), powered by identity virtualization, is a multi-tenant solution that enables you to access identities across your entire infrastructure, no matter where or how they're stored. Our federated identity and directory service, RadiantOne FID, virtualizes the identity stores, validating the user against a variety of sources—including multiple Active Directory domains and forests, LDAP directories, databases, and web services—then CFS acts as a secure token service (STS), gathering the requested attributes and building an encrypted claim in the form that the application understands. CFS can securely deliver claims to many of today's mission-critical applications, including Office 365, WebEx, Sharepoint, Google apps, Salesforce, and Jive.

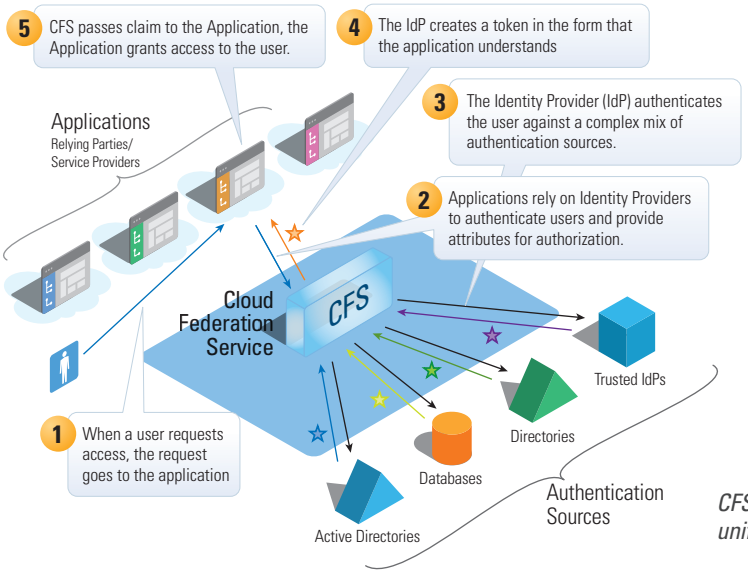
CFS enables a secure federated infrastructure, and creates one access and audit point to connect all your internal identity and authentication sources to the growing world of cloud applications.

Key Capabilities

Link Your Enterprise to the Cloud in a Secure, Logical, and Easy-to-Manage Way

CFS enables better service and stronger security when you need to provide all enterprise users with secure and uniform access to cloud applications.

- **Federated authentication across all sources:** With many different identity sources and authentication methods, delegating login to the right source is a complex task. CFS, combined with RadiantOne FID, provides cloud applications with a single virtual source for identity data, transparently forwarding authentication to each identity source. This provides single sign-on (SSO) to users across different AD domains and forests for multiple cloud applications.
- **Federate users across different domains and forests:** CFS can aggregate across AD forests without managing multiple trust relationships, so integrating Microsoft into the rest of your infrastructure is a breeze.
- **Enhanced security:** Cloud security is a critical concern, both for your users and your business. With RadiantOne, credential checking stays local, and claims are encrypted and sent over SSL, ensuring that private information stays that way. CFS's Level of Assurance (LOA) and Circle of Trust features add more layers of access control, enabling authorization decisions based on the levels you assign to authentication methods and applications, and user authentication locations.
- **Two-form factor authentication:** Administrators can ensure security by enabling two-form factor authentication through CFS. This makes it more difficult for a hacker to access the account with just a stolen password.
- **Simplified management of users and groups:** CFS provides a user-friendly interface, allowing administrators to manage groups and permissions without going through FID. Users can be registered via CFS, and automatically added to FID like any other identity.
- **Simplified audits:** Because authentication is managed in one central place, auditing is easy and security breaches are greatly reduced. A user access log displays all available information from CFS, including user activity and log files, making audit reports a one-step process. All reports can be exported to Excel.
- **Reduced synchronization and password management:** Rather than implement complex synchronization solutions to accommodate new applications and their specific protocol and authentication requirements, RadiantOne allows you to extend identities from your existing identity stores to the cloud.
- **Finer-grained authorization:** A more complete user profile means finer-grained authorization policies. Since CFS comes pre-integrated with RadiantOne FID, you can use claim attributes coming from multiple authentication systems.
- **A more scalable infrastructure:** CFS offers flexible deployments to meet both your current and future needs. You no longer need to add another directory just to authenticate users who are already stored in AD. CFS turns your identity sources into a robust identity provider, delivering complete user profiles based on all your authentication sources.

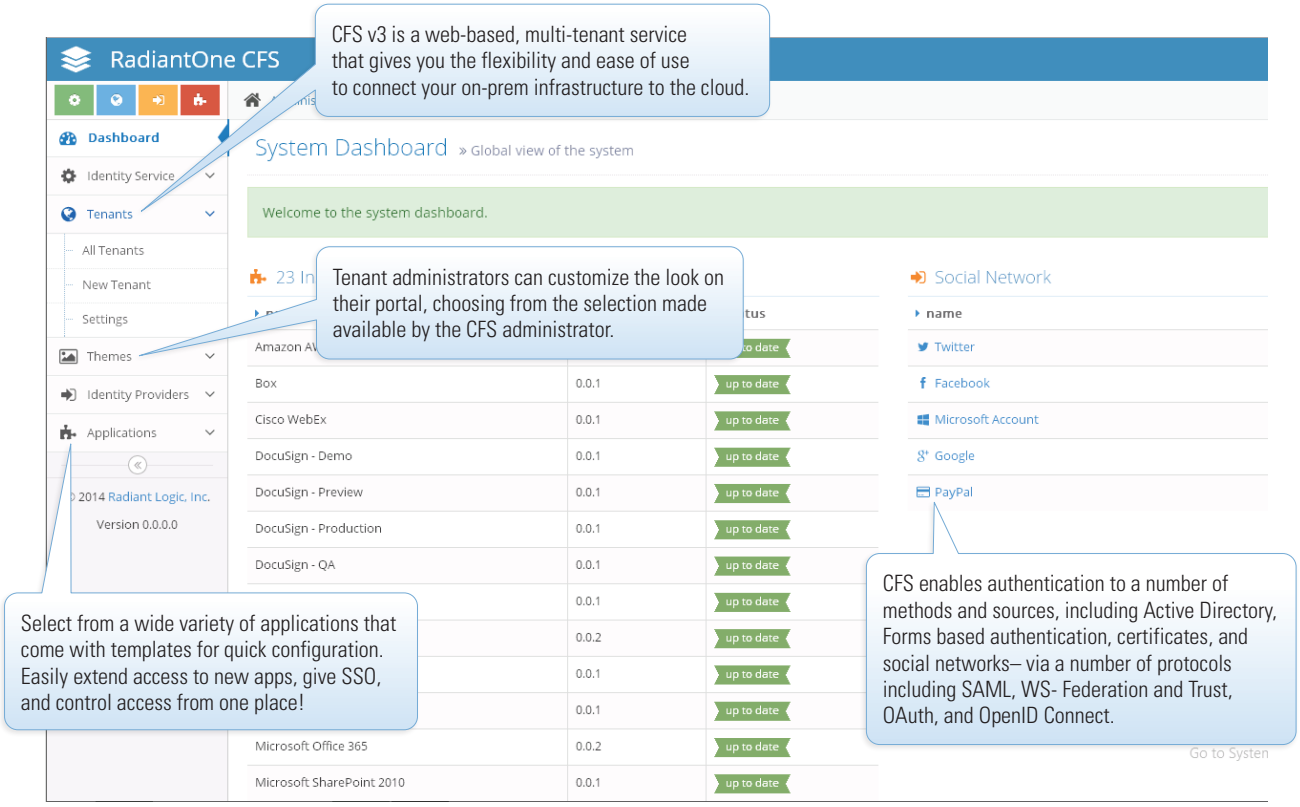


Working in concert with RadiantOne virtual directory technology, the **Cloud Federation Service** acts as an identity provider (IdP) and a secure token service (STS). FID authenticates identities stored in disparate silos, including multiple Active Directories domains and forests, LDAP, databases, and web services.

Because each application expects a different claim, every attribute—no matter where it comes from—must be remapped according to the application's requirements. To meet the varying needs of different applications, RadiantOne CFS builds vendor-specific claims configurations, drawing on attributes pulled by the FID from across the identity infrastructure. The encrypted token is then delivered to the consuming application in a format that application understands.

CFS provides all enterprise users with secure and uniform access to cloud applications

Features



In conjunction with the RadiantOne Federated Identity and Directory Service, CFS turns your entire identity infrastructure into a powerful identity provider.

The RadiantOne Cloud Federation Service:

- Is a **Microsoft-certified** third-party SSO provider.
- Acts as a **complete Security Token Service** (STS).
- Builds claims based on attributes culled from all identity sources, including **AD, LDAP directories, databases, and applications**.
- Is fully **web-based**, so configuration of the system is all done through the web interface.
- Allows authentication from third-party sites such as Twitter, Facebook, Google Apps, Paypal, Microsoft accounts, and more.
- Allows users in any AD domain and forest to be authenticated using Windows Integrated Authentication, so **users can leverage their AD credentials for non-Microsoft applications** and achieve SSO.
- Provides template mappings for cloud applications such as **Google Apps, Salesforce, SharePoint 2010, Jive**, and more!
- Trusts additional external identity providers supporting Windows Azure ACS.
- Supports **multiple authentication systems**, including form-based, certificate, AD domains and forest, and other trusted IdPs.
- Delivers **SSO both inside and outside the firewall**, so users can sign on securely from remote locations and still access all their applications.
- Uses an **LDAP filter** to limit which users have access to each application or can use each authentication system.

Specifications

See the *Hardware Sizing Guide* to get the best performance with RadiantOne.

System Requirements and Platform Support

OPERATING SYSTEM ENVIRONMENTS

- Windows Server 2012
- Windows Server 2012 R2

DISK AND MEMORY

- Memory: 4 GB minimum
- Disk Space: 750 MB
- CPU: Intel Pentium 2.4 GHz or equivalent, 2-4 cores

OTHER MICROSOFT REQUIREMENTS

- IIS 7.5 (or higher)
- .NET Framework 4.6.1
- ASP.NET v4.5
- PowerShell 4.0

Authentication and Identity Sources

DIRECTORY SERVERS

Microsoft Active Directory 2000, 2003 and 2008

Active Directory Lightweight Directory Service (AD-LDS)

Active Directory Application Mode (ADAM)

SunONE Directory Server 4.x, 5.x

Sun Java System Directory v6.x IBM Directory Server 5+

Novell eDirectory v8+

Lotus Notes/Domino

Oracle Internet Directory v9 & v10

CA Directory r12.x

RadiantOne FID

Any LDAP v3 Service

Applications

CFS supports federated applications through the protocols SAML 2, WS-Federation, OAuth 2 and OpenID Connect.

Identity Providers

- Login / Password Authentication (Forms Based Authentication)
- Certificate/PIV card Authentication
- Social Networks
  - Facebook
  - GitHub
  - Google
  - Instagram
  - LinkedIn
  - Microsoft Account
  - PayPal
  - Twitter
  - WordPress
  - Yahoo
- Active Directory (RadiantOne Trust Connectors)
- External Trusted Identity Providers
  - Microsoft AD FS
  - OpenAM
  - RSA SecurID (deprecated)
  - Other Ws-Federation Identity Providers...