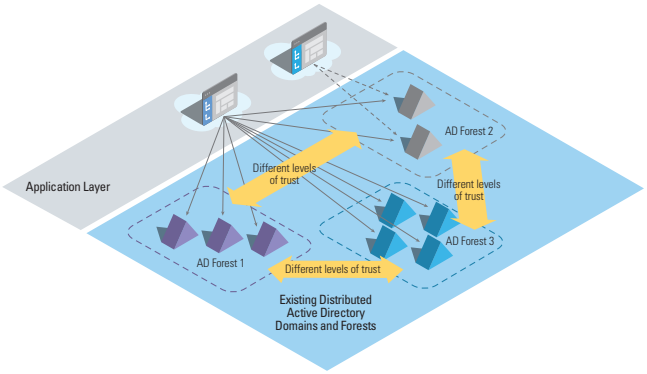
All the Benefits of AD Consolidation—Without Disruption

Enabling Office 365: Securely Connect or Move Your Identity Infrastructure to Azure AD with Our Advanced Identity Integration Layer and Big Data-Driven Directory Storage

In any discussion of identity, Active Directory inevitably plays a major role. While external identities are becoming increasingly desirable targets, the fact remains that for most enterprises, employees remain a central audience—especially in the era of Office 365. For many internal applications, AD should be the authoritative source of all employee data, that single unified list that drives security and access. Unfortunately, achieving this global view of identity is difficult due to fragmentation across multiple domains and forests—and configuring internal applications to chase those different directories is a huge challenge.



For many large and medium enterprises, Active Directory is a fragmented world of multiple domains and forests

Today's enterprises have stretched the use of AD beyond the traditional LAN-based deployments for which it was designed. This growth of domains and forests has left many companies with complex thickets of identity that are difficult to maintain or evolve. The move to the cloud, along with new access demands imposed by mobility, is placing increasing stress on today's complicated AD infrastructures—and this lack of flexibility is slowing IT's ability to support the business, reducing productivity as costs rise.

Consolidating AD: New Requirements for your Identity Infrastructure

Companies are moving toward a consolidated identity and directory model for a diverse array of reasons: to enhance their security model; simplify management; reduce expenses by eliminating high maintenance, support, and licensing costs; ensure compliance in an increasingly complex regulatory environment, and to ease the migration to cloud apps and, in the case of Office 365, cloud directories.

With Microsoft transitioning its Office tools to a SaaS model, it's becoming increasingly imperative for companies to address their messy backends—and for most, that means dealing with an ungovernable proliferation of domains and forests. Microsoft consultants often suggest that companies consolidate domains and forests into one "super domain" but this is a major infrastructure undertaking, involving huge professional services budgets and long timelines measured in years instead of weeks.

Large enterprises deal with many issues when trying to consolidate AD into a single domain, such as rationalizing duplicate accounts and group names, dealing with untrusted AD forests after M&As, and integrating Azure AD Connect across multiple forests. You could use Identity Manager to flatten the existing list of entries, but the need for complex sync logic and connections grows with the number of domains. And Microsoft Azure AD requires a flat list of unique users without duplicates, so many companies require complex correlations to create this unified list.

Even if your company has a long-term goal of AD consolidation, an integration layer like **RadiantOne FID can be quickly deployed to address more immediate goals,** such as provisioning Azure AD and enabling Office 365.

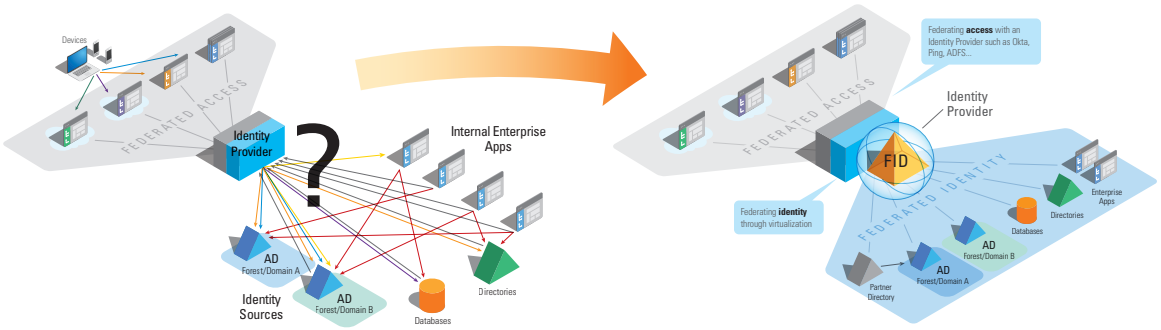
A physical AD consolidation creates many new migration, network organization, and management headaches. Plus, it would be of limited use across many use cases—including Azure AD—since it wouldn't include essential non-AD attribute sources, such as LDAP, SQL, or APIs. For many companies, the effort outweighs the benefit.

So what's the quickest, easiest way to create this normalized list, while streamlining your infrastructure and provisioning SaaS apps and cloud directories?

© Copyright 2019 Radiant Logic, Inc. All rights reserved.

Create a Quick Win: Inject Flexibility into Your Infrastructure with RadiantOne FID

There's a better way to manage your AD infrastructure. A logical "consolidation" based on advanced virtualization saves time and budget while extending and enriching your view of identity with non-AD sources. RadiantOne FID Federated Identity & Directory Service gives you a unique list of users where every user is represented once, as well as complete global profiles drawn from all your identity sources, from AD to LDAP, SQL, and web service APIs.



Fragmentation exists within and beyond your AD infrastructure—so a virtualized "consolidation" offers the needed flexibility to deal with all your domains and forests, as well as all your other attribute sources

Build a Consolidated View by Federating Identity—Not just Centralizing It

Based on advanced virtualization, RadiantOne FID integrates and rationalizes identity, enabling a virtual consolidation of all your identity stores that's cached in a more neutral LDAP directory. With RadiantOne FID, it's easy to:

- **Get the right list of identities and groups** into Office 365 and all your other apps, no matter where they're hosted.
- **Authenticate users to the correct authoritative store** and authorize accessing attributes drawn from your AD infrastructure and beyond.
- **Create a reference image for quickly provisioning SaaS apps**, then feed your identity provider exactly the information it needs to authenticate and authorize users in the cloud.
- **Save time and money** onboarding new apps, integrating M&As, and accessing the cloud.

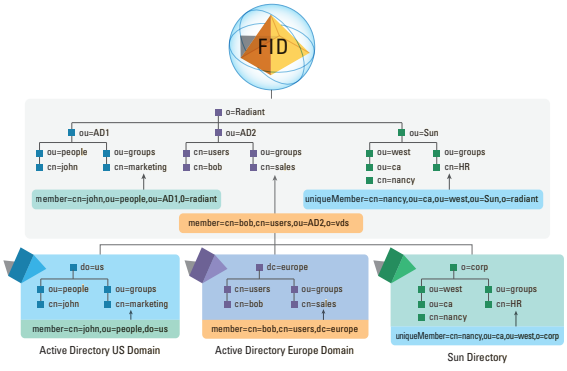
Create a global view of your identity with RadiantOne FID, then sync that ideal ID view to Azure AD using Azure AD Connect.

RadiantOne FID: How It Works

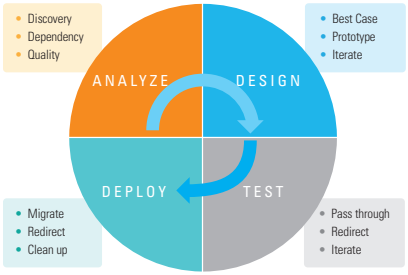
At its foundational level, RadiantOne FID is an identity hub built on a virtualization layer, designed to address the challenges of authentication and authorization. This virtual layer provides an integrated view of identity and is used as the basis for provisioning and synchronizing to the cloud, while HDAP, the Big Data Directory acts as the flexible store for that idealized identity.

1 **Inventory all your existing data sources:** Discover and extract the metadata (including schemas, hierarchies, and data models) from each AD, LDAP, SQL, and API, then map this information to a common naming. Model-driven virtualization enables RadiantOne FID to integrate identity and create multiple views of your infrastructure.

Inventory the identity sources and remap them into a common namespace.



© Copyright 2019 Radiant Logic, Inc. All rights reserved.

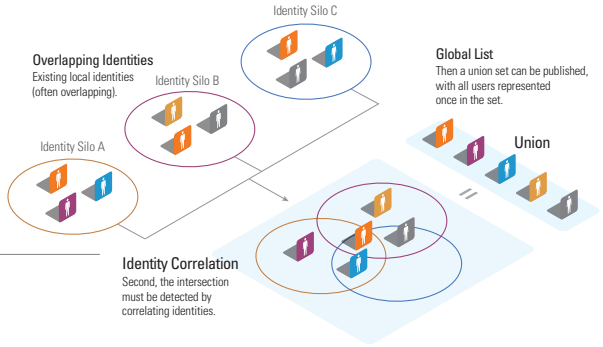


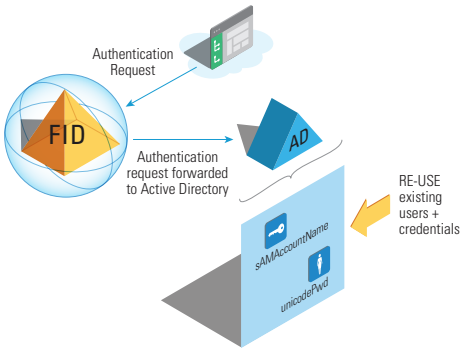
2 Discover the dependencies: RadiantOne makes it easy to inventory and intercept existing client application requests, acting as an abstraction layer between your applications and directory infrastructure, so you can migrate at your own pace, while your authentication and authorization systems keep humming along. This transparent process guarantees that when you migrate to the new directory, there will be no missing objects, attributes, or policies for your existing applications.

Once all the dependencies have been identified, it's easy to remodel the system in a more responsive way that works better for your business, now and in the future

3 Integrate identity to create a global list of users: Create a global unique reference list, where each user from across the identity infrastructure is represented once and only once, using aggregation, simple correlation, or even advanced correlation logic such as cascading matching rules based on complex normalization and soundex algorithms.

Integrate identities across silos



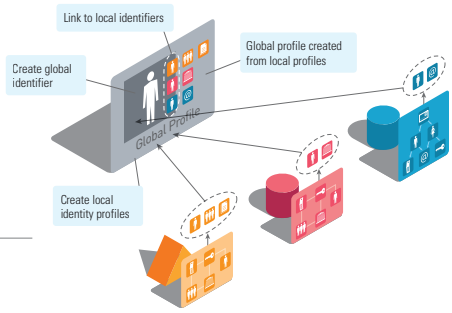


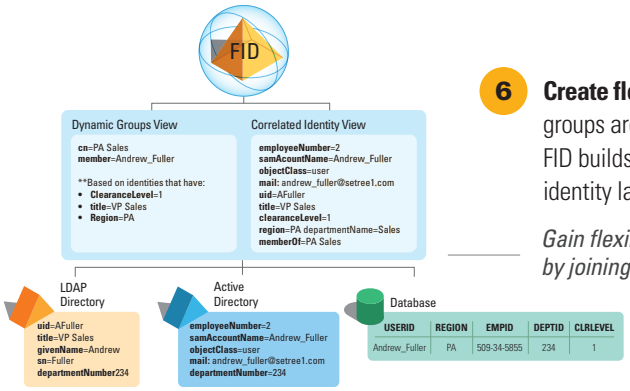
4 Manage diverse credentials checking mechanisms: RadiantOne FID stores this global unique reference list, allowing fast lookups to identify users and retrieve groups and profile information, while still delegating credentials checking to the authoritative backend data sources when needed.

Identify the user in the global list and delegate authentication to the appropriate local store

5 Build global profiles: Manage complex joins across diverse data sources— including AD, LDAP, SQL, and web services—for complete user profiles that applications can use for authorization. These profiles can form the reference image to be provisioned and synced to cloud applications.

Inventory the identity sources and remap them into a common namespace

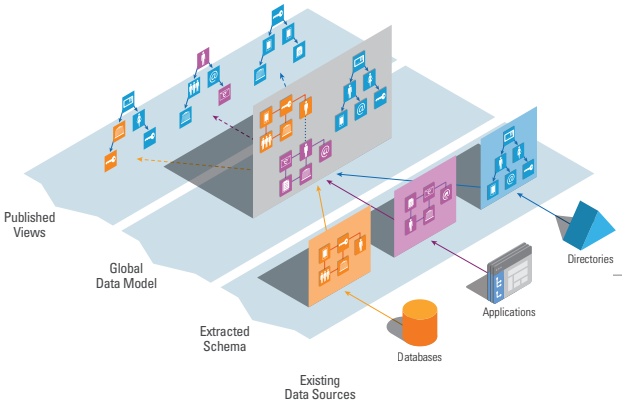




6 Create flexible group definitions: Often, applications use groups to authorize access—but most groups are managed manually, leading to management headaches and security risks. RadiantOne FID builds dynamic, attribute-based groups to enable much more flexible authorization at the identity layer.

Gain flexibility in groups definition by joining user attributes

© Copyright 2019 Radiant Logic, Inc. All rights reserved.

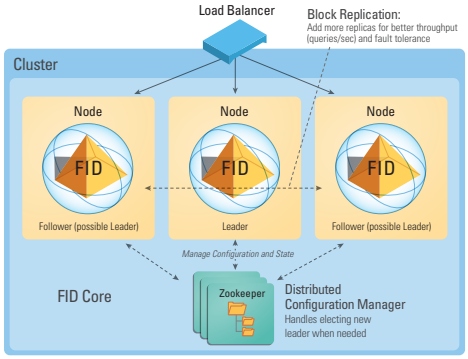


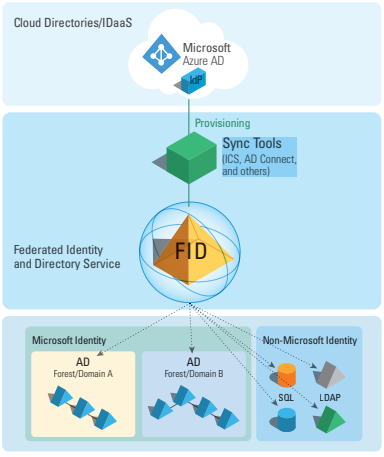
7 **Create custom-tailored virtual views:** Build a flexible namespace to give each application the precise data it needs—in exactly the format it requires. It's easy to extend views to additional backends for faster application onboarding or change views to meet new requirements.

RadiantOne FID uses data modeling to create virtual views

8 **Cache data for speed and scalability:** The materialized view from across all your domains and forests—along with every other attribute source—is stored as a Big Data-driven LDAP directory, allowing you to scale to hundreds of millions of users without sacrificing performance. This store can be cached on-premises or synced directly to Azure AD.

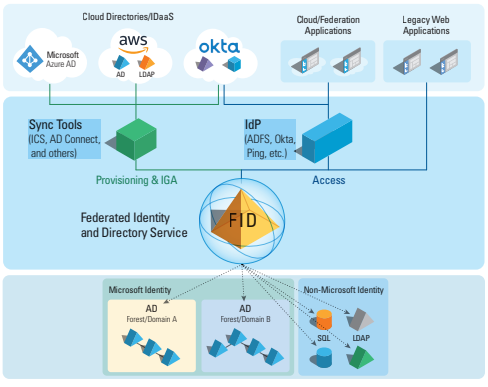
Highly available, highly scalable architecture





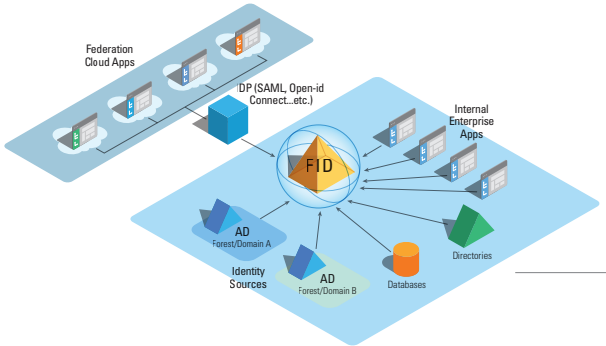
9 **Provision to Azure AD:** With this infinitely-customizable reference image, it's easy to provision cloud applications such as Office 365 with the appropriate user information—and keep this data in sync with authoritative data stores on-premises.

RadiantOne FID provides a reference list to "sync" to cloud apps and authenticate users



10 **Provision Other Cloud Directories, such as AWS:** For enhanced flexibility depending on your business needs, you can also provision Active Directory—as well as all your other attribute stores—to an AD instance or LDAP directory hosted on AWS.

By federating identity with RadiantOne FID, it's easy to provision to AWS or another non-Microsoft cloud directory



11 **Feed your IdP:** This reference image can also be used to provide IdPs with the customized identity information they require to facilitate authentication and authorization for SaaS apps. (You can also feed your IGA tool with the exact version of identity it requires for optimal function.)

The federated identity and directory service acts as an authentication and attribute hub to support the IdP

© Copyright 2019 Radiant Logic, Inc. All rights reserved.

12 **Use RadiantOne FID to achieve other identity goals:** While RadiantOne FID can consolidate your identity to reach Azure AD and enable Office 365, it also adds needed agility to your infrastructure, making it much easier to tackle a world of other identity imperatives, such as: enabling SSO, enhancing authorization & groups management, optimizing WAM/federation, onboarding apps or M&As quickly, ensuring IGA compliance and easier administration, and enhancing customer experience & SSO.

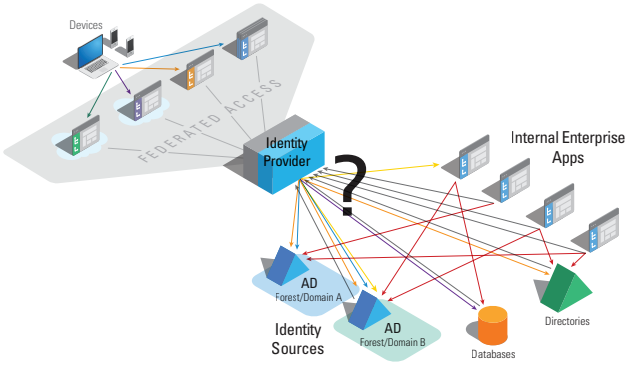
RadiantOne in Action

Insurance Giant Solves the Challenge of "Continuous M&As" While Integrating Seasonal Workers

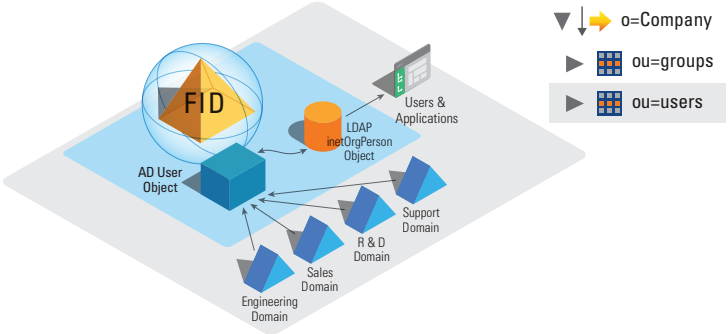
As this sizable insurance provider grew organically **over years of mergers and acquisitions, well-meaning IT administrators allowed the company's AD infrastructure to expand into multiple complex forests**. Following a merger that combined IT departments, this newly formed entity found it increasingly difficult for end users to access their applications, particularly since several lines of business have peak seasons that require seasonal staffing.

For instance, the company offers cellphone hand-set insurance, where insurance claims peak during summer. To meet this increased demand, the company staffs up during this time of year. In the company's digital cable business—which had been part of the other newly-merged company—the high-volume time is during the NFL football season. As each side of the business was hiring and firing during seasonal peaks, they changed to a flex-schedule where these employees just migrated with the seasons—but **the problem was that these are still two different companies on the backend**.

IT initially planned to do an AD migration to get everyone into a single forest, but the opportunity costs were too high. Instead, the team federated its diverse, distributed identity infrastructure with RadiantOne FID, normalizing identity from across all its different data stores and bringing it into a centralized directory. Now the employees from across all the different domains and forests have access to the same applications—starting with WAM and single sign-on and moving on to the targeted applications that are causing its claims organization the most pain. So **the company gets all the benefits of AD consolidation, plus a unified view of identity for cloud applications and web services**.



The company had 13 AD domains in 12 forests, with at least 2 accounts provisioned per employee upon hiring, as well as additional accounts in other domains. LDAP apps were tied to a single LDAP server/domain for logins and access, leading to "duplicate" accounts being provisioned for access to specific applications.



RadiantOne provides a single "view" of all users and groups in all connected AD domains, to simplify administration and improve end user experience by reducing the number of accounts required to access applications.

© Copyright 2019 Radiant Logic, Inc. All rights reserved.