DATASHEET

Authentication Services

The next generation of Active Directory bridge technology

Benefits

- Eliminates complexity by allowing UNIX, Linux and Mac OS X systems to participate as "full citizens" in Active Directory
- Consolidates the administration of AD-enabled systems and AD Bridge
- Delivers strong authentication as part of the AD bridge solution
- Provides centralized authentication and single sign-on
- Facilitates the migration of all systems and users to a single Active Directory-based infrastructure
- Simplifies security and compliance

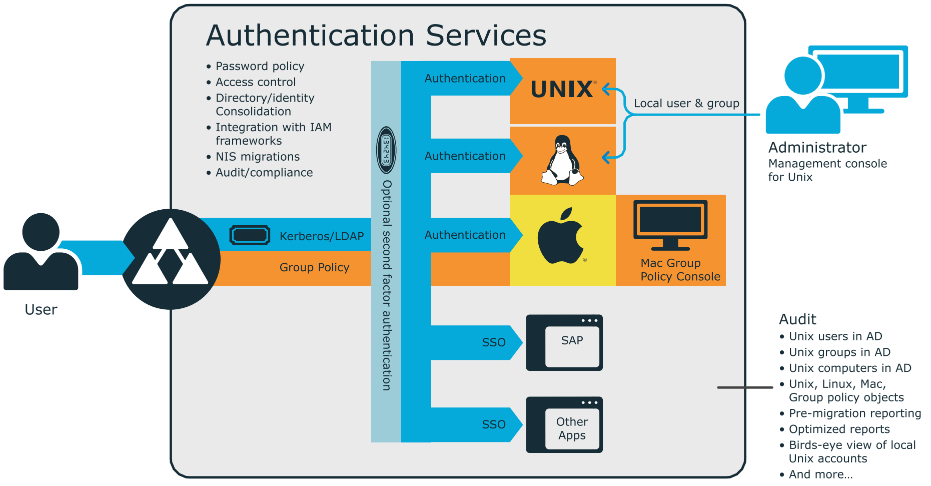
System requirements

For a complete list of system requirements, visit oneidentity.com/Authentication-Services

Authentication Services provides enterprise-wide access, authentication and authorization for UNIX, Linux and Mac OS X systems by using an organization's existing Active Directory (AD) infrastructure. Authentication Services' patented technology allows non-Windows resources to become part of the AD trusted realm, and extends AD's security, compliance and authentication capabilities to UNIX, Linux and Mac OS X.

Authentication Services is the undisputed leader in the Active Directory bridge market with nearly 1,000 customers and more than 5 million deployed licenses. Only Authentication Services provides the functionality, flexibility and scope of integration to meet the needs of the most complex and demanding heterogeneous global organizations.

ONE IDENTITY™



Authentication Services natively implements Kerberos, LDAP and single sign-on for UNIX, Linux and Mac OS X systems in the same way they are implemented in Windows.

Tools for managing your AD bridge

Authentication Services has robust and flexible UNIX utilities, as well as flexible deployment options. It contains a powerful set of tools for creating and managing your AD bridge, including:

- Product configuration and licensing
- Guidance to help with initial setup and integrating systems with AD
- A broad range of migration and deployment options
- Pre-migration assessment and preparation
- NIS migration tools
- Group Policy and local UNIX users and groups management tools
- Simplified and compliant auditing and reporting
- Strong authentication for non-Windows systems

Strong Auntentication

Authentication Services includes licenses for powerful AD-based, one-time password (OTP), strong authentication across all supported UNIX, Linux and Mac OS X platforms. In addition, Authentication Services extends Windows-based smart cards to UNIX and Linux and supports third-party OTP solutions.

Audit, alerting and change tracking

Only Authentication Services gathers the vital data demanded by auditors. Authentication Services enables you to audit, alert and provide a detailed change history of UNIX-centric information managed by Active Directory.

Compliance

Authentication Services uses the same industry standards as AD to provide a compliant alternative to multiple identity stores and points of authentication, as well as non-compliant directories, such as NIS. It also quickly and easily gathers the critical information demanded by auditors, and seamlessly facilitates strong authentication for non-Windows systems.

Migration

Ideally, most heterogeneous organizations want to consolidate into one secure and robust directory for all of their systems. Authentication Services can help you quickly achieve that goal by streamlining the process of integrating UNIX, Linux and Mac OS X systems and users to the AD domain. It also facilitates a fast and accurate migration from multiple authentication mechanisms, identities and directories into a single AD-based infrastructure. Capabilities include:

- Mapped User Mode provides an elegant alternative to a full migration. It allows the migration to proceed at its own pace while quickly resolving the most pressing compliance requirements. Mapped User Mode enables organizations to achieve immediate compliance with no impact on the Active Directory schema.
- UNIX Personality Management creates alternate UNIX "personalities" to define profiles in AD for different systems, using standard schema attributes based on the default AD schema definition.
- Ownership Alignment Tool simplifies the time-consuming final step of resolving user-ID conflicts at the end of a migration.
- It provides a flexible tool set for aligning the ownership of conflicting files; this allows you to quickly realign user namespace conflicts before, during or after your primary migration to AD.
- Full RFC 2307 NIS Map Support provides full support for users migrating their NIS infrastructure into Active Directory's RFC 2307 NIS maps, enabling them to completely retire their existing NIS infrastructure. RFC 2307 is supported with advanced NIS map import wizards, NIS map editors for Windows, and full RFC 2307 support in the Authentication Services NIS proxy.
- UNIX Account Import Wizard imports users and groups to personalities from sources such as NIS, local files or remote shells. It also enables you to choose sophisticated matching criteria (for linking to account principal) from pop-ups. This greatly simplifies the tedious work of migrating users into AD.

Authentication Services natively integrates UNIX, Linux and Mac OS X systems to allow them to act as **full citizens within AD** and benefit from AD’s security and compliance advantages.

Enterprise Group Policy

Authentication Services provides an easily implemented, infinitely scalable, and natively integrated extension of the Windows Rights Management Service Group Policy to UNIX, Linux and Mac OS systems. Through this framework, you can leverage the existing Group Policy extensions built into the product, or develop your own based on the simple ADM template methodology, or the more capable client-side extensions. Authentication Services includes generic scripting, file copying and customization, as well as a collection of powerful prepackaged Group Policies and flexible policy management. In addition, the product leverages existing Windows security policies, making AD entirely authoritative for UNIX, Linux and Mac OS X access control. Authentication Services includes a powerful Group Policy interface for Mac OS X systems that provides control over the entire range of Mac policy and preferences, including support for third-party applications through Preference Manifest integration. Authentication Services also audits and tracks changes to Group Policy Objects.

Active Directory for UNIX, Linux and Mac OS X

Authentication Services seamlessly extends an existing AD infrastructure to the rest of the enterprise. Authentication Services natively integrates UNIX, Linux and Mac OS X systems to allow them to act as full citizens within AD and benefit from AD’s security and compliance advantages. Key capabilities include:

- Extends AD password policy to UNIX, Linux and Mac OS X
- Supports the most complex AD environments including multiple domains, cross-forest trusts, and nested groups
- Leverages AD’s ARC4 strong encryption (128-bit keys) for UNIX, Linux and Mac OS X to enhance security
- Synchronizes UNIX system clocks with AD
- Supports the RFC 2307 schema definition as implemented in Windows Server 2003 (R2)
- Supports custom schema configuration as well as implementation options for pre-R2 schemas without extension.

Centralized authentication and single sign-on

Authentication Services natively implements Kerberos and LDAP on UNIX, Linux and Mac OS X systems in the same way they are implemented in Windows. In addition, it provides single sign-on for many applications (including SAP and Siebel), a powerful application programming interface (API) that allows you to add single sign-on to internally developed applications and guidance for creating single sign-on to a number of popular applications (such as DB2, PuTTY, Samba and Apache).

"One Identity has more than 1,300 customers using its AD bridge product. One particular reference customer has **65,000 UNIX servers** under management, which is five times larger than any of the other AD bridge vendors' largest deployments."

Active Directory Bridge Products: Getting More Value from the Windows Infrastructure

Centralized access control

Authentication Services enables you to configure access rules using several options:

- Local, file-based access lists that determine what users can access on the UNIX and Linux machines (down to the level of the individual services). These can then be centrally managed through Group Policy.
- UNIX Personality Management helps control access by defining the user namespace for a given set of computer hosts.
- Windows security policies and the User Workstation features can provide granular, per-user access control to UNIX computer objects in AD.

Simplified identity management

Authentication Services enables you to simplify identity management based on your existing AD investment. Using Authentication Services, AD-based identity management solutions— including those for provisioning, password management, strong authentication, privileged account management, and auditing and reporting—from and other vendors can be naturally extended to non-Windows systems. Authentication Services can also work with an existing IAM framework to reduce the number of systems that require custom integration and individually managed connectors. Extensive cross-platform support Authentication Services provides centralized authentication support for the widest range of UNIX, Linux and Mac OS X platforms including Solaris, IBM AIX, HP-UX, SuSE, RedHat, Fedora, VMware, and others. For a complete list of supported platforms refer to **www.oneidentity.com/Authentication-Services**

About One Identity

The One Identity family of identity and access management (IAM) solutions, offers IAM for the real world including business-centric, modular and integrated, and future-ready solutions for identity governance, access management, and privileged management.

Learn more at OneIdentity.com

© 2017 Quest Software Inc. ALL RIGHTS RESERVED. Quest, and the Quest logo are trademarks and registered trademarks of Quest Software Inc. in the U.S.A. and other countries. For a complete list of Quest Software trademarks, please visit our website at www.quest.com/legal. All other trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.