SOLUTION BRIEF

# ENSURE ACCESS CONTROL FOR EVERY ENTERPRISE APPLICATION AND USER

## A10 NETWORKS AAM ENFORCES ENTERPRISE-WIDE AUTHENTICATION, AUTHORIZATION AND AUDITING

An identity and access management (IAM) system provides authentication, authorization and auditing for compliance. A10 Networks AAM (Application Access Management) solution can augment an existing IAM solution to help enterprises enforce access control for every application and user. AAM enables enterprises to follow security best practices by offering the appropriate level of access control, logging and auditing for all applications – on-premise or cloud – including web access for every user across an organization.

Most IAM solutions support only a few client login mechanisms, meaning some applications used in an enterprise cannot be brought easily into the IAM domain. This holds true for many popular third-party applications as well as the ones brewed in house.

Such applications may or may not support popular authentication mechanisms including Kerberos, SAML and Multifactor Authentication offered by an IAM solution. The ungoverned or decentralized access to such applications often leaves a backdoor open, increasing the probability of a security breach due to unauthorized access. In addition, due to the decentralized nature, it also becomes difficult to audit user activities and perform an investigation on user actions to track a breach.

### CHALLENGE

How can enterprises enforce authentication and authorization policies to ensure security and regulatory compliance for every application and user? Especially when enterprise applications have multiple authentication points and use different client logon mechanisms.

### SOLUTION

A10 AAM supports an extensive list of client login mechanisms and can work with existing authentication servers seamlessly to help achieve centralized access management and auditing goals by covering every application's authentication needs.

### BENEFITS

- Provides single sign-on (SSO) to unify and consolidate multiple authentication points
- Supports many authentication types, including multifactor authentication (MFA)
- Access control for security, visibility and compliance
- Eases migration to Office 365

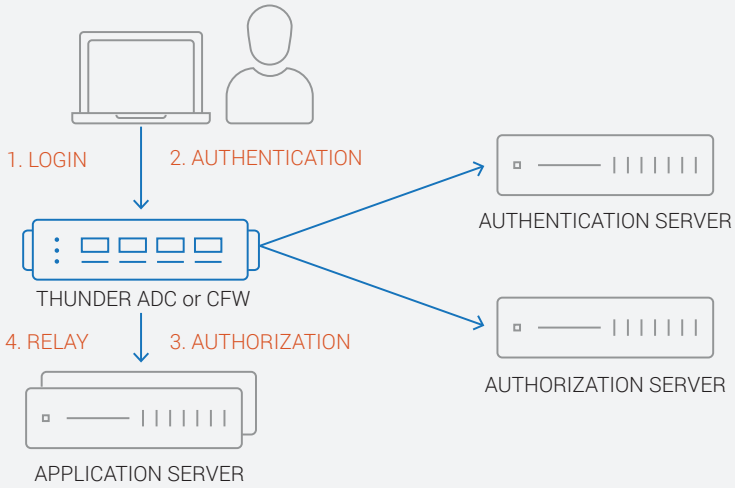


**Figure 1.** A10'S AAM Solution

## *THE CHALLENGE*

The average enterprise user accesses many different applications, often with different credentials, partly due to the applications themselves using disparate authentication mechanisms. With multiple authentication points, access management can become complicated, time-consuming and expensive, while increasing the possibility for overlooked backdoor access, which can potentially lead to a security breach. Lack of adequate access control policies leaves an organization vulnerable to data theft and regulatory violations.

Many enterprise applications do not support different client login mechanisms and most IAM solutions support only a few client login mechanisms. This is a major hindrance to efforts to centralize authentication and authorization.

Additionally, migration from on-premise to the cloud for applications such as Office 365 introduces new challenges when attempting to also move access controls and compliance policies. From staging to production, each phase can take considerable time and effort. A solution that supports both on-premise and cloud application workloads can alleviate this burden.

The right solution must support a broad spectrum of client login mechanisms to guarantee adoption across applications, both on-premise and in the cloud. It must also offer features to ensure regulatory and security compliance.

# A10 APPLICATION AND ACCESS MANAGEMENT

The A10 AAM solution, which is available on A10 Thunder® ADC and Thunder CFW appliances without any additional license, is specifically designed to provide unmatched access control compliance coverage with an extensive list of supported client login mechanisms to meet demanding enterprise requirements.

**Key benefits of A10 AAM solution are:**

- Provides **single sign-on (SSO)** to **unify** and **consolidate** multiple authentication points:

  A10 AAM can help unify access policies and offers a full featured logging capability to consolidate all applications into one, simplified interface. Centralized consolidation of multiple authentication points by augmenting existing identity infrastructure.

  The goal is to bring all applications including the ones left out by existing identity solutions under AAM's domain to eliminate backdoor access and potential data breaches.

With A10's AAM:

1. SSO can be configured by one of many supported methods for applications that do not have a native authentication mechanism.
2. Applications already leveraging an existing IAM solution will continue to work normally by using AAM's authentication relay feature.
3. All applications with different authentication methods, whether already using IAM or not, can be brought under AAM domain.
4. Each application's access policies can be configured and enforced independently.

| *CLIENT LOGIN* | *METHOD (AUTHENTICATION SERVERS)* |
|---|---|
| HTTP Basic | LDAP, RADIUS, NTLM, Kerberos, Token (Active Directory and OpenLDAP) |
| NTLM | NTLM (Active Directory) |
| Kerberos | Kerberos (Active Directory, MIT Kerberos Server) |
| Form | LDAP, RADIUS, NTLM, Kerberos |
| SAML | SAML IdP (ADFS 2.0/3.0, Ping Federate, Shibboleth, OKTA, Sailpoint, CA SiteMinder) |
| 2 Factor Auth | RSA SecurID, Entrust Identity Guard, Duo, Censornet |
| MS SQL TDS | LDAP, RADIUS, NTLM, Kerberos (Active Directory) |
| OCSP | OCSP (MSFT Enterprise CA, OpenSSL) |

**Figure 2.** Some of the supported authentication protocols and servers

- **Access control** for security, visibility and compliance:

  Actions can be allowed or denied, and options for authentication can be enforced for compliance reasons. With each authentication enforcement, user sessions are tracked and further actions by users can also be logged.

  Each policy can be applied to an individual user or group, based on AD attributions, and policies can be enforced for a specific URL and domain by using wildcard constructs.

  Once the access policies are in effect, high-speed logging to syslog, SIEM or Splunk is available for access logs. These logs can be filtered on per rule basis for granular analysis.

  Configuring application access policies is quick and efficient using A10 AppCentric Templates (ACT).

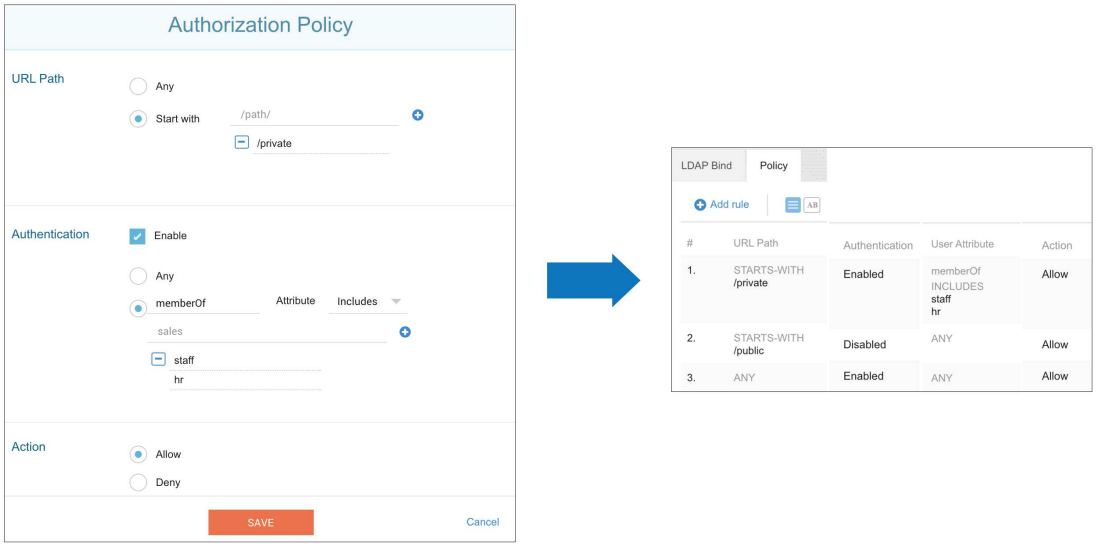


**Figure 3**. Authorization policy construct using ACT

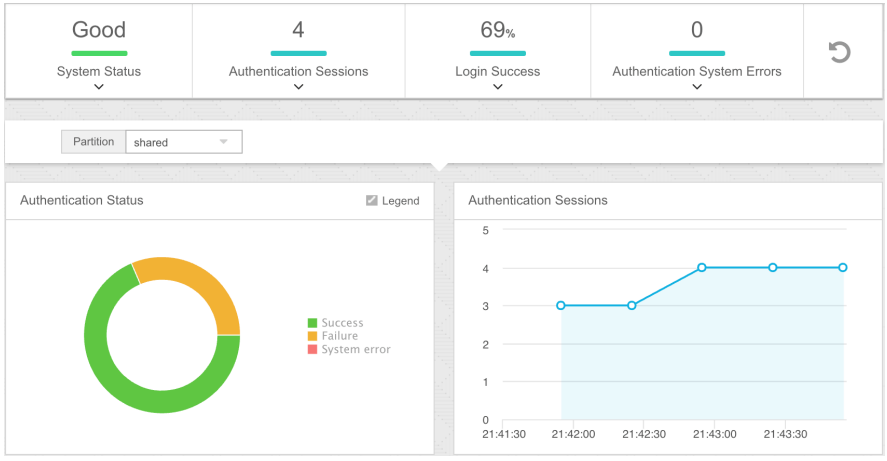


**Figure 4.** Authentication dashboard

- Ease **migration** to **Office 365**:

  Migration to Office 365 is an involving process that takes careful planning and consideration before cutting over from staging to production.

  A10's AAM supports on-premise and cloud Office workloads, which can be a tremendous help in the migration process. With a few simple steps, all on-premise policies and logging configurations can be moved to the cloud instance for enforcement. And on-premise and cloud policies can be active at the same time during the migration, which ensures security and compliance at all times.

  One popular approach for migration is moving users to Office 365 in small chunks based on AD attributes. This eases migration and avoids an enterprise-wide outage if something goes wrong. A10 AAM's ability to directly leverage AD attributes for policy enforcement is extremely useful for such a phased rollout.

## SUMMARY

Today's IAM and IdP solutions cannot cover authentication and authorization needs for every enterprise application, leaving enterprises vulnerable to compliance and security breaches.

A10 AAM is available on A10 Thunder ADC and Thunder CFW appliances. AAM was designed specifically for one purpose: to ensure appropriate compliance coverage for all applications and all users by enforcing access control in a centralized manner. AAM supports both on-premise and cloud workloads, and is highly customizable and flexible, supporting an extensive list of client login methods cover almost every application for every user in any enterprise.

## NEXT STEPS

For more information, please contact your A10 representative and visit: www.a10networks.com.

## ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) is a Secure Application Services™ company, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com
or tweet @a10Networks.

## LEARN MORE

ABOUT A10 NETWORKS

### CONTACT US

a10networks.com/contact



Part Number: A10-SB-19186-EN-01 OCT 2017