F5 White Paper

# Simplifying Single Sign-On with F5 BIG-IP APM and Active Directory

Implementing single sign-on supported by Active Directory to manage application access in multi-domain environments across a diverse set of devices, applications, and services is challenging. An F5 BIG-IP APM and Microsoft Active Directory solution simplifies operational configuration while consolidating identity and application access management.

**by Lori MacVittie**
Senior Technical Marketing Manager

# Contents

# Introduction

In addition to simplifying identity and access management infrastructure, two key benefits of single sign-on (SSO) are increased user productivity and reduced operational costs, realized by fewer authentication-related help desk calls and the elimination of redundant user credential stores. With SSO, users don't have to maintain multi-system credentials or enter them separately for every application, and they have fewer password resets or other access management–related issues. Leveraging a centralized source of authority for access management and authentication reduces the chances for orphaned and duplicate accounts. A unified approach to supporting authentication and authorization for web applications enables organizations to consolidate identity access management infrastructure and realize enhanced security at a reduced operational cost.

Providing SSO across applications deployed on heterogeneous platforms requires standardization on a common identity and access management framework. One such standard is Kerberos, long hailed as the most secure method of providing identity management services across a broad cross-section of applications and systems. Identity management stores often support Kerberos authentication and authorization as a means to enable integration across heterogeneous environments—but this does not always achieve the desired result. An IT organization's efforts to standardize on Microsoft Active Directory and its underlying support of Kerberos-based authentication and authorization will be hindered by their inability to use Active Directory authentication to authorize non-Microsoft applications, clients, and systems. This is increasingly problematic for organizations seeking to deliver on the promise of IT as a Service (ITaaS) by architecting a dynamic data center, as recent years have seen an explosion in the growth of device diversity and most devices do not support Active Directory or Kerberos. The resulting architectures required to implement SSO in such heterogeneous environments are a complex set of interconnections between disparate solutions that are fragile and not easily adapted to support emerging technology and devices such as smart phones and tablets.

Version 11 of F5® BIG-IP® Access Policy Manager™ (APM) enables organizations to implement Kerberos-based single sign-on with Active Directory across heterogeneous applications, while simultaneously providing flexible and highly scalable web access management. The result is a simplified and consolidated architecture that provides the identity and access management services required of a dynamic data center.

# BIG-IP APM Kerberos Support

Support for Kerberos authentication is not new for F5 or its solutions. What is new in BIG-IP v11 is the inclusion of Kerberos authentication in BIG-IP APM, which enables organizations to provide SSO and web access management for an increasingly diverse set of clients, platforms, and applications. The ability to leverage both advanced client authentication and access management, combined with the innate programmability of the core BIG-IP platform through iRules®, makes for a simpler, more flexible, and secure environment that improves user productivity.

BIG-IP APM Kerberos authentication support comprises two new features: Kerberos Single Sign-On and Kerberos End-User Logon.

## Kerberos Single Sign-On

The primary purpose of Kerberos Single Sign-On is to provide seamless authentication to web or application servers once the identity of the user has been established. A user logging in to their Windows desktop, for example, can expect to be transparently authenticated and authorized to any SSO-enabled application using Kerberos. Because users enter their credentials only once rather than for each application, user productivity improves and there are fewer incidents of lost or forgotten credentials that result in costly support calls.

The BIG-IP APM and Active Directory deployment assumes that the underlying infrastructure implements Kerberos, for example using Active Directory Domain Services (AD DS) and Integrated Windows Authentication. AD DS stores directory data such as user credentials, groups, and roles, and manages user login processes, authentication, and directory searches. Integrated Windows Authentication uses Kerberos v5 authentication and NTLM authentication, forcing client browsers to prove knowledge of passwords using cryptographic exchanges rather than passing clear-text passwords. AD DS and Integrated Windows Authentication transparently provide SSO capabilities by interacting seamlessly to exchange the appropriate credentials and tokens to authenticate and authorize user access. For enhanced security and flexibility, an organization may choose to use Kerberos Single Sign-On even if the authentication method involves clear text passwords.

BIG-IP APM acts as a Kerberos proxy by obtaining credentials and authenticating them to the application requested on behalf of the user. BIG-IP APM first derives the user's Kerberos credentials from data obtained by the authentication method. Then, using the appropriate Kerberos protocol extensions—Service for User and

Constrained Delegation—BIG-IP APM uses the extracted credentials to obtain a service ticket to both itself and the application being accessed by the user. Once BIG-IP APM has a service ticket, it inserts the appropriate HTTP Authorization header into the application request and authenticates the user transparently. This process allows non-Microsoft, non-Kerberos-enabled clients, applications, and systems to participate in SSO environments.

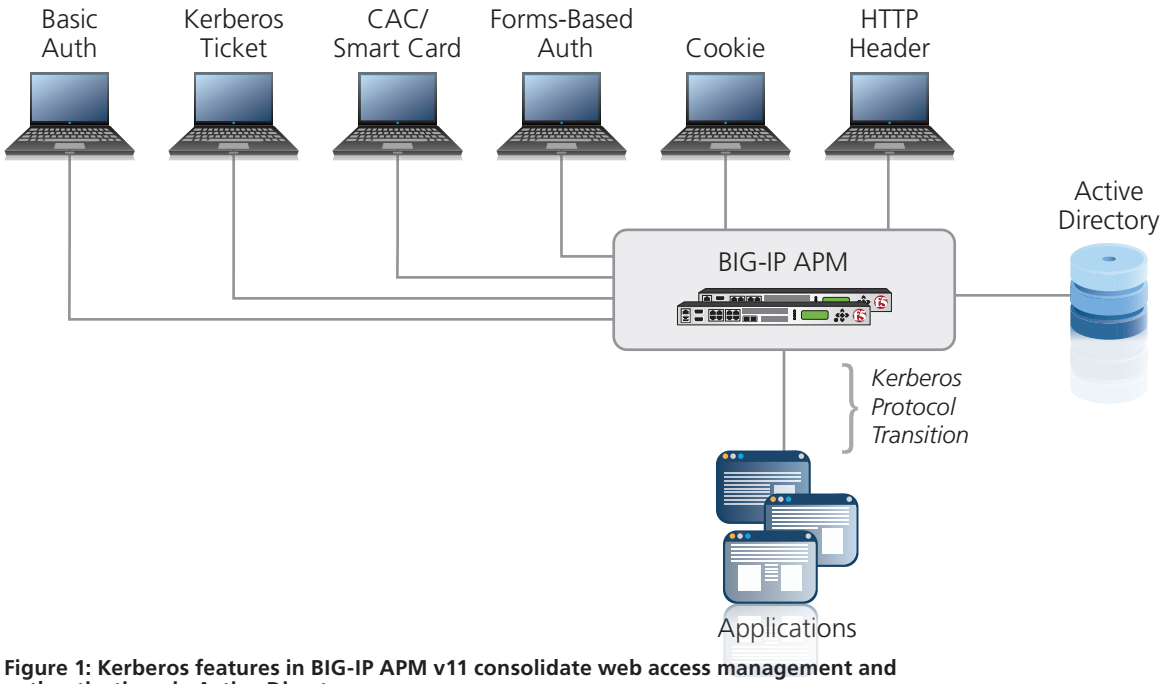


**Figure 1: Kerberos features in BIG-IP APM v11 consolidate web access management and authentication via Active Directory**

BIG-IP APM also supports authentication via client certificates. Where certificates are used, the front end authentication to BIG-IP APM is typically done via OCSP (Online Certificate Status Protocol), which affords BIG-IP APM a more timely view of the revocation status of the presented certificate.

Benefits of Kerberos Single Sign-On in BIG-IP APM include:

- Supports multiple virtual servers and simplifies configuration.
- Makes the design of authentication processes for Active Directory implementations straightforward.
- Reduces operational costs and architectural complexity by eliminating the need for separate web access management solutions.
- Consolidates authentication management via a unified Kerberos Protocol Transition solution, improving security and reducing associated support structure costs.

## Kerberos End-User Logon

People are increasingly using personal devices—tablets, smart phones, and even home computers—to access corporate resources. This requires an increasingly context-aware web access authentication and authorization infrastructure. With the variety of devices comes a vast array of differences in client capabilities for authenticating and subsequently interacting with corporate resources.

In the quest to support all types of devices without significantly increasing operational costs or the complexity of the policies governing access to them, organizations often fall back on the lowest common denominator: an HTTP-based login form. This has been essential for supporting new client types without incurring the cost and delays associated with building new policies; but for internal users who must key in credentials multiple times, it can be detrimental to user productivity. This undermines SSO initiatives and can result in the perception of failure on the part of IT.

Of the 82 percent of American adults who own a cell phone, 8 percent use that phone to conduct work-related business.

Source: "Our Cell Phone Use, By the Numbers," CNN (October 2010)

To address this, BIG-IP APM now supports two alternatives to the traditional HTTP form-based login: Kerberos/SPNEGO or Basic authentication challenge. Supporting these alternatives is particularly beneficial for users who are already authenticated to the local domain, as it avoids forcing an additional request for credentials on the user. With the Kerberos End-User Logon feature, the user can authenticate to BIG-IP APM based on HTTP Basic authentication or Kerberos/SPNEGO authentication.

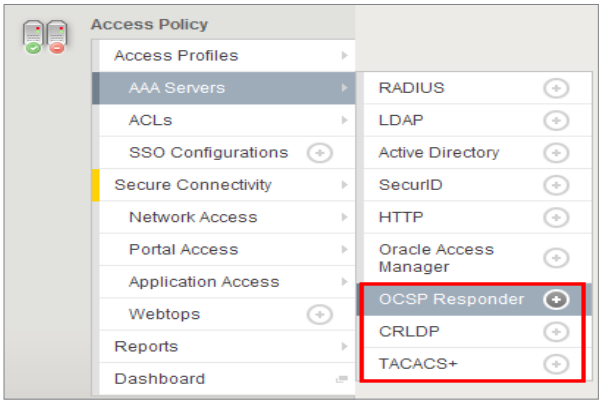


**Figure 2: BIG-IP APM supports a broad set of authentication mechanisms for maximum flexibility in identity access management architecture design**

This allows non-Microsoft, non-Kerberos-enabled clients to take advantage of a unified, Kerberos-enabled SSO infrastructure, providing the appearance to the user of single sign-on from any client with transparent authentication and authorization services.

Kerberos End-User Logon in BIG-IP APM:

- Provides greater flexibility in login mechanisms to better align with organizations' client, application, and operational requirements.
- Eliminates explicit authentication by domain users when attempting to access web application resources via BIG-IP APM.
- Improves organizations' security posture by eliminating the transmission of passwords to BIG-IP APM with Kerberos/SPNEGO authentication.

# Unified Identity and Access Management

The advantage of using Kerberos capabilities in BIG-IP APM to enable a seamless SSO environment is in the ability to simultaneously apply access policy enforcement. BIG-IP APM is a context-aware access policy enforcement platform that provides IT organizations with the flexibility they need to implement and enforce policies that govern access from a wide variety of devices and locations to applications and corporate resources.

By leveraging a unified web access management solution like BIG-IP APM, IT organizations have a centralized location from which to apply context-sensitive access policies, such as restricting access to applications by client, location, or any other available network, client, or resource variable. This enables IT organizations to seamlessly identify users and apply policies at a strategic point of control, never allowing unauthorized users to even attempt to authenticate to the application or resource. This dramatically decreases the effect of access-related attacks, such as brute force and dictionary attacks, that can degrade application performance by unnecessarily consuming resources.

Using BIG-IP APM for both single sign-on and access management enables infrastructure consolidation. Traditional web access management solutions are often stand-alone solutions that require complex integration with identity management systems, such as Active Directory, or that additionally require the deployment of server-side agents. Agent-based solutions are limited in application platform support and introduce yet another point of failure and maintenance that can negatively affect IT efficiency and availability. A single, centralized solution that can provide authentication and authorization support as well as access policy management reduces deployment and management

requirements. It also has the added benefit of eliminating multiple integration points through which requests must be directed, each of which introduces potential performance problems.

# Conclusion

As the number of devices, diverse applications, and services that IT must support continues to expand, so does the need for a simplified identity and access management infrastructure. Leveraging Kerberos to provide a consistent authentication and authorization framework through Microsoft Active Directory for all users, regardless of location or device, results in reduced operational costs and enhanced user productivity.

IT organizations seeking to extend an Active Directory identity management system to devices and applications that do not natively support Kerberos or Microsoft integration face challenges that can be addressed by deploying BIG-IP APM. By providing a strategic point of control at which standardized Kerberos authentication and authorization services can be proxied, BIG-IP APM reduces the complexity of the underlying infrastructure and extends a common identity and access management framework to all users and applications.

By consolidating web application access management and authentication services with BIG-IP APM, organizations can realize a more cohesive, integrated identity and access management infrastructure that remains flexible while also maintaining a highly positive security posture. Simplification remains a key component of success. Simplification of the data center architecture through consolidation of web access and identity management offers reduced costs in terms of administration, licensing, and related hardware deployment costs. This consolidation also provides flexible policy enforcement options, making it easier to adapt to new devices with which users access applications and services. Simplifying the user experience improves user productivity while driving down support costs associated with identity management, such as expensive password reset services.

F5 BIG-IP APM simplifies identity and access management without sacrificing features, functionality, or flexibility.

**F5 Networks, Inc.** 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com


CS01-00050 0511