Enterprise IT organizations face increasing complexity and cost as they seek to offer mobile users easy access to all applications from anywhere on any device. The challenges include:

Application Proliferation Once upon a time remote users could stay productive connecting over a single enterprise VPN to enterprise email and a few centrally hosted applications. Staying productive today often means connecting to scores of legacy, Web, on-premises virtual and cloud/SaaS applications and services.

Device Proliferation Thanks to the proliferation of tablets and smart phones--and Bring Your Own Device (BYOD) and Corporate Owned Personally Enabled (COPE) programs--users now access applications from anywhere on any of a number devices hosting a variety of operating systems, security and compliance postures and mixes of personal and enterprise applications and data.

Authentication Proliferation: There are more authentication mechanisms to choose from than ever before, including NIS, RADIUS, form-based, LDAP, SAML, Diameter and Kerberos. Organizations may deploy any or all of them in any number of combinations, making managing authentication an increasingly complex IT undertaking.

The result? Users often have to remember multiple logins and bookmark multiple URL’s and portals to stay productive, while enterprises find themselves managing a proliferation of point remote access, specialized gateway and identity and access control solutions for different devices and applications. Add the need to vet all those different remote devices, users and authentication mechanisms for compliance with security policies, and the complexity not only consumes IT resources but opens up security gaps, thanks to:

Bad user password habits such as password reuse across applications, weak passwords and passwords stored in email or text files, or on paper.

Inefficient IT processes that allow users to access sensitive applications and information after they leave the organization or switch roles.

Security inconsistencies from managing access by multiple device types, services, vendors, access control mechanisms and support services with different features, architectures, quirks and terminology.

Citrix NetScaler Unified Gateway: Secure User Identity and Achieve Granular Access Control with Federation and Single Sign-On
Improving Application Security with Federated Access and Single Sign-On

For many enterprises, the solution is a centralized single sign-on (SSO) infrastructure that leverages the enterprise directory with federation, multifactor authentication and centralized access control to give users one URL and login to access all their enterprise applications and services—without having to type in another URL or enter credentials a second time. At the same time, it provides IT with a single identity, access control and management infrastructure, closing the inevitable security and management gaps inherent in juggling multiple gateway solutions. Such a solution would offer the best of all worlds, combining enhanced user productivity with IT efficiency, cost effectiveness, security and compliance.

Unfortunately, comprehensive single sign-on solutions have been elusive as applications, device types and authentication mechanisms proliferated. Solutions that could once be considered single sign-on have not kept up as enterprise added cloud solutions and migrated internal applications to the public cloud.

Citrix NetScaler Unified Gateway

The good news is that enterprises can now achieve federation and single sign-on across enterprise, Web, SaaS and on-premises virtual applications and desktops via NetScaler Unified Gateway. NetScaler Unified Gateway leverages its Authentication, Authorization and Auditing (AAA) features with content switching to enable users to access all their authorized enterprise applications through a single gateway and URL. Organizations deploying NetScaler today for their XenApp and Xen Desktop infrastructure can easily expand its functionality for single sign-on across enterprise legacy, Web, virtual and public, private and hybrid cloud applications. Customers using third-party single sign-on and application delivery solutions and gateways can deploy a single solution for all their single sign-on needs by consolidating on NetScaler Unified Gateway.

Citrix NetScaler achieves single sign-on with the following features:

**A customized, branded Web portal and URL** that provides users on a variety of devices with a single point of access to all organization data center and cloud applications, including virtual applications and desktops.

**Unified remote access** Each user gets access only to the resources he is authorized for based on roles and access rights. The user logs in once to access and switch between applications without having to enter credentials again.

**nFactor authentication** with any number, order and priority of authentication factors—including smart cards and digital certificates—with authorization through LDAP, TACACS+ or RADIUS.

**Centralized granular access control policies** for all internal, virtual, web and cloud resources. Consolidation on NetScaler offers consistency for users and reduced risk of security gaps for IT compared to deploying multiple access control engines.
**SAML 2.0 federation**, allowing NetScaler to be deployed as either a SAML Service Provider (SP) or an Identity Provider (IdP), with federated access to cloud services via an enterprise’s internal directory infrastructure. NetScaler SAML works with Microsoft ADFS 2.0 IDP to provide Active-Directory-based user access to Microsoft cloud services such as Office 365 Exchange. NetScaler SP also works with many other SAML 2.0 compliant IdPs such as SecureAuth, IBM Tivoli, Oracle Access Manager, Shibboleth, SiteMinder and SimpleSAMLphp.

NetScaler SAML IdP provides identity federation with multiple cloud services, including Office365, Google Apps, Salesforce, ShareFile and others.

The following use cases demonstrate how IT can leverage NetScaler Unified Gateway to simplify single sign-on to a variety of on premises, migrated and cloud-based applications.

**Use Case: Migrating Users to a Cloud SaaS or ADFS Cloud Application**

Organizations migrating users to a cloud SaaS solution often have to choose between two risky identity options:

1. Migrating the entire working enterprise user directory to the cloud.
2. Maintaining the working user directory on premises but synchronizing it with a read-only mirror directory image in the cloud.

The first option is simply unacceptable to many security sensitive and compliant organizations, as it cedes management and security of the working enterprise directory to the cloud provider and requires user login information to travel outside the organization, often over the public Internet. While the second scenario could be considered less risky, many organizations may be reluctant to open an extra enterprise port for directory synchronization.

Thanks to the NetScaler Unified Gateway, both risky scenarios are no longer necessary. Enterprises can migrate applications to the cloud and continue to authenticate users exclusively to an internal managed enterprise directory. Netscaler accomplishes this through identity federation, using internal SAML or ADFS federation services to provide the cloud service with a secure trusted token containing a series of claims about the authenticated user, including his or her identity, that are in turn validated by the cloud services own federation services.

Federation be accomplished two ways:

1. Organizations can leverage Netscaler’s AAA for Traffic Management (AAA-TM) feature to serve as an ADFS proxy that accepts and forwards cloud requests from remote users to an internal enterprise ADFS server farm and the cloud application provider’s federation service. By acting as an ADFS proxy, rather than simply load balancing a separate ADFS proxy farm, NetScaler reduces the number of components in the Enterprise DMZ. The diagram below shows how user identity and access to cloud services are accomplished in this scenario.

![Diagram showing NetScaler used as ADFS Proxy](figure1.png)

**Figure 1: NetScaler used as ADFS Proxy**
2. NetScaler Unified Gateway can also serve directly as the SAML or ADFS identity provider itself eliminating internal ADFS or SAML proxy and federation servers completely. The architectural diagram for this scenario is below:

![Architectural Diagram](image)

Figure 2: NetScaler Unified Gateway as ADFS Identity Provider

Netscaler can provide federated cloud access via trusted IDaaS providers, such as Azure Active Directory, as well.

In all cases, the user experience remains essentially the same as it was prior to migration, with all AAA and federation occurring almost instantly in the background.

**Use Case: Implementing Single Sign-on Across All Applications**

The NetScaler Unified Gateway can provide SSO to all applications, including Intranet applications, clientless applications such as SharePoint and Outlook Web Access, SaaS applications accessed via ADFS and SAML, virtual XenApp and XenDesktop applications and any preconfigured NetScaler served applications.

IT can provide SSO through a single URL by stepping through the NetScaler Unified Gateway configuration wizard. The wizard walks the administrator through creation of all necessary virtual servers, policies and expressions and applies proper settings based on provided administrator responses. In the process it configures the Unified Gateway primary virtual server, an SSL Server Certificate for the Unified Gateway Virtual Server, a primary and any secondary enterprise authentication mechanisms, a portal theme and optional portal customization, and the means for user single sign-on access to authorized applications via the gateway portal.

![SSO Diagram](image)

Figure 3: NetScaler Unified Gateway provides Single Sign-On across all applications
Summary

Enterprises looking to simplify and reduce the costs and risks associated with user remote access to internal and cloud enterprise applications can achieve their goals via the single sign-on capabilities of NetScaler 11.0’s Unified Gateway. A single NetScaler Unified Gateway solution can replace all existing remote access and AAA gateways, slashing administrative costs and compliance and security risks dramatically.