SAASPASS and NetScaler Unified Gateway

Full-stack identity and remote access through a single URL

SAASPASS combined with NetScaler® Unified Gateway™ provides easy-to-use identity and access management, combining multifactor authentication and single sign-on (SSO) for a broad range of applications and end-point devices.
In an increasingly challenging global security environment, organizations need to protect their applications, data and intellectual property against diverse risks. Professional hackers, cyberterrorism, targeted malware, ransomware, and high-profile security breaches have all become commonplace. Unfortunately, even a single security failure can result in very real strategic, reputational, and financial losses.

Traditional username and password security measures are no longer sufficient, no matter the complexity of the passwords, or how often they are changed. In fact, up to 86% of all hacks are related to usernames and passwords (Verizon 2017 Data Breach Investigation Report). As a result, multi-factor authentication is now increasingly required to verify user identity across a host of devices.

**SAASPASS and NetScaler Unified Gateway**

The near-universal move to cloud-based applications and software as a service (SaaS) has vastly complicated security challenges. In simpler times, traditional virtual private networks (VPNs) offered secure remote access to local or on-premise information and traditional client-server applications—typically for a small or restricted group of users (e.g., salespeople). Now, organizations must provide fine-granularity secure access for everyone—employees, partners, and customers.

To be effective, authentication solutions must be comprehensive, and must support the full range of applications, including on-premise applications, legacy enterprise applications, virtual desktops, newer SaaS applications, and cloud applications. Moreover, to remain productive, users need to be able to authenticate quickly and easily—on any device, from anywhere—while retaining secure access to their own personal applications and data.

The combination of SAASPASS full-stack identity management and access with Citrix NetScaler Application Delivery Controller (ADC) provides security and compliance beyond the corporate network to users that access Citrix virtual workspaces as well as other applications. NetScaler Unified Gateway eliminates the need for users to remember and login to multiple URLs using different credentials by offering a single URL for access to all enterprise resources with secure single sign-on (SSO) access. Combined with NetScaler Unified Gateway, SAASPASS provides easy-to-use two-factor authentication, simplifying security for both administrators and users.
Context-aware security and multi-factor authentication through a single URL

Organizations need to provide efficient, effective, and secure access to applications and data, regardless of endpoint. The modern decentralized application architecture means that users have to remember multiple credentials and login to various URL, leading to both user and administrative complexity. Beyond user names and passwords, administrators need to validate identity with substantially more context, and provide fine-granularity access to exactly the applications and data required. At the same time, administrators need to avoid creating a complex patchwork of different access methods and VPNs that can expose their own security vulnerabilities.

Organizations are often faced with stitching together two or more point solutions for multi-factor authentication, single sign-on, endpoint access, password management, and even physical control access. This leaves users to grapple with a less productive environment and causes administrative headaches, complexity, and security vulnerabilities. For example, many users leaving an organization typically retain access to on-line corporate assets—simply because of administrative complexity.

Single sign-on access to all applications

As shown in Figure 1, the combination of NetScaler Unified Gateway and SAASPASS provides multi-factor authentication and SSO to a wide range of applications from any device. Applications can be deployed in a datacenter, in the cloud, or delivered as SaaS and can include:

- Web applications (Sharepoint, internal employee portals, etc.)
- Traditional client/server or enterprise applications (e.g., Microsoft Outlook).
- Virtual desktop infrastructure (VDI) including XenApp, XenDesktop, Microsoft RDP, and VMware Horizon.
- SaaS applications (Office 365, Salesforce, Workday, etc.)
- Mobile applications on most any device.

Figure 1. SAASPASS and NetScaler Unified Gateway provide multifactor authentication and SSO to diverse application types, independent of user location and endpoint device.
SAML based federated identity and on-premise user directory

To achieve SSO to cloud-based applications, many solutions require that organizations move their user directory to the cloud, which is high-risk for any enterprise. Instead, NetScaler Unified Gateway provides identity federation using Security Assertion Markup Language (SAML) or Active Directory Federation Services (ADFS). This capability lets enterprises migrate applications to the cloud while continuing to authenticate users against an on-premise enterprise directory. SAML also provides critical integration between SAASPASS and NetScaler.

Easy SAASPASS multi-factor authentication

As a part of the solution, SAASPASS provides easy two-factor authentication, while NetScaler Unified Gateway integrates with and supports all authentication mechanisms and protocols. SAASPASS includes a flexible policy-based authentication framework that supports dynamic policies. The single access URL offered by NetScaler also helps simplify the user experience. The result is multifactor authentication and SSO to hundreds of enterprise applications.

Comprehensive VPN-based remote access

As application technologies have evolved, traditional single-purpose VPNs have become insufficient. The SAASPASS and Citrix solution includes:

• A fully configurable and customizable portal for publishing applications
• Support for all end-user devices
• Support for all authentication mechanisms
• Support for all SSO protocols

Seamless NetScaler and SAASPASS integration

Authentication is the very essence of security. Before access is provided to critical applications or data, security protocols must identify the user and whether they really are who they say they are. Figure 2 illustrates how SAASPASS utilizes SAML integration to work with NetScaler Unified Gateway to provide out-of-band multifactor authentication using a smart device.

![Figure 2. SAASPASS works with NetScaler Universal Gateway via SAML 2.0 integration, offering out-of-band multifactor authentication.](image-url)
Authentication steps are keyed to the illustration:

A. The user first accesses the NetScaler portal and requests authentication.
B. The portal sends a SAML assertion to SAASPASS.
C. The user is then sent to a login page where the user scans a QR code with a smart device.
D. A SAML token is then sent to NetScaler.
E. The user is then logged in to the resource server.

NetScaler Unified Gateway for effective single sign-on
NetScaler Unified Gateway provides SSO to applications in the data center, cloud, or delivered as SaaS. It consolidates remote access infrastructure allowing users to access any app from any device, securely. Consolidation on NetScaler offers consistency for users and reduced risk of security gaps for IT, compared to deploying multiple access control engines. Features include:

- **A customized, branded Web portal.** A custom portal provides a single URL offering users on a variety of devices with a single point of access to all relevant data center and cloud applications, including virtual applications and desktops.
- **Unified remote access.** Each user gets access only to the resources he or she 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.** Authentication can be performed 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.** Policies can be specified for all internal, virtual, web and cloud resources, allowing considerable flexibility and customization.

SAASPASS for simple out-of-band multifactor authentication
SAASPASS is the only comprehensive full-stack identity and access management solution on the market. It protects access to remote or cloud-based resources with five-minute integration for most enterprise cloud services. SAASPASS provides:

- **Managed and compliant security services.** SAASPASS helps companies meet GDPR, DFARS NIST 800-171, HIPAA and other security compliance requirements.
- **Support for all devices.** SAASPASS supports all endpoints with no additional device to carry. It secures Macs and PCs, supports any smart device, and provides both online and offline authentication methods.
- **Wide-ranging integration options.** SAASPASS can be easily extended to protect any application, physical location, or login.
- **Multiple instant login modalities.** A number of login modalities are supported, including proximity login, scan login, push login, on-device login, and remote login.
- **Unique security features.** SAASPASS features no-PIN storage, multidevice support, and a modular design to help thwart zero-day attacks.
Conclusion
Applications are evolving rapidly, and so are the threats to both corporate and personal security. SAASPASS combined with NetScaler lets you move quickly to secure critical applications and data whether on-premise, in the cloud, or delivered as SaaS. Sophisticated yet simple single sign-on from NetScaler combined with multi-factor authentication from SAASPASS makes it easy to rapidly on-board and off-board users, integrate applications, and secure more of vital corporate resources. The combination greatly simplifies management, securing user identities while actually improving the user experience.