Benefits of Two-Factor Authentication with Citrix NetScaler

CITRIX READY

SMSPassword | CITRIX

The world is becoming increasingly mobile. Not so long ago, a workplace referred to a physical location. But with the increased mobility that technology has enabled, boundaries are blurring. A workplace is less a place and more a concept. It is a technological leap that offers great opportunities and conveniences for employees and employers alike.

But the world is also becoming increasingly dangerous. Incidents of cybercrime are escalating at unprecedented rates. The need for remote access to systems, networks and data has never been greater, and each user granted remote access becomes a new target of opportunity for criminals.

Many companies still rely upon the ancient defensive methodology of password protection. But password defenses are all too easy to breach — 73 percent of the population reuses passwords, according to TeleSign, vastly diminishing their effectiveness.[1] Accordingly, password protection is a flawed methodology that, in many cases, does little more than momentarily slow a cybercriminal's greedy grab for proprietary data and system access.

Two-factor authentication provides a much more robust defense than a simple query-password system. This paper describes SMSPassword's industry-leading two-factor system and discusses how two-factor authentication can make all the difference in foiling today's technologically savvy cybercriminals. Also described is the effectiveness of teaming Citrix NetScaler with SMSPassword's two-factor solution to meet the growing need for a remote access security solution for enterprises worldwide.

Business Challenge Summary

123456. That simple string of consecutive digits holds a dubious distinction. According to *Computerworld*, it was the most used password on the planet in 2015. It would be hard to imagine a more flimsy password, but the word "password" would come close. And indeed, "password" was the second most used password in 2015. Many users, however, decided to beef up their defense against hackers by making the most used password far more difficult to guess. They added a couple of digits to create the third most used password in 2015: 12345678.[2]

It is a good time to be a hacker.

[1] https://www.telesign.com/resources/press-releases/report-70-percent-of-consumers-are-losing-faith-in-passwords-want-additional-account-security

[2] http://www.computerworld.com/article/3024404/security/worst-most-common-passwords-for-the-last-5-years.html

The use of a password-query system to protect valuables is an ancient concept. Passwords have been used to protect data and systems access since the dawn of the information age. The very first shared system, MIT's Compatible Time-Sharing System (CTSS), was password protected in the early 1960s. Ironically — but not coincidentally — the CTSS may also have been the very first computer system to be hacked, according to *Wired Magazine*.

Though one-factor authentication vehicles such as passwords and PINs have comprised a primary bulwark of computer system security for decades, the faults of one-factor authentication are becoming better known — and more costly. According to the *Verizon 2016 Data Breach Investigations Report*, "63 percent of confirmed data breaches involved weak, default or stolen passwords." [3]

One-factor authentication solutions such as password protection obviously do not successfully protect everything. And it is becoming more and more correct to state that one-factor authentication solutions do not successfully protect anything. Cybercriminals are constantly upping their game and devising inventive ways to foil one-factor solutions — for example, keylogging malware for snaring passwords from unsuspecting users or hijacking data from point-of-sale devices.

The burgeoning threat of phishing attacks continues to result in the widespread theft of user credentials. According to the *Verizon 2016 Data Breach Investigations Report*, approximately one out of every seven users will click on an email attachment during a phishing attack — and with very little hesitation. It's no surprise, then, that cybercriminals are placing serious focus upon phishing methodologies. Verizon's report revealed that in 2015, the perpetrators behind fully 89 percent of all phishing attacks were organized crime syndicates.

Various forms of malware, such as ransomware, spyware and others, are also escalating, both in the total number of attacks and in the success rate. Verizon's report reveals that ransomware made the largest leap in reported malware occurrences in 2015.

Two-factor authentication solutions have certainly provided a more effective defense against the many and varied modern security threats. But many commonly deployed two-factor authentication solutions, such producing a hardware token in addition to providing a password, have likely frustrated users more than they've foiled cybercriminals. The inherent inconveniences of some two-factor methodologies — often clunky and slow — tend to send user frustration rates soaring and adoption rates plummeting.

The need for a two-factor authentication solution that can foil cybercriminals without frustrating users has never been more obvious or urgent — particularly in conjunction with the growing trend toward remote accessibility. Accordingly, more and more organizations are seeking a two-factor authentication methodology that combines effective security with usability and affordability.

CITRIX® Receiver

[3] http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Top Three Features to Consider in a Two-Factor Authentication Solution

Maximizing the potential of two-factor authentication requires the installation of a system that delivers a full range of key capability and usability features. The following, in particular, should be considered must-have features for two-factor solutions undergoing evaluation for deployment in any organization:

CITRIX® NetScaler

1. **Integration with Citrix NetScaler and Active Directory:** Organizations considering the selection and implementation of a two-factor solution must certainly evaluate the ease of integration of the solution with software components already in place. At the vast majority of organizations, there are two key pieces of software with which the selected two-factor solution must smoothly interface.

   Citrix NetScaler is an Application Delivery Controller (ADC). NetScaler's superiority over competing ADCs — NetScaler offers up to five times the performance of the closest competitor, according to Citrix — makes it the first choice for most organizations. Microsoft Active Directory is incorporated in most Windows Server operating systems. Therefore it is essential for most organizations that any two-factor solution under consideration offers easy integration with both of these widely deployed software tools.

2. **Cost Effectiveness:** This is the bottom line when evaluating any new tool. That certainly applies to two-factor authentication solutions. While available two-factor solutions represent a wide range of upfront costs, it's also important to evaluate long-term, ongoing costs. Some solutions, for example, require an annual license renewal fee which can substantially inflate total cost of ownership (TCO) over the effective lifetime of the solution. Vendors that charge according to SMS volume can also sometimes inflate usage costs; look for solutions that provide unlimited SMS at no extra charge.

3. **On-Site Solution:** For most organizations, the ability to exercise complete control over any two-factor solution is a desirable benefit. But not all two-factor solutions offer complete on-site capability. Many require that a certain amount of control be relinquished to off-site third parties — the off-site generation of passwords, for example — which can introduce a potential point of weakness that may be exploited by cybercriminals. SMSPassword provides organizations with the flexibility to choose how and where SMS messages are dispatched: third-party or internally with organization-owned modem or SIM card.

Citrix Ready Secure Remote Access Program Overview

Citrix solutions deliver a complete portfolio of products supporting secure access of apps and data anytime, at any place, on any device and on any network. These include:

CITRIX® XenApp

1. XenApp and XenDesktop to manage apps and desktops centrally inside the data center

2. XenMobile to secure mobile applications and devices while providing a great user experience

CITRIX®
XenMobile

3. ShareFile to provide controlled and audited data access, storage and sharing, both on-premise and in the cloud

4. NetScaler to contextualize and control connectivity with end-to-end system and user visibility

Citrix solutions also integrate with third-party security products to provide advanced levels of system management and identity, endpoint and network protection. The Citrix Ready Secure Remote Access program was launched to identify and showcase partner products that are proven to smoothly integrate with Citrix products, and that work to enhance Secure Remote Access by adding extra layers of security. The Citrix Ready Secure Remote Access program serves as an aid to IT executives in quickly and easily finding and sourcing solutions for their Secure Remote Access needs, helping to secure organizations' corporate networks from theft of data, DDoS and other security attacks that may be perpetuated via Remote Access.

Citrix advises that organizations can best defend against Remote Access security attacks by following five best practices — pillars of focus that support enterprise security:

1. **Identity and Access:** Administrators must be able to identify users requesting access to a system and limit the degree of access granted. In comparison to simple password-based systems, two-factor authentication offers a vast improvement in the ability to properly identify requests for access. The degree of access granted to each individual user should be based on context. The principle of least privilege helps to ensure that users are granted rights that are limited only to those required in the performance of their jobs.
2. **Network Security:** The growing demand for remote access complicates the process of securing a network. Yet the integrity of network security must be maintained while supporting remote access for mobile and third-party users. Network and host segmentation can be useful in shrinking surfaces that are vulnerable to attack. And implementing a multi-layer approach helps to boost network security while ensuring availability.
3. **Application Security:** All types of applications are potential targets for hackers, but the veritable explosion of apps has created many additional points of vulnerability for most enterprises. Apps on mobile devices are particularly susceptible to exploitation. An important step in reducing risk is enacting centralization and the encrypted delivery of applications. Containerization for mobile apps and inspection of incoming data streams can help to reduce app-related security vulnerabilities.
4. **Data Security:** The security of enterprise data can be enhanced by the centralization and hosted delivery of data by enforcing secure file sharing (to reduce data loss) and by the containerization of data (both in-transit and at rest).
5. **Monitoring and Response:** Vigilance and fast action are required to successfully counter the attacks that most enterprises face on a daily basis. A rapid response to breaches is critically important, given that even the most secure systems are

not completely invulnerable to successful attacks. Rapid detection and response to successful attacks serve to minimize damage and help to limit susceptibility to imminent additional attacks. End-to-end visibility into application traffic supports faster identification of security breaches and system anomalies.

The Benefits and Burdens of Remote Access

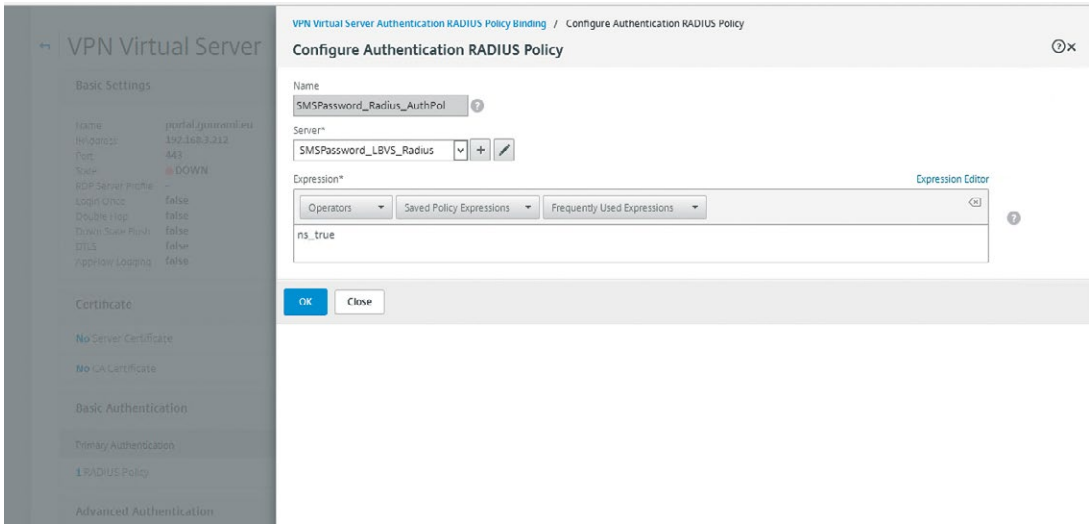
Remote access has enabled an entirely new paradigm of workplace flexibility and productivity. Mobility enhancing tools such as tablets, smartphones and other devices have transformed many enterprise roles into an any place, any time proposition. Workers have benefited from schedules that offer more flexibility, enhancing both work and home life. Companies have benefited from the leaps of productivity that remote access enables.

But this ongoing paradigm shift has required that enterprises find ways to balance the protection of sensitive data with the impact of remote access upon user flexibility — the widespread use of Virtual Public Networks (VPNs) over unsecured networks, for example.

While remote access does increase the burden of safeguarding enterprise systems and data, the benefits of remote access justifies the need for an increased focus upon security. The Citrix Ready Secure Remote Access program is designed to help enterprises conform to the five security pillars listed above while meeting the skyrocketing demand for more remote access capabilities.

SMSPassword has been selected to participate in the Citrix Ready Secure Remote Access program. SMSPassword's two-factor authentication solution has demonstrated the ability to consistently conform with and support the five security pillars of the Secure Remote Access program.

Key features of SMSPassword include:



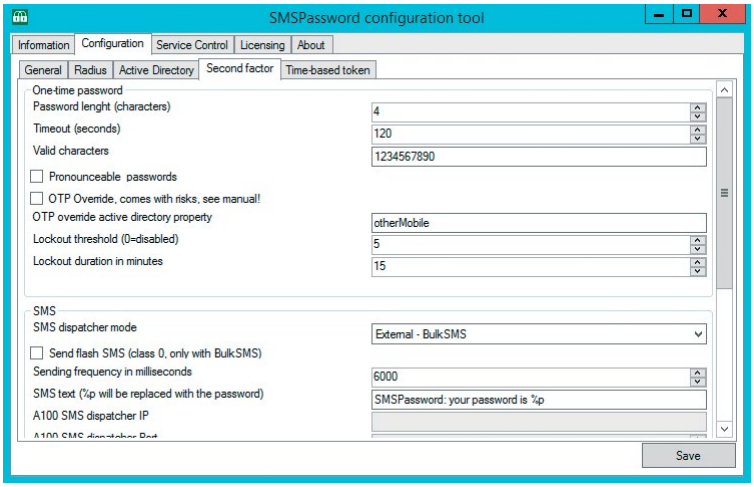
- **Use of RADIUS:** SMSPassword uses Remote Authentication Dial-In User Service (RADIUS) networking protocol. RADIUS enables the maintenance of user profiles in a centralized database, making them assessable to designated remote servers. RADIUS has become established as the industry standard for providing network authorization and authentication services, and is used in Citrix NetScaler to authenticate incoming external users.

- **Securing of XenDesktop, XenApp, VPN and File Share:** Through RADIUS, SMSPassword can be used to secure external Citrix XenDesktop and XenApp sessions, along with VPN and file sharing. SMSPassword works in conjunction with RADIUS to verify the identity of users via the submitted two-factor credentials: the user's standard password along with SMSPassword's real-time-generated, one-time password.

CITRIX®
XenDesktop

Overview of SMSPassword

SMSPassword provides organizations worldwide the ability to easily and cost-effectively implement two-factor authorization capability. SMSPassword's two-factor authorization solution combines a crucial additional layer of security with a user-friendly methodology. Second-factor authorization is enabled by sending the user a one-time password (OTP), generated in real time after the user has entered the domain password.



Unique features of SMSPassword's two-factor authorization methodology include:

- **Flexible OTP Delivery:** One-time passwords are generated and conveniently sent to the user's mobile phone. Any mobile phone is suitable for receipt of the OTP; smartphones are not necessary. SMSPassword also offers the option of generating time-based OTPs via an app installed on the user's Android or iOS device.

- **Second Factor on Second Screen:** Users enter their domain password on the initial login screen. Upon successful verification of domain password, the OTP is generated and sent to user. Simultaneously, the initial login screen is replaced with a second screen prompting entry of the SMSPassword OTP. The process is smooth, simple, fast and confusion-free for users.

- **Token-Trashing:** The requirement of using physical tokens for second-factor authorization is clumsy and inconvenient for users — particularly for remote access. Users must remember to always have the token on their person. But SMSPassword requires only a mobile phone. And everybody always has their mobile phone on hand, no matter where in the world they might be.

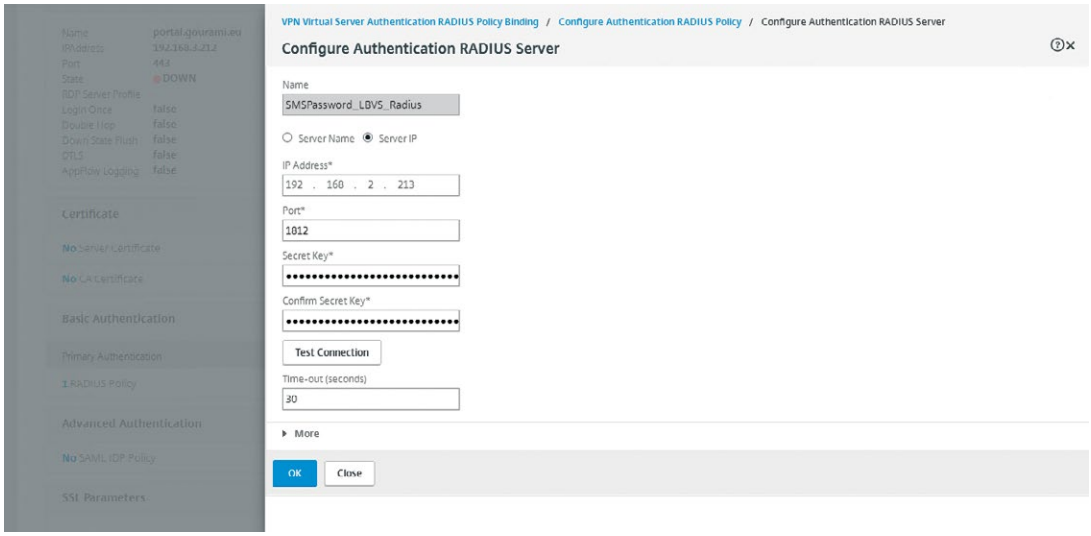
- **Superior Security:** SMSPassword one-time passwords are generated randomly, in real time during the login event. They can be neither predicted nor stolen in advance. Once sent, one-time passwords expire in just minutes, adding an extra layer of security. And users can be locked out of the system after a designated number of failed login attempts.

- **Reliable Redundancy:** Reliability is obviously crucial for any two-factor authorization solution. SMSPassword enables maximum reliability by enabling the redundancy of multi-node setup. Any number of servers may be designated as SMSPassword servers. During a login scenario, a network load balancer (such as Citrix NetScaler) will send a heartbeat check to every node. If a node doesn't respond, the load balancer proceeds

to the next designated node. Multi-node capability helps to assure that SMSPassword two-factor authorization will be instantly and always available, even during partial system outages. But though multiple nodes increase reliability, they aren't necessary. SMSPassword is compatible with a single-node operation.

SMSPassword integrates perfectly with Citrix NetScaler, enabling secure remote access to applications, networks and desktops. A redundant two-factor authentication RADIUS server, SMSPassword is Citrix NetScaler ready. Unlike many two-factor solutions, SMSPassword sends OTPs over a separate network, providing an additional layer of security by separating the first and second factor. Even if a company's primary internet connection is compromised, cybercriminals won't have access to the second-factor OTPs.

No external third party-owned hardware is required. SMSPassword also reduces external dependencies by enabling complete in-house control; the solution can be configured 100 percent on site, unlike many two-factor solutions that require a VPN tunnel to an external RADIUS server. SMSPassword typically can be installed on existing machines, and ongoing administration is very simple — NetScaler and SMSPassword do all the work.



SMSPassword Solution Detail

The protection of two-factor authorization is only minutes away for companies that decide to deploy SMSPassword — installation is that fast and easy, requiring just seven quick steps. The ease of integration with users' existing Active Directory further minimizes the cost and effort of SMSPassword setup. The minimal installation effort helps to keep costs low from the very beginning.

TCO is minimized by SMSPassword's low-cost / no-cost SMS messaging, even for unlimited SMS. And though SMSPassword was designed specifically to work with Citrix NetScaler, it also works with other solutions that use RADIUS. That added flexibility helps to contain costs.

SMSPassword was designed to be light and smart to contain costs and enhance efficiency and usability. No database is required — user's existing Active Directory serves as the database for SMSPassword. Installation of SMSPassword does not require Active Directory schema changes or the addition of Windows roles. In many cases installation can even be as simple as just copying and pasting .exe files. SMSPassword also provides the option of combining with an existing Windows server, such as a Citrix Storefront server.

And since everyone owns a mobile phone, all employees at every organization are equipped to start receiving OTPs from SMSPassword. The latest and greatest phone technology is not necessary — even an ancient flip-phone will work.

A Proven Partnership that Minimizes the Cost and Complexity of Two-Factor Authorization

Many companies are scrambling to find better bulwarks of defense against the current explosion of cybercrime. They are searching for solutions that keep systems and data more secure. But they are also seeking solutions that enhance security without associated incurred costs that blow budgets out of the water or complications that slow the productivity of users. SMSPassword offers the extra layer of security that companies seek with two-factor authentication that is affordable to implement, easy to use, and extremely effective.

SMSPassword's solution is proven to integrate seamlessly and easily with Citrix network security systems to provide an unbeatable two-factor authentication platform. SMSPassword's certification by the Citrix Ready Secure Remote Access program provides enterprises with a proven, reliable remote access security solution for facing the ever-escalating security needs of the modern business environment. For companies seeking to protect themselves against the modern-day scourge of cybercrime, the partnership of Citrix and SMSPassword offers an affordable, proven resource for enhanced security.

For more information about SMSPassword, please visit: https://smspassword.com/

For more information about Citrix Ready, please visit: https://citrixready.citrix.com/

Appendix

Learn more about the enterprise security advantages provided by Citrix NetScaler Unified Gateway at: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/best-practices-for-enterprise-security.pdf

Learn more about how SMSPassword integrates with Citrix NetScaler at: https://smspassword.com/manuals/citrix-netscaler-manual

To learn more about the Citrix Ready Program partnership with SMSPassword, please visit: https://citrixready.citrix.com/smspassword/smspassword.html

To learn more about security solutions for business enterprises, contact Citrix and SMSPassword.

About Citrix Ready

Citrix Ready identifies recommended solutions that are trusted to enhance the Citrix Delivery Center infrastructure. All products featured in Citrix Ready have completed verification testing, thereby providing confidence in joint solution compatibility. Leveraging its industry-leading alliances and partner ecosystem, Citrix Ready showcases select trusted solutions designed to meet a variety of business needs. Through the online catalog and Citrix Ready branding program, you can easily find and build a trusted infrastructure. Citrix Ready not only demonstrates current mutual product compatibility, but through continued industry relationships also ensures future interoperability. Learn more at citrixready.citrix.com.

About SMS Password

SMSPassword is a global operating company founded in the Netherlands and is all about security and trust, helping companies to face the security challenges the modern age present. SMSPassword's mission is to offer maximum security while utilizing existing standards. This message is heard and appreciated by our customer's around the globe. Top reasons for our customers to chose SMSPassword; on-premises, adaptiveness, ease of administration and redundancy. Find out more at smspassword.com.