



Convenient Two-Factor Authentication with sendQuick ConeXa and Citrix NetScaler

The workforce is becoming increasingly mobile. Advances in technology have enabled work and workers to escape the physical bounds of the office. At many companies employees can log in and gain access to proprietary data and systems from anywhere in the world. It is a technological leap that offers great opportunities and conveniences for employees and employers alike.

But though remote access offers extraordinary levels of convenience and productivity, it also imposes increased levels of risk. Cybercrime is escalating at an unprecedented rate. And the increase in mobility has added fuel to the cybercrime conflagration by opening a vast new frontier of opportunity for cybercriminals. The need for remote access to systems, networks and data has never been greater, but each user granted remote access becomes a new target for criminals.

Many companies still rely upon password protection, but password defenses are all too easy to breach. Seventy-three percent of the population reuses passwords, according to TeleSign, vastly diminishing their effectiveness. 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 systems access.

Two-factor authentication provides a much more robust defense than a simple query-password system. This paper discusses TalariaX's industry-leading two-factor system, as well as 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 TalariaX's two-factor solution to meet the growing need for a remote access security solution for enterprises worldwide.

Business Challenge Summary

Magically transport an office worker from a few decades ago to the present day, and that astonished person would certainly notice more than a few changes in the workplace. But apart from fashion changes and the presence of faster, more capable office equipment, it is likely that the largest change that time-displaced person would notice is the office itself: in many instances, it is no longer a brick-and-mortar location. Instead, it is a virtual office that springs into existence each time an employee logs in with their laptop or other device.

For a rapidly growing percentage of workers, that virtual office is the only office they know — and the only one they need. More workers than ever before enjoy the flexibility and convenience of working from home — or from a hotel, or from an airplane, or from a coffee shop. They can bring their personal virtual office to life at any time from any location.

The boom in mobility has benefited employees with work arrangements that offer greater flexibility and convenience. The companies that employ the mobile workforce have also benefited from increases in productivity and a reduction in operational costs. In many cases, mobility has enabled companies to keep a pool of talented workers ready and able to work on demand as needed, slashing costs during times when those workers aren't required.

But there is a cloud with that silver lining. Cybercriminals have done an outstanding job of keeping up with the technological advances that have enabled mobility. More than ever, criminals are feasting on a bounty of ill-gotten access to data and systems. In particular, companies that still rely upon ancient pre-mobility security methodologies are prime prey for cybercriminals.



Perhaps the most ancient of security methodologies is the reliance upon a single password to prevent unauthorized entry into a system. Single-factor authentication is a security methodology that cybercriminals love, because they've found it so easy to foil. Phishing attacks, malware infections, keylogging and brute force attacks are just some of the tried and true methodologies used to illicitly harvest passwords by the millions every year.

Therefore it is a simple and indisputable fact that with every single login attempt, the receipt of the correct password does not confirm that the user is a valid user. It could just as well be a cybercriminal attempting to make use of one of those millions of harvested passwords.

CITRIX®
Receiver

But there is a way to confirm that users logging into a system are who they claim to be. Adding a second level of authentication, generated in real time and sent directly to the user's phone, eliminates fraudulent attempts at gaining access to systems and data. Two-factor authentication is the key to realizing the benefits of mobility, while retaining the integrity of systems and data security.

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

Many of the world's best-known technology companies — Google, Twitter, Facebook, Microsoft, Amazon, Apple and many others — now enjoy the enhanced security provided by a two-factor solution, according to CNET. But maximizing the potential of a two-factor authentication methodology requires the installation of a system that delivers a full range of capabilities. The following, in particular, should be considered must-have features for two-factor solutions undergoing evaluation for deployment in any organization:

1. **Easy Deployment:** A stumbling block that sometimes prevents organizations from implementing a two-factor solution is the difficulty of deployment. Many two-factor solutions require the issuance of physical tokens — potentially to tens of thousands of users. Some solutions require the embedding of cryptographic keys within code, or the scanning and storage of biometric data such as fingerprints. Two-factor solutions that impose requirements such as these can require massive effort and expense just to implement. They also tend to require user participation during the deployment process that is likely to be highly disruptive and, for a time, counterproductive.

The ideal two-factor solution for most organizations demands no user participation to implement, requires little or no modification of existing code, and is a self-contained solution that does not rely upon physical tokens.

2. **Low Implementation Cost:** Just as with solutions that are difficult to deploy, solutions that are exorbitantly expensive to implement present a significant stumbling block. Many of the difficult and complex deployment requirements noted above tend to drive implementation costs to budget-busting levels. However, two-factor solutions are available that keep both the difficulty and cost of implementation quite low.
3. **Easy Integration:** Integrating a two-factor system with existing hardware, software and systems can be nightmarishly difficult. But it doesn't have to be. Organizations that carefully choose the right two-factor solution can expect easy integration with Active Directory, RADIUS and local/external databases.
4. **Comprehensive SMS Alerting Capability:** The two-factor solution should have the capability of sending all types of alerts using SMS text, including customizable user messaging.

CITRIX®
XenApp

CITRIX®
XenMobile

CITRIX®
ShareFile

CITRIX®
NetScaler

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:

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
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 perpetrated via Remote Access.

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

1. **Identity and Access:** Administrators must be able to confirm the identity of 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 confirm user identity in 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 also 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 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. Indeed, the very meaning of the word “workplace” must be redefined to be less location-specific and more worker-specific. The adoption of mobility enhancing tools such as tablets, smartphones and other devices has transformed many enterprise roles into any place, any time propositions. Workers have benefited from schedules that offer more flexibility, helping to enhance both work- and home-life. Companies have benefited from the leaps in 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 justify 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.

The screenshot displays the 'VPN Configuration' window in the sendQuick ConeXa management console. The interface includes a sidebar with navigation options such as 'Logs', 'Authentication Configuration', 'RADIUS Client Configuration', 'VPN Configuration', 'Remote DB Configuration', 'LDAP Configuration', 'System Configuration', and 'User Management'. The main configuration area contains the following fields and options:

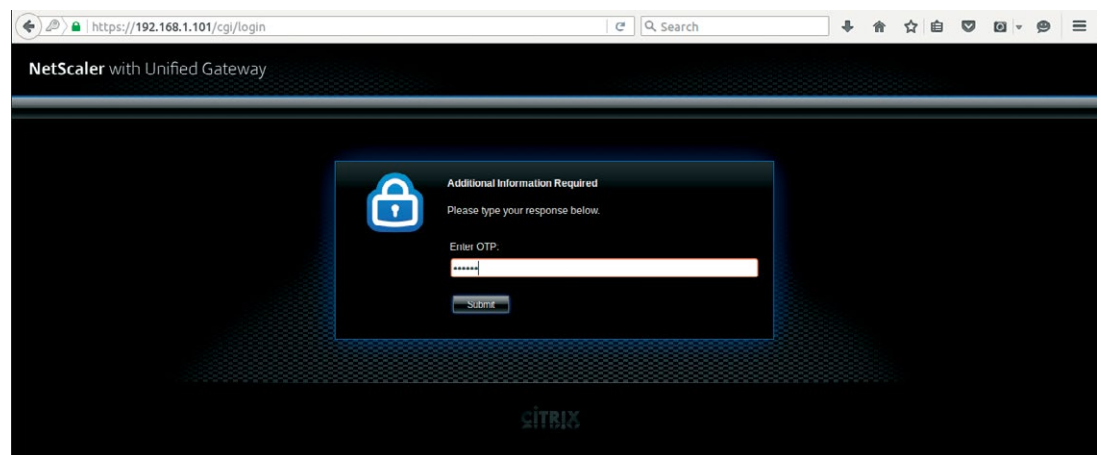
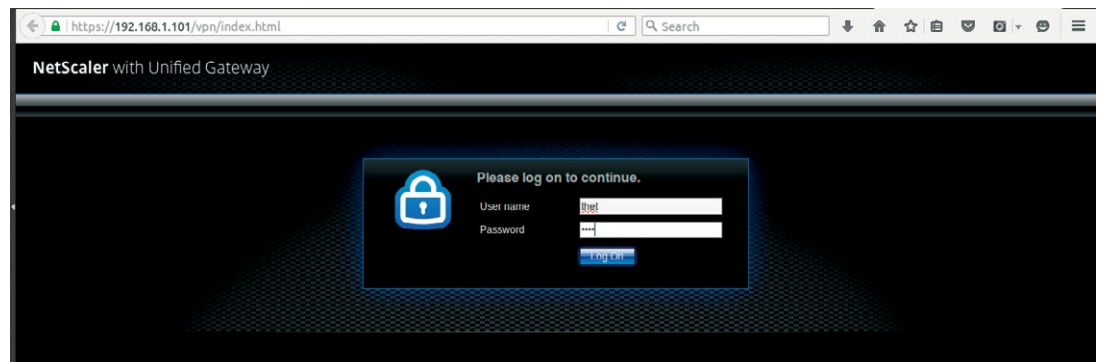
- Captive Portal Controller Name:** A dropdown menu set to 'None'. A tooltip indicates: 'Select Controller Name if this vpn configuration is for captive portal. Default: None.'
- NAS-IP / NAS-ID:** A text input field containing '192.168.1.80'.
- Authentication Type:** A dropdown menu set to 'Two Factor Access Challenge'.
- Authentication Server:** A dropdown menu set to 'LDAP'.
- Return Option:** Two checkboxes: 'Return LDAP group as Radius attribute : Filter-Id (11)' (checked) and 'Return LDAP group as Radius attribute : Class (25)' (unchecked).
- LDAP Servers:** A dropdown menu set to 'AD213'. A tooltip indicates: 'Authentication through LDAP server such as Active Directory or OpenLDAP. Select LDAP server from list, which is predefined in LDAP Server Configuration page.'
- OTP Prompt Message (Access Challenge):** A text input field containing 'Enter OTP:'.

On the right side of the configuration window, there is a table titled 'Selected VPN(s)' with an 'Update' button and several rows of configuration data.

TalariaX has been selected to participate in the Citrix Ready Secure Remote Access program. TalariaX's sendQuick ConeXa 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 sendQuick ConeXa include:

- **Identity Protection:** TalariaX's SMS notification is sent directly to the user's phone. TalariaX sendQuick ConeXa uses an integrated SMS server that generates a one-time password for two-factor authentication that neither compromises the user's identity, nor places access to systems or data in the wrong hands.
- **Improved Network and Data Security:** TalariaX sendQuick ConeXa offers an effective, efficient methodology for restricting access to proprietary systems and data. Only authorized personnel will be able to receive the one-time password sent directly to users' phones via SMS messaging. And the short shelf life of the OTP — expiration time can be adjusted per client's preference — adds an additional layer of security that further reduces the likelihood of an unauthorized login.
- **Seamless Integration with Citrix NetScaler:** TalariaX sendQuick ConeXa is designed to integrate seamlessly with NetScaler. Configuring NetScaler to run with sendQuick ConeXa is a simple, straightforward process that requires only minutes to complete.



CITRIX
XenDesktop

Overview of TalariaX sendQuick ConeXa

TalariaX sendQuick ConeXa gives organizations worldwide the ability to easily and cost-effectively implement two-factor authentication. TalariaX's two-factor authentication solution combines a crucial additional layer of security with a user-friendly and administration-friendly methodology. Second-factor authentication 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 TalariaX's two-factor authentication methodology include:

- **All-In-One Two-Factor Authentication System:** TalariaX provides a simplified means of strengthening authorization security. SendQuick ConeXa is an all-in-one, single-box appliance that supports two-factor login authorization and authentication. The single-box design enables quick and easy plug-and-play implementation, and the SMS messaging platform eliminates the need for the distribution of physical tokens among the user base — an expensive, disruptive, time-consuming process that is required by many two-factor security solutions.
- **SMS One-Time Passwords:** SMS messaging is the most convenient, cost-effective method for the delivery of one-time passwords. SMS-based password distribution eliminates the need for hardware tokens or for additional hardware of any kind. Users only need their personal phones. SMS-based password distribution is also a clientless approach; there is no need to install or maintain software on users' phones. No other two-factor authentication methodology can compete with SMS messaging for easy and inexpensive implementation, minimal maintenance and support costs, and user convenience.

The screenshot displays the configuration interface for TalariaX sendQuick ConeXa. The primary authentication method is set to RADIUS. The configuration fields include IP Address (192.168.1.42), Port (1812), Time out (3 seconds), and Secret Key. The secondary authentication method is set to None. The Basic Settings sidebar on the right shows a checklist of components: Virtual Server, Server Certificate, Authentication, Portal Theme, and Applications, all of which are checked.

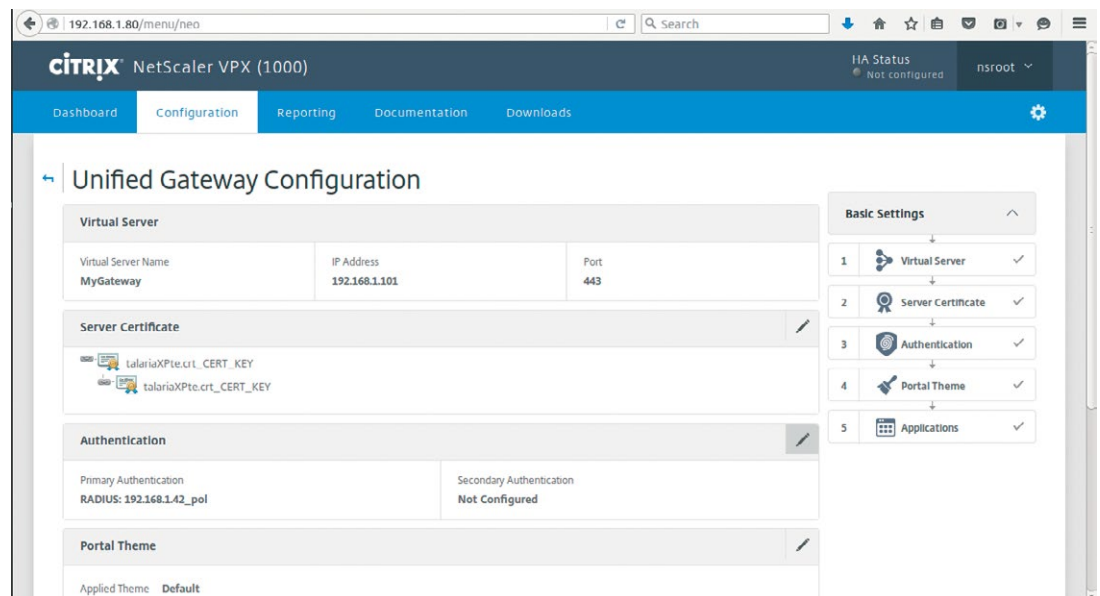
- **Transparent, Easy Process for Users:** Many two-factor authentication solutions are considerably less than user friendly. Some demand that the user always have a physical token on hand. Some require that specialized software be downloaded and maintained on users' phones. But TalariaX sendQuick ConeXa may well be the most user-friendly

two-factor authentication solution on the market. During login to NetScaler, the user is required only to have their mobile phone at hand — and everyone always has their phone with them. TalariaX handles everything else: sendQuick ConeXa quickly generates a unique one-time password, sends it to the user's phone, and authenticates the user once they've entered the OTP. The OTPs are only six to ten characters; users don't have to endure the frustrating and error-prone process of typing in a huge, indecipherable string of characters.

TalariaX sendQuick ConeXa integrates perfectly with Citrix NetScaler, enabling secure remote access to data and systems. TalariaX supports many different database servers, including Active Directory and RADIUS — also used by Citrix NetScaler — facilitating the integration of both internal and external user lists. NetScaler and sendQuick ConeXa handle authentication the same way, further enhancing their compatibility.

No external third-party-owned hardware is required; sendQuick ConeXa is a complete plug-and-play solution. And sendQuick ConeXa also reduces external dependencies by enabling complete in-house control. The solution can be configured 100 percent on site. TalariaX sendQuick ConeXa typically can be installed on existing machines, and ongoing administration is very simple — NetScaler and sendQuick ConeXa do all the work.

TalariaX helps to keep two-factor authentication affordable by permitting unlimited users; no user licenses are required. SendQuick ConeXa supports multiple VPN sessions, further bolstering efficiency and minimizing operational costs.



The screenshot displays the Citrix NetScaler VPX (1000) configuration interface. The browser address bar shows the URL `192.168.1.80/menu/neo`. The interface includes a navigation menu with options: Dashboard, Configuration, Reporting, Documentation, and Downloads. The main content area is titled "Unified Gateway Configuration" and is divided into several sections:

- Virtual Server:** A table with columns for Virtual Server Name, IP Address, and Port. The entry is "MyGateway" with IP Address "192.168.1.101" and Port "443".
- Server Certificate:** A section showing two certificates: "talariaXPte.crl_CERT_KEY" and "talariaXPte.crt_CERT_KEY".
- Authentication:** A section with two columns: "Primary Authentication" (RADIUS: 192.168.1.42_pol) and "Secondary Authentication" (Not Configured).
- Portal Theme:** A section with "Applied Theme" set to "Default".

On the right side, there is a "Basic Settings" panel with a list of five items, each with a checkmark:

- 1 Virtual Server ✓
- 2 Server Certificate ✓
- 3 Authentication ✓
- 4 Portal Theme ✓
- 5 Applications ✓

TalariaX sendQuick ConeXa Solution Detail

TalariaX sendQuick ConeXa uses SMS messaging to send one-time passwords to individual users for two-factor authentication. But sendQuick ConeXa may also be used to send customized messages and text alerts to individual users for all network, security and IT management issues. You can use sendQuick ConeXa, for example, to notify IT team members via SMS text about any issues requiring immediate response.

The self-contained, single-box design of sendQuick ConeXa provides a number of unique advantages, including:

- Easy integration with NetScaler (using RADIUS for two-factor authentication and with email, SNMP Trap, Syslog for SMS text alerts)
- Fast response to user authentication requests and rapid OTP deliveries
- Little downtime and minimal maintenance requirements
- Familiar SMS technology — almost everybody uses SMS on a daily basis — facilitating user convenience and ease of management
- Low cost deployment; the only external requirement is Citrix NetScaler

TalariaX has developed a sterling reputation for providing hassle-free support. Combined with sendQuick ConeXa's support for unlimited users, TalariaX's two-factor solution provides outstanding ROI for companies looking to move beyond a simple query-password security solution.

A Proven Partnership that Makes the Benefits of Two-Factor Authentication Easily Obtainable

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 costs that blow budgets out of the water, or complications that slow the productivity of users. TalariaX sendQuick ConeXa offers the extra layer of security that companies seek with two-factor authentication that is affordable to implement, easy to use and extremely effective.

TalariaX's solution is proven to integrate seamlessly and easily with Citrix network security systems to provide an unbeatable enterprise two-factor authentication platform. TalariaX's selection to 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 TalariaX offers an affordable, proven resource for enhanced security.

For more information about TalariaX, please visit: <http://www.talariax.com/web/index.html>

For more information about Citrix NetScaler, please visit:
<https://www.citrix.com/products/netscaler-adc/>

To learn more about the Citrix Ready Program partnership with TalariaX, please visit:
<https://citrixready.citrix.com/talariax-pteltd/sendquick-conexa.html>

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

For more details about sendQuick ConeXa, download the data sheet.

See how easily sendQuick integrates with NetScaler by [downloading the configuration guide](#).

To learn more about security solutions for business enterprises, contact [Citrix](#) and [TalariaX](#).



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 TalariaX

TalariaX developed sendQuick®, the industry's leading appliance-based SMS Text gateway solutions for enterprise messaging. sendQuick has been used by over 1,500 corporations in 40 countries. Our solutions include IT alerts and notifications, 2-factor authentication with SMS OTP, marketing and emergency broadcasting for various industries such as banking, finance, insurance, manufacturing, retail, government, education, and healthcare. These have been effective to improve enterprise responsiveness, improved business workflows, and increased operational effectiveness. Learn more about us at www.talariax.com

Copyright © 2016 Citrix Systems, Inc. All rights reserved. Citrix XenDesktop and Citrix Ready are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.

