



# Advanced Authentication for NetIQ SecureLogin

*Advanced Authentication fits into your environment to increase the security of your organization's identity and access procedures.*

## BUSINESS CHALLENGE

Borderless and unprotected networks, combined with always-fallible human nature, make it difficult for organizations to keep their assets secure, even with good identity and access management.

## SOLUTION BENEFITS

The Advanced Authentication framework from NetIQ works with NetIQ® SecureLogin and NetIQ Access Manager™ and integrates with scanners and hardware of all kinds. Using Advanced Authentication you can:

- Provide single sign-on to applications of all kinds
- Add multi-factor authentication
- Enhance security for mobile workers

## The Changing Landscape of Security

Each day, modern workers must access multiple applications, often on many different platforms. For every application, users need to remember a unique username and password. Soon they start writing down passwords— and that is just one of the security issues created by modern work habits. The growth of borderless networks means that your users may not be at a tangible location on a known device anymore. Authentication for the modern enterprise needs to somehow become both more secure and easier for users.

Advanced authentication, also known as multi-factor authentication, is one way to increase security. It places a strong security layer between your corporate assets and unproven entities by requiring multiple kinds of credentials. These credentials might include who you are, what you know or what you have. For example: security questions are something you know and a proximity card is an example of something that you have. A fingerprint is something you are. Advanced Authentication takes advantage of all these kinds of credentials. When combined with single-sign on technology in the right solution, it has the potential to solve modern organizations' problems.

## NetIQ Advanced Authentication Framework

Though this brief focuses on NetIQ® SecureLogin, the NetIQ Advanced Authentication framework works with both NetIQ SecureLogin and NetIQ Access Manager™. This framework enables you to verify and attest who has accessed internal and cloud based applications and resources. For organizations that have internal or industry-related compliance policies, the framework provides a policy engine to

centralize policy creation and enforcement for all users.

NetIQ's advanced authentication framework integrates with most any authentication reader or device, eliminating the need for multiple authentication solutions and providing the most cost efficient multi-factor authentication available.

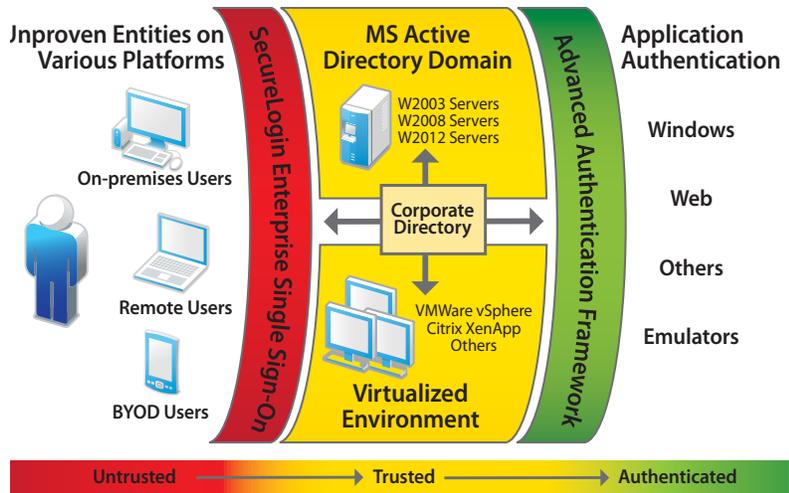
## Advanced Authentication with NetIQ SecureLogin

NetIQ SecureLogin allows users to access local and network resources using a single set of credentials. When users log into their workstation, laptop or session, NetIQ SecureLogin automatically authenticates them to all of their applications and resources, providing the user with a seamless access experience to relevant services. With only one password to remember, users no longer need to write them down and the risk of forgetting that one password is greatly reduced.

Advanced Authentication for NetIQ SecureLogin provides integrations for multi-factor authentication devices as well as other strong authentication technologies, providing an industry-leading level of choice and flexibility. Using Advanced Authentication for NetIQ Secure Login, organizations can set up high-security methods that take advantage of multi-factor criteria. NetIQ SecureLogin supports a wide range of readers for proximity cards, fingerprint scanners for biometric scans, and other types of devices. Multi-factored authentication provides fast and simple high security for your information and applications. It enables users to walk up to a computer, tap their card, and have access to all their appropriate applications in seconds.

### SSO with Advanced Authentication Muscle

NetIQ SecureLogin SSO with Advanced Authentication can allow you to meet regulatory and logical obligations even though the majority of Windows forms and web sites are limited to password authentication. NetIQ SecureLogin stipulates a secondary or “step-up” authentication at startup of an application and at any specified transaction, thus proving identity when and where you require it.



### Take Your Pick. Advanced Authentication from NetIQ Works with them all:

SmartCard, Certificates	Biometric	Proximity Card	Soft Token or One-Time Password
SmartCards offer trusted security and non-repudiation through difficult to extract PKI based certificates.	Biometrics can provide unique hard to replicate scans for superior accuracy at a reasonable cost.	Proximity Card technology is simplistic and provides ease-of-use in a multi-purpose inexpensive format.	Soft Token (OTP) is a popular Oath based solution that provides good security without adding devices.
Radius or Hard Token	SMS, Out-of Band	Flash Drive	Challenge Response
Hard Token (Radius) is a very popular Oath based solution that provides high security using tokens.	SMS is a low cost option that sends a server minted OTP to the user's cellular device for entry and authentication.  Out-of-Band is a low cost option that sends a message to, and requires a response from the user's cellular device	Flash Drive authentication is a low tech, low cost option that utilizes a PIN to open an encrypted file on the drive.	Challenge Response is a zero cost option that requires a user to answers pre-enrolled questions for authentication.

**Worldwide Headquarters**  
 1233 West Loop South, Suite 810  
 Houston, Texas 77027 USA  
**Worldwide:** +1 713.548.1700  
**U.S. / Canada Toll Free:** 888.323.6768  
 info@netiq.com  
 www.netiq.com  
 http://community.netiq.com

**For a complete list of our offices**  
 in North America, Europe, the  
 Middle East, Africa, Asia-Pacific  
 and Latin America, please visit  
[www.netiq.com/contacts](http://www.netiq.com/contacts).

Follow us:   