

Autenticación avanzada para NetIQ SecureLogin

La opción de autenticación avanzada se adapta a su entorno para aumentar la seguridad de la identidad de su organización y sus procedimientos de acceso.

La autenticación avanzada para SecureLogin de un vistazo

■ Cómodo acceso:

Ofrece una entrada única a aplicaciones de todo tipo.

■ Seguridad sólida:

Agrega autenticación de varios factores.

■ Seguridad móvil:

Mejora la seguridad de los empleados que trabajan fuera de la oficina.

El cambiante paisaje de la seguridad

Los trabajadores de hoy en día deben acceder a múltiples aplicaciones a diario y con bastante frecuencia desde distintas plataformas. Para cada aplicación, los usuarios deben recordar un nombre de usuario y una contraseña únicos. Por eso empiezan a anotar las contraseñas y este es solo uno de los muchos problemas de seguridad derivados de los actuales hábitos de trabajo. El crecimiento de las redes sin límites implica que los usuarios pueden no estar en una ubicación física de un dispositivo concreto. La autenticación en la empresa moderna necesita de alguna forma ser más segura y sencilla para los usuarios.

La autenticación avanzada, también conocida como autenticación de múltiples factores, es una manera de aumentar la seguridad. Coloca un importante nivel de seguridad entre los activos de empresa y las entidades no probadas mediante la solicitud obligatoria de varios tipos de credenciales. Entre otras, estas credenciales pueden incluir su identidad, sus conocimientos o sus posesiones. Las preguntas de seguridad, por ejemplo, serían algo que usted sabe y la tarjeta de proximidad, algo que usted tiene. Una huella digital es algo que se es. La autenticación avanzada aprovecha todos estos tipos de credenciales. Cuando se combina con tecnología de entrada única adecuada, cuenta con los recursos para resolver los problemas de la empresa moderna.

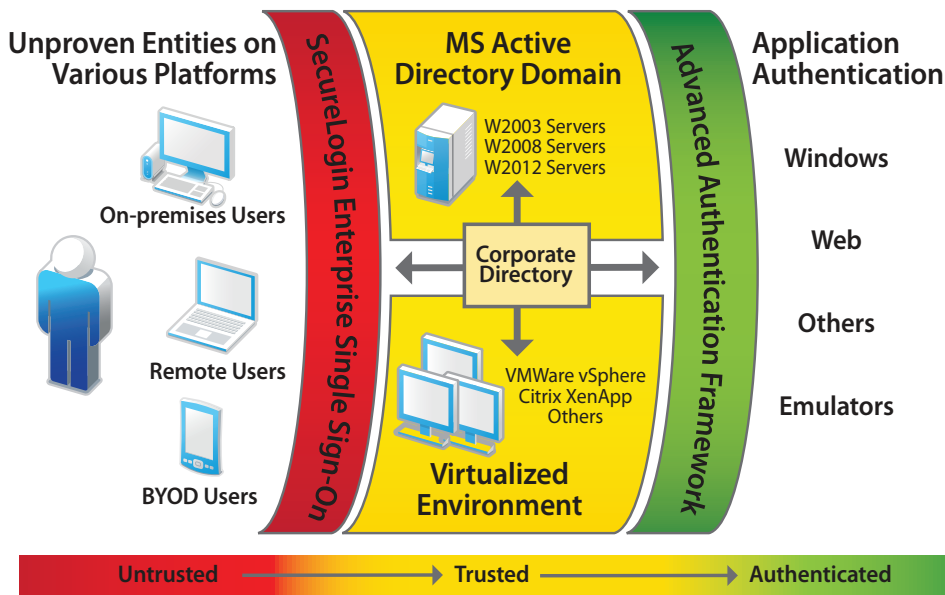
NETIQ ADVANCED AUTHENTICATION FRAMEWORK

Aunque este resumen se centra en NetIQ® SecureLogin, el Advanced Authentication Framework de NetIQ funciona tanto con NetIQ SecureLogin como con NetIQ Access Manager™. Este marco permite verificar y certificar quién ha accedido a las aplicaciones y recursos tanto internos como basados en la nube. Para las organizaciones que cuentan con políticas de cumplimiento interno o relacionadas con el sector, este marco proporciona un motor de políticas para centralizar la creación y cumplimiento de las mismas por parte de los usuarios.

El Advanced Authentication Framework de NetIQ se integra en la mayoría de los lectores o dispositivos de autenticación, eliminando la necesidad de múltiples soluciones de autenticación y facilitando la autenticación más eficiente de múltiples factores.

Autenticación avanzada con NetIQ SecureLogin

NetIQ SecureLogin permite a los usuarios acceder a los recursos de red y locales con un único conjunto de credenciales. Cuando los usuarios se conectan a su estación de trabajo, portátil o simplemente inician sesión, NetIQ SecureLogin autentica automáticamente todas sus aplicaciones y recursos, con lo que el usuario puede disfrutar de una experiencia



NetIQ
Argentina
+54 11 5258 8899

Chile
+56 2 2864 5629

Colombia
+57 1 622 2766

México
+52 55 5284 2700

Panamá
+507 2 039291

España
+34 91 781 5004

Venezuela
+58 212 267 6568

contact-es@netiq.com
www.netiq.com/communities
www.netiq.com

Para obtener una lista completa
de nuestras oficinas en América del Norte, Europa, Oriente Medio, África, Asia-Pacífico y América Latina, visite www.netiq.com/contacts.

www.netiq.com

de acceso sin problemas a los servicios pertinentes. Con una sola contraseña que recordar, no habrá necesidad de apuntarla en ningún sitio. Además, el riesgo de olvidarla se reduce considerablemente.

La opción de autenticación avanzada de NetIQ SecureLogin permite la integración en dispositivos de autenticación de varios factores, así como otras tecnologías de autenticación importantes, con un nivel de elección y flexibilidad líder del sector. Gracias a las funciones de autenticación avanzada para NetIQ SecureLogin, las organizaciones pueden establecer métodos de alta seguridad que aprovechan criterios de muchos factores. NetIQ SecureLogin es compatible con una amplia gama de lectores de tarjetas de proximidad, escáneres biométricos de huellas digitales y otros tipos de dispositivos. La autenticación de muchos

factores proporciona un alto grado de seguridad de forma rápida y sencilla en información y aplicaciones. Permite a los usuarios acceder a sus aplicaciones en segundos con tan solo acceder a un ordenador e introducir sus credenciales.

SSO CON OPCIÓN DE AUTENTICACIÓN AVANZADA

NetIQ SecureLogin SSO con autenticación avanzada le puede ayudar a cumplir las obligaciones lógicas y normativas, incluso si la mayoría de los formularios de Windows y sitios web están limitados a la autenticación por contraseña. NetIQ SecureLogin establece un autenticación secundaria o "complementaria" al iniciar una aplicación y en cualquier transacción especificada, es decir, proporciona la identidad cuando y donde es necesario.

Haga su selección. La opción de autenticación avanzada de NetIQ funciona con todos ellos:

Tarjetas inteligentes y certificados	Biométrica	Tarjeta de Proximidad	Testigos de software o contraseña desechable
Las tarjetas inteligentes ofrecen seguridad de confianza y sin rechazo a través de certificados basados en PKI difíciles de extraer.	La biometría puede proporcionar exploraciones únicas difíciles de repetir para obtener una precisión superior a un coste razonable.	La tecnología de tarjetas de proximidad es muy sencilla y supone un formato asequible, multifunción y fácil de utilizar.	El testigo temporal (OTP) es una solución basada en una autorización que garantiza la seguridad sin necesidad de añadir dispositivos.
Radius o testigo permanente	SMS, fuera de banda	Memoria USB	Preguntas de seguridad
El testigo permanente (RADIUS) es una solución muy conocida, basada en una autorización y que proporciona un alto nivel de seguridad mediante el uso de testigos.	El SMS es una opción de bajo coste que envía un testigo temporal (OTP) desechable acuñado por el servidor al dispositivo móvil del usuario para que este pueda acceder a la aplicación y autenticarse. La opción de fuera de banda es una opción de bajo coste que consiste en enviar un mensaje al dispositivo móvil del usuario del que se requiere respuesta.	La autenticación por unidad de memoria flash es una opción de bajo coste y tecnología sencilla que utiliza un PIN para abrir un archivo cifrado en la unidad.	Con las preguntas de seguridad estará utilizando una opción de coste cero que requiere que el usuario responda a una serie de preguntas para realizar la autenticación.