Safeguarding the Business with Flexible Multi-Factor Authentication

PROVIDE AUTHORIZED USERS WITH CONVENIENT AND SECURE ACCESS TO EXPAND E-BUSINESS AND ENABLE A PRODUCTIVE MOBILE WORKFORCE.

As your business grows, it's likely the number of people requiring access to your systems and valuable assets does as well. While connecting these resources has become more convenient given the rise in mobile devices, the risks associated with delivering secure, convenient access has grown in cost and complexity.

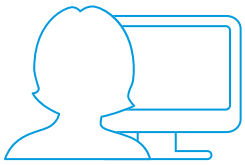
Synchronoss Universal ID reduces the risk of targeted attacks, credential theft, and identify fraud by providing a powerful layer of authentication security. Whether you want to extend access to employees, partners, vendors, or customers, this reliable approach verifies user identities and ensures only the right people gain access your network—so both you and your users can conduct business safely, confidently, and securely.

Universal ID effectively safeguards one of the most vulnerable and frequently exploited elements of traditional authentication: the password. In a 2016 Verizon study of more than 64,000 incidents, the number-one cause of data breaches involved weak, default, or stolen passwords, and over 95% of web application incidents involve stolen credentials. Incorporating secure, multifactor authentication, Synchronoss helps to protect your enterprise by combining a single-use passcode, which cannot be guessed or reused, with the traditional authentication sequence. This additional layer of defense exponentially increases the security of authentication.

OVER 95% OF WEB APPLICATION INCIDENTS INVOLVE STOLEN CREDENTIALS

Synchronoss

Enjoy Security with Simplicity and Cost-Efficiency



ENTERPRISES MUST NOW BE CONCERNED WITH A PASSWORD STOLEN FROM A LESS SECURE LOCATION THAT COULD POTENTIALLY BE USED TO GAIN ACCESS TO THEIR INFRASTRUCTURE.

The Synchronoss Universal ID platform provides strong and secure access to critical systems and sensitive data across the enterprise for local or remote users, partners, and customers. The solution provides a significant increase in security through a high-availability, expertly managed cloud infrastructure and provides rapid deployment, cost conservation, and end-user satisfaction.

ENHANCE SECURITY AND USABILITY

By combining a single-use passcode to the traditional log-in sequence, users can easily access the network and the associated resources required for them to conduct business without experiencing the additional burden often resulting from increased security policies.

Universal ID allows individuals to use their own devices and select from a variety of methods (SMS, a voice call, email, a mobile app, and more) to obtain the passcode, allowing them to customize their authentication experience to best suit their needs.

With the option of QR-based authentication, there's no need to enter usernames and passwords at all. Using a preregistered and bound mobile application, users simply scan a QR code displayed on the log-in page to gain quick, secure access to your website. Where increased security is desired, an additional PIN or password can be incorporated following the scan to add another layer of security onto the authentication process.

REDUCE RISK AND RENDER STOLEN PASSWORDS USELESS

The longstanding attempt to improve password security by increasing their complexity and frequency of change has unfortunately caused a reverse affect. The added complexity has largely caused users to make simple adjustments to standard passwords (adding "!" or "1") and reuse passwords across various accounts to ease their pain in managing and remembering them. If a password is compromised, the attacker may have access to any location using that same password, as opposed to only the exploited target. As a result of vast reuse of passwords, enterprises must now be concerned with a password stolen from a less secure location that could potentially be used to gain access to their infrastructure.

Universal ID prevents these scenarios through the on-demand generation of a single-use passcode delivered to a device in the user's possession in combination with the standard log-in, without which the stolen password cannot be used to gain access.

Synchronoss

VERIFY IDENTITIES OF EMPLOYEES AND THIRD PARTIES

Extending access to remote employees, consultants, partners, or customers outside of your direct control results in an additional layer of complexity to prove the users gaining access to your critical resources are who they claim to be. Universal ID was the first to be government certified by Federal Identity, Credential, and Access Management (FICAM) to incorporate a flexible multilevel identify verification process to identify individuals as part of the credential issuance process.

Using this native identity verification process, Synchronoss can ensure, with the highest certainty possible, that individuals are who they claim to be before issuing a credential and allowing them access to your environment and critical infrastructure.

IMPROVE TIME TO VALUE

As a cloud-based solution, Synchronoss Universal ID allows customers to quickly roll out services and manage users with ease. Universal ID provides repeatable, on-demand enrollment and authentication processes and secure log-in capabilities that can be delivered quickly and easily scale to serve millions of users.

MINIMIZE AND CONTROL COSTS

Universal ID provides a manageable operating expense model because the solution is delivered via the cloud and the need for specialized hardware or software IT expertise is eliminated. Competitively priced, the solution reduces operating costs associated with managing digital identities, audit preparation, onboarding of new customers, and management of help-desk queries.

EXPERIENCE BEST-IN-CLASS AVAILABILITY, SCALABILITY, AND SECURITY

Universal ID is housed at geographically dispersed data centers and is a secure, reliable, and scalable high-availability solution. The solution is administered and monitored by a staff of world-class security experts following best practices, processes, and procedures used to support carrier, enterprise, and government customers operating some of the world's largest and most complex networks.

Synchronoss Universal ID data centers meet Federal Information Security Modernization Act (FISMA) High requirements, providing security management and near-real-time security event correlation and analysis in the most stringent environments.

LEVERAGE STRONG CREDENTIALS TO SECURELY APPROVE CRITICAL TRANSACTIONS

Synchronoss Universal ID also includes a digital signature service that meets enterprise, government, and healthcare regulations for the management and use of digital signatures. Identity-verified individuals granted the appropriate, strong credential can apply legally recognizable digital signatures to government forms, legal documents, e-prescriptions, and other forms requiring a legally binding signature for approval. Universal ID helps businesses securely and efficiently process critical transactions in an efficient and compliant way by leveraging the secure Synchronoss platform.

UNIVERSAL ID HELPS BUSINESSES SECURELY AND EFFICIENTLY PROCESS CRITICAL TRANSACTIONS IN AN EFFICIENT AND COMPLIANT WAY BY LEVERAGING THE SECURE SYNCHRONOSS PLATFORM.

Synchronoss

THE NUMBER-ONE

CAUSE OF DATA BREACHES INVOLVED WEAK, DEFAULT, OR STOLEN PASSWORDS.

ACHIEVE AND MAINTAIN COMPLIANCE

Ever-evolving regulatory mandates bring a layer of complexity and uncertainty to securing access to your infrastructure that can impact your organization from an operational and fiscal perspective. Synchronoss Universal ID is architected to strict standards and backed by government and industry certifications, giving security professionals the confidence that Universal ID verifies identities and secures authentications to the highest standards, including:

- FICAM Level 1, 2, and 3 accredited
- FISMA Authority to Operate (ATO)
- Federal Bridge Certification Authority (FBCA) cross-certified issuer
- SAFE-BioPharma Bridge Certification Authority (SBCA) cross-certified issuer
- National Institute of Standards and Technology (NIST) 800-53 and 800-63-2
- Federal Information Processing Standard (FIPS) 199 and 140-2
- Health Insurance Portability and Accountability Act (HIPAA) and Drug Enforcement Administration (DEA) Code of Federal Regulation (CFR) Part 1311
- U.S. Access Board Section 508
- EU General Data Protection Regulation
- UK tScheme

1. SOURCE: 2016 Verizon Data Breach Report

ABOUT SYNCHRONOSS

REALIZE THE EXCITING POTENTIAL OF ENTERPRISE MOBILITY

Uncompromised productivity and security. Our Secure Mobility Platform meets today's needs and can help make tomorrow's possibilities a reality. It is designed to enhance and complement existing mobility investments, so you get a better ROI—and can finally experience the true power of mobility.

Since 2000, we've provided cloud solutions and software-based activation to communication service providers across the globe. Companies such as AT&T, Verizon Wireless, Comcast, Time Warner Cable, Apple, and Microsoft have used our scalable technology solutions to allow their customers to connect, synchronize, and activate connected devices and services that power the connected world.

We have more than 100 seminal patents, plus one of the largest, most comprehensive technology platforms in production—which currently serves more than 3 billion mobile subscribers. So what does that mean for you?

We know mobility. We know security. We can help your organization do secure business, everywhere.

LEARN MORE

To find out how you can start reducing risk, better securing your business and allowing you to deliver information, and act on opportunities serving partners and customers with confidence, visit: http://www.synchronoss.com/identity/

Synchronoss