

La autenticación multifactor de TrustLayer brinda protección contra la vulnerabilidad de cuentas mediante el uso de contraseñas débiles o robadas, ya sea que se hayan obtenido mediante phishing, ingeniería social, ataques de fuerza bruta o comprados en línea.

MFA está completamente integrado con la plataforma TrustLayer, que también incluye seguridad de correo electrónico, seguridad web y seguridad de aplicaciones en la nube. La plataforma TrustLayer proporciona un único portal web para la configuración y gestión centralizada de políticas, así como para la visualización de datos y la generación de informes.

MFA se basa principalmente en la nube, lo que simplifica la implementación y acelera la rentabilidad para organizaciones de todos los tamaños. No requiere una infraestructura compleja y los principales proveedores ofrecen clientes de autenticación fáciles de instalar.

El servicio Cloud MFA está disponible además del producto TrustLayer de MFA local, diseñado específicamente para organizaciones que desean que los componentes principales se ejecuten en sus propios entornos. La autenticación multifactor en la nube proporciona un panel único para analizar y gestionar la actividad de autenticación de usuarios en múltiples sistemas, servicios y aplicaciones, independientemente de si los usuarios están en la red corporativa o trabajando de forma remota.

TrustLayer MFA admite diferentes políticas de despacho para la entrega de OTP a través de una variedad de métodos, incluidos SMS y correo electrónico, así como a través de una aplicación móvil TrustLayer para Android y Apple iOS.

La conmutación por error automática entre múltiples métodos de entrega proporciona una mayor seguridad de que los usuarios recibirán las OTP, incluso sin cobertura móvil, por ejemplo. La conmutación por error se realiza en el backend y ofrece una experiencia de usuario fluida, a diferencia de otras opciones donde los usuarios deben seleccionar manualmente su método de autenticación.

AUTENTICACION MULTIFACTOR

- El backend 100% basado en la nube simplifica la implementación y la gestión
- Diseñado para brindar una experiencia de usuario inigualable, diseñado para una seguridad superior
- Multiinquilino y multinivel: ideal para organizaciones de cualquier tamaño, así como para MSP.
- Códigos de acceso de un solo uso (OTP) específicos de cada sesión, bloqueados en sesiones individuales para evitar el phishing
- Los OTP generados en tiempo real brindan mayor seguridad que las secuencias predeterminadas basadas en el tiempo.
- Las políticas de despacho ofrecen una selección de métodos de entrega de OTP con conmutación por error automática para garantizar la entrega independientemente de la situación o ubicación del usuario.
- Bloqueo con un solo clic de usuarios individuales para revocar inmediatamente el acceso a todos los servicios protegidos por MFA
- Aplicación TrustLayer para dispositivos Android y Apple iOS para notificaciones push OTP cifradas de extremo a extremo
- Soporte listo para usar para una amplia gama de sistemas, servicios y aplicaciones, incluidos todos los principales proveedores de VPN (incluidos Citrix y Cisco), Microsoft (incluido OWA) y las principales aplicaciones en la nube (incluidos O365 y Salesforce)

Ya sea que los datos de auditoría se requieran únicamente para la visibilidad de la actividad de autenticación o para una certificación más formal del cumplimiento de políticas internas o estándares, regulaciones y legislación externos, la autenticación multifactor proporcionará la evidencia necesaria.

Timestamp	Status	Reason	User	Auth Method	Device
2017-05-25 09:21:43	Failed	Session expired	UserPassExpir...	SMS	Citrix V...
2017-05-25 09:02:05	Failed	Password validation failed	User	N/A	Citrix V...
2017-05-25 16:21:10	Failed	Session expired	User	SMS	HS Websh...
2017-05-25 16:21:10	Failed	Session expired	User	SMS	HS Websh...
2017-05-25 16:21:10	Failed	Session expired	User	SMS	HS Websh...
2017-05-25 09:05:74	Failed	Password validation failed	UserPjyhwf	N/A	Citrix V...
2017-05-24 10:00:41	Failed	Session expired	User2	SMS	Testing
2017-05-24 16:21:10	Failed	Session expired	User	SMS	HS Websh...
2017-05-24 10:08:41	Failed	Session expired	User2	SMS	Testing
2017-05-25 09:05:48	Failed	Password validation failed	User	N/A	Citrix V...
2017-05-24 10:09:00	Success	Session expired	User2	SMS	Testing
2017-05-25 16:21:10	Failed	Session expired	User	SMS	HS Websh...
2017-05-24 10:09:00	Success	Session expired	User2	SMS	Testing
2017-05-24 10:09:00	Success	Session expired	User2	SMS	Testing
2017-05-24 09:03:51	Success	N/A	UserPIN	SMS	Citrix V...
2017-05-24 10:09:00	Success	Session expired	User2	SMS	Testing
2017-05-24 16:21:10	Failed	Session expired	User	SMS	HS Websh...
2017-05-24 10:08:41	Failed	Session expired	User2	SMS	Testing
2017-05-25 16:21:10	Failed	Session expired	User	SMS	HS Websh...
2017-05-24 10:09:00	Success	Session expired	User2	SMS	Testing

La MFA de Censornet utiliza memoPasscodes™, una forma única de generar códigos de acceso que los hace muy fáciles de memorizar y simples de ingresar para los usuarios al iniciar sesión. La aleatoriedad del código de acceso, y por lo tanto la seguridad, no se ven afectadas.

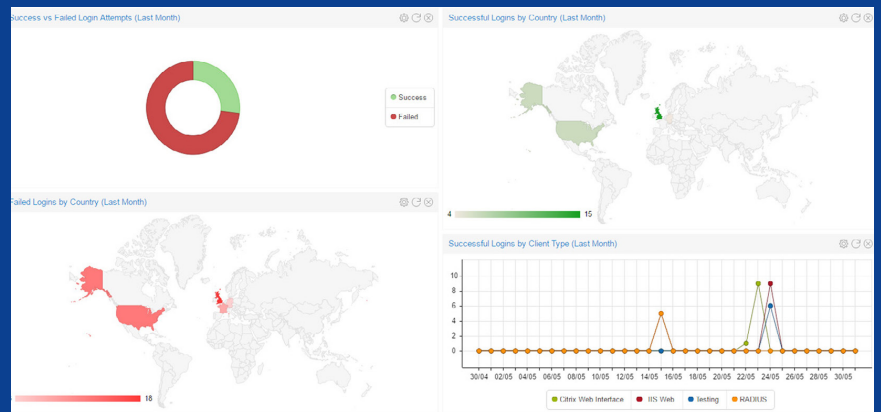
MFA utiliza el motor de sincronización de AD de TrustLayer Platform, lo que permite una integración completa con Microsoft® Active Directory, con opciones para usar sincronización local o en la nube.

La sincronización local utiliza un servicio de conector de AD (agente) instalado localmente que envía todos los objetos, o todos los objetos desde un punto configurable en el árbol de AD, a TrustLayer Cloud. Las actualizaciones diferenciales se realizan cada 15 segundos. La sincronización en la nube utiliza una conexión LDAP o LDAPS para extraer objetos.

La sincronización local tiene la ventaja adicional de no requerir cambios en las reglas del firewall. Ambos métodos requieren una cuenta de servicio de solo lectura en AD. Una vez configurada, la sincronización de AD (y, por lo tanto, la identidad) está disponible en todos los componentes de TrustLayer Platform.

La MFA de TrustLayer utiliza memoPasscodes™, una forma única de generar códigos de acceso.

La autenticación multifactor está completamente integrada con la plataforma TrustLayer, que proporciona visualización de datos completa e informes con un amplio conjunto de atributos y criterios. El análisis y los informes están disponibles por hora, usuario, dirección IP, datos de geo-IP, inicio de sesión correcto o incorrecto y tipo de cliente.



CARACTERÍSTICAS CLAVE

Clientes de autenticación / Compatibilidad con protocolos

Soporte para proteger un número ilimitado de clientes de autenticación:

- RADIUS (protege el acceso VPN, por ejemplo, Citrix Access Gateway o Cisco VPN)
- Inicio de sesión de Windows (protege el acceso RDP a los servidores)

www.cobranetworks.com

	<ul style="list-style-type: none">• ADFS (protege aplicaciones en la nube como Salesforce o Google Apps)• Citrix Web Interface (pre-dates Citrix Access Gateway with RADIUS)• IIS Website (protects Outlook Web Access or RD Web Access)
Soporte del proveedor	<ul style="list-style-type: none">• Los proveedores compatibles incluyen Barracuda, Check Point, Cisco, Citrix, F5, Google, Juniper Networks, Microsoft, OpenVPN, Palo Alto Networks, Salesforce, Teldat y VMWare.
Políticas de envío de OTP	<p>Las políticas de envío definen el método de entrega de OTP con anulación para usuarios individuales. Los métodos de entrega incluyen:</p> <ul style="list-style-type: none">• SMS• Email• TrusLayer App• SMS con conmutación por error al correo electrónico• Aplicación TrustLayer con conmutación por error a SMS
Generador de códigos aleatorios OTP	<ul style="list-style-type: none">• Basado en un algoritmo aprobado FIPS 140-2.
Tipo de SMS	<ul style="list-style-type: none">• Soporte para SMS estándar y Flash.
Aplicación móvil TrustLayer MFA	<ul style="list-style-type: none">• Available for Android and iOS for OTP push with end to end encryption.
Transmisión OTP	<ul style="list-style-type: none">• Los costos de transmisión de OTP están incluidos (sujeto a la política de uso justo).

INFORMES

Visibilidad en tiempo real	<ul style="list-style-type: none">• Los gráficos de productividad muestran visibilidad instantánea del cumplimiento de las políticas definidas. Consulte la actividad de autenticación en tiempo real por usuario, dirección IP, datos de geo-IP, resultado del inicio de sesión y tipo de cliente de autenticación. Vea exactamente qué usuarios se autentican en qué sistemas, servicios y aplicaciones.
-----------------------------------	--

Generador de informes

- Los administradores pueden definir sus propios informes según los nombres de campos y criterios disponibles.
- Los informes se pueden guardar y luego exportar a CSV o PDF. Se pueden buscar en los informes de auditoría por criterios como hora, usuario, dirección IP, datos de geo-IP, inicio de sesión correcto o incorrecto y tipo de cliente.

Programación y alertas

- Vincular informes a programaciones y, opcionalmente, recibir un informe solo cuando haya contenido (modo de alerta).
- Alerta sobre inicios de sesión fallidos, usuarios específicos, etc.

Informes de tendencias principales

- Una selección de informes de tendencias predefinidos con datos en gráficos y tablas. Los informes de tendencias se pueden exportar a PDF y enviar por correo electrónico.

Vistas múltiples

- Analizar e informar por usuario, dirección IP, datos geográficos de IP, resultado de inicio de sesión y tipo de cliente de autenticación.

Retención de registros y archivado automático

- Los datos de registro de MFA se archivan automáticamente después de un año y están disponibles para su descarga desde la plataforma TrustLayer durante 12 meses más. Existen periodos de retención más largos.

GESTIÓN

Sincronización de usuarios

- El servicio de sincronización de Active Directory garantiza que los cambios en Active Directory se repliquen.

Interfaz web

- Totalmente integrado con la plataforma TrustLayer.

DESPLIEGUE

Backend

- Totalmente redundante, altamente escalable y 100 % basado en la nube, distribuido desde múltiples centros de datos ubicados en EE. UU., Reino Unido y Europa continental.

Clientes de autenticación

- Agentes fáciles de instalar implementados en servicios locales protegidos por MFA para conectarse al backend de la nube.