Módulo Profile

El **Módulo Profile** constituye el centro neurálgico del sistema ADO STS, proporcionando una plataforma integral para la gestión, monitoreo y análisis de casos de fraude. Este módulo centraliza todas las herramientas especializadas necesarias para combatir el fraude digital, integrando tecnologías avanzadas de biometría comportamental, inteligencia ambiental y análisis relacional.

Arquitectura del Módulo

El Módulo Profile está diseñado como una solución modular que permite a los analistas de seguridad acceder a diferentes funcionalidades especializadas desde una interfaz unificada:

- **Blocklist**: Sistema de prevención mediante listas de bloqueo
- **Fraud Cases**: Gestión activa de casos de fraude
- **Fraud History**: Análisis histórico y tendencias
- **Graph**: Visualización de análisis relacional
- **Change Password**: Gestión de credenciales de usuario

Blocklist

> **Blocklist** es un sistema de prevención proactivo que permite gestionar y mantener listas dinámicas de elementos identificados como fraudulentos o potencialmente riesgosos. Este módulo actúa como la primera línea de defensa del sistema, bloqueando automáticamente accesos desde fuentes conocidamente comprometidas, el módulo Blocklist implementa un sistema de filtrado multicapa que categoriza amenazas según diferentes vectores de ataque. Utiliza algoritmos de machine learning para actualizar automáticamente las listas de bloqueo basándose en patrones de comportamiento fraudulento detectados en tiempo real.

Categorías de Filtros Disponibles:

Filtro	Descripción	Aplicación
Phishing	Detecta elementos relacionados con ataques de suplantación de identidad	Bloqueo de dominios, IPs y patrones maliciosos
ATO Fraud	Account Takeover - Casos de toma de cuentas no autorizadas	Prevención de accesos desde dispositivos comprometidos
Remote Access Fraud	Fraudes ejecutados mediante acceso remoto no autorizado	Detección de herramientas de acceso remoto maliciosas
Cell Phone Theft	Dispositivos móviles reportados como robados	Bloqueo basado en IMEI y características del dispositivo

Filtro	Descripción	Aplicación
Confirmed Fraud Checked	Casos de fraude confirmados y verificados por analistas	Lista definitiva de elementos fraudulentos
Suspected Fraud Checked	Casos bajo investigación con alta probabilidad de fraude	Lista de elementos en observación
Digital Fraud	Fraudes digitales de naturaleza general	Patrones de comportamiento anómalo en transacciones
Social Engineering Fraud	Casos de manipulación psicológica para obtener información	Detección de patrones de ingeniería social
Session Is GPS Enabled	Control de sesiones con geolocalización activa	Validación de ubicación geográfica
Sim Swap	Casos de intercambio fraudulento de tarjetas SIM	Prevención de ataques de SIM swapping
Malware Fraud	Dispositivos infectados con software malicioso	Detección de firmas de malware y comportamiento anómalo
Is New Device	Dispositivos no reconocidos en el perfil del usuario	Control de acceso desde dispositivos nuevos
Is Owner Device	Verificación de propiedad legítima del dispositivo	Validación de autenticidad del propietario

Casos de Uso Principales:

- **Prevención Automatizada**: Bloqueo inmediato de amenazas conocidas sin intervención manual
- **Gestión de Riesgos**: Creación de políticas personalizadas de prevención según el perfil de riesgo
- **Inteligencia de Amenazas**: Mantenimiento de bases de datos actualizadas de vectores de ataque
- **Cumplimiento Regulatorio**: Documentación de medidas preventivas para auditorías

---

Fraud Cases

> **Fraud Cases** es el centro de comando para la gestión activa de casos de fraude, proporcionando herramientas completas para el seguimiento, investigación y resolución de incidentes de seguridad en tiempo real, este módulo implementa un sistema de gestión de casos (Case Management System) especializado en fraude, que permite la coordinación eficiente entre equipos de análisis, la priorización inteligente de casos y el seguimiento completo del ciclo de vida de cada incidente desde su detección hasta su resolución.

Dashboard de Alertas:

Métricas en Tiempo Real (24h):

- **Total Alerts**: Volumen total de alertas generadas
- **Assigned to Me**: Casos asignados al analista actual
- **Pending Alerts**: Casos pendientes de revisión
- **New Alerts**: Nuevas detecciones no procesadas
- **Confirmed Fraud**: Casos confirmados como fraudulentos

Estados de Clasificación:

Estado	Descripción	Acción Requerida
Confirmed Genuine	Actividad confirmada como legítima	Cierre de caso - Sin acción
New No Answer	Casos nuevos sin respuesta del usuario	Investigación adicional requerida
Reviewed	Casos revisados pendientes de decisión final	Escalamiento o cierre
Suspected Fraud	Alta probabilidad de actividad fraudulenta	Investigación profunda

Sistema de Tracking Completo:

- **CSID**: Identificador único de sesión de cliente
- **UID**: Identificador único de usuario
- **Brand**: Marca o entidad asociada al caso
- **Session Time**: Duración y timing de la sesión sospechosa
- **Actions**: Registro de acciones tomadas
- **Priority**: Nivel de prioridad asignado
- **Status**: Estado actual del caso

Filtros y Herramientas de Análisis:

- **Filtros Dinámicos**: New, Reason, User Group, Brand
- **Búsqueda Avanzada**: Por UID, dispositivo, ubicación
- **Análisis Temporal**: Created On, Last Update, Last Call Time
- **Clasificación Detallada**: Decision, Assigned To, Fraud Type, Report Type

Aplicaciones Operacionales:

- **Investigación Forense**: Análisis detallado de patrones de comportamiento sospechoso
- **Gestión de Workload**: Distribución eficiente de casos entre analistas
- **Escalamiento Automático**: Priorización basada en nivel de riesgo
- **Reporting Ejecutivo**: Generación de reportes para management
- **Coordinación de Respuesta**: Sincronización de acciones entre departamentos

---

Fraud History

> **Fraud History** mantiene un repositorio histórico completo y analítico de todos los casos de fraude procesados por el sistema, proporcionando capacidades avanzadas de análisis retrospectivo, identificación de tendencias y generación de inteligencia operacional. este módulo implementa un sistema de Business Intelligence especializado en seguridad, que transforma los datos históricos de fraude en insights accionables para la toma de decisiones estratégicas y la optimización continua de los sistemas de prevención.

Ventanas Temporales de Análisis:

Métricas Comparativas:

- **Past 24 Hours**: Análisis de actividad reciente y detección de patrones emergentes
- **Past 7 Days**: Tendencias semanales y variaciones operacionales
- **Past 30 Days**: Análisis mensual para planificación estratégica

Categorización Estadística:

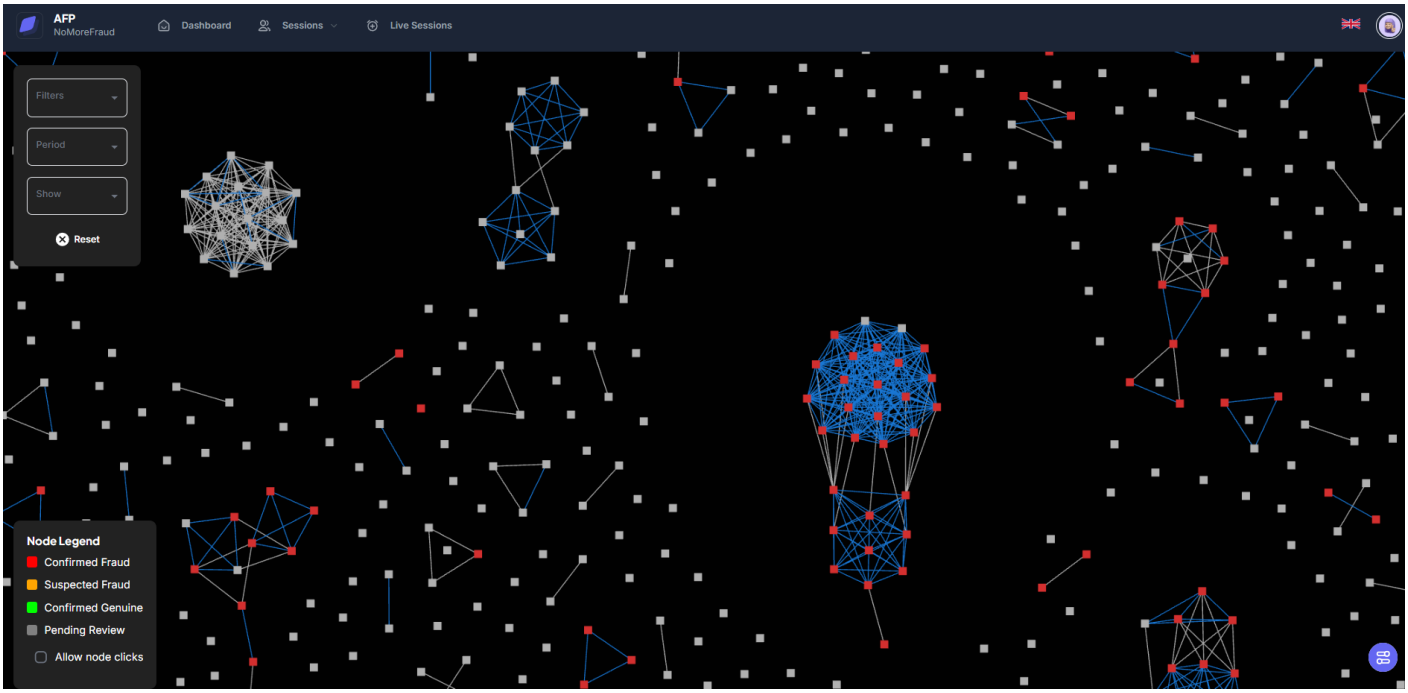
Métrica	Definición	Valor Estratégico
Total Cases	Volumen total de casos procesados	Indicador de carga operacional
Confirmed Fraud	Casos definitivamente fraudulentos	Tasa de efectividad de detección
Confirmed Genuine	Casos confirmados como legítimos	Medición de falsos positivos
Suspected Fraud	Casos en investigación	Pipeline de casos pendientes
No Answer	Casos sin respuesta del usuario	Métrica de engagement
New	Casos nuevos en el período	Tendencia de nuevas amenazas
Percent New Sessions	Porcentaje de sesiones nuevas	Indicador de crecimiento
Percent Approve	Tasa de aprobación	Eficiencia del sistema

Aplicaciones Analíticas:

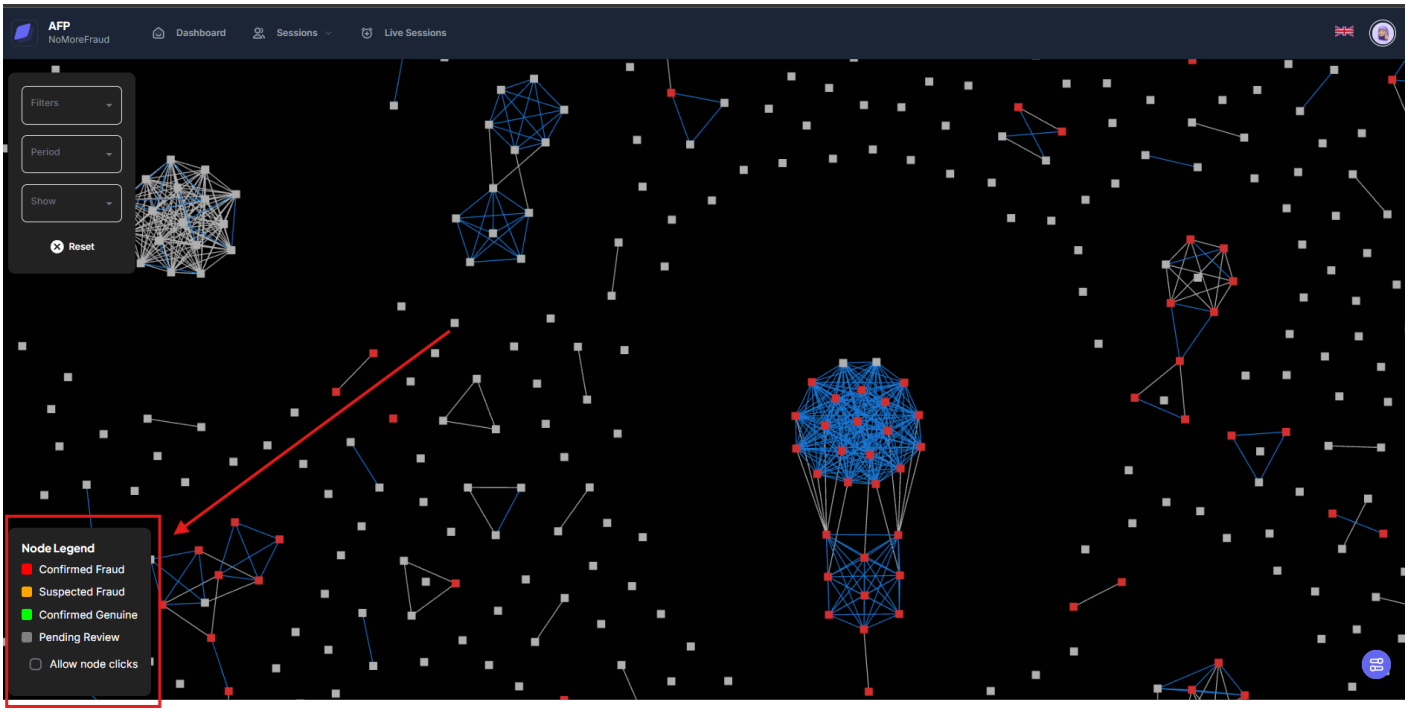
- **Trend Analysis**: Identificación de patrones temporales y estacionales
- **Performance Metrics**: Evaluación de efectividad de medidas preventivas
- **Predictive Analytics**: Modelado de tendencias futuras basado en datos históricos
- **Compliance Reporting**: Generación automatizada de reportes regulatorios
- **Risk Assessment**: Evaluación continua del landscape de amenazas
- **ROI Analysis**: Medición del retorno de inversión en medidas de seguridad

Graph

> **Graph** proporciona capacidades avanzadas de visualización y análisis relacional, transformando datos complejos de fraude en representaciones gráficas interactivas que revelan conexiones ocultas, patrones de comportamiento y estructuras de fraude organizadas, este módulo implementa tecnologías de análisis de grafos y network analysis para crear representaciones visuales multidimensionales de las relaciones entre entidades (usuarios, dispositivos, ubicaciones, redes). Utiliza algoritmos de clustering y detección de comunidades para identificar grupos de fraude coordinados y patrones de comportamiento anómalo.



Sistema de Visualización:



Node Legend (Leyenda de Nodos):

- **Confirmed Fraud**: Entidades confirmadas como fraudulentas
- **Suspected Fraud**: Entidades bajo sospecha de fraude
- **Confirmed Genuine**: Entidades verificadas como legítimas
- **Pending Review**: Entidades pendientes de clasificación

Tipos de Conexiones Relacionales:

Tipo de Relación	Descripción	Aplicación
User-Device	Vínculos entre usuarios y dispositivos	Detección de device sharing anómalo
Device-Network	Conexiones entre dispositivos y redes Wi-Fi	Análisis de ubicación y contexto
User-Location	Relaciones geográficas de usuarios	Detección de imposibilidad geográfica
Behavioral Patterns	Similitudes en patrones de comportamiento	Identificación de automatización
Network Infrastructure	Conexiones de infraestructura de red	Análisis de ISP y routing

Algoritmos de Análisis:

Algoritmo	Descripción	Aplicación Específica
Cluster Detection	Identificación automática de grupos relacionados	Agrupa entidades con comportamientos similares o conexiones frecuentes
Community Analysis	Detección de comunidades de fraude organizadas	Identifica redes estructuradas de fraude con múltiples participantes

Algoritmo	Descripción	Aplicación Específica
Centrality Measures	Identificación de nodos críticos en redes de fraude	Encuentra elementos centrales que coordinan actividades fraudulentas
Anomaly Detection	Detección de conexiones anómalas o sospechosas	Identifica relaciones inusuales que no siguen patrones normales
Temporal Analysis	Evolución de conexiones a lo largo del tiempo	Analiza cómo se desarrollan y cambian las relaciones fraudulentas

Casos de Uso Especializados:

Tipo de Análisis	Caso de Uso	Descripción Técnica	Indicadores de Fraude
Detección de Fraude Familiar	Múltiples usuarios - Mismo dispositivo	Análisis de patrones de uso compartido legítimo vs. fraudulento	Cambios drásticos en biometría comportamental, horarios de uso inconsistentes
Análisis de Ubicación Geográfica	Usuarios diferentes - Misma red Wi-Fi	Detección de call centers fraudulentos o farm operations	Alta concentración de usuarios sospechosos en misma ubicación física
Patrones de Dispositivos	Mismo comportamiento - Dispositivos diferentes	Identificación de automatización y bot networks	Biometría comportamental idéntica en múltiples dispositivos
Análisis de ISP y Infraestructura	Múltiples cuentas - Mismo proveedor	Detección de infraestructura compartida para operaciones fraudulentas	Clustering de actividad sospechosa por proveedor de internet

Herramientas Interactivas:

Herramienta	Funcionalidad	Beneficio Operacional
Filtros Temporales	Análisis por períodos específicos	Permite análisis histórico y identificación de patrones estacionales
Control de Visualización	Ajuste de profundidad y densidad del grafo	Optimiza la visualización según complejidad de la red analizada
Node Interaction	Exploración detallada mediante clicks en nodos	Facilita la investigación forense de entidades específicas
Export Capabilities	Generación de reportes visuales para presentaciones	Permite documentación y comunicación efectiva de hallazgos

Revision #5
Created 29 June 2025 02:41:38 by roger de avila
Updated 30 June 2025 14:48:28 by roger de avila