

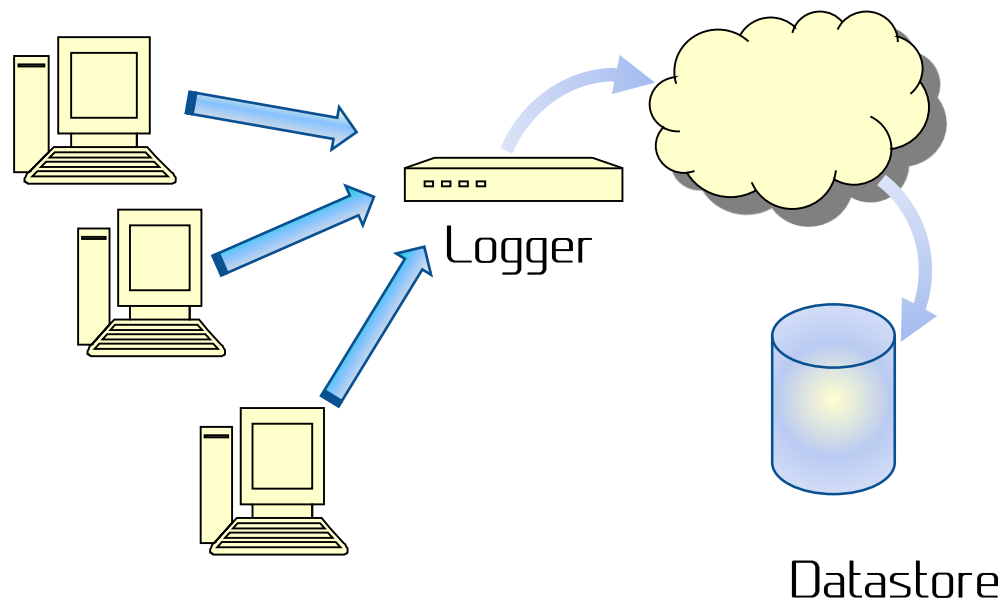
LegalLogger

La soluzione per il log management conforme al GDPR

Cosa è Legallogger?

Un sistema di
centralizzazione dei log orientato
al rispetto di quanto previsto
dal GDPR

NON E' UN SIEM



Cosa controlla LegalLogger

Controlla i seguenti eventi:

- L'accesso agli oggetti
- L'accesso al servizio Active Directory
- Login/Logout Utenti
- Access Base Dati
 - Oracle
 - MSSQL
 - MYSQL
 -
- Gli eventi di sistema
- La gestione degli account
- Inventario Hw&Sw della rete

Archivia e conserva

- colleziona i log
- li rende inalterabili con una marca temporale
- li invia cryptati ad un Server Centrale utilizzando un canale SSL



Cosa controlla LegalLogger

- SYSLOG priority/facility auth.info

FORTINET

0100032001/2/3/5/6/7/8/9/21

0100039424/25/26/36/37/38/47/48

0100043

WATCHGUARD

3E00-0002

3E00-0004

0207-0001

ORACLE

Oracle Audit

*Nix

All Session

EventID	Descrizione
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4776	The domain controller attempted to validate the credentials for an account
4777	The domain controller failed to validate the credentials for an account
4720	A user account was created
4726	A user account was deleted
4663	An attempt was made to access an object
4647	User initiated logoff
4659	A handle to an object was requested with intent to delete
4656	A handle to an object was requested
307	Printer
18453	MSSQLServer
1102	The audit log was cleared
6416	A new external device was recognized by the system.



Legal Logger: come lo fa ?

Tramite Agent (sistemi Windows)

L'agente installato sul sistema controllato (Server) registra gli eventi e li inoltra verso il collector

Il collector archivia i log all'interno di un database strutturato

Ogni 24 ore il Logger esporta i file di log in formato XML, li comprime e li firma

Senza Agent (Sistemi *nix)

Si usa il protocollo Syslog

Il collector archivia i log all'interno di un database strutturato

Ogni 24 ore il Logger esporta i file di log in formato XML, li comprime e li firma



Legal Logger: è sicuro ?

Ogni log è firmato localmente con un certificato rilasciato dalla Certification Authority centrale

Ogni log è marcato temporalmente tramite interfacciamento con il server Infocamere delle Camere di Commercio

Ogni log è inviato tramite Virtual Private Network SSL (RSA 2048 bit) al Datastore

Ogni log è archiviato su file system con un sistema di criptazione DSA 1024

Ogni log è accessibile solo tramite certificato X.509 personale

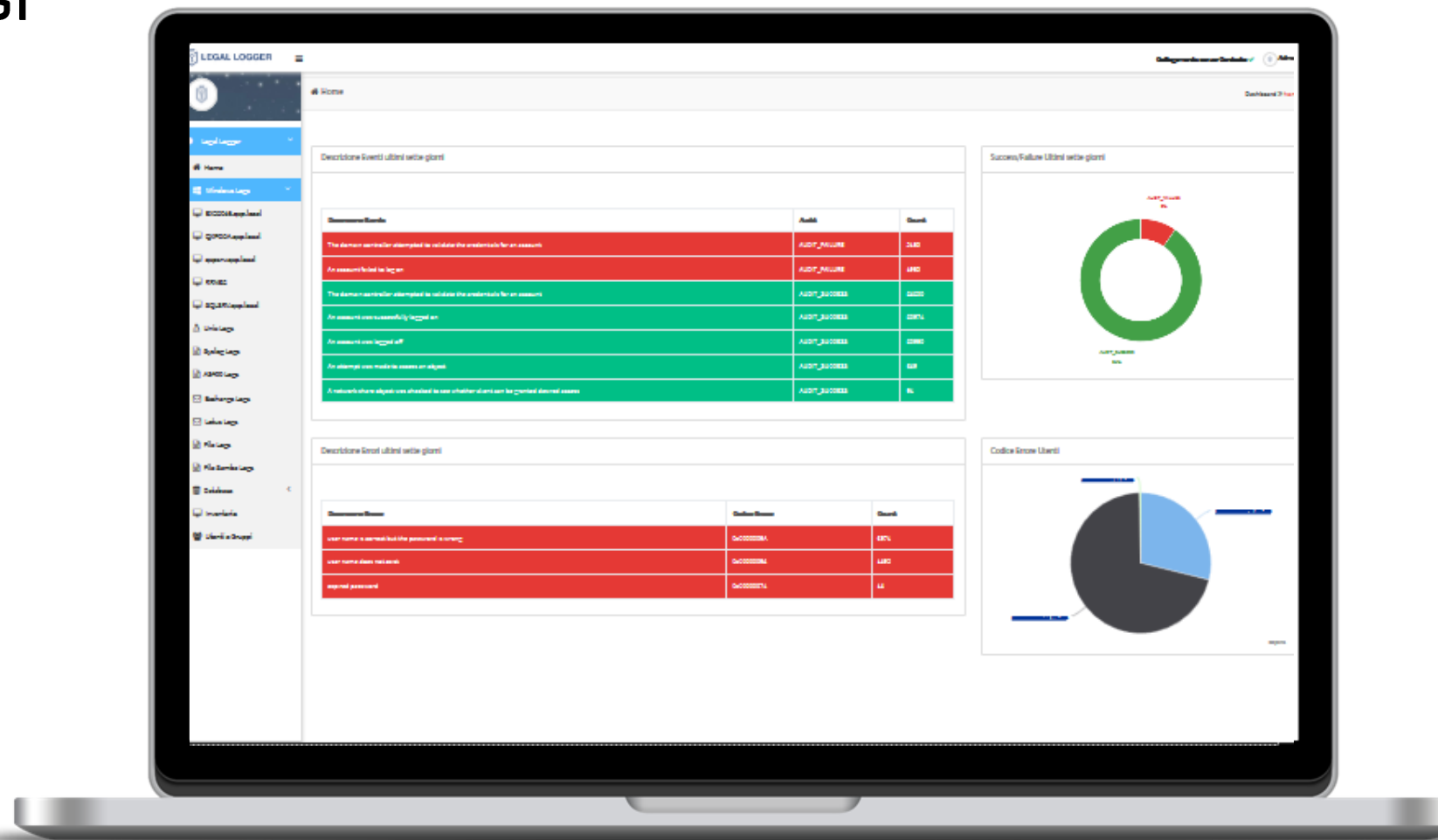
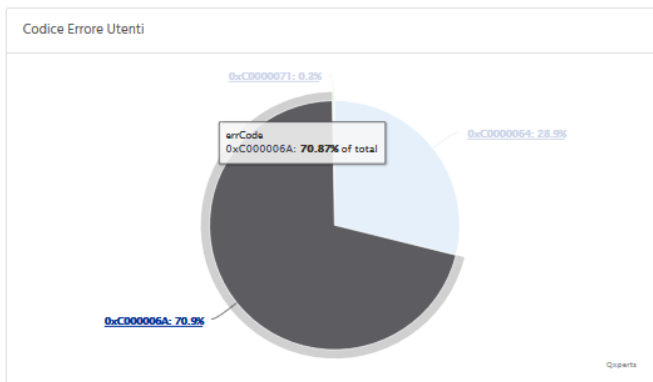
Il Datastore è composto da due server situati a grande distanza con replica dei dati in tempo reale (Cluster Geografico con GFS Global File System) garantendo così anche il Disaster Recovery in caso di eventi straordinari



Dashboard iniziale

Numero di accessi Success/Failure

Grafico interattivo





Dettaglio Log per Host

The screenshot shows the LEGAL LOGGER interface with a sidebar on the left containing navigation options like Home, Windows Logs, QXPDA, qpsrv, SQLSRV, Unix Logs, Syslog Logs, AS400 Logs, Active Directory Logs, Lotus Logs, File Logs, File Samba Logs, Database, and Inventario. The main content area displays a table of log entries for the host '0x35811a7d'. The table has columns for EventTime, Hostname, EventType, Action, Username, Source, and Dettagli. Two entries are visible:

EventTime	Hostname	EventType	Action	Username	Source	Dettagli
2019-10-10 08:37:46	qpsrv-app.local	AUDIT_SUCCESS	LogOff	gestoredc	0.0.0.0	
2019-10-10 08:36:14	qpsrv-app.local	AUDIT_SUCCESS	Login	gestoredc	172.30.3.12	

The screenshot shows the LEGAL LOGGER interface on a laptop screen. The dashboard displays summary statistics for the host 'qpsrv.qxp.local':

- Accessi Falliti: 9
- Totale Utenti: 4
- Totale Accessi: 1712

There is also a chart titled 'Utenti Accessi Falliti' showing a single data point for 'gestoredc'.

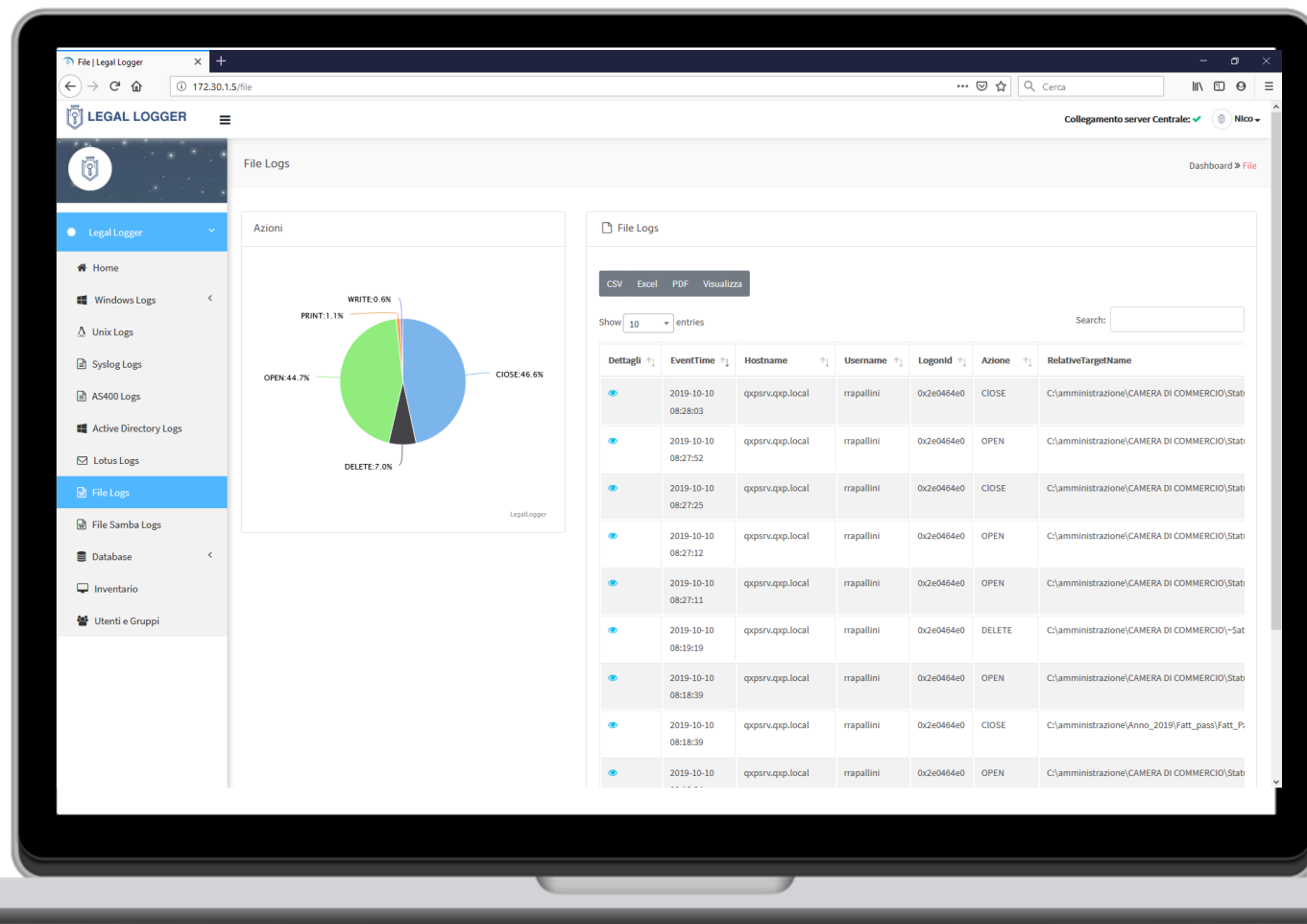
The 'Windows Logs' section is expanded, showing a table of log entries:

EventTime	EventType	EventId	Username	Source	LogonID	Dettagli
2019-10-10 08:37:46	4634	AUDIT_SUCCESS	gestoredc	0.0.0.0	0x35811a7d	
2019-10-10 08:36:14	4624	AUDIT_SUCCESS	gestoredc	172.30.3.12	0x35811a7d	
2019-10-10 08:36:14	4624	AUDIT_SUCCESS	gestoredc	172.30.3.12	0x35811aa2	
2019-10-10 08:36:14	4634	AUDIT_SUCCESS	gestoredc	0.0.0.0	0x35811aa2	
2019-10-10 08:14:37	4634	AUDIT_SUCCESS	rrapallini	0.0.0.0	0x35745977	



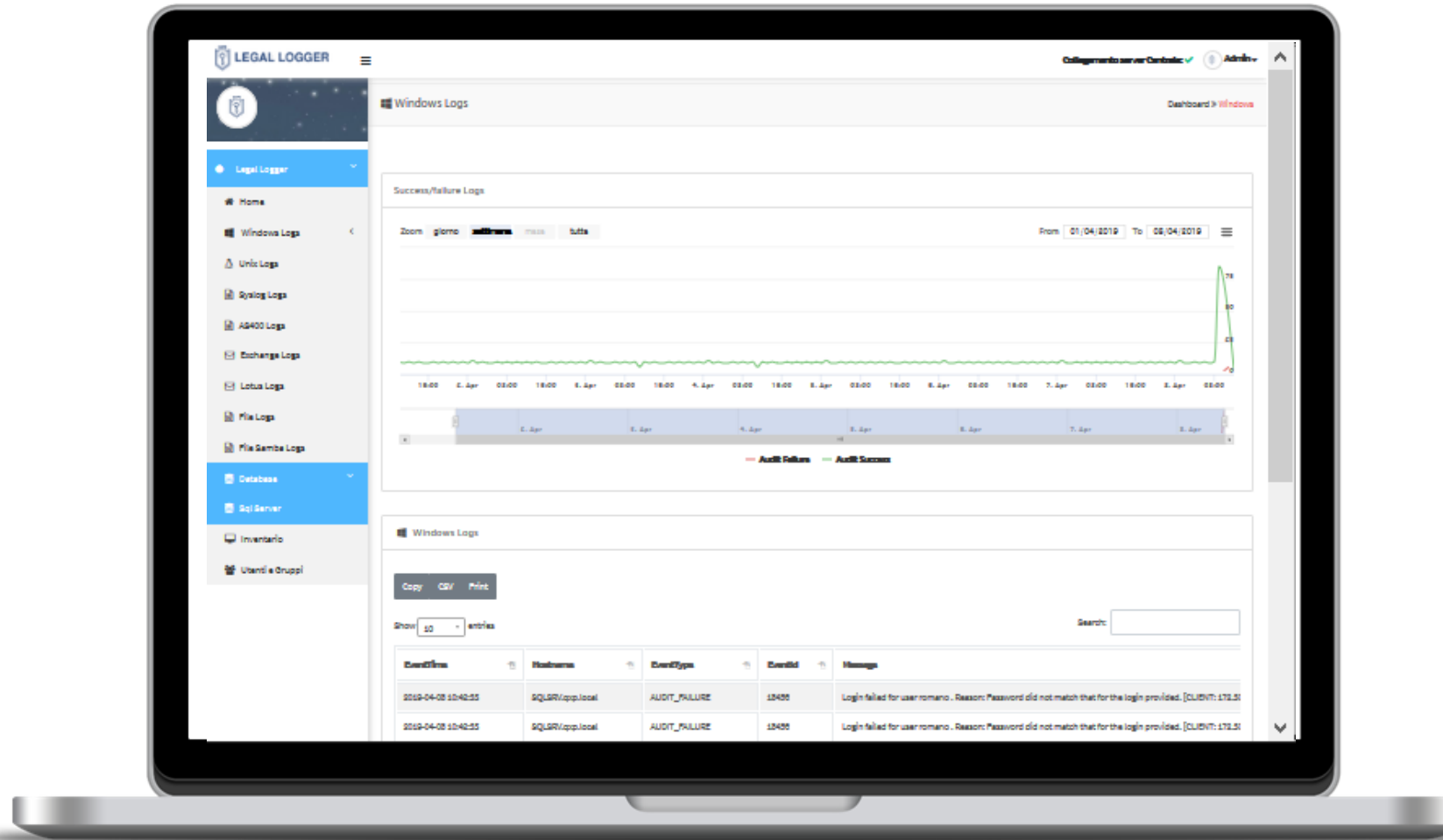
Dettaglio accesso alle condivisioni di rete con full path file e azione

- Open
- Write
- Close
- Delete
- Print



Dettgali Accessi alle Basi dati Aziendali
MSSQL
MYSQL
ORACLE

.....





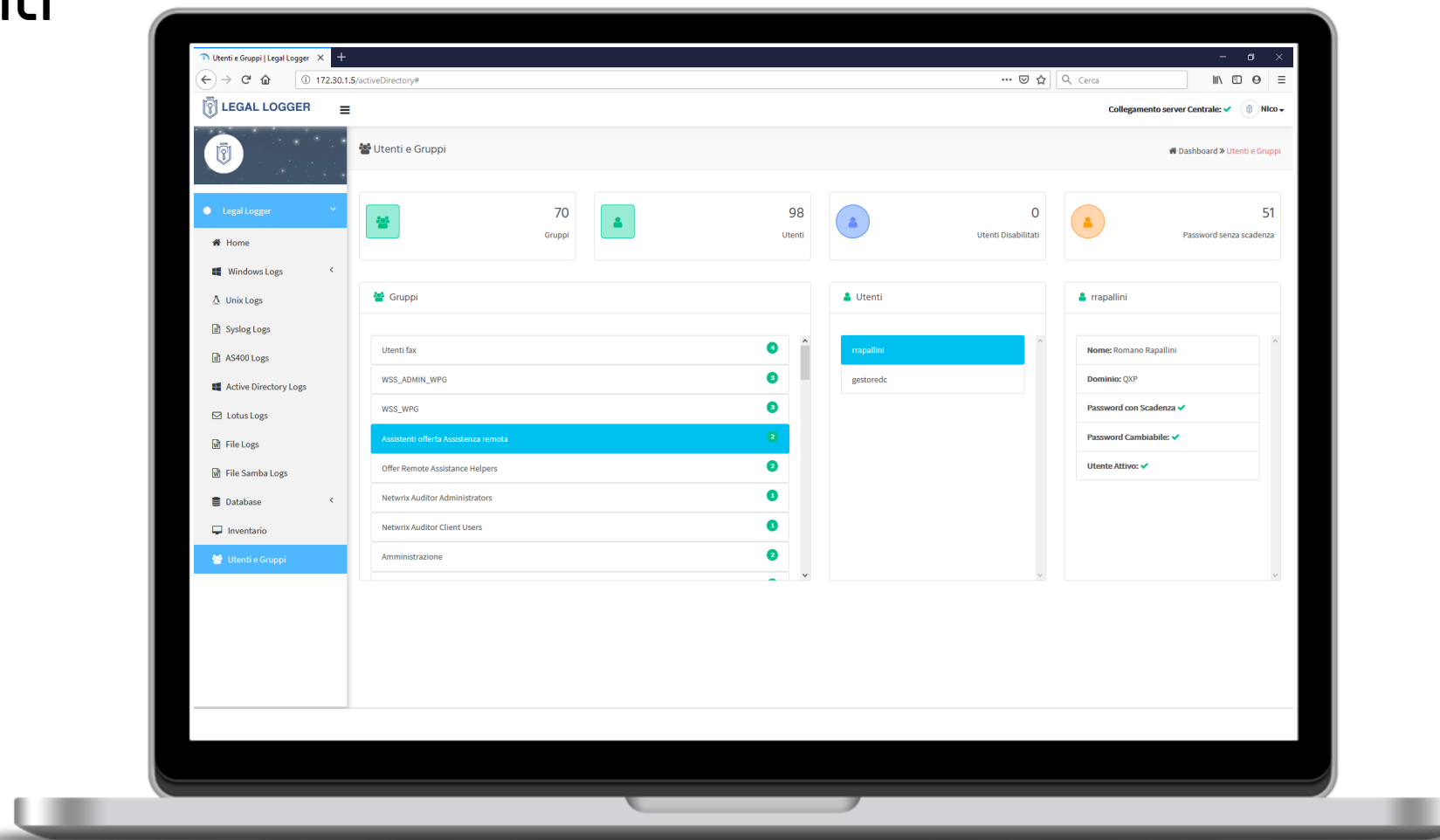
Struttura AD Utenti e Gruppi

Raccoglie le informazioni dal Domain Controller sugli account AD rilevando:

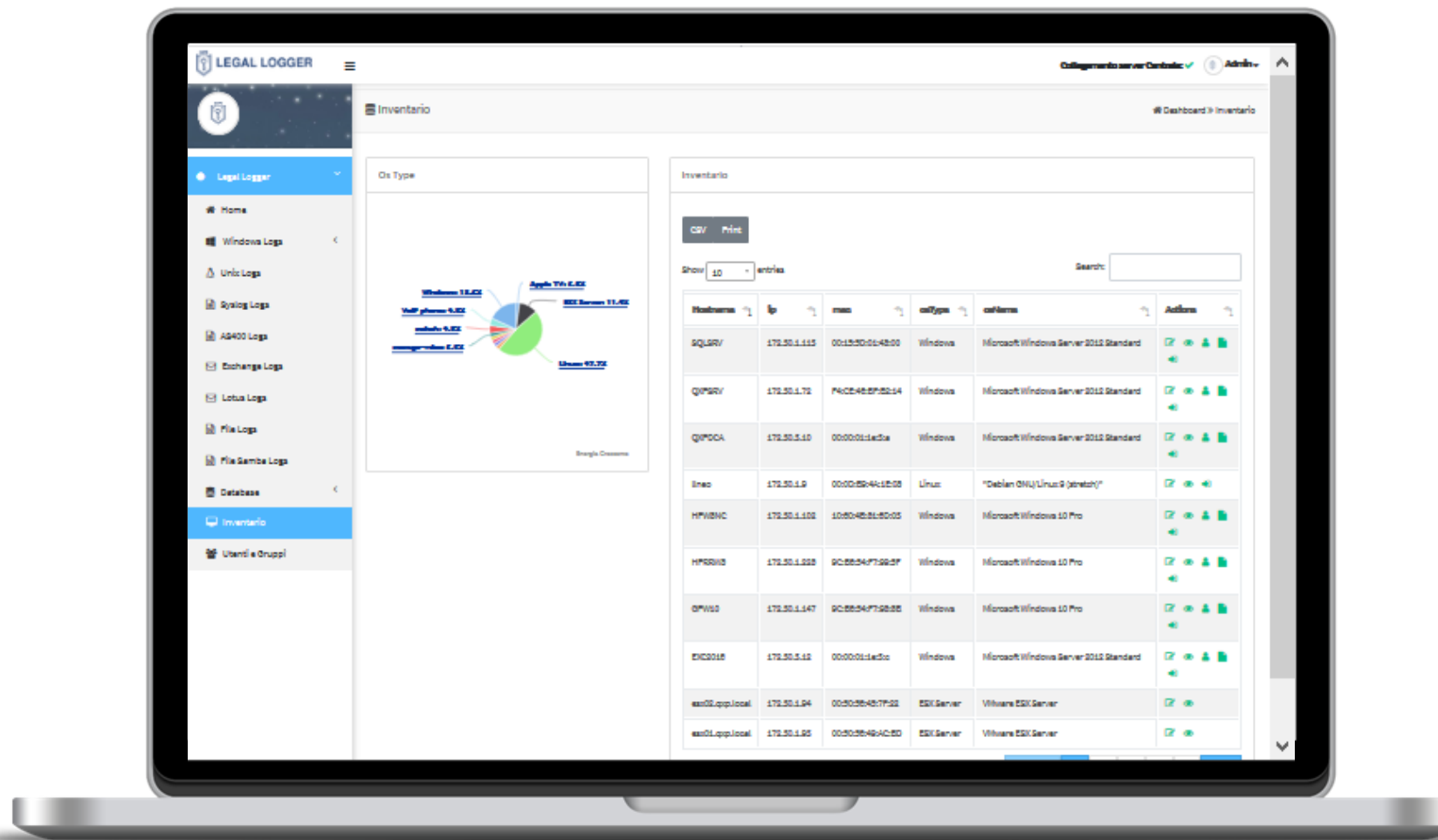
Gruppi/Utenti

Informazioni su utenti quali :

- Gruppo Appartenenza
- Password Con Scadenza
- Password cambiabile
- Utente Attivo

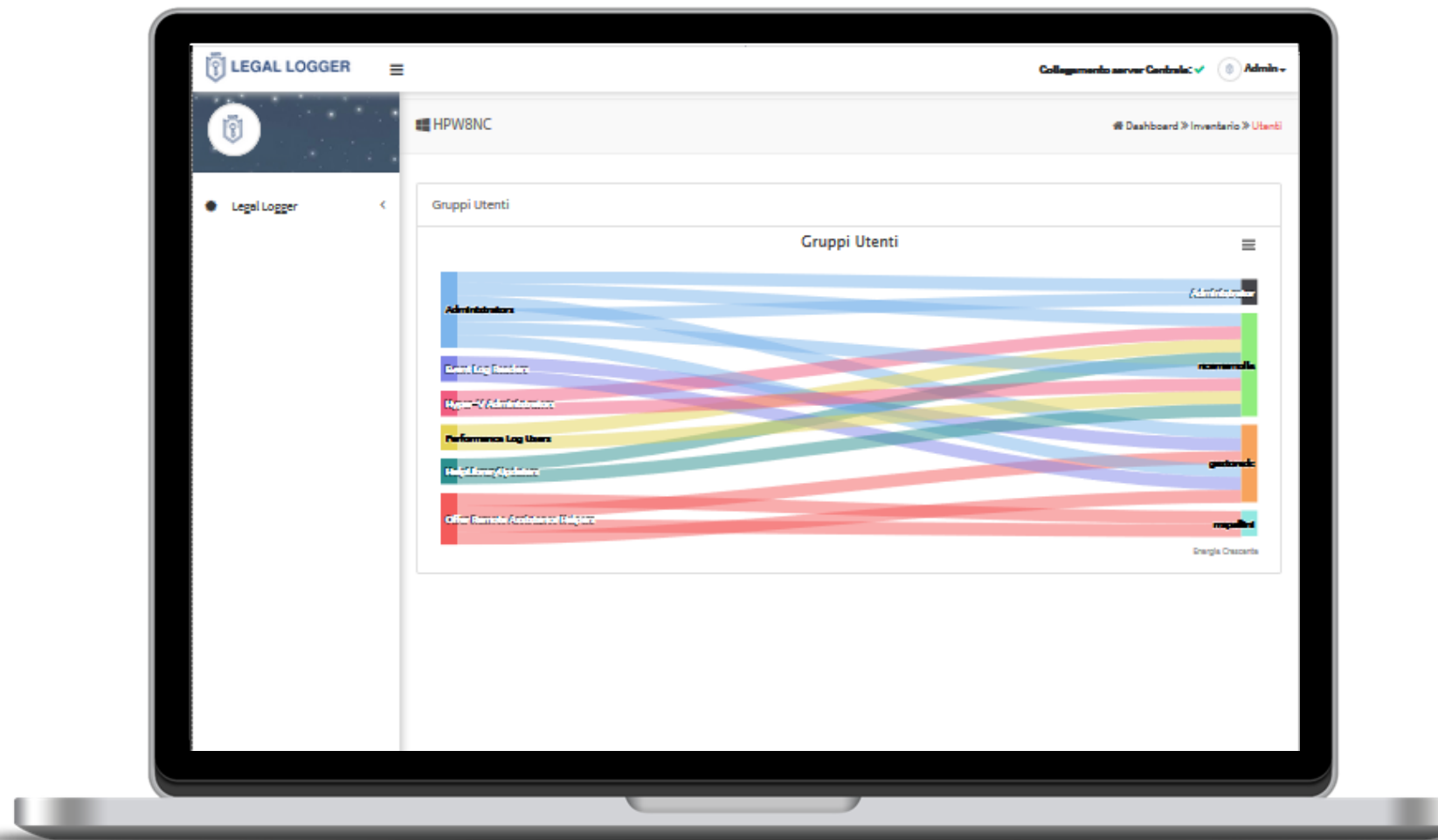


Inventory della Rete tramite WMI e rsh in ambiente *nix

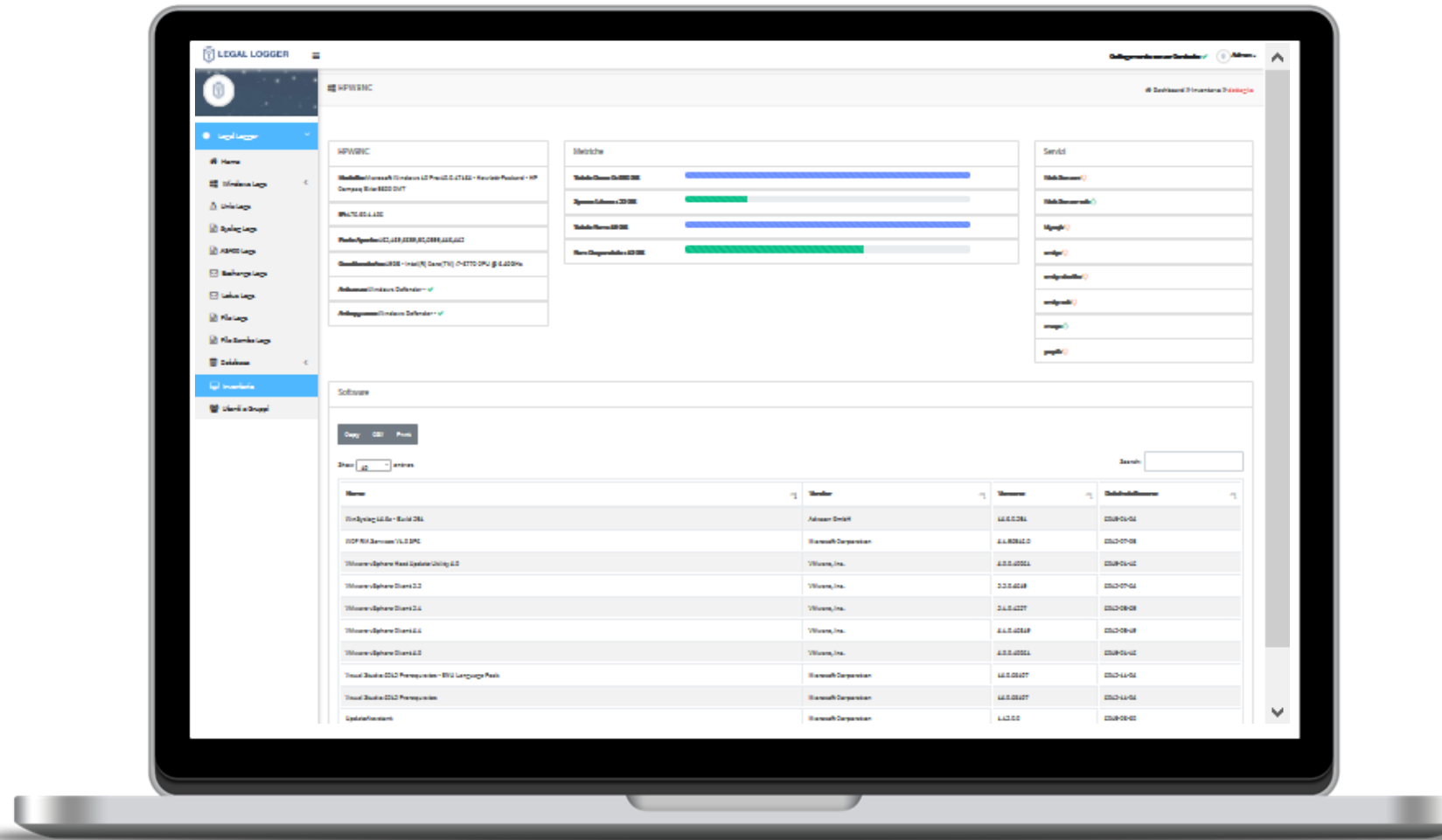




Controllo diritti Utente su singola Workstation



Dettaglio caratteristiche Hw e software installato



The screenshot displays the 'LEGAL LOGGER' interface for a device named 'HPV585C'. The interface is divided into several sections:

- Hardware Details:** A table listing various hardware components and their specifications.

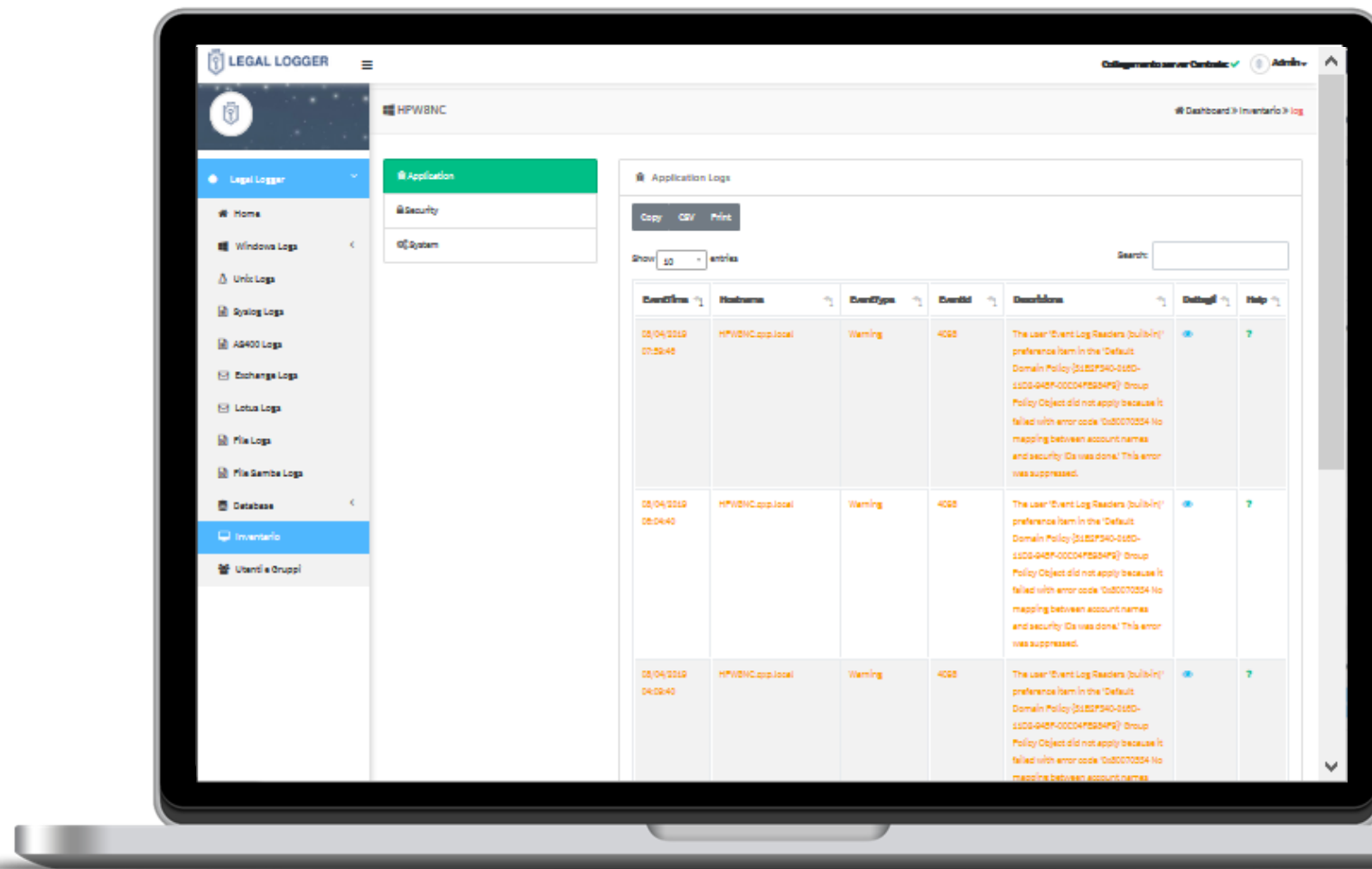
Component	Value
Modello/Processore/Windows ID/Processore/Versione/Modello/Chipset/BIOS/UEFI	HP Compaq Elite 8520 D177
Modello/ID/UEFI	HP/7C/83/4/32
Processore/Modello/ID/UEFI/Processore/Modello/ID/UEFI	Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz
Adattatore/Modello/Modello/ID/UEFI	Adattatore/Modello/Modello/ID/UEFI
Adattatore/Modello/Modello/ID/UEFI	Adattatore/Modello/Modello/ID/UEFI
- Memorie:** A section showing memory usage with progress bars for 'Totale Memoria Usata', 'Spazio Libero', 'Totale Memoria', and 'Mem. Dispositivo'.

Category	Usage
Totale Memoria Usata	~80%
Spazio Libero	~20%
Totale Memoria	~100%
Mem. Dispositivo	~80%
- Software:** A table listing installed software applications.

Nome	Vendor	Versione	Installato/Disinstallato
WinSxss 6.0 - Build 761	Adrian Smith	6.0.6.0.1	03/09/2014
PDF Kit Services 16.0 SP0	Harworth Corporation	16.0.0.0.0	03/09/2014
Willware-Sphere Host Update Utility 6.0	Willware, Inc.	6.0.0.0.0	03/09/2014
Willware-Sphere Drivers 2.0	Willware, Inc.	2.0.0.0.0	03/09/2014
Willware-Sphere Drivers 2.0	Willware, Inc.	2.0.0.0.0	03/09/2014
Willware-Sphere Drivers 6.0	Willware, Inc.	6.0.0.0.0	03/09/2014
Willware-Sphere Drivers 6.0	Willware, Inc.	6.0.0.0.0	03/09/2014
Visual Studio 2012 Perceptron - EU Language Pack	Harworth Corporation	11.0.0.0.0	03/09/2014
Visual Studio 2012 Perceptron	Harworth Corporation	11.0.0.0.0	03/09/2014
UpdateFramework	Harworth Corporation	1.0.0.0.0	03/09/2014



Tramite accesso WMI è possibile leggere Eventi anche in modalità agentless





Report Giornalieri

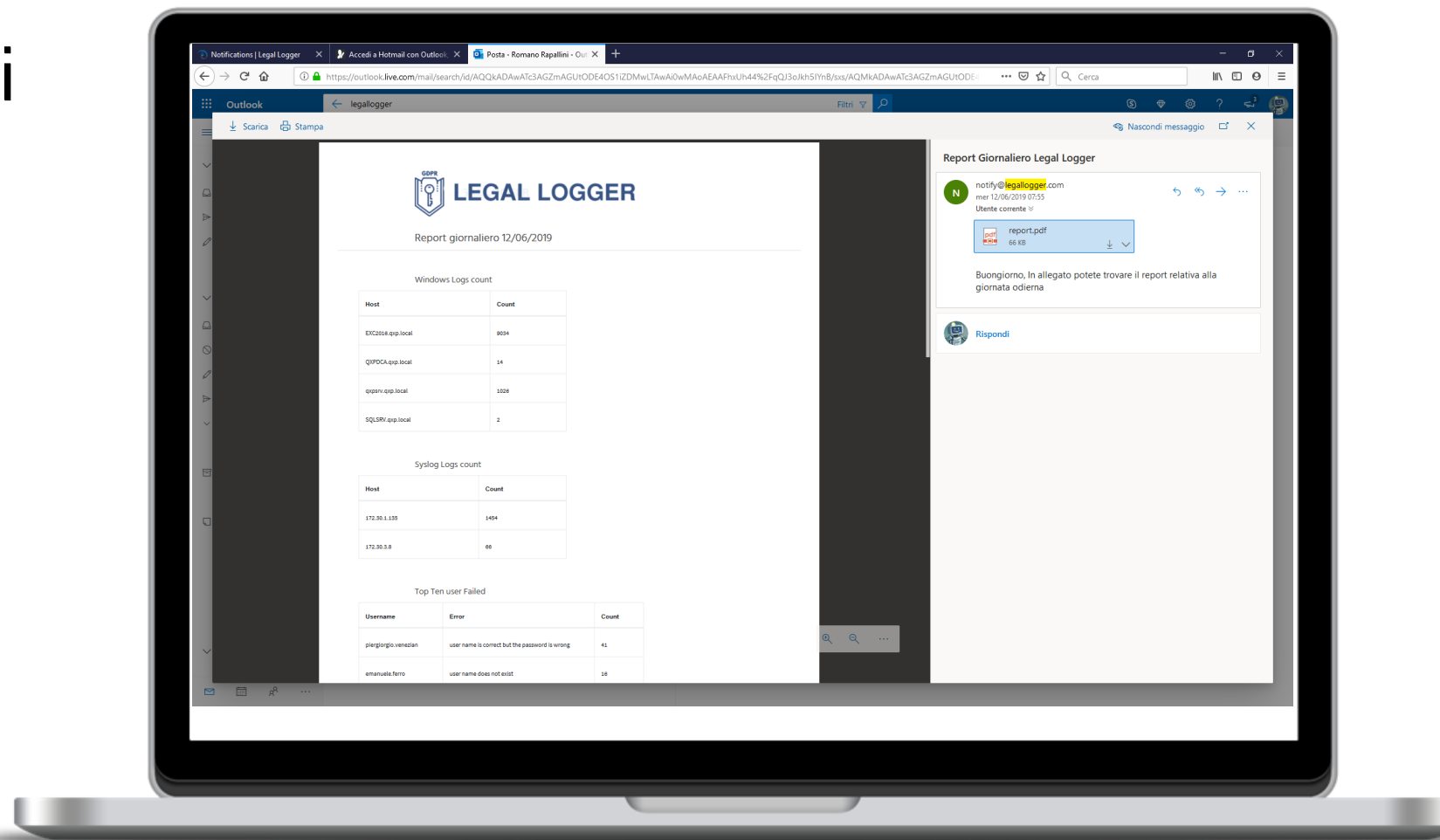
Report riepilogativo

Numero Eventi registrati

Server con Agent Attivi

Server Syslog Attivi

Top user fail

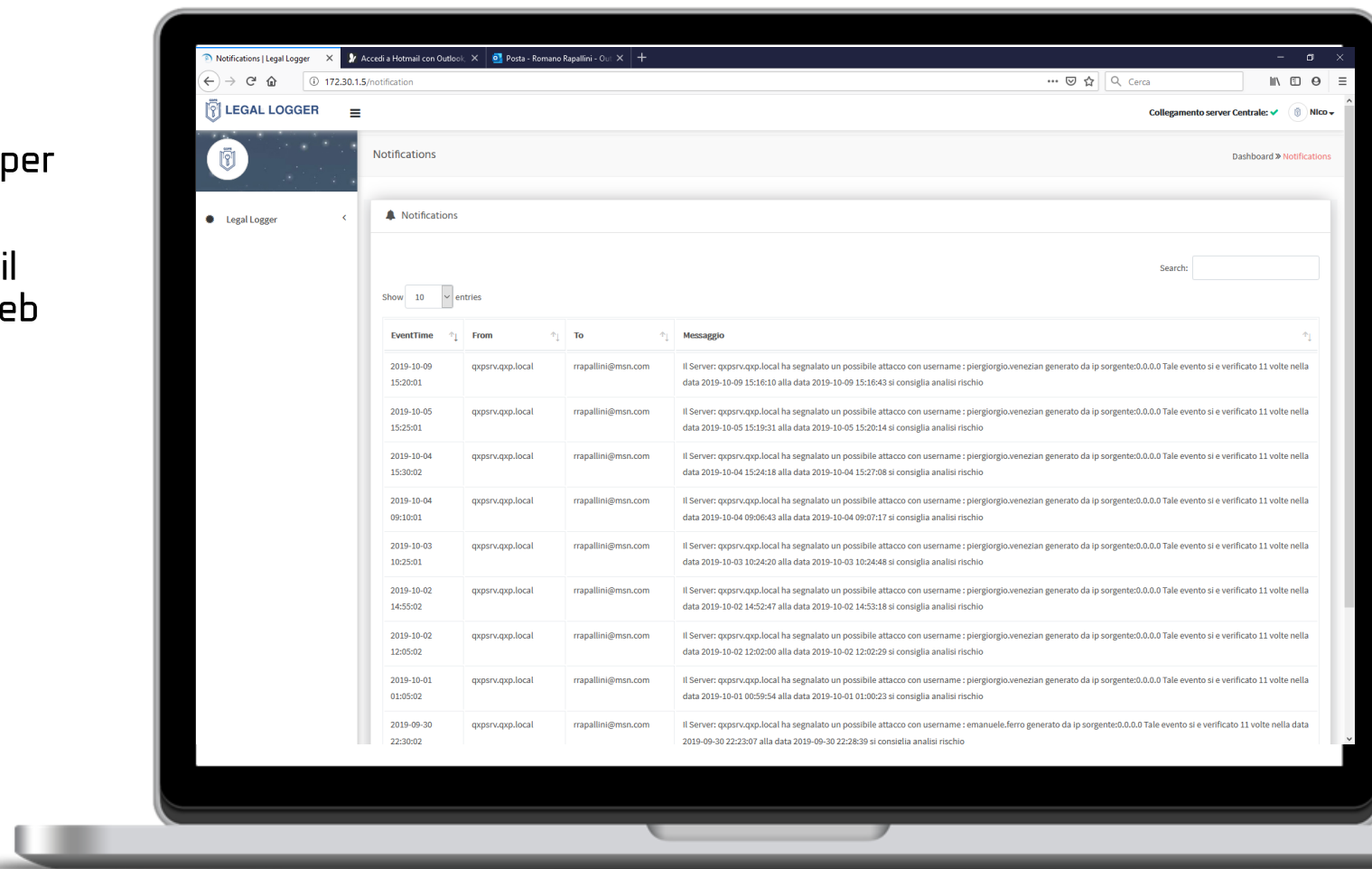




Allert in tempo Reale

Vengono inviati allert in tempo reale per tentativi di attacco Brute Force

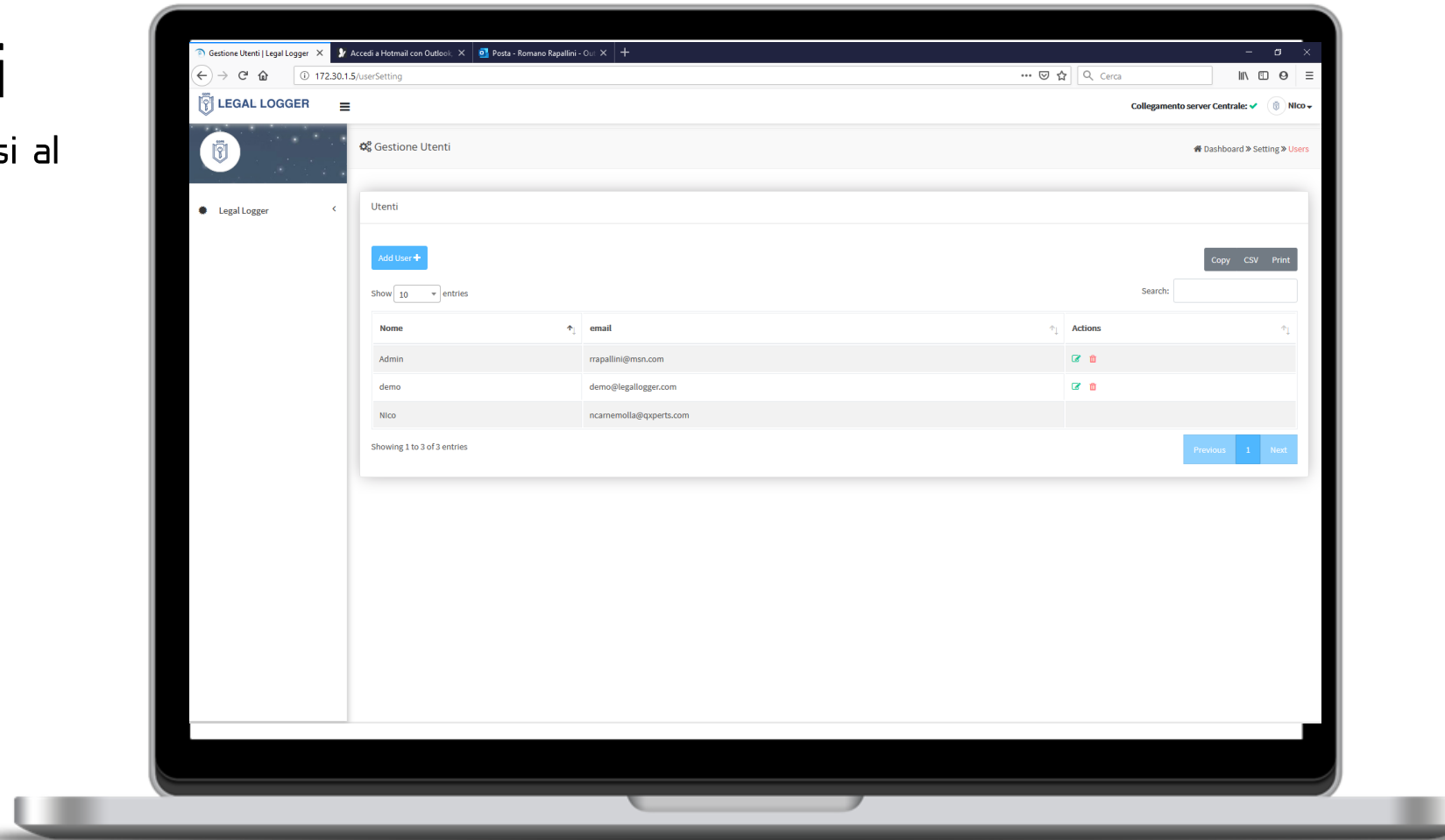
Le segnalazioni vengo inviate via Mail con registro delle segnalazioni via Web



Gestione accessi

È possibile configurare diversi accessi al sistema per

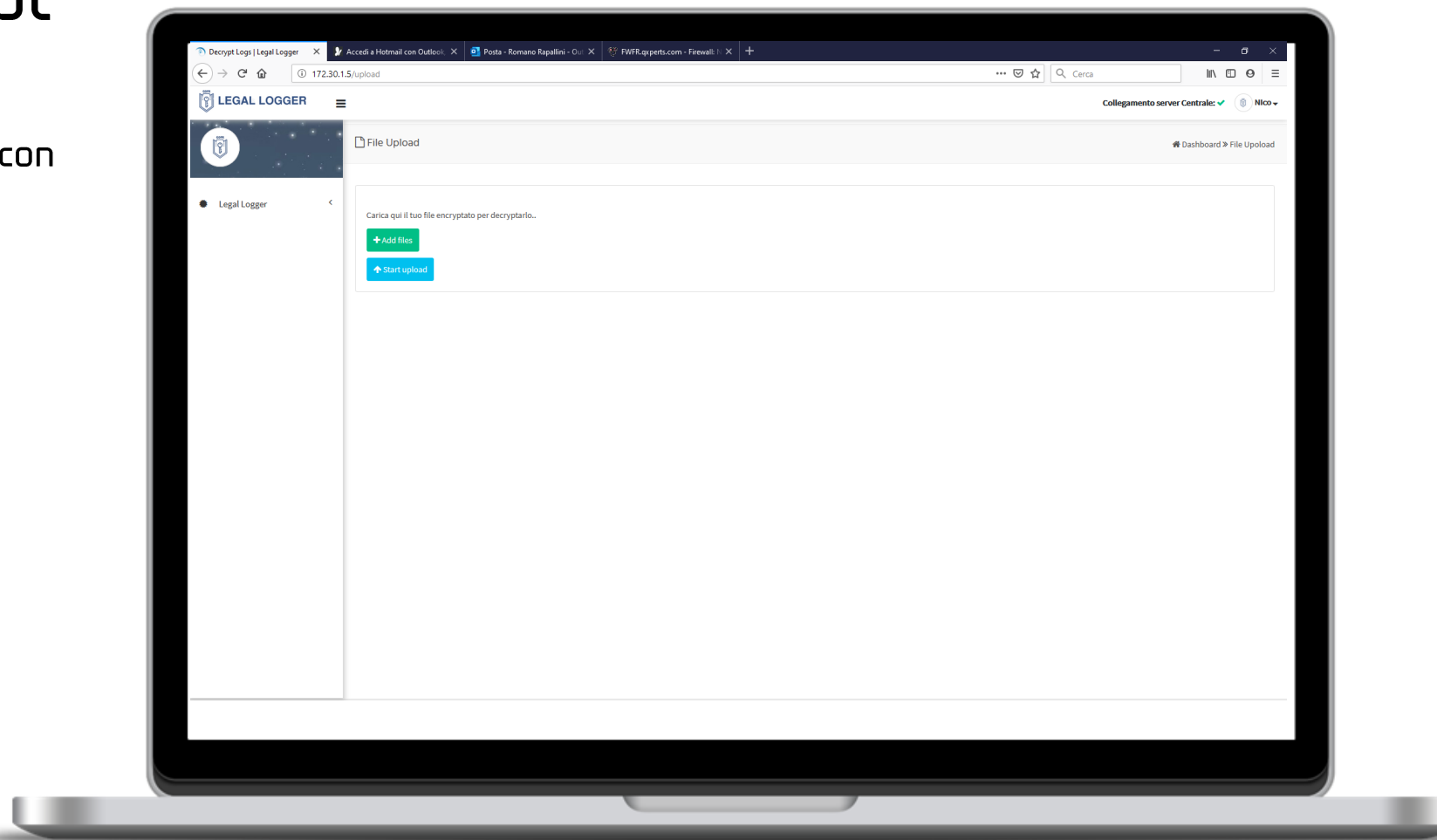
- amministratori
- auditor
- Ogni accesso è registrato



Funzione di decrypt LOG

I log archiviati in cloud sono cryptati con chiave privata.

Per poterli visualizzare è necessario caricarli





- Sviluppo Plugin Custom

Plugin Disponibili

- Salesforce
- Google For Works