



SEVIO

Audit

Document ID: audit_it_v_25_01

<https://sevio.it/>



Note legali

Il contenuto di questo documento è fornito nello stato in cui si trova. Non vengono fornite garanzie di alcun tipo relative al contenuto. Sevio si riserva il diritto di rivedere questo documento o ritirarlo in qualsiasi momento senza alcun preavviso.

In nessun caso Sevio sarà responsabile per qualsiasi perdita di dati o di reddito o per qualsiasi danno speciale, incidentale e consequenziale o indiretto, in qualsiasi modo causato.

Ulteriori informazioni su Sevio sono disponibili al seguente indirizzo Internet: <https://sevio.it/>.

Revisioni

Revisioni	Data	Descrizione
25_01	02/01/2025	Emissione

Indice

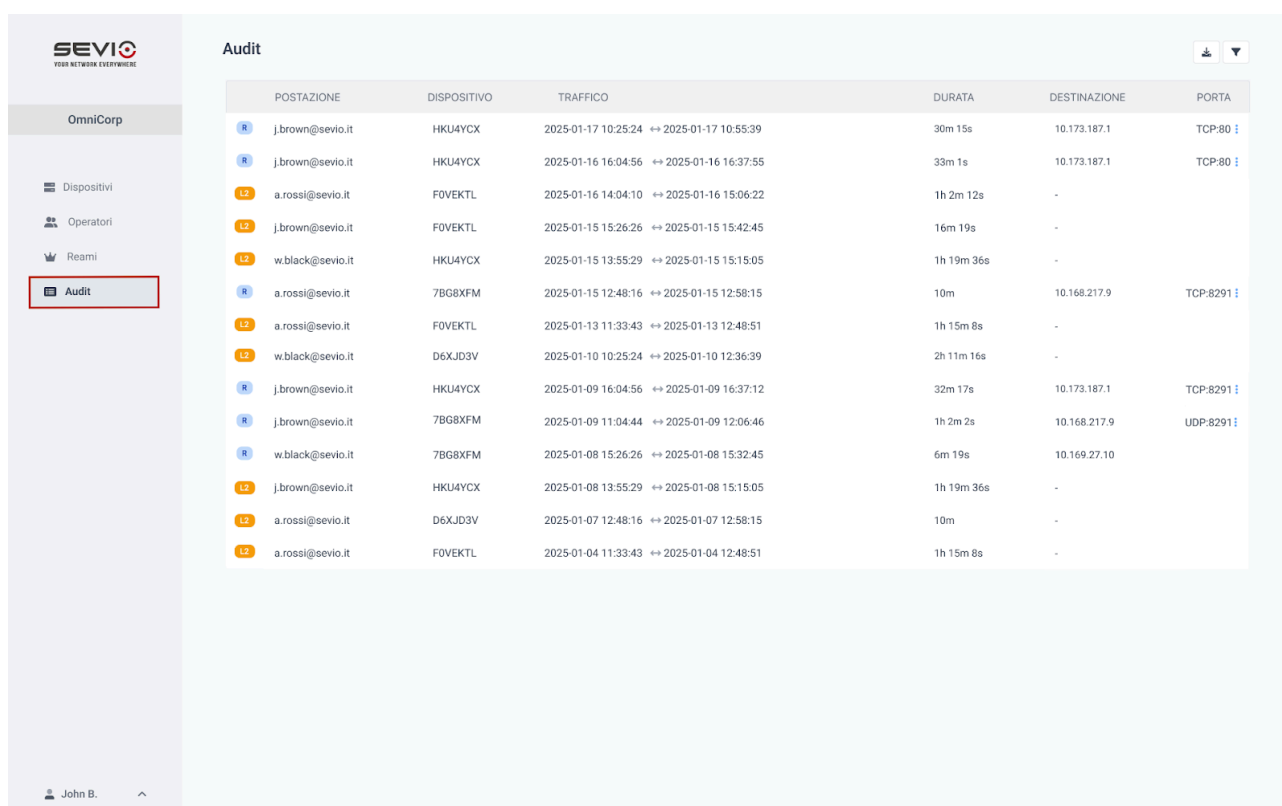
Descrizione generale	4
Action Bar	5
Esportazione dei Dati.....	5
Filtri di Ricerca.....	5
Lista Audit	6
Normalizzazione dei Dati	7
Storico delle Sessioni	7

Descrizione generale

La sezione Audit è stata progettata per offrire un tracciamento dettagliato delle sessioni di accesso ai Dispositivi, tramite connessioni di tipo VPN Realm e VPN L2.

Questa funzionalità consente di monitorare le attività di ciascuna Postazione verso i Sevio Router associati, garantendo un controllo efficace e una maggiore trasparenza sugli accessi.

La sezione Audit è accessibile dagli Utenti Owner e Admin.



The screenshot displays the SEVIO Audit interface. On the left is a navigation sidebar with the SEVIO logo and menu items: OmniCorp, Dispositivi, Operatori, Reami, and Audit (highlighted with a red box). The main area shows a table titled 'Audit' with columns: POSTAZIONE, DISPOSITIVO, TRAFFICO, DURATA, DESTINAZIONE, and PORTA. The table contains 16 rows of session data.

POSTAZIONE	DISPOSITIVO	TRAFFICO	DURATA	DESTINAZIONE	PORTA
j.brown@sevio.it	HKU4YCX	2025-01-17 10:25:24 ↔ 2025-01-17 10:55:39	30m 15s	10.173.187.1	TCP:80
j.brown@sevio.it	HKU4YCX	2025-01-16 16:04:56 ↔ 2025-01-16 16:37:55	33m 1s	10.173.187.1	TCP:80
a.rossi@sevio.it	FOVEKTL	2025-01-16 14:04:10 ↔ 2025-01-16 15:06:22	1h 2m 12s	-	-
j.brown@sevio.it	FOVEKTL	2025-01-15 15:26:26 ↔ 2025-01-15 15:42:45	16m 19s	-	-
w.black@sevio.it	HKU4YCX	2025-01-15 13:55:29 ↔ 2025-01-15 15:15:05	1h 19m 36s	-	-
a.rossi@sevio.it	7BG8XFM	2025-01-15 12:48:16 ↔ 2025-01-15 12:58:15	10m	10.168.217.9	TCP:8291
a.rossi@sevio.it	FOVEKTL	2025-01-13 11:33:43 ↔ 2025-01-13 12:48:51	1h 15m 8s	-	-
w.black@sevio.it	D6XJD3V	2025-01-10 10:25:24 ↔ 2025-01-10 12:36:39	2h 11m 16s	-	-
j.brown@sevio.it	HKU4YCX	2025-01-09 16:04:56 ↔ 2025-01-09 16:37:12	32m 17s	10.173.187.1	TCP:8291
j.brown@sevio.it	7BG8XFM	2025-01-09 11:04:44 ↔ 2025-01-09 12:06:46	1h 2m 2s	10.168.217.9	UDP:8291
w.black@sevio.it	7BG8XFM	2025-01-08 15:26:26 ↔ 2025-01-08 15:32:45	6m 19s	10.169.27.10	-
j.brown@sevio.it	HKU4YCX	2025-01-08 13:55:29 ↔ 2025-01-08 15:15:05	1h 19m 36s	-	-
a.rossi@sevio.it	D6XJD3V	2025-01-07 12:48:16 ↔ 2025-01-07 12:58:15	10m	-	-
a.rossi@sevio.it	FOVEKTL	2025-01-04 11:33:43 ↔ 2025-01-04 12:48:51	1h 15m 8s	-	-

Action Bar

📄 Esportazione dei Dati

Consente di scaricare il file .csv contenente dati relativi al Dispositivo, all'Operatore, alla Postazione, alla durata delle sessioni, al tipo di VPN utilizzato, all'IP di destinazione e alle Porte.

OmniCorp

VPN	Dispositivo	Nome dispositivo	Postazione	Operatore	Data di inizio	Data di fine	Durata(s)	IP destinazione	Porte
Realm	HKU4YCX	Plant - R600	j.brown@sevio.it	John Brown	2025-1-17 10:25:24	2025-1-17 10:55:39	1815	10.173.187.1	TCP: 80
Realm	HKU4YCX	Plant - R600	j.brown@sevio.it	John Brown	2025-1-16 16:04:56	2025-1-16 16:37:55	1980	10.173.187.1	TCP: 80
L2	F0VEKTL	Plant - R200	a.rossi@sevio.it	Andrea Rossi	2025-1-16 14:04:10	2025-1-16 15:06:22	3732		
L2	F0VEKTL	Plant - R200	j.brown@sevio.it	John Brown	2025-1-15 15:26:26	2025-1-15 15:42:45	979		
L2	HKU4YCX	Plant - R600	w.black@sevio.it	William Black	2025-1-15 13:55:29	2025-1-15 15:15:05	4776		
Realm	7BG8XFM	Plant - R200	a.rossi@sevio.it	Andrea Rossi	2025-1-15 12:48:16	15/01/2025 12:58:16	600	10.168.217.9	TPC: 8291
L2	F0VEKTL	Plant - R200	a.rossi@sevio.it	Andrea Rossi	2025-1-13 11:33:43	2025-1-13 12:48:51	4508		
L2	D6XJD3V	Plant - R600	w.black@sevio.it	William Black	2025-1-10 10:25:24	2025-1-10 12:36:39	7875		
Realm	HKU4YCX	Plant - R600	j.brown@sevio.it	John Brown	2025-1-9 16:04:56	2025-1-9 16:37:12	2036	10.173.187.1	TPC: 8291
Realm	7BG8XFM	Plant - R200	j.brown@sevio.it	John Brown	2025-1-9 11:04:44	2025-1-9 12:06:46	3612	10.168.217.9	UDP:8291
Realm	7BG8XFM	Plant - R200	w.black@sevio.it	William Black	2025-1-8 15:26:26	2025-1-8 15:32:45	372	10.169.27.10	
L2	HKU4YCX	Plant - R600	j.brown@sevio.it	John Brown	2025-1-8 13:55:29	2025-1-8 15:15:05	4776		
L2	D6XJD3V	Plant - R600	a.rossi@sevio.it	Andrea Rossi	2025-1-7 12:48:16	2025-1-7 12:58:15	600		
L2	F0VEKTL	Plant - R200	a.rossi@sevio.it	Andrea Rossi	2025-1-4 11:33:43	2025-1-4 12:48:51	4508		

🔍 Filtri di ricerca

Gli Utenti hanno la possibilità di applicare diversi filtri per perfezionare la ricerca dei dati:

- **Data** - per visualizzare le sessioni all'interno di un intervallo di date specifico.
- **Postazione** - per selezionare i risultati in base alla Postazione.
- **Service Tag** - per individuare rapidamente le sessioni relative ad un Dispositivo.
- **Traffico** - per filtrare i risultati in base allo stato di inizio e di fine delle sessioni.

Filtro ✕

Service Tag

Postazione

Da

A

Lista Audit

	POSTAZIONE	DISPOSITIVO	TRAFFICO	DURATA	DESTINAZIONE	PORTA
R	j.brown@sevio.it	HKU4YCX	2025-01-17 10:25:24 ↔ 2025-01-17 10:55:39	30m 15s	10.173.187.1	TCP:80 ⓘ
R	j.brown@sevio.it	HKU4YCX	2025-01-16 16:04:56 ↔ 2025-01-16 16:37:55	33m 1s	10.173.187.1	TCP:80 ⓘ
L2	a.rossi@sevio.it	F0VEKTL	2025-01-16 14:04:10 ↔ 2025-01-16 15:06:22	1h 2m 12s	-	
L2	j.brown@sevio.it	F0VEKTL	2025-01-15 15:26:26 ↔ 2025-01-15 15:42:45	16m 19s	-	
L2	w.black@sevio.it	HKU4YCX	2025-01-15 13:55:29 ↔ 2025-01-15 15:15:05	1h 19m 36s	-	
R	a.rossi@sevio.it	7BG8XFM	2025-01-15 12:48:16 ↔ 2025-01-15 12:58:15	10m	10.168.217.9	TCP:8291 ⓘ
L2	a.rossi@sevio.it	F0VEKTL	2025-01-13 11:33:43 ↔ 2025-01-13 12:48:51	1h 15m 8s	-	
L2	w.black@sevio.it	D6XJD3V	2025-01-10 10:25:24 ↔ 2025-01-10 12:36:39	2h 11m 16s	-	
R	j.brown@sevio.it	HKU4YCX	2025-01-09 16:04:56 ↔ 2025-01-09 16:37:12	32m 17s	10.173.187.1	TCP:8291 ⓘ
R	j.brown@sevio.it	7BG8XFM	2025-01-09 11:04:44 ↔ 2025-01-09 12:06:46	1h 2m 2s	10.168.217.9	UDP:8291 ⓘ
R	w.black@sevio.it	7BG8XFM	2025-01-08 15:26:26 ↔ 2025-01-08 15:32:45	6m 19s	10.169.27.10	
L2	j.brown@sevio.it	HKU4YCX	2025-01-08 13:55:29 ↔ 2025-01-08 15:15:05	1h 19m 36s	-	
L2	a.rossi@sevio.it	D6XJD3V	2025-01-07 12:48:16 ↔ 2025-01-07 12:58:15	10m	-	
L2	a.rossi@sevio.it	F0VEKTL	2025-01-04 11:33:43 ↔ 2025-01-04 12:48:51	1h 15m 8s	-	

Connessione: indica la tipologia di connessione utilizzata.

- R (Realm) - monitora l'accesso effettivo al Dispositivo.
- L2 - registra il traffico verso un Dispositivo specifico.

Postazione: identifica la Postazione che ha effettuato l'accesso. Cliccando su questo parametro sono visibili ulteriori dettagli relativi all'Operatore associato alla Postazione.

Dispositivo: codice univoco (Service Tag) del Dispositivo a cui si è collegata la Postazione. Cliccando sul Service Tag sono visibili i parametri del Router.

Traffico: visualizza l'intervallo temporale della sessione, dalla data e ora di inizio a quella di fine. Se la sessione non è ancora terminata, sarà visibile dal Portale come "in corso".

Durata: calcola la durata totale della sessione.

Destinazione: mostra l'indirizzo IP del Dispositivo di destinazione. Parametro disponibile solo per la connessione VPN Realm.

Porta: Indica la Porta coinvolta nella connessione. Qualora siano coinvolte più Porte nella connessione, tramite ⓘ è possibile visualizzarne l'elenco completo. Parametro disponibile solo per la connessione VPN Realm.

Nota: in caso di visualizzazione ridotta, cliccando ⓘ saranno visibili tutti i dati della Lista Audit.

Normalizzazione dei Dati

La normalizzazione dei dati è impostata a 30 minuti.

Se non viene rilevato traffico entro 30 minuti dall'ultima entry registrata, il sistema chiude automaticamente la sessione, impostando la data di fine con la data e l'ora dell'ultimo evento rilevato.

Una sessione può risultare:

- **In corso** - se sono trascorsi meno di 30 minuti dall'ultimo evento.
- **Terminata** - se sono trascorsi più di 30 minuti dall'ultimo evento.

La normalizzazione viene effettuata esclusivamente per le connessioni VPN di Reame, poiché per le connessioni L2 è disponibile la data esatta di connessione e disconnessione.

Storico delle Sessioni

Ogni Utente può consultare lo storico delle sessioni per un massimo di 15 giorni, dopodiché i dati verranno sovrascritti.



Sevio Srl – Via della Pusterla,36 20826 Misinto (MB) - IT

Tel. +39 02 97070785

Assistenza tecnica: support@sevio.it

Ufficio vendite: sales@sevio.it

<https://sevio.it/>

Document ID: audit_it_v_25_01

<https://sevio.it/>