Table of Contents

Ð Ñ Ñ ÐµÑ Ñ Ð¸Ð½Ñ Ð¸Ð´ÐµÐ½Ñ Ð¾Ð².....1
Ð Ð±Ñ Ð¸Ðµ Ñ Ð²ÐµÐ´ÐµÐ½Ð¸Ñ 1
Ð¨Ð°Ð±Ð»Ð¾Ð½Ñ Ð¾Ñ Ñ ÐµÑ Ð¾Ð² Ð¸Ð½Ñ Ð¸Ð´ÐµÐ½Ñ Ð¾Ð²**.....1
Ð Ñ Ð°Ð²Ð¸Ð»Ð° Ð¾Ñ Ñ ÐµÑ Ð¾Ð² Ð¸Ð½Ñ Ð¸Ð´ÐµÐ½Ñ Ð¾Ð²**.....2
ÐiÐ¾Ð·Ð´Ð°Ð½Ð½Ñ Ðµ Ð¾Ñ Ñ ÐµÑ Ñ Ð¸Ð½Ñ Ð¸Ð´ÐµÐ½Ñ Ð¾Ð²**.....3

Ð Ñ Ñ ÐµÑ Ñ Ð¸Ð½Ñ Ð¸Ð´ÐµÐ½Ñ Ð¾Ð²

Ð Ð±Ñ Ð¸Ðµ Ñ Ð²ÐµÐ´ÐµÐ½Ð¸Ñ

Documentation: ☑
Product: SIEM
Version: 7.x
Ð Ð´Ð°Ð½Ð½Ð¾Ð¼ Ñ Ð°Ð·Ð´ÐµÐ»Ðµ Ð°Ð´Ð¼Ð¸Ð½Ð¸Ñ Ñ Ñ Ð°Ñ Ð¾Ñ Ð¼Ð¾Ð¶ÐµÑ Ñ Ð¾Ñ Ð¼Ð¸Ñ Ð¾Ð²Ð°Ñ Ñ Ð¾Ñ Ñ Ñ Ñ Ñ Ð¾Ð± Ð¸Ð½Ñ Ð¸Ð´ÐµÐ½Ñ Ð°Ñ Ð¸Ð½Ñ Ð¾Ñ Ð¼Ð°Ñ Ð¸Ð¾Ð½Ð½Ð¾Ð¹ Ð±ÐµÐ·Ð¾Ð¿Ð°Ñ Ð½Ð¾Ñ Ñ Ð¸. Ð Ñ Ñ ÐµÑ Ñ Ð¼Ð¾Ð³Ñ Ñ Ñ Ð¾Ð·Ð´Ð°Ð²Ð°Ñ Ñ Ñ Ñ Ð² Ñ Ð¾Ð¾Ñ Ð²ÐµÑ Ñ Ñ Ð²Ð¸Ð¸ Ñ Ñ Ð¾Ð·Ð´Ð°Ð½Ð½Ñ Ð¼Ð¸Ð¿Ñ Ð°Ð²Ð¸Ð»Ð°Ð¼ Ð¸Ñ Ð°Ð±Ð»Ð¾Ð½Ð°Ð¼; Ð¾Ñ Ñ Ñ Ñ Ð´Ð¾Ñ Ñ Ñ Ð¿ÐµÐ½ Ð´Ð»Ñ Ñ ÐºÐ°Ñ Ð¸Ð²Ð°Ð½Ð¸Ñ Ð¸Ð»Ð¸ Ð¿ÐµÑ ÐµÐ´Ð°Ñ Ð¸ Ð½Ð° ÐºÐ¾Ð½Ð½ÐµÐºÑ Ð¾Ñ .

Ð Ð°Ð·Ð´ÐµÐ» Ñ Ð¾Ñ Ñ Ð¾Ð¸Ñ Ð¸Ð· Ñ Ñ ÐµÑ Ð¿Ð¾Ð´Ñ Ð°Ð·Ð´ÐµÐ»Ð¾Ð²
- **Ð¨Ð°Ð±Ð»Ð¾Ð½Ñ Ð¾Ñ Ñ ÐµÑ Ð¾Ð²**
Ð¸Ð½Ñ Ð¸Ð´ÐµÐ½Ñ Ð¾Ð², **Ð Ñ Ð°Ð²Ð¸Ð»Ð° Ð¾Ñ Ñ ÐµÑ Ð¾Ð²**
Ð¸Ð½Ñ Ð¸Ð´ÐµÐ½Ñ Ð¾Ð² Ð¸ **ÐiÐ¾Ð·Ð´Ð°Ð½Ð½Ñ Ðµ Ð¾Ñ Ñ ÐµÑ Ñ**
Ð¸Ð½Ñ Ð¸Ð´ÐµÐ½Ñ Ð¾Ð². Ð§Ñ Ð¾Ð±Ñ Ñ Ð¾Ð·Ð´Ð°Ñ Ñ Ð¾Ñ Ñ ÐµÑ ,
Ð½ÐµÐ¾Ð±Ñ Ð¾Ð´Ð¸Ð¼Ð¾ Ð²Ñ Ð¿Ð¾Ð»Ð½Ð¸Ñ Ñ Ñ Ð»ÐµÐ´Ñ Ñ Ñ Ð¸Ðµ Ð´ÐµÐ¹Ñ Ñ Ð²Ð¸Ñ :

Ð Ð°Ð¸Ð¼ÐµÐ½Ð¾Ð²Ð°Ð½Ð¸Ðµ	Ð Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ
Ð¨Ð°Ð³ 1. ÐiÐ¾Ð·Ð´Ð°Ñ Ñ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð¾ Ñ Ð¾Ð·Ð´Ð°Ð½Ð¸Ñ Ð¾Ñ Ñ ÐµÑ Ð°.	ÐiÐ¾Ð·Ð´Ð°Ñ Ñ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð¾ Ñ Ð¾Ð·Ð´Ð°Ð½Ð¸Ñ Ð¾Ñ Ñ ÐµÑ Ð°, Ð² ÐºÐ¾Ñ Ð¾Ñ Ð¾Ð¼ Ñ ÐºÐ°Ð·Ð°Ñ Ñ Ð½ÐµÐ¾Ð±Ñ Ð¾Ð´Ð¸Ð¼Ñ Ðµ Ð¿Ð°Ñ Ð°Ð¼ÐµÑ Ñ Ñ Ñ Ð¾Ð·Ð´Ð°Ð½Ð¸Ñ Ð¾Ñ Ñ ÐµÑ Ð°.
Ð¨Ð°Ð³ 2. Ð Ð°Ð¿Ñ Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ñ ÐµÑ .	Ð Ñ Ð±Ñ Ð°Ñ Ñ Ð¸Ð½Ñ Ð¸Ð´ÐµÐ½Ñ Ð¸ Ñ Ð³ÐµÐ½ÐµÑ Ð¸Ñ Ð¾Ð²Ð°Ñ Ñ Ð¾Ñ Ñ ÐµÑ .
Ð¨Ð°Ð³ 3. Ð Ð¾Ð»Ñ Ñ Ð¸Ñ Ñ Ð¾Ñ Ñ ÐµÑ .	Ð Ð°Ð¿Ð¸Ñ Ð¸ Ð¾ Ñ Ð¾Ð·Ð´Ð°Ð½Ð¸Ð¸ Ð¾Ñ Ñ ÐµÑ Ð¾Ð² Ð´Ð¾Ñ Ñ Ñ Ð¿Ð½Ñ Ð² Ñ Ð°Ð·Ð´ÐµÐ»Ðµ **ÐiÐ¾Ð·Ð´Ð°Ð½Ð½Ñ Ðµ Ð¾Ñ Ñ ÐµÑ Ñ Ð¸Ð½Ñ Ð¸Ð´ÐµÐ½Ñ Ð¾Ð²**.

Ð¨Ð°Ð±Ð»Ð¾Ð½Ñ Ð¾Ñ Ñ ÐµÑ Ð¾Ð² Ð¸Ð½Ñ Ð¸Ð´ÐµÐ½Ñ Ð¾Ð²

Documentation: ☑
Product: SIEM
Version: 7.x
Ð¨Ð°Ð±Ð»Ð¾Ð½ Ð¾Ð¿Ñ ÐµÐ´ÐµÐ»Ñ ÐµÑ Ð²Ð½ÐµÑ Ð½Ð¸Ð¹ Ð²Ð¸Ð´ Ð¸ Ð¿Ð¾Ð»Ñ , ÐºÐ¾Ñ Ð¾Ñ Ñ Ðµ Ð±Ñ Ð´Ñ Ñ Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ Ñ Ñ Ñ Ð² Ð¾Ñ Ñ ÐµÑ Ðµ. Ð¨Ð°Ð±Ð»Ð¾Ð½Ñ Ð¾Ñ Ñ ÐµÑ Ð¾Ð² Ð¸Ð½Ñ Ð¸Ð´ÐµÐ½Ñ Ð¾Ð² Ð´ÐµÐ»Ñ Ñ Ñ Ñ Ð½Ð° 2 ÐºÐ°Ñ ÐµÐ³Ð¾Ñ Ð¸Ð¸:

- **Ð¤Ð¾Ñ Ð¼Ð° ÐºÐ»Ñ Ñ -Ð·Ð°ÐºÐ»Ñ Ñ ÐµÐ½Ð¸Ðµ** â Ñ Ð°Ð±Ð»Ð¾Ð½Ñ , Ð¿Ð¾Ð·Ð²Ð¾Ð»Ñ Ñ Ñ Ð¸Ðµ Ð½Ð°Ñ Ñ Ñ Ð¾Ð¸Ñ Ñ Ð¿Ð¾Ð»Ñ , ÐºÐ¾Ñ Ð¾Ñ Ñ Ðµ Ð½ÐµÐ¾Ð±Ñ Ð¾Ð´Ð¸Ð¼Ð¾ Ð¾Ñ Ð¾Ð±Ñ Ð°Ð·Ð¸Ñ Ñ Ð² Ð¾Ñ Ñ Ñ Ñ Ðµ. Ð¨Ð°Ð±Ð»Ð¾Ð½Ñ Ð´Ð°Ð½Ð½Ð¾Ð³Ð¾ Ñ Ð¸Ð¿Ð° Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ Ð¼Ð¾Ð¶ÐµÑ Ñ Ð¾Ð·Ð´Ð°Ð²Ð°Ñ Ñ

Ñ Ð°Ð¼Ð¾Ñ Ñ Ð³Ñ Ñ ÐµÐ»Ñ Ð½Ð¾.

- **Ð Ð½Ñ Ð¸Ð´ÐµÐ½Ñ Ñ** â Ð³Ñ Ñ Ð¿Ð° Ñ Ð°Ð±Ð»Ð¾Ð½Ð½Ð¾Ð² Ð´Ð»Ñ Ñ Ð¾Ð·Ð´Ð°Ð½Ð¸Ñ Ð¸Ð¾ Ð¸Ð½Ñ Ð¸Ð´ÐµÐ½Ñ Ð°Ð¼. Ð¨Ð°Ð±Ð»Ð¾Ð½Ñ Ð¿Ñ ÐµÐ´Ð¾Ñ Ñ Ð°Ð²Ð»Ñ Ñ ÐºÐ¾Ð¼Ð¿Ð°Ð½Ð¸ÐµÐ¹ UserGate.

Ð Ð°Ð¶Ð´Ñ Ð¹ Ñ Ð°Ð±Ð»Ð¾Ð½ Ñ Ð¾Ð´ÐµÑ Ð¶Ð¸Ñ Ð½Ð°Ð·Ð¾Ð²Ð°Ð½Ð¸Ðµ, Ð¾Ð¿Ð¸Ñ Ð°Ð½Ð¸Ðµ Ð¾Ñ Ð¸Ð¾ Ð¸Ð¾Ð±Ñ Ð¾Ð¾Ð±Ñ Ð¾Ð¾Ð±Ñ Ð¾

Ð Ð¾Ñ Ð»Ðµ Ñ Ð¾Ð·Ð´Ð°Ð½Ð¸Ñ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð° Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ñ ÐµÐ»Ñ Ð¼Ð¾Ð¶ÐµÑ Ð·Ð°Ð¿Ñ Ñ Ñ Ð¸Ñ Ñ Ñ Ð¾Ð·Ð´Ð°Ð½Ð¸Ðµ Ð¾Ñ Ñ Ñ Ñ Ð° Ð¿Ð¾Ð²Ñ Ð±Ñ Ð°Ð½Ð½Ð¾Ð¼Ñ Ð¸Ð½Ñ Ð¸Ð´ÐµÐ½Ñ Ñ . Ð Ð¾Ñ Ð»Ðµ Ñ Ð¾Ñ Ð¼Ð¸Ñ Ð¾Ð²Ð°Ð½Ð¸Ñ Ð¾Ñ Ñ Ñ Ñ Ð´Ð¾Ñ Ñ Ñ Ð¿ÐµÐ½ Ð´Ð»Ñ Ñ ÐºÐ°Ñ Ð¸Ð²Ð°Ð½Ð¸Ñ Ð»Ð¾ÐºÐ°Ð»Ñ Ð½Ð¾ Ð¸Ð»Ð¸ Ð¿ÐµÑ ÐµÐ´Ð°Ñ Ð¸ Ð½Ð° Ð²Ñ Ð±Ñ Ð°Ð½Ð½Ñ Ð¹ ÐºÐ¾Ð½Ð½ÐµÐºÑ Ð¾Ñ .

Ð¡Ð¾Ð·Ð´Ð°Ð½Ð½Ñ Ðµ Ð¾Ñ Ñ ÐµÑ Ñ Ð¸Ð½Ñ Ð¸Ð´ÐµÐ½Ñ Ð¾Ð²

Documentation: ☑
Product: SIEM
Version: 7.x
Ð Ñ Ð°Ð·Ð´ÐµÐ»Ðµ **Ð¡Ð¾Ð·Ð´Ð°Ð½Ð½Ñ Ðµ Ð¾Ñ Ñ ÐµÑ Ñ Ð¸Ð½Ñ Ð¸Ð´ÐµÐ½Ñ Ð¾Ð²** Ñ Ñ Ð°Ð½Ñ Ñ Ñ Ñ Ð²Ñ Ðµ Ñ Ñ Ð¾Ñ Ð¼Ð¸Ñ Ð¾Ð²Ð°Ð½Ð½Ñ Ðµ Ð¾Ñ Ñ ÐµÑ Ñ . Ð Ñ Ñ ÐµÑ Ñ Ñ Ð¾Ð·Ð´Ð°Ñ Ñ Ñ Ñ Ð² Ñ Ð¾Ñ Ð¼Ð°Ñ Ðµ pdf Ð¸Ð»Ð¸ html. Ð Ð»Ñ ÐºÐ°Ð¶Ð´Ð¾Ð³Ð¾ Ð¾Ñ Ñ ÐµÑ Ð° Ñ ÐºÐ°Ð·Ñ Ð²Ð°ÐµÑ Ñ Ñ Ð½Ð°Ð·Ð²Ð°Ð½Ð¸Ðµ Ð¾Ñ Ñ ÐµÑ Ð°, ÐºÐ¾Ñ Ð¾Ñ Ð¾Ðµ Ñ Ð¾Ð²Ð¿Ð°Ð´Ð°ÐµÑ Ñ Ð½Ð°Ð·Ð²Ð°Ð½Ð¸ÐµÐ¼ Ð¿Ñ Ð°Ð²Ð¸Ð»Ð° Ð¾Ñ Ñ ÐµÑ Ð°, Ð¸Ñ Ð¿Ð¾Ð»Ñ Ð·Ð¾Ð²Ð°Ð½Ð½Ð¾Ð³Ð¾ Ð´Ð»Ñ Ñ Ð¾Ð·Ð´Ð°Ð½Ð¸Ñ Ð´Ð°Ð½Ð½Ð¾Ð³Ð¾ Ð¾Ñ Ñ ÐµÑ Ð°, Ð²Ñ ÐµÐ¼Ñ Ñ Ð¾Ð·Ð´Ð°Ð½Ð¸Ñ Ð¾Ñ Ñ ÐµÑ Ð° Ð¸ Ñ Ð°Ð¹Ð» Ð¾Ñ Ñ ÐµÑ Ð° Ñ Ñ ÐºÐ°Ð·Ð°Ð½Ð¸ÐµÐ¼ ÐµÐ³Ð¾ Ñ Ð°Ð·Ð¼ÐµÑ Ð°. Ð Ñ Ðµ Ð¾Ñ Ñ ÐµÑ Ñ Ð´Ð¾Ñ Ñ Ñ Ð¿Ð½Ñ Ð´Ð»Ñ Ñ ÐºÐ°Ñ Ð¸Ð²Ð°Ð½Ð¸Ñ Ð¸ Ñ Ð´Ð°Ð»ÐµÐ½Ð¸Ñ .

Ð Ñ ÐµÐ¼Ñ Ñ Ñ Ð°Ð½ÐµÐ½Ð¸Ñ Ð³Ð¾Ñ Ð¾Ð²Ñ Ñ Ð¾Ñ Ñ ÐµÑ Ð¾Ð² (Ñ Ð¾Ñ Ð°Ñ Ð¸Ñ) Ð½Ð°Ñ Ñ Ñ Ð°Ð¸Ð²Ð°ÐµÑ Ñ Ñ Ð¿Ð¾ Ð½Ð°Ð¶Ð°Ñ Ð¸Ñ Ð½Ð° ÐºÐ½Ð¾Ð¿ÐºÑ **Ð Ð°Ñ Ñ Ñ Ð¾Ð¸Ñ Ñ** .