2025 JULY 4

Orange The Client ver 1.6

사용설명서(일반)

기업 관리자용

오렌지랩스(주)
부산광역시 해운대구 센텀중앙로 97, 에이동 2801 호

저작권

프 로 그 램 등 록 부

프로그램 등록번호	C-2023-041100			
프로그램의 명칭	Orange The Client(오렌지 더 클라이언트)			
창 작 연 월 일	2020.05.21	공표연월일	2022.12.14	
등 록 연 월 일	2023.09.13			
프로그램 저 작 자	성명 또는 상호	오렌지랩스 주식회사	주민등록번호 또는 법 인 등 록 번 호	110111-8581385
	주 소 및 국 적	서울특별시 금천구 벚꽃로 244 601호		대한민국
	지 분	1분의 1		
프로그램복제물에 관한 사항	소스파일, 실행파일 File (on-line) 1			

프로그램저작권란

1	등 록 부 문 컴퓨터프로그램저작물 저작권 등록 처리일자 : 2023.09.13 ① 신 청 인 오렌지랩스 주식회사 (110111-8581385) 서울특별시 금천구 벚꽃로 244 601호 ② 저작(권)자 오렌지랩스 주식회사(1/1) 110111-8581385 서울특별시 금천구 벚꽃로 244 601호 ③ 등 록 원 인 저작자 : 오렌지랩스 주식회사, 창작 : 2020.05.21, 공표 : 2022.12.14 ④ 접 수 번 호 2023-045527 ⑤ 접 수 일 자 2023.09.06 ⑥ 등 록 일 자 2023.09.13
2	프로그램 저작권 양도 처리일자 : 2024.01.08 (개작권 포함) ① 등록권리자 이피엠에스 주식회사(1/1) 110111-8796380 서울특별시 금천구 벚꽃로 244 601호 (가산동) ② 등록의무자 오렌지랩스 주식회사 110111-8581385 부산광역시 해운대구 센텀중앙로 97 에이동 2801호 (재송동) ③ 등록원인과 그 연월일 저작재산권 보유지분 전부 이전 계약(2023.12.26) ④ 이전 대상범위 저작재산권 보유지분 전부 이전-2차적저작물작성권 포함 ⑤ 등록연월일 2024.01.08 ⑥ 당사자간의 특약 -

순위번호 : 1 > 저작자목록

1) 오렌지랩스 주식회사(110111-8581385), 국적:대한민국, 지분 : 1/1, 주소:서울특별시 금천구 벚꽃로 244 601호
전화:010-9425-8957, 이메일:kimsj@onenetsys.co.kr

순위번호 : 2 > 등록권리자목록

1) 이피엠에스 주식회사(110111-8796380), 국적:대한민국, 지분 : 1/1, 주소:서울특별시 금천구 벚꽃로 244 601호 (가산동)
전화:02-6671-6905, 이메일:hjna@onenetsys.co.kr

순위번호 : 2 > 등록의무자목록

1) 오렌지랩스 주식회사(110111-8581385), 국적:대한민국, 주소:부산광역시 해운대구 센텀중앙로 97 에이동 2801호 (재송동)
전화:02-6672-0010, 이메일:kimsj@onenetsys.co.kr

판매 및 기술 지원 문의

공급사	오렌지시스(주)
제품 안내	https://orangesys.co.kr/product/theclient
연락처	02-6671-6900
주소	서울 금천구 디지털로 178, 가산퍼블릭 B동 726-729
온라인 문의 및 기술 지원 요청	https://orangesys.co.kr/contact/inquiry

지원 언어

한글

<목차>

<표 목차>

<그림 목차>

1 개 요

Orange The Client는 기업의 PC 성능 저하와 장애 분석을 위한 솔루션입니다.

1.1 목적

Orange The Client는 엔드포인트 동작을 모니터링해 성능과 장애 관련 이슈를 탐지하고, 상황에 맞는 정보를 제공합니다. 또한 영향을 받는 시스템을 개선하기 위한 조치를 수행할 수 있습니다. 기업의 관리자는 **Orange The Client**를 통해 기업 내 모든 **PC**에서 발생하는 성능 저하와 장애를 중앙에서 분석하고 관리할 수 있습니다.

1.1.1 실시간 성능/장애 모니터링

- 복잡한 과정을 거쳐야 했던 원인 분석을 본 솔루션을 통해 단시간에 명확히 수행 가능
- 증상, 영향도, 외부환경 데이터를 수치화하여, 확인이 어려웠던 증상 원인을 간략한 시각화로 파악
- 실시간 정보집계, 자동화, 트래픽의 축소를 통해 투입 인원 및 소요 시간 절감 가능

[그림 1] 제품의 목적

1.2 제품 버전 체계

Orange The Client 제품의 버전 체계는 4가지 번호의 조합으로 구성됩니다.

주버전(Major).부버전(Minor).수정버전(Patch).빌드번호(Build)

항목	의미
주 버전(Major)	기본 구조 및 기능 대규모 변경. 하위 호환성 미보장.
부 버전(Minor)	기능 추가 또는 기존 기능의 향상.
수정 버전(Patch)	기존 기능의 버그 수정, 성능 개선, 보안 패치 등.
빌드 번호(Build)	빌드 시 증가. 단 수정 버전이 오르는 경우 0부터 재시작.

[표 1] 제품 버전 체계

예를 들어 제품의 버전이 1.6.234.3인 경우, 주 버전 1, 부 버전 6, 수정 버전 234, 빌드 번호 3인 것입니다.

고객사에 제공되는 버전 정보는 주 버전과 부 버전 2가지입니다.
본 매뉴얼은 **Orange The Client** v1.6 제품에 대해 기술된 것이므로, 1.6.x.x 대 모든 제품에 대해서 공통적으로 적용되는 내용을 다루고 있습니다.

1.3 구성

본 설명서는 다음과 같이 구성되어 있습니다.

1장 개요

문서의 개요, 목적, 구성에 대해 설명합니다.

2장 제품 구성

제품의 전체 구조와 구성 요소에 대해 설명합니다.

3장 운영 환경 정보

제품이 동작되는 운영 환경에 대해 설명합니다.

4장 제품 업데이트

제품을 업데이트 하는 방법에 대해 설명합니다.

5장 에이전트 사용 가이드

제품의 구성 요소 중 하나인 에이전트를 사용하는 방법을 설명합니다.

6장 매니저 사용 가이드

제품의 구성 요소 중 하나인 매니저를 사용하는 방법을 설명합니다.

7장 탐지 증상

제품이 탐지하는 주요 성능 저하 및 장애와 관련된 증상에 대해 설명합니다.

8장 부록

1.4 데이터 백업 및 복구

Orange The Client 제품 내부의 데이터를 백업하거나 복구하는 작업은 제품 사용자(기업 관리자 등)에 의해 직접 수행 가능하지 않도록 제한되어 있으며, 필요에 의해 요청 시 자사 엔지니어에 의해 수행이 가능합니다.

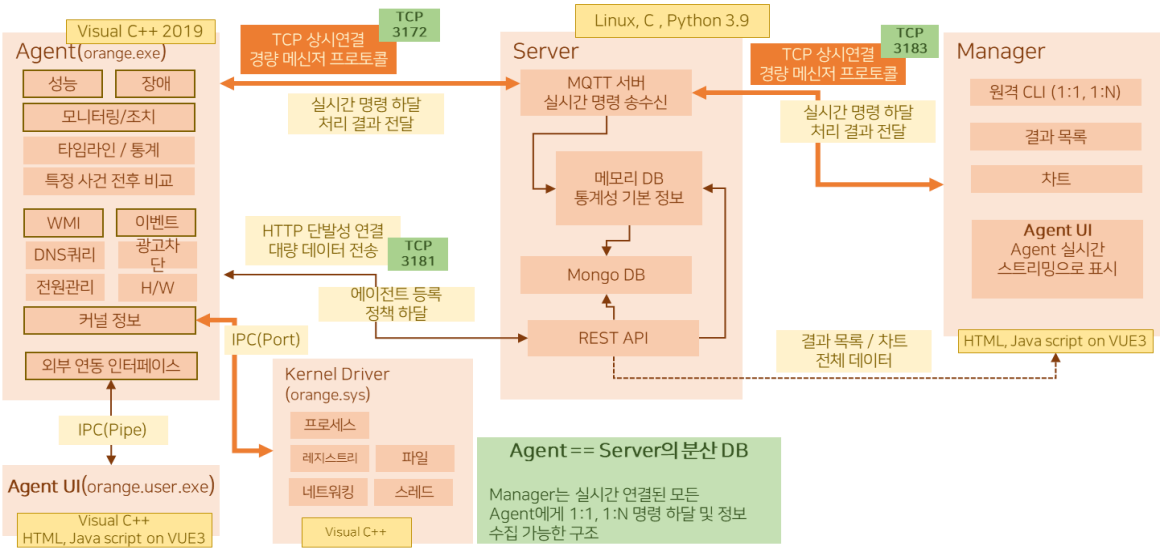
2 제품 구성

이 장에서는 **Orange The Client**의 전체 구조와 구성 요소에 대해 설명합니다.

2.1 전체 구조

본 제품은 아래 그림과 같이 크게 **①매니저**, **②서버**, **③에이전트**로 기본 구성되어 있습니다.

- 분산된 각 요소가 네트워크를 통해 상시 연결된 실시간 구조
- Scale Out과 클라우드 서비스 적용이 가능한 시스템 구조
- 행위 기반 정보 수집과 분석의 자동화



[그림 2] 제품 전체 구조

2.2 구성 요소

2.2.1 매니저

기업의 관리자에게 웹 기반 **Orange The Client** 관리 콘솔을 제공합니다. 매니저를 통해 수집된 정보를 확인하고 연결된 PC들을 원격으로 관리할 수 있습니다.

2.2.2 서버

Orange The Client의 모든 데이터 및 설정을 저장하는 중앙 관리 시스템입니다.
서버는 기업 관리자에게 매니저를 제공하고 사용자 PC에 설치된 에이전트와 상시 TCP 연결을 통해 사용자 PC가 NAT 내부에 존재하더라도 실시간 양방향 처리가 가능합니다.

2.2.3 에이전트

사용자 PC에 설치된 소프트웨어입니다. 사용자 PC에서 발생하는 관련 이벤트를 수집하고 필요

시 관리자에 의한 원격 조치를 수행합니다.
PC에서 발생된 관련 이벤트를 수집, 분석 후 서버로 전송합니다.

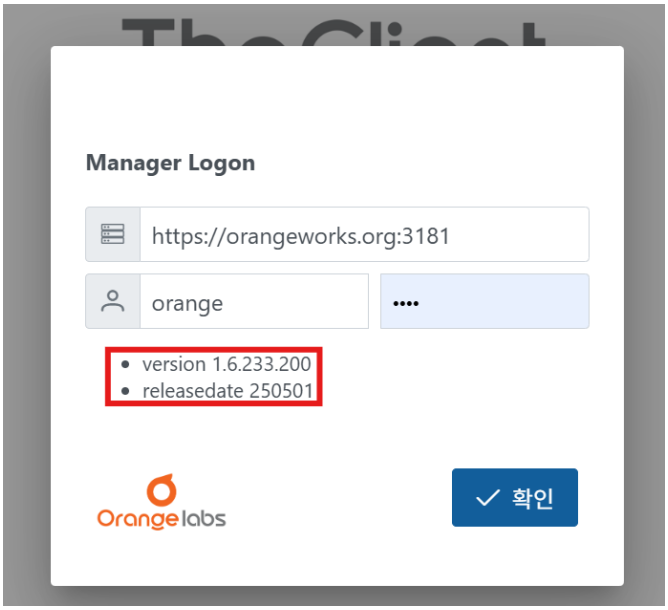
2.2.4 구성 요소별 시스템 사양

구분		권장 사양
매니저(관리자 PC)	System	웹 브라우저를 실행할 수 있는 환경
	Browser	Chrome 지원 (최신 버전 권장)
서버	OS	Linux Ubuntu 24.04 x64
	RAM	16GB 이상
	HDD	256GB 이상 여유 공간
에이전트(사용자 PC)	OS	MS Windows 10 (x64), 11(x64)
	CPU	Dual Core 2GHz 이상
	RAM	2GB 이상
	HDD	100GB 이상 여유 공간
	NIC	100Mbps 1개 이상

[표 2] 구성 요소별 시스템 사양

2.2.5 구성 요소별 버전 확인 방법

2.2.5.1 매니저



[그림 3] 매니저 로그온 화면

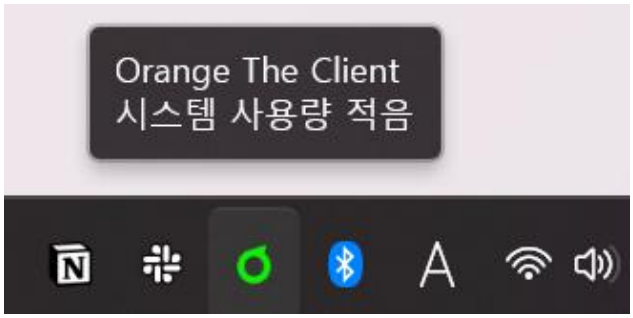
매니저 로그온 창에 매니저 버전과 릴리즈 일이 표시됩니다.

2.2.5.2 서버

[그림 4] 매니저 상단 배너

매니저 로그온 후 상단에 서버 버전과 작성일이 표시됩니다.

2.2.5.3 에이전트



[그림 5] 에이전트 트레이 아이콘

사용자 PC 트레이 아이콘에 마우스 커서를 대면, 에이전트 버전이 표시됩니다.

	IP	갱신	사용자	도메인	증상	유형	CPU(…	Memory(…	I/O	버전
	175.113.78.2	25-05-02 18:07:31	케찹	바나나그룹	0	VM	0.5	2.2/4.1	112.6KB	1.6.233.200
	175.113.78.2	25-05-02 18:07:30	마요네즈	바나나그룹	0	VM	3.3	3.7/4.1	983KB	1.6.233.200
	211.54.64.209	25-05-02 18:07:31	ON1	부사장실	0	노트북	3.4	7.1/8.1	2.2MB	1.6.233.200
	211.54.64.209	25-05-02 18:07:28	남서울학군단	부사장실	2	노트북	29.5	6/8.1	5.2MB	1.6.233.200
	175.113.78.2	25-05-02 18:07:32	알파로메오	오렌지랩스	0	PC	16.7	6.9/8.1	12.5MB	1.6.233.200
	175.113.78.2	25-05-02 18:07:31	오렌지1	오렌지랩스	0	PC	9.9	44.9/65.4	36.5MB	1.6.233.200
	175.113.78.2	25-05-02 18:07:30	흑진주2	오렌지랩스	3	노트북	9.2	9.2/16.2	1.4MB	1.6.233.200
	175.113.78.2	25-05-02 18:07:29	바나나	오렌지랩스	5	PC	92.3	58/65.4	134MB	1.6.233.200
	183.107.140.196	25-05-02 18:07:29	안승민(회사)	오렌지랩스	3	노트북	21.4	17.4/32.2	8.1MB	1.6.233.200

[그림 6] 매니저에서 에이전트 버전 확인

또는 관리자는 매니저에서 설치된 에이전트 버전 확인이 가능합니다.

3 운영 환경 정보

이 장에서는 **Orange The Client**가 동작하기 위한 운영 환경에 대해 설명합니다.

3.1 서버

Orange The Client의 서버는 물리적인 단독 장비 또는 VM 장비에서 동작할 수 있습니다.

제조사가 지정한 장비에 설치된 형태로 납품되며, 제조사 지정 장비는 3가지 유형이 있고 사용자 PC 수에 따라 서버 장비가 달라집니다.

3.1.1 제조사 지정 장비

모델	Demo	TC1000	TC10000
CPU	Intel N100(4C4T) * 1	Intel Zeon E-224G(4C4T) 3.5GHz	Intel Zeon 4208(8C16T) 2.10GHz
Memory	4GB 이상	16GB 이상	32GB 이상
SSD	128GB 이상	480GB 이상	960GB 이상
HDD	-	-	-
수용 에이전트	1 ~ 100	1,000 이상	5,000 이상
하드웨어 제조사	Chatree T9 등 미니PC로 구성	Lenovo SR250	Lenovo SR530

[표 3] 제조사 지정 장비

3.1.2 그 외 환경

인증 테스트 등을 위해 클라우드 상에 VM 서버 구축, 제공이 가능합니다.
고객사의 서버 장비에 설치를 원할 경우 제조사와 별도 상담 후 설치가 가능합니다.

3.1.3 SSH 연결

서버 시스템 관리를 위해 SSH 접속이 가능하며 그 방법은 엔지니어용 매뉴얼에 기술돼 있습니다.

3.2 매니저

웹 브라우저를 열고 다음 링크로 이동합니다. 아래 링크를 복사해 브라우저 주소창에 입력합니다. "서버 IP 주소"를 실제 IP 주소 또는 도메인명으로 변경합니다.

https://"서버 IP 주소"/manager

3.3 에이전트

에이전트는 서버에서 에이전트 설치 파일을 다운로드 받아 Windows OS에 설치할 수 있습니다. 자세한 가이드는 “에이전트 사용 가이드” 챕터의 “설치 파일 다운로드”를 참고하면 됩니다.

3.4 방화벽 요구 사항

Orange The Client가 제대로 동작하려면 아래 포트들이 방화벽으로부터 개방돼야 합니다.

SRC IP	DEST IP	Service	참고
에이전트	서버	TCP/3172	TCP 상시 연결(Plain Text)
에이전트	서버	TCP/3181	RESTAPI(SSL)
에이전트	서버	TCP/3182	TCP 상시 연결(SSL)
에이전트	서버	TCP/443	업데이트 수신(SSL)
관리자 PC	서버	TCP/3181	RESTAPI
관리자 PC	서버	TCP/3183	Web Socket(SSL)
관리자 PC	서버	TCP/443	매니저 웹 접속(SSL)
관리자 PC	서버	TCP/50022	SSH

[표 4] 방화벽 요구 사항

4 제품 업데이트

이 장에서는 **Orange The Client**의 업데이트에 대해 설명합니다
설치 후 제조사 또는 고객사 요청에 의해 **Orange The Client**가 업데이트된 경우, 기술 지원 엔지니어의 고객사 방문 후 업데이트 작업이 필요합니다.

4.1 서버/매니저

기술 지원 엔지니어가 서버에 SSH 로그인 후 업데이트된 제품 패키지 다운로드 및 새 제품 패키지로 업데이트 수행 후 바로 반영됩니다.

4.2 에이전트

업데이트된 에이전트 설치본이 서버에 의해 자동으로 배포, 업데이트 됩니다.

4.3 무결성 검사

Orange The Client 제품 패키지는 내부적으로 서버, 매니저, 에이전트 3개 부분으로 나누어져 있고, 각 부분마다 별도로 PACKAGE라는 정보 파일을 가지고 있습니다. PACKAGE에는 주요 파일들의 SHA256이 기록돼 있습니다.

4.3.1 서버

서버의 서비스들은 자신의 파일 해시가 PACKAGE에 기록된 대상 파일 SHA256과 일치할 경우에만 수행되며 변조된 경우 자동으로 종료됩니다.

4.3.2 매니저

(1) 매니저 로그온 등 주요 기능을 제공하는 서버의 REST API 제공 서비스는 구동 직후 서버의 PACKAGE와 자신의 일치 여부를 검사합니다.
(2) 매니저 웹 프로그램 파일과 매니저 PACKAGE 파일에 기록된 파일별 SHA256을 비교, 일치하지 않는 경우, 자동으로 종료해 매니저가 동작하지 않게 됩니다.

4.3.3 에이전트

(1) 주기적으로 서버에 보관된 PACKAGE 파일과 에이전트의 PACKAGE 파일을 비교해서 업데이트가 있는 경우, 서버로부터 새로운 에이전트 설치파일을 다운로드 받습니다.
(2) 다운로드 받은 새로운 에이전트 설치파일과 서버에서 제공한 PACKAGE 파일에 기록된 SHA256을 비교, 일치하지 않으면 해당 에이전트 설치파일을 수행하지 않습니다.
(3) (2)항목에서 서로 SHA256이 일치해도, 새로운 에이전트 설치본이 제조사의 코드사인으로 전자 서명된 경우에만 새로운 에이전트 설치파일을 수행합니다.

5 에이전트 사용 가이드

본 장은 **Orange The Client**의 사용자 PC 설치 부분인 에이전트에 대해 설명합니다. 에이전트는 사용자 PC에서 발생하는 관련 이벤트를 수집하고 필요 시 관리자에 의한 원격 조치를 수행합니다.

5.1 설치 파일 다운로드

서버에서 에이전트 설치 파일을 다운로드 받아 Windows OS에 설치할 수 있습니다.

5.1.1 다운로드 링크

https://"서버 IP 주소" 접속 후, 에이전트 다운로드 링크를 클릭합니다.

[그림 7] 에이전트 다운로드 링크

서버 주소에 맞게 자동으로 에이전트 설치파일이 다운로드 됩니다.

5.1.2 URL 입력을 통한 에이전트 설치 파일 다운로드

아래 링크를 복사해 브라우저 주소창에 입력합니다.
"서버 IP 주소"를 실제 IP 주소 또는 도메인명으로 변경합니다.

> https://"서버 IP 주소"/update

5.1.3 에이전트 설치 파일 명

설치 파일은 접속 대상 서버 주소와 포트로 구성됩니다.

> ORANGE.x64_"서버 IP 주소"_"서버 포트".exe

서버 IP 주소는 "OrangeTheClient.com"과 같은 도메인 네임과 "182.19.28.22"와 같은 IP 형식 모두 지원합니다. 서버 포트가 지정되지 않은 경우 기본 값인 3181 포트를 사용합니다.

5.1.3.1 서버가 2개의 주소를 가지는 경우

서버가 사내 주소, 사외 주소와 같이 2개 주소를 가진 경우, 동일한 서버라도 매니저를 접속한 위치에 따라 다운로드 되는 설치 파일 명이 달라집니다.

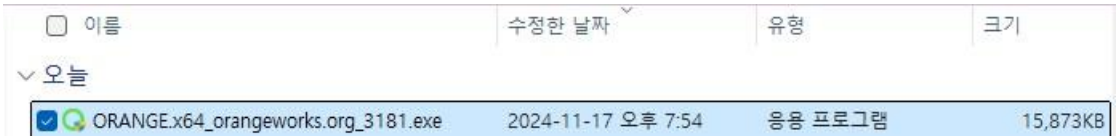
https://111.111.111.111로 매니저 접속 → "ORANGE.x64_111.111.111.111_3181.exe" 로 다운로드.

https://222.222.222.222로 매니저 접속 → "ORANGE.x64_222.222.222.222_3181.exe" 로 다운로드.

각 에이전트 설치 파일을 해당 대역의 PC로 배포하면 됩니다.

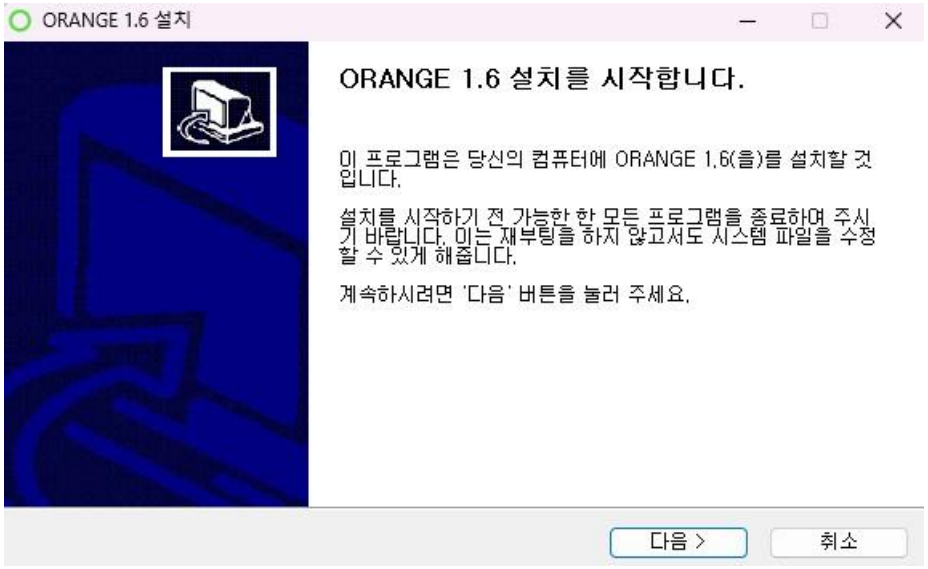
설치 후 에이전트는 매니저 서버에 설정된 2개 주소를 모두 받고 이후 자신이 접속할 수 있는 매니저 서버로 자동 접속됩니다.

5.2 설치 파일 실행



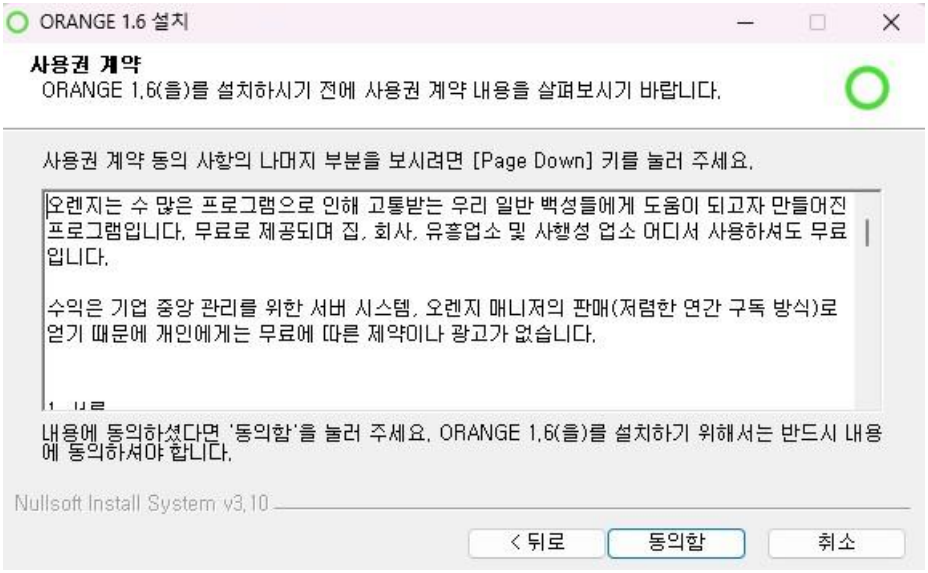
[그림 8] 에이전트 설치 파일 실행

다운로드 받은 에이전트 설치파일을 실행합니다. 파일명엔 접속 대상 서버의 주소가 적혀 있으므로 이름을 바꾸지 않고 그대로 실행합니다.



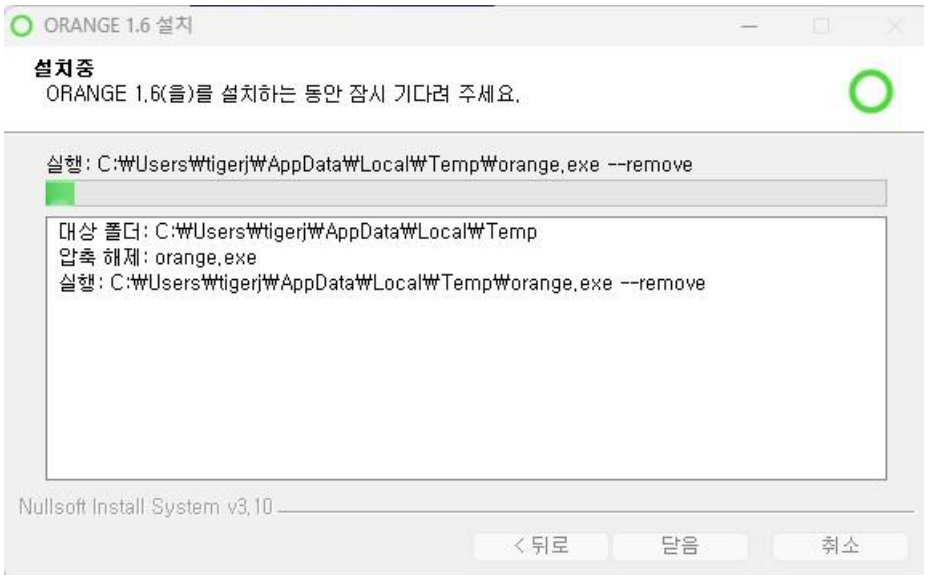
[그림 9] 에이전트 설치 시작

"다음"을 클릭합니다.



[그림 10] 에이전트 설치 약관 동의

"동의함"을 클릭합니다.



[그림 11] 에이전트 설치 진행 중

설치가 완료되면 자동으로 설치 창이 닫힙니다.

5.3 조용한 설치

다운로드 받은 에이전트 설치 파일을 실행할 때 실행 인자로 "/S"를 주면 에이전트 설치 파일은 사용자에게 별다른 메시지 없이 조용하고 빠르게 설치됩니다.

```
ORANGE.x64_111.111.111.111_3181.exe /S
```

5.4 설치 삭제

사용자가 프로그램 추가/삭제에서 에이전트를 삭제할 수 있으며, 또는 관리자가 매니저를 통해

원격으로 에이전트를 삭제할 수 있는 기능도 제공합니다.

5.4.1 사용자 직접 삭제

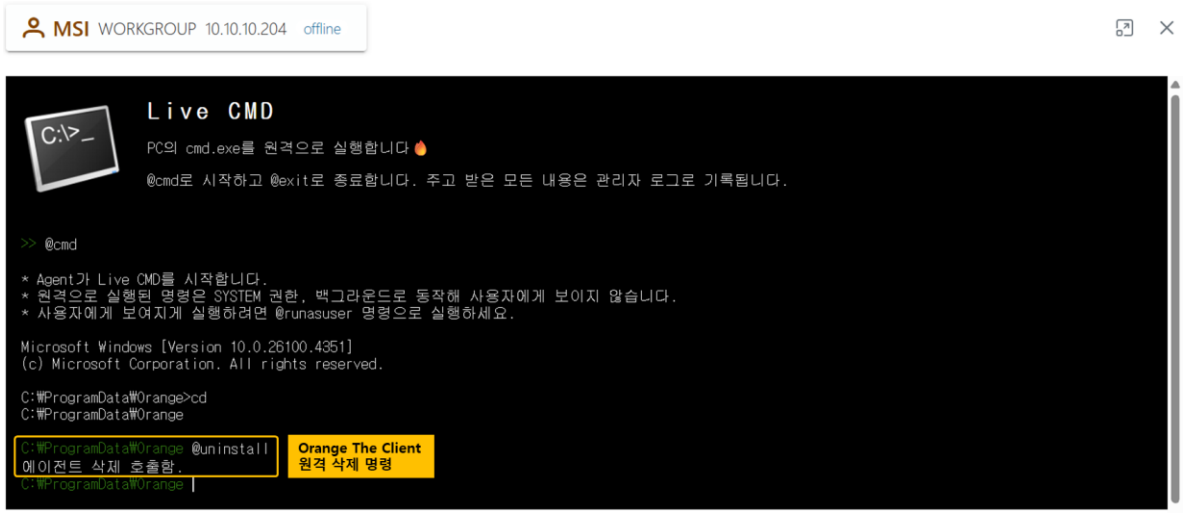
윈도우 설정의 프로그램 추가/제거에서 ORANGE 1.6에 대해 제거를 클릭해서 직접 삭제할 수 있습니다.

[그림 12] 윈도우 앱 설정에서 오렌지 에이전트 제거

5.4.2 원격 설치 삭제

매니저의 사용자 목록에서, 삭제를 원하는 단말을 선택합니다. Live CMD를 실행한 뒤, @cmd 명령과 @uninstall 에이전트 명령을 수행합니다.

Live CMD에 대한 자세한 실행 방법은 "매니저 사용 가이드" 챕터의 "Live CMD"를 참고하시길 바랍니다.



[그림 13] Live CMD 실행 화면

5.4.3 삭제 확인

설치가 삭제된 에이전트는 매니저 삭제 목록에 표시됩니다.

[그림 14] 매니저에서 삭제된 에이전트 목록 확인

5.5 트레이

5.5.1 아이콘

에이전트 설치 후, 윈도우 트레이 메뉴 항목에 동그란 아이콘이 표시되며 아이콘은 CPU 사용량

에 따라 색상이 변경됩니다.

[그림 15] 에이전트 트레이 아이콘 종류

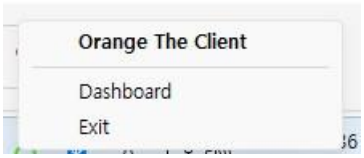
구분	사용량
사용량 적음	CPU 사용량 30% 이하
사용량 보통	CPU 사용량 31 ~ 70%
사용량 많음	CPU 사용량 71% 이상

[표 5] 트레이 아이콘 설명

CPU 사용량 계산 방법은 윈도우 작업 관리자와 다를 수 있으며 **Orange The Client** 에이전트 자체 계산 방식에 따릅니다.

5.5.2 메뉴

트레이 아이콘을 우클릭하면, 트레이 메뉴가 나타납니다.



[그림 16] 에이전트 트레이 메뉴

버튼	기능
Orange The Client	제품 소개 페이지
Dashboard	PC 현황을 보여주는 에이전트 UI
Exit	에이전트 종료

[표 6] 트레이 메뉴 설명

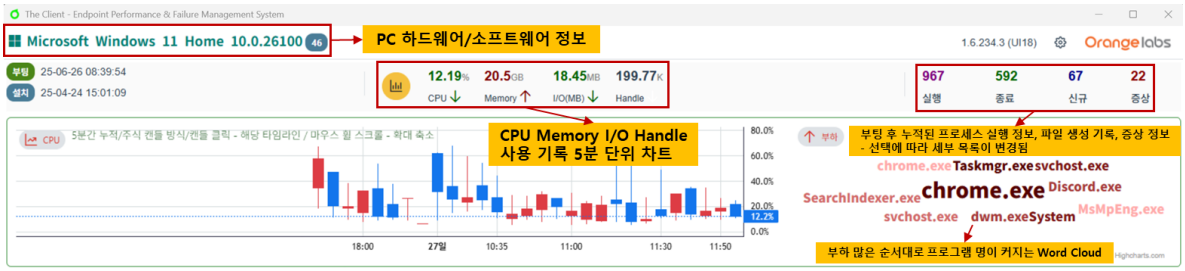
5.6 서버 통신

에이전트는 PC의 현재 부팅 상태에서 발생한 정보만을 보관하며, 서버와 통신이 가능한 상태에서는 실시간으로 서버로 정보를 전송합니다. 통신이 단절된 상태에서 발생한 증상에 대한 기록은, 다음 부팅 후 서버와의 네트워크가 연결됐을 때 전송하게 됩니다. 서버와 통신이 불가능한 상태에서 증상이 발생한 경우, 재부팅이 되더라도 관련 내용이 서버로 전송되지 않습니다.

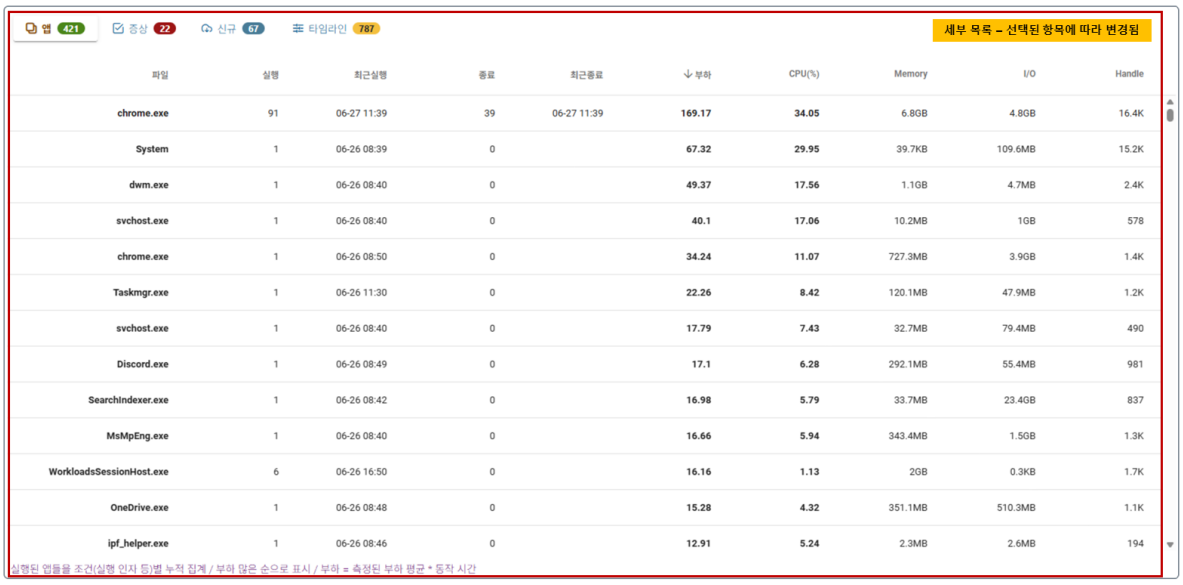
5.7 에이전트 UI

5.7.1 프로세스 실시간 모니터링

부팅 이후 PC에서 실행된 모든 프로그램들이 누적돼 표시됩니다. (이번 부팅 이전의 증상은 서버에 보관되며 매니저에서만 확인 가능합니다)



[그림 17] 에이전트 프로세스 실시간 모니터링



파일	실행	최근실행	종료	최근종료	부하	CPU(%)	Memory	I/O	Handle
chrome.exe	91	06-27 11:39	39	06-27 11:39	169.17	34.05	6.8GB	4.8GB	16.4K
System	1	06-26 08:39	0		67.32	29.95	39.7KB	109.6MB	15.2K
dwm.exe	1	06-26 08:40	0		49.37	17.56	1.1GB	4.7MB	2.4K
svchost.exe	1	06-26 08:40	0		40.1	17.06	10.2MB	1GB	578
chrome.exe	1	06-26 08:50	0		34.24	11.07	727.3MB	3.9GB	1.4K
Taskmgr.exe	1	06-26 11:30	0		22.26	8.42	120.1MB	47.9MB	1.2K
svchost.exe	1	06-26 08:40	0		17.79	7.43	32.7MB	79.4MB	490
Discord.exe	1	06-26 08:49	0		17.1	6.28	292.1MB	55.4MB	981
SearchIndexer.exe	1	06-26 08:42	0		16.98	5.79	33.7MB	23.4GB	837
MsMpEng.exe	1	06-26 08:40	0		16.66	5.94	343.4MB	1.5GB	1.3K
WorkloadsSessionHost.exe	6	06-26 16:50	0		16.16	1.13	2GB	0.3KB	1.7K
OneDrive.exe	1	06-26 08:48	0		15.28	4.32	351.1MB	510.3MB	1.1K
ipf_helper.exe	1	06-26 08:46	0		12.91	5.24	2.3MB	2.6MB	194

[그림 18] 에이전트 프로그램 실행 목록

세부 목록에 부팅 이후 PC에서 실행된 모든 프로그램들이 누적돼 표시됩니다.

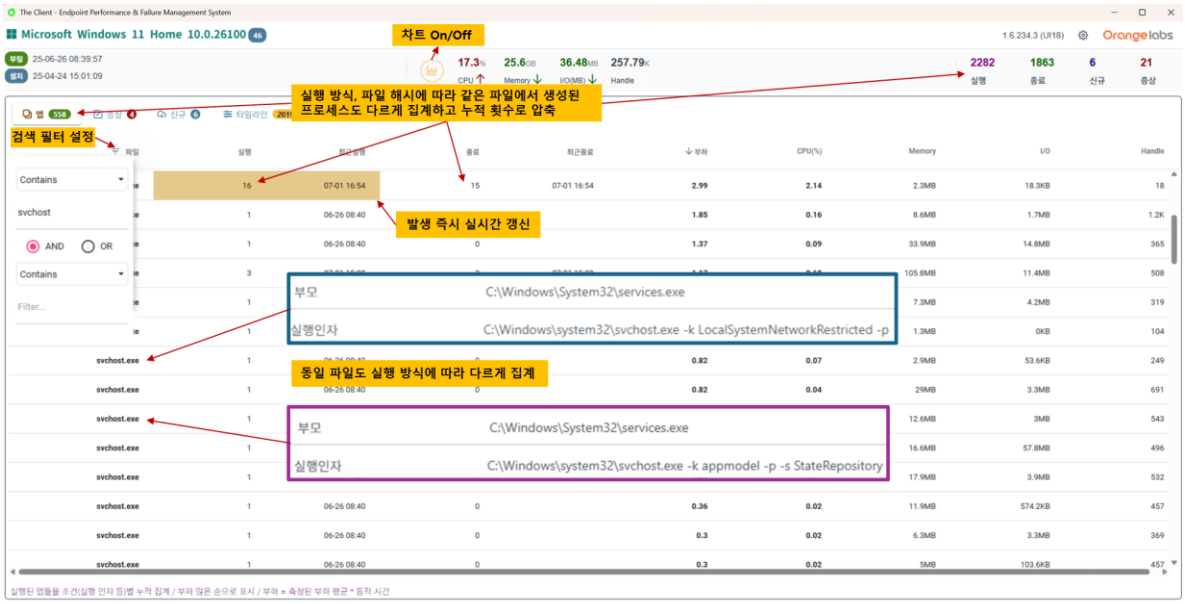
파일	실행	최근실행	종료	최근종료	부하	CPU(%)	Memory	I/O	Handle
chrome.exe	95	06-27 11:58	43	06-27 11:58	177	31.1	6.8GB	5.9GB	16.4K
System	1	06-26 08:39	0		67.87	27.67	39.7KB	116.8MB	15.2K
dwm.exe	1	06-26 08:40	0		51.44	16.1	1.1GB	5.3MB	2.4K
svchost.exe	1	06-26 08:40	0		40.78	15.58	10.1MB	1GB	579
chrome.exe	1	06-26 08:50	0		36.2	10.22	726MB	4.9GB	1.4K
Taskmgr.exe	1	06-26 11:30	0		22.88	7.76	120.2MB	52.4MB	1.3K
svchost.exe	1	06-26 08:40	0		18.12	6.83	33.6MB	82.2MB	490

[그림 19] 에이전트 프로그램 실행 목록의 집계 방식 설명

동일 파일에서 실행된 프로세스라도, 동일한 실행 방식으로 실행된 프로그램들끼리 Grouping 집계해, 집계 건수를 압축하면서도 각 프로세스간 차이를 명확히 구분해 보여줍니다.

5.7.2 검색

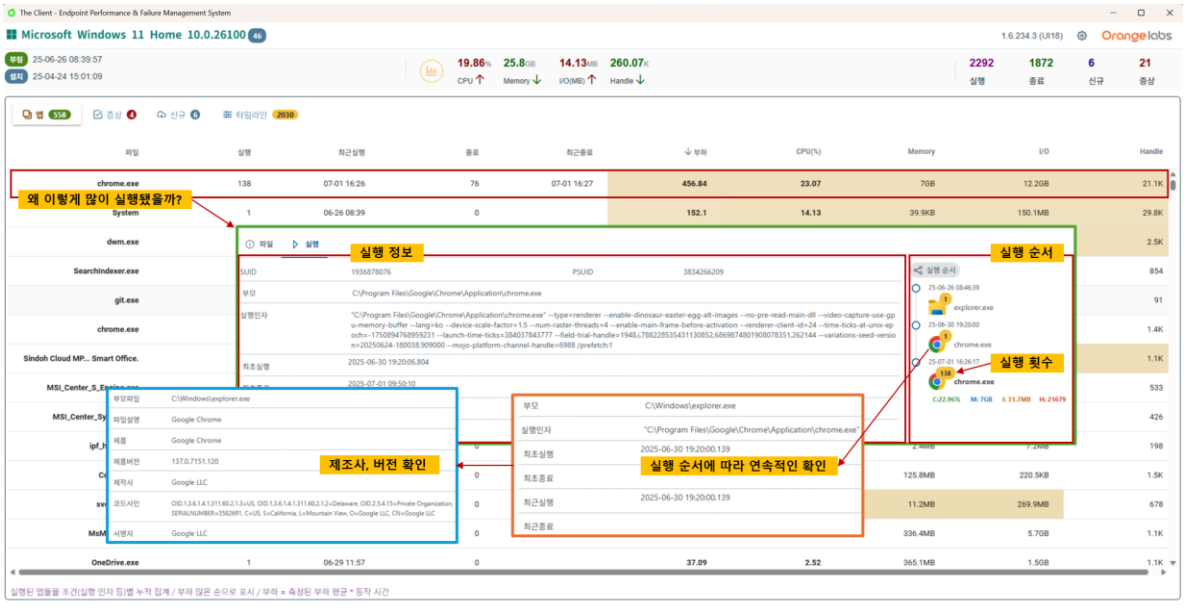
그리드 컬럼에 검색 필터와 정렬 방식을 설정할 수 있어 원하는 대상만 쉽게 모니터링 할 수 있습니다.



[그림 20] 에이전트 프로그램 실행 목록의 검색 필터 설정

5.7.3 파일과 프로세스 정보

표시된 파일명을 클릭하면 파일 정보와 실행된 프로세스 정보를 표시합니다.



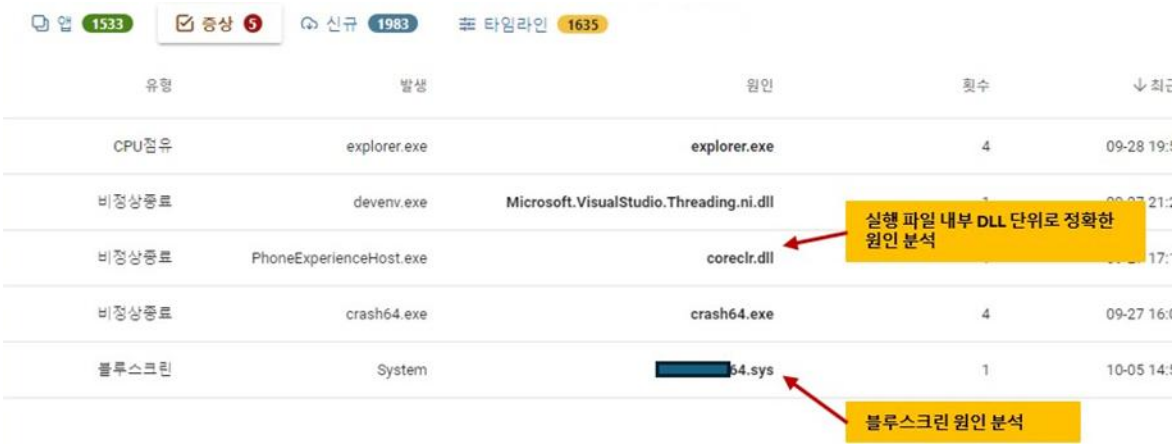
[그림 21] 에이전트 프로그램 실행 목록에서 파일명 클릭

5.7.4 증상

프로세스별로 증상의 발생 빈도를 쉽게 파악할 수 있도록, 발생 빈도와 비례하는 텍스트 크기로 프로세스의 파일명을 표시합니다. (참조: 해당 워드 클라우드 기능은 Highcharts.com 외부 라이브러리가 사용되었습니다)

[그림 22] 에이전트에서 프로세스별 증상 발생 빈도에 따른 워드 클라우드 표시

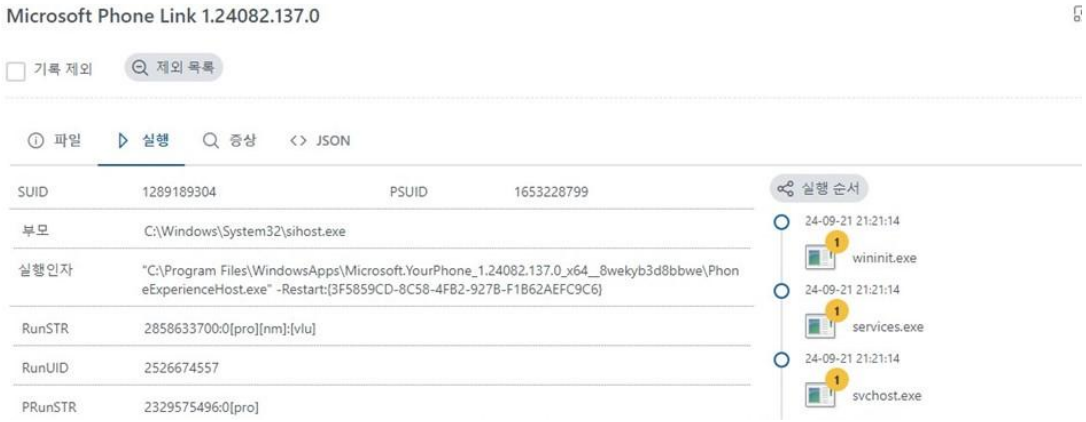
에이전트는 프로세스 실시간 탐지 및 분석기, 메모리 덤프 분석기를 내장합니다. 프로세스 동작 과정에서 생긴 문제점을 즉시 파악하고 분석해 원인을 도출합니다. 실행 파일 내부 dll 단위로 원인 탐지가 가능해, 정확한 원인을 파악하여 문제 해결을 빨리 할 수 있도록 해줍니다.



[그림 23] 에이전트의 프로세스 증상 목록

5.7.4.1 문제가 발생된 프로세스 정보

"발생" 컬럼을 클릭하면 문제가 발생한 프로세스 정보를 볼 수 있습니다. 프로세스 실행 정보를 "실행" 탭에서 확인할 수 있습니다.



[그림 24] 문제가 발생된 프로세스 정보

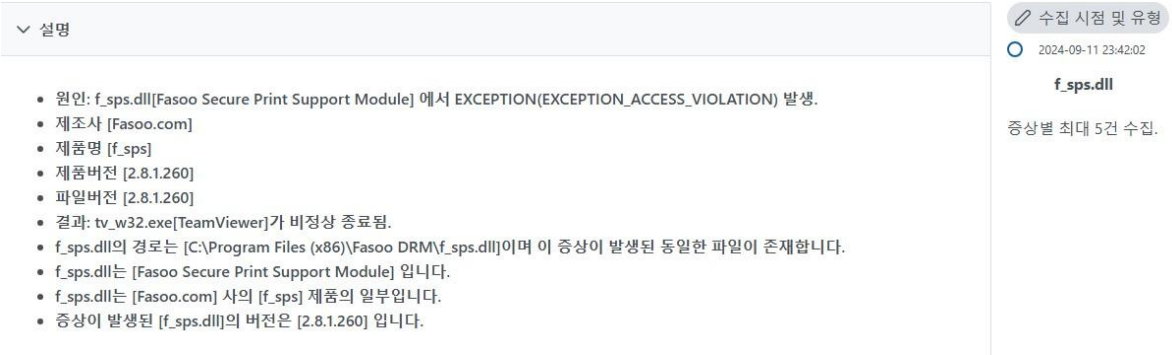
5.7.4.2 문제를 일으킨 원인 정보

"원인" 컬럼을 클릭하면 문제를 일으킨 원인 정보를 볼 수 있습니다. 프로세스가 아닌 파일 정

보이므로, "실행" 탭은 나타나지 않습니다.

[그림 25] 문제를 일으킨 원인 정보

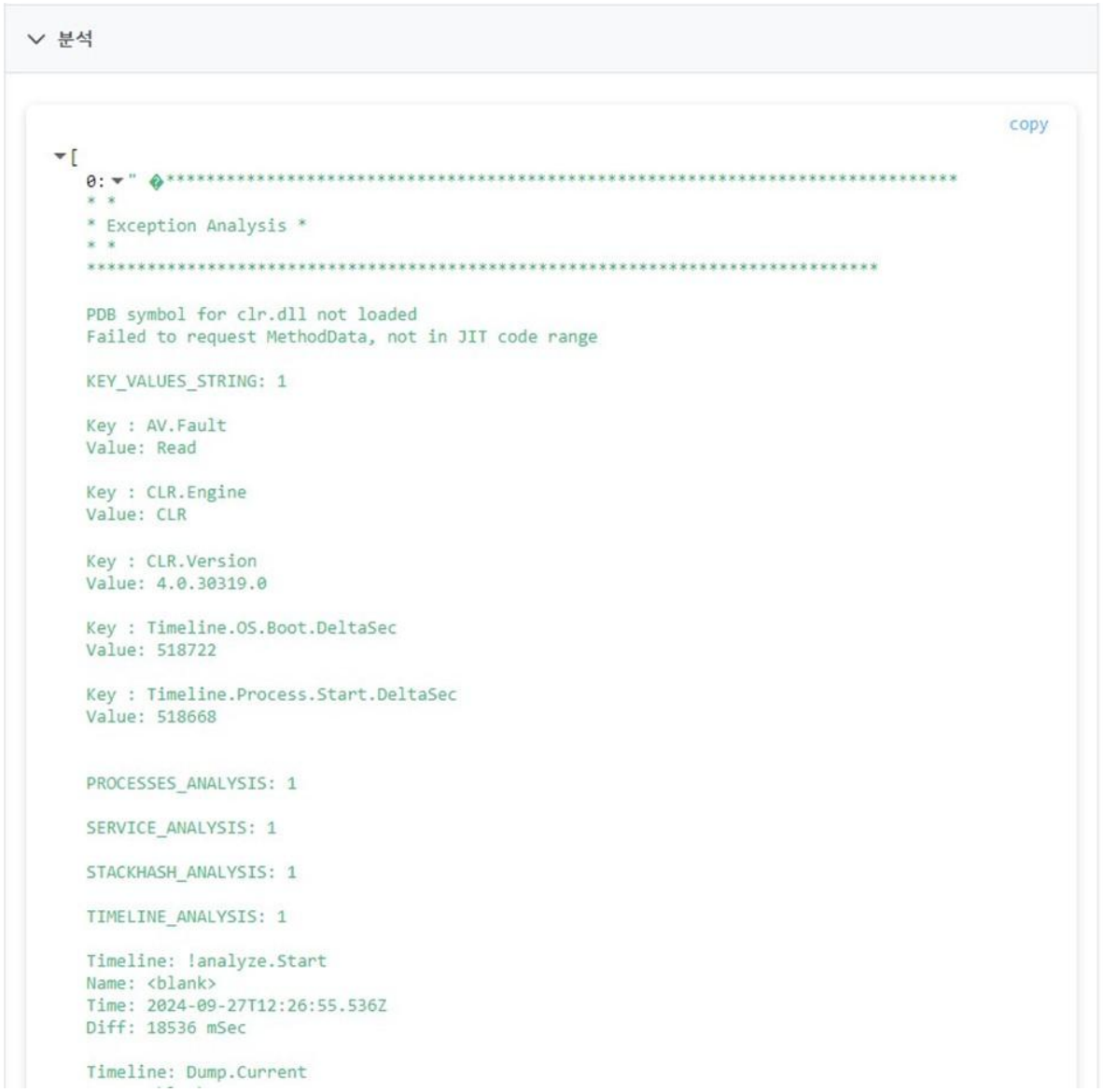
5.7.4.3 증상 설명



[그림 26] 증상 설명

5.7.4.4 개발자들을 위한 WinDbg 분석

증상이 프로세스 비정상 종료인 경우 WinDbg로 분석된 결과와 동일한 내용을 제공합니다.



[그림 27] 증상 분석

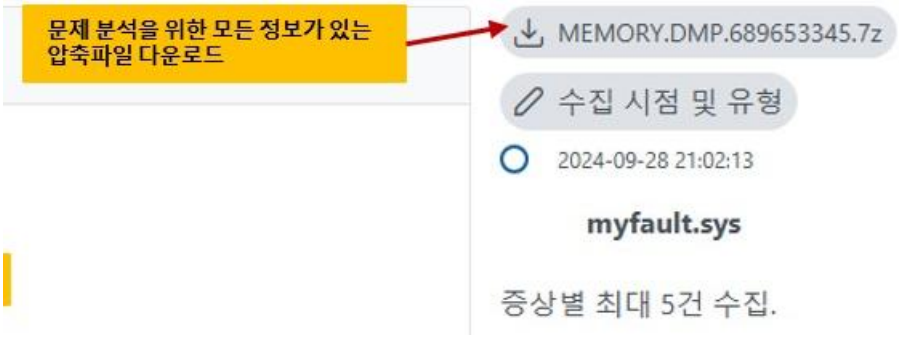
5.7.4.5 함수 호출 분석

[그림 28] 함수 호출 분석

실행 파일의 구조 및 자체 보호를 하는 실행 파일 등의 실행 상황에 따라 함수 호출 분석이 되지 않을 수 있습니다.

5.7.4.6 증상 발생 시점 관련 정보 수집

블루스크린(BSOD), 실행 파일 비정상 종료인 경우, 대상 시스템 또는 프로세스의 메모리 덤프와 관련 파일을 포함한 증상 정보 파일을 7z 방식으로 압축해 제공합니다.



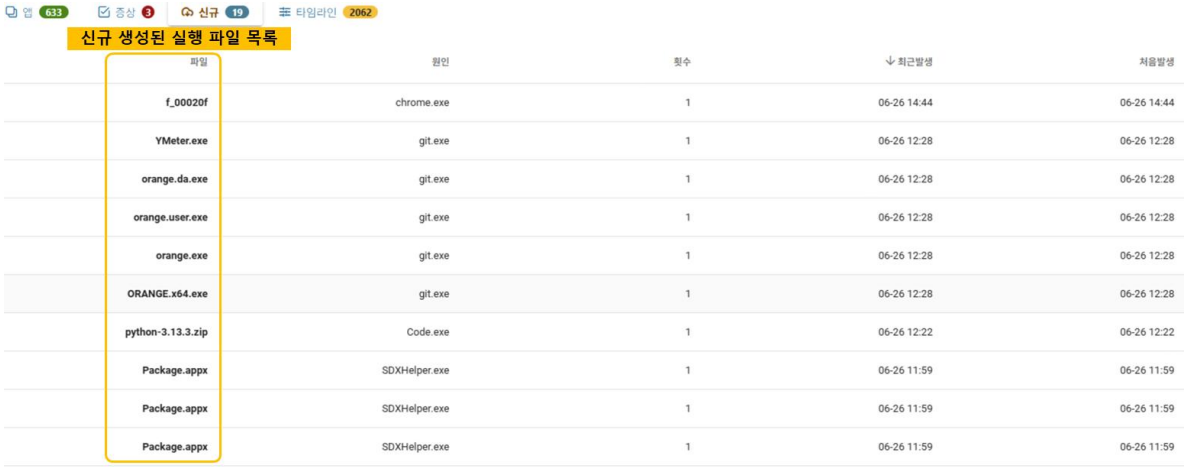
[그림 29] 증상 발생 시점 관련 정보 수집

압축 파일 안에는 아래 내용이 들어 있어 개발사가 해당 문제를 빠르게 분석하고 해결하는 데 큰 도움이 됩니다.

[그림 30] 증상 정보 파일 목록

5.7.5 신규 생성된 실행 파일 정보

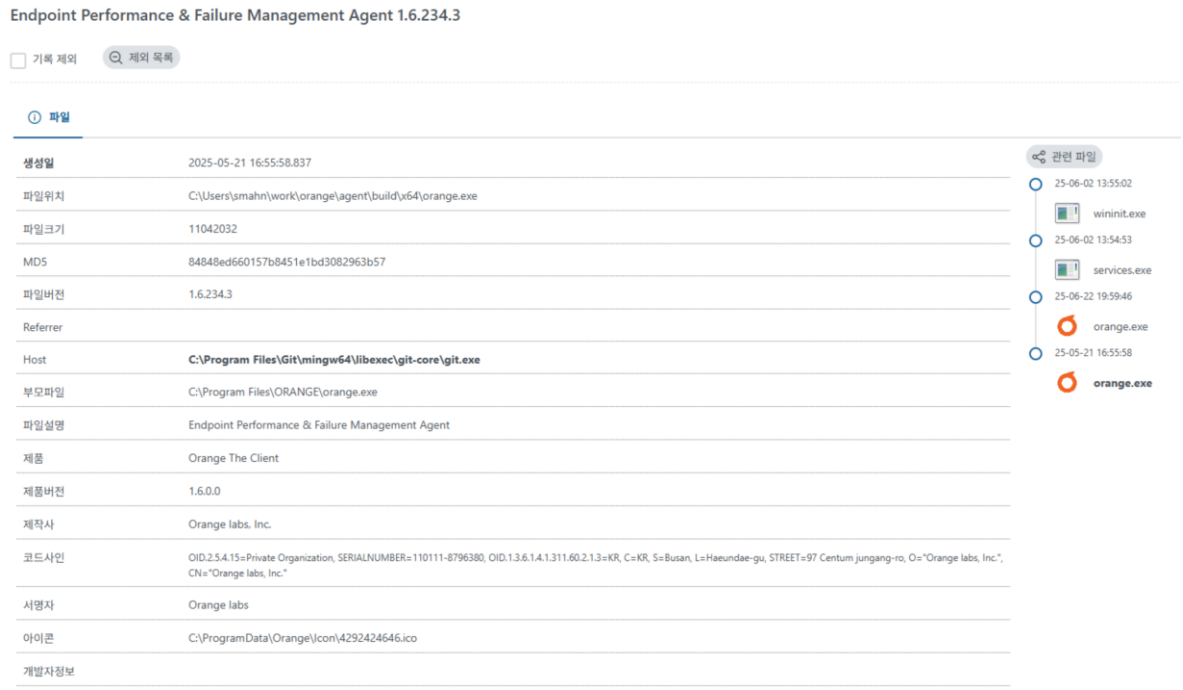
에이전트가 실행된 이후, 새로 생성된 실행 파일의 목록과 개수를 확인할 수 있습니다.



파일	원인	횟수	최근발생	처음발생
f_00020f	chrome.exe	1	06-26 14:44	06-26 14:44
YMeter.exe	git.exe	1	06-26 12:28	06-26 12:28
orange.da.exe	git.exe	1	06-26 12:28	06-26 12:28
orange.user.exe	git.exe	1	06-26 12:28	06-26 12:28
orange.exe	git.exe	1	06-26 12:28	06-26 12:28
ORANGE.x64.exe	git.exe	1	06-26 12:28	06-26 12:28
python-3.13.3.zip	Code.exe	1	06-26 12:22	06-26 12:22
Package.appx	SDXHelper.exe	1	06-26 11:59	06-26 11:59
Package.appx	SDXHelper.exe	1	06-26 11:59	06-26 11:59
Package.appx	SDXHelper.exe	1	06-26 11:59	06-26 11:59

[그림 31] 신규 생성된 실행 파일 목록

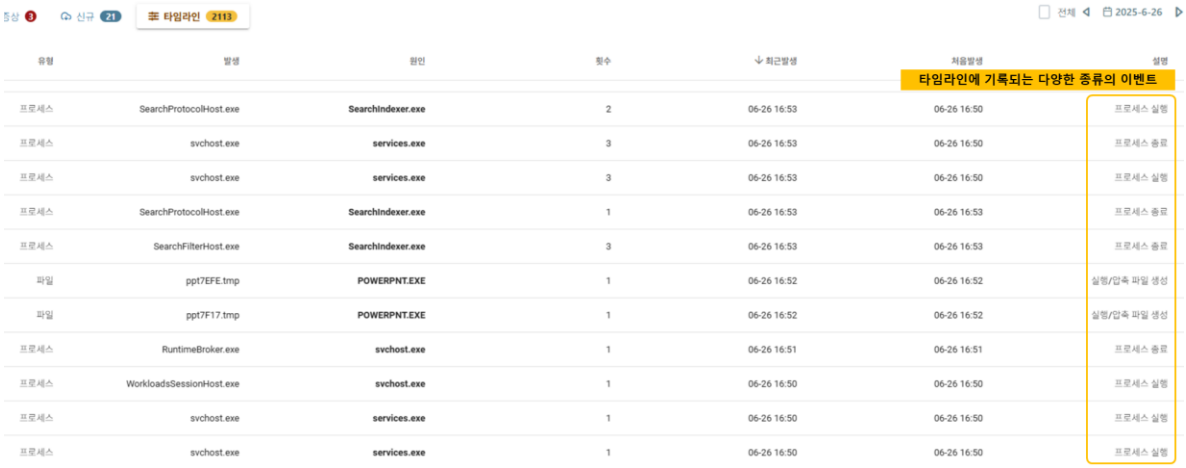
"파일" 컬럼을 클릭하면, 새로 생성된 실행 파일의 상세 정보를 조회할 수 있습니다.



[그림 32] 신규 실행 파일 상세 정보

5.7.6 타임라인

에이전트가 기록 대상인 다양한 이벤트(프로세스의 실행과 종료, 실행 파일과 압축 파일의 생성 등)와 증상의 발생 내역과 횟수를 조회할 수 있습니다.



[그림 33] 타임라인

5.7.7 PC 하드웨어/소프트웨어 정보

[그림 34] PC 하드웨어/소프트웨어 정보

홈 화면 상단 좌측에 표시된 Windows 명칭을 클릭하면 PC 하드웨어/소프트웨어 세부 정보가 표시됩니다.

5.7.7.1 설치 프로그램 정보

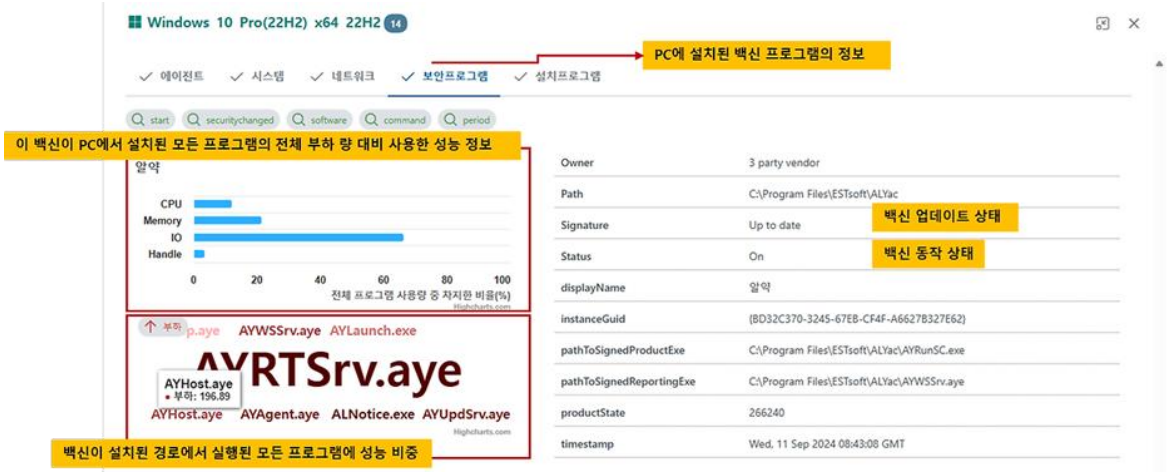
Orange The Client는 다릅니다. 그저 설치된 프로그램 목록만 표시하지 않습니다. 평소 수집된 성능 정보를 바탕으로 설치된 프로그램을 발생 부하 순으로 보여줍니다.

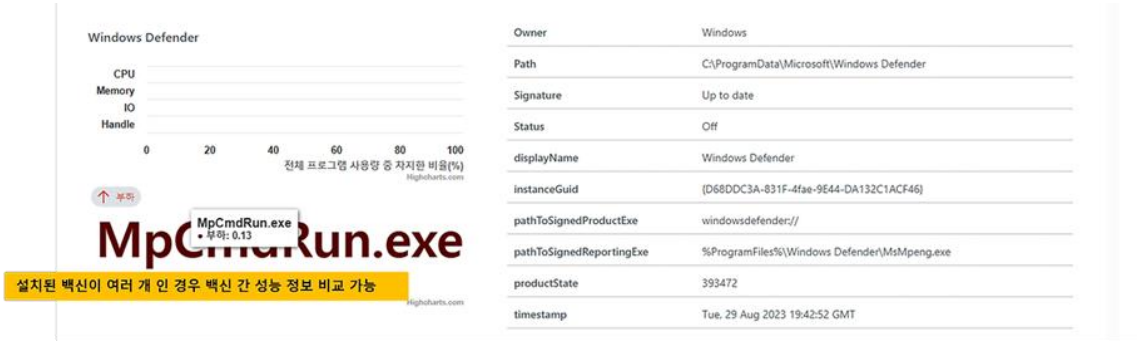
[그림 35] 설치 프로그램 정보

수집된 성능 정보가 필요하므로 설치 직후에는 나오지 않을 수 있습니다.
설치 프로그램에 따라 윈도우 프로그램 설치 정보에 자신의 설치 경로가 설정되지 않는 경우도 있으며, 이런 경우 성능 정보는 표시되지 않을 수 있습니다.

5.7.7.2 보안프로그램

PC에 설치된 백신 프로그램들의 성능 정보가 표시됩니다.
백신 프로그램이 스스로 자신을 백신 프로그램으로 시스템에 등록한 프로그램에 한해 표시되며, 백신 프로그램이 자신을 중복해 등록해 놓은 경우 중복해서 표시됩니다.

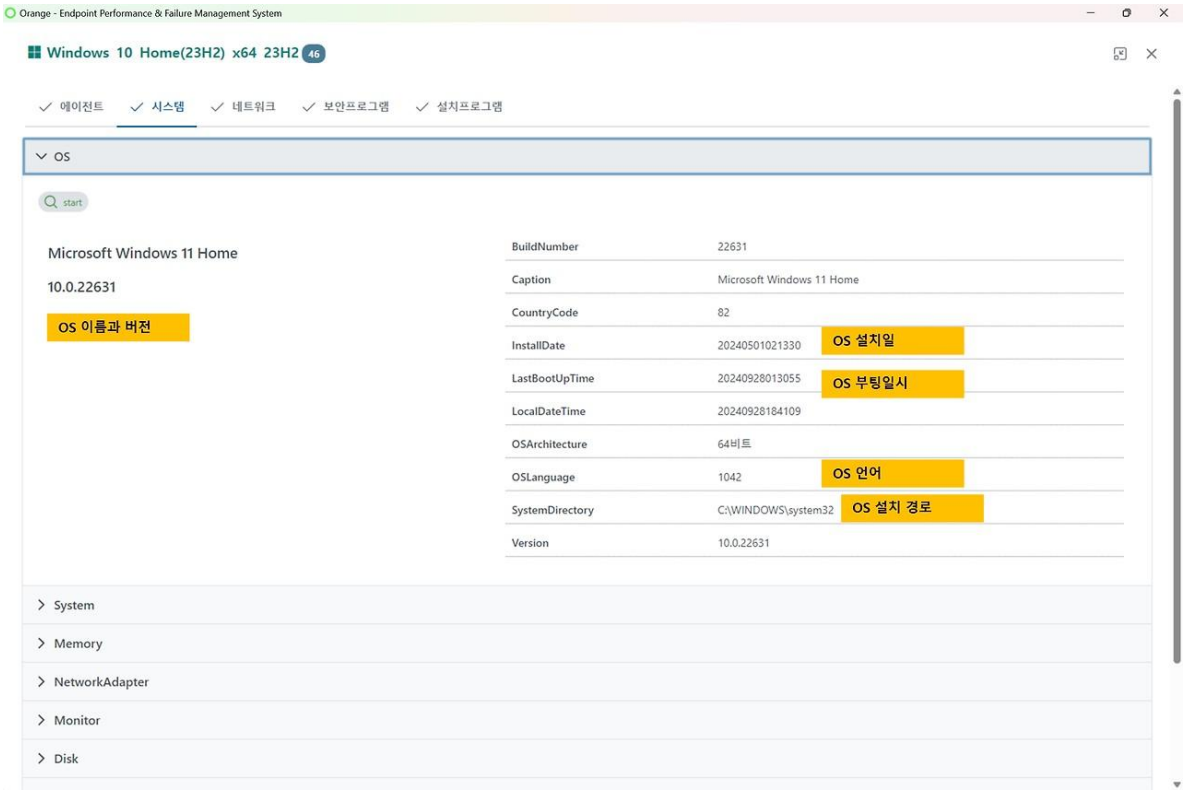




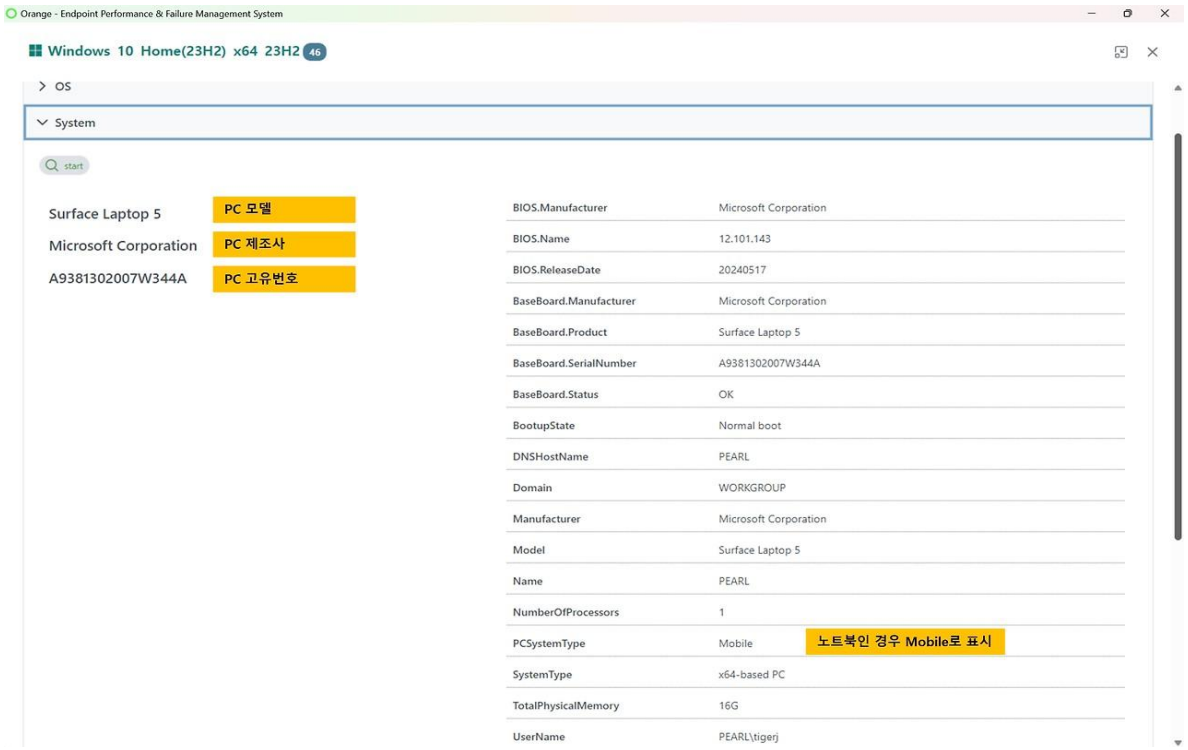
[그림 36] 보안프로그램 정보

5.7.7.3 시스템

PC에 설치된 OS, System, Memory, NetworkAdapter, Monitor, Disk, DiskDrive, Printer, VideoCard, Fan과 같은 하드웨어 정보가 표시됩니다. 하드웨어 정보는 시스템에 해당 내용이 등록된 경우 표시됩니다. 하드웨어에 따라 실제로 존재하지만 시스템에 제대로 등록되지 않는 경우에는 표시되지 않습니다.



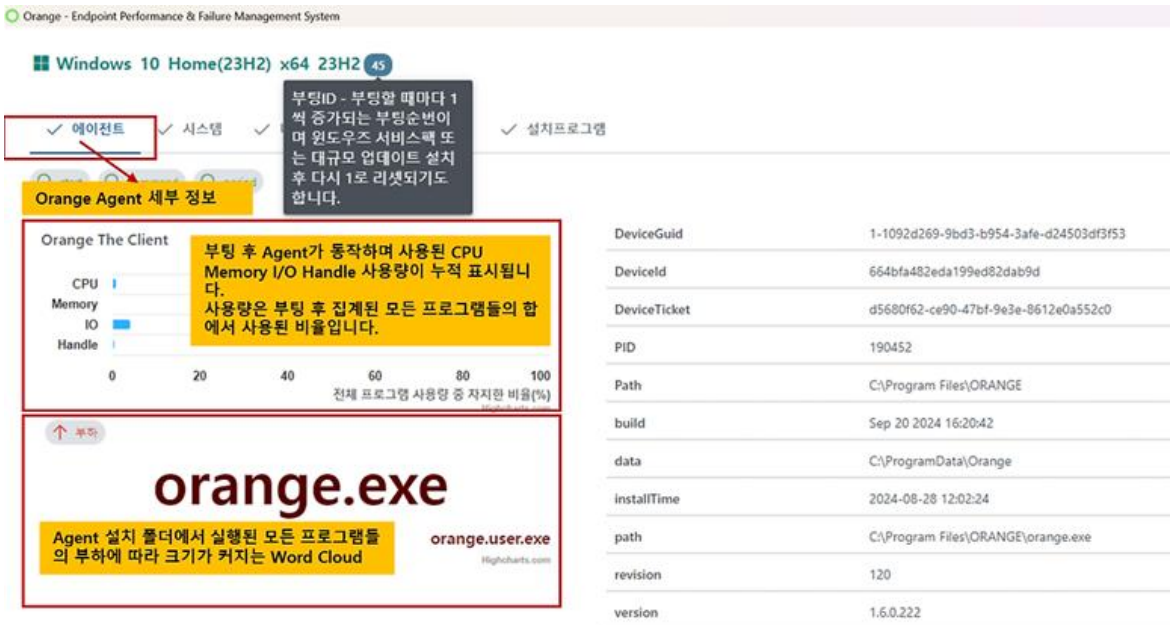
[그림 37] 시스템 정보(OS)



[그림 38] 시스템 정보(System)

5.7.7.4 에이전트

정보를 수집하는 **Orange The Client** 에이전트의 사용 부하를 직관적으로 보여줍니다.
CPU 등의 사용량 정보는 이 PC에서 실행된 모든 프로그램들의 합산된 부하 중 차지한 비율로, 평소 부하가 적은 PC인 경우 전체 사용량이 적어 **Orange The Client**의 비율이 높아질 수 있습니다.

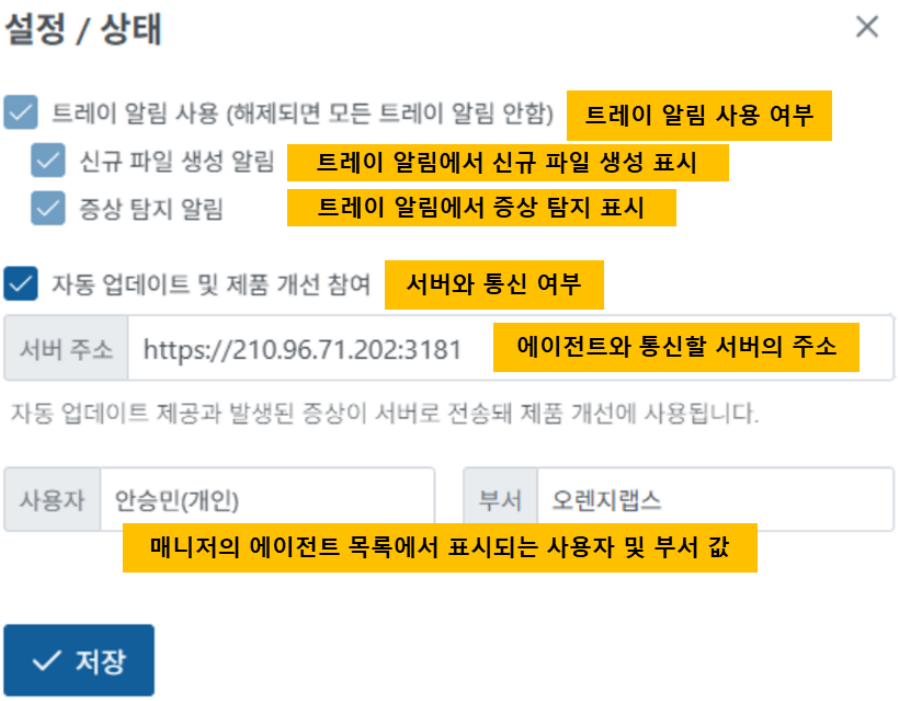


[그림 39] 에이전트 정보

5.8 설정

에이전트 UI의 우측 상단의 톱니바퀴 버튼을 선택하면 에이전트 설정에 진입할 수 있습니다.

[그림 40] 에이전트 설정 버튼



[그림 41] 에이전트 설정

"트레이 알림 사용"은 에이전트의 트레이 알림 기능을 사용할지 여부를 결정합니다. 세부 옵션인 "신규 파일 생성 알림"은 트레이 알림에서 신규 실행 파일 생성을 표시할지 여부를 결정하며, "증상 탐지 알림"은 증상 탐지를 표시할지 여부를 결정합니다.

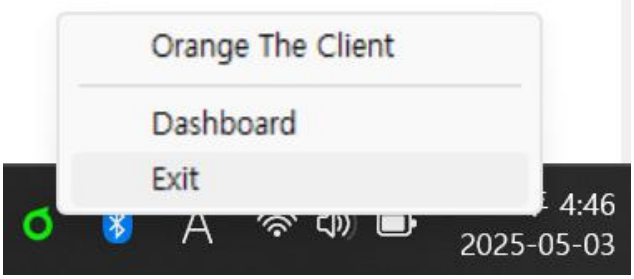
"자동 업데이트 및 제품 개선 참여"는 에이전트가 서버와 통신을 지속할지 여부를 결정합니다. 해당 옵션이 선택이 되어 있고 서버와 통신이 정상적으로 수행되고 있으면 매니저 화면에서 에이전트는 온라인 상태로 표시됩니다. 선택이 되어 있지 않다면 매니저 화면에서 에이전트는 오프라인 상태로 표시됩니다.

또한 "자동 업데이트 및 제품 개선 참여"가 선택이 되면, 설정의 "저장" 버튼을 클릭할 때, 에이전트는 서버로부터 상단의 트레이 알림에 대한 설정 값들을 불러옵니다. 선택이 된 경우에 상단의 트레이 알림 관련 설정 값들을 에이전트 자체적으로 수정하는 기능이 모두 비활성화되는 것은 이 때문입니다.
선택이 되어 있지 않다면, 이러한 서버와의 설정 동기화 동작은 발생하지 않으며 에이전트는 서버와 무관하게 자신만의 설정 값들을 사용하게 됩니다.

5.9 종료 및 재시작

5.9.1 종료

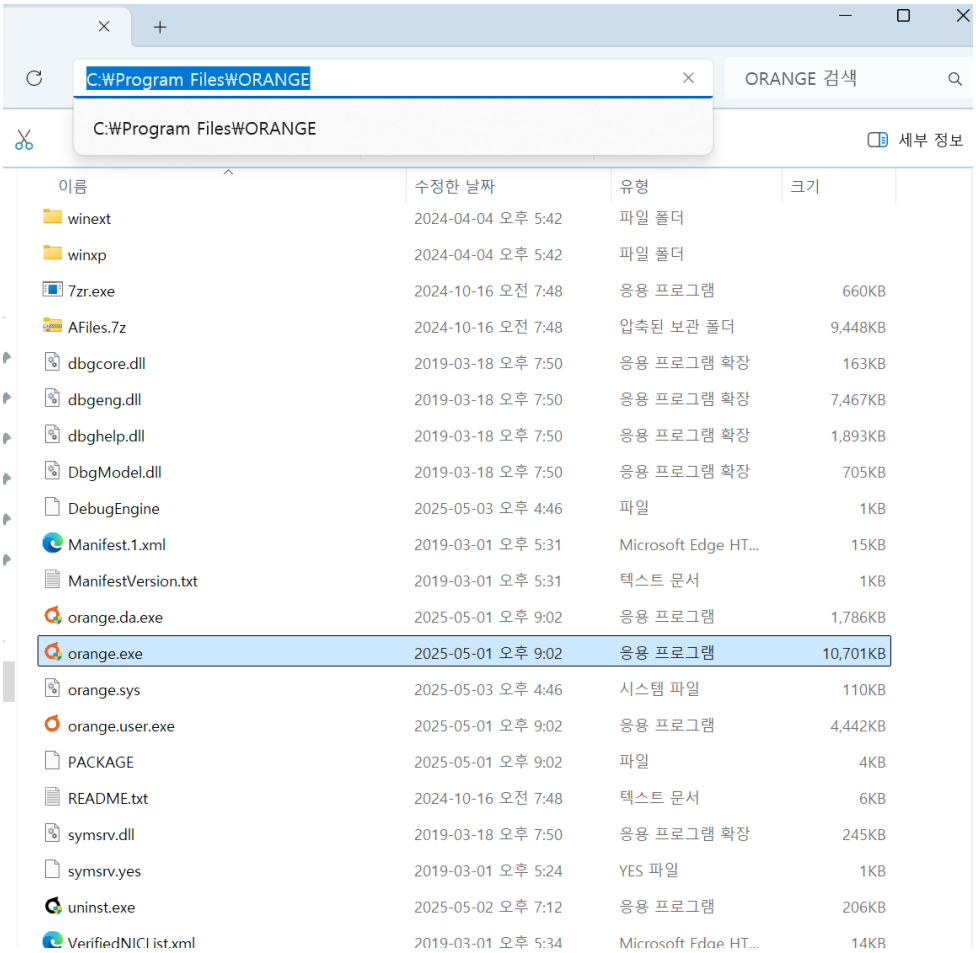
에이전트를 종료하려면, 트레이에서 Exit 버튼을 클릭하면 됩니다.



[그림 42] 트레이로 에이전트 종료

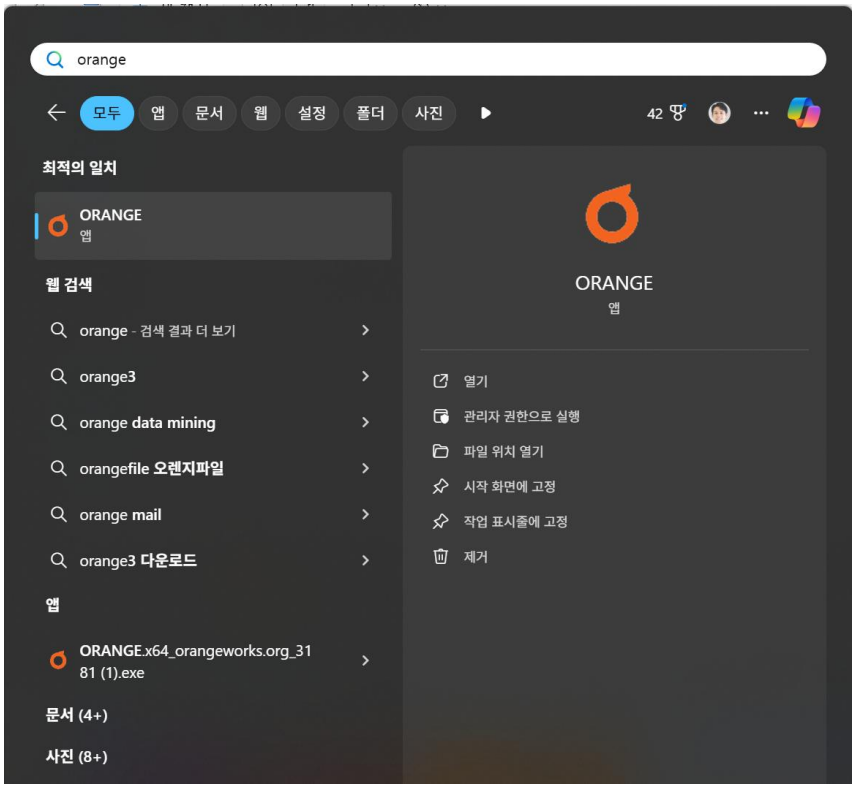
5.9.2 재시작

에이전트 종료 이후 재시작하려면, 프로그램 위치로 이동하여 orange.exe를 실행하면 됩니다.



[그림 43] 에이전트 실행 파일

또는 윈도우 작업표시줄의 시작 버튼 클릭 후, "orange"를 검색하여 실행하면 됩니다.

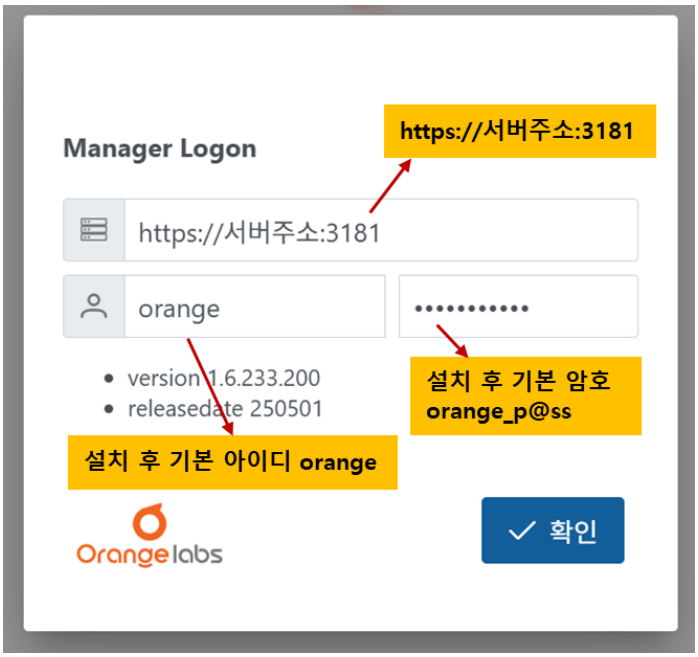


[그림 44] orange 검색 후 실행

6 매니저 사용 가이드

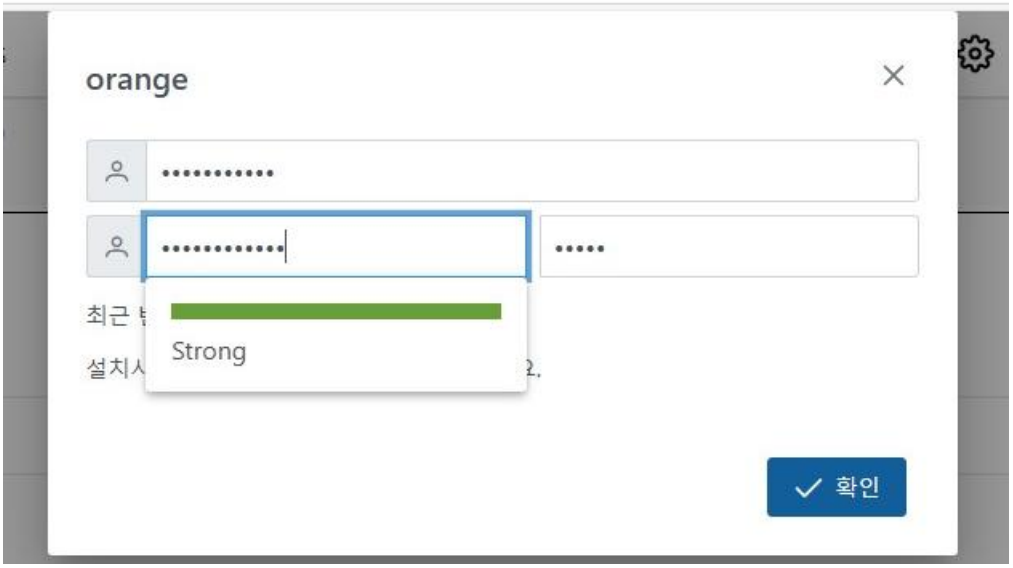
본 장은 기업 관리자에게 **Orange The Client**의 관리 콘솔을 제공하는 매니저에 대해 설명합니다. 매니저를 통해 수집된 정보를 확인하고 연결된 PC들을 원격으로 관리할 수 있습니다.

6.1 로그온



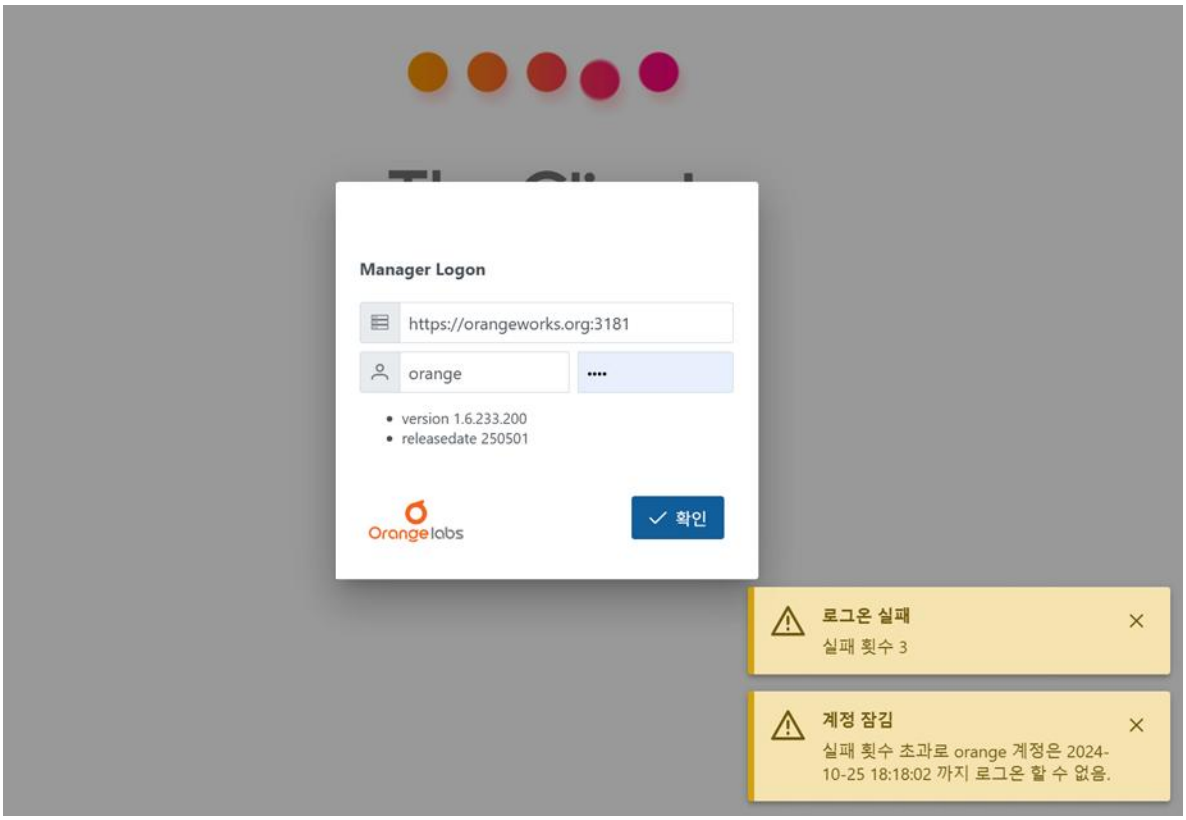
[그림 45] 매니저 로그온 화면

설치 후 기본 아이디는 orange, 비밀번호는 orange_p@ss로 설정됩니다. 해당 비밀번호를 사용하여 최초 로그온 후, 변경이 필요합니다. 이를 위한 비밀번호를 변경창이 표시됩니다.



[그림 46] 비밀번호 변경 화면

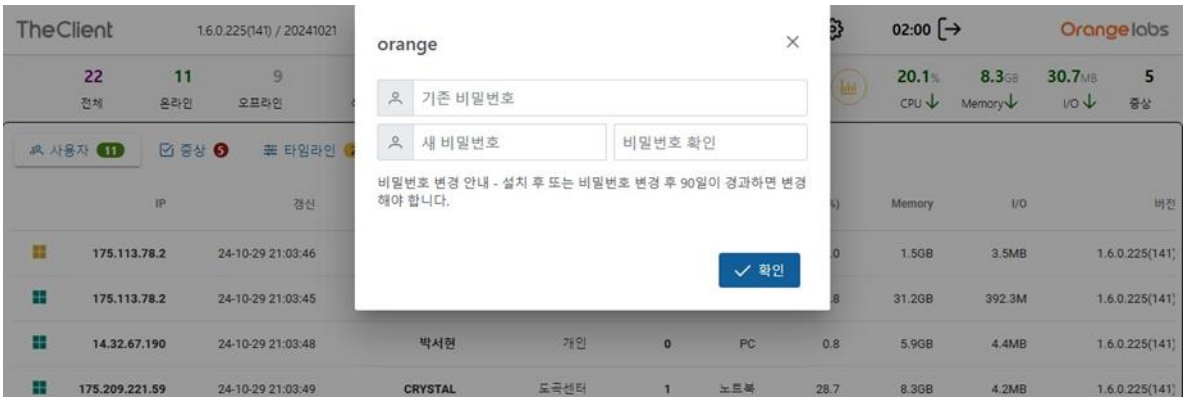
비밀번호는 숫자와 특수문자 각 1자 이상, 영문은 2자 이상 포함된 8자 이상 문자열로 사용해야 하며 공백이 없어야 합니다.
3회 이상 로그온 정보가 틀릴 경우, 해당 관리자 계정은 1시간 동안 접근할 수 없게 잠기게 됩니다.



[그림 47] 로그온 실패 화면

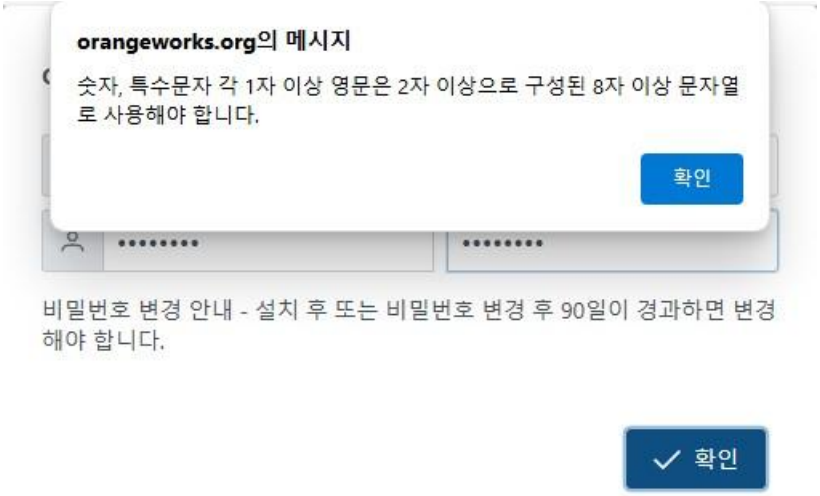
6.2 관리자 비밀번호 변경

최초 설치 후, 비밀번호 변경 후 90일이 경과하면 비밀번호를 변경하도록 설정창이 표시됩니다.



[그림 48] 관리자 비밀번호 변경

6.2.1 비밀번호 규칙



[그림 49] 비밀번호 규칙

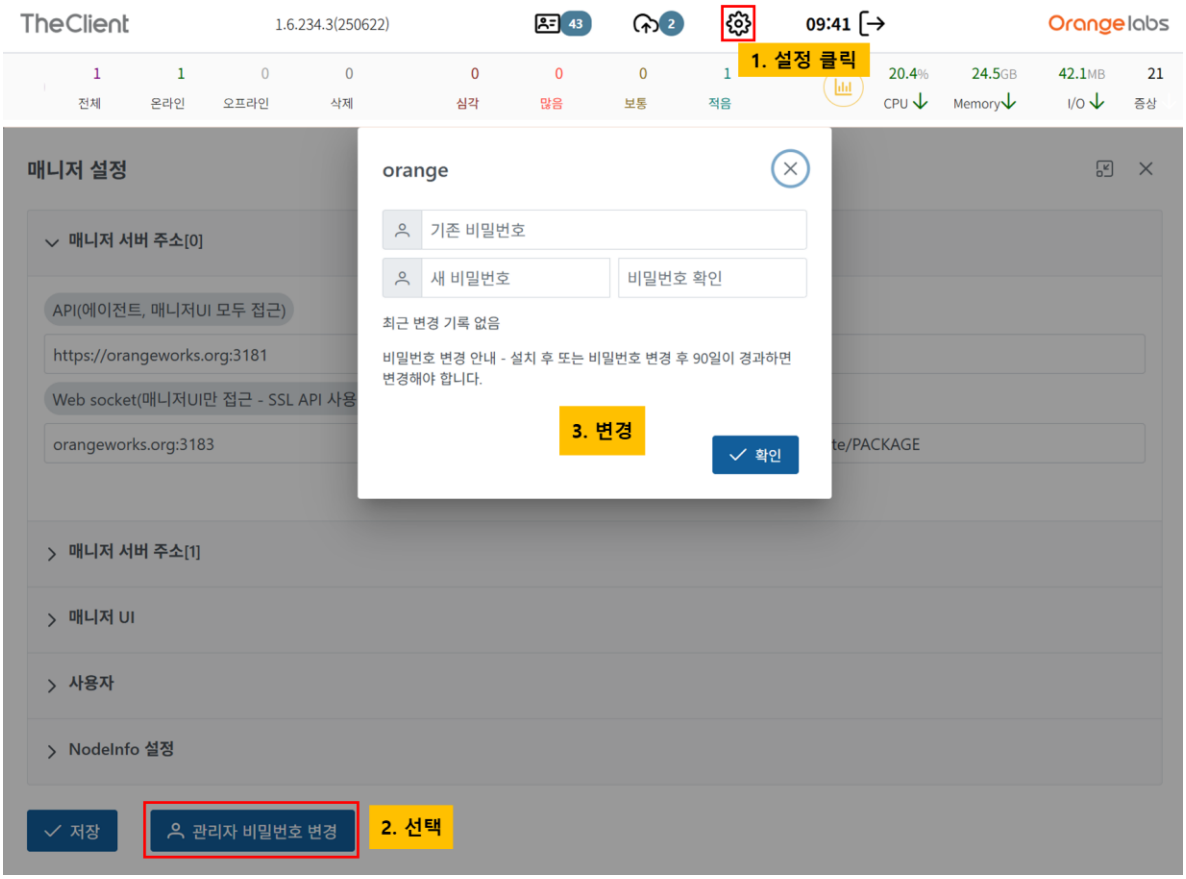
관리자 비밀번호는 bcrypt hash 방식으로 저장되고 매번 로그온마다 내용이 갱신됩니다.
DB에 저장된 관리자 비밀번호가 유출돼도 관리자 비밀번호를 유추할 수 없습니다. 또한 최근 변경된 비밀번호 10개가 저장되어, 이전에 사용한 비밀번호는 재사용할 수 없습니다.

[그림 50] 관리자 비밀번호가 DB에 저장되는 방식

DB에는 위와 같은 방식으로 내용이 저장됩니다.

6.2.2 비밀번호 변경

필요시 직접 비밀번호를 변경할 수 있습니다. 비밀번호는 숫자와 특수문자 각 1자 이상, 영문은 2자 이상 포함된 8자 이상 문자열로 사용해야 하며 공백이 없어야 합니다.



[그림 51] 직접 비밀번호 변경

6.3 자동 로그아웃

일정 시간 관리자 입력이 없는 경우 매니저는 자동으로 로그아웃 됩니다.

[그림 52] 자동 로그아웃 설정

"설정 > 매니저UI > 자동 로그아웃"에서 자동 로그아웃 시간을 조정할 수 있으며, 1초 이상 600

초 이하로 설정할 수 있습니다.

[그림 53] 자동 로그아웃 시간 표시

남은 시간은 화면 상단 좌측에 표시되며 시간이 초과되면 자동으로 로그아웃되어 다시 로그온 화면이 표시됩니다.

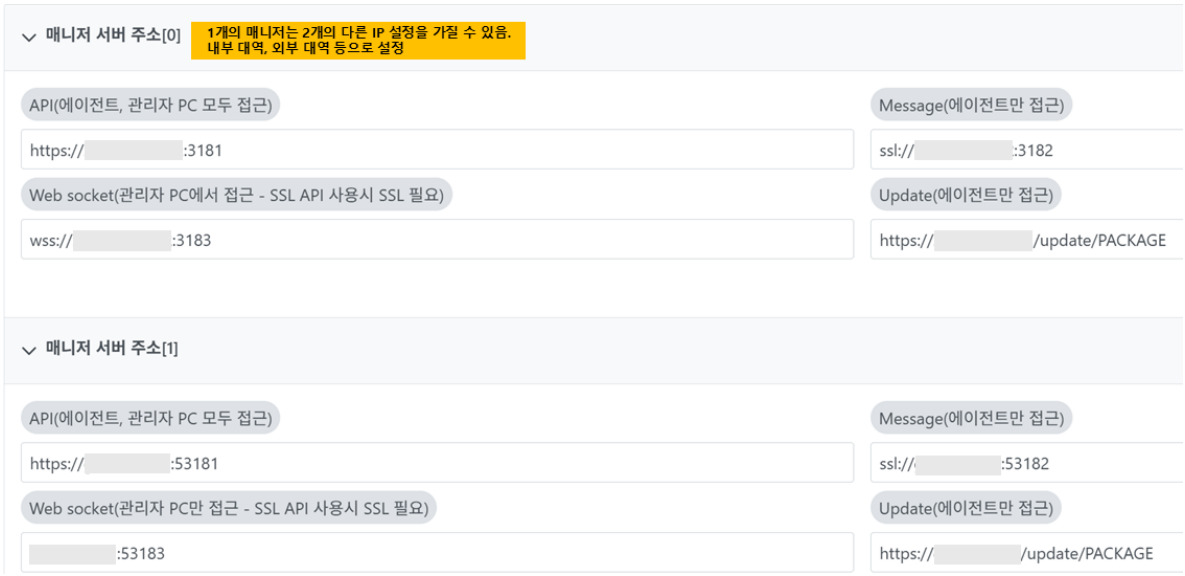
6.4 홈 화면 구성

전체적인 매니저 홈 화면 구성은 아래 그림과 같습니다.

[그림 54] 홈 화면 구성

6.5 설정

6.5.1 매니저 서버 주소



[그림 55] 매니저 서버 주소 설정

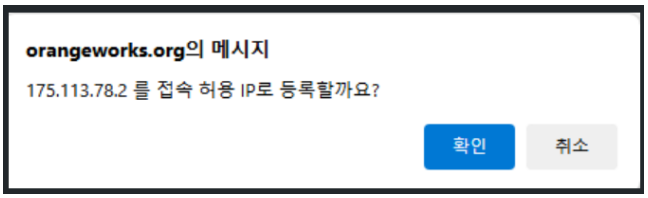
한 대의 서버에 2개까지 서로 다른 IP 또는 도메인명을 서버 주소로 설정할 수 있습니다. 에이전트는 2개의 서버 주소 중 자신이 연결 가능한 서버로 연결합니다. 노트북 사용자가 사내, 사외에서 번갈아 사용하면 에이전트는 상태에 따라 접근 가능한 서버로 연결됩니다.

6.5.2 매니저

[그림 56] 매니저 UI 설정

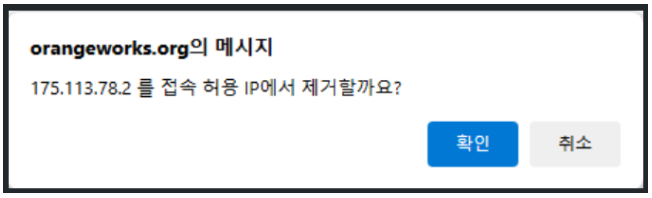
"동일 관리자 아이디 중복 로그인 방지 설정"의 경우, 변경 후 관리자 로그인을 다시 해야 적

용이 됩니다.
"등록된 IP에서만 접속 허용"에서 접속을 허용할 IP를 등록할 수 있습니다.



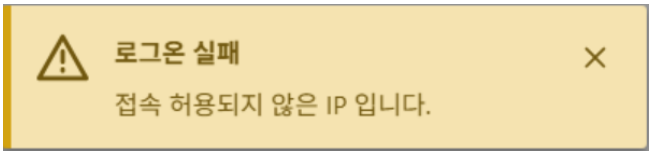
[그림 57] 접속 허용 IP 등록

이미 등록된 IP를 접속 허용 IP 목록에서 제거할 수 있습니다.



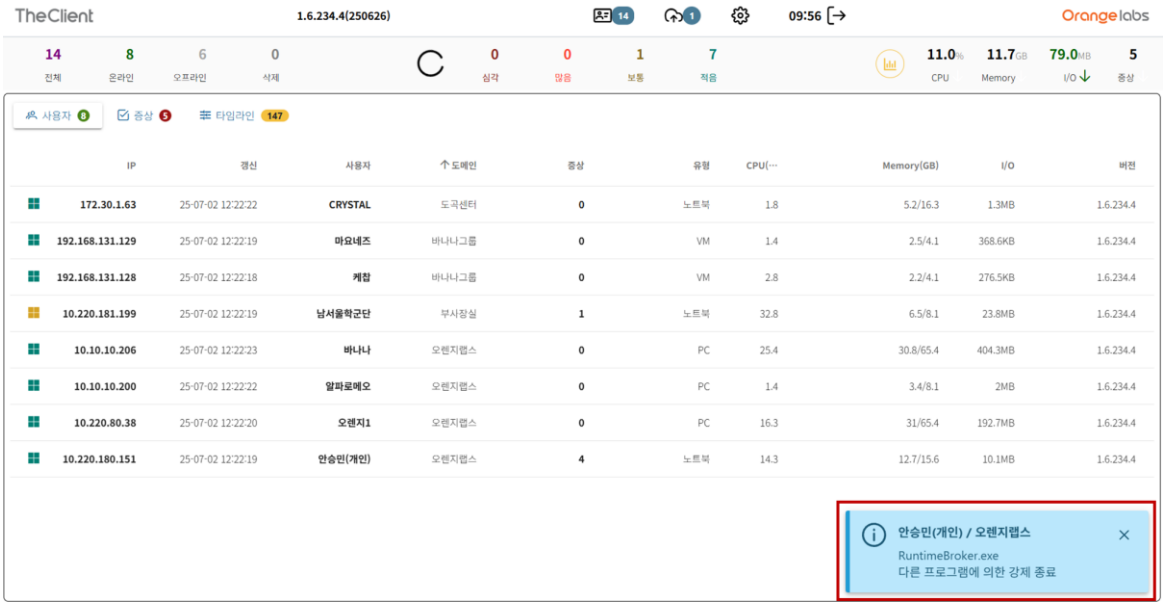
[그림 58] 접속 허용 IP 제거

접속 허용이 되지 않은 IP로 로그온을 시도하는 경우면, 실패하게 됨을 화면 하단에서 확인할 수 있습니다.



[그림 59] 접속 허용되지 않은 IP 로그온 실패

"자동 로그아웃 시간"을 체크하는 경우, 관리자의 입력이 입력한 시간 동안 없으면 자동 로그아웃 됩니다. 최소 60초 이상의 숫자로 설정해야 합니다.
"증상 발생시 알림"를 체크하는 경우, 에이전트에서 증상이 탐지되는 경우 매니저 화면에서 이를 확인할 수 있는 토스트 메시지를 아래와 같이 확인할 수 있습니다.



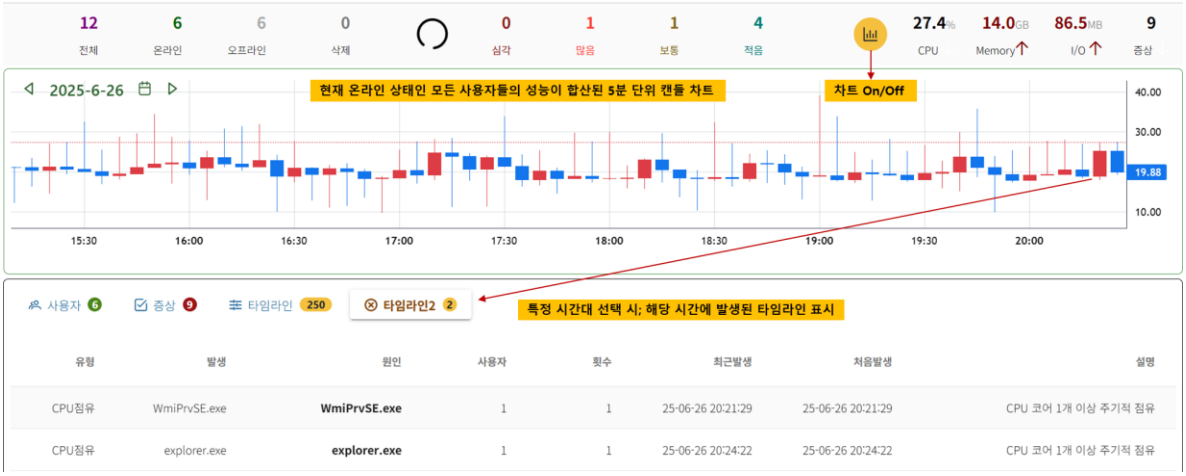
[그림 60] 증상 알림 토스트 메시지

6.5.3 사용자

사용자(에이전트) 측으로 전달되는 설정입니다.

[그림 61] 매니저 사용자(에이전트) 설정

6.6 성능 차트

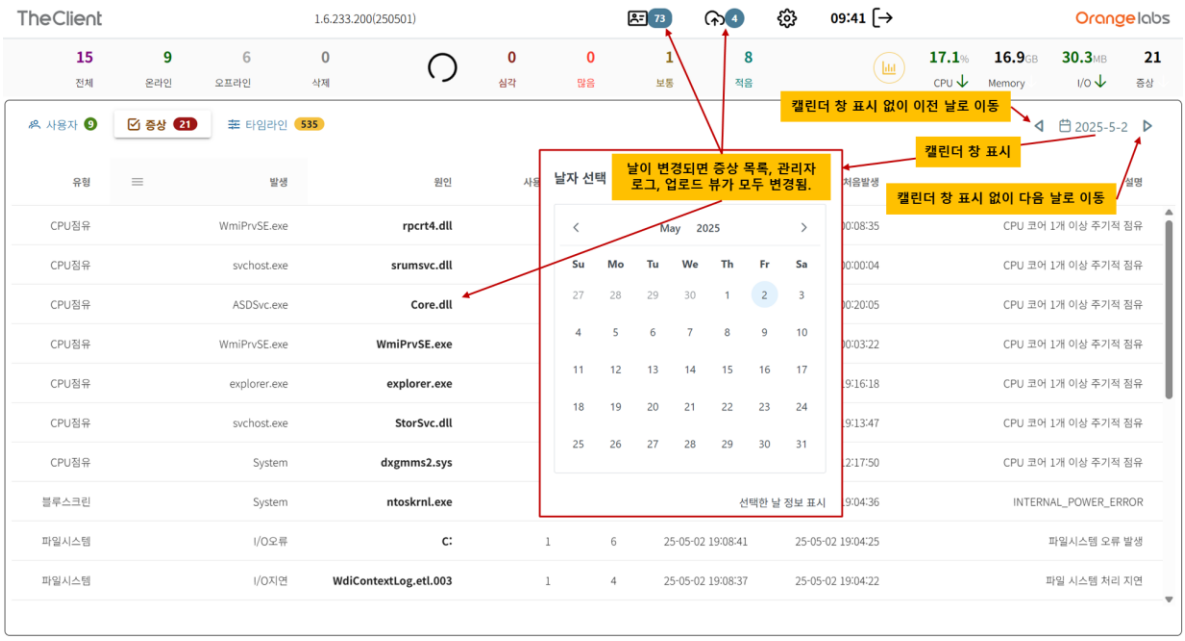


[그림 62] 매니저 성능 차트

성능 차트에는 사내 온라인 상태인 모든 에이전트의 데이터가 합산된 형태로 차트가 5분 단위 캔들(시작, 고점, 저점, 종료) 형태로 표시됩니다. 각 캔들을 클릭하면 해당 시간대에 발생된 타임라인이 하단 목록에 표시됩니다.

6.7 표시 날짜 선택

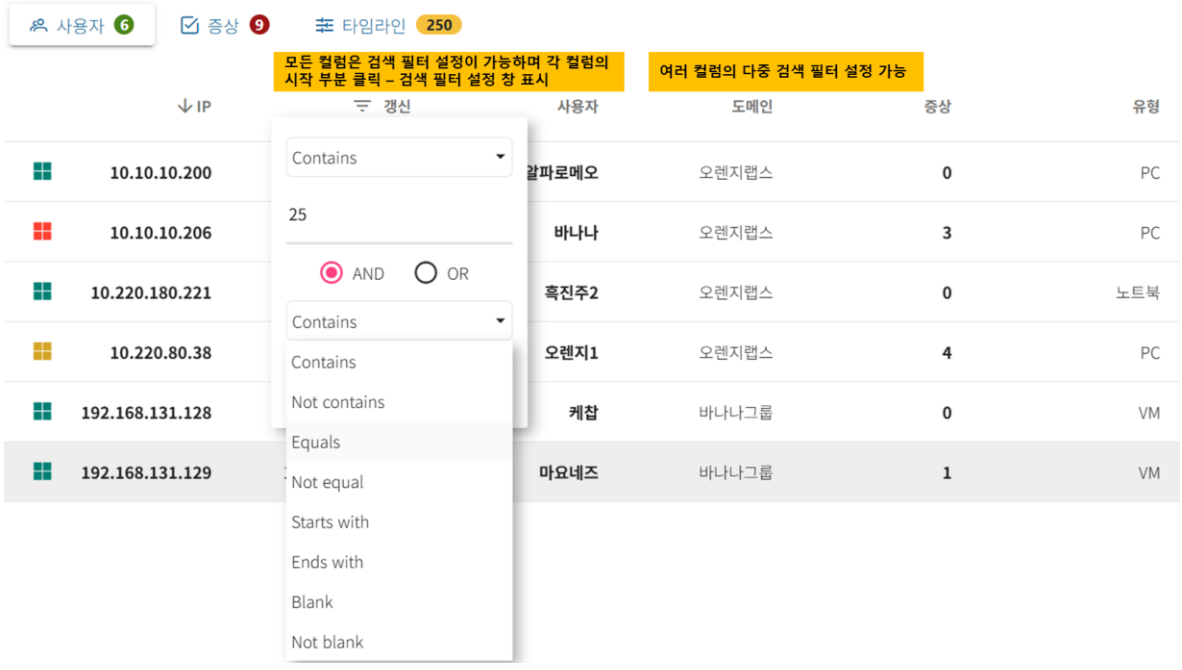
목록 화면의 "증상" 탭은 발생된 증상들이 서버에서 수집한 날짜별로 집계되어 표시됩니다. 매니저는 빠른 검색을 위해 1일 단위로 데이터를 저장하고 표시합니다.



[그림 63] 표시 날짜 선택

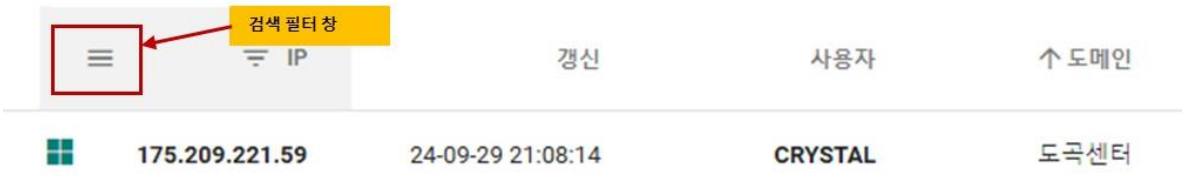
6.8 검색 필터

매니저에서 제공하는 그리드는 검색 필터를 제공합니다.



[그림 64] 검색 필터

검색 필터를 제공하는 컬럼에 마우스를 대면 아래와 같이 검색 필터 창을 호출하는 표시가 나타납니다.



[그림 65] 검색 필터 창 호출

검색 필터는 다중으로 설정 가능하고 이후 검색 필터에 해당되는 데이터만 표시됩니다.

6.9 정렬

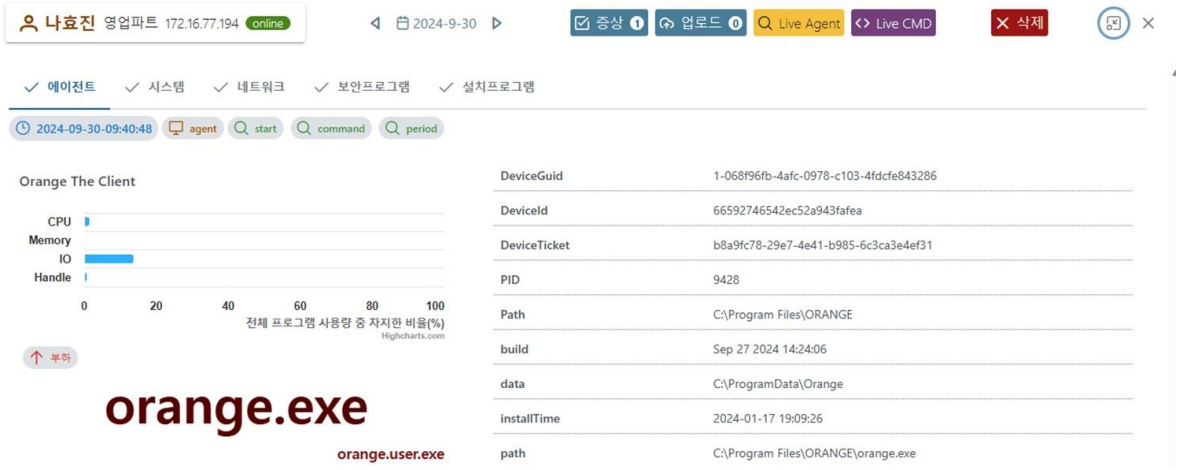
검색 필터 창을 호출하는 표시 외 부분을 누르면 오름차순, 내림차순 정렬이 변경되며 정렬이 설정되면 아래(내림차순) 또는 위(오름차순) 방향 화살표가 표시됩니다.

[그림 66] 정렬 설정 변경

6.10 사용자 정보

어느 목록에서나 사용자를 선택하면 PC의 세부 정보 화면으로 진입합니다.

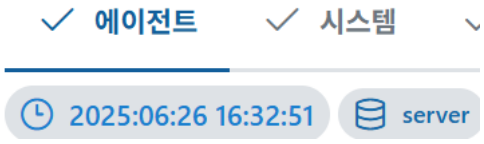
6.10.1 에이전트 정보



[그림 67] 매니저에서 조회한 에이전트 정보

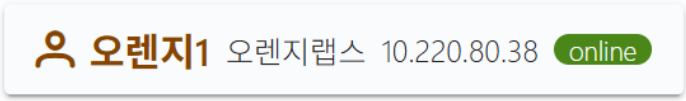
6.10.2 정보 표시 아이콘

매니저는 기본적으로 서버에 저장된 에이전트의 과거 자산 정보를 표시하며, 수집된 시각과 정보 제공자를 표시합니다.



[그림 68] 에이전트 정보 수집 시각 및 정보 제공자

Orange The Client는 실시간 구조로 대상 에이전트가 online인 경우 명령 수집 명령을 발송합니다.

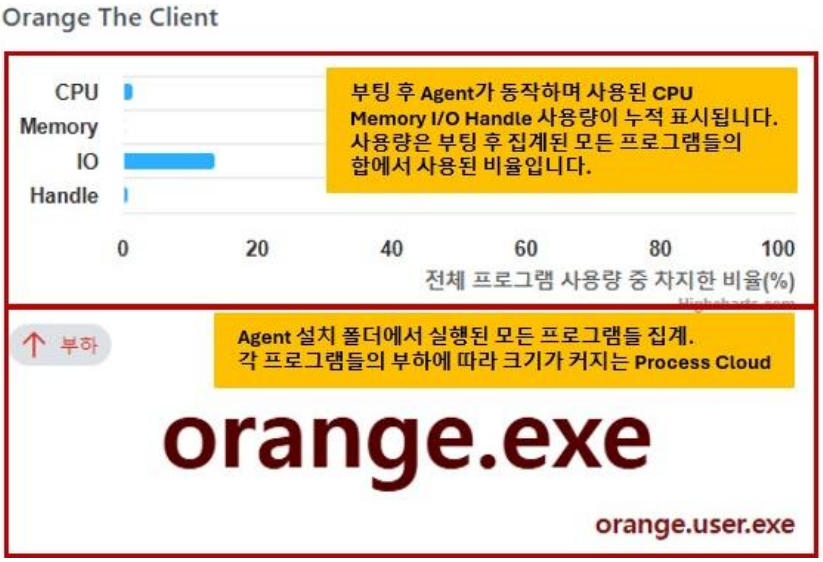


[그림 69] 에이전트의 online 여부

에이전트에서 바로 지금 수집한 정보가 도착하면 수집된 시각과 정보 제공자는 아래와 같이 변경됩니다.

[그림 70] 에이전트 정보 수집 관련 정보

에이전트의 성능 정보를 표시해 성능, 장애 모니터링 과정에서 발생한 부하를 표시합니다.



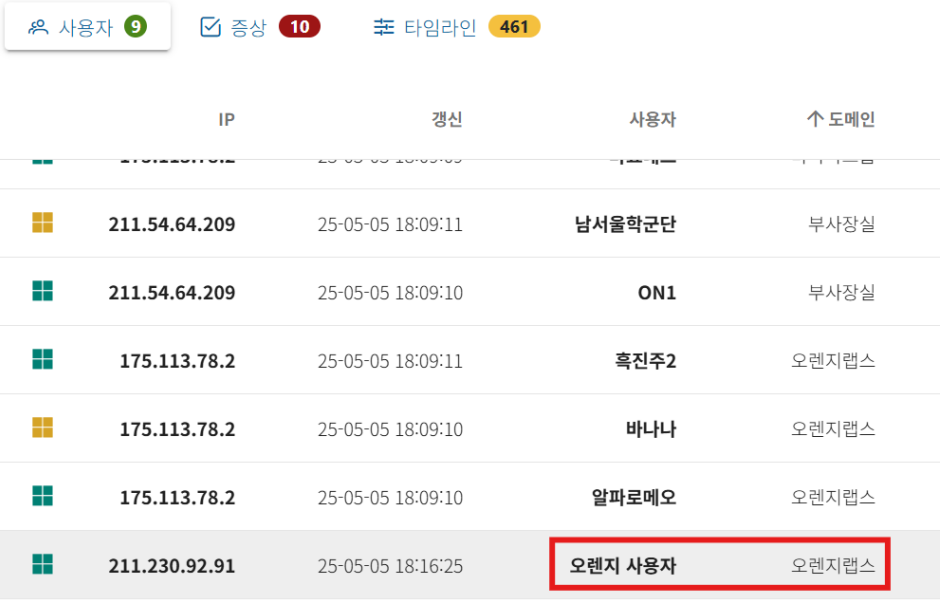
[그림 71] 에이전트 부하 정보

6.10.3 보안 프로그램 등 그 외 항목

"에이전트 사용 가이드" 챕터의 "에이전트 UI > PC 하드웨어/소프트웨어 정보"에 설명된 것과 동일한 내용이 매니저로 표시되며 에이전트가 온라인인 경우 에이전트의 실시간 정보를, 에이전트가 오프라인인 경우 서버에 저장된 정보가 표시됩니다.

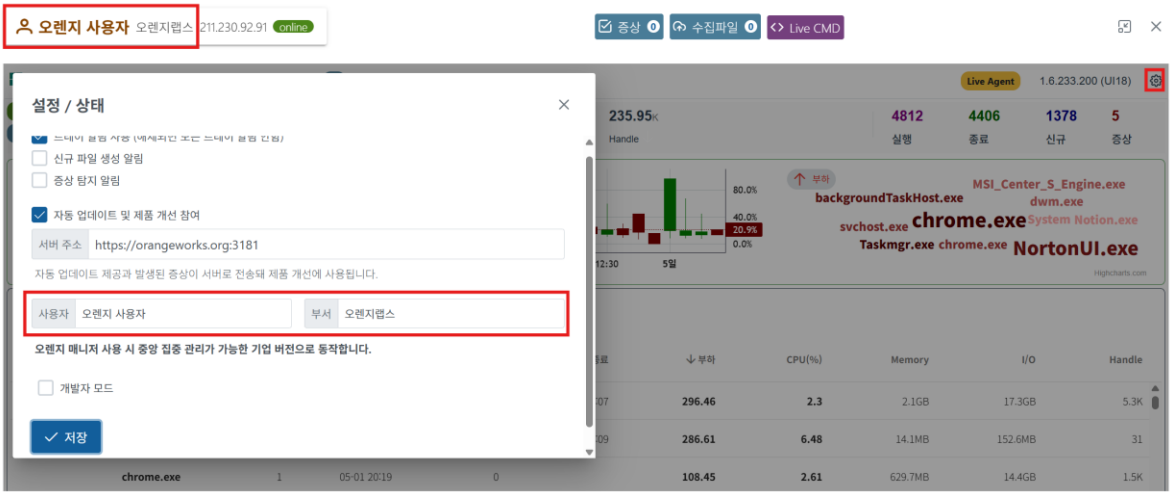
6.10.4 사용자 명 및 도메인 명 변경

사용자 목록에서 아래 그림처럼 나타나는 사용자 명과 도메인 명을 변경할 수 있습니다.



[그림 72] 사용자 목록의 사용자 명 및 도메인 명 확인

사용자 목록에서 "사용자" 컬럼을 클릭한 뒤, 6.11에서 설명할 "Live Agent" 버튼을 클릭하고 우측 상단에 톱니바퀴를 선택하면 아래처럼 사용자 명과 부서 명 값을 입력할 수 있습니다. 해당 값을 입력하면 좌측 상단에서 바뀐 사용자 명과 부서 명을 확인할 수 있고, 사용자 목록에서도 사용자 명 및 도메인 명이 바뀐 것을 확인할 수 있습니다.



[그림 73] Live Agent의 설정에서 사용자 명 및 부서 명 변경

6.11 Live Agent

매니저에서 "Live"로 시작되는 기능(Live Agent와 Live CMD)은 사용자가 온라인으로 표시된 경우 사용 가능합니다.

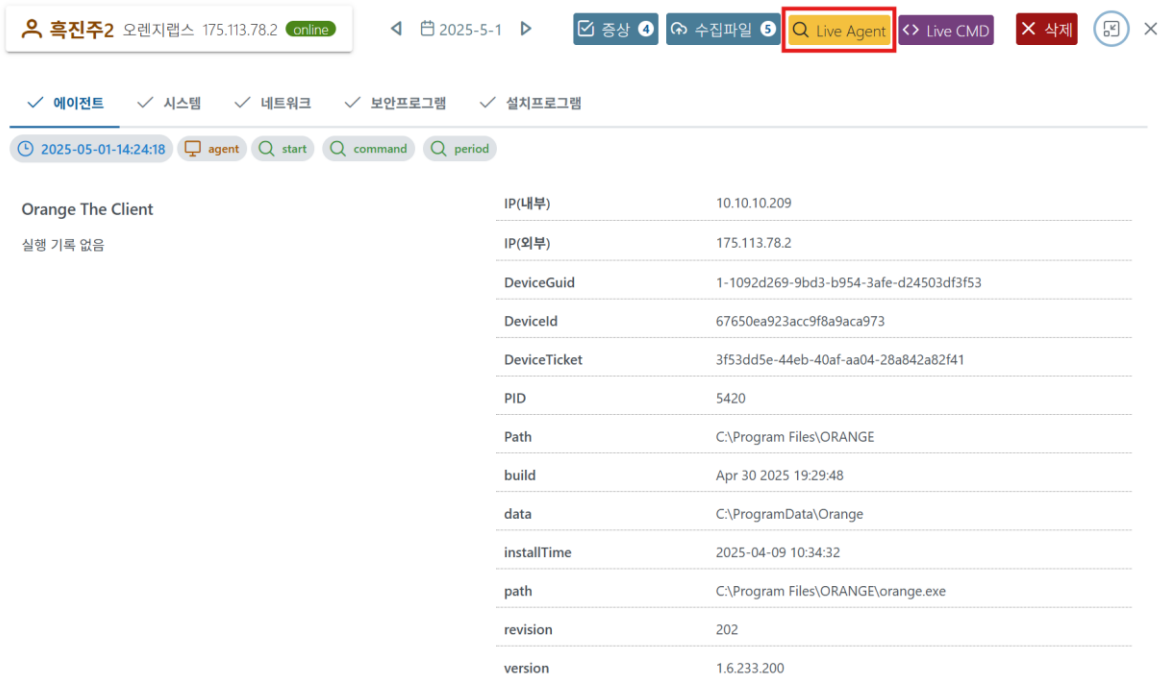
대상 에이전트가 온라인인 경우 매니저에서 에이전트 UI를 실시간으로 표시합니다. 표시되는 정보는 서버가 아닌 에이전트에서 실시간으로 보내온 정보이며, 에이전트 -> 서버 -> 매니저와 같은 데이터 흐름을 거쳐 표시됩니다.

6.11.1 사용 방법

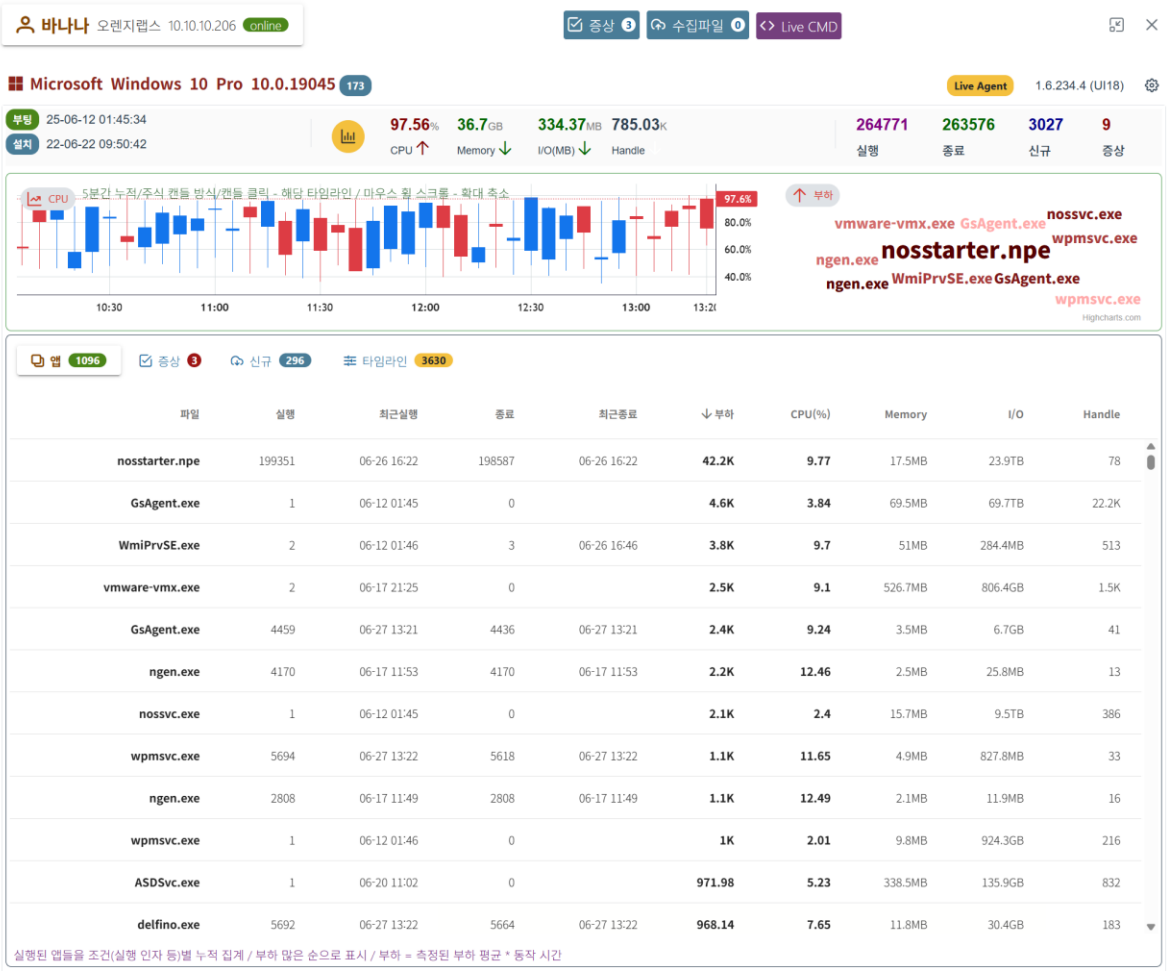
사용자 목록에서 "사용자" 컬럼을 직접 클릭하면 Live Agent를 곧바로 실행할 수 있습니다.

[그림 74] 사용자 목록에서 Live Agent 직접 실행

또는, 사용자 목록에서 "사용자" 컬럼 이외를 클릭하면 세부 정보 화면에 진입하는데, 우측 상단의 Live Agent 버튼을 클릭해도 실행할 수 있습니다.



[그림 75] 사용자 세부 정보 화면에서 Live Agent 버튼 클릭



파일	실행	최근실행	종료	최근종료	↓부하	CPU(%)	Memory	I/O	Handle
nosstarter.npe	199351	06-26 16:22	198587	06-26 16:22	42.2K	9.77	17.5MB	23.9TB	78
GsAgent.exe	1	06-12 01:45	0		4.6K	3.84	69.5MB	69.7TB	22.2K
WmiPrvSE.exe	2	06-12 01:46	3	06-26 16:46	3.8K	9.7	51MB	284.4MB	513
vmware-vmx.exe	2	06-17 21:25	0		2.5K	9.1	526.7MB	806.4GB	1.5K
GsAgent.exe	4459	06-27 13:21	4436	06-27 13:21	2.4K	9.24	3.5MB	6.7GB	41
ngen.exe	4170	06-17 11:53	4170	06-17 11:53	2.2K	12.46	2.5MB	25.8MB	13
nossvc.exe	1	06-12 01:45	0		2.1K	2.4	15.7MB	9.5TB	386
wpmsvc.exe	5694	06-27 13:22	5618	06-27 13:22	1.1K	11.65	4.9MB	827.8MB	33
ngen.exe	2808	06-17 11:49	2808	06-17 11:49	1.1K	12.49	2.1MB	11.9MB	16
wpmsvc.exe	1	06-12 01:46	0		1K	2.01	9.8MB	924.3GB	216
ASDSvc.exe	1	06-20 11:02	0		971.98	5.23	338.5MB	135.9GB	832
delfino.exe	5692	06-27 13:22	5664	06-27 13:22	968.14	7.65	11.8MB	30.4GB	183

[그림 76] Live Agent 화면

6.12 Live CMD

Live CMD는 매니저에서 원격으로 사용자 PC의 윈도우 CMD를 호출하고 결과를 확인할 수 있는 기능입니다.

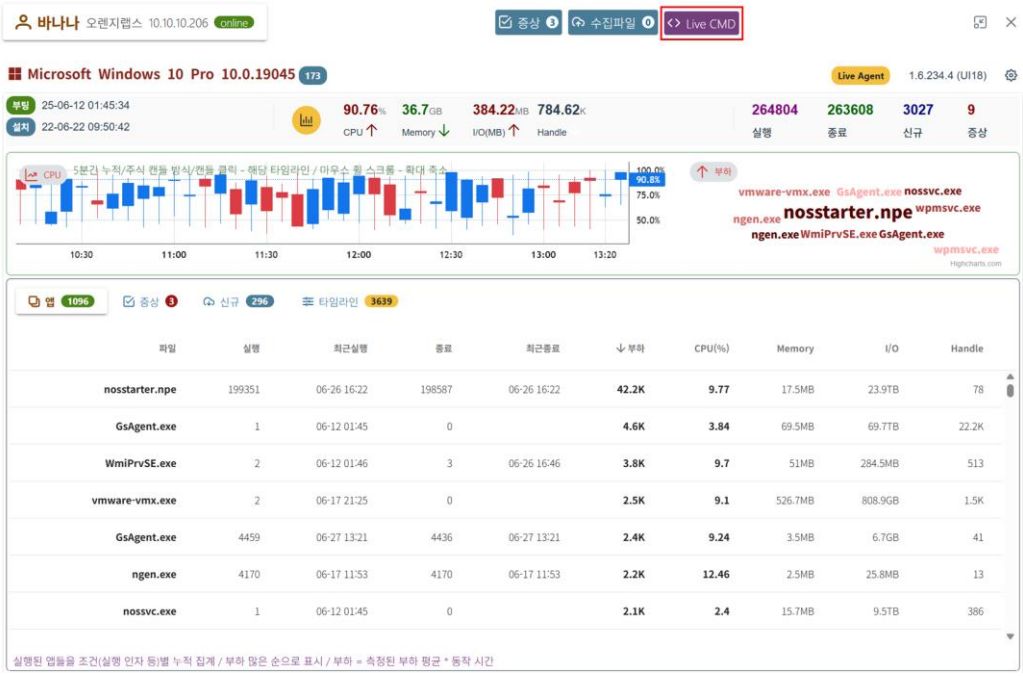
서버에 저장되지 않고 매니저에 의해 제공되지 않는 더 자세한 정보를 사용자 PC와 실시간 연결해 확인하고, 추가적인 명령을 수행하거나 필요한 파일을 수집할 수 있습니다.

6.12.1 시작 방법

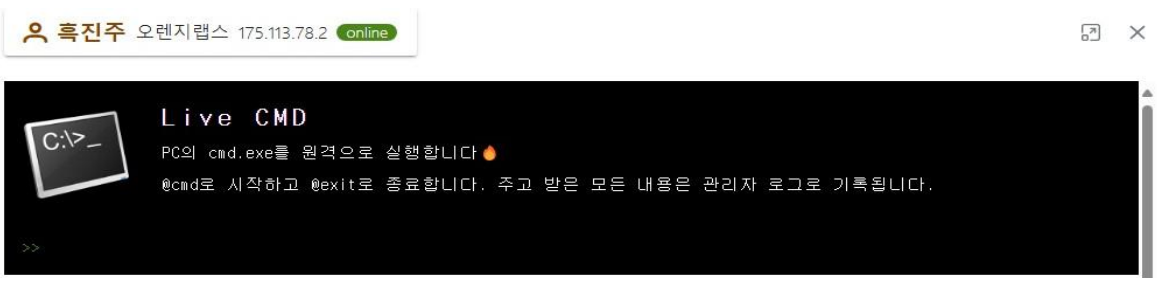
사용자 세부 정보 화면의 우측 상단의 Live CMD 버튼을 클릭하면 시작할 수 있습니다.

[그림 77] 사용자 세부 정보 화면에서 Live CMD 버튼 클릭

Live Agent 화면에서도, 같은 방법으로 Live CMD를 시작할 수 있습니다.



[그림 78] Live Agent 화면에서 Live CMD 버튼 클릭



[그림 79] Live CMD 실행 창

Live CMD에서 사용된 모든 명령과 응답은 관리자 로그에 저장되고, 관리자 로그는 삭제할 수 없습니다.

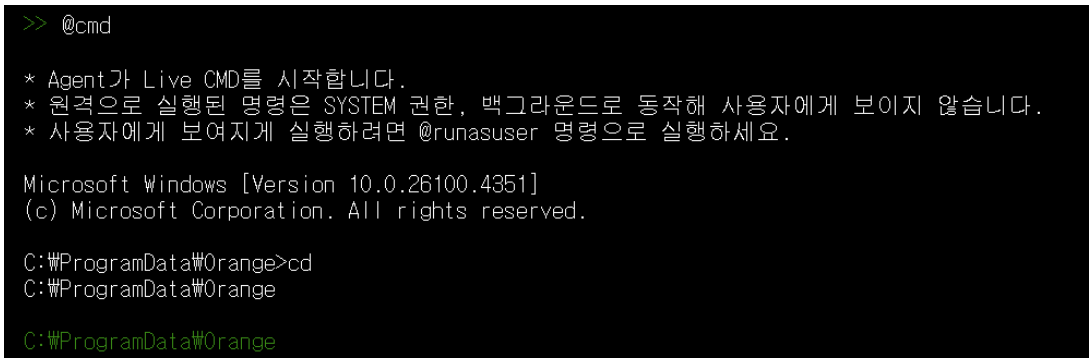
6.12.2 명령어

6.12.2.1 Live CMD 시작 및 종료 명령

시작과 종료 시 항상 다음 명령어를 수행합니다.

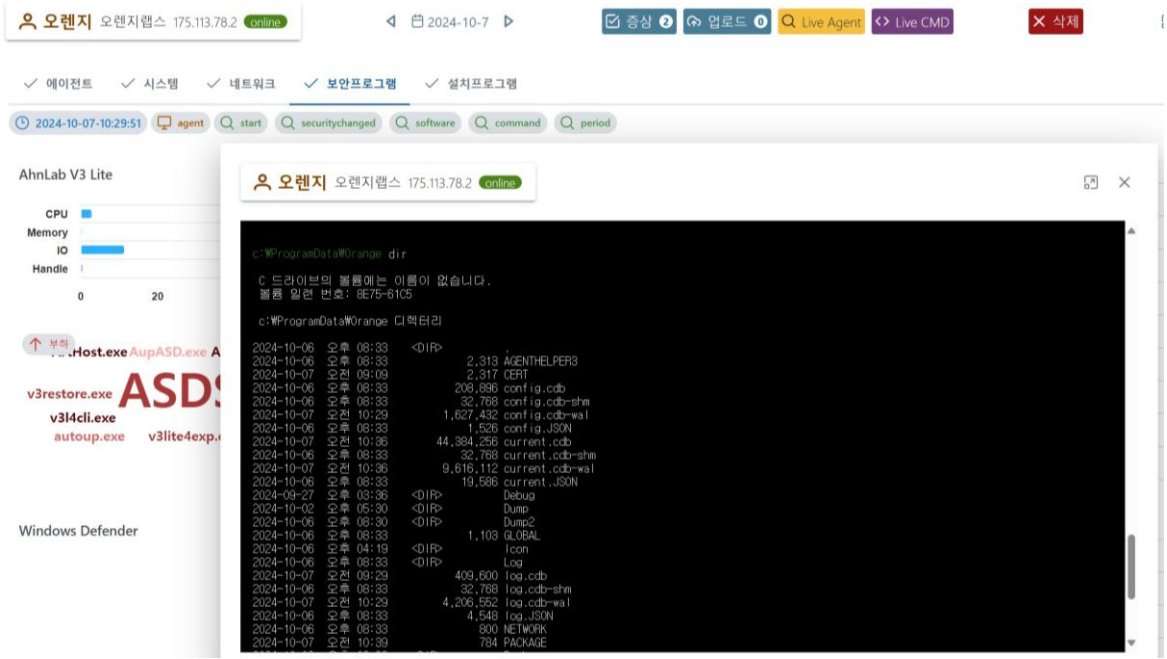
@cmd	사용자 에이전트에게 Live CMD 시작을 알림. 사용자 에이전트는 해당 관리자가 적법한 절차로 접근했는지 확인하고, 시스템에 Live CMD 사용 기능이 활성화된 경우 원격 cmd가 시작됩니다.
@exit	Live CMD를 종료합니다.

[표 7] Live CMD 시작과 종료 명령

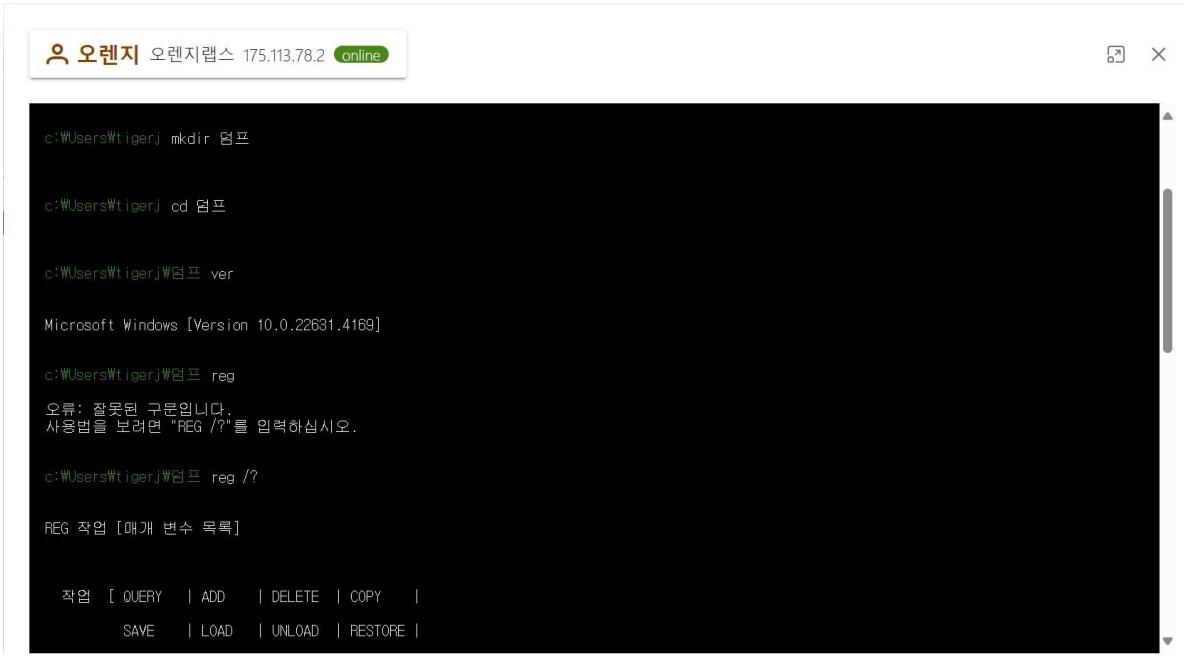


[그림 80] Live CMD @cmd 명령 실행

녹색으로 사용자 PC의 경로가 표시되면 매니저와 에이전트가 1:1로 연결되었음을 의미합니다. 이후 윈도우 CMD 명령을 원격으로 수행하고 결과를 확인할 수 있습니다.



[그림 81] Live CMD에서 dir 명령 실행 예시



[그림 82] Live CMD에서 각종 명령 실행 예시

윈도우 CMD 명령 외에 에이전트가 수행하는 Live CMD 전용 명령들이 추가적으로 제공됩니다.

6.12.2.2 PC 관련 명령

@reboot	PC 재시작
@shutdown	PC 종료
@runasuser	사용자 권한으로 프로그램 실행@runasuser [프로세스경로] 프로세스가 원도우 Path에 존재하는 경우 프로세스명 만으로도 실행됩니다. <예시>@runasuser notepad.exe 에이전트는 시스템 권한으로 백그라운드에서 동작하므로, 원격으로 실행된 명령의 결과는 사용자에게 보이지 않습니다. @runasuser는 명령의 결과가 사용자에게 보이도록 하기 위해, 로그온한 사용자의 권한으로 프로그램을 실행시키도록 합니다.
@kill	프로그램 강제 종료@kill [프로세스명] 프로세스 경로는 지원하지 않으며 프로세스명으로 강제 종료합니다. 해당 프로세스명을 가진 프로세스가 여러 개인 경우 모두 종료됩니다. 특정 프로세스의 부하가 많은 경우 긴급 조치할 때 사용할 수 있습니다. <예시>@kill notepad.exe

[표 8] Live CMD PC 관련 명령

6.12.2.3 에이전트 및 파일 수집 관련 명령

@restart	Orange The Client 에이전트 재시작
@uninstall	Orange The Client 삭제

@upload	파일 수집@upload [파일명] 현재 경로에 있는 [파일명]을 수집합니다. 특정 폴더에 있는 파일을 수집하기 위해선 해당 폴더로 cmd 명령으로 이동하면 됩니다. 기본으로 설정된 수집할 수 있는 파일은 실행 파일(.exe, .sys, .dll)과 메모리덤프 파일(.dmp)이며 파일의 확장자가 아닌 파일의 내부 데이터를 파일 포맷을 판단합니다. 수집된 파일은 업로드 파일 뷰에서 확인할 수 있으며, 업로드된 파일은 모두 관리자 로그에 기록됩니다. <예시> @upload a.exe @upload *.dmp
clear	Live CMD 화면 소거

[표 9] Live CMD 에이전트 및 파일 수집 관련 명령

6.12.2.4 파일 수집 관련 명령

[그림 83] Live CMD에서 @upload 명령 실행 예시

@upload 명령으로 현 디렉터리의 파일을 수집할 수 있습니다. 파일 수집은 백그라운드로 순차적으로 전송되며 전송 중에도 Live CMD를 계속 진행할 수 있습니다.

수집 대상 파일은 Windows Memory Dump 파일과 PE 파일로 제한됩니다. 대상 파일 여부는 파일의 내부 포맷을 읽고 판단하므로, 확장자를 바꿔도 대상이 아닌 파일은 수집되지 않아 개인정보의 외부 유출을 방지합니다.

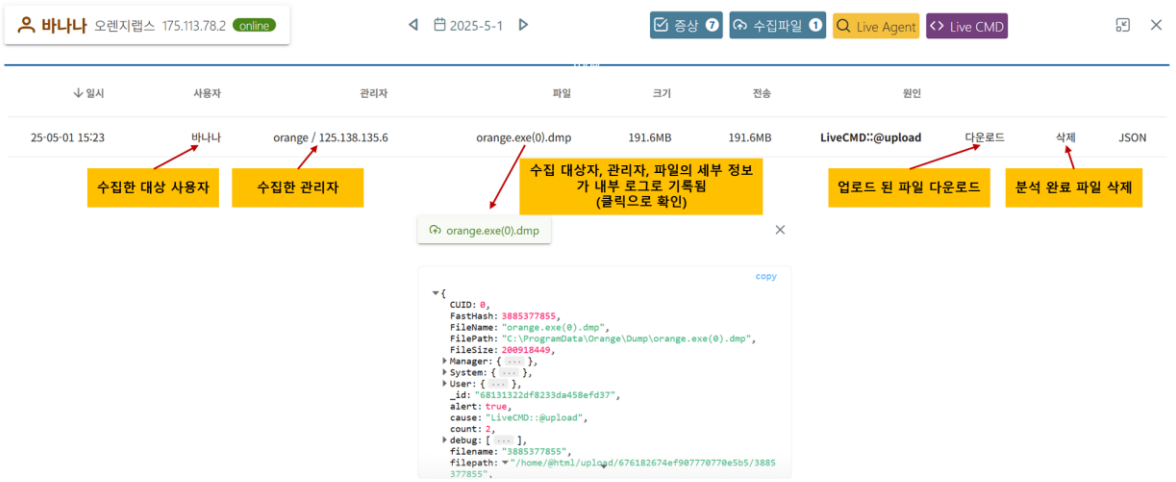
디스크 자원의 절감을 위해, 서버에 기존에 수집된 동일 파일(해시로 구분)에 대해 @upload 명령이 실행되는 경우, 기존 수집된 동일 파일로 수집 파일 리스트에 표시하며 파일 업로드가 실제 수행되지는 않습니다.

6.12.2.5 수집 파일 리스트

사용자 세부 정보 화면 상단의 "수집파일" 버튼을 클릭하면 수집 파일 리스트를 확인할 수 있습니다.

[그림 84] 수집파일 버튼

각각의 수집된 파일은 수집 파일 리스트에서 확인할 수 있습니다.



[그림 85] 수집 파일 리스트

수집된 파일의 대상 사용자, 관리자, 파일에 대한 자세한 정보가 내부 로그로 기록됩니다.

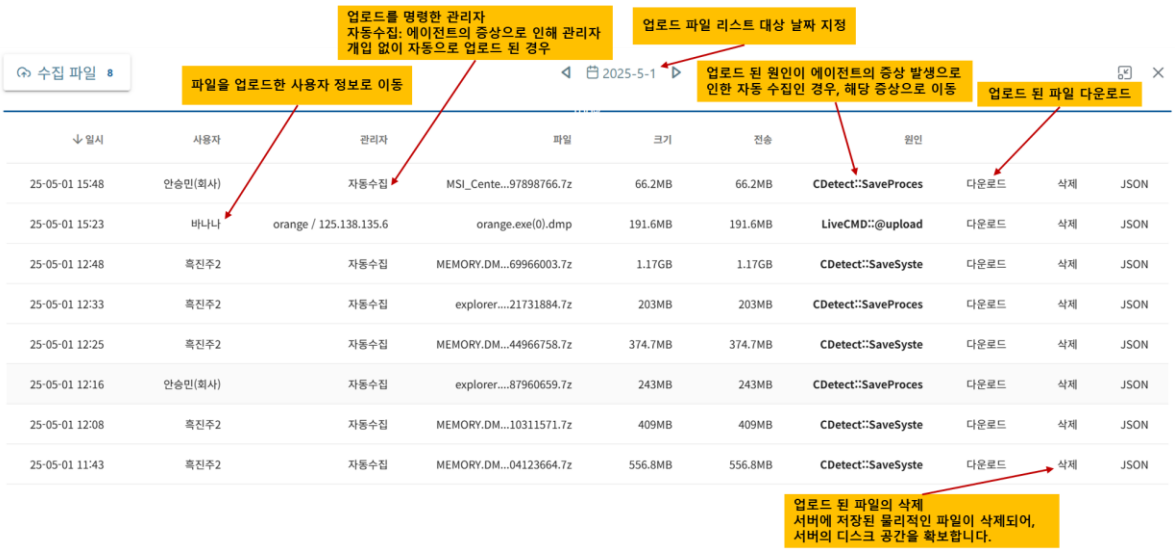
6.13 수집 파일 관리

수집 파일 관리 기능을 통해, 에이전트가 서버로 업로드한 파일들을 조회하고, 각 파일을 다운로드 및 삭제할 수 있습니다.

매니저의 메인 화면에서 상단의 "수집 파일 관리" 버튼을 클릭하면 진입할 수 있습니다.

[그림 86] 수집 파일 관리 버튼

수집 파일 관리 화면은 아래 그림과 같습니다. 개별 컬럼을 클릭하여 정보 조회 또는 파일 다운로드 및 삭제 기능을 수행할 수 있습니다.



[그림 87] 수집 파일 관리

6.13.1 자동 수집

프로세스 크래시 및 BSOD 발생시에는 관련 파일이 에이전트에 의해 자동 수집되며 수집 내용은 아래와 같이 구성됩니다.

- 문제가 발생된 실행 파일과 메모리 덤프 파일
- 문제를 일으킨 파일
- WinDbg 분석서(텍스트)
- Orange The Client 자체 분석 파일(JSON)

6.13.2 관리자 수집

관리자에 의해 수집된 파일은 수집한 관리자, IP가 표시됩니다.

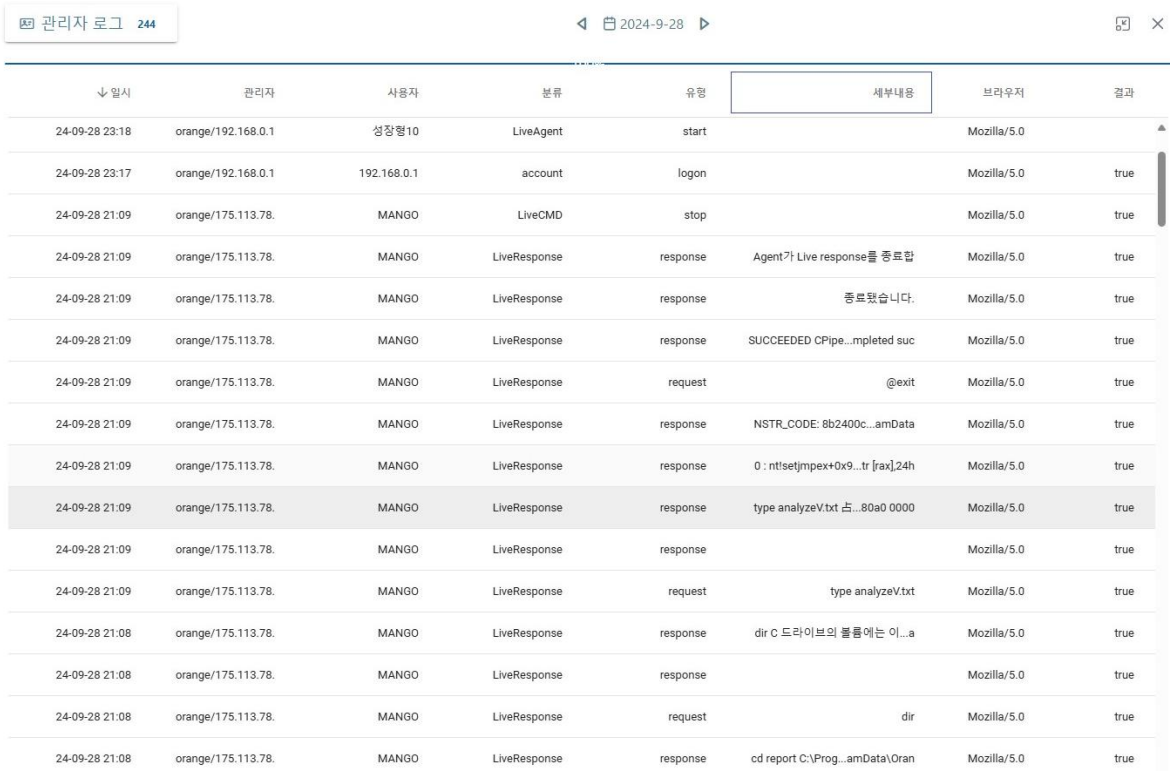
6.13.3 수집 파일 삭제

에이전트로부터 자동 수집된 증상 관련 파일은 크기가 클 수 있으므로 확인이 완료된 파일은 삭제해줘야 합니다.

6.14 관리자 로그

관리자가 매니저에서 수행한 주요 행동에 대한 로그를 남깁니다.
매니저의 메인 화면에서 상단의 "관리자 로그" 버튼을 클릭하면 진입할 수 있습니다.

[그림 88] 관리자 로그 버튼

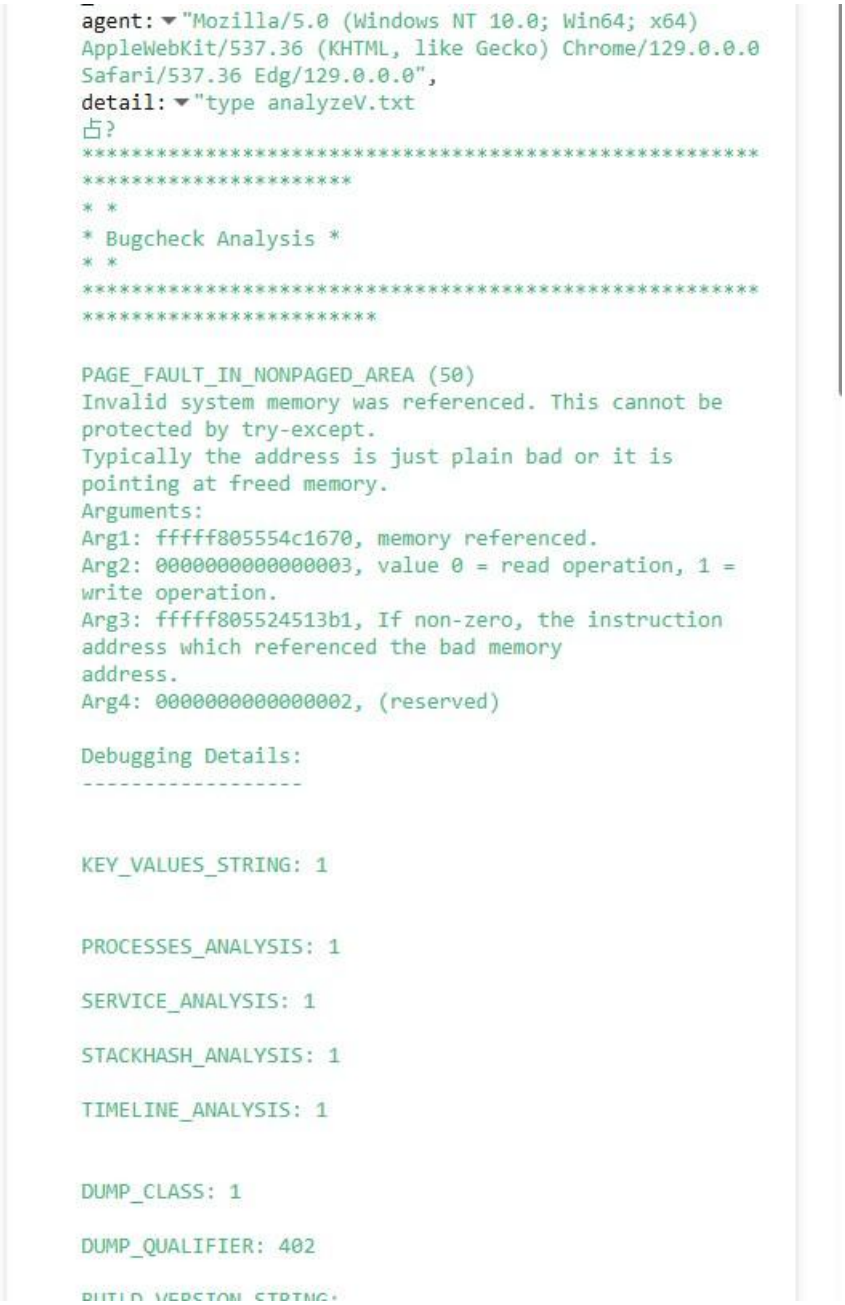


일시	관리자	사용자	분류	유형	세부내용	브라우저	결과
24-09-28 23:18	orange/192.168.0.1	성장형10	LiveAgent	start		Mozilla/5.0	
24-09-28 23:17	orange/192.168.0.1	192.168.0.1	account	logon		Mozilla/5.0	true
24-09-28 21:09	orange/175.113.78.	MANGO	LiveCMD	stop		Mozilla/5.0	true
24-09-28 21:09	orange/175.113.78.	MANGO	LiveResponse	response	Agent가 Live response를 종료합	Mozilla/5.0	true
24-09-28 21:09	orange/175.113.78.	MANGO	LiveResponse	response	종료됐습니다.	Mozilla/5.0	true
24-09-28 21:09	orange/175.113.78.	MANGO	LiveResponse	response	SUCCEEDED CPipe...mpleted suc	Mozilla/5.0	true
24-09-28 21:09	orange/175.113.78.	MANGO	LiveResponse	request	@exit	Mozilla/5.0	true
24-09-28 21:09	orange/175.113.78.	MANGO	LiveResponse	response	NSTR_CODE: 8b2400c...amData	Mozilla/5.0	true
24-09-28 21:09	orange/175.113.78.	MANGO	LiveResponse	response	0 : nt!setjmpex+0x9...tr [rax],24h	Mozilla/5.0	true
24-09-28 21:09	orange/175.113.78.	MANGO	LiveResponse	response	type analyzeV.txt 占...80a0 0000	Mozilla/5.0	true
24-09-28 21:09	orange/175.113.78.	MANGO	LiveResponse	response		Mozilla/5.0	true
24-09-28 21:09	orange/175.113.78.	MANGO	LiveResponse	request	type analyzeV.txt	Mozilla/5.0	true
24-09-28 21:08	orange/175.113.78.	MANGO	LiveResponse	response	dir C 드라이브의 볼륨에는 이...a	Mozilla/5.0	true
24-09-28 21:08	orange/175.113.78.	MANGO	LiveResponse	response		Mozilla/5.0	true
24-09-28 21:08	orange/175.113.78.	MANGO	LiveResponse	request	dir	Mozilla/5.0	true
24-09-28 21:08	orange/175.113.78.	MANGO	LiveResponse	response	cd report C:\Prog...amData\Oran	Mozilla/5.0	true

[그림 89] 관리자 로그

남겨진 로그는 삭제할 수 없으니 모든 행동에 대해 관리자는 주의해야 합니다.
특히 사용자 개인 정보 관련 민감한 부분이 될 수 있는 Live CMD 사용시 주고받은 모든 내용이 관리자 로그로 기록됩니다.

관리자 로그 세부 내용은 JSON 형태로 제공됩니다.



[그림 90] 관리자 로그 세부 내용(JSON)

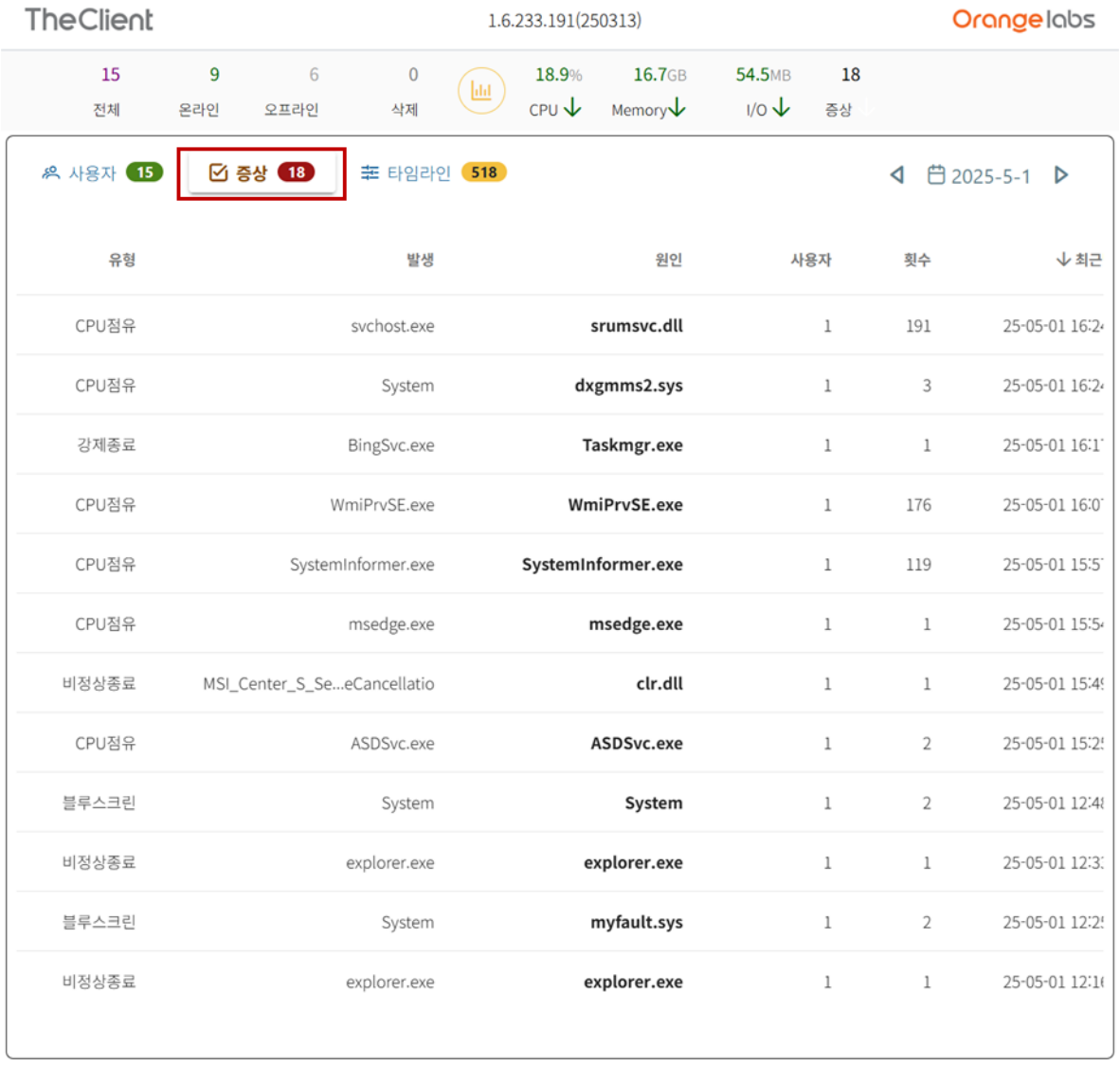
7 탐지 증상

Orange The Client의 에이전트는 PC의 성능 저하 및 장애와 관련된 여러 가지 증상을 탐지할 수 있습니다. 본 장에서는 탐지 가능한 증상들이 어떻게 탐지, 분석 및 표시되는지 설명합니다.

7.1 탐지된 증상 조회 방법

에이전트에서 탐지된 증상 정보는 에이전트와 매니저 모두에서 조회 가능합니다(에이전트가 매니저에 해당 정보를 전달합니다).

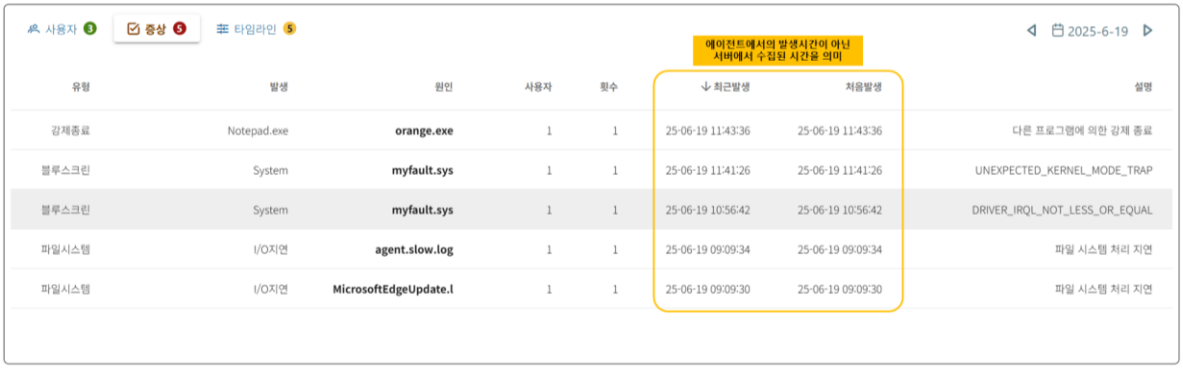
매니저에서 증상 목록을 조회하려면, 메인 화면에서 증상 탭을 클릭하면 됩니다.



[그림 91] 매니저에서 증상 목록 표시

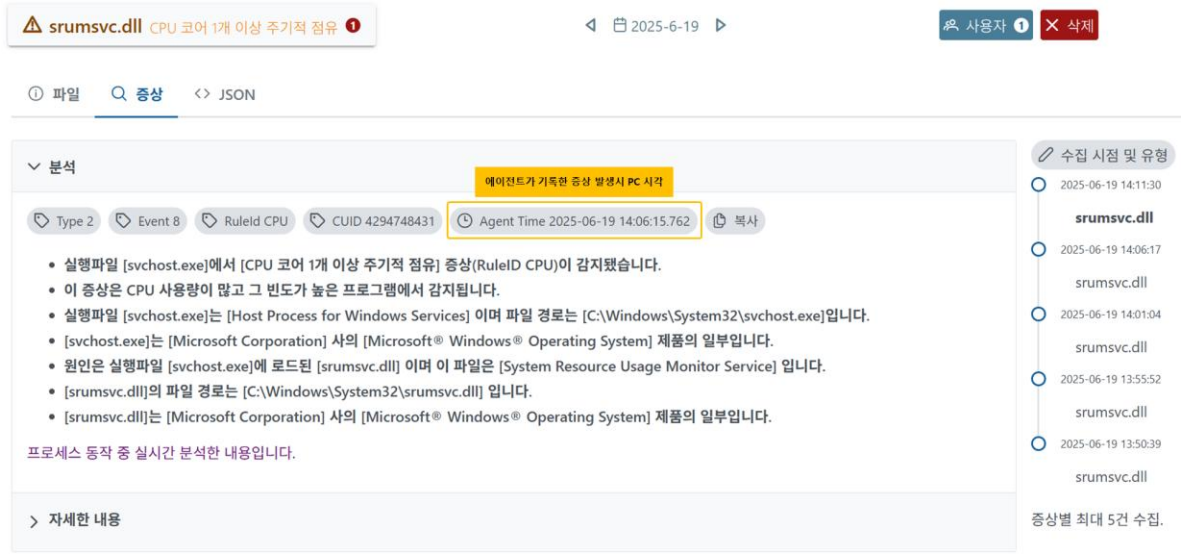
증상 탭의 "최근발생" 컬럼과 "처음발생" 컬럼은 에이전트들에서 발생한 증상을 서버에서 마지

막으로 수집한 시각과 처음 수집한 시각을 의미합니다. 에이전트에서 증상이 발생한 PC 시각을 의미하지 않습니다(에이전트가 설치된 PC 시각이 부정확할 수 있기 때문입니다).



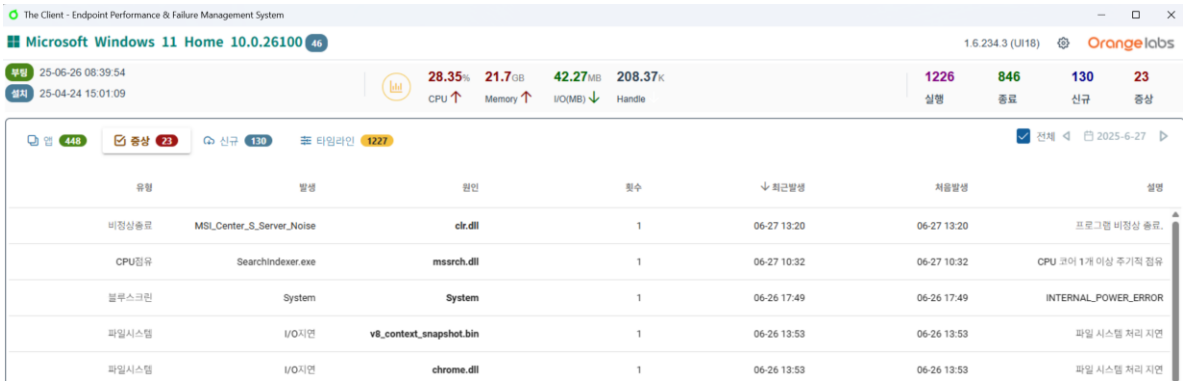
[그림 92] 최근발생 컬럼과 처음발생 컬럼

에이전트가 기록한 증상 발생시 PC 시각을 알고 싶다면 개별 증상을 클릭하고, 증상 탭에서 해당 내용을 확인할 수 있습니다.



[그림 93] 에이전트가 기록한 증상 발생시 PC 시각 확인

에이전트에서 증상 목록을 조회하려면, 매니저의 경우와 마찬가지로 메인 화면에서 증상 탭을 클릭하면 됩니다.



[그림 94] 에이전트에서 증상 목록 표시

7.2 증상 종류

7.2.1 CPU 점유

특정 프로세스가 CPU 자원을 과도하게 점유하는 현상을 탐지합니다. 과점의 기준은 프로세스가 반복적인 모니터링 동안 연속 5회 이상, 하나 이상의 CPU 코어를 100% 사용한 경우로 정의됩니다. 이때의 모니터링 주기는 PC의 성능 상태 및 자원 사용 상황에 따라 동적으로 조정됩니다. 에이전트(Agent)는 전체 시스템에 부담을 주지 않기 위해, 모든 프로세스의 성능 정보를 주기적으로 수집하지는 않습니다. 대신, 커널에서 특정 프로세스의 I/O 활동이 감지되었을 때, 해당 프로세스의 커널 객체가 보유한 성능 정보를 활용하여 CPU 사용률 등을 파악합니다. 이러한 설계는 프로세스의 동작 특성에 따라 성능 정보 수집 주기가 달라지는 특징을 가지며, 이는 의도적으로 계획된 동작 방식으로 Agent의 부하를 최소화합니다.

그러나 I/O 활동 없이 CPU만을 집중적으로 사용하는 프로세스의 경우, 커널 수준에서 탐지가 이뤄지지 않기 때문에 일정 시간 이상(예: 1분) 성능 정보가 수집되지 않은 프로세스에 대해서는 유저 영역(User-mode)에서 추가적인 성능 수집 로직이 실행됩니다. 이로써 CPU 과점 현상을 누락 없이 탐지할 수 있습니다.

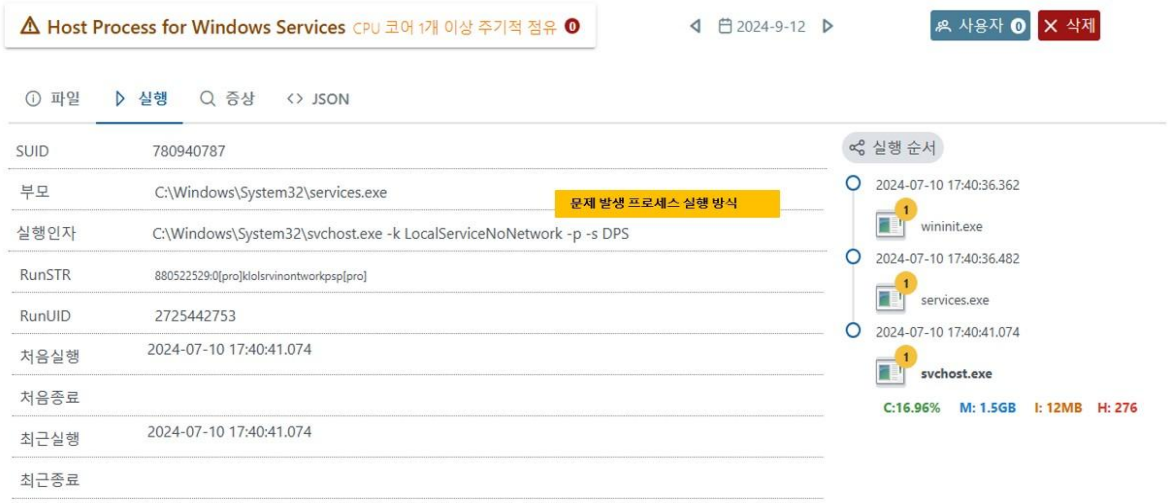
[그림 95] CPU 점유

문제의 발생과 원인이 같은 파일일 수도 있지만 다를 수도 있습니다.

에이전트는 별도의 도구(WinDbg 같은 개발자용 디버그툴) 없이도, 실시간 프로세스 분석을 통해 자체적으로 이런 문제 사항들을 즉시 탐지하고 분석할 수 있습니다.

7.2.1.1 발생 – 프로세스의 실행 정보

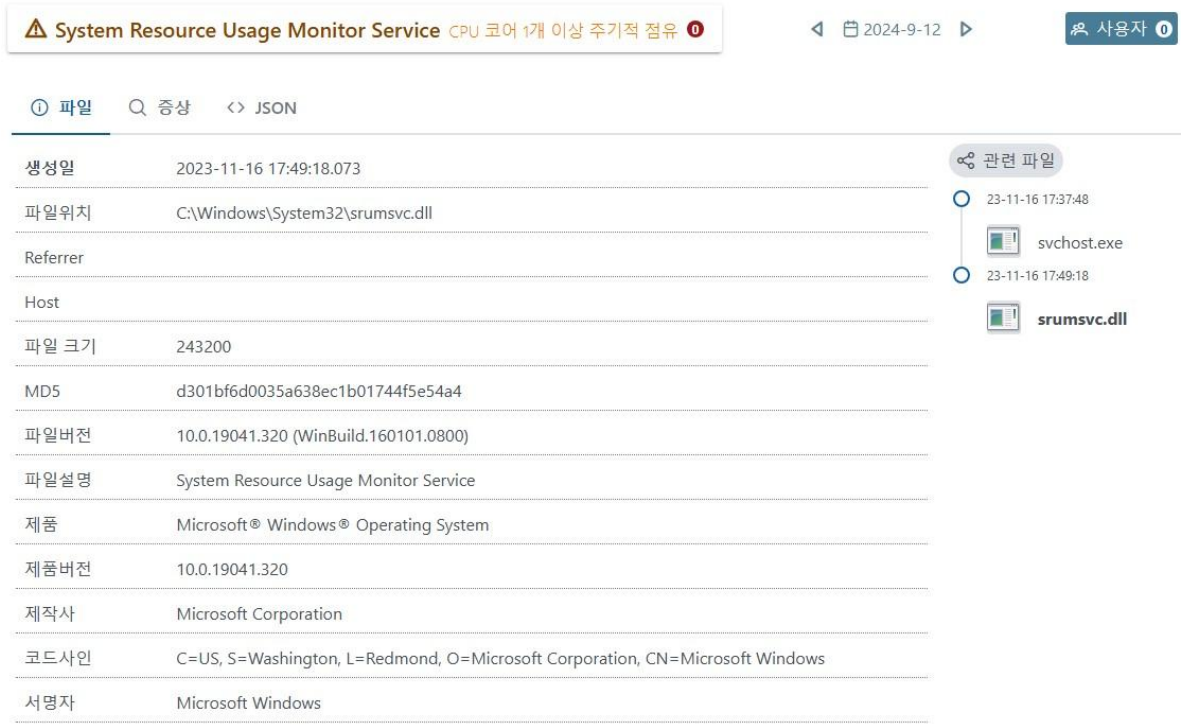
"발생" 컬럼을 클릭하면 증상이 발생한 프로세스의 실행 정보를 확인할 수 있습니다.



[그림 96] 프로세스 실행 정보

7.2.1.2 원인 – 모듈 정보

"원인" 컬럼을 클릭하면 증상의 원인이 되는 모듈 정보를 확인할 수 있습니다.



[그림 97] 문제 원인이 되는 모듈 정보

7.2.1.3 분석

모듈 정보 화면의 "증상" 탭 아래에서는 증상을 분석한 내용을 확인할 수 있습니다.

[그림 98] 분석 내용

7.2.1.4 수집 파일

없음.

7.2.2 블루스크린(BSOD) 분석

[그림 99] 블루스크린(BSOD) 발생 화면

블루스크린 발생 후 윈도우가 다시 부팅되면 에이전트는 자동으로 블루스크린 발생시 윈도우가 생성한 덤프파일 분석합니다.
윈도우 버전에 따라 블루스크린 발생 후 생성되는 덤프 파일의 유형이 기본값으로 "미니덤프" 일 수 있으나, 덤프 파일 유형 중 데이터 양이 가장 적은 미니덤프로는 정확한 원인 분석이 되지 않을 수 있습니다. 에이전트는 현재 시스템의 디버깅 정보 쓰기 옵션이 "미니덤프" 또는 "덤프 파일 생성 안함"으로 설정된 경우, 자동으로 "커널 메모리 덤프" 또는 "전체 메모리 덤프"가 생성되도록 설정을 변경하는데, 이 경우 윈도우 재부팅 후에 해당 변경이 반영됩니다.

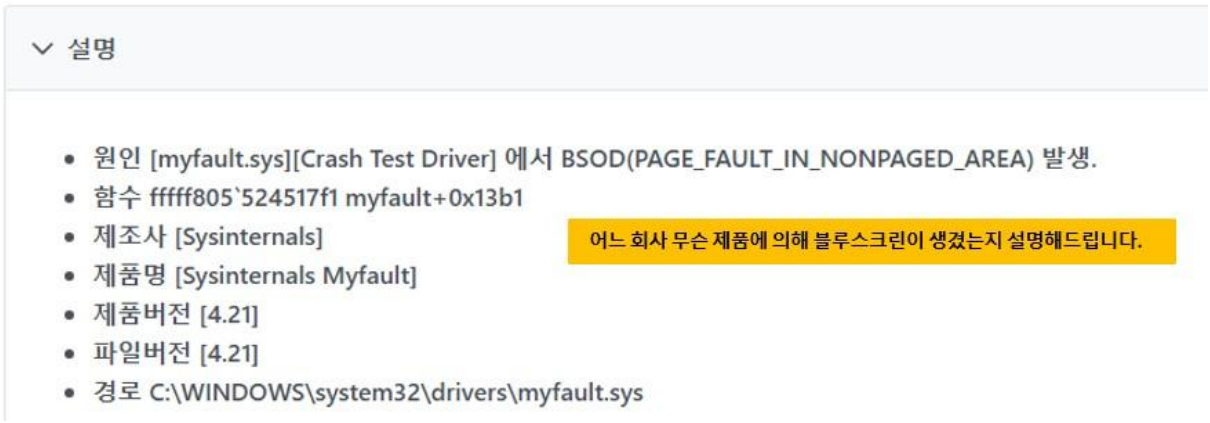
7.2.2.1 원인 – 커널 드라이버 모듈

증상 목록에 블루스크린을 발생시킨 원인 파일이 표시됩니다.

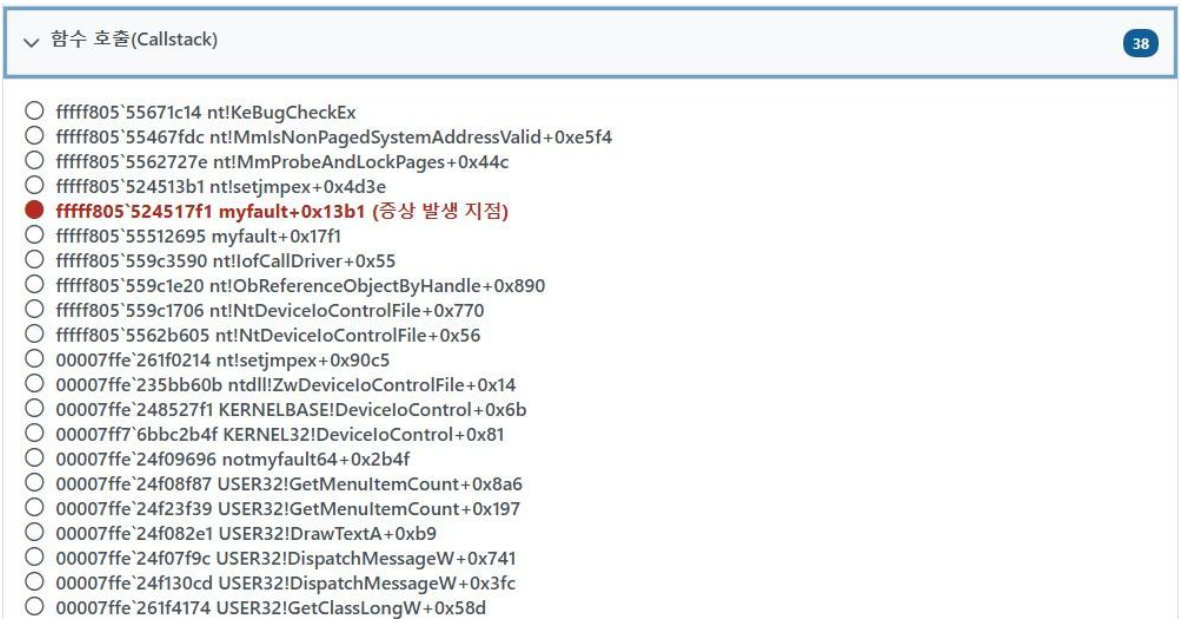
[그림 100] 문제 원인이 되는 커널 드라이버 모듈 정보

7.2.2.2 분석

원인 파일을 클릭하면 블루스크린에 대한 분석 내용이 표시됩니다.



[그림 101] 분석 내용



[그림 102] 함수 호출(Callstack) 내용

7.2.2.3 수집 파일

- 시스템 커널 파일
- 원인 모듈 파일
- 시스템 메모리 덤프 파일
- WinDbg 분석 파일(텍스트)
- 자체적인 분석 내용이 담긴 파일(JSON)

7.2.3 프로세스 강제 종료

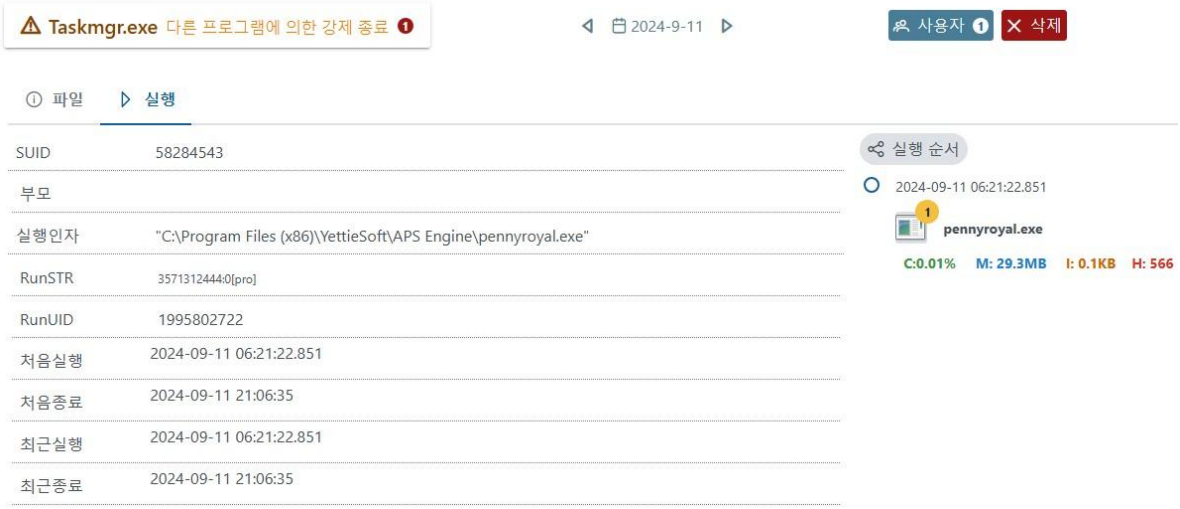
프로세스(원인 프로세스)가 다른 프로세스(발생 프로세스)를 강제로 종료시킨 경우입니다.

유형	발생	원인	사용자	횟수	↓최근발생	처음발생	설명
CPU점유	svchost.exe	srumsvc.dll	1	211	24-09-29 19:08:19	24-09-29 00:02:59	CPU 코어 1개 이상 주기적 점유
CPU점유	svchost.exe	wdi.dll	1	12	24-09-11 23:57:32	24-09-11 21:18:46	CPU 코어 1개 이상 주기적 점유
비정상종료	tv_w32.exe	f_sps.dll	1	1	24-09-11 23:43:59	24-09-11 23:43:59	프로그램 비정상 종료.
CPU점유	OneDrive.exe	SyncEngine.dll	1	1	24-09-11 22:23:46	24-09-11 22:23:46	CPU 코어 1개 이상 주기적 점유
강제종료	Creative.App.exe	Taskmgr.exe	1	1	24-09-11 21:12:35	24-09-11 21:12:35	다른 프로그램에 의한 강제 종료
강제종료	pennyroyal.exe	Taskmgr.exe	1	1	24-09-11 21:06:47	24-09-11 21:06:47	다른 프로그램에 의한 강제 종료

[그림 103] 프로세스 강제 종료

7.2.3.1 발생 프로세스

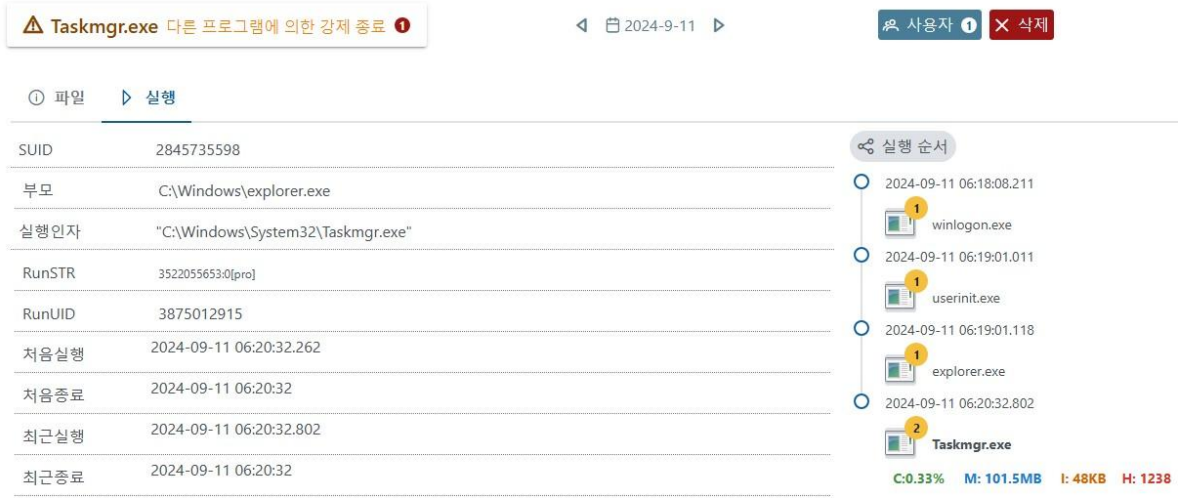
"발생" 컬럼에 있는 프로그램 명을 선택하면 아래 화면에서 강제 종료된 프로세스의 실행 정보와 실행 순서와 같은 자세한 내용을 확인할 수 있습니다.



[그림 104] 발생 프로세스 정보

7.2.3.2 원인 프로세스

"원인" 컬럼에 있는 프로그램 명을 선택하면 아래 화면에서 강제 종료의 원인인 프로세스의 실행 정보와 실행 순서와 같은 자세한 내용을 확인할 수 있습니다.



[그림 105] 원인 프로세스 정보

7.2.3.3 분석

다른 증상과는 달리, 위 발생 프로세스와 원인 프로세스의 명확한 제공으로 분석을 대신합니다.

7.2.3.4 수집 파일

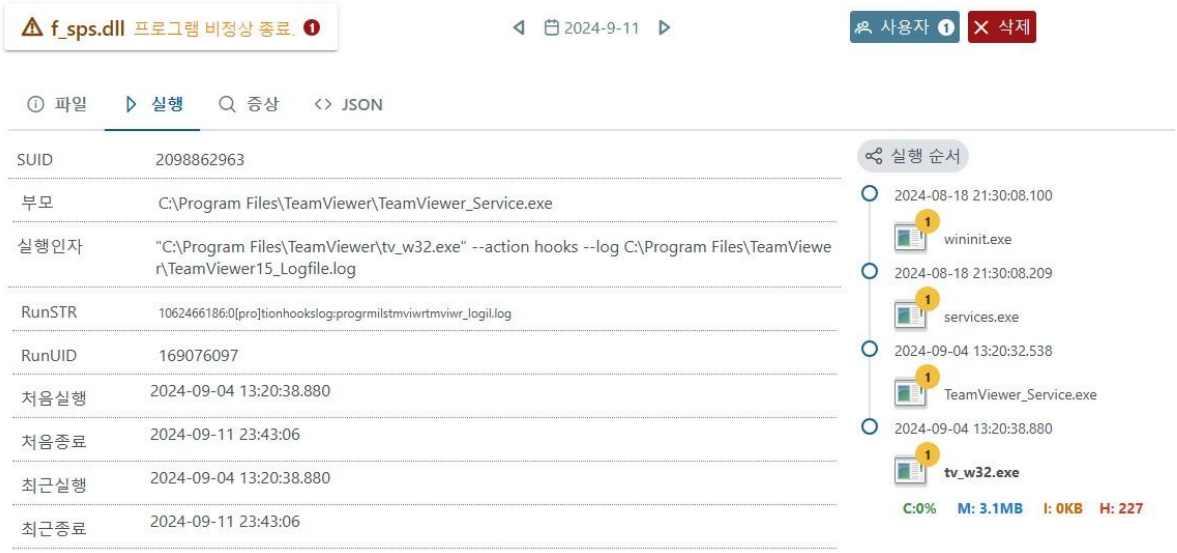
없음.

7.2.4 프로세스 비정상 종료

특정 프로세스가 비정상 종료된 경우, 실시간 탐지 및 원인 분석 후 관련 정보들을 수집해 파일로 제공합니다.

7.2.4.1 발생 프로세스

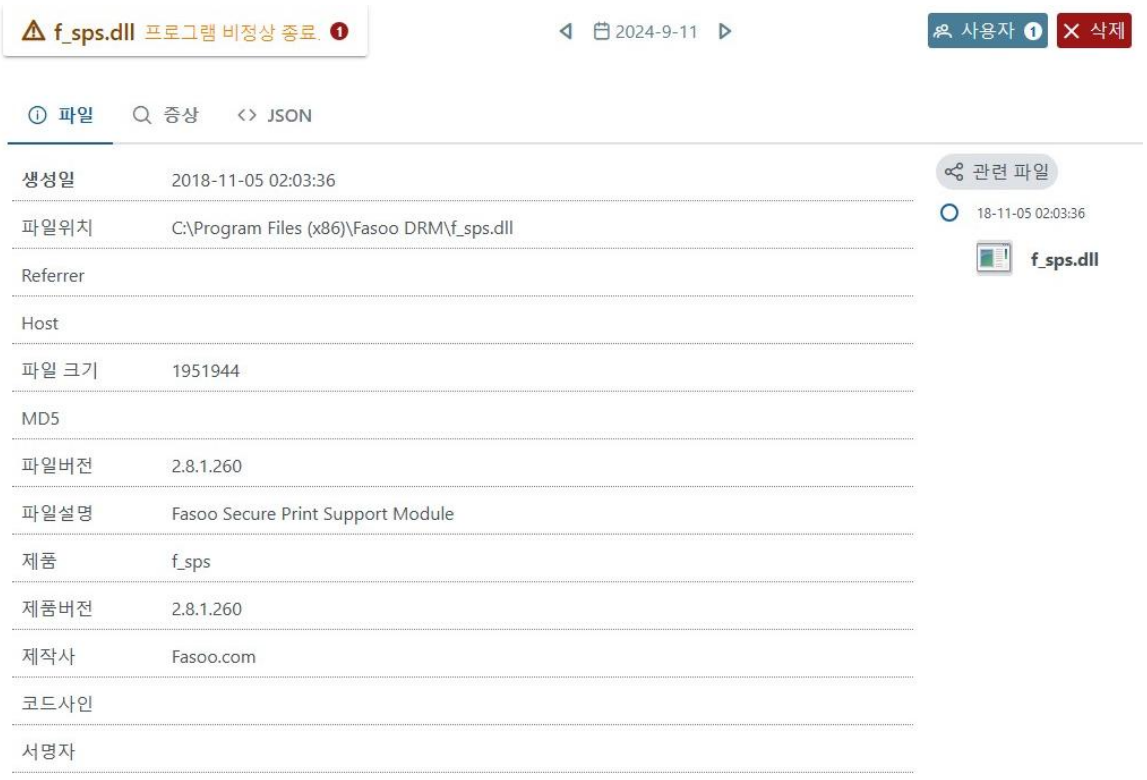
"발생" 컬럼에 있는 프로그램 명을 선택하면 아래 화면에서 비정상 종료된 프로세스의 실행 정보와 실행 순서와 같은 자세한 내용을 확인할 수 있습니다.



[그림 106] 발생 프로세스 정보

7.2.4.2 원인 파일

"원인" 컬럼에 있는 프로그램 명을 선택하면 아래 화면에서 비정상 종료의 원인인 프로그램의 정보 등의 자세한 내용을 확인할 수 있습니다.



[그림 107] 원인 파일 정보

7.2.4.3 분석

원인 파일 화면의 "증상" 탭에서 비정상 종료에 대한 분석 내용이 표시됩니다.

[그림 108] 분석 내용

7.2.4.4 수집 파일

- 발생된 프로세스 파일
- 원인 파일
- 발생된 프로세스 메모리 덤프 파일
- 분석된 내용이 기록된 파일

8 부록