# Oracle ILOM 보안 설명서

펌웨어 릴리스 3.0, 3.1 및 3.2

부품 번호: E40360-03
2014년 8월

# 목차

# 이 설명서 사용

- **개요** — *Oracle ILOM* 보안 설명서는 Oracle ILOM 보안 작업 지침에 대한 웹 및 CLI 정보를 제공합니다. 이 설명서를 Oracle ILOM 설명서 라이브러리에 있는 다른 설명서와 함께 사용하십시오.
- **대상** — 이 설명서는 기술 지원 담당자, 시스템 관리자, 인증된 Oracle 서비스 공급자 및 시스템 하드웨어 관리 경험이 있는 사용자를 대상으로 합니다.
- **필요한 지식** — Oracle 서버를 구성하고 관리해 본 경험

## 제품 설명서 라이브러리

본 설명서 및 기타 관련 설명서는 Oracle ILOM 설명서 라이브러리(http://www.oracle.com/goto/ILOM/docs)에서 제공합니다.

## Oracle 지원 액세스

Oracle 고객은 My Oracle Support를 통해 온라인 지원에 액세스할 수 있습니다. 자세한 내용은 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info를 참조하거나, 청각 장애가 있는 경우 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs를 방문하십시오.

## 설명서 접근성

Oracle의 접근성 개선 노력에 대한 자세한 내용은 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc에서 Oracle Accessibility Program 웹 사이트를 방문하십시오.

## 피드백

다음 위치에서 이 설명서에 대한 피드백을 보낼 수 있습니다.

http://www.oracle.com/goto/docfeedback

# Oracle ILOM 펌웨어 릴리스별 보안 기능

다음 표를 참조하여 Oracle ILOM 보안 기능이 제공되는 펌웨어 릴리스를 확인하십시오.

| 사용 가능한 펌웨어 버전 | 보안 기능 | 세부 정보 참조: |
|---|---|---|
| 모두 | 인증 및 권한 부여 | ■ "Oracle ILOM 사용자 액세스 보안" [22] |
| 모두 | 전용 보안 관리 연결 | ■ "물리적 관리 연결 보안" [13]<br>■ "보안 관리 연결 유지 관리" [49] |
| 모두 | 암호화되어 미리 구성된 네트워크 포트 | ■ "미리 구성된 서비스 및 네트워크 포트" [17] |
| 모두 | IPMI 2.0 보안 관리 | ■ "보안을 최대화하도록 IPMI 관리 액세스 구성" [44] |
| 모두 | 보안 셸 암호화 구성 | ■ 서버측 키를 사용하여 SSH 연결 암호화 [40]<br>■ 자동 CLI 인증을 위해 사용자 계정에 SSH 키 추가 [41] |
| 모두 | SNMP 3.0 보안 관리 | ■ "보안을 최대화하도록 SNMP 관리 액세스 구성" [42] |
| 모두 | SSL 프로토콜 및 인증서 | ■ Oracle ILOM에 사용자 정의 SSL 인증서 및 개인 키 업로드 [35]<br>■ OpenSSL을 사용하여 SSL 인증서 및 개인 키 얻기 [34]<br>■ 가장 강력한 SSL 및 TLS 암호화 등록 정보 사용 [36] |
| 모두 | 원격 콘솔 암호화 및 보안 프로토콜 | ■ "원격 KVMS 보안 사용" [52] |
| 3.0.4 이상 | KVMS 호스트 잠금 구성 | ■ KVMS 세션 종료 시 호스트 액세스 잠금 [29] |
| 3.0.4 이상 | 세션 시간 초과 구성 | ■ 활성 웹 세션에 대한 시간 초과 간격 설정 [37]<br>■ 비활성 CLI 세션에 대한 시간 초과 간격 설정 [39] |
| 3.0.12 이상 | 로컬 호스트 상호 연결 인증 세션 | ■ "선호하는 인증된 호스트 상호 연결 액세스" [50] |
| 3.0.8 이상 | 로그인 배너 구성 | 로그인 배너로 시스템 액세스 보안 설정(3.0.8 이상) [31] |
| 3.0.8 - 3.1.2 | WS-Management 보안 액세스 | ■ "보안을 최대화하도록 WS-Management 액세스 구성" [46] |
| 3.1.0 이상 | 별도의 감사 로그 | ■ "감사 이벤트를 모니터링하여 허용되지 않은 액세스 찾기" [57] |
| 3.1.0 이상 | 물리적 보안 존재 확인 | ■ "`root` 계정 기본 암호를 재설정하기 위한 물리적 보안 존재" [56] |

| 사용 가능한 펌웨어 버전 | 보안 기능 | 세부 정보 참조: |
|---|---|---|
| 3.2.4 이상 | IPMI 1.5 구성 가능 등록 정보 | ■ “보안을 최대화하도록 IPMI 관리 액세스 구성” [44] |
| 3.2.4 이상 | TLS 프로토콜 버전 1.1 및 1.2 | ■ 가장 강력한 SSL 및 TLS 암호화 등록 정보 사용 [36] |
| 3.2.4 이상 | KVMS 세션 수 | ■ Remote System Console Plus의 표시 가능 KVMS 세션 제한(3.2.4 이상) [30] |
| 3.2.4 이상 | FIPS 준수 암호화 지원 | ■ “배치 시 FIPS 모드 구성 여부 선택” [14]<br>■ “FIPS 모드가 사용으로 설정된 경우 지원되지 않는 기능” [16]<br>■ “사용자 액세스 보안을 위한 배치 후 고려 사항” [54] |

# 추가 보안 정보

Oracle ILOM 보안 설정에 대한 자세한 내용은 이 설명서의 다음 절을 참조하십시오.

- Oracle ILOM 보안 관련 최적의 방법 점검 목록
- Oracle ILOM 보안을 위한 배치 관련 최적의 방법
- Oracle ILOM 보안을 위한 배치 후 최적의 방법

# Oracle ILOM 보안 관련 최적의 방법 점검 목록

Oracle Integrated Lights Out Manager(ILOM)는 모든 Oracle 서버 및 대부분의 레거시 Sun 서버에 사전 설치된 SP(서비스 프로세서)입니다. 시스템 관리자는 Oracle ILOM의 사용자 인터페이스를 사용하여 원격 서버 관리 작업과 실시간 서버 상태 모니터링 작업을 수행합니다.

Oracle ILOM 보안 관련 최적의 방법이 사용 환경에 알맞게 구현되었는지 확인하려면 시스템 관리자가 다음 점검 목록에서 권장된 보안 작업을 참조해야 합니다.

- "서버 배치를 위한 보안 점검 목록" [9]
- "서버 배치 후 보안 점검 목록" [10]

### 관련 정보

- Oracle ILOM 보안을 위한 배치 관련 최적의 방법 .
- Oracle ILOM 보안을 위한 배치 후 최적의 방법
- Oracle ILOM 펌웨어 릴리스별 보안 기능 [7]

## 서버 배치를 위한 보안 점검 목록

새 서버의 배치를 계획할 때 어떤 Oracle ILOM 보안 방식이 가장 적합한지 확인하려면 시스템 관리자가 다음 표 1. "점검 목록 - 서버 배치 시 Oracle ILOM 보안 구성 "에서 권장된 보안 작업 목록을 참조해야 합니다.

**표 1** 점검 목록 - 서버 배치 시 Oracle ILOM 보안 구성

| ✓ | **보안 작업** | **적용 가능한 펌웨어 버전** | **세부 정보 참조:** |
|---|---|---|---|
| | Oracle ILOM에 대한 보안 전용 관리 연결을 설정합니다. | 모든 펌웨어 버전 | ■ "물리적 관리 연결 보안" [13] |
| | 배치 시 또는 배치 후 FIPS 140-2 보안 준수가 필요한지 아니면 전혀 필요하지 않은지 여부를 결정합니다. | 펌웨어 버전 3.2.4 이상 | ■ "배치 시 FIPS 모드 구성 여부 선택" [14]<br>■ "FIPS 모드가 사용으로 설정된 경우 지원되지 않는 기능" [16] |

| ✓ | 보안 작업 | 적용 가능한 펌웨어 버전 | 세부 정보 참조: |
|---|---|---|---|
| | 미리 구성된 관리자 root 계정에 제공된 기본 암호를 수정합니다. | 모든 펌웨어 버전 | ■ "공유 사용자 계정 생성 방지" [23]<br>■ 처음 로그인할 때 root 계정에 대한 기본 암호 수정 [27] |
| | 미리 구성된 Oracle ILOM 서비스 및 열려 있는 네트워크 포트를 대상 환경에 적용할 수 있는지 여부를 결정합니다. | 모든 펌웨어 버전 | ■ "서비스 및 열린 네트워크 포트 보안" [17] |
| | Oracle ILOM에 대한 사용자 액세스를 구성합니다. | 모든 펌웨어 버전 | ■ "Oracle ILOM 사용자 액세스 보안" [22]<br>■ 역할 기반 권한을 가진 로컬 사용자 계정 만들기 [28] |
| | KVMS 세션 종료 시 호스트 운영 체제에 대한 액세스를 잠글지 여부를 결정합니다. | 펌웨어 버전 3.0.4 이상 | ■ KVMS 세션 종료 시 호스트 액세스 잠금 [29] |
| | SP에서 실행된 원격 KVMS 세션을 다른 SP 사용자가 보지 못하도록 제한할지 여부를 결정합니다. | 펌웨어 버전 3.2.4 이상 | ■ Remote System Console Plus의 표시 가능 KVMS 세션 제한(3.2.4 이상) [30] |
| | 사용자 로그인 시 또는 사용자 로그인 직후 보안 배너 메시지를 표시할지 여부를 결정합니다. | 펌웨어 버전 3.0.8 이상 | ■ 로그인 배너로 시스템 액세스 보안 설정(3.0.8 이상) [31] |
| | 최대 보안 등록 정보가 모든 Oracle ILOM 사용자 인터페이스에 대해 설정되었는지 확인합니다. | 모든 펌웨어 버전 | ■ "보안을 최대화하도록 Oracle ILOM 인터페이스 구성" [33] |

# 서버 배치 후 보안 점검 목록

사용 환경의 기존 서버에서 어떤 Oracle ILOM 보안 방식이 유지 관리하는 데 가장 적합한지 확인하려면 시스템 관리자가 다음 표 2. "점검 목록 - 서버 배치 후 Oracle ILOM 보안 유지 관리 "에서 권장된 보안 작업 목록을 참조해야 합니다.

**표 2** 점검 목록 - 서버 배치 후 Oracle ILOM 보안 유지 관리

| ✓ | 보안 작업 | 적용 가능한 펌웨어 버전 | 세부 정보 참조: |
|---|---|---|---|
| | Oracle ILOM에 대한 보안 관리 연결을 유지 관리합니다. | 모든 펌웨어 버전 | ■ "인증되지 않은 호스트 KCS 장치 액세스 방지" [49]<br>■ "선호하는 인증된 호스트 상호 연결 액세스" [50]<br>■ "IPMI 2.0 암호화를 사용하여 채널 보안 설정" [51] |
| | 원격 KVMS 및 직렬 텍스트 기반 세션이 Oracle ILOM에서 안전하게 실행되었는지 확인합니다. | 모든 펌웨어 버전 | ■ "KVMS 원격 통신 및 암호화" [53]<br>■ "원격 KVMS 공유 액세스로부터 보호" [53]<br>■ "호스트 직렬 콘솔 공유 액세스로부터 보호" [54] |

| ✓ | 보안 작업 | 적용 가능한 펌웨어 버전 | 세부 정보 참조: |
|---|---|---|---|
| | Oracle ILOM에 대한 사용자 액세스를 유지 관리하고 추적합니다. | 모든 펌웨어 버전 | ■ "사용자 액세스 보안을 위한 배치 후 고려 사항" [54] |
| | 미리 구성된 관리자 `root` 계정의 분실 암호를 재설정하는 데 필요한 보안 작업 | 펌웨어 버전 3.1 이상 | ■ "`root` 계정 기본 암호를 재설정하기 위한 물리적 보안 존재" [56] |
| | 서버 배치 후 Oracle ILOM에서 FIPS 140-2 준수 모드를 수정해야 할 경우에 필요한 보안 작업 | 펌웨어 버전 3.2.4 이상 | ■ 배치 후 FIPS 모드 수정 [58]<br>■ "FIPS 모드가 사용으로 설정된 경우 지원되지 않는 기능" [16] |
| | 서버에서 소프트웨어 및 펌웨어가 최신 버전인지 확인합니다. | 모든 펌웨어 릴리스 | ■ "최신 소프트웨어 및 펌웨어로 업데이트" [60] |

# Oracle ILOM 보안을 위한 배치 관련 최적의 방법

다음 항목을 참조하여 서버 배치 시 구현할 Oracle ILOM 보안을 위한 최적의 방법을 결정할 수 있습니다.

- “물리적 관리 연결 보안” [13]
- “배치 시 FIPS 모드 구성 여부 선택” [14]
- “서비스 및 열린 네트워크 포트 보안” [17]
- “Oracle ILOM 사용자 액세스 보안” [22]
- “보안을 최대화하도록 Oracle ILOM 인터페이스 구성” [33]

### 관련 정보

- Oracle ILOM 보안 관련 최적의 방법 점검 목록.
- Oracle ILOM 보안을 위한 배치 후 최적의 방법
- Oracle ILOM 펌웨어 릴리스별 보안 기능 [7]

## 물리적 관리 연결 보안

Oracle ILOM은 Oracle 서버를 유지 관리하고 모니터링하는 데 전용 관리 채널을 사용하는 OOB(아웃오브밴드) 관리 도구입니다. 인밴드 관리 도구가 포함된 서버와 달리, Oracle 서버에는 원격 관리 기능이 내장되어 있으므로 시스템 관리자가 서비스 프로세서에 있는 별도의 전용 네트워크 커넥터를 통해 Oracle ILOM에 보안 상태로 액세스할 수 있습니다. Oracle ILOM의 관리 기능은 시스템 관리자가 Oracle 서버를 모니터링하고 관리할 수 있는 특정 기능을 제공하지만, Oracle ILOM은 범용 컴퓨터 엔진으로 사용하거나 신뢰할 수 없는 비보안 네트워크 연결을 통해 액세스할 수 없습니다.

Oracle ILOM에 대한 물리적 관리 연결을 로컬 직렬 포트, 전용 네트워크 관리 포트 또는 표준 데이터 네트워크 포트를 통해 설정할지 여부에 관계없이, 서버 또는 CMM(섀시 모니터링 모듈)에 있는 이 물리적 포트는 항상 신뢰할 수 있는 내부 네트워크 또는 전용 보안 관리 또는 개인 네트워크에 연결되어야 합니다. Oracle ILOM에 대한 물리적 관리 연결을 설정할 경우 추가 지침은 다음 표를 참조하십시오.

| Oracle ILOM에 대한 물리적 포트 관리 연결 | 지원되는 Oracle 하드웨어 | 관리 연결 보안 지침 |
|---|---|---|
| 전용 연결 | ■ 서버(포트: NET MGT)<br>■ CMM(포트: NET MGT) | 일반 데이터 네트워크 트래픽과 구분하려면 SP(서비스 프로세서)에 전용 내부 네트워크를 사용하십시오.<br>Oracle ILOM에 대한 전용 네트워크 관리 연결 설정에 대한 자세한 내용은 다음을 참조하십시오.<br>■ *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(3.2.x)*, 전용 네트워크 관리 연결 |
| 로컬 연결 | ■ 서버(포트: SER MGT)<br>■ CMM(포트: SER MGT) | 물리적 서버 또는 CMM에서 직접 Oracle ILOM에 액세스하려면 로컬 직렬 관리 연결을 사용하십시오.<br>Oracle ILOM에 대한 로컬 직렬 관리 연결 설정에 대한 자세한 내용은 다음을 참조하십시오.<br>■ *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(3.2.x)*, Oracle ILOM에 대한 로컬 직렬 네트워크 관리 연결 |
| 사이드밴드 연결 | 서버(포트: NET0, NET1, NET2, NET3) | 두 개의 별도 네트워크 연결이 필요하지 않도록 케이블 관리 및 네트워크 구성을 단순화해야 할 때마다 공유 이더넷 데이터 네트워크를 사용하여 서비스 프로세서 SP에 액세스하십시오.<br>Oracle ILOM에 대한 사이드밴드 관리 연결 설정에 대한 자세한 내용은 다음을 참조하십시오.<br>■ *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(3.2.x)*, 사이드밴드 관리 연결<br>**참고** - 사이드밴드 관리는 대부분의 Oracle 서버에서 지원됩니다. |

**참고** - 보안 공격으로부터 보호하려면 **Oracle ILOM SP를 공용 네트워크(예: 인터넷)에 연결하면 안됩니다**. Oracle ILOM SP 관리 트래픽을 별도의 관리 네트워크에 유지하고 시스템 관리자에게만 액세스 권한을 부여해야 합니다.

# 배치 시 FIPS 모드 구성 여부 선택

Oracle ILOM 펌웨어 릴리스 3.2.4부터 Oracle ILOM CLI 및 웹 인터페이스에서 FIPS(Federal Information Processing Standard) 준수를 위한 구성 가능한 모드를 제공합니다. 이 모드가 사용으로 설정된 경우 Oracle은 시스템 기밀 데이터 또는 중요 데이터를 보호하기 위해 FIPS 140-2 보안 표준에 따라 암호화 알고리즘을 사용합니다.

펌웨어 3.2.4 이상이 포함된 서버를 배치하는 시스템 관리자는 다른 Oracle ILOM 등록 정보를 구성하기 전에 FIPS 모드를 구성할지 여부를 결정해야 합니다. 기본적으로 Oracle ILOM의 FIPS 준수 모드는 사용 안함으로 설정되어 제공됩니다. FIPS 준수 모드를 변경하면 모든 구성 데이터가 출하 시 기본값으로 재설정됩니다.

배치 시(Oracle ILOM 등록 정보를 구성하기 전) FIPS 준수 모드를 사용으로 설정하려면 배치 시 FIPS 모드 사용으로 설정 [15]을 참조하십시오. 사용자 정의 구성 등록 정보가 이미 Oracle ILOM에 설정되어 있으며 FIPS 등록 정보를 수정해야 하는 경우 "FIPS 모드 수정을 위한 배치 후 작업" [58]을 참조하십시오.

# ▼ 배치 시 FIPS 모드 사용으로 설정

---

**참고** - Oracle ILOM의 FIPS 준수 모드는 State 및 Status 등록 정보로 표시됩니다. State 등록 정보는 Oracle ILOM에서 구성된 모드를 나타내고, Status 등록 정보는 Oracle ILOM의 작동 모드를 나타냅니다. FIPS State 등록 정보가 변경된 경우 다음에 Oracle ILOM을 재부트해야 변경 사항이 작동 모드(FIPS Status 등록 정보)에 적용됩니다.

---

**시작하기 전에**

- FIPS State 및 Status 등록 정보는 기본적으로 사용 안함으로 설정되어 제공됩니다.
- FIPS가 사용으로 설정(구성되어 작동 가능함)된 경우 Oracle ILOM의 일부 기능이 지원되지 않습니다. FIPS가 사용으로 설정된 경우 지원되지 않는 기능 목록은 표 3. "FIPS 모드가 사용으로 설정된 경우 Oracle ILOM에서 지원되지 않는 기능"을 참조하십시오.
- FIPS State 등록 정보를 수정하려면 Admin(a) 역할이 필요합니다.
- FIPS 준수에 대한 구성 가능한 등록 정보는 Oracle ILOM 펌웨어 3.2.4 이상부터 사용할 수 있습니다. 펌웨어 릴리스 3.2.4 이전에는 Oracle ILOM에서 FIPS 준수에 대해 구성 가능한 등록 정보를 제공하지 않습니다.
- Oracle ILOM에서 FIPS 모드 State 및 Status 등록 정보를 수정할 경우 사용자 정의 구성 설정이 모두 출하 시 기본값으로 재설정됩니다.

1. **Oracle ILOM 웹 인터페이스에서 ILOM Administration -> Management Access -> FIPS를 누릅니다.**

2. **FIPS 페이지에서 다음을 수행합니다.**

   a. **FIPS State 확인란을 선택하여 구성된 FIPS 등록 정보를 사용으로 설정합니다.**

   b. **Save를 눌러 변경 내용을 적용합니다.**

   구성에 대한 자세한 내용은 FIPS 웹 페이지에서 `More details...` 링크를 누릅니다.

3. **Oracle ILOM에서 FIPS 작동 모드 상태를 변경하려면 다음 단계를 수행하여 Oracle ILOM을 재부트합니다.**

   a. **웹 인터페이스에서 ILOM Administration -> Maintenance -> SP Reset을 누릅니다.**

**b. SP Reset 페이지에서 SP Reset 버튼을 누릅니다.**

Oracle ILOM이 재부트될 때 다음과 같은 동작이 발생합니다.

- 마지막으로 구성된 FIPS State(사용)가 시스템에 적용됩니다.
- Oracle ILOM에서 이전에 구성된 사용자 정의 구성 설정이 출하 시 기본값으로 재설정됩니다.
- Oracle ILOM에서 현재 사용으로 설정된 작동 상태를 반영하도록 FIPS Status 등록 정보가 업데이트됩니다.

  FIPS Status 메시지에 대한 전체 목록 및 설명을 보려면 FIPS 페이지의 `More details` 링크를 누릅니다.
- FIPS 방패 아이콘이 웹 인터페이스의 마스트헤드 영역에 나타납니다.
- 지원되지 않는 모든 FIPS 기능이 CLI 및 웹 인터페이스에서 사용 안함으로 설정되거나 제거됩니다.

  지원되지 않는 FIPS 기능에 대한 전체 목록 및 설명을 보려면 FIPS 페이지의 `More details` 링크를 누릅니다.

### 관련 정보

- "FIPS 모드가 사용으로 설정된 경우 지원되지 않는 기능" [16]
- "FIPS 모드 수정을 위한 배치 후 작업" [58]
- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(3.2.x)*, FIPS 모드 등록 정보 구성

## FIPS 모드가 사용으로 설정된 경우 지원되지 않는 기능

Oracle ILOM에서 FIPS 준수를 사용으로 설정할 경우 Oracle ILOM의 다음과 같은 FIPS 140-2 비준수 기능이 지원되지 않습니다.

**표 3** FIPS 모드가 사용으로 설정된 경우 Oracle ILOM에서 지원되지 않는 기능

| 지원되지 않는 FIPS 모드 기능 | 설명 |
|---|---|
| IPMI 1.5 | FIPS 모드가 사용으로 설정되어 있고 시스템에서 실행 중인 경우 IPMI 1.5 구성 등록 정보가 Oracle ILOM CLI 및 웹 인터페이스에서 제거됩니다. IPMI 2.0 서비스는 Oracle ILOM에서 자동으로 사용으로 설정됩니다. IPMI 2.0에서는 FIPS 준수 모드 및 비준수 모드가 모두 지원됩니다. |
| Oracle ILOM System Remote Console의 펌웨어 호환성 | Oracle ILOM의 FIPS 모드는 Oracle ILOM Remote System Console의 이전 펌웨어 버전이 최신 Oracle ILOM Remote System Console 펌웨어 버전과 호환되지 못하도록 합니다.<br><br>예를 들어 Oracle ILOM Remote System Console 클라이언트 펌웨어 버전 3.2.4는 Oracle ILOM Remote System Console 펌웨어 버전 3.2.3 및 이전 버전과 역호환됩니다. 그러나 Oracle ILOM Remote System Console 클라이언트 펌웨어 버전 3.2.2 및 이전 버전은 Oracle ILOM Remote System Console 펌웨어 버전 3.2.4 및 이후 버전과 호환되지 않습니다. |

| 지원되지 않는 FIPS 모드 기능 | 설명 |
|---|---|
| | **참고** - Oracle ILOM Remote System Console Plus에는 이 펌웨어 호환성 제한 사항이 적용되지 않습니다. Oracle ILOM Remote System Console Plus는 최신 서비스 프로세서 시스템(예: SPARC T5 이상 시스템) 및 Oracle Server x4-4, x4-8 이상 시스템에 제공됩니다. Oracle ILOM Remote System Console은 이전 서비스 프로세서 시스템(예: SPARC T3 및 T4) 및 Sun Server x4-2/2L/2B 및 이전 시스템에 제공됩니다. |
| LDAP(Lightweight Directory Access Protocol) | FIPS 모드가 사용으로 설정되어 있고 시스템에서 실행 중인 경우 Oracle ILOM의 LDAP 구성 등록 정보가 Oracle ILOM CLI 및 웹 인터페이스에서 자동으로 제거됩니다.<br>**참고** - 원격 인증 서비스 Active Directory 및 LDAP/SSL은 FIPS 준수 모드 및 비준수 모드에서 모두 지원됩니다. |
| RADIUS(Remote Authentication Dial-In User Service) | FIPS 모드가 사용으로 설정되어 있고 시스템에서 실행 중인 경우 Oracle ILOM의 RADIUS 구성 등록 정보가 Oracle ILOM CLI 및 웹 인터페이스에서 자동으로 제거됩니다.<br>**참고** - 원격 인증 서비스 Active Directory 및 LDAP/SSL은 FIPS 준수 모드 및 비준수 모드에서 모두 지원됩니다. |
| SNMP(Simple Network Management Protocol) DES 및 MD5 | FIPS 모드가 사용으로 설정되어 있고 시스템에서 실행 중인 경우 DES 프라이버시 프로토콜 및 MD5 인증 프로토콜에 대한 SNMP 구성 등록 정보가 Oracle ILOM CLI 또는 웹 인터페이스에서 지원되지 않습니다. |

# 서비스 및 열린 네트워크 포트 보안

서비스 및 해당 네트워크 포트가 Oracle ILOM에서 올바르게 구성되었는지 확인하려면 다음 항목을 참조하십시오.

- “미리 구성된 서비스 및 네트워크 포트” [17]
- “불필요한 서비스 및 열린 포트 관리” [18]
- “서비스 및 네트워크 포트 구성” [19]

## 미리 구성된 서비스 및 네트워크 포트

Oracle ILOM은 기본적으로 대부분의 서비스가 사용으로 설정된 상태로 사전 구성됩니다. 이는 Oracle ILOM의 배치를 단순하고 직관적으로 만듭니다. 하지만 서버의 각 열린 서비스 네트워크 포트는 악의적인 사용자의 잠재적 공격 지점을 나타냅니다. 따라서 초기 Oracle ILOM 설정과 목적을 이해하고 배치된 시스템에 실제로 필요한 서비스를 선택하는 것이 중요합니다. 최상의 보안을 위해서는 필요한 Oracle ILOM 서비스만 사용으로 설정하십시오.

다음 표는 Oracle ILOM에서 기본적으로 사용으로 설정되는 서비스를 나열합니다.

**표 4** 기본적으로 사용으로 설정되는 서비스 및 포트

| 서비스 | 포트 |
|---|---|
| HTTPS로 HTTP 재지정 | 80 |
| HTTPS | 443 |

| 서비스 | 포트 |
|---|---|
| IPMI | 623 |
| Oracle ILOM Remote Console용 원격 KVMS | 5120, 5121, 5122, 5123, 5555, 5556, 7578, 7579 |
| Oracle ILOM Remote Console Plus용 원격 KVMS | 5120, 5555 |
| 서비스 태그 | 6481 |
| SNMP | 161 |
| Single Sign-on | 11626 |
| SSH | 22 |

다음 표는 Oracle ILOM에서 기본적으로 사용 안함으로 설정되는 서비스를 보여줍니다.

**표 5** 기본적으로 사용 안함으로 설정되는 서비스 및 포트

| 서비스 | 포트 |
|---|---|
| HTTP | 80 |

# 불필요한 서비스 및 열린 포트 관리

모든 Oracle ILOM 서비스는 선택적으로 사용 안함으로 설정하여 해당 서비스에 대한 각 열린 네트워크 포트를 닫을 수 있습니다. 대부분의 서비스는 기본적으로 사용으로 설정되지만 일부 기능을 사용 안함으로 설정하거나 기본 설정을 변경하여 Oracle ILOM 환경을 더욱 안전하게 만들 수 있습니다. 모든 Oracle ILOM 서비스를 사용 안함으로 설정할 수 있지만, 이 경우 해당 기능을 사용하지 못하게 됩니다. 일반적으로 배치 환경에서 반드시 필요한 서비스만 사용으로 설정하십시오. 네트워크 서비스를 일부만 사용으로 설정하여 얻게 되는 보안 이점과 이로 인한 기능 손실의 단점을 서로 비교해야 합니다.

다음 표에서는 각 서비스를 사용 또는 사용 안함으로 설정할 경우 미치는 영향에 대해 설명합니다.

**표 6** 서비스를 사용 안함으로 설정할 경우

| 서비스 | 설명 | 사용/사용 안함으로 설정 결과 |
|---|---|---|
| HTTP | Oracle ILOM 웹 인터페이스에 액세스하기 위한 암호화되지 않은 프로토콜 | 이 서비스를 사용으로 설정하면 암호화된 HTTP(HTTPS)보다 성능이 빨라집니다. 하지만 이 프로토콜을 사용하면 민감한 정보가 암호화 없이 인터넷을 통해 전송됩니다. |
| HTTPS | Oracle ILOM 웹 인터페이스에 액세스하기 위한 암호화된 프로토콜 | 이 서비스를 사용으로 설정하면 웹 브라우저와 Oracle ILOM 사이의 통신이 안전해집니다. 하지만 Oracle ILOM에 열린 네트워크 포트가 필요하므로 서비스 거부와 같은 공격을 받을 수 있는 취약점이 높아집니다. |

| 서비스 | 설명 | 사용/사용 안함으로 설정 결과 |
|---|---|---|
| Servicetag | 서버를 식별하고 서비스 요청을 효율화하는 데 사용되는 Oracle 검색 프로토콜 | 이 서비스를 사용 안함으로 설정하면 Oracle Enterprise Manager Ops Center에서 Oracle ILOM을 검색하지 못하게 되고 다른 Oracle 자동 서비스 솔루션으로 통합되지 않습니다.<br><br>Servicetag 상태는 Oracle ILOM CLI에서만 구성할 수 있습니다. 예를 들어 servicetag 상태 등록 정보를 수정하려면 다음과 같이 입력하십시오.<br><br>`set /SP/services/servicetag state=`*enabled\|disabled* |
| IPMI | 표준 관리 프로토콜 | 이 서비스를 사용 안함으로 설정하면 Oracle Enterprise Manager Ops Center 및 타사 소프트웨어에 대한 일부 Oracle 관리 커넥터에서 시스템을 관리하지 못하게 됩니다. |
| SNMP | Oracle ILOM의 건전성 모니터링 및 수신된 트랩 통지 모니터링을 위한 표준 관리 프로토콜 | 이 서비스를 사용 안함으로 설정하면 Oracle Enterprise Manager Ops Center 및 타사 소프트웨어에 대한 일부 Oracle 관리 커넥터에서 시스템을 관리하지 못하게 됩니다. |
| KVMS | 원격 키보드, 비디오, 마우스 및 저장소 제공을 위한 프로토콜 세트 | 이 서비스를 사용 안함으로 설정하면 호스트 콘솔 및 원격 저장소 기능을 사용하지 못하게 되어 Oracle ILOM Remote System Console(또는 Oracle ILOM Remote System Console Plus) 및 Storage Redirection CLI 응용 프로그램을 사용할 수 없습니다. |
| SSH | 원격 셸 액세스를 위한 보안 프로토콜 | 이 서비스를 사용 안함으로 설정하면 네트워크를 통한 명령줄 액세스가 허용되지 않고 Oracle Enterprise Manager Ops Center에서 Oracle ILOM을 검색하지 못할 수 있습니다. |
| SSO | 사용자가 사용자 이름과 암호를 입력해야 하는 횟수를 줄이는 Single Sign-On 기능 | 이 서비스를 사용 안함으로 설정하면 KVMS를 실행할 때 암호를 다시 입력해야 하고 CMM(섀시 모니터링 모듈)에서 블레이드 SP로 드릴다운할 때도 암호를 다시 입력해야 합니다. |

개별 네트워크 서비스를 사용 및 사용 안함으로 설정하는 방법은 "서비스 및 네트워크 포트 구성" [19] 항목을 참조하십시오.

# 서비스 및 네트워크 포트 구성

Oracle ILOM에서 관리 서비스 및 해당 네트워크 포트를 구성하는 방법에 대한 지침은 다음 절차를 참조하십시오.

- 프로토콜 관리 서비스 상태 및 포트 수정 [20]
- KVMS 서비스 상태 및 포트 수정 [21]
- Single Sign-On 서비스 상태 및 포트 수정 [21]

서비스 및 해당 네트워크 포트는 Oracle ILOM CLI(명령줄 인터페이스) 또는 웹 인터페이스를 통해 사용 또는 사용 안함으로 설정할 수 있습니다. 이 절의 절차는 모든 Oracle ILOM 펌웨어 릴리스에 대한 웹 기반 탐색 지침을 제공합니다. CLI 지침 또는 구성 등록 정보에 대한 추가 세부 정보는 각 절차 뒤에 나오는 관련 정보 절에 나열된 해당 설명서를 참조하십시오.

# ▼ 프로토콜 관리 서비스 상태 및 포트 수정

시작하기 전에 **시작하기 전에**

- Oracle ILOM에서 기본적으로 사용 또는 사용 안함으로 설정되는 프로토콜 서비스 및 네트워크 포트를 확인하려면 다음 표를 참조하십시오.
  - 표 4. “기본적으로 사용으로 설정되는 서비스 및 포트”
  - 표 5. “기본적으로 사용 안함으로 설정되는 서비스 및 포트”
- 프로토콜 서비스의 State 등록 정보를 수정하려면 Oracle ILOM에서 Admin(a) 역할이 필요합니다.

네트워크 서비스의 State 등록 정보를 수정하려면 다음 단계를 수행하십시오.

1. **Oracle ILOM 웹 인터페이스에서 Management Access 서비스로 이동합니다.**

   예를 들면 다음과 같습니다.

   - **3.0.x 웹 인터페이스에서 Configuration -> System Management Access를 누릅니다.**
   - **3.1 이상 웹 인터페이스에서 ILOM Administration -> Management Access를 누릅니다.**

2. **아래에 나열된 적합한 Management Access -> 서비스 탭을 누릅니다.**

| Management Access -> | 설명 |
|---|---|
| Web Server | Web Server 페이지에서는 HTTP 및 HTTPS 프로토콜 관리 액세스에 대한 서비스 상태 및 포트 지정을 관리할 수 있습니다. |
| IPMI | IPMI 페이지에서는 IPMI 프로토콜 관리 액세스에 대한 서비스 상태 및 포트 등록 정보를 관리할 수 있습니다. |
| SNMP | SNMP 페이지에서는 SNMP 관리 액세스에 대한 서비스 상태 및 포트 등록 정보를 관리할 수 있습니다. |
| SSH | SSH 페이지에서는 SSH(보안 셸) 관리 액세스에 대한 서비스 상태 등록 정보를 관리할 수 있습니다. |

3. **Management Access -> 서비스 페이지에서 State 등록 정보를 수정한 다음 Save를 눌러 변경 내용을 적용합니다.**

   프로토콜 서비스의 State 등록 정보를 사용 안함으로 설정하면 해당 프로토콜 서비스 네트워크 포트가 닫히고 Oracle ILOM에서 프로토콜 서비스를 사용하지 못하게 됩니다.

### 관련 정보

- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, 관리 서비스 및 네트워크 기본 등록 정보
- *Oracle ILOM 3.1* 구성 및 유지 관리 설명서, 관리 서비스 및 네트워크 기본 등록 정보
- *Oracle ILOM 3.0* 일상적인 관리 - *CLI* 절차 안내서, 네트워크 설정 구성
- *Oracle ILOM 3.0* 일상적인 관리 - 웹 절차 안내서, 네트워크 설정 구성

## ▼ KVMS 서비스 상태 및 포트 수정

시작하기 전에 **시작하기 전에**

- KVMS 서비스 State 등록 정보는 Oracle ILOM에서 기본적으로 사용으로 설정됩니다. KVMS 서비스와 연관된 열린 네트워크 포트 목록은 표 4. “기본적으로 사용으로 설정되는 서비스 및 포트”를 참조하십시오.
- Oracle ILOM에서 KVMS State 등록 정보를 수정하려면 Admin(a) 역할이 필요합니다.

1. **Oracle ILOM 웹 인터페이스에서 KVMS 탭으로 이동합니다.**

   예를 들면 다음과 같습니다.

   - **3.0.x 웹 인터페이스에서 Remote Control -> KVMS를 누릅니다.**
   - **3.1 이상 웹 인터페이스에서 Remote Console -> KVMS를 누릅니다.**

2. **KVMS 탭에서 KVMS State 등록 정보를 수정한 다음 Save를 눌러 변경 내용을 적용합니다.**

   State 등록 정보를 사용 안함으로 설정하면 해당 열린 KVMS 서비스 네트워크 포트가 닫히며 이로 인해 a) 원격 호스트 콘솔, b) Oracle ILOM Remote Console 및 Oracle ILOM Remote Storage CLI 또는 Oracle ILOM Remote Console Plus를 사용하지 못하게 됩니다.

### 관련 정보

- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, 로컬 클라이언트 KVMS 설정 구성
- *Oracle ILOM 3.1* 구성 및 유지 관리 설명서, 로컬 클라이언트 KVMS 설정 구성
- *Oracle ILOM 3.0* 원격 리디렉션 콘솔 - 웹 및 *CLI* 안내서, 초기 설정 작업

## ▼ Single Sign-On 서비스 상태 및 포트 수정

시작하기 전에 **시작하기 전에**

- SSO(Single Sign-On) 서비스의 State 등록 정보 및 해당 네트워크 포트(1126)는 Oracle ILOM에서 기본적으로 사용으로 설정됩니다.
- SSO 서비스 State 등록 정보를 수정하려면 Oracle ILOM에서 Admin(a) 역할이 필요합니다.

1. **Oracle ILOM 웹 인터페이스에서 User Account 탭으로 이동합니다.**

   예를 들면 다음과 같습니다.

   - **3.0.x 웹 인터페이스에서 User Management -> User Account를 누릅니다.**
   - **3.1 이상 웹 인터페이스에서 ILOM Administration -> User Account를 누릅니다.**

2. **User Account 탭에서 SSO State 등록 정보를 수정한 다음 Save를 눌러 변경 내용을 적용합니다.**

   Oracle ILOM에서 SSO State 등록 정보를 사용 안함으로 설정하면 a) 열려 있는 SSO 네트워크 포트가 닫히고 b) KVMS 콘솔 실행 시 암호를 다시 입력하라는 메시지가 사용자에게 표시되며 c) CMM 사용자의 경우 암호를 다시 입력하지 않고도 블레이드 서버 SP로 이동할 수 있습니다.

**관련 정보**

- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, Single Sign-On 서비스
- *Oracle ILOM 3.1* 구성 및 유지 관리 설명서, Single Sign-On 서비스
- *Oracle ILOM 3.0* 일상적인 관리 - *CLI* 절차 안내서, Single Sign-On 구성
- *Oracle ILOM 3.0* 일상적인 관리 - 웹 절차 안내서, Single Sign-On 구성

# Oracle ILOM 사용자 액세스 보안

Oracle ILOM에서 사용자 액세스 보안을 설정하려면 다음 항목을 참조하십시오.

# 공유 사용자 계정 생성 방지

보안 환경을 유지하려면 공유 계정을 만들지 마십시오. 공유 계정은 사용자 계정 암호를 공유하는 사용자 계정입니다. 공유 계정을 만드는 대신 사용자 계정 처리를 위한 이상적인 방법은 Oracle ILOM에 액세스하는 각 사용자에 대해 고유한 암호를 만드는 것입니다. 사용자 계정과 암호 조합은 해당 사용자만 알고 있어야 합니다.

---

**참고** - Oracle ILOM은 최대 10개의 로컬 사용자 계정을 지원합니다. 더 많은 사용자가 Oracle ILOM에 액세스해야 하는 경우 디렉토리 서비스(예: LDAP 또는 Active Directory)를 구성하여 중앙 데이터베이스를 통해 더 많은 계정을 지원할 수 있습니다. 자세한 내용은 "원격 인증 서비스 및 보안 프로파일" [26]을 참조하십시오.

---

고유한 암호를 사용하여 개별 사용자 계정을 설정한 후 시스템 관리자는 미리 구성된 관리자 `root` 계정에 고유한 암호를 지정했는지 확인해야 합니다. 그렇지 않고 고유한 암호를 사용하지 않을 경우 미리 구성된 관리자 `root` 계정이 공유 계정으로 간주됩니다. 인증되지 않은 사용자가 미리 구성된 관리자 `root` 계정을 사용하지 못하도록 하려면 암호를 수정하거나 미리 구성된 `root` 계정을 Oracle ILOM에서 제거해야 합니다. 미리 구성된 관리자 `root` 계정에 대한 자세한 내용은 처음 로그인할 때 `root` 계정에 대한 기본 암호 수정 [27]을 참조하십시오.

고유 암호를 사용한 보안 계정 설정에 대한 추가 지침은 "사용자 계정 및 암호 관리를 위한 보안 지침" [24]을 참조하십시오.

사용자 계정 구성 정보는 "보안을 최대화하도록 사용자 액세스 구성" [27]을 참조하십시오.

# 역할 기반 권한 지정

모든 Oracle ILOM 사용자 계정에는 일련의 역할 기반 권한이 지정됩니다. 이러한 역할 기반 권한은 Oracle ILOM 내의 개별 기능에 대한 액세스를 제공합니다. 사용자가 시스템을 모니터링만 하고 구성 변경 작업은 할 수 없도록 사용자 계정을 구성할 수 있습니다. 또는 사용자가 사용자 계정 만들기 및 수정을 제외한 대부분의 구성 옵션을 수정하도록 허용할 수 있습니다. 또한 서버 전원을 제어하고 원격 콘솔에 액세스할 수 있는 사용자를 제한하는 것도 가능합니다. 권한 레벨을 이해하고 조직의 사용자에게 적절하게 권한을 지정하는 것이 중요합니다.

다음 표에서는 개별 Oracle ILOM 사용자 계정에 지정할 수 있는 권한 목록을 정의합니다.

**표 7** 사용자 계정 권한 설명

| 역할 | 설명 |
|---|---|
| `Admin(a)` | 다른 권한(User Management 등)을 통해 명시적으로 부여되는 구성 옵션을 제외하고 사용자가 모든 Oracle ILOM 구성 옵션을 변경할 수 있습니다. |

| 역할 | 설명 |
|---|---|
| User Management(u) | 사용자가 사용자 추가 및 제거, 사용자 암호 변경 및 인증 서비스 구성 작업을 수행할 수 있습니다. 이 역할을 가진 사용자는 모든 권한을 가진 두번째 사용자 계정을 만들 수 있으므로 이 역할은 모든 사용자 역할 중 가장 높은 레벨의 권한을 가집니다. |
| Console(c) | 사용자가 호스트 콘솔에 원격으로 액세스할 수 있습니다. 이 원격 콘솔 액세스를 통해 사용자는 BIOS 또는 OBP(OpenBoot PROM)에 액세스하여 시스템에 대한 액세스 권한을 얻기 위한 방법으로 부트 동작을 변경할 수도 있습니다. |
| Reset and Host Control(r) | 사용자가 호스트 전원을 제어하고 Oracle ILOM을 재설정할 수 있습니다. |
| Read-only(o) | 사용자가 Oracle ILOM 사용자 인터페이스에 대한 읽기 전용 액세스 권한만 가집니다. 모든 사용자가 이 액세스 권한을 가지므로 누구나 로그 및 환경 정보를 읽고 구성 설정을 볼 수 있습니다. |

로컬 사용자 계정 만들기 및 역할 기반 권한 지정에 대한 자세한 내용은 역할 기반 권한을 가진 로컬 사용자 계정 만들기 [28]를 참조하십시오.

# 사용자 계정 및 암호 관리를 위한 보안 지침

Oracle ILOM 사용자 계정 및 암호를 관리하는 경우 다음과 같은 보안 지침을 고려하십시오.



## 사용자 계정 관리 지침

| 사용자 계정 관리 지침 | 설명 |
|---|---|
| 사용자 계정 공유 사용 안함 | 항상 Oracle ILOM 사용자마다 별도의 계정을 만들어야 합니다.<br><br>Oracle ILOM에서는 로컬 사용자 계정을 10개까지 지원합니다. 관리하는 사이트가 많아 사용자 계정이 10개 이상 필요한 경우 타사 사용자 인증 서비스(예: LDAP 또는 Active Directory) 사용을 고려해야 합니다.<br><br>Oracle ILOM에서 외부 인증 서비스를 통해 사용자 인증을 구현하는 자세한 방법은 "원격 인증 서비스 및 보안 프로파일" [26]을 참조하십시오. |
| 로컬 사용자 계정에 대해 규칙을 준수하는 이름 선택 | 로컬 Oracle ILOM 사용자 계정에 대한 사용자 이름을 선택하는 경우 사용자 이름은 다음 규칙을 따라야 합니다.<br><br>■ 길이가 4 - 16자여야 합니다(첫 자는 문자여야 함).<br>■ 조직에서 고유해야 합니다.<br>■ 공백, 마침표(.) 또는 콜론(:)이 포함되지 않아야 합니다. |
| 로컬 사용자 계정에 대해 규칙을 준수하는 암호 선택 | 로컬 Oracle ILOM 사용자 계정에 대한 암호를 선택하는 경우 암호는 다음 규칙을 따라야 합니다. |

| 사용자 계정 관리 지침 | 설명 |
|---|---|
| | ■ 항상 최대 16자를 포함하는 강력한 암호여야 합니다.<br>■ 대문자와 소문자가 섞여 있고 특수 문자가 한 개 또는 두 개 포함되어 있는 강력하고 복잡한 암호를 만들어야 합니다,<br>■ 공백, 마침표(.) 또는 콜론(:)이 포함되지 않아야 합니다.<br>■ 회사의 암호 관리 정책을 따라야 합니다.<br><br>Oracle ILOM에서 암호 관리에 대한 자세한 내용은 "사용자 계정 및 암호 관리를 위한 보안 지침" [24]을 참조하십시오. |
| 직무에 따라 사용자 계정 권한 제한(최소 권한 원칙) | 최소 권한 원칙이란 좋은 보안 습관을 위해 사용자에게 작업을 수행할 수 있는 최소한의 권한을 부여하는 것입니다. 책임, 역할, 권한 등의 과도한 부여(특히 조직의 수명 주기 초기에)는 시스템 오용으로 이어질 수 있습니다. 정기적으로 사용자 권한을 검토하여 각 사용자의 현재 작업 책임과의 관련성을 확인하십시오.<br><br>Oracle ILOM은 각 사용자에 대한 사용자 권한을 제어할 수 있는 기능을 제공합니다. 작업 역할을 기준으로 각 사용자 계정에 적절한 사용자 역할 권한이 지정되도록 하십시오.<br><br>역할 기반 권한을 가진 사용자 계정을 만드는 자세한 방법은 역할 기반 권한을 가진 로컬 사용자 계정 만들기 [28]를 참조하십시오. |

## 암호 관리 지침

| 암호 관리 지침 | 설명 |
|---|---|
| 처음 로그인한 즉시 기본 암호(changeme) 변경 | 처음 로그인할 때 Oracle ILOM에 액세스할 수 있도록 로컬 관리자 계정(root)이 시스템에 제공됩니다. 보안 환경을 만들려면 Oracle ILOM에 처음 로그인한 후 제공된 관리자 암호(changeme)를 변경해야 합니다.<br><br>root 관리자 계정에 대한 허용되지 않은 액세스가 제공되면 사용자는 Oracle ILOM의 모든 기능에 제한 없는 액세스가 가능합니다. 따라서 강력하고 안전한 암호를 지정하는 것이 매우 중요합니다. |
| 정기적으로 모든 Oracle ILOM 계정 암호 변경 | 악의적인 작업을 방지하고 암호가 현재 암호 정책을 준수하도록 하려면 정기적으로 모든 Oracle ILOM 암호를 변경해야 합니다. |
| 강력하고 복잡한 암호를 만들기 위한 일반적인 원칙 적용 | 강력하고 복잡한 암호를 만들려면 다음과 같은 일반적인 원칙을 적용하십시오.<br><br>■ 길이가 16자 미만인 암호를 만들지 마십시오.<br>■ 사용자 이름, 직원 이름 또는 가족 이름이 포함된 암호를 만들지 마십시오.<br>■ 쉽게 추측할 수 있는 암호를 선택하지 마십시오.<br>■ 연속된 숫자 문자열(예: 12345)이 포함된 암호를 만들지 마십시오.<br>■ 단순 인터넷 검색으로 쉽게 검색 가능한 단어 또는 문자열이 포함된 암호를 만들지 마십시오.<br>■ 사용자가 동일한 암호를 여러 시스템에서 재사용하지 않도록 합니다.<br>■ 사용자가 이전 암호를 재사용하지 않도록 합니다. |
| **암호 관리 정책은 IT 보안 관리자에게 문의** | 회사의 암호 관리 요구 사항 및 정책이 충족되었는지 확인하려면 IT 보안 관리자에게 문의하십시오. |

# 원격 인증 서비스 및 보안 프로파일

Oracle ILOM은 각 Oracle ILOM 인터페이스에서 로컬 사용자를 구성하는 대신 외부의 중앙 사용자 저장소를 사용하도록 구성할 수 있습니다. 이 경우 사용자 자격 증명을 중앙에서 만들고 수정하며 여러 시스템에 사용자가 액세스할 수 있는 편의성이 추가됩니다.

인증 서비스를 선택하고 구성하기 전에 이러한 서비스가 어떻게 작동하고 각각 어떻게 구성해야 하는지 이해해야 합니다. 인증 이외에 지원되는 각 서비스는 Oracle ILOM 사용자 권한이 원격 사용자에 대해 어떻게 지정되는지 정의하는 권한 부여 규칙을 구성할 수 있는 기능도 제공합니다. 올바른 사용자 역할 또는 권한이 지정되도록 하십시오.

다음 표에서는 Oracle ILOM에서 지원하는 사용자 인증 서비스에 대해 설명합니다.

**표 8** 원격 인증 서비스 및 보안 프로파일

| 서비스 이름 | 보안 프로파일 | 정보 |
|---|---|---|
| Active Directory | 높음 | ■ 이 서비스는 기본적으로 안전합니다.<br>■ 엄격한 인증 모드를 사용하려면 인증 서버가 필요하지만 추가적인 보안 층이 제공됩니다. |
| LDAP/SSL(Lightweight Directory Access Protocol/Secure Socket Layer) | 높음 | ■ 이 서비스는 기본적으로 안전합니다.<br>■ 엄격한 인증 모드를 사용하려면 인증 서버가 필요하지만 추가적인 보안 층이 제공됩니다. |
| 레거시 LDAP | 낮음 | ■ 의심되는 악의적인 사용자가 없는 개인 보안 네트워크에서 이 서비스를 사용하십시오. |
| RADIUS(Remote Authentication Dial In User Service) | 낮음 | ■ 의심되는 악의적인 사용자가 없는 개인 보안 네트워크에서 이 서비스를 사용하십시오. |

높은 보안 프로파일의 서비스는 채널 보호를 위한 인증서 및 기타 형식의 강력한 암호화로 보호되므로 매우 안전한 환경에서 사용할 수 있습니다. 낮은 보안 프로파일의 서비스는 기본적으로 사용 안함으로 설정됩니다. 이 낮은 보안 레벨의 제한 사항을 이해하고 수락하는 경우에만 이러한 낮은 보안 프로파일을 사용으로 설정하십시오.

원격 인증 서비스 구성에 대한 자세한 내용은 아래의 해당 Oracle ILOM 설명서를 참조하십시오.

- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, 사용자 계정 설정 및 유지 관리
- Oracle ILOM 3.1 구성 및 유지 관리 설명서, 사용자 계정 설정 및 유지 관리
- *Oracle ILOM 3.0* 일상적인 관리 - *CLI* 절차 안내서, 사용자 계정 관리
- *Oracle ILOM 3.0* 일상적인 관리 - 웹 절차 안내서, 사용자 계정 관리

# 보안을 최대화하도록 사용자 액세스 구성

보안을 최대화하도록 Oracle ILOM 사용자 액세스를 가장 잘 구성하는 방법은 다음 항목을 참조하십시오.



Oracle ILOM에서 사용자 액세스 등록 정보는 CLI(명령줄 인터페이스) 또는 웹 인터페이스를 사용하여 구성할 수 있습니다. 이 절의 절차는 모든 Oracle ILOM 펌웨어 릴리스에 대한 웹 기반 탐색 지침을 제공합니다. CLI 지침 또는 구성 등록 정보에 대한 추가 세부 정보는 각 절차 뒤에 나오는 관련 정보 절에 나열된 해당 설명서를 참조하십시오.

## ▼ 처음 로그인할 때 root 계정에 대한 기본 암호 수정

처음 로그인할 때 Oracle ILOM에 액세스할 수 있도록 미리 정의된 관리자(root) 계정과 기본 암호(changme)가 시스템에 제공됩니다. Oracle ILOM에 대한 허용되지 않은 액세스를 방지하기 위해 미리 구성된 root 계정과 함께 제공되는 기본 암호(changeme)를 처음 로그인할 때 변경해야 합니다. 그렇지 않을 경우 미리 구성된 root 계정 및 기본 암호(changeme)가 공유 계정으로 사용되므로 모든 사용자가 관리자 액세스 권한을 갖게 됩니다.

미리 구성된 관리자 root 계정과 함께 제공되는 기본 암호(changeme)를 수정하려면 다음과 같은 웹 기반 지침을 따르십시오.

---

**참고** - 미리 구성된 root 계정에 액세스할 수 없는데 Oracle ILOM 관리자 기능에 액세스해야 하는 경우 시스템 관리자에게 관리자 권한이 있는 사용자 계정을 문의하십시오.

---

**시작하기 전에**

- "사용자 계정 및 암호 관리를 위한 보안 지침" [24]을 검토합니다.

---

**참고** - Oracle ILOM 기능에 대한 허용되지 않은 액세스를 방지하기 위해서는 강력한 보안 암호를 root 계정에 지정해야 합니다. 강력한 암호에는 소문자와 대문자 조합, 적어도 하나의 특수 문자(예: % 또는 $)가 포함되어야 합니다.

---

- Oracle ILOM에서 로컬 사용자 계정과 암호를 수정하려면 User Management(u) 역할이 필요합니다.

1. **Oracle ILOM 웹 인터페이스에서 User Account 페이지로 이동합니다.**

   예를 들면 다음과 같습니다.

   - **3.0.x 웹 인터페이스에서 User Management -> User Accounts를 누릅니다.**
   - **3.1 이상 웹 인터페이스에서 User Management -> User Accounts를 누릅니다.**

2. **User Account 페이지에서 `root` 계정에 대해 Edit를 누릅니다.**

   Edit: User Root 대화 상자가 나타납니다.

3. **Edit: User Root 대화 상자에서 다음을 수행합니다.**

   - **New Password 텍스트 상자에 고유한 암호를 입력한 다음 Confirm New Password 텍스트 상자에 같은 암호를 다시 입력합니다.**
   - **Save를 눌러 변경 내용을 적용합니다.**

**관련 정보**

- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, 로컬 사용자 계정 구성
- *Oracle ILOM 3.1* 구성 및 유지 관리 설명서, 로컬 사용자 계정 구성
- *Oracle ILOM 3.0* 일상적인 관리 - *CLI* 절차 안내서, 사용자 계정 수정
- *Oracle ILOM 3.0* 일상적인 관리 - 웹 절차 안내서, 사용자 계정 수정
- “`root` 계정 기본 암호를 재설정하기 위한 물리적 보안 존재” [56]

## ▼ 역할 기반 권한을 가진 로컬 사용자 계정 만들기

**시작하기 전에**

Oracle ILOM은 한 개의 SP 또는 CMM(섀시 모니터링 모듈)에 최대 10개의 로컬 사용자 계정을 만들고 저장하는 것을 지원합니다. Oracle ILOM 사용자에게는 구성된 계정에서 허용하는 한도에 따라 기능을 사용할 수 있도록 해주는 일련의 권한이 지정됩니다.

---

**참고** - 또는 원격 인증 서비스를 통해 추가 사용자 계정을 지원하도록 시스템 관리자가 Oracle ILOM을 구성할 수 있습니다. 원격 인증 서비스 구성을 사용할 경우 로그인, 암호 및 권한이 외부 사용자 저장소에서 파생됩니다. 자세한 내용은 “원격 인증 서비스 및 보안 프로파일” [26]을 참조하십시오.

---

역할 기반 액세스 권한을 가진 로컬 사용자 계정 구성에 대한 웹 기반 지침은 다음을 참조하십시오.

**시작하기 전에**

- "사용자 계정 및 암호 관리를 위한 보안 지침" [24]을 검토합니다.
- 표 7. "사용자 계정 권한 설명"을 검토합니다.
- 권한을 가진 로컬 사용자 계정을 만들려면 Oracle ILOM에서 User Management(u) 역할이 필요합니다.

1. **Oracle ILOM 웹 인터페이스에서 User Account 페이지로 이동합니다.**

   예를 들면 다음과 같습니다.

   - **3.0.x 웹 인터페이스에서 User Management -> User Accounts를 누릅니다.**
   - **3.1 이상 웹 인터페이스에서 User Management -> User Accounts를 누릅니다.**

2. **User Account 페이지에서 Add를 누릅니다.**

   Add User 대화 상자가 나타납니다.

3. **Add User 대화 상자에서 다음을 수행합니다.**

   a. **User Name 텍스트 상자에 사용자 이름을 지정합니다.**

   b. **Roles 드롭다운 목록에서 적합한 사용자 프로파일(administrator, operator 또는 advanced)을 선택합니다.**

   c. **New Password 텍스트 상자에 고유한 암호를 입력한 다음 Confirm New Password 텍스트 상자에 같은 암호를 다시 입력합니다.**

   d. **Save를 눌러 변경 내용을 적용합니다.**

**관련 정보**

- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, 사용자 계정 만들기 및 사용자 역할 지정
- *Oracle ILOM 3.1* 구성 및 유지 관리 설명서, 사용자 계정 만들기 및 사용자 역할 지정
- *Oracle ILOM 3.0* 일상적인 관리 - *CLI* 절차 안내서, 사용자 계정 추가 및 역할 지정
- *Oracle ILOM 3.0* 일상적인 관리 - 웹 절차 안내서, 사용자 계정 추가 및 역할 지정

## ▼ KVMS 세션 종료 시 호스트 액세스 잠금

원격 KVMS를 사용할 때 호스트 콘솔은 공유 네트워크 리소스로 간주되므로 한 사용자가 호스트 콘솔에 로그인하고 호스트 운영 체제에서 로그아웃하지 않은 상태로 Oracle ILOM Remote System Console, Remote System Console Plus 또는 Storage Redirection CLI

응용 프로그램을 닫을 경우 원격 KVMS를 사용하여 동일 콘솔에 연결하는 두번째 사용자는 이전에 인증된 운영 체제 세션을 사용할 수 있습니다. 이러한 이유로 Oracle ILOM은 원격 KVMS 세션의 연결이 해제될 때마다 호스트 운영 체제를 자동으로 잠그는 기능을 제공합니다. 최대 보안을 위해서는 Oracle ILOM에서 이 기능을 사용으로 설정하거나 구성하십시오.

KVMS 세션을 종료한 후 원격 호스트 데스크탑을 잠그려면 다음과 같은 웹 기반 지침을 참조하십시오. 호스트 잠금 기능을 사용으로 설정하는 방법은 *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*를 참조하십시오.

**시작하기 전에**

- Oracle ILOM에서 호스트 잠금 모드 등록 정보를 수정하려면 Console(c) 역할이 필요합니다.
- Oracle ILOM에서 호스트 잠금 모드 기능을 사용하려면 펌웨어 3.0.4 이상이 필요합니다.
- 호스트 잠금 모드 기능은 기본적으로 사용 안함으로 설정됩니다.

1. **Oracle ILOM 웹 인터페이스에서 KVMS 페이지로 이동합니다.**

   예를 들면 다음과 같습니다.

   - **3.0.x 웹 인터페이스에서 Remote Console -> KVMS를 누릅니다.**
   - **3.1 이상 웹 인터페이스에서 Remote Control -> KVMS를 누릅니다.**

2. **KVMS 페이지의 Host Lock Settings 섹션에서 다음 작업 중 하나를 수행합니다.**

   - **잠금 모드(Windows, Custom 또는 Disabled)를 지정합니다.**
   - **Save를 눌러 변경 내용을 적용합니다.**

**관련 정보**

- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, 호스트 데스크탑 잠금
- *Oracle ILOM 3.1* 구성 및 유지 관리 설명서, 호스트 데스크탑 잠금
- *Oracle ILOM 3.0* 원격 리디렉션 콘솔 *CLI* 및 웹 안내서, KVMS 잠금

## ▼ Remote System Console Plus의 표시 가능 KVMS 세션 제한(3.2.4 이상)

**시작하기 전에**

펌웨어 릴리스 3.2.4부터 Remote System Console Plus 기본 사용자의 경우 Maximum Client Session Count를 1개의 세션 뷰어로 제한하여 비디오 재지정 세션 중에 입력된 기밀 데이터를 SP의 로그인한 다른 세션 사용자가 보지 못하도록 설정할 수 있습니다. 기본적으로

Oracle ILOM Remote System Console Plus의 Maximum Client Session Count 등록 정보는 4개의 세션 뷰어로 설정됩니다.

Oracle ILOM Remote System Console Plus의 Maximum Client Session Count 등록 정보를 수정하려면 다음과 같은 웹 기반 지침을 참조하십시오.

**시작하기 전에**

- Oracle ILOM Remote System Console Plus의 KVMS Maximum Client Session Count 등록 정보는 펌웨어 릴리스 3.2.4 이상부터 사용 가능합니다.

---

**참고** - Oracle ILOM Remote Console을 지원하는 시스템에서는 KVMS Maximum Client Session Count 등록 정보를 구성할 수 없습니다.

---

- Oracle ILOM Remote System Console Plus는 펌웨어 릴리스 3.2.1부터 새로 릴리스된 SP 시스템에서만 사용 가능합니다.
- KVMS Maximum Client Session Count 등록 정보를 수정하려면 Oracle ILOM에서 Console(c) 역할이 필요합니다.
- Oracle ILOM에서 Maximum Client Session Count 등록 정보를 재설정할 경우 SP의 활성 Oracle ILOM Remote System Console Plus 비디오 세션이 모두 종료됩니다.
- 기본적으로 SP당 최대 4개의 System Console Plus 비디오 재지정 세션을 Oracle ILOM의 Redirection 페이지에서 실행할 수 있습니다.

1. **Oracle ILOM 웹 인터페이스에서 Remote Console -> KVMS를 눌러 KVMS 페이지로 이동합니다.**
2. **KVMS 페이지에서 Maximum Client Session Count 등록 정보를 수정합니다(허용되는 값: *4*(기본값)|*1*|*2*|*3*).**
3. **Save를 눌러 변경 내용을 적용합니다.**

**관련 정보**

- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, 원격 장치 재지정 등록 정보

## ▼ 로그인 배너로 시스템 액세스 보안 설정(3.0.8 이상)

**시작하기 전에**

펌웨어 릴리스 3.0.8부터 Oracle ILOM에서 시스템 관리자는 Oracle ILOM CLI 및 웹 인터페이스에 로그인할 때 모든 사용자에게 배너 메시지를 표시할 수 있습니다. 로그인 배너를 사용할 경우 원격 장치에 의한 허용되지 않은 시스템 액세스로부터 보호하고, 허용되는 시스템 사용과 관련한 의무사항을 인증된 합법적인 사용자에게 숙지시킬 수 있습니다.

구현하는 배너 메시지는 정보 보안 정책에 따라 작성되어야 합니다. 작성 메시지에 대한 자세한 지침은 사이트 관리자 또는 보안 관리자에게 문의하십시오.

로그인 시 모든 사용자에게 배너 메시지를 표시하려면 다음과 같은 웹 기반 지침을 참조하십시오.

**시작하기 전에**

- 배너 메시지를 만들려면 Admin(a) 역할이 필요합니다.
- 배너 메시지는 Oracle ILOM 펌웨어 릴리스 3.0.8 이상의 구성에 사용할 수 있습니다.
- 관리자는 로그인 페이지 또는 사용자가 Oracle ILOM에 로그인한 직후에 나타나는 대화 상자에 배너 메시지를 표시하도록 구성할 수 있습니다.

1. **Oracle ILOM 웹 인터페이스에서 Banner Message 페이지로 이동합니다.**

   예를 들면 다음과 같습니다.

   - **3.0.x 웹 인터페이스에서 System Information -> Banner Messages를 누릅니다.**
   - **3.1 이상 웹 인터페이스에서 ILOM Administration -> Management Access -> Banner Messages를 누릅니다.**

2. **Banner Message 페이지에서 다음을 수행합니다.**

   a. **로그인 페이지에 메시지가 나타나도록 하려면 Connect Message 텍스트 상자에 메시지를 입력합니다. 그렇지 않고 사용자가 로그인한 후에 메시지가 대화 상자에 나타나도록 하려면 Login Message 텍스트 상자에 메시지를 입력합니다.**

   b. **Login Message Acceptance 확인란을 선택하여 메시지를 표시합니다. 그렇지 않은 경우 Login Message Acceptance 확인란을 선택 해제하여 메시지가 표시되지 않도록 합니다.**

   c. **Save를 눌러 변경 내용을 적용합니다.**

### 관련 정보

- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, 배너 메시지 구성 등록 정보
- *Oracle ILOM 3.1* 구성 및 유지 관리 설명서, 배너 메시지 구성 등록 정보
- *Oracle ILOM 3.0* 일상적인 관리 - *CLI* 절차 안내서, 배너 메시지 표시
- *Oracle ILOM 3.0* 일상적인 관리 - 웹 절차 안내서, 배너 메시지 표시

# 보안을 최대화하도록 Oracle ILOM 인터페이스 구성

보안을 최대화하도록 Oracle ILOM 인터페이스를 구성하려면 다음 항목을 참조하십시오.



## 보안을 최대화하도록 웹 인터페이스 구성

보안을 최대화하도록 Oracle ILOM 웹 인터페이스를 가장 잘 구성하는 방법은 다음 항목을 참조하십시오.

---

**참고** - Oracle ILOM에서 웹 관리 인터페이스 등록 정보는 CLI(명령줄 인터페이스) 또는 웹 인터페이스를 사용하여 구성할 수 있습니다. 이 절의 절차는 모든 Oracle ILOM 펌웨어 릴리스에 대한 웹 기반 탐색 지침을 제공합니다. CLI 지침 또는 구성 등록 정보에 대한 추가 세부 정보는 각 절차 뒤에 나오는 관련 정보 절에 나열된 해당 설명서를 참조하십시오.

---



### 신뢰할 수 있는 SSL 인증서 및 개인 키를 사용하여 보안 향상

SSL(Secure Socket Layer) 인증서는 네트워크를 통한 통신을 암호화하고 서버나 클라이언트의 신뢰성을 확인하는 데 사용됩니다. Oracle ILOM에는 인증서를 업로드할 필요 없이 HTTP over SSL 프로토콜을 바로 사용할 수 있도록 자체 서명된 SSL 인증서가 포함되어 있습니다. Oracle ILOM 웹 인터페이스에 처음으로 연결할 때 사용자에게 자체 서명된 인증서가 사용될 것임을 통지하고 사용을 수락할지 물어봅니다. 제공된 인증서를 사용하면 웹 브라우저와 Oracle ILOM 사이의 모든 통신이 완전히 암호화됩니다.

하지만 보안 향상을 위해 신뢰할 수 있는 인증서를 만들어 업로드할 수도 있습니다. 신뢰할 수 있는 인증서란 인증서가 신뢰할 수 있는 인증 기관에서 부여되었음을 의미합니다. 알려진 인증 기관의 신뢰할 수 있는 인증서를 사용하면 Oracle ILOM 웹 서버의 신뢰성이 보장됩니다. 신뢰할 수 없는(자체 서명된) 인증서를 사용하면 MITM(man-in-the-middle) 공격 가능성이 있습니다.

임시 자체 서명 인증서 또는 인증 기관 서명 인증서를 가져와서 업로드하려면 다음 절차를 참조하십시오.

## ▼ OpenSSL을 사용하여 SSL 인증서 및 개인 키 얻기

이 절차는 OpenSSL 툴킷을 사용하여 SSL 인증서 및 개인 키를 만드는 방법에 대해 간략히 설명합니다.

---

**참고** - Oracle ILOM에서는 OpenSSL을 사용하여 SSL 인증서를 생성할 필요가 없습니다. OpenSSL은 데모용으로 이 절차에 사용되었습니다. SSL 인증서를 생성하는 데 다른 도구를 사용할 수 있습니다.

---

임시 자체 서명 인증서 또는 인증 기관 서명 인증서를 사용하기 위한 요구 사항은 사이트 관리자 또는 보안 관리자가 결정해야 합니다. SSL 인증서(임시 자체 서명 인증서 또는 인증 기관 서명 인증서)를 가져와야 하는 경우 아래의 OpenSSL 명령줄 지침 예를 따르십시오.

---

**참고** - SSL 인증서를 생성하는 데 추가 OpenSSL 지침이 필요한 경우 OpenSSL 툴킷과 함께 제공되는 사용자 설명서를 참조해야 합니다.

---

1. **인증서와 개인 키를 저장할 네트워크 공유 또는 로컬 디렉토리를 만듭니다.**

2. **OpenSSL 툴킷을 사용하여 RSA 개인 키를 새로 생성하려면 다음과 같이 입력합니다.**

   ```
   openssl genrsa -out <foo>.key 2048
   ```

   여기서 *<foo>*는 개인 키의 이름입니다.

   ---

   **참고** - 이 개인 키는 2048비트 RSA 키이며, ASCII 텍스트로 읽을 수 있도록 PEM 형식으로 저장됩니다.

   ---

3. **OpenSSL 툴킷을 사용하여 CSR(인증서 서명 요청)을 새로 생성하려면 다음과 같이 입력합니다.**

   ```
   openssl req -new -key <foo>.key -out <foo>.csr
   ```

   여기서 *<foo>*는 인증서 서명 요청의 이름입니다.

   ---

   **참고** - CSR 생성 중 몇 가지 정보를 입력하라는 프롬프트가 표시됩니다.

   ---

현재 작업 디렉토리에 *<foo>*.csr 파일이 표시되어야 합니다.

4. **SSL 인증서를 생성하려면 다음 중 하나를 수행합니다.**

   - **임시 자체 서명 인증서(365일 동안 유효) 생성**

     자체 서명 SSL 인증서는 server.key 개인 키와 server.csr 파일에서 생성됩니다.

     OpenSSL 툴킷을 사용하여 다음과 같이 입력합니다.

     ```
     openssl x509 -req -days 365 -in <foo>.csr
     -signkey <foo>.key -out <foo>.cert
     ```

     여기서 *<foo>*는 개인 키(.key) 또는 인증서(.cert)에 지정된 이름입니다.

---

**참고** - 이 임시 인증서를 사용할 경우 서명 인증 기관을 알 수 없어서 신뢰할 수 없다는 내용의 오류가 클라이언트 브라우저에 표시됩니다. 이 오류를 허용할 수 없는 경우 서명된 인증서를 발행해 줄 것을 인증 기관에 요청해야 합니다.

---

   - **인증 기관 공급자의 공식 서명이 있는 인증서 얻기**

     인증서 서명 요청(*<foo>*.csr)을 SSL 인증 기관 공급자에게 제출합니다. 대부분의 인증 기관 공급자는 웹 응용 프로그램 화면에서 CSR 출력을 잘라내어 붙여 넣을 것을 요청합니다. 서명된 인증서를 받는 데 보통 최대 7일(영업일)이 걸릴 수 있습니다.

5. **새 SSL 인증서와 개인 키를 Oracle ILOM에 업로드합니다.**

   Oracle ILOM에 사용자 정의 SSL 인증서 및 개인 키 업로드 [35] 지침을 참조하십시오.

## ▼ Oracle ILOM에 사용자 정의 SSL 인증서 및 개인 키 업로드

**시작하기 전에**

- Oracle ILOM에서 웹 서버 등록 정보를 수정하려면 Admin(a) 역할이 필요합니다.
- 새 (임시 자체 서명 또는 인증 기관 서명) HTTPS 인증서 및 개인 키를 얻습니다. OpenSSL 툴킷 사용 지침은 OpenSSL을 사용하여 SSL 인증서 및 개인 키 얻기 [34]를 참조하십시오.
- 네트워크 또는 로컬 파일 시스템을 통해 새 HTTPS 인증서 및 개인 키에 액세스할 수 있는지 확인합니다.

1. **Oracle ILOM 웹 인터페이스에서 SSL Certificate 페이지로 이동합니다.**

   예를 들면 다음과 같습니다.

- **3.0.x 웹 인터페이스에서 Configuration -> System Management Access -> SSL Certificate를 누릅니다.**
- **3.1 이상 웹 인터페이스에서 ILOM Administration -> Management Access -> SSL Certificate를 누릅니다.**

2. **SSL server 페이지에서 다음을 수행합니다.**

   a. **Load Certificate 버튼을 눌러 File Transfer Method 등록 정보에 지정된 사용자 정의 인증서 파일을 업로드합니다.**

   b. **Load Custom Private Key 버튼을 눌러 File Transfer Method 등록 정보에 지정된 사용자 정의 개인 키 파일을 업로드합니다.**

   c. **Save를 눌러 변경 내용을 적용합니다.**

**관련 정보**

- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, SSL 인증서 및 개인 키 구성 등록 정보
- *Oracle ILOM 3.1* 구성 및 유지 관리 설명서, SSL 인증서 및 개인 키 구성 등록 정보
- *Oracle ILOM 3.0* 일상적인 관리 - *CLI* 절차 안내서, SSL 인증서 업로드
- *Oracle ILOM 3.0* 일상적인 관리 - 웹 절차 안내서, SSL 인증서 업로드

## ▼ 가장 강력한 SSL 및 TLS 암호화 등록 정보 사용

기본적으로 Oracle ILOM에서는 가장 강력한 암호화를 사용하는 가장 강력한 Secure Socket Layer 암호화(SSLv3 및 TLS v1.0, v1.1, v1.2) 프로토콜만 사용할 수 있습니다. 그러나 경우에 따라 이전 웹 브라우저 사용을 지원하기 위해 SSLv2 또는 이보다 약한 암호화를 사용해야 할 수 있습니다.

---

**참고** - SSL 및 TLSv1.0은 펌웨어 릴리스 3.1.0부터 지원됩니다. TLS v1.1 및 v1.2는 펌웨어 릴리스 3.2.4부터 Oracle ILOM에서 지원됩니다.

---

가능하다면 웹 인터페이스는 시스템과 함께 제공되는 기본 웹 서버 보안 설정으로 구성해야 합니다. Oracle ILOM에서 웹 서버 보안 등록 정보를 보거나 수정하려면 다음과 같은 웹 기반 지침을 참조하십시오.

**시작하기 전에**

- Oracle ILOM에서 웹 서버 등록 정보를 수정하려면 Admin(a) 역할이 필요합니다.
- SSLv3 및 TLS v1.0은 기본적으로 펌웨어 릴리스 3.1.x, 3.2.1, 3.2.2 및 3.2.3을 실행하는 서버 SP에서 지원되며 사용으로 설정됩니다.
- SSLv3 및 TLS v1.0, v1.1, v1.2는 기본적으로 펌웨어 릴리스3.2.4 이상을 실행하는 서버 SP에서 지원되며 사용으로 설정됩니다.
- SSLv2 및 약한 암호화에 대한 등록 정보는 기본적으로 사용 안함으로 설정됩니다.

1. **Oracle ILOM 웹 인터페이스에서 ILOM Administration -> Management Access -> Web Server를 누릅니다.**
2. **Web Server 페이지에서 SSL, TLS 또는 약한 암호화에 대한 웹 보안 등록 정보를 확인하거나 수정합니다.**
3. **Save를 눌러 변경 내용을 적용합니다.**

**관련 정보**

- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, 웹 서버 구성 등록 정보
- *Oracle ILOM 3.1* 구성 및 유지 관리 설명서, 웹 서버 구성 등록 정보

## ▼ 활성 웹 세션에 대한 시간 초과 간격 설정

Oracle ILOM 웹 세션 시간 초과 간격은 깜박 잊고 로그아웃하지 않은 웹 액세스 사용자에게 보안을 제공합니다. 웹 세션 시간 초과 간격은 비활성 HTTP 또는 HTTPS 웹 세션이 자동으로 로그아웃되기 전 경과해야 하는 시간(분)을 지정합니다. 이 기능을 사용할 경우 인증되지 않은 사용자가 Oracle ILOM에 대해 인증된 웹 세션을 유지하고 있는 방치된 컴퓨터를 찾을 수 있는 위험이 줄어듭니다.

HTTP 및 HTTPS 세션에 대해 설정된 웹 세션 시간 초과 간격을 확인하거나 수정하려면 다음과 같은 웹 기반 지침을 참조하십시오.

**시작하기 전에**

- HTTP 및 HTTPS 연결에 대해 설정된 기본 웹 세션 시간 초과 간격은 15분입니다.

---

**참고** - 세션 시간 초과를 낮추면 세션이 그만큼 빨리 만료되므로 사용자가 자신의 사용자 이름과 암호를 더 자주 다시 입력해야 합니다. 반면, 세션 시간 초과를 낮추면 방치 상태의 인증된 웹 세션이 활성 상태로 유지되는 기간이 짧아집니다.

---

- 웹 서버 등록 정보를 수정하려면 Admin(a) 역할이 필요합니다.

- HTTP 및 HTTPS 세션 시간 초과 간격 등록 정보는 Oracle ILOM의 펌웨어 릴리스 3.0.4 이상을 실행하는 서버 SP에서만 구성할 수 있습니다.

1. **Web Server 페이지로 이동합니다.**

   예를 들면 다음과 같습니다.

   - **3.0.x 웹 인터페이스에서 Configuration -> System Management Access -> Web Server를 누릅니다.**
   - **3.1 이상 웹 인터페이스에서 ILOM Administration -> Management Access -> Web Server를 누릅니다.**

2. **Web Server 페이지에서 다음을 수행합니다.**

   a. **HTTP 또는 HTTP Session Timeout 등록 정보로 이동합니다.**

   b. **1-720분 범위의 숫자를 입력하여 비활성 웹 세션이 자동으로 로그아웃되기 전 경과해야 하는 시간(분)을 지정합니다.**

   c. **Save를 눌러 변경 내용을 적용합니다.**

### 관련 정보

- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, 웹 서버 구성 등록 정보
- *Oracle ILOM 3.1* 구성 및 유지 관리 설명서, 웹 서버 구성 등록 정보
- *Oracle ILOM 3.0* 일상적인 관리 - 웹 절차 안내서, 세션 시간 초과 설정

# 보안을 최대화하도록 CLI 구성

보안을 최대화하도록 Oracle ILOM CLI(명령줄 인터페이스)를 가장 잘 구성하는 방법은 다음 항목을 참조하십시오.


- 비활성 CLI 세션에 대한 시간 초과 간격 설정 [39]
- 서버측 키를 사용하여 SSH 연결 암호화 [40]
- 자동 CLI 인증을 위해 사용자 계정에 SSH 키 추가 [41]


Oracle ILOM에서 CLI 관리 등록 정보는 CLI(명령줄 인터페이스) 또는 웹 인터페이스를 사용하여 구성할 수 있습니다. 이 절의 절차는 모든 Oracle ILOM 펌웨어 릴리스에 대한 웹 기반 탐색 지침을 제공합니다. CLI 지침 또는 구성 등록 정보에 대한 추가 세부 정보는 각 절차 뒤에 나오는 관련 정보 절에 나열된 해당 설명서를 참조하십시오.

## ▼ 비활성 CLI 세션에 대한 시간 초과 간격 설정

SSH(Secure Shell) 프로토콜을 통해 Oracle ILOM에 연결하거나 직렬 연결을 사용하여 액세스되는 Oracle ILOM CLI는 비활성 CLI 세션을 닫을 수 있는 구성 가능한 세션 시간 초과 간격을 지원합니다. 이 기능을 구성할 경우 인증되지 않은 사용자가 Oracle ILOM에 대해 인증된 CLI 세션을 유지하고 있는 방치된 컴퓨터를 찾을 수 있는 위험이 줄어듭니다.

보안을 최대화하기 위해서는 Oracle ILOM CLI가 공유 콘솔에 사용되는 환경에서 CLI 세션 시간 초과 간격을 구성해야 합니다. CLI 세션 시간 초과 간격은 15분 이하로 설정하는 것이 이상적입니다.

비활성 Oracle ILOM CLI 세션에 대해 설정된 시간 초과 간격 등록 정보를 확인하거나 수정하려면 다음과 같은 웹 기반 지침을 참조하십시오.

시작하기 전에 **시작하기 전에**

- CLI 등록 정보를 수정하려면 Admin(a) 역할이 필요합니다.
- SSH 연결에 대해 설정된 기본 CLI 세션 시간 초과 간격은 사용 안함으로 설정되어 0분으로 설정됩니다.

---

**참고** - CLI 시간 초과 간격이 0으로 설정된 경우 세션이 유휴 상태로 남아 있는 시간에 관계없이 Oracle ILOM에서 비활성 CLI 세션을 닫지 않습니다.

---

- CLI 세션 시간 초과 간격 등록 정보는 Oracle ILOM의 펌웨어 릴리스 3.0.4 이상을 실행하는 서버 SP에서만 구성할 수 있습니다.

1. **Oracle ILOM 웹 인터페이스에서 CLI 페이지로 이동합니다.**

   예를 들면 다음과 같습니다.

   - **3.0.x 웹 인터페이스에서 Configuration -> System Management Access -> CLI를 누릅니다.**
   - **3.1 이상 웹 인터페이스에서 ILOM Administration -> Management Access -> CLI를 누릅니다.**

2. **CLI 페이지에서 다음을 수행하여 CLI 세션 시간 초과 간격을 설정합니다.**

   a. **Enable 확인란을 선택합니다.**

   b. **1-1440분 범위의 숫자를 입력하여 비활성 명령줄 세션이 자동으로 로그아웃되기 전 경과해야 하는 시간(분)을 지정합니다.**

   c. **Save를 눌러 변경 내용을 적용합니다.**

### 관련 정보

- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, CLI 세션 시간 초과 구성 등록 정보
- *Oracle ILOM 3.1* 구성 및 유지 관리 설명서, CLI 세션 시간 초과 구성 등록 정보
- *Oracle ILOM 3.0* 일상적인 관리 - *CLI* 절차 안내서, CLI 세션 시간 초과 설정

## ▼ 서버측 키를 사용하여 SSH 연결 암호화

Oracle ILOM은 원격 클라이언트가 명령줄 인터페이스를 통해 Oracle ILOM에 안전하게 연결하여 관리할 수 있도록 SSH(Secure Shell) 서버 기능을 제공합니다. SSH 프로토콜은 서버측 키를 사용하여 관리 채널을 암호화하고 모든 통신을 보호합니다. 또한 SSH 클라이언트는 이러한 키를 사용하여 SSH 서버의 신뢰성을 확인합니다.

Oracle ILOM은 출하 시의 기본 시스템을 처음 부트할 때 일련의 고유한 SSH 키를 생성합니다. 새로운 서버측 키가 필요할 경우 Oracle ILOM은 추가 SSH 서버측 키를 수동으로 생성하는 기능을 지원합니다.

SSH 서버측 암호화 키를 확인하거나 수동으로 생성하려면 다음과 같은 웹 기반 지침은 참조하십시오.

### 시작하기 전에

- SSH 서버 등록 정보를 수정하려면 Admin(a) 역할이 필요합니다.

1. **Oracle ILOM 웹 인터페이스에서 SSH Server 페이지로 이동합니다.**

   예를 들면 다음과 같습니다.

   - **3.0.x 웹 인터페이스에서 System Management -> SSH Server를 누릅니다.**
   - **3.1 이상 웹 인터페이스에서 ILOM Administration -> Management Access-> SSH Server를 누릅니다.**

2. **SSH Server 페이지에서 생성된 RSA 및 DSA 키 정보를 검토하거나 다음을 수행합니다.**

   a. **Generate RSA Key를 눌러 새 키를 생성합니다.**

   b. **Generate DSA Key를 눌러 새 키를 생성합니다.**

### 관련 정보

- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, SSH 서버 구성 등록 정보

- *Oracle ILOM 3.1* 구성 및 유지 관리 설명서, SSH 서버 구성 등록 정보
- *Oracle ILOM 3.0* 일상적인 관리 - 웹 절차 안내서, 새 SSH 키 생성
- *Oracle ILOM 3.0* 일상적인 관리 - *CLI* 절차 안내서, 새 SSH 키 생성

## ▼ 자동 CLI 인증을 위해 사용자 계정에 SSH 키 추가

생성된 사용자 정의 SSH 키 쌍(DSA 또는 RSA)을 개별 사용자 계정에 사용할 수 있습니다. 이때 공개 키는 Oracle ILOM에 업로드됩니다. 이 기능은 수동 개입 없이 실행되는, 일반 텍스트 암호가 포함되어 있지 않은 스크립트를 사용하는 경우에 유용합니다. 사용자는 네트워크 기반 SSH 연결을 통해 원격 시스템에서 서비스 프로세서 명령을 자동 또는 정기적으로 실행하는 스크립트를 작성할 수 있습니다.

생성된 공개 SSH 키와 함께 Oracle ILOM 계정을 업로드하고 추가하려면 다음과 같은 웹 기반 지침을 참조하십시오.

**시작하기 전에**

- SSH 연결 도구(예: ssh-keygen)를 사용하여 개인 및 공개 SSH 키를 생성한 다음 생성된 SSH 키 파일을 원격 SSH 시스템에 저장합니다.
- SSH 공개 키를 다른 사용자 계정에 추가하려면 User Management(u) 역할이 필요합니다.
- SSH 공개 키를 자신의 사용자 계정에 추가하려면 Read Only(o) 역할이 필요합니다.

1. **Oracle ILOM 웹 인터페이스에서 User Account 페이지로 이동합니다.**

   예를 들면 다음과 같습니다.

   - **3.0.x 웹 인터페이스에서 User Management -> User Accounts를 누릅니다.**
   - **3.1 이상 웹 인터페이스에서 ILOM Administration -> User Management -> User Accounts를 누릅니다.**

2. **User Account 페이지에서 다음을 수행합니다.**

   a. **SSH Keys 섹션을 아래로 스크롤한 다음 Add를 누릅니다.**

   b. **User 목록에서 사용자 계정을 선택합니다.**

   c. **목록에서 전송 방법을 선택한 다음 공개 SSH 키를 업로드하는 데 필요한 전송 방법 등록 정보를 지정합니다.**

3. **Load를 눌러 공개 SSH 키를 업로드하고 선택한 사용자 계정에 추가합니다.**

### 관련 정보

- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, 로컬 SSH 키를 사용하는 CLI 인증
- *Oracle ILOM 3.1* 구성 및 유지 관리 설명서, 로컬 SSH 키를 사용하는 CLI 인증
- *Oracle ILOM 3.0* 일상적인 관리 - 웹 절차 안내서, 사용자 계정 관리
- *Oracle ILOM 3.0* 일상적인 관리 - *CLI* 절차 안내서, 사용자 계정 관리

# 보안을 최대화하도록 SNMP 관리 액세스 구성

SNMP는 시스템을 모니터링하거나 관리하는 데 사용되는 표준 프로토콜입니다. Oracle ILOM은 모니터링과 관리 모두를 위한 SNMP 솔루션을 제공하지만 사용하기 전에 구성이 필요합니다. 이 서비스를 구성하기 전에 다양한 SNMP 사용자 구성 가능 옵션의 보안 영향을 이해하는 것이 중요합니다. 자세한 내용은 다음 정보를 참조하십시오.


- SNMPv3 암호화 및 사용자 인증 사용 [42]
- “구성 가능한 객체를 지원하는 Sun SNMP MIB” [43]


## ▼ SNMPv3 암호화 및 사용자 인증 사용

SNMPv1 및 SNMPv2c는 암호화를 제공하지 않으며 커뮤니티 문자열을 인증 형식으로 사용합니다. 커뮤니티 문자열은 네트워크를 통해 일반 텍스트로 전송되며 대개 개별 사용자가 전용으로 사용하는 것이 아니라 여러 사용자 간에 공유됩니다. 반면 SNMPv3는 암호화를 사용하여 보안 채널을 제공하며 개별 사용자 이름과 암호를 사용합니다. SNMPv3 사용자 암호는 지역화되므로 관리 스테이션에 안전하게 저장할 수 있습니다.

SNMPv1, SNMPv2c 및 SNMPv3는 모두 Oracle ILOM에서 지원되며 개별적으로 사용 또는 사용 안함으로 설정할 수 있습니다. 또한 “sets”를 사용 또는 사용 안함으로 설정하여 추가적인 보안 층을 제공할 수 있습니다. 이 구성 가능한 옵션에 따라 SNMP 서비스에서 구성 가능한 SNMP MIB 등록 정보를 설정할 수 있는지 여부가 결정됩니다. sets를 효과적으로 사용 안함으로 설정하면 SNMP 서비스를 모니터링용으로만 유용하게 만들 수 있습니다.

기본적으로 SNMPv1 및 SNMPv2c는 사용 안함으로 설정됩니다. SNMPv3는 기본적으로 사용으로 설정되지만 사용하기 전에 하나 이상의 SNMP 사용자를 만들어야 합니다. 사전 구성된 SNMPv3 사용자는 없습니다.

Oracle ILOM에서 SNMP 관리를 구성하려면 다음과 같은 웹 기반 지침을 참조하십시오.

### 시작하기 전에

- 최대 SNMP 보안을 위해서는 SNMPv1 및 SNMPv2c를 모니터링용으로만 사용하고 이러한 보안이 약한 프로토콜이 사용으로 설정될 경우 “sets”를 사용으로 설정하지 마십시오.

- SNMP sets는 SNMPv3 관리에 대해서만 사용으로 설정해야 합니다. SNMP Set 등록 정보는 기본적으로 사용 안함으로 설정됩니다.
- SNMPv3 sets를 사용하려면 SNMPv3 사용자 계정을 구성해야 합니다. 미리 구성된 SNMPv3 사용자 계정은 제공되지 않습니다.
- SNMP 서비스의 State 등록 정보는 기본적으로 사용으로 설정됩니다.
- SNMP 등록 정보를 수정하려면 Admin role(a) 권한이 필요합니다.
- SNMPv3 사용자 계정을 추가하거나 수정하려면 User management(u) 권한이 필요합니다.

1. **Oracle ILOM 웹 인터페이스에서 SNMP 페이지로 이동합니다.**

   예를 들면 다음과 같습니다.

   - **3.0.x 웹 인터페이스에서 System Management Access -> SNMP를 누릅니다.**
   - **3.1 이상 웹 인터페이스에서 ILOM Administration -> Management Access -> SNMP를 누릅니다.**

2. **SNMP 페이지에서 SNMP 등록 정보를 확인하거나 수정한 다음 Save를 눌러 변경 내용을 적용합니다.**

   추가 지침은 이 절차의 관련 정보 절에 나열된 설명서를 참조하십시오. 펌웨어 버전 3.2 이상을 실행하는 사용자의 경우 SNMP 페이지의 `More details` 링크를 누르면 추가 정보를 볼 수 있습니다.

### 관련 정보

- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, SNMP 설정 구성
- *SNMP* 및 *IPMI*에 대한 *Oracle ILOM* 프로토콜 관리 참조*(*펌웨어 *3.2.x)*, SNMP 설정 구성
- *Oracle ILOM 3.1 SNMP, IPMI, CIM, WS-Man* 프로토콜 관리 참조 설명서, SNMP 설정 구성
- *Oracle ILOM 3.0 SNMP, IPMI, CIM, WS-Man* 프로토콜 관리 참조 설명서, SNMP 설정 구성

## 구성 가능한 객체를 지원하는 Sun SNMP MIB

구성 가능한 객체를 지원하며 "sets"를 적용할 수 있는 Oracle Sun MIB는 다음과 같습니다.

- `SUN-HW-CTRL-MIB` - 이 MIB는 하드웨어 정책(예: 전원 관리)을 구성하는 데 사용됩니다.
- `SUN-ILOM-CONTROL-MIB` - 이 MIB는 Oracle ILOM 기능(예: 사용자 만들기 및 서비스 구성)을 구성하는 데 사용됩니다.

**참고** - 1) MIB 객체가 수정을 지원하고, 2) MIB 객체의 `MAX-ACCESS` 요소가 `read-write`로 설정되었고, 3) set를 수행하려고 시도하는 사용자에게 해당 작업 수행 권한이 부여된 경우 MIB 객체를 설정할 수 있습니다.

# 보안을 최대화하도록 IPMI 관리 액세스 구성

보안을 최대화하도록 Oracle ILOM IPMI 관리 액세스를 가장 잘 구성하는 방법은 다음 항목을 참조하십시오.



## ▼ 향상된 인증 및 패킷 암호화를 위해 IPMI v2.0 사용

Oracle ILOM에서는 원격 관리에 IPMI v1.5와 v2.0을 모두 지원하지만, 시스템 관리자는 항상 IPMI v2.0 -I lanplus 인터페이스를 사용하여 Oracle 서버를 안전하게 관리해야 합니다. -I lanplus 인터페이스는 IPMI 버전 2.0부터 향상된 인증 및 데이터 무결성 검사를 제공합니다.

펌웨어 릴리스 3.2.4부터 Oracle ILOM은 IPMI v1.5 세션을 사용 또는 사용 안함으로 설정할 수 있는 구성 가능한 등록 정보를 제공합니다. 보안 향상을 위해 IPMI v1.5 등록 정보는 기본적으로 사용 안함으로 설정됩니다. IPMI v1.5 등록 정보가 사용 안함으로 설정된 경우 Oracle ILOM에 대한 IPMI v1.5 세션 연결이 모두 차단됩니다.

펌웨어 릴리스 3.2.4부터 제공되는 IPMI 등록 정보 서비스 State 또는 구성 가능한 IPMI v1.5 등록 정보를 확인하거나 수정하려면 다음 절차를 참조하십시오.

**시작하기 전에**

- Oracle ILOM에서 IPMI 등록 정보를 수정하려면 Admin(a) 역할이 필요합니다.
- IPMI 서비스의 State 등록 정보는 기본적으로 사용으로 설정됩니다. 사용하기 전에 Oracle ILOM에서 적절한 역할 기반 권한(Administrator, Operator)으로 사용자 계정을 구성하여 IPMI 관리 기능을 수행해야 합니다.
- Oracle ILOM 펌웨어 3.2.4 이상을 실행하는 SP의 경우 IPMI v2.0 관리 세션이 지원되며, IPMI v1.5 관리 세션은 기본적으로 지원되지 않습니다. IPMI v1.5 등록 정보는 Oracle ILOM에서 구성할 수 있습니다.

---

**참고** - Oracle ILOM에서 IPMI v1.5 세션이 사용 안함으로 설정된 경우 IPMItool 사용자가 IPMI 2.0 -I lanplus 옵션을 사용해야 합니다.

---

- Oracle ILOM 펌웨어 3.2.3 또는 이전 릴리스를 실행하는 SP의 경우 IPMI v2.0 및 v1.5 관리 세션이 Oracle ILOM에서 지원됩니다. IPMI v1.5 등록 정보는 Oracle ILOM에서 구성할 수 없습니다.

---

**참고** - IPMI v1.5 세션에서는 향상된 인증 및 패킷 암호화를 지원하지 않습니다. 향상된 인증 및 IPMI 패킷 암호화의 경우 IPMI v2.0을 사용해야 합니다.

---

1. **Oracle ILOM 웹 인터페이스에서 IPMI 페이지로 이동합니다.**

   예를 들면 다음과 같습니다.

   - **3.0.x 웹 인터페이스에서 Configuration -> System Management Access -> IPMI를 누릅니다.**
   - **3.1 이상 웹 인터페이스에서 ILOM Administration-> Management Access -> IPMI를 누릅니다.**

2. **IPMI 페이지에서 해당 IPMI 등록 정보를 확인하거나 수정한 다음 Save를 눌러 변경 내용을 적용합니다.**

   추가 IPMI 구성 지침은 아래의 관련 정보 절에 나열된 해당 설명서를 참조하십시오.

### 관련 정보

- *SNMP* 및 *IPMI*에 대한 *Oracle ILOM* 프로토콜 관리 참조*(*펌웨어 *3.2.x)*, IPMI를 사용하여 서버 관리
- *Oracle ILOM 3.1 SNMP, IPMI, CIM, WS-MAN* 프로토콜 관리 참조 설명서, IPMI를 사용하여 서버 관리
- *Oracle ILOM 3.0 SNMP, IPMI, CIM, WS-MAN* 프로토콜 관리 참조 설명서, IPMI를 사용하여 서버 관리
- “IPMI 보안 지침 및 최적의 방법” [45]
- “IPMI 2.0 인증 암호 슈트 지원” [46]

## IPMI 보안 지침 및 최적의 방법

설정된 IPMI 시스템 관리 세션이 안전하고 사이버 공격에 취약하지 않은지 확인하기 위해 시스템 관리자가 수행해야 하는 작업은 다음과 같습니다.

- IPMI 버전 1.5(`-I lan` IPMItool 인터페이스)를 사용하여 IPMI 원격 관리 세션을 설정하지 마십시오. IPMItool(`-I lanplus` IPMItool 인터페이스)와 같은 명령줄 도구를 사용하는 경우 IPMI 버전 2.0을 명시적으로 사용해야 합니다.
- IPMI 암호는 정기적으로 변경하십시오. Oracle ILOM 사용자 계정의 수명 주기를 적절하게 관리해야 합니다.

  자세한 내용은 "Oracle ILOM 사용자 액세스 보안" [22]을 참조하십시오.
- 외부에서 이뤄지는 네트워크 액세스를 제한하십시오. 전용 이더넷 관리 채널을 사용하여 Oracle ILOM과 통신하십시오.

  자세한 내용은 "물리적 관리 연결 보안" [13]을 참조하십시오.
- IT 보안 관리자와 협력하여 서버 관리 및 IPMI 보안을 위한 최적의 방법과 정책을 작성하십시오.

### IPMI 2.0 인증 암호 슈트 지원

암호 슈트를 통해 IPMI 버전 2.0에서 인증, 기밀성 및 무결성 검사가 지원됩니다. 이 암호 슈트는 IPMI 2.0 사양에 설명된 RMCP+ Authenticated Key-Exchange Protocol을 사용합니다.

Oracle ILOM은 클라이언트와 서버 간 보안 IPMI 2.0 세션을 설정하는 데 다음과 같은 암호 슈트 키 알고리즘을 지원합니다.

- **암호 슈트 2** - 암호 슈트 2는 인증 알고리즘과 무결성 알고리즘을 모두 사용합니다.
- **암호 슈트 3** - 암호 슈트 3은 인증, 기밀성 및 무결성에 대한 세 알고리즘을 모두 사용합니다.

---

**참고** - Oracle ILOM은 모든 IPMI 2.0 트래픽을 암호화하기 위해 IPMI 2.0 암호 유형 0(암호화되지 않은 작동 모드)에 대한 지원을 구현하지 않습니다.

---

## 보안을 최대화하도록 WS-Management 액세스 구성

펌웨어 릴리스 3.0.8부터 펌웨어 릴리스 3.1.2까지 Oracle ILOM은 서버의 상태를 모니터링하고 Ws-Management(Ws-Man)라는 프로토콜을 사용하여 인벤토리 정보를 제공하는 표준 웹 서비스 인터페이스를 제공합니다.

Oracle ILOM Ws-Man 인터페이스에서는 호스트의 피어 제어 및 Oracle ILOM SP 자체 재설정도 허용됩니다. Ws-Man은 SOAP(Simple Object Access Protocol) 기반 프로토콜로서 HTTP(S) 프로토콜을 활용합니다. Oracle ILOM Ws-Man 인터페이스는 HTTP 또는 HTTPS와 함께 전송으로 사용될 수 있습니다. HTTPS가 사용될 경우 채널은 SSL 인증서를 사용하여 암호화됩니다. SSL 인증서 사용에 따른 보안상 이점 및 자체 서명 인증서와 신뢰할 수 있는 인증서의 차이점에 대한 자세한 내용은 "신뢰할 수 있는 SSL 인증서 및 개인 키를 사용하여 보안 향상" [33]을 참조하십시오.

이 웹 서비스 인터페이스는 SSL 인증서가 사용될 경우에만 사용하십시오. 최대 보안을 위해서는 HTTPS를 전송 방식으로 사용하십시오. 웹 서버 등록 정보 구성에 대한 자세한 내용은 “보안을 최대화하도록 웹 인터페이스 구성” [33]을 참조하십시오.

# Oracle ILOM 보안을 위한 배치 후 최적의 방법

다음 항목을 사용하여 서버 배치 후 구현할 Oracle ILOM 보안을 위한 최적의 방법을 결정할 수 있습니다.



**관련 정보**

- Oracle ILOM 보안을 위한 배치 관련 최적의 방법
- Oracle ILOM 보안 관련 최적의 방법 점검 목록

## 보안 관리 연결 유지 관리

Oracle ILOM에 대한 보안 관리 연결을 유지 관리하려면 다음 정보를 고려하십시오.



## 인증되지 않은 호스트 KCS 장치 액세스 방지

Oracle 서버는 호스트와 Oracle ILOM 간에 KCS(Keyboard Controller Style) 인터페이스라는 표준 저속 연결을 지원합니다. 이 지원되는 KCS 인터페이스는 IPMI(Intelligent Platform Management Interface) 버전 2.0 사양과 완벽하게 호환되며 마찬가지로 사용 안함으로 설정할 수 없습니다.

KCS 장치 액세스는 호스트에서 Oracle ILOM을 구성하는 편리한 방법이지만, 물리적 KCS 장치에 대한 커널 또는 드라이버 액세스 권한을 가진 운영 체제 사용자가 인증 없이 Oracle

ILOM 설정을 수정할 수 있으므로 이 유형의 액세스를 사용할 경우 보안 위험이 발생할 수도 있습니다. 일반적으로 `root` 또는 관리자 사용자만 KCS 장치에 액세스할 수 있습니다. 하지만 KCS 장치에 대해 폭넓은 액세스를 제공하도록 대부분의 운영 체제를 구성할 수 있습니다.

예를 들어 KCS 액세스 권한을 가진 운영 체제 사용자는 다음을 수행할 수 있습니다.

- Oracle ILOM 사용자를 추가하거나 만듭니다.
- 사용자 암호를 변경합니다.
- ILOM 관리자로 Oracle ILOM CLI에 액세스합니다.
- 로그 및 하드웨어 정보에 액세스합니다.

일반적으로 이 장치는 Linux 또는 Oracle Solaris에서 `/dev/kcs0` 또는 `/dev/bmc`이고, Microsoft Windows에서 `ipmidrv.sys` 또는 `imbdrv.sys`입니다. BMC(Baseboard Management Controller) 드라이버 또는 IPMI 드라이버라고도 하는 이 장치에 대한 액세스는 호스트 운영 체제의 일부인 알맞은 액세스 제어 방식을 사용하여 신중하게 제어해야 합니다.

호스트 IPMI KCS 장치를 사용하여 Oracle ILOM 설정을 구성하는 또 다른 방법으로 Oracle ILOM 상호 연결 인터페이스 사용을 고려하십시오. 자세한 내용은 "선호하는 인증된 호스트 상호 연결 액세스" [50]를 참조하십시오.

하드웨어 장치(예: KCS 장치)에 대한 액세스를 제어하거나 보호하는 자세한 방법은 호스트 운영 체제와 함께 제공되는 설명서를 참조하십시오,

## 선호하는 인증된 호스트 상호 연결 액세스

KCS 인터페이스보다 빠른 대안으로 호스트 운영 체제의 클라이언트는 내부 고속 상호 연결을 통해 Oracle ILOM과 통신할 수 있습니다. 상호 연결은 IP 스택을 실행하는 내부 Ethernet-over-USB 연결로 구현됩니다. Oracle ILOM에는 호스트의 클라이언트가 연결하는 데 사용할 수 있는 내부 라우팅 불가능 IP 주소가 부여됩니다.

하드웨어 장치에 대한 보호된 액세스에 의존하는 KCS 인터페이스와 달리 LAN 상호 연결은 기본적으로 모든 운영 체제 사용자가 사용할 수 있습니다. 따라서 LAN 상호 연결을 통한 Oracle ILOM 연결에는 네트워크를 통해 Oracle ILOM 관리 포트로 들어오는 연결과 같이 인증이 필요합니다.

또한 관리 네트워크에서 노출되는 모든 서비스나 프로토콜은 호스트에 대한 LAN 상호 연결을 통해 사용 가능하게 됩니다. 호스트의 웹 브라우저를 사용하여 Oracle ILOM 웹 인터페이스에 액세스하거나 보안 셸 클라이언트를 사용하여 Oracle ILOM 명령줄 인터페이스에 연결할 수 있습니다. 모든 경우에 LAN 상호 연결을 사용하려면 유효한 사용자 이름과 암호를 제공해야 합니다.

LAN 상호 연결은 기본적으로 사용 안함으로 설정됩니다. 사용 안함으로 설정되면 호스트 운영 체제에 표시되는 이더넷 장치가 없으며 채널이 존재하지 않습니다. Oracle Hardware Management Pack을 통해 LAN 상호 연결을 프로비전하고 구성할 수 있습니다.

보안 전용 호스트 상호 연결을 통한 Oracle ILOM 관리에 대한 자세한 내용은 다음 중 하나를 참조하십시오.

- 펌웨어 릴리스 3.2 이상의 경우, *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2x)*에서 전용 상호 연결 SP 관리 연결을 참조하십시오.
- 펌웨어 릴리스 3.1.x의 경우, *Oracle ILOM 3.1* 구성 및 유지 관리 설명서에서 전용 상호 연결 SP 관리 연결을 참조하십시오.
- 펌웨어 릴리스 3.0.12 - 3.0.16의 경우 *Oracle ILOM 3.0* 웹 절차 안내서에서 로컬 호스트 상호 연결 구성을 참조하십시오.

# IPMI 2.0 암호화를 사용하여 채널 보안 설정

IPMI(Intelligent Platform Management Interface) 버전 2.0은 RMCP+(Remote Management and Control Protocol+)라는 암호화된 네트워크 프로토콜을 지원합니다. 이 프로토콜은 대칭 키 기반 시도-응답 방식을 사용하여 채널을 암호화합니다. 이 방식은 민감한 데이터가 암호화되지 않은 상태로 네트워크를 통해 전송되지 않도록 하며, 트래픽을 암호화하고 해독하려면 사용자 암호가 필요합니다. Oracle ILOM은 모든 IPMI 2.0 트래픽을 암호화하기 위해 IPMI 2.0 암호 유형 0(암호화되지 않음) 작동 모드에 대한 지원을 구현하지 않습니다.

IPMItool의 경우 `-I lanplus` 플래그를 사용하여 암호화된 RMCP+ 세션을 설정해야 함을 나타냅니다.

자세한 내용은 `ipmitool` 설명서를 참조하십시오.

---

**참고** - 펌웨어 릴리스 3.2.4부터 Oracle ILOM은 IPMI 1.5에 대한 구성 가능한 등록 정보를 제공합니다. 기본적으로 IPMI 1.5 등록 정보는 사용 안함으로 설정됩니다. 자세한 내용은 향상된 인증 및 패킷 암호화를 위해 IPMI v2.0 사용 [44]을 참조하십시오.

---

# 원격 관리에 보안 프로토콜 사용

Oracle ILOM은 여러 가지 원격 관리 프로토콜을 지원합니다. 동일한 프로토콜의 암호화 버전과 비암호화 버전에 대한 지원이 모두 제공되는 경우도 있습니다. 보안상 가능하다면 항상 가장 안전한 프로토콜을 사용해야 합니다. 지원되는 암호화 및 비암호화 프로토콜 목록은 다음 표를 참조하십시오.

**표 9** 지원되는 보안 프로토콜

| 범주 | 보안/암호화 | 비암호화 |
|---|---|---|
| 웹 브라우저 액세스 | HTTPS | HTTP |
| 명령줄 액세스 | SSH | 지원되지 않음 |

| 범주 | 보안/암호화 | 비암호화 |
|---|---|---|
| IPMI 액세스 | IPMI v2.0 | IPMI v1.5 |
| 프로토콜 액세스 | SNMPv3 | SNMPv1/v2c |

## 신뢰할 수 있는 네트워크 보안 관리 연결 설정

Oracle ILOM이 있는 모든 Oracle 서버에는 네트워크를 통해 Oracle ILOM에 연결하는 데 사용되는 전용 관리 포트가 있습니다. 전용 관리 포트를 사용하면 관리를 위한 전용 및 보안 네트워크가 제공됩니다. 일부 시스템에서는 표준 서버 데이터 포트에서 호스트와 Oracle ILOM에 모두 액세스할 수 있도록 허용하는 사이드밴드 관리도 지원합니다. 사이드밴드 관리를 사용하면 두 개의 별도 네트워크 연결이 필요하지 않으므로 케이블 관리 및 네트워크 구성이 간소화됩니다. 하지만 전용 또는 사이드밴드 관리 포트가 신뢰할 수 있는 네트워크에 연결되어 있지 않으면 Oracle ILOM 트래픽이 신뢰할 수 없는 네트워크를 통해 전송될 수도 있습니다.

따라서 Oracle ILOM에서 가장 안전한 보안 환경을 유지하기 위해서는 서버의 전용 네트워크 관리 포트 또는 사이드밴드 관리 포트가 항상 신뢰할 수 있는 내부 네트워크 또는 전용 보안 관리/개인 네트워크에 연결되어 있어야 합니다.

## 보안 로컬 직렬 관리 연결 설정

서버에 있는 물리적 직렬 관리 포트를 통해 터미널 서버 또는 덤프 터미널을 로컬에서 Oracle ILOM에 연결할 수 있습니다. Oracle ILOM에 대한 보안 로컬 관리 연결을 유지하려면 터미널 장치가 내부 네트워크 또는 개인 네트워크에도 연결된 경우 해당 장치를 로컬 직렬 관리 포트에 연결하지 마십시오.

# 원격 KVMS 보안 사용

Oracle ILOM은 원격으로 호스트 서버의 키보드, 비디오 및 마우스를 원격 클라이언트로 재지정하고 원격 저장소를 마운트할 수 있는 기능을 제공합니다. 이러한 기능을 통칭하여 원격 KVMS라고 합니다. 원격 KVMS를 통해 클라이언트 시스템에서 Oracle ILOM Remote Console, Remote Console Plus 및 Storage Redirection CLI라는 Java 응용 프로그램을 실행하여 서버에서 호스트 운영 체제의 그래픽 콘솔을 볼 수 있습니다.

원격 KVMS 및 직렬 텍스트 기반 세션이 Oracle ILOM에서 안전하게 실행되었는지 확인하려면 다음 사항을 고려하십시오.

- “KVMS 원격 통신 및 암호화” [53]
- “원격 KVMS 공유 액세스로부터 보호” [53]
- “호스트 직렬 콘솔 공유 액세스로부터 보호” [54]

# KVMS 원격 통신 및 암호화

Oracle ILOM Remote System Console, Remote System Console Plus 및 CLI Storage Redirection 응용 프로그램은 일련의 네트워크 프로토콜을 사용하여 Oracle ILOM과 원격으로 통신합니다. 이러한 Java 응용 프로그램을 사용하여 호스트 키보드 및 마우스를 제어하고 원격 서버에서 로컬 저장 장치(CD 또는 DVD 드라이브 등)를 마운트할 수 있습니다.

다음 표는 원격 KVMS 정보가 네트워크를 통해 전송되는 방식을 더 자세하게 설명합니다.

**표 10** KVMS 기능 및 암호화

| KVMS 기능 | 암호화 여부 | 설명 |
|---|---|---|
| 마우스 재지정 | 암호화 | 마우스의 좌표가 네트워크를 통해 Oracle ILOM으로 안전하게 전송됩니다. |
| 키보드 재지정 | 암호화 | 클라이언트 시스템에서 입력하는 모든 문자가 암호화된 프로토콜을 사용하여 Oracle ILOM으로 전송됩니다. |
| 비디오 재지정 | 암호화 | 비디오 데이터가 Java 클라이언트와 Oracle ILOM 사이에 암호화된 프로토콜을 사용하여 전송됩니다. |
| 저장소 재지정 | 암호화되지 않음 | 저장 장치에서 읽고 쓰는 데이터가 암호화 없이 네트워크를 통해 Oracle ILOM로 전송됩니다. |

원격 KVMS를 통해 사용으로 설정된 네트워크 포트 목록은 표 4. “기본적으로 사용으로 설정되는 서비스 및 포트”를 참조하십시오.

# 원격 KVMS 공유 액세스로부터 보호

원격 KVMS 비디오 콘솔은 해당 서버에 연결된 실제 모니터를 볼 경우 보이는 모든 것을 재지정합니다. Oracle ILOM에 대한 KVMS 세션을 사용하는 여러 원격 클라이언트가 있을 수 있지만 일반적으로 단일 서버에 대한 비디오 출력은 하나만 있으므로 각 세션은 모두 동일한 비디오를 표시합니다.

마찬가지로 한 원격 KVMS 세션에서 화면에 입력하는 내용은 동일 시스템에 연결된 다른 KVMS 사용자에게도 표시됩니다. 가장 중요한 사항으로 한 사용자가 Oracle ILOM Remote Console, Remote Console Plus 또는 Storage Redirection CLI 응용 프로그램 내에서 호스트 운영 체제에 권한이 있는 사용자로 로그인할 경우 다른 모든 KVMS 사용자가 인증된 해당 세션을 공유할 수 있습니다. 따라서 원격 KVMS 기능은 공유 연결을 허용한다는 사실을 알고 있어야 합니다.

원격 KVMS 재지정 세션을 종료한 이후에도 유휴 상태로 남아 있는 인증된 운영 체제 세션으로부터 보호하려면 다음을 수행해야 합니다.

- 원격 KVMS 재지정 세션을 종료할 때 호스트 운영 체제를 자동으로 잠그도록 Oracle ILOM을 구성합니다.

  지침은 KVMS 세션 종료 시 호스트 액세스 잠금 [29]을 참조하십시오.
- 방치된 상태의 인증된 사용자 세션이 자동으로 닫히도록 호스트 운영 체제에서 시간 초과 간격을 설정합니다.

  지침은 해당 호스트 운영 체제의 사용 설명서를 참조하십시오.

Oracle ILOM Remote System Console Plus 사용자가 Oracle ILOM에서 실행된 표시 가능 KVMS 세션 수를 제한해야 하는 경우 Remote System Console Plus의 표시 가능 KVMS 세션 제한(3.2.4 이상) [30]을 참조하십시오.

## 호스트 직렬 콘솔 공유 액세스로부터 보호

대부분의 운영 체제에 대한 호스트 콘솔은 텍스트 기반의 직렬 콘솔로 사용할 수도 있습니다. 이 콘솔은 Oracle ILOM CLI의 명령줄에서 `start /HOST/console` 명령을 실행하여 사용할 수 있습니다. 그래픽 콘솔과 유사하게 모든 Oracle ILOM 사용자가 사용할 수 있는 직렬 콘솔은 하나뿐입니다. 따라서 이것도 공유 리소스로 간주됩니다. 한 사용자가 직렬 콘솔에서 호스트 운영 체제에 로그인한 다음 로그아웃하지 않은 상태로 콘솔 재지정을 종료할 경우 직렬 콘솔의 두번째 사용자는 이전에 인증된 운영 체제 세션에 액세스할 수 있습니다.

콘솔 재지정 세션이 종료되면 Oracle ILOM은 DTR(Data Transfer Request) 신호를 호스트 운영 체제에 보냅니다. 이 신호가 수신되면 많은 운영 체제에서는 사용자를 자동으로 로그아웃시킵니다. 하지만 일부 운영 체제는 이 기능을 지원하지 않습니다.

- Oracle Linux 5에는 기본적으로 작동하는 DTR 신호 지원 기능이 있습니다.
- Oracle Linux 6에는 DTR 지원 기능이 있지만 수동으로 사용으로 설정해야 합니다.
- Oracle Solaris에는 DTR 신호에 대한 지원 기능이 없습니다. 보안 위험을 줄이기 위해 사용자는 호스트 운영 체제에서 세션 시간 초과를 구성할 수 있습니다.

호스트 직렬 재지정 세션을 종료한 이후에도 유휴 상태로 남아 있는 인증된 운영 체제 세션으로부터 보호하기 위한 지침은 다음을 참조하십시오.

- 호스트 운영 체제의 DTR 신호 기능이 지원되는지 여부를 확인하고 지원될 경우 이 기능이 기본적으로 사용으로 설정되었는지 확인합니다.

  DTR 신호에 대한 자세한 내용은 해당 호스트 운영 체제의 사용 설명서를 참조하십시오.
- 호스트 운영 체제에서 세션 시간 초과 간격을 구성합니다.

  호스트 운영 체제에서 세션 시간 초과 간격을 설정하는 방법은 해당 호스트 운영 체제의 사용 설명서를 참조하십시오.

# 사용자 액세스 보안을 위한 배치 후 고려 사항

보안 사용자 액세스를 유지 관리하려면 다음 사항을 고려하십시오.

# 암호 관리 적용

모든 Oracle ILOM 암호는 정기적으로 변경하십시오. 그러면 악의적인 작업을 막을 수 있고 암호가 현재 암호 정책을 준수하게 됩니다.

보통 사용자가 자신의 암호를 변경하지만, 사용자 관리 권한을 가진 시스템 관리자는 다른 사용자 계정과 연관된 암호를 수정할 수 있습니다.

Oracle ILOM 사용자 계정과 연관된 암호를 변경하려면 다음과 같은 웹 기반 지침을 참조하십시오.

---

**참고** - CLI 지침 또는 사용자 관리 구성 등록 정보에 대한 기타 세부 정보는 다음 절차의 관련 정보 절에 나열된 설명서를 참조하십시오.

---

## ▼ 로컬 사용자 계정 암호 수정

**시작하기 전에**

- "사용자 계정 및 암호 관리를 위한 보안 지침" [24]을 검토합니다.
- 다른 사용자 계정과 연관된 암호 또는 권한을 수정하려면 User Management(u) 역할이 필요합니다.
- Operator(o) 역할은 사용자가 자신의 계정에 대한 암호를 수정할 수 있도록 허용합니다.

1. **Oracle ILOM 웹 인터페이스에서 User Account 페이지로 이동합니다.**

   예를 들면 다음과 같습니다.

   - **3.0.x 웹 인터페이스에서 User Management -> User Accounts를 누릅니다.**
   - **3.1 이상 웹 인터페이스에서 User Management -> User Accounts를 누릅니다.**

2. **User Account 페이지에서 수정하려는 계정에 대해 Edit를 누릅니다.**

   Edit: User Name 대화 상자가 나타납니다.

3. **Edit: User Name 대화 상자에서 다음을 수행합니다.**

- **New Password 텍스트 상자에 고유한 암호를 입력한 다음 Confirm New Password 텍스트 상자에 같은 암호를 다시 입력합니다.**
- **Save를 눌러 변경 내용을 적용합니다.**

**관련 정보**

- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, 로컬 사용자 계정 구성
- *Oracle ILOM 3.1* 구성 및 유지 관리 설명서, 로컬 사용자 계정 구성
- *Oracle ILOM 3.0* 일상적인 관리 - *CLI* 절차 안내서, 사용자 계정 수정
- *Oracle ILOM 3.0* 일상적인 관리 - 웹 절차 안내서, 사용자 계정 수정

## root 계정 기본 암호를 재설정하기 위한 물리적 보안 존재

Oracle ILOM에 대한 root 사용자 암호를 잊어버린 경우 재설정할 수 있습니다. root 암호를 재설정하려면 직렬 포트를 통해 Oracle ILOM에 연결합니다. 대부분의 경우 Oracle ILOM 직렬 포트에 연결하려면 시스템에 대한 물리적인 액세스가 필요하지만 직렬 콘솔은 터미널 서버에 연결할 수 있습니다. 터미널 서버는 물리적인 직렬 포트에 대한 네트워크 액세스 권한을 효과적으로 부여합니다.

터미널 서버가 사용될 때 네트워크를 통해 root 암호를 재설정하지 못하도록 하기 위해 대부분의 서버에는 물리적 존재 확인 기능이 있습니다. 이 경우 서버에 대한 물리적 액세스를 증명하기 위한 방법으로 서버에 있는 버튼을 눌러야 합니다. 최대 보안을 위해서는 Oracle ILOM 직렬 포트가 터미널 서버에 연결될 때마다 존재 확인 기능이 사용으로 설정되어 있는지 확인하십시오.

물리적 존재 확인 기능을 확인하거나 수정하려면 다음과 같은 웹 기반 지침은 참조하십시오.

---

**참고** - CLI 지침 또는 root 계정 등록 정보에 대한 기타 세부 정보는 다음 절차의 관련 정보 절에 나열된 설명서를 참조하십시오.

---

### ▼ 물리적 존재 확인 설정

**시작하기 전에**

- Oracle ILOM의 물리적 존재 확인 모드는 기본적으로 사용으로 설정됩니다.
- Oracle ILOM에서 물리적 존재 확인 모드를 사용하려면 펌웨어 버전 3.1 이상이 필요합니다.

1. **Oracle ILOM 웹 인터페이스에서 ILOM Administration -> Identification을 누릅니다.**

2. **Identification 페이지에서 Physical Presence Check 등록 정보로 이동한 후 다음 중 하나를 수행합니다.**

   - **Physical Presence 확인란을 선택하여 사용으로 설정합니다. 사용으로 설정된 경우 기본 Oracle ILOM 암호를 복구하기 위해 물리적 시스템의 Locator 버튼을 눌러야 합니다.**

     -또는-

   - **Physical Presence 확인란을 선택 해제하여 사용 안함으로 설정합니다. 사용 안함으로 설정된 경우 물리적 시스템의 Locator 버튼을 누르지 않고도 기본 Oracle ILOM 관리자 루트 암호를 재설정할 수 있습니다.**

3. **Save를 눌러 변경 내용을 적용합니다.**

**관련 정보**

- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, 장치 식별 구성 등록 정보
- *Oracle ILOM 3.1* 구성 및 유지 관리 설명서, 장치 식별 구성 등록 정보
- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, `root` 계정에 대한 암호 복구
- *Oracle ILOM 3.1* 구성 및 유지 관리 설명서, `root` 계정에 대한 암호 복구

# 감사 이벤트를 모니터링하여 허용되지 않은 액세스 찾기

Oracle ILOM 감사 로그는 모든 로그인 및 구성 변경 사항을 기록합니다. 각 감사 로그 항목에는 이벤트와 연관된 사용자 및 시간 기록이 표시됩니다. 감사 이벤트는 변경 사항 추적 및 Oracle ILOM에 대한 무단 변경 및 허용되지 않은 액세스가 있었는지 여부를 확인하는 데 유용한 도구가 될 수 있습니다.

Oracle ILOM 감사 로그에서 이벤트를 확인하려면 다음과 같은 웹 기반 지침은 참조하십시오.

---

**참고** - CLI 지침 또는 감사 로그에 대한 기타 세부 정보는 다음 절차의 관련 정보 절에 나열된 설명서를 참조하십시오.

---

## ▼ 감사 로그 보기

**시작하기 전에**

- 감사 로그는 Oracle ILOM 펌웨어 릴리스 3.1부터 사용 가능합니다. 펌웨어 릴리스 3.1 이전에는 감사 이벤트가 Oracle ILOM 이벤트 로그에 캡처되었습니다.
- 감사 로그의 항목을 지우려면 Oracle ILOM에서 Admin(a) 역할 권한이 필요합니다.

1. **웹 인터페이스에서 ILOM Administration -> Logs -> Audit를 누릅니다.**
2. **Audit log 페이지에서 컨트롤을 사용하여 로그 항목을 필터링하거나 로그에서 이벤트를 지웁니다.**

   펌웨어 버전 3.2 이상을 실행하는 사용자의 경우 Audit 페이지의 `More details` 링크를 누르면 추가 정보를 볼 수 있습니다.

**관련 정보**

- *Oracle ILOM* 시스템 모니터링 및 진단을 위한 사용 설명서*(*펌웨어 *3.2.x)*, Oracle ILOM 로그 항목 관리
- *Oracle ILOM 3.1* 사용 설명서, Oracle ILOM 로그 항목 관리

# FIPS 모드 수정을 위한 배치 후 작업

펌웨어 릴리스 3.2.4부터 Oracle ILOM은 FIPS 준수에 대한 구성 가능한 등록 정보를 제공합니다. 기본적으로 이 등록 정보는 사용 안함으로 설정되어 제공됩니다. Oracle ILOM에서 FIPS 준수의 작동 상태를 수정할 경우 사용자 정의 구성 등록 정보가 모두 출하 시 기본 설정으로 재설정됩니다. Oracle ILOM에서 사용자 정의 구성 설정의 손실을 방지하려면 다른 Oracle ILOM 설정을 구성하기 전에 FIPS 준수를 수정해야 합니다. Oracle ILOM 구성 배치 후 FIPS 준수를 수정해야 하는 경우 사용자 정의 설정이 손실되지 않도록 다음 지침을 참조하십시오.

## ▼ 배치 후 FIPS 모드 수정

펌웨어 업데이트를 수행한 후 또는 Oracle ILOM에서 사용자 정의 구성 등록 정보를 지정한 후 FIPS 모드 작동 상태를 수정해야 하는 경우 이 절차를 수행하십시오.

---

**참고** - Oracle ILOM의 FIPS 준수 모드는 State 및 Status 등록 정보로 표시됩니다. State 등록 정보는 Oracle ILOM에서 구성된 모드를 나타내고, Status 등록 정보는 Oracle ILOM의 작동 모드를 나타냅니다. FIPS State 등록 정보가 변경된 경우 다음에 Oracle ILOM을 재부트해야 변경 사항이 작동 모드(FIPS Status 등록 정보)에 적용됩니다.

---

**시작하기 전에**

- FIPS 준수에 대한 구성 가능한 등록 정보는 Oracle ILOM 펌웨어 3.2.4 이상부터 사용할 수 있습니다. 펌웨어 릴리스 3.2.4 이전에는 Oracle ILOM에서 FIPS 준수에 대해 구성 가능한 등록 정보를 제공하지 않습니다.
- FIPS가 사용으로 설정(구성되어 작동 가능함)된 경우 Oracle ILOM의 일부 기능이 지원되지 않습니다. FIPS가 사용으로 설정된 경우 지원되지 않는 기능 목록은 "FIPS 모드가 사용으로 설정된 경우 지원되지 않는 기능" [16]을 참조하십시오.
- 이 절차를 수행하려면 Admin(a) 역할이 필요합니다.

1. **Oracle ILOM 웹 인터페이스에서 Oracle ILOM 구성을 백업합니다.**

   예를 들면 다음과 같습니다.

   a. **ILOM Administration -> Configuration Management -> Backup/Restore를 누릅니다.**

   b. **Backup/Restore 페이지에서 More details... 링크를 눌러 추가 지침을 확인합니다.**

---

**참고** - 펌웨어 업데이트 후 Oracle ILOM에 손쉽게 다시 연결하려면 Preserve the Configuration에 대한 펌웨어 업데이트 옵션을 사용으로 설정해야 합니다.

---

---

**참고** - 1단계를 수행하기 전에 2단계를 수행한 경우 백업된 XML 구성 파일을 편집한 후 FIPS 설정을 제거해야 합니다. 그렇지 않을 경우 백업된 Oracle ILOM XML 파일과 서버에서 실행 중인 FIPS 작동 모드 상태 간에 불일치한 구성이 생기는데, 이는 허용되지 않습니다.

---

2. **펌웨어 업데이트가 필요한 경우 다음 단계를 수행합니다.**

   a. **ILOM Administration -> Maintenance -> Firmware Update를 누릅니다.**

   b. **Firmware Update 페이지에서 More details... 링크를 눌러 추가 지침을 확인합니다.**

3. **다음과 같이 Oracle ILOM FIPS 준수 모드를 수정합니다.**

a. **ILOM Administration -> Management Access -> FIPS를 누릅니다.**

b. **FIPS 페이지에서 `More details` 링크를 눌러 다음을 수행하는 방법에 대한 지침을 확인합니다.**

- **FIPS State 구성 수정**
- **SP를 재설정하여 시스템의 FIPS 작동 상태 업데이트**

4. **다음과 같이 백업된 Oracle ILOM 구성을 복원합니다.**

a. **ILOM Administration -> Configuration Management -> Backup/Restore를 누릅니다.**

b. **Backup/Restore 페이지에서 `More details` 링크를 눌러 추가 지침을 확인합니다.**

**관련 정보**

- "배치 시 FIPS 모드 구성 여부 선택" [14]
- "FIPS 모드가 사용으로 설정된 경우 지원되지 않는 기능" [16]
- *Oracle ILOM* 구성 및 유지 관리를 위한 관리자 설명서*(*펌웨어 *3.2.x)*, FIPS 모드 등록 정보 구성

# 최신 소프트웨어 및 펌웨어로 업데이트

서버의 소프트웨어 및 펌웨어 버전을 최신 버전으로 유지하십시오.

- My Oracle Support에 게시된 업데이트를 정기적으로 확인합니다.
- 항상 서버에 사용 가능한 소프트웨어 또는 펌웨어의 최신 릴리스 버전을 설치하여 버그 수정 및 향상된 기능을 사용합니다.
- 설치된 모든 소프트웨어에 필요한 보안 패치를 설치합니다.

서버에서 Oracle ILOM 펌웨어를 업데이트하려면 다음 지침을 참조하십시오.

## ▼ Oracle ILOM 펌웨어 업데이트

**시작하기 전에**

- Oracle ILOM 펌웨어를 업데이트하려면 Oracle ILOM에서 Admin(a) 역할이 필요합니다.

- 모든 Oracle ILOM 사용자에게 일정이 잡힌 펌웨어 업데이트를 통지하고 펌웨어 업데이트가 완료될 때까지 모든 클라이언트 세션을 닫도록 요청합니다.
- 펌웨어 업데이트 프로세스가 완료되는 데 다소 시간이 걸립니다. 이 시간 동안 다른 Oracle ILOM 작업을 수행해서는 안됩니다.

1. **MOS(My Oracle Support) 웹 사이트에서 서버에 사용 가능한 최신 소프트웨어 업데이트를 다운로드합니다.**

   필요한 경우 서버와 함께 제공된 설명서를 참조하여 MOS에서 소프트웨어 업데이트를 가져오기 위한 지침을 확인합니다.

   ---

   **참고** - 사용 중인 서버에 사용 가능한 최신 Oracle ILOM 펌웨어 버전은 MOS에 게시된 해당 서버에 대한 최신 소프트웨어 패치에 포함되어 있습니다.

   ---

2. **펌웨어 이미지를 로컬 또는 네트워크 공유 드라이브에 저장합니다.**

3. **웹 인터페이스에서 Firmware Update 페이지로 이동합니다.**

   예를 들면 다음과 같습니다.

   - **3.0.x 웹 인터페이스에서 Maintenance -> Firmware를 누릅니다.**
   - **3.1 이상 웹 인터페이스에서 ILOM Administration -> Maintenance -> Firmware Upgrade를 누릅니다.**

4. **Firmware Upgrade 페이지에서 Enter Firmware Upgrade Mode를 누른 다음 프롬프트의 내용을 따릅니다.**

   Oracle ILOM 펌웨어 3.2 이상을 실행하는 사용자의 경우 Firmware Upgrade 페이지에서 `More details` 링크를 누릅니다.