D'Amo DA-MYQ

사용자 설명서

v5.0.52

2023. 12. 12

디아모 개발부

Penta SECURITY

D'Amo DA-MYQ v5.0

이 문서는 제품의 개발사인 당사의 임직원, 당사와 NDA 체결된 파트너사 및 EULA 체결된 고객사의 임직원을 대상으로 작성한다.

매뉴얼 안내

펜타시큐리티의 제품 매뉴얼은 다음과 같이 분류하며 각 문서의 보안 등급에 따라 필요한 정보를 제공한다.

문서명	문서 보안 등급	정의
사용자 설명서	SL4	• 제품과 함께 고객에게 제공되는 기본 설명서이다. • 제품 기능에 대한 개요(Concept) 및 각 기능에 대해 설명한다. • 제품(H/W, S/W)를 설치하기 위한 절차 및 동작 확인을 위한 최소한의 설정과 서비스의 이용 방법을 설명한다.
파트너 안내서	SL3	• 파트너사의 엔지니어에게 제공된다. • 고객에게 공개되지 않는 기능의 '설정/운영 방법'을 각 절차에 따라 개조식으로 설명한다.
특정 고객용 설명서	SL2~SL4	사이트 패키지 등과 같이 특정 사이트의 고객에게 제공한다.
개발자 안내서	SL2~SL4	• 고객의 개발자 또는 협력사에 제공한다. • 제품과 함께 제공되는 API를 이용하여 응용 서비스 개발이 가능한 정보를 제공한다.

유지보수에 관한 정보는 별도 유지 보수 계약서에 명시되므로, 본 매뉴얼에서는 제공하지 않는다.

매뉴얼 표기법

이 문서는 다음과 같은 표기법에 준하여 작성한다.

표기법

표기법	설명	예
(*)	필수 입력 항목이다.	-
ex), 예)	예제 표기	• ex) 회사(기관명) • 예) 작성 방법

표기법	설명	예
{ }	사용자 환경에 따라 입력되는 값이 상이할 경우	{설치 디렉터리}₩ABC.exe 파일을 입력해 주세요.
[ ]	• Command Line 명령어에서 사용자가 선택적으로 입력하는 옵션 정보 • CLI 표기법은 각 제품 특성을 고려하여 별도 정의하며, 상세 내용은 해당 제품의 <CLI 명령어 설명서>를 참고한다.	도스 창에서 DIR[₩W]를 입력하세요.
	메뉴/기능 버튼 이름	[시작]-[모든 프로그램]-[관리도구]
	항목 이름	설정 파일의 [KEYINFO] 항목
<>	문서의 이름이나 소제목 등을 적을 때	<CLI 명령어 설명서>를 참고한다.
' '	강조하는 말이나 글 앞/뒤에 사용	'신규 정책'을 기반으로...
-	특정 기능을 수행하기 위해 진입하는 메뉴 또는 기능의 이름을 분리할 때	[키 관리]-[데이터 암호화 키]-[변경]

회사 안내

설립연도		1997년 07월
본사	**사명**	펜타시큐리티(주)
	소재지	서울시 영등포구 여의공원로 115 세우빌딩 9층 (TEL: 02.780.7728 FAX: 02.786.5281)
	R&D센터	펜타보안기술연구소
		IoT융합보안연구소
일본 법인	**법인명**	Penta Security K.K
	소재지	도쿄 신주쿠 이치가야타마치 3-8, 이치가야 카가쿠기쥬츠 이노베이션센터 빌딩 12층
베트남 지사	**지사명**	Penta Security Inc.
	소재지	9th Floor, Hanoi Women's Union Building, No 7 Ton That Thuyet, Dich Vong Hau, Cau Giay, Hanoi, Vietnam

만든 사람들

작성 및 편집: 디아모 개발부
표지 및 디자인: 디자인 팀
교정·교열: 품질관리실

차례

제품 매뉴얼에 관하여

목적

본 문서는 제품과 함께 고객에게 제공되며, 사용자가 보다 쉽고 편리하게 **D'Amo DA-MYQ**을 사용할 수 있도록 돕기 위해 작성되었다.

사전 지식

본 문서를 이해하기 위해 필요한 사전 지식은 아래와 같다.

- Windows, Unix, Linux 환경에 대한 기초 지식
- DB에 대한 기초 지식

오픈 소스 라이선스 목록

오픈 소스 소프트웨어 라이선스에 따라, 본 **D'Amo DA-MYQ** 제품에 포함되어 있는 오픈 소스 소프트웨어 목록은 다음과 같다.

오픈 소스 라이선스의 목록

오픈 소스	라이선스 타입
N/A	N/A

제품 개요

D'Amo DA-MYQ는, DBMS Application Encryption의 약자로 **API 형태의 DB 서버 암호화 제품**이다.

D'Amo DA-MYQ는 애플리케이션 서버에 암복호화 API를 삽입하여 **DBMS의 부담을 최소화** 함으로써, **효과적인 DB 보안 기능**을 제공한다.

주요 기능 및 특징

본 제품은, 다음과 같은 기능과 특징을 갖는다.

보안성

키 관리와 관리자 인증을 통한 보안성 강화

- 하이브리드 암호 시스템을 사용하여 **암복호화 키를 이중 암호화** 한다.
- 별도의 하드웨어를 통해 **강력한 키 관리 기능**을 지원한다.(D'Amo SG-KMS 적용 시)

편의성

다양한 알고리즘과 GUI를 통한 편의성 증대

- 관리자 시스템에서 키 관리와 설정(D'Amo SG-KMS 적용 시)을 가능하게 함으로써, **관리자의 편의성**을 증대한다.

- 관리도구를 통해 **정책 설정** 및 **로그/시스템 현황** 정보를 제공한다.
- 직관적인 GUI와 CLI를 제공한다.

확장성

다양한 알고리즘과 환경 지원

- **국내·외 표준 암호화 알고리즘**을 지원한다.
- **이기종(Heterogeneous) DBMS간 데이터 연동** 시, 데이터 암호 키가 다른 경우에도 안전한 연동이 가능하다.
- **관리 대상 DBMS 추가** 시, D'Amo DA-MYQ 설치 만으로 **기존 암호화 관리 체계와 통합**이 가능하다.

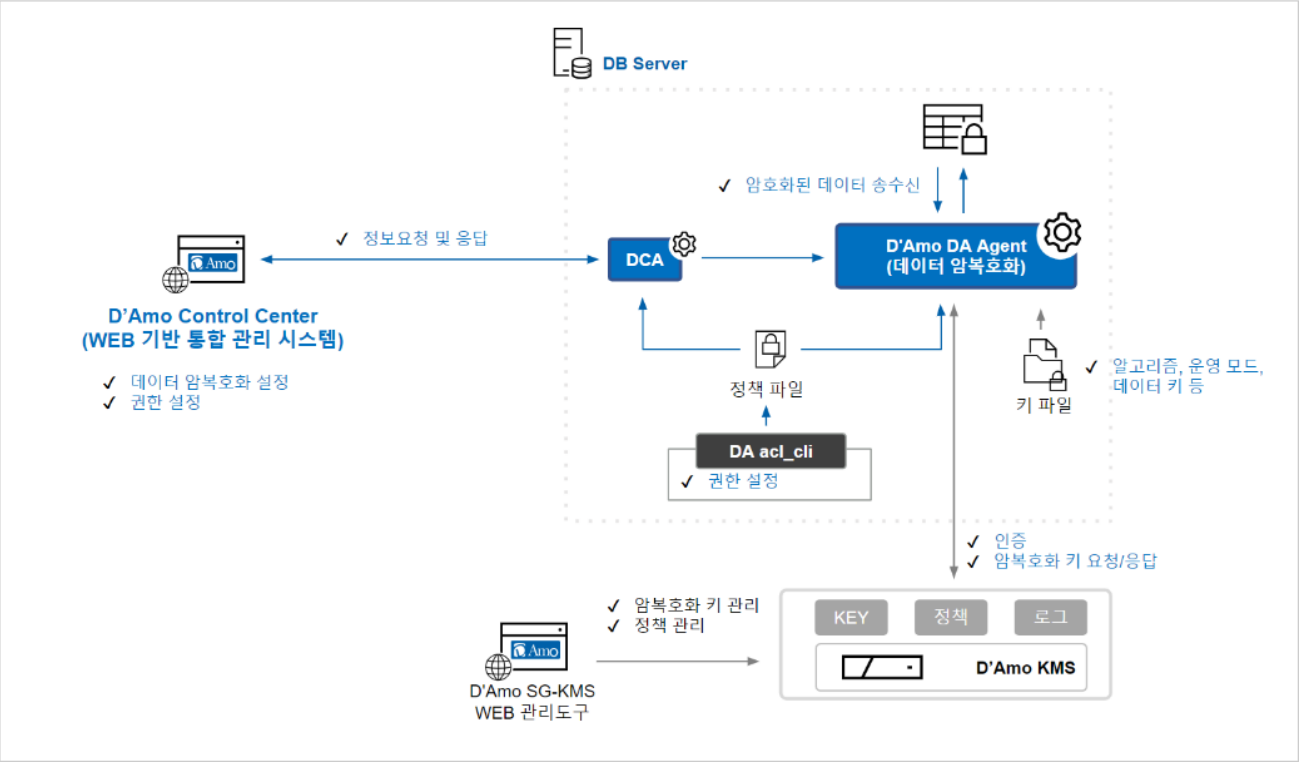
제품 구성

소프트웨어 제품인 D'Amo DA-MYQ는 다음과 같이 구성되어 있다.

D'Amo DA-MYQ 시스템의 구성

D'Amo DA-MYQ를 구성하는 시스템의 각 요소와 주변 제품과의 관계를 아래에 나타낸다.

D'Amo DA-MYQ 시스템의 구성도



각 시스템의 구성 요소와 그 역할은 다음과 같다.

D'Amo DA-MYQ의 구성 요소와 역할

구성 요소	설명
D'Amo Control Center 관리 도구	D'Amo 구성 요소간의 간편한 관리 업무를 지원하며, DCA와 통신할 수 있다.
D'Amo Control Agent(이하 DCA)	D'Amo Control Center 관리도구에서 수행한 작업을 DA-MYQ 로 중계하여 실제 제품이 정상적으로 동작하는지 모니터링하며, D'Amo Control Center 관리도구의 접근 제어를 수행한다.
D'Amo DA Agent(Security Library)	암호화 서버에 설치되는 제품으로써, 사용자에게 데이터 및 파일의 암복호화 API 기능을 제공하는 라이브러리이다.
DA-MYQ acl_cli	사용자 이름 기반으로 암복호화 권한 부여 기능을 제공하는 유틸리티이다.
SG-KMS	암호화 키, 정책, 에이전트 관리 기능을 제공한다.
SG-KMS 관리도구	SG-KMS 기능을 간편하게 사용할 수 있도록 GUI[a]를 제공한다.

a **GUI**: 그래픽 사용자 인터페이스(graphical user interface)

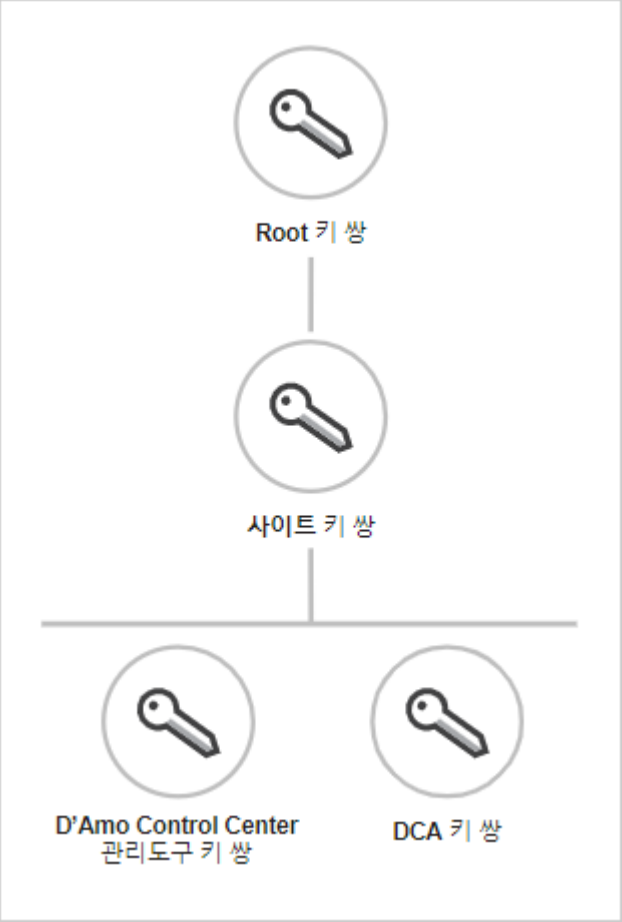
키 시스템

D'Amo DA-MYQ의 키 시스템의 구조 및 구성은 다음과 같다.

D'Amo DA-MYQ 키 시스템의 구조

D'Amo DA-MYQ는 안전한 사용자 인증과 데이터 보호를 위해 **PKI 기반의 다양한 키를 생성·관리**하며, 그 구조는 다음과 같다.

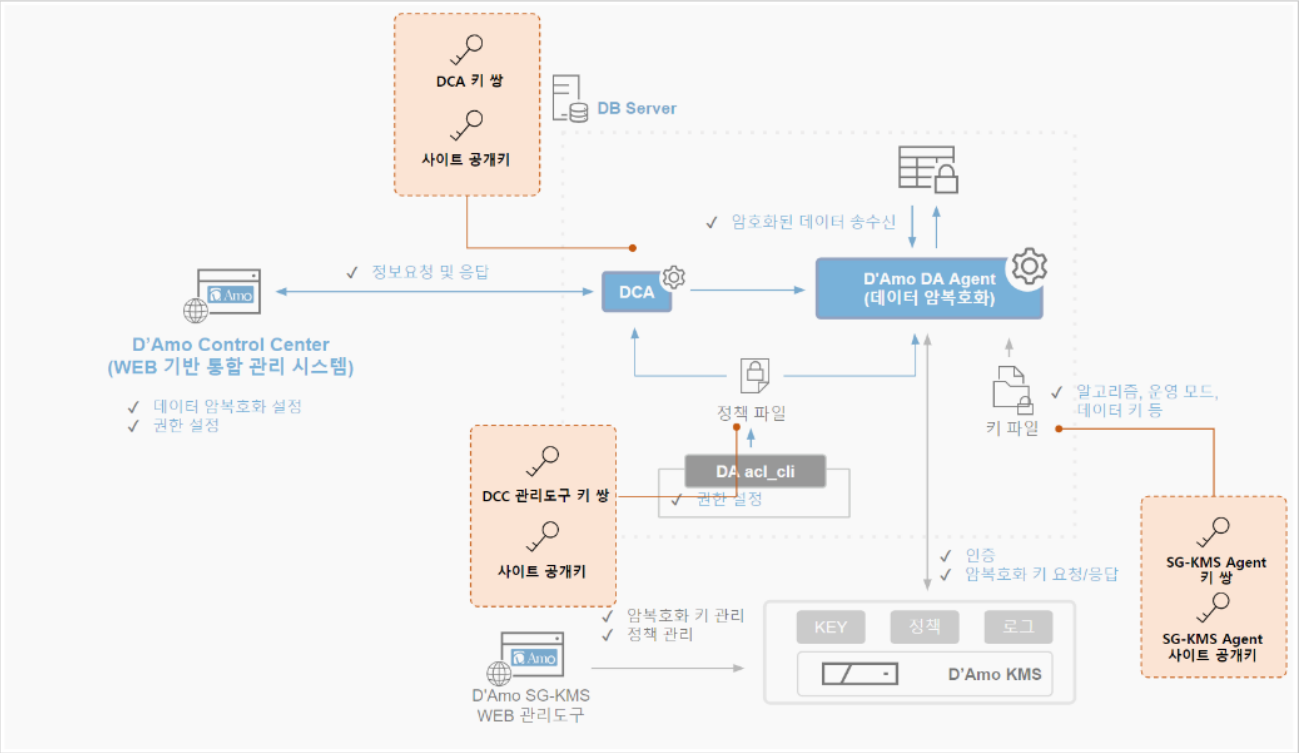
D'Amo DA-MYQ 키 시스템의 구조도



D'Amo DA-MYQ 키 시스템의 구성

D'Amo DA-MYQ 사용을 위한 키의 위치는 다음과 같다.

D'Amo DA-MYQ 키 시스템의 구성도



각 키 시스템의 구성 요소와 역할은 다음과 같다.

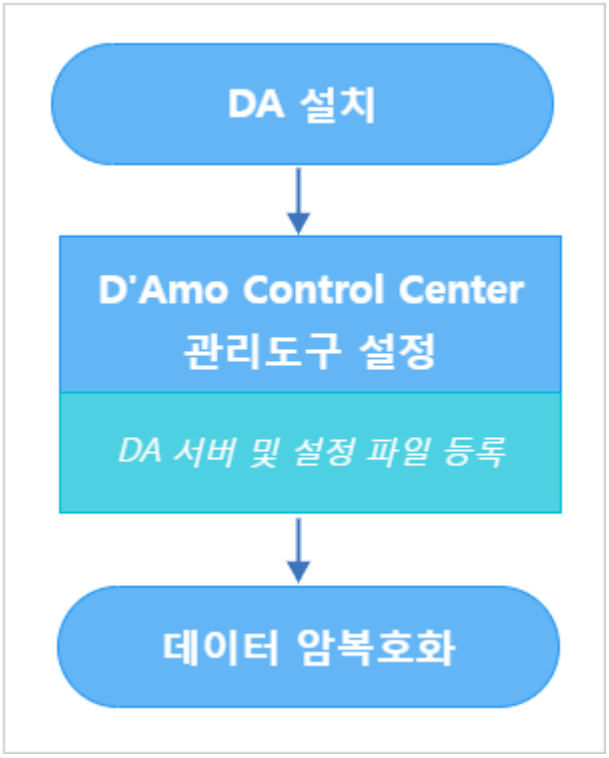
D'Amo DA-MYQ 키 시스템의 구성 요소와 특징

구성 요소	설명
사이트 공개키	D'Amo Control Center와 DA-MYQ간 인증을 위한 키 쌍이다.
D'Amo Control Center 관리도구 키 쌍	D'Amo Control Center의 보안관리자가 인증 및 DCA와의 상호 인증 시에 사용한다.
DCA 키 쌍	DCA가 설치되는 서버에 설치하여 D'Amo Control Center와 각 제품과의 상호 인증 시에 사용한다.
SG-KMS Agent 키 쌍	SG-KMS와 DA-MYQ 간(1:1) 인증 시에 사용한다.
SG-KMS 사이트 공개키	SG-KMS와 DA-MYQ(1:n)가 연동하는 데에 필요한 인증 키 쌍이다.

D'Amo DA-MYQ 동작 과정

D'Amo DA-MYQ 설치부터 암복호화까지의 대략적인 절차는 다음과 같다.

D'Amo DA-MYQ의 동작



파트 I.

설치 및 설정 안내서

여기에서는 고객(또는 엔지니어)가 제품(소프트웨어, 하드웨어)을 설치하기 위한 간략한 절차가 기술되며, 제품의 동작을 확인하기 위한 최소한의 설정 방법을 포함한다.

1.

설치 안내서

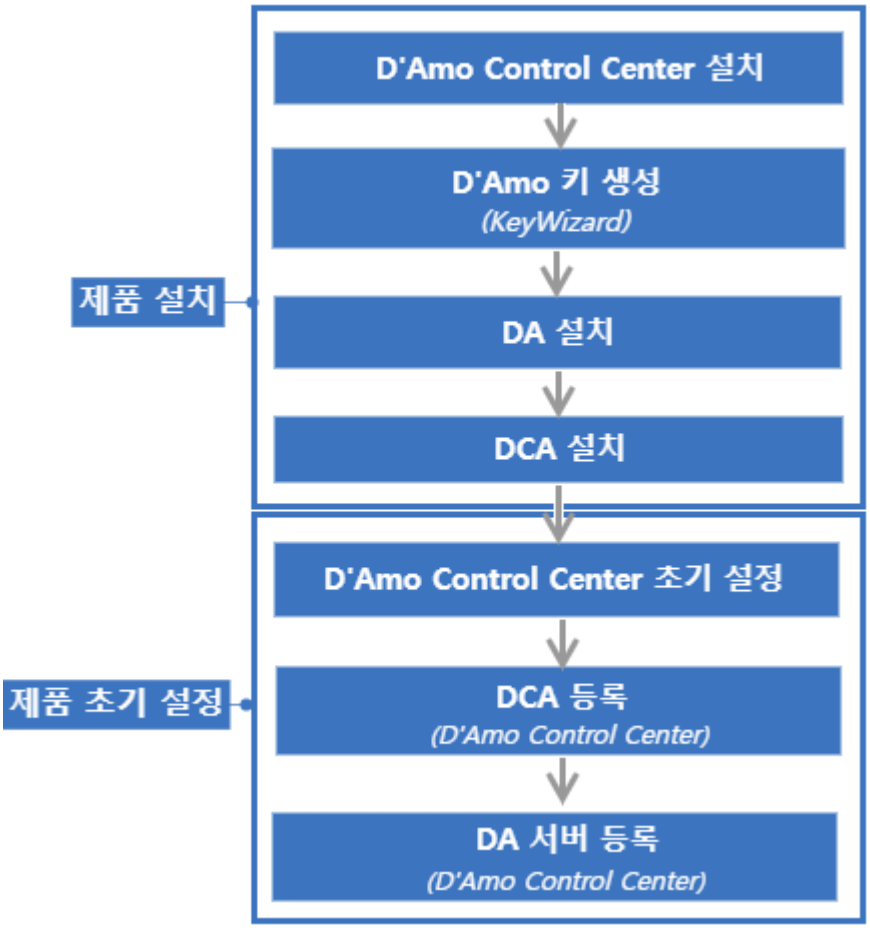
1.1 시작하기 전에

본 안내서는 **DA-MYQ 5.0**을 기반으로 **제품을 설치하는 방법**에 대해 설명한다.

여기에서는 D'Amo Control Center 장비가 설치된 이후, **DA-MYQ를 설치하는 과정부터** 설명한다.

제품 운영을 위해 필요한 설치 및 초기 설정 단계의 전체적인 흐름은 다음과 같다.

그림 1-1 설치 및 설정 단계



여기에서는 설치 단계에 해당하는 DCA 설치 단계까지 설명하고, 설치 이후 단계에 대해서는 DA-MYQ의 <초기 설정 안내서>를 참고한다.

본 안내서에서는 D'Amo Control Center 장비가 설치된 이후, **DA-MYQ를 설치하는 과정부터** 설명한다.

1.2 D'Amo Control Center 설치하기

DA-MYQ 운영을 위해 필요한 D'Amo Control Center의 설치 과정은, <D'Amo Control Center 사용자 설명서 - 설치 안내서>를 참고하여 실시한다.

1.3 D'Amo 키 생성하기

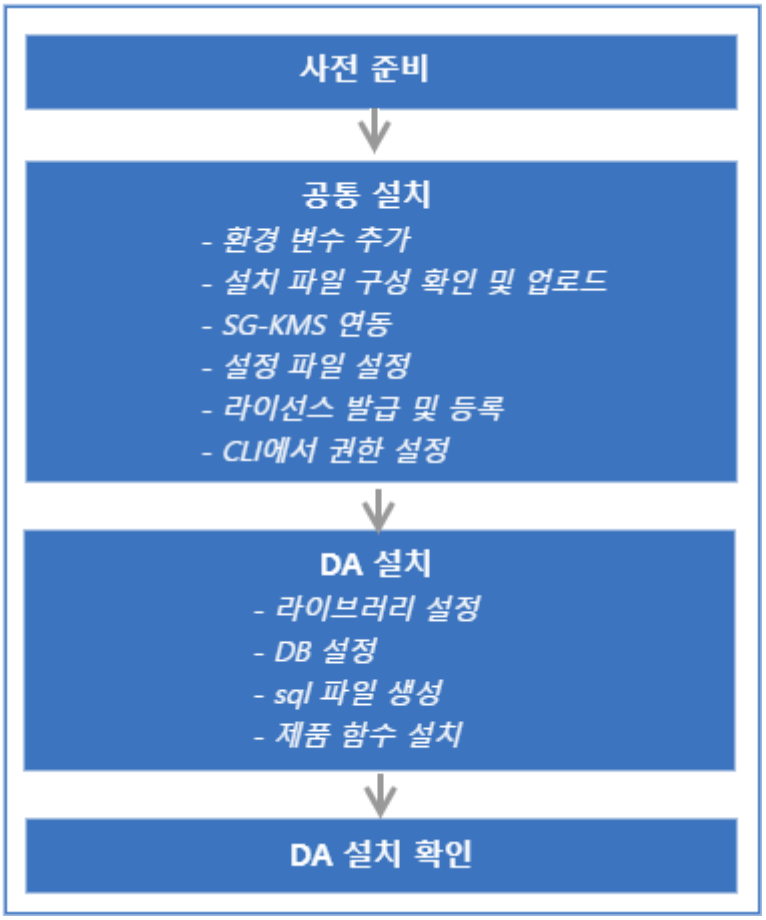
D'Amo Control Center 설치 후 가장 먼저 사이트 키 생성이 필요하다.

제품 운영에 필요한 키 생성 방법에 대해서는, <관리도구 운영설명서 - 화면 구성 요소>의 [키 발급하기]를 참고하여 진행한다.

1.4 DA-MYQ 설치하기

DA-MYQ 설치 절차는 다음과 같다.

그림 1-2 DA-MYQ 설치 절차의 흐름도



1.4.1 사전 준비

DA-MYQ 설치하기 전, 지원 환경을 확인한다.

표 1-1 지원 운영 체제 및 DB 서버

구분	지원 시스템 및 언어
운영 체제	• Linux 2.6 이상 • Windows 10 이상 (Windows Server 2016 이상) ◦ **Windows 8, 2012 및 2012 R2는 제외됨**
DB 서버	MySQL 5.0 이상

다음의 항목을 수행 및 확인한다.

- DB 서버 재시작
- DB 계정명 확인
- DB 서버의 DBA[1] 권한을 소유한 계정 정보 확인
- DB 설치 계정으로 DA-MYQ 디렉터리 생성

1.4.2 공통 설치하기

DA-MYQ 서버를 설치하기 전, 공통 설치를 진행한다.

1.4.2.1 환경 변수 추가하기

DA-MYQ를 설치하기 전, 환경 변수[2]를 추가해야 한다.

DA-MYQ를 설치할 경로는 '**절대 경로**'로 입력하는 것을 권장한다.

Linux의 '**/root**', Windows의 '**바탕화면**' 과 '**C:₩Program Files**' 아래 및 '**공백**'이 포함된 경로로 DA_INST_HOME 설정을 진행할 경우, 접근 권한 등의 이유로 문제가 발생할 수 있기 때문에 해당 경로로 설정하는 것을 권장하지 않는다.

1. **DBA(Database Administrator)**: DB 설치, 구성, 업그레이드, 관리 및 감시하는 일을 맡는 관리자를 의미한다.
2. **환경 변수(Environment Variable)**: 프로세스가 컴퓨터에서 동작하는 방식에 영향을 미치는 동적인 값들의 모임

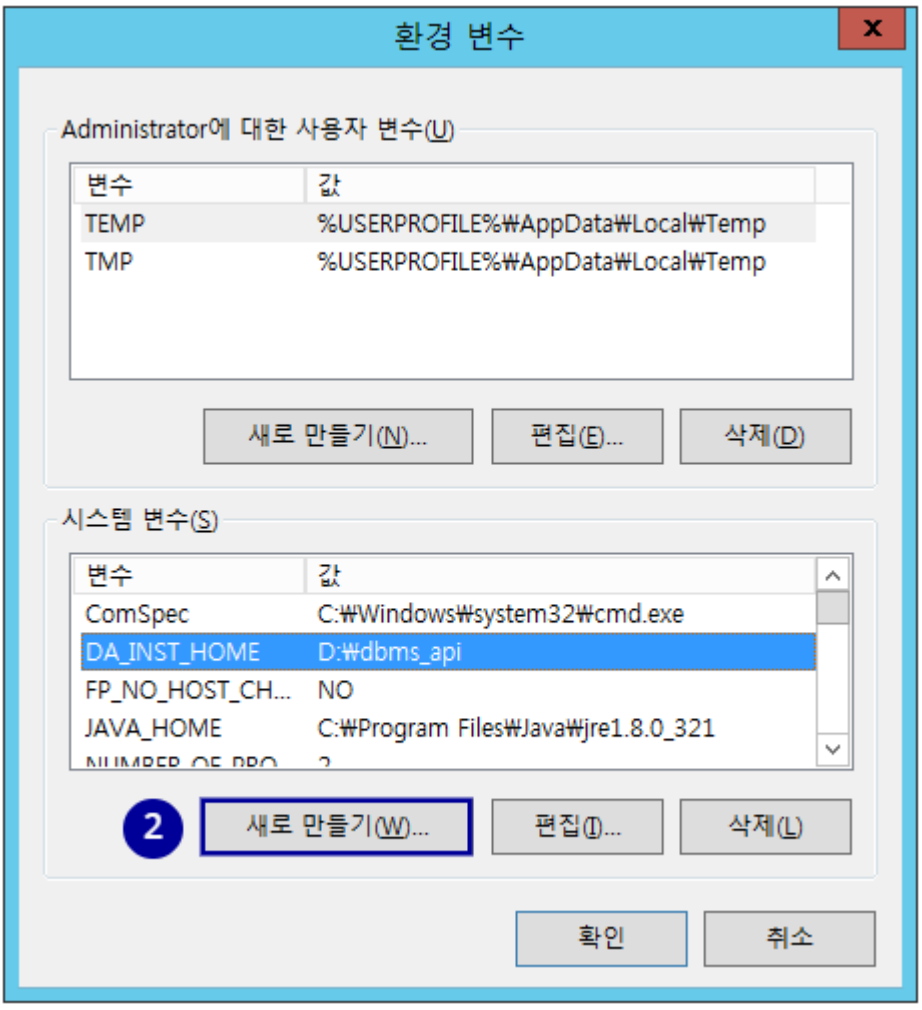
Windows(Windows Server)의 경우

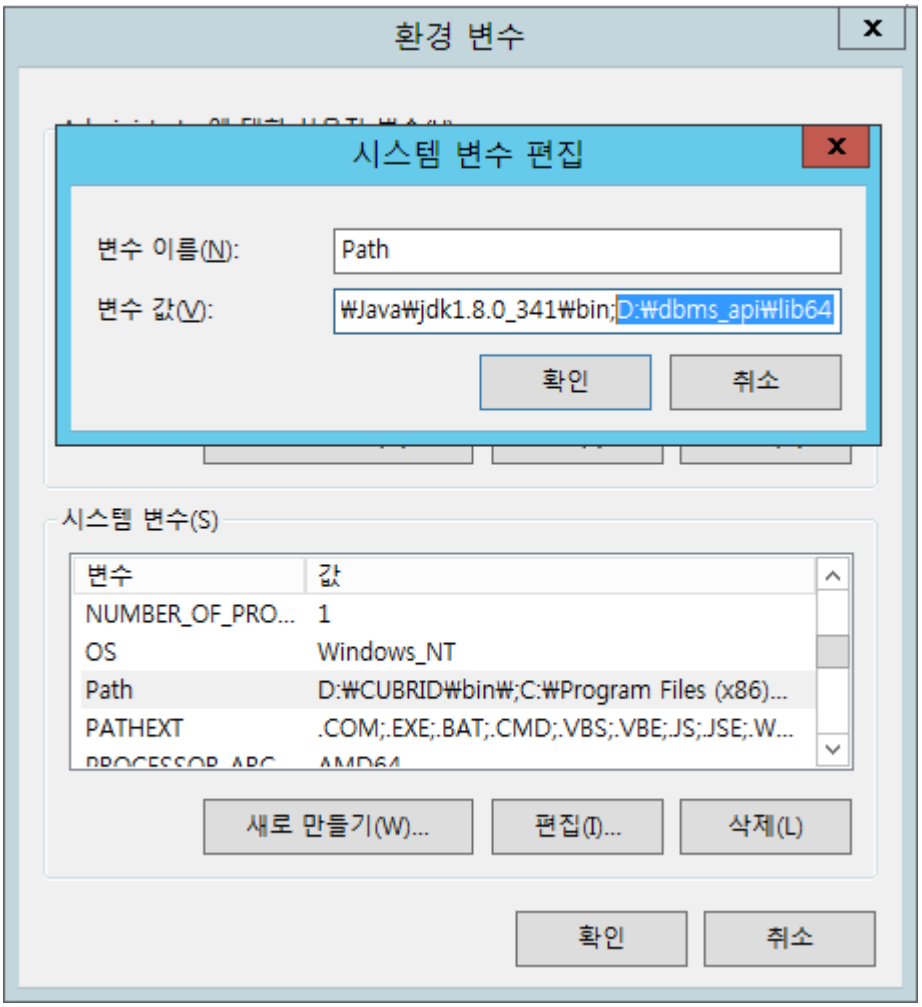
1. **[내 PC] - 마우스 우클릭 [속성] - [고급 시스템 설정]**으로 이동한다.
2. [환경 변수]를 클릭한 후, [시스템 변수] 하단에 위치한 **[새로 만들기]**을 클릭한다.

표 1-2 환경 변수 추가_Windows(Windows Server)

시스템 변수명	설명
DA_INST_HOME	• 해당 변수는 '새로 만들기'한다. • 값에 DA-MYQ를 설치할 경로를 입력한다.
PATH	• 이미 추가되어 있는 PATH 변수에 값을 추가한다. • 값에 DA-MYQ 설치 경로₩lib{bit}를 입력한다.

그림 1-3 환경 변수 설정 화면





3. 환경 변수를 추가한 후, [확인]을 클릭한다.
4. 환경 변수 설정을 적용하기 위하여 Windows를 재시작한다.

Linux(Unix)의 경우

1. 운영하는 Shell 프로파일을 확인한다.
2. 아래의 표를 참고하여, 운영 체제별 라이브러리 경로명을 확인한다.

표 1-3 운영 체제별 라이브러리 경로명

운영 체제	라이브러리 경로명
HP_UX	SHLIB_PATH
AIX	LIBPATH
Linux, SunOS	LD_LIBRARY_PATH

3. Bash Shell을 사용할 경우, .profile 파일에 '**export 변수 이름=변수 값**' 형태로 명령어와 라이브러리 경로명을 입력한다.

```
export DA_INST_HOME=/dbms_api
export LD_LIBRARY_PATH=$DA_INST_HOME/lib64:$LD_LIBRARY_PATH
```

4. C Shell을 사용할 경우, .cshrc 파일에 '**setenv 변수 이름 변수 값**' 형태로 명령어와 라이브러리 경로명을 입력한다.

```
setenv DA_INST_HOME /dbms_api
setenv LD_LIBRARY_PATH /dbms_api/lib64:$LD_LIBRARY_PATH
```

5. MySQL 환경변수를 설정한다.

```
systemctl set-environment DA_INST_HOME="/dbms_api"
```

6. 환경 변수 설정을 적용하기 위하여 MySQL을 재시작한다.

1.4.2.2 설치 파일 구성 확인 및 업로드하기

준비한 Install_DAmo_{제품명}_{버전}_SCP_{SCP 버전}.zip 파일의 압축을 해제할 경우, DCA 설치 패키지는 '**{OS}_{bit}/dca**'경로에 포함되어 있다.

설치 파일 구성을 확인한 후, 다음과 같이 해당 파일을 업로드한다.

1. DA-MYQ 패키지 파일에서 필요한 디렉터리 및 파일을 확인한다.

Windows(Windows Server) 패키지 구성

표 1-4 DA-MYQ 패키지 구성

디렉터리	파일명	설명
WINDOWS_{bit}₩da-myq	• acl_cli.exe • privilege.damo	암복호화 권한을 설정할 수 있는 실행 파일 및 권한 파일
	• scpdb_agent.ini	DA-MYQ 설정 파일
	₩key	D'Amo Control Center에서 발급한 제품 키 쌍 설치 시 사용할 디렉터리
	₩key₩kms	SG-KMS에서 생성한 Agent 키 쌍 설치 시 사용할 디렉터리
	₩log	암복호화 권한 로그가 생성되는 디렉터리
	₩backup	백업파일이 생성되는 디렉터리
WINDOWS_{bit}₩da-myq₩lib{bit}	• ciscc-4.0.dll • damocm-4.0.dll • damoscpdb.dll • logw-0.2.dll	DA-MYQ 라이브러리
	• 001.inner_function.mys	

디렉터리	파일명	설명
WINDOWS_{bit}₩da-myq₩sql	• 002.user_interface.mys • 003.grant_execute_functions.sql • install_make.sh	DA-MYQ DB 함수 설치 파일

Linux 패키지 구성

표 1-5 DA-MYQ 패키지 구성

디렉터리	파일명	설명
Linux_{bit}₩da-myq	• acl_cli • privilege.damo	암복호화 권한을 설정할 수 있는 실행 파일 및 권한 파일
	• scpdb_agent.ini	DA-MYQ 설정 파일
	₩key	D'Amo Control Center에서 발급한 제품 키 쌍 설치 시 사용할 디렉터리
	₩key₩kms	SG-KMS에서 생성한 Agent 키 쌍 설치 시 사용할 디렉터리
	₩log	암복호화 권한 로그가 생성되는 디렉터리
	₩backup	백업파일이 생성되는 디렉터리
Linux_{bit}₩da-myq₩lib{bit}	• libciscc-4.0.so • libdamocm-4.0.so • libdamoscpdb.so • liblogw-0.2.so	DA-MYQ 라이브러리
Linux_{bit}₩da-myq₩sql	• 001.inner_function.mys • 002.user_interface.mys • 003.grant_execute_functions.sql • install_make.sh	DA-MYQ DB 함수 설치 파일

표 1-6 복사할 패키지 및 파일

패키지/키 파일명	설명
{OS}_{bit}₩da-myq	DA-MYQ 설치에 필요한 디렉터리 및 파일
{OS}_{bit}₩da-myq₩lib{bit}	
{OS}_{bit}₩da-myq₩sql	
{OS}_{bit}₩da-myq₩log	
{OS}_{bit}₩da-myq₩backup	

{OS}_{bit}₩da-myq₩key	• D'Amo Control Center v4.0.304.0 이상에서 발급한 제품 키 쌍
	• acl_cli 로그인에 사용되는 키 쌍
	• damo_com_DA(.cer, .key, .spin) 파일을 아래의 이름 형태로 파일명 지정
	  ◦ damo_agt.cer
	  ◦ damo_agt.key

패키지/키 파일명	설명
	◦ damo_agt.spin
{OS}_{bit}₩da-myq₩key₩kms	SG-KMS 연동에 필요한 키 쌍

2. 설치 파일에 접근 권한을 부여한다.

```
cd $DA_INST_HOME
chmod 755 log backup lib{bit}/* acl_cli sql/install_make.sh
```

3. mysql을 구동하는 OS 유저를 확인한다.

```
ps -ef ¦ grep mysqld
```

4. mysql 구동 OS 유저에게 DA_INST_HOME 설정 소유자 권한을 부여한다.

```
chown -R <OS_USER>:<OS_GROUP> $DA_INST_HOME
```

표 1-7 $DA_INST_HOME 소유자 권한 부여

파라미터	설명
OS_USER	• '**mysql**' 을 구동하는 OS 유저를 입력한다.
OS_GROUP	• '**mysql**' 을 구동하는 OS 유저의 그룹을 입력한다.

$DA_INST_HOME이 /dbms_api/da-myq 처럼 '**/**', 하단에 바로 위치 하지 않은 경우, $DA_INST_HOME 상위 폴더인 /dbms_api 폴더 또한 mysql 구동 OS 유저에게 소유자 권한을 부여 해야한다.

1.4.2.3 SG-KMS 연동하기

DA-MYQ는 SG-KMS[3]에서 만든 '암호화 키'를 이용해 데이터를 암복호화 할 수 있다.

표 1-8 SG-KMS의 암호화 키 사용하는 방법

방법	설명
SG-KMS와 연동하기	SG-KMS와 연동하여, SG-KMS에서 만든 암호화 키를 호환하여 사용한다.
SG-KMS의 암호화 키 내보내기	SG-KMS에서 생성한 암호화 키를 '**SCP 키 파일**[a]'로 내보내기 한 후, 사용한다.

a **SCP 키 파일**: .scp 및 .scps 키 파일을 의미함

여기에서는 SG-KMS와 연동하기 위해, SG-KMS에서 DA-MYQ 정보를 등록하고 연동에 필요한 키를 내보내기 하는

3. **SG-KMS**: 암호화 키·암호화 정책 등을 생성 및 관리할 수 있는, 펜타시큐리티(주)의 DB 보안 솔루션

방법에 대해 설명한다.

사전 준비

SG-KMS 연동을 진행하기 전, 다음 사항을 확인한다.

표 1-9 준비 항목

준비 항목	설명	
연동 가능한 SG-KMS 버전 정보	SG-KMS v3.0	v3.0.9.0 이상 지원
	SG-KMS v4.0	• v4.0.104.5 이상 지원 • v4.0.302.0 이상 지원
SG-KMS	• SG-KMS 관리도구 • SG-KMS 관리도구에 접속할 수 있는 아이디 및 비밀번호 • SG-KMS 사용자 설명서	

본 안내서에서는 SG-KMS의 키 종류 및 SG-KMS 관리도구 사용법에 대한 내용은 다루지 않는다. 자세한 사항은 <**SG-KMS 사용자 설명서(SL4)**>를 참고한다.

SG-KMS 버전별 연동 방법

SG-KMS는 버전에 따라 연동하는 방법이 다르다.
연동할 SG-KMS의 버전을 확인한 후, 다음 안내서를 참고하여 연동을 진행한다.

표 1-10 SG-KMS 버전별 연동 방법

SG-KMS 버전	참고 자료
SG-KMS v3.0.9 이상	• <관리도구 사용 설명서>를 참고하여, SG-KMS 연동을 진행한다. • 해당 안내서는 **SG-KMS v3.0.25** 기준으로 작성되었다.
SG-KMS v4.0.104.5 이상	• <D'Amo Agent 연동 안내서>를 참고하여, SG-KMS 연동을 진행한다. • 해당 안내서는 **SG-KMS v4.0.176** 기준으로 작성되었다.
SG-KMS v4.0.302 이상	• <Agent 연동 안내서>를 참고하여, SG-KMS 연동을 진행한다. • 해당 안내서는 **SG-KMS v4.0.302** 기준으로 작성되었다.

1.4.2.4 설정 파일 설정하기

여기에서는 DA-MYQ 운영을 위해, 설정 파일을 수정하는 방법에 대해 설명한다. 설정 이외 항목에 대한 자세한 설명은 <DA-MYQ 운영 설명서>의 '**DA-MYQ 설정 파일**'을 참고한다.

1.4.2.4.1 암호화 키 설정하기

SG-KMS와 연동 또는 키 내보내기를 통해 DA-MYQ에서 사용할 **'암호화 키'**를 가져오기 한다.

해당 키를 사용하기 위해서는, 다음과 같이 설정한다.

1. DA-MYQ의 '**scpdb_agent.ini**' 설정 파일에서 [KEYINFO] 섹션으로 이동한다.
2. 아래의 표를 참고하여, 암호화 키 정보를 입력한다.

표 1-11 KEYINFO 섹션

항목	설명
공통	• KEY1, KEY2, KEY3 등 사용하는 암호화 키 개수에 따라, 항목을 추가할 수 있다. • **주석(#)을 삭제**한 후, 사용한다.
KEY1=ServiceID**(*)**	• SG-KMS와 통신을 하여 '**암호화 키**'를 가져와 데이터를 암복호화 한다. • SG-KMS에서 생성한 서비스 ID 를 입력한다.
#KEY2=SCP_FilePath	• SG-KMS 통신 없이 SCP 키 파일에서 '**암호화 키**'를 가져와 데이터를 암복호화 한다. • SCP 키 파일의 절대 경로, 파일명 및 확장자를 입력한다.
#KEY3=ServiceID,SCP_FilePath	• SG-KMS 통신에 실패할 경우, SCP 키 파일로 내보내기한 '**암호화 키**'를 사용한다. • SG-KMS에서 생성한 서비스 ID와 SCP 키 파일의 절대 경로, 파일명 및 확장자를 함께 입력한다. • 서비스 ID와 SCP 키 파일 정보를 모두 입력할 경우, **공백 없이** 입력한다.

Windows(Windows Server)의 경우

```
[KEYINFO] 예시

KEY1=DA_AES256
KEY2=D:\dbms_api\key\DA_AES256.SCPS
KEY3=DA_AES256,D:\dbms_api\key\DA_AES256.SCPS
```

Linux(Unix)의 경우

```
[KEYINFO] 예시

KEY1=DA_AES256
KEY2=/dbms_api/key/DA_AES256.SCPS
KEY3=DA_AES256,/dbms_api/key/DA_AES256.SCPS
```

3. SG-KMS와 연동한 경우, 설정 파일의 [Server]과 [Server2]를 추가적으로 수정한다.

표 1-12 SERVER 섹션

항목	설명	
Server(*)	ServerIP	• SG-KMS의 IP를 입력한다. • 입력 가능한 IP 수: 최대 10개
	ServerPort	• SG-KMS의 포트를 입력한다. • 기본값: 2525
Server2	ServerIP	• HA 대상인 Slave SG-KMS의 IP를 입력한다.
	ServerPort	• HA 대상인 Slave SG-KMS의 포트를 입력한다. • 기본값: 2525

```
[Server] 예시

ServerIP=192.168.22.25
ServerPort=2525
```

4. 설정 파일의 [AGENT] 섹션을 설정한다.

표 1-13 AGENT 섹션

항목	설명
AgentID(*)	SG-KMS 관리도구에서 설정한 D'Amo Agent의 Agent ID를 입력한다.
SiteCertFilePath(*)	SG-KMS 장비에서 설정한 사이트 공개키(.cer)의 절대 경로 및 파일명을 입력한다.
CertFilePath(*)	SG-KMS 관리도구에서 설정한 D'Amo Agent의 공개키(.cer)의 절대 경로 및 파일명을 입력한다.
KeyFilePath(*)	SG-KMS 관리도구에서 설정한 D'Amo Agent의 개인키(.key)의 절대 경로 및 파일명을 입력한다.
SPIN(*)	• SG-KMS 관리도구에서 설정한 D'Amo Agent의 SPIN 값을 입력한다. • 파일명: damo-scp_PENTA-{Agent명}.spin

Windows(Windows Server)의 경우

```
[AGENT] 예시

AgentID=DA
SiteCertFilePath=D:\dbms_api\key\kms\damo-site_PENTA.cer
CertFilePath=D:\dbms_api\key\kms\damo-scp_PENTA-SA_TEST.cer
KeyFilePath=D:\dbms_api\key\kms\damo-scp_PENTA-SA_TEST.key
SPIN=Tstg3bmj4He6ZnaPxnlF
```

Linux(Unix)의 경우

```
[AGENT] 예시

AgentID=DA
SiteCertFilePath=/dbms_api/key/kms/damo-site_PENTA.cer
CertFilePath=/dbms_api/key/kms/damo-scp_PENTA-SA_TEST.cer
KeyFilePath=/dbms_api/key/kms/damo-scp_PENTA-SA_TEST.key
SPIN=Tstg3bmj4He6ZnaPxnlF
```

키 파일을 DA-MYQ 설치 폴더 하위의 '**key/kms 경로**'에 업로드할 것을 권장한다.

5. 모든 항목을 수정한 후, 설정 파일을 저장한다.

1.4.2.4.2 로그 설정하기

DA-MYQ에서 사용할 로그 생성 경로 및 로그 레벨을 설정한다.

로그 설정을 하는 방법은 다음과 같다.

1. DA-MYQ의 '**scpdb_agent.ini**' 설정 파일에서 [AGENT] 섹션으로 이동한다.
2. 아래의 표를 참고하여, 암호화 키 정보를 입력한다.

표 1-14 [AGENT] 설정

항목	설명
LogDir**(*)**	DA-MYQ의 각종 로그를 생성 할 절대 경로를 입력한다.
LogLevel**(*)**	DA-MYQ의 로그 수준을 입력한다. • 0: NO • 4: LEVEL4_ERROR(기본 값) • 6: LEVEL6_NOTICE • 8: LEVEL8_DEBUG

Windows(Windows Server)의 경우

```
[AGENT] 예시

LogDir=D:\dbms_api\log
LogLevel=4
```

Linux(Unix)의 경우

```
[AGENT] 예시

LogDir=/dbms_api/log
LogLevel=4
```

3. 모든 항목을 수정한 후, 설정 파일을 저장한다.

1.4.2.5 라이선스 발급 및 등록하기

DA-MYQ를 사용하기 위해, ICS[4]에서 라이선스를 발급 받아 등록한다.

1. 환경에 따라, 라이선스를 발급 받는다.
2. 발급 받은 라이선스 파일을 아래의 디렉터리에 복사한다.

표 1-15 환경별 디렉터리 위치

환경	디렉터리 위치
Windows(Windows Server)	%DA_INST_HOME%
Linux(Unix)	$DA_INST_HOME

3. 복사한 라이선스 파일명을 '**damo_lic.cer**'로 변경하여, 라이선스 등록을 완료한다.

1.4.2.6 CLI에서 권한 설정하기

acl_cli을 실행하여 DB 계정별로 암복호화 권한의 정책을 설정한다. 설정된 정책에 따라, 암복호화를 제어한다.

1.4.2.6.1 DA-MYQ acl_cli 실행하기

acl_cli 파일을 실행하여 암복호화 권한을 설정한다.

DA-MYQ acl_cli 실행 시 권한 정보가 변경되기 때문에, 현재 폴더를 포함한 하위 폴더 모두 '**쓰기 권한**'을 가지고 있어야 한다.

1. 환경에 따라, 아래의 디렉터리로 이동한다.

4. **ICS(Intelligent Customer Support)**: 펜타시큐리티(주) 제품의 라이선스를 관리하는 포털 사이트

표 1-16 환경별 디렉터리 위치

환경	디렉터리 위치
Windows(Windows Server)	%DA_INST_HOME%
Linux(Unix)	$DA_INST_HOME

2. 명령어를 입력하여 acl_cli 파일을 실행한다.

Windows(Windows Server)의 경우

```
cd %DA_INST_HOME%
acl_cli.exe -start
```

Linux(Unix)의 경우

```
cd $DA_INST_HOME
./acl_cli -start
```

3. acl_cli 파일을 실행한 경우, Agent 키의 비밀번호를 입력한다.

```
Enter the PIN of CLI-Key : <Agent 키 비밀번호 입력>
```

1.4.2.6.2 DA-MYQ acl_cli 설정하기

DA-MYQ acl_cli 파일을 실행한 후, 정책을 추가하여 DB 계정 단위로 암복호화 권한을 설정한다.

1. *SET PRIV ENC* 명령어를 입력하여, 권한 설정 모드로 이동한다.
2. 아래의 표를 참고하여, 각 파라미터의 값을 입력한다.

```
SET PRIV ENC <USER>"<KEY_NAME>"<ENC>"<DEC>
```

표 1-17 DA-MYQ acl_cli 정책 추가

파라미터	설명
USER(*)	• 권한을 적용하고자 하는 DB의 계정명을 입력한다. • DB에 저장된 DB USER의 대소문자 여부를 확인하고 동일하게 입력해야 한다.
KEY_NAME(*)	• 정책에 할당할 암호화 키명을 입력한다. • 암호화 키명은 scpdb_agent.ini 파일 [KEYINFO] 섹션의 KEY1, KEY2, KEY3과 같은 값을 의미한다. 예) SET PRIV ENC SCP"KEY1"1"1
	해당 계정에 암호화 권한을 부여할지 여부를 설정한다.

파라미터	설명
ENC(*)	• 0: 암호화 권한 미부여 • 1: 암호화 권한 부여
DEC(*)	해당 계정에 복호화 권한을 부여할지 여부를 설정한다. • 0: 복호화 권한 미부여 • 1: 복호화 권한 부여

3. *SAVE ALL* 명령어를 입력하여, 추가한 정책을 저장한다.

```
SAVE ALL
```

표 1-18 DA-MYQ acl_cli 정책 저장

구분	설명
SAVE ALL	• 정책 추가·삭제 후 *SAVE ALL*을 입력하면, 설정한 정책이 저장된다. • 설정한 정책을 저장하지 않을 경우, acl_cli에 적용되지 않는다.

4. *SHOW ALL* 명령어를 입력하여, 추가된 정책이 제대로 적용되어 있는지 확인한다.

```
SHOW ALL
```

5. *SHOW PRIV ENC* 명령어를 입력하여, DB 계정별 암복호화 권한을 조회한다.

```
SHOW PRIV ENC <USER>
```

표 1-19 DA-MYQ acl_cli 정책 조회

파라미터	설명
USER(*)	• DA-MYQ acl_cli에 추가된 특정 DB 사용자의 정책을 조회한다. • 권한이 적용된 DB의 계정명을 입력한다. 예) SHOW PRIV ENC SCP

acl_cli 설정에 대한 자세한 설명은, <**DA-MYQ 운영 설명서**>를 참고한다.

1.4.3 DA-MYQ 설치하기

공통 설치를 완료한 후, DA-MYQ 서버를 설치한다.

1.4.3.1 라이브러리 설정하기

운영 체제에 따라, 라이브러리를 설정한다.

Windows(Windows Server) 패키지 구성

1. {MySQL 설치 경로}₩lib₩plugin 디렉터리로 이동한다.
2. 다음 파일을 설치파일에서 복사하여 라이브러리를 설정한다.

- damoscpdb.dll
- damocm-4.0.dll
- logw-0.2.dll

> 라이브러리 파일이 제대로 인식되지 않을 경우, 위의 파일을 '**C:₩Windows₩System32**' 디렉터리로 복사하여 라이브러리를 설정한다.

Linux의 경우

1. {MySQL 설치 경로}/lib/plugin 디렉터리에 '**libdamoscpdb.so**' 파일을 복제한다.

```
cd {MySQL 설치 경로}/lib/plugin
cp $DA_INST_HOME/libdamoscpdb.so libdamoscpdb.so
```

2. /usr/lib64 디렉터리에 '**libdamocm-4.0.so, liblogw-0.2.so**' 파일을 복제한다.

```
cd /usr/lib64
cp $DA_INST_HOME/libdamocm-4.0.so libdamocm-4.0.so
cp $DA_INST_HOME/liblogw-0.2.so liblogw-0.2.so
```

> 파일 복제 시, root 계정이 필요하다.

1.4.3.2 DB 설정하기

다음과 같이 DB를 설정한다.

1.4.3.2.1 DB 계정 생성하기(권장사항)

제품 운용을 위해, DB에서 DA-MYQ 함수를 사용할 계정 생성을 권장한다.

이 매뉴얼에서는 'SCP' 계정을 비밀번호 'qwer1234'로 생성하였다고 가정한다.

1. *CREATE USER* 명령어를 사용하여 DB 계정을 생성한다.

```
CREATE USER 'SCP'@'%' IDENTIFIED BY 'qwer1234';
CREATE USER 'SCP'@'localhost' IDENTIFIED BY 'qwer1234';
```

2. 권한을 부여한다.

```
GRANT ALL PRIVILEGES ON *.* TO 'SCP'@'%' WITH GRANT OPTION;
GRANT ALL PRIVILEGES ON *.* TO SCP@'localhost' WITH GRANT OPTION;
```

1.4.3.2.2 plugin_dir 설정하기

Windows(Windows Server) 의 경우

1. {MySQL 설치 경로} 디렉터리에서 my.cnf 파일을 열어 plugin_dir 속성 및 {MySQL 설치 경로}₩lib₩plugin 경로를 추가한다.

```
plugin_dir = E:\mysql-5.7.20-winx64\lib\plugin
```

2. {MySQL 설치 경로} 디렉터리에서 my.ini 파일을 생성 후 plugin_dir 속성을 추가하여 damoscpdb.dll 파일이 있는 경로를 설정한다.

```
[mysqld]
basedir=E:\mysql-5.7.20-winx64
datadir=E:\mysql-5.7.20-winx64\data
port=3306

plugin_dir=E:\mysql-5.7.20-winx64\lib\plugin
```

Unix(Linux) 의 경우

1. /etc/ld.so.conf.d 디렉터리에서 mysql_damo.conf 파일을 생성 후 libdamoscpdb.so 파일이 있는 경로를 추가하고 저장한다.

```
/home/dbms_api/lib{bit}
```

2. /etc 디렉터리에서 my.cnf 파일을 열어 plugin_dir 속성 및 {MySQL 설치 경로}/lib/plugin 경로를 추가한다.

```
plugin_dir = /usr/local/mysql/lib/plugin
```

3. *ldconfig* 명령어를 입력해서 변경 내용들을 적용한다.

> *ldconfig* 명령어를 사용할 경우, 암호 모듈의 무결성 값을 저장하는 텍스트 파일(.hmac) 관련 오류가 발생할 수 있다. 이 경우, 제품 구동(LINK)과 관련없기 때문에 무시하고 변경 내용을 적용한다.

4. {MySQL 설치 경로} 디렉터리에서 my.ini 파일을 생성한 후, plugin_dir 속성을 추가하여 libdamoscpdb.so 파일이 있는 경로를 설정한다.

```
[mysqld]
basedir=/usr/local/mysql
datadir=/usr/local/mysql/data
port=3306

plugin_dir=/usr/local/mysql/lib/plugin
```

1.4.3.3 sql 파일 생성하기

다음과 같이 sql 파일을 생성한다.

Windows(Windows Server)의 경우

1. %DA_INST_HOME%₩sql 디렉터리로 이동한다.

```
install_make.bat <D_INI>
```

표 1-20 sql 파일 생성_Windows(Windows Server)

파라미터	설명
D_INI	• '**scpdb_agent.ini**' 설정 파일이 위치한 경로를 입력한다. • scpdb_agient.ini 파일 경로가 D:₩dbms_api일 경우, 다음과 같이 입력한다. 예) install_make.bat D:₩dbms_api

Linux(Unix)의 경우

1. $DA_INST_HOME/sql 디렉터리로 이동한다.

```
./install_make.sh <D_INI>
```

표 1-21 sql 파일 생성_Linux(Unix)

파라미터	설명
D_INI	• '**scpdb_agent.ini**' 설정 파일의 경로를 입력한다. • scpdb_agient.ini 파일 경로가 /home/dbms_api일 경우, 다음과 같이 입력한다. 예) ./install_make.sh /home/dbms_api

2. 다음 파일이 제대로 생성되었는지 확인한다.

- 001.inner_function.mys.sql
- 002.user_interface.mys.sql

1.4.3.4 제품 함수 설치하기

'**{DA-MYQ 설치 디렉터리}/sql**'에서 DB 계정으로 접속한 후, 함수를 설치한다.

다음은 SCP 계정이며, 비밀번호가 qwer1234 일 경우 DB 함수를 설치하는 예이다.

1. $DA_INST_HOME/sql 경로로 이동한다.

```
cd $DA_INST_HOME/sql
```

2. 아래의 명령어를 실행해 DB 함수를 설치한다.

```
mysql [DBNAME] -uSCP -pqwer1234 < 001.inner_function.mys.sql
mysql [DBNAME] -uSCP -pqwer1234 < 002.user_interface.mys.sql
```

Linux에서 Security 기능(SELinux/Apparmor)이 활성화된 환경에서 함수를 설치할 경우, ERROR 1126이 발생할 수 있다. 이 경우, MySQL에 대한 SELinux/Apparmor를 비활성화로 변경한 후 함수 재설치를 진행한다.

3. 특정 DB 사용자에게 함수 실행 권한을 부여한다.

```
mysql [DBNAME] -uSCP -pqwer1234 < 003.grant_execute_functions.sql
```

표 1-22 함수 설치

파라미터	설명
DBNAME	• 설치하려고 하는 database의 이름을 입력한다. • DBNAME이 damodb 일 경우, 다음과 같이 입력한다. 예) mysql damodb -uSCP -pqwer1234 < 003.grant_execute_functions.sql

1.4.4 제품 설치 확인하기

DB 서버 설치까지 완료한 후, 다음 절차에 따라 제품이 제대로 설치되었는지 확인한다.

1. DB에 접속한다.
2. 암복호화 함수를 호출한다.

```
SELEC ENC_STR('<KEY_NAME>', 'abc') AS RESULT; 함수 호출하기
SELECT ENC_STR('KEY1', 'abc') AS RESULT;
+----------------------------------+
¦ RESULT                           ¦
+----------------------------------+
¦ E6878572B3287A049906A8CA57F0207C ¦
+----------------------------------+
1 row in set (0.00 sec)

SELEC DEC_STR('<KEY_NAME>', ENC_STR('<KEY_NAME>', 'abc')) AS RESULT; 함수 호출하기
SELECT DEC_STR('KEY1', ENC_STR('KEY1', 'abc')) AS RESULT;
+----------------+
¦ RESULT         ¦
+----------------+
¦ abc            ¦
+----------------+
1 row in set (0.00 sec)
```

3. 다음 파라미터의 값이 제대로 적용되어 있는지 확인한다.

표 1-23 파라미터 확인

파라미터	설명
KEY_NAME	• 암복호화에 사용하는 키명이다. • 암복호화 키명은 scpdb_agent.ini 파일 [KEYINFO] 섹션의 KEY1, KEY2, KEY3와 같은 값을 의미한다.

1.5 DCA 설치하기

DA-MYQ 운영을 위해 필요한 DCA의 설치 및 설정 과정은 <DCA 설치 안내서> 참고하여 실시한다.

2.

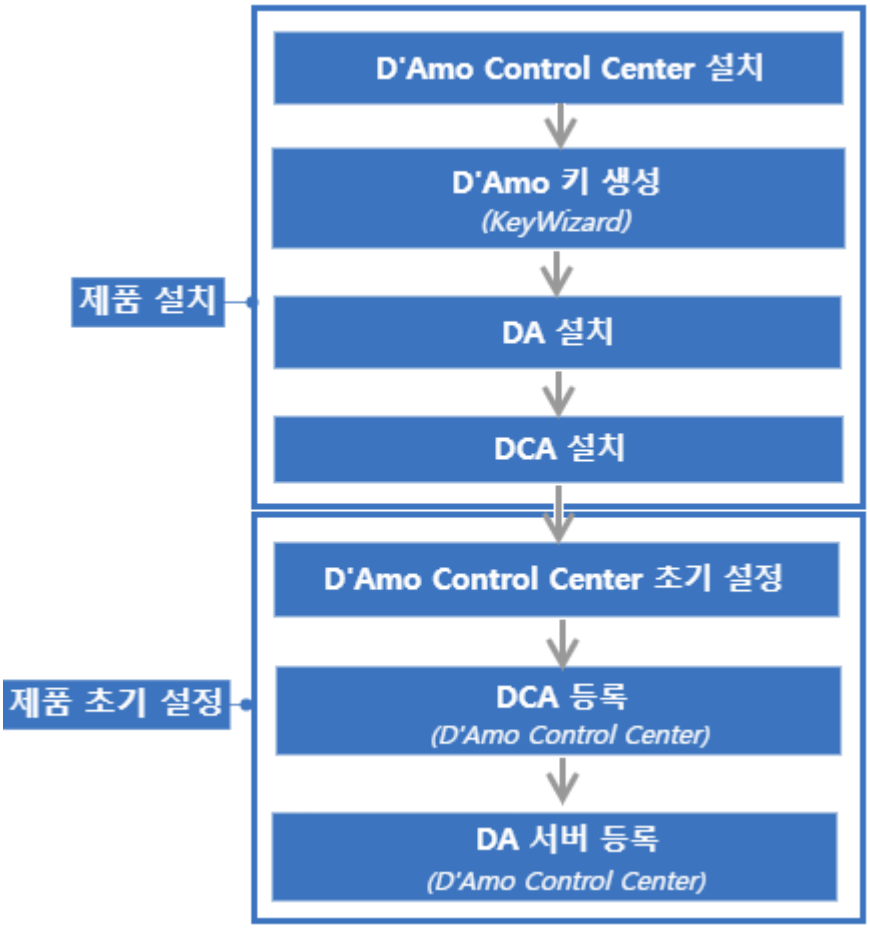
초기 설정 안내서

2.1 시작하기 전에

본 안내서는 D'Amo Control Center, DA-MYQ, DCA 설치를 모두 완료한 후, 각 기능을 사용하기 위해 필요한 **초기 설정에 대해 설명**한다.

제품 설치 완료 후, 초기 설정 단계의 전체적인 흐름은 다음과 같다.

그림 2-1 설치 및 설정 단계



2.2 D'Amo Control Center 초기 설정하기

D'Amo Control Center 설치 후 필요한 초기 설정에 대해서는, <D'Amo Control Center 사용자 설명서 - 초기 설정 안내서>를 참고한다.

2.3 DCA 등록하기

D'Amo Control Center에서 DA-MYQ 서버를 등록 및 관리하기 위해, DCA를 등록해야 한다. DCA 등록에 대해서는, <D'Amo Control Center 사용자 설명서 - 관리도구 운영 설명서>를 참고한다.

2.4 DA-MYQ 서버 등록하기

DA-MYQ가 설치된 서버를 D'Amo Control Center에 등록하는 방법은 다음과 같다.

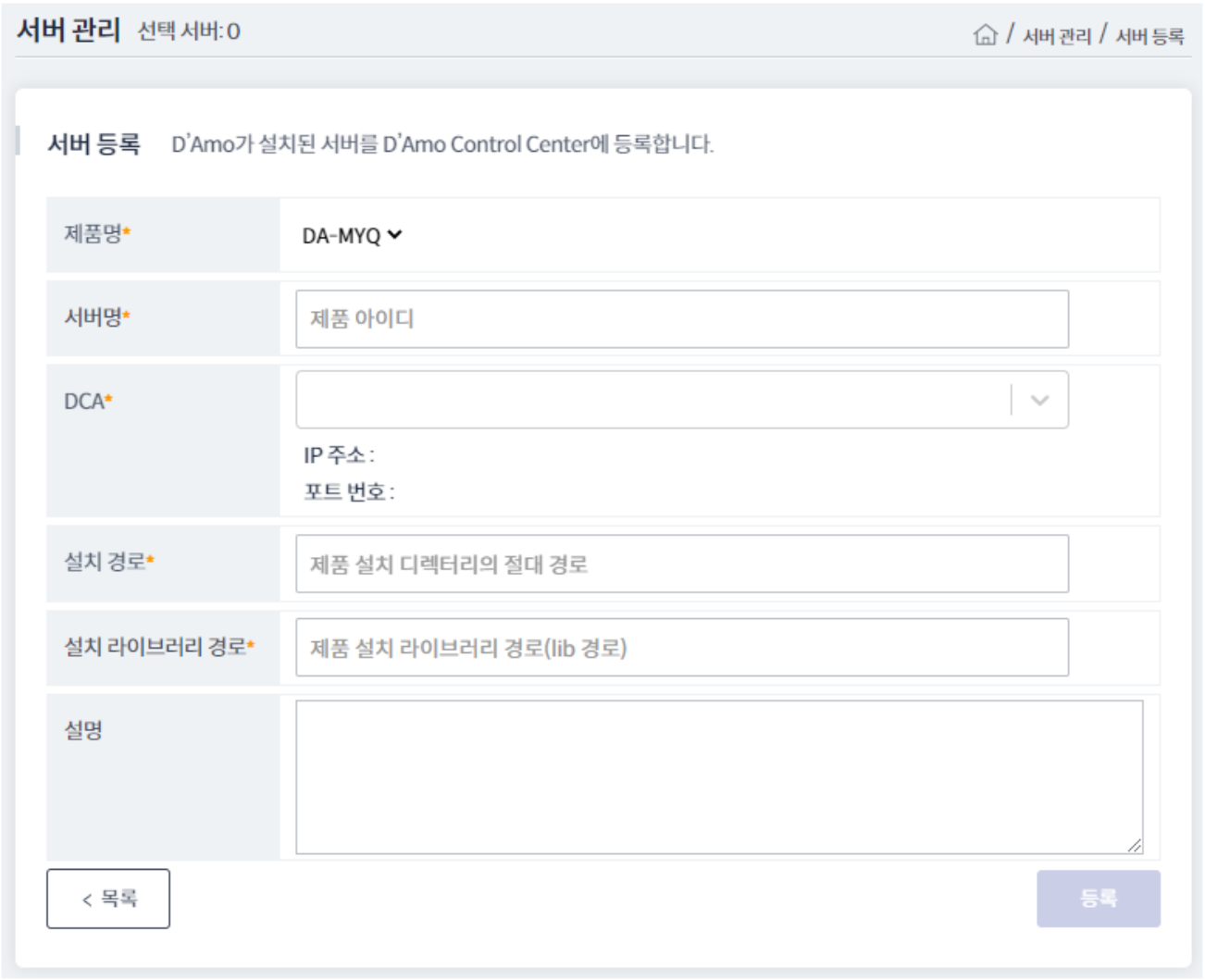
1. 메인 메뉴에서 [서버 관리] - **[서버 등록]**으로 이동한다.
2. **[제품명]**에서 *DA-MYQ*를 선택한다.
3. 아래의 표를 참고하여, 서버 등록 시 필수 입력 항목을 설정한다.

표 2-1 서버 관리_서버 등록

항목		설명
제품명**(*)**		• 등록할 서버의 제품 유형인 DA-MYQ 를 선택한다. • 선택한 제품 유형에 따라, 설정 항목이 출력된다.
서버명**(*)**		• 등록할 DA-MYQ 서버 아이디를 입력한다. • 특수문자(#'") 제외, 모든 문자열로 입력할 수 있다. (1~128자)
DCA**(*)**	IP 주소	• 등록할 DA-MYQ 서버의 DCA IP 주소를 입력한다. • 모든 문자열로 입력할 수 있다. (1~2000자)
	포트 번호	• 등록할 DA-MYQ 서버의 DCA 포트 번호를 입력한다. • 숫자만 입력할 수 있다. (0~65535)
설치 경로**(*)**		• DA-MYQ 서버가 설치된 절대 경로를 입력한다. • 모든 문자열로 입력할 수 있다. (1~255자)
설치 라이브러리 경로**(*)**		• DA-MYQ 서버의 라이브러리가 설치된 폴더의 절대 경로를 입력한다. • 모든 문자열로 입력할 수 있다. (1~255자)
		• 등록할 서버에 대한 추가 정보를 입력한다.

항목	설명
설명	• 한글, 영문자, 숫자, 특수문자 (!,@,$,&,(,),_,+,-,=,:,',,,.)만 입력할 수 있다. (0~512자)

그림 2-2 DA-MYQ 서버 등록하기



4. DA-MYQ 서버 정보를 입력한 후, **[등록]**을 클릭한다.
5. 정상적으로 서버 등록이 완료되면, [서버 목록]에서 해당 서버 정보를 확인할 수 있다.

3.

삭제 안내서

3.1 시작하기 전에

본 안내서는 **제품의 잘못된 설치 또는 마이그레이션 시**에 **정상적으로 제품을 삭제하기 위해** 작성되었다. 이는 일반 프로그램과는 달리 정확한 절차에 따라 삭제되어야 올바른 후속 작업이 진행되므로 다음 안내에 따라 진행한다.

DA-MYQ 5.0 기준으로 DA-MYQ의 삭제 절차는 다음과 같다.

3.2 DA-MYQ 삭제하기

다음 절차에 따라, DA-MYQ 삭제를 진행한다.

3.2.1 암호화 해제하기

다음 순서에 따라, 암호화 해제를 진행한다.

1. 암호화된 데이터가 존재하는지 확인한다.
2. 암호화된 데이터가 있을 경우, 복호화 함수를 호출하여 '**암호화 해제**'를 진행한다.
    - 다음 파라미터를 참고하여, 복호화 함수를 사용한다.

표 3-1 명령어 파라미터

파라미터	설명
I_KEY	• 암복호화 시 사용하는 암호화 키명 • 암호화 키명은 scpdb_agent.ini 파일의 [KEYINFO] 섹션에서 KEY1, KEY2, KEY3와 같은 값

파라미터	설명
ENC_TABLE	암호화 데이터가 저장된 컬럼이 있는 테이블
ENC_COLUMN	암호화 데이터가 저장된 컬럼

ENC_STR 함수로 암호화한 경우

```
# UPDATE <ENC_TABLE> SET <ENC_COLUMN>=DEC_STR('<I_KEY>', <ENC_COLUMN>); 호출하기
UPDATE EMPOLYEE SET JUMIN_NO=DEC_STR('KEY1', JUMIN_NO);
```

ENC_B64 함수로 암호화한 경우

```
# UPDATE <ENC_TABLE> SET <ENC_COLUMN>=DEC_B64('<I_KEY>', <ENC_COLUMN>); 호출하기
UPDATE EMPOLYEE SET JUMIN_NO=DEC_B64('KEY1', JUMIN_NO);
```

3.2.2 DB 함수 삭제하기

DROP FUNCTION 명령어를 사용하여 함수를 제거한다.

```
DROP FUNCTION IF EXISTS ENC_STR;
DROP FUNCTION IF EXISTS ENC_B64;
DROP FUNCTION IF EXISTS DEC_STR;
DROP FUNCTION IF EXISTS DEC_B64;
DROP FUNCTION IF EXISTS ENC_STR_FPE;
DROP FUNCTION IF EXISTS ENC_B64_FPE;
DROP FUNCTION IF EXISTS DEC_STR_FPE;
DROP FUNCTION IF EXISTS DEC_B64_FPE;
DROP FUNCTION IF EXISTS INDEX_STR;
DROP FUNCTION IF EXISTS DEC_INDEX_STR;
DROP FUNCTION IF EXISTS DEC_INDEX_B64;
DROP FUNCTION IF EXISTS HASH_STR;
DROP FUNCTION IF EXISTS HASH_B64;
DROP FUNCTION IF EXISTS HEXTOB64;
DROP FUNCTION IF EXISTS B64TOHEX;
DROP FUNCTION IF EXISTS CONFIG_REINIT;
```

```
DROP FUNCTION IF EXISTS ScpEnc_Str;
DROP FUNCTION IF EXISTS ScpEnc_B64;
DROP FUNCTION IF EXISTS ScpDec_Str;
DROP FUNCTION IF EXISTS ScpDec_B64;
DROP FUNCTION IF EXISTS ScpIndex_Str;
DROP FUNCTION IF EXISTS ScpDecIndex_Str;
DROP FUNCTION IF EXISTS ScpDecIndex_B64;
DROP FUNCTION IF EXISTS ScpHash_Str;
DROP FUNCTION IF EXISTS ScpHash_B64;
DROP FUNCTION IF EXISTS ScpHex_TO_B64;
DROP FUNCTION IF EXISTS ScpB64_TO_Hex;
DROP FUNCTION IF EXISTS ScpConfig_ReInit;
DROP FUNCTION IF EXISTS raise_error;
```

3.2.3 DB 설정하기

각 환경에 따라, 다음과 같이 DB를 설정한다.

Windows(Windows Server)의 경우

1. {MySQL 설치 경로} 디렉터리에서 my.cnf 파일을 열어 plugin_dir 속성 및 {MySQL 설치 경로}/lib/plugin 경로를 삭제한다.

2. {MySQL 설치 경로} 디렉터리에서 my.ini 파일을 열어 plugin_dir 속성 및 damoscpdb.dll 파일이 있는 경로를 삭제한다.

Unix(Linux)의 경우

1. /etc/ld.so.conf.d 디렉터리에서 mysql_damo.conf 파일을 삭제한다.

```
rm -rf /etc/ld.so.conf.d/mysql_damo.conf
```

2. {MySQL 설치 경로} 디렉터리에서 my.cnf 파일을 열어 plugin_dir 속성 및 {MySQL 설치 경로}/lib/plugin 경로를 삭제한다.

3. *ldconfig* 명령어를 입력해서 변경 내용들을 적용한다.

ldconfig 명령어를 사용할 경우, 암호 모듈의 무결성 값을 저장하는 텍스트 파일(.hmac) 관련 오류가 발생할 수 있다. 이 경우, 제품 구동(LINK)과 관련없기 때문에 무시하고 변경 내용을 적용한다.

4. {MySQL 설치 경로} 디렉터리에서 my.ini 파일을 열어 plugin_dir 속성 및 libdamoscpdb.so 파일이 있는 경로를 삭제한다.

3.2.4 라이브러리 삭제하기

Windows(Windows Server) 의 경우

다음 파일을 {MySQL 설치 경로}₩lib₩plugin 디렉터리에서 삭제한다.

- damoscpdb.dll
- damocm-4.0.dll
- logw-0.2.dll

Unix(Linux) 의 경우

1. 아래의 명령어를 실행하여, {MySQL 설치 경로}/lib/plugin 디렉터리에서 삭제한다.

```
cd {MySQL 설치 경로}/lib/plugin
rm -rf libdamoscpdb.so
```

2. /usr/lib64 디렉터리에 libdamocm-4.0.so, liblogw-0.2.so} 파일을 삭제한다.

```
cd /usr/lib64
rm -rf libdamocm-4.0.so
rm -rf liblogw-0.2.so
```

심볼릭 링크 삭제 시, root 계정이 필요하다.

3.2.5 설치 디렉토리 삭제하기

1. DA-MYQ가 설치된 디렉터리를 삭제한다.

Windows(Windows Server)의 경우

```
echo %DA_INST_HOME%
rmdir /s %DA_INST_HOME%
```

Linux(Unix)의 경우

```
echo $DA_INST_HOME
rm -rf $DA_INST_HOME
```

2. DA-MYQ 설치 디렉터리가 삭제되었는지 확인한다.

Windows(Windows Server)의 경우

```
dir %DA_INST_HOME%
파일을 찾을 수 없습니다.
```

Linux(Unix)의 경우

```
ls -al $DA_INST_HOME
No such file or directory
```

파트 II.

운영 설명서

여기에서는 제품 설치 및 설정 완료 후 제품 운영 시에 필요한 기본적인 설명을 포함하며 구체적으로는 다음과 같은 내용을 다룬다.

- Hidden 기능을 제외한 모든 기능과 그 사용법
- 설정 파일의 입력 값 설명
- 오류 발생 시의 대응 방안 및 오류 코드 일람 등

제품에는 하드웨어와 소프트웨어를 모두 포함한다.

1.

관리도구 운영 설명서

1.1 시작하기 전에

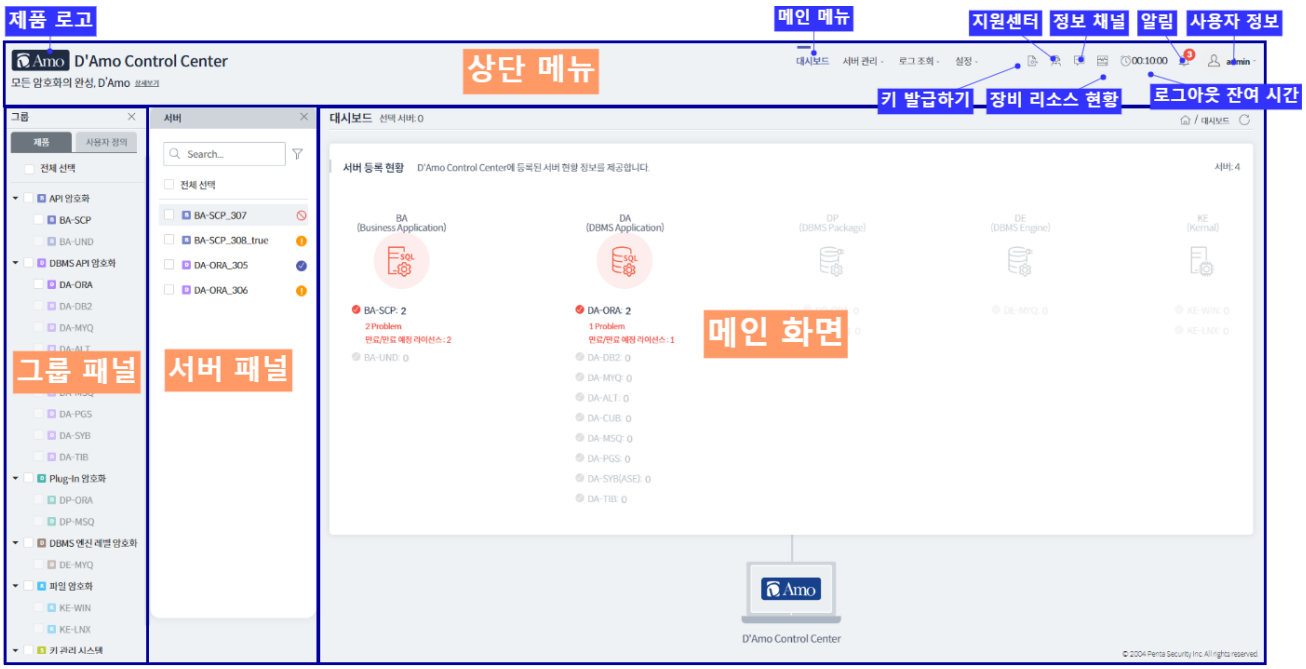
본 설명서는 **DA-MYQ 5.0**을 기반으로, DA-MYQ 입문자가 D'Amo Control Center 관리도구를 통해 **DA-MYQ 서버 설정을 보다 쉽게 운영**할 수 있도록 작성되었다.

DA-MYQ 서버 관리 이외의 기능에 대한 자세한 설명은 D'Amo Control Center의 **<관리도구 운영 설명서>**를 참고한다.

1.2 화면 구성

여기에서는 DA-MYQ 운영에 필요한 서버 관리 기능에 한해 설명하기 때문에, 서버 관리 화면 기준으로 화면 구성 요소에 대해 설명한다.

그림 1-1 D'Amo Control Center의 첫 화면



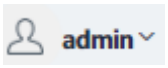
1.2.1 상단 메뉴와 메인 화면

관리도구의 가장 상위에 고정된 메뉴바인 **상단 메뉴**와, 화면에서 유일하게 변동되는 **메인 화면**의 구성 요소는 다음과 같다.

표 1-1 화면 구성 요소_상단 메뉴와 메인 화면

구분	구분	아이콘	설명
	제품 로고	D'Amo Control Center	선택 시 첫 화면으로 이동한다.
	D'Amo 제품 개요	모든 암호화의 완성, D'Amo 상세보기	[상세보기] 버튼 클릭 시, D'Amo 제품 관련 계층 관련 그림을 제공한다.
	메인 메뉴	-	대시보드, 서버 관리, 로그 조회, 설정과 같은 주요 기능을 다룰 수 있는 메뉴를 제공한다.
	지원센터 바로가기		펜타시큐리티의 지원센터 홈페이지로 이동할 수 있는 링크를 제공한다.
			• 제품 키를 발급하는 기능을 제공한다. • 해당 아이콘 클릭 시, '키 발급하기' 팝업에서 타입 선택 후 설정할 비밀번호를 입력하면 사이트 및 제품

구분	구분	아이콘	설명
상단 메뉴	키 발급하기		인증서, 키를 발급 받을 수 있다. (포맷: .zip) ◦ DP-ORA, DP-MSQ 제품의 경우 키 로딩 방식을 추가로 선택해야한다. ◦ 비밀번호 입력 조건 ▪ 영문자, 숫자, 특수문자의 조합으로 구성한다. ▪ 특수문자는 다음 중 1문자 이상을 포함한다. ((,), !, @, $, &, *, _, +, -, =, ₩, :, ', ,, .) ▪ 3자 이상의 연속된 문자열(ex. 123, 321, abc, cba 등)과 3자 이상 동일한 문자열(ex. aaa, 111 등)은 설정할 수 없다.
	정보 채널 바로가기		펜타시큐리티의 카카오톡 정보 채널 홈페이지로 이동할 수 있는 링크를 제공한다.
	제품 리소스 현황 조회		DCC 서버의 CPU, 메모리, 디스크의 사용 현황을 툴팁으로 제공한다.
	로그아웃 잔여 시간		• 로그인 후, 자동 로그아웃까지 남은 시간을 보여준다. • 관리도구 브라우저 위에서 마우스의 움직임이 포착될 때, 로그아웃 잔여 시간이 초기화된다.
	알림		유지보수 코드 미등록, 유지보수 코드 만료 예정, 라이선스 만료 및 만료 예정, 설정 템플릿 적용 결과 등 DCC에서 발생하는 알림을 툴팁으로 확인할 수 있게 제공한다.
			현재 관리도구에 로그인한 계정 아이디와 함께 다음의 추가 정보를 제공한다. • 언어: 관리도구의 언어 설

구분	구분	아이콘	설명
	사용자 정보		정 • 로그아웃: 클릭 시 관리도구에서 로그아웃 • 관리도구 버전 정보: 현재 접속한 관리도구 버전의 상세 정보
메인 화면	-	-	상단 메뉴에서 선택된 메뉴에 해당하는 정보를 화면에 표시한다.
	숨김 패널		• 숨김 처리한 그룹 및 서버 패널의 책갈피 형태이다. • 각 책갈피를 클릭하면 해당 패널이 다시 화면 좌측에 펼쳐진다.

1.2.2 그룹 패널

D'Amo 제품별로 그룹핑한 목록을 트리 구조로 표시하는 '제품' 탭과 사용자가 추가한 그룹 정보를 트리 구조로 보여주는 '사용자 정의' 탭이 존재한다.

기본적으로 보여지는 탭은 '제품' 탭이며 [설정]-[시스템]-[그룹 패널 기본 탭] 에서 초기 세팅 시 보여질 탭을 설정할 수 있다.

'제품' 탭의 경우 아래와 같은 기능을 제공한다.

표 1-2 화면 구성 요소_그룹 패널_제품탭

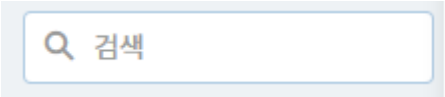
구분	아이콘	설명
제품 목록		그룹핑된 제품군 목록을 트리 구조로 제공하며, 관리도구 설치 여부에 따라 다음과 같이 표시된다. • 설치 제품 ◦ 활성화 상태로 표시되고 선택 박스 체크 시 우측 '서버 패널'에 표시된다. • 미설치 제품 ◦ 비활성화 상태로 표시되고 해당 항목은 선택할 수 없다. • 첫 계층의 체크박스 왼쪽에 역삼각형을 클릭하여 해당 제품군을 접거나 펼칠 수 있다.
라벨		제품군에 따라 부여된 고유 라벨로 서버 패널에서도 동일하게 표현된다.
제품 개요		• 각 제품명에 마우스 오버 시, 항목 우측에 표시되는 아이콘이다.

구분	아이콘	설명
		• 에 다시 마우스 오버하면, 해당 제품에 대한 간략한 소개가 툴팁으로 제공된다.
닫기		• 클릭 시 화면에서 해당 패널이 숨김 처리되고, 나머지 우측 화면이 확장된다. • '메인 화면' 좌측에 숨겨진 패널이 책갈피 형태로 만들어지고 해당 책갈피를 클릭하면 다시 패널이 펼쳐진다.

'사용자 정의' 탭의 경우 아래와 같은 기능을 제공하며, 이 탭의 이름은 [설정]-[시스템]-[사용자 정의 그룹 패널명] 에서 수정할 수 있다.

만약, 설정한 이름이 긴 경우에는 말줄임표 처리하며 툴팁으로 전체 설정 값을 확인할 수 있다.

표 1-3 화면 구성 요소_그룹 패널_사용자 정의 탭

구분	아이콘	설명
검색		• 등록된 그룹을 검색할 수 있는 기능을 제공한다. • 검색 기준은 그룹의 이름을 이용한다.
그룹 목록		• 사용자가 등록된 그룹을 트리 형식으로 표시한다. • 자신이 권한을 보유하고 있는 그룹만 보여진다. ◦ 보안관리자의 경우에는 등록되어있는 모든 그룹이 보여진다. • 트리 형식의 첫 계층은 그룹 카테고리이며 두 번째 계층은 서버 그룹을 나타낸다. • 첫 계층 옆에 역삼각형 아이콘을 클릭하여 해당 그룹 카테고리에 속한 내용을 접어서 숨기거나 다시 클릭하여 접힌 내용을 펼칠 수 있다.

1.2.3 서버 패널

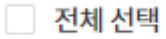
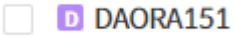
그룹 패널에서 선택한 제품별 서버 목록을 표시하고, 선택된 제품이 없는 경우에는 등록된 전체 서버 목록을 보여준다.

- 현재 로그인한 계정이 해당 그룹의 권한을 보유하고 있더라도, 그룹 권한이 부여되지 않은 서버라면 표시되지 않는다. 필요한 경우 보안관리자가 서버에 그룹 권한을 부여할 수 있다.

서버 패널을 구성하는 각 요소와 제공하는 기능은 다음과 같다.

표 1-4 화면 구성 요소_서버 패널

구분	아이콘	설명
검색창		서버 항목 전체에 대한 '사용자 지정 검색'이 가능하다. • 아이디 기반으로 검색할 수 있으며, 입력 문자열이 포함된

구분	아이콘	설명
		아이디를 가진 서버 목록만 필터링 된다.
필터		서버 항목 전체에 대한 상태 별 필터 기능을 제공한다.
전체 선택		현재 보여지는 모든 서버를 선택하는 기능을 제공한다.
서버		• 선택한 서버의 연결 상태는 아이콘을 통해 표시한다. ◦ 헬스 체크가 OFF로 설정된 서버의 경우, 서버 연결 상태를 나타내는 아이콘은 표시되지 않는다. • 마우스 오버 시 다음의 정보를 제공한다. ◦ 서버명 ◦ 서버 상태 ◦ IP 주소 ◦ 포트 번호 ◦ 라이선스 상태 ◦ 라이선스 만료일 ◦ 최종 헬스 체크 시간 ◦ 최근 사용일 ▪ 실제로 제품을 통해 암호화가 이루어진 날짜를 제공한다. • 체크 박스를 이용하여 해당 서버를 선택할 수 있다.
서버 상태		• 서버 상태 아이콘은 헬스 체크가 ON으로 설정되어야만 표시된다. • 헬스 체크가 정상적으로 이루어진 서버의 경우 해당 아이콘이 표시되고, 마우스 오버 시 다음 정보를 제공한다. ◦ 서버 상태: '정상 연결'로 표시
		• 서버 상태 아이콘은 헬스 체크가 ON으로 설정되어야만 표시된다. • 헬스 체크에 실패한 서버의 경우 해당 아이콘이 표시되고, 마우스 오버 시 다음 정보를 제공한다. ◦ 서버 상태: '에러'로 표시 • 에러 아이콘 클릭 시 다음과 같은 내용을 팝업으로 표시한다. ◦ 메시지: 오류가 발생한 원인과 해결 방안을 제시
		• 해당 서버의 라이선스가 만료됐을 때 표시된다. • 만료 아이콘 클릭 시 다음과 같은 내용을 팝업으로 표시한다. ◦ 메시지: 라이선스 만료로 인한 관리도구 사용 불가 내용 및 문의 메일 주소 안내
닫기		• 클릭 시 화면에서 해당 패널이 숨김 처리되고, 반대 방향의 화면이 확장된다. • '메인 화면' 좌측에 숨겨진 패널이 책갈피 형태로 만들어지고 해당 책갈피를 클릭하면 다시 패널이 펼쳐진다.

1.3 서버 등록

DA-MYQ 가 설치된 서버를 D'Amo Control Center 관리도구에 등록한다.

관리도구 화면에서 공통적으로 사용되는 각 아이콘의 기능은 <관리도구에서 사용되는 아이콘과 버튼 >을 참고한다.

표 1-5 서버 관리_서버 등록

항목		설명
제품명**(*)**		• 등록할 서버의 제품 유형인 DA-MYQ 를 선택한다. • 선택한 제품 유형에 따라, 설정 항목이 출력된다.
서버명**(*)**		• 등록할 DA-MYQ 서버 아이디를 입력한다. • 특수문자(#'") 제외, 모든 문자열로 입력할 수 있다. (1~128자)
DCA**(*)**	IP 주소	• 등록할 DA-MYQ 서버의 DCA IP 주소를 입력한다. • 모든 문자열로 입력할 수 있다. (1~2000자)
	포트 번호	• 등록할 DA-MYQ 서버의 DCA 포트 번호를 입력한다. • 숫자만 입력할 수 있다. (0~65535)
설치 경로**(*)**		• DA-MYQ 서버가 설치된 절대 경로를 입력한다. • 모든 문자열로 입력할 수 있다. (1~255자)
설치 라이브러리 경로**(*)**		• DA-MYQ 서버의 라이브러리가 설치된 폴더의 절대 경로를 입력한다. • 모든 문자열로 입력할 수 있다. (1~255자)
설명		• 등록할 서버에 대한 추가 정보를 입력한다. • 한글, 영문자, 숫자, 특수문자 (!,@,$,&,(,),_,+,-,=,:,',,,.)만 입력할 수 있다. (0~512자)

1.4 서버 목록

등록된 DA-MYQ 서버 정보를 목록 형태로 보여주며, 각 서버의 수정 및 설정을 진행한다.

관리도구 화면에서 공통적으로 사용되는 각 아이콘의 기능은 <관리도구에서 사용되는 아이콘과 버튼>을 참고한다.

그림 1-2 서버 목록 화면

표 1-6 서버 관리_서버 목록

항목	설명
현재 등록 서버 수	현재 등록된 제품 서버 수를 보여준다.
설정	등록된 서버 운영에 필요한 다음 항목을 조회 및 관리한다. • 서버 기본 정보 • 라이선스 정보 • 설정 파일 복구 • 그룹 정보 • SG-KMS 연동 설정 • 운영 설정 • 암호화 설정 • 암복호화 권한 설정
수정	등록된 서버의 아이디 및 IP 주소를 수정할 수 있다.
상태	• 헬스 체크가 'ON'으로 설정된 경우에 한해 표시되며, 서버의 연결 상태를 나타낸다. • 각 상태 값에 대한 설명은 <화면 구성 요소_서버 패널>을 참고한다. • 각 상태는 5초 주기로 갱신되나, 헬스체크 주기에 따라 5초 이상의 시간이 소요될 수 있다.
제품명	등록된 서버의 제품 유형을 표시한다.
서버명	등록된 서버의 설정 아이디를 표시한다.
IP 주소	등록된 서버의 설정 IP 주소를 표시한다.
포트 번호	등록된 서버의 설정 포트 정보를 표시한다.
헬스 체크	• 헬스 체크는 다음 정보를 기반으로 [상태]를 표시한다. ◦ DCA Plugin에서 DA-MYQ ID의 라이브러리 로딩 여부 ◦ scpdb_agent.ini 파일 접근 가능 여부 ◦ 암복호화 함수의 최종 접근 날짜(info 파일) read 여부 • 토글 스위치를 이용하여 헬스 체크 여부를 설정한다. ◦ ON: 헬스 체크 기능 사용 ◦ OFF: 헬스 체크 기능 미사용
최종 헬스 체크 시간	• 헬스 체크가 마지막으로 진행된 시간을 나타낸다. • 설정된 헬스 체크 주기에 따라 이루어진다.
최근 사용일	등록된 서버가 마지막으로 사용된 일자를 표시한다.

1.4.1 서버 목록 설정

[서버 목록]에서 설정 아이콘을 클릭하여, 해당 서버의 기본 정보 설정, 설정 파일 복구, SG-KMS 연동 설정 등을 관리한다.

1.4.1.1 서버 기본 정보

등록한 DA-MYQ 서버의 기본 정보를 관리한다.

표 1-7 서버 기본 정보

항목	설명	항목	설명
서버명	DA-MYQ 서버의 아이디를 표시한다.	설치 제품	설치한 서버의 제품 유형을 보여준다.
IP 주소	DCA가 설치된 DA-MYQ 서버의 IP 주소를 표시한다.	제품 버전	DA-MYQ 서버의 버전 정보를 표시한다.
포트 번호	DA-MYQ 서버의 DCA 포트 번호를 표시한다.	상태	DA-MYQ 서버의 상태를 '정상/비정상'으로 표시한다.
설치 경로**(*)**	• DA-MYQ 서버가 설치된 절대 경로를 표시하며, 수정할 수 있다. • 수정 시, 모든 문자열로 입력할 수 있다. (1~255자)		
설정 라이브러리 경로**(*)**	• DA-MYQ 서버의 라이브러리가 설치된 폴더의 절대 경로를 표시하며, 수정할 수 있다. • 수정 시, 모든 문자열로 입력할 수 있다. (1~255자)		
설명	• DA-MYQ 서버에 대한 추가 정보를 입력한다. • 수정 시, 모든 문자열로 입력할 수 있다. (0~255자)		

1.4.1.2 라이선스 정보

DA-MYQ 서버의 라이선스 정보를 요약해서 제공한다.

표 1-8 서버 관리 설정_라이선스 정보

항목	설명	항목	설명
라이선스 유형	DA-MYQ 서버의 라이선스 유형을 표시한다. • 단품 : 단품 계약 라이선스 • 볼륨 : 볼륨 계약 라이선스 • 클라우드 : 클라우드 환경 라이선스	라이선스 상태	DA-MYQ 서버의 라이선스 상태를 표시한다. • 유효: 유효한 라이선스 • Invalid: 유효하지 않는 라이선스
납품 계약번호	DA-MYQ 서버 라이선스의 납품 계약번호를 표시한다.	계약 시작일	DA-MYQ 서버의 라이선스 시작일을 표시한다.
코어	DA-MYQ 서버에 허용된 최대 CPU 코어 수를 표시한다.	계약 만료일	DA-MYQ 서버의 라이선스 만료일을 표시한다.

1.4.1.3 설정 파일 복구

DA-MYQ 설정 파일(scpdb_agent.ini)의 백업 경로 설정 및 설정 파일 복구 기능을 제공한다.

표 1-9 서버 관리 설정_설정 파일 복구

항목		설명
백업된 설정 파일 경로		백업 된 DA-MYQ 서버의 설정 파일 경로를 표시한다.
현재 설정 파일 내용		현재 DA-MYQ 설정 파일에 설정된 내용을 표시한다.
백업 정보	백업 설정 파일 저장 경로(*)	• 백업 된 DA-MYQ 설정 파일이 저장된 경로를 표시한다. • 설정 파일을 백업할 경로를 입력한 후, 아이콘을 클릭하여 경로를 수정할 수 있다. • 반드시 DCA를 실행한 계정이 '**읽기 및 쓰기 권한**'이 있는 경로를 DA-MYQ 백업 설정 파일 저장 경로로 설정해야 한다. • DA-MYQ 설정 파일에서 [IniBackupDir] 미 설정 시, 설정 파일이 있는 경로가 자동으로 설정된다.
	백업된 설정 파일(*)	• 백업 된 DA-MYQ 설정 파일을 드롭다운 형태로 보여준다. • 백업된 설정 파일은 '**scpdb_agent_D{YYYYMMDDHHMMSS}.ini**' 형태로 추가된다. • 복구할 설정 파일 선택 후 [복구]를 클릭할 경우, 해당 설정 파일로 복구된다.
설정 파일 정보	현재 설정 파일	현재 DA-MYQ 설정 파일에 설정된 내용을 표시한다.
	복구할 설정 파일	[백업된 설정 파일]에서 선택한 설정 파일에 설정된 내용을 표시한다.

Windows(Windows Server)에서 프로그램 파일 등의 관리자 권한이 필요한 경로를 설정하기 위해, 반드시 DCA를 '**관리자 권한**'으로 실행해야 한다.

1.4.1.4 SG-KMS 연동 설정

DA-MYQ 서버 운영에 필요한 SG-KMS 연동 설정 기능을 제공한다.

DA-MYQ 설정 파일(scpdb_agent.ini)을 수정할 경우, 반드시 D'Amo Control Center 관리도구의 '**새로 고침**' 기능을 사용하여 관리도구에 설정 값을 적용한다.

표 1-10 SG-KMS 연동 설정_연동 서버

구분	항목	설명
연동 서버	서버	• 연동할 SG-KMS 서버 번호를 보여준다. • 서버명은 '**서버+{숫자}**' 형태로 자동 부여된다. • 최대 10개까지 추가할 수 있다.
	IP 주소**(*)**	• 연동할 SG-KMS의 IP 또는 도메인 정보를 입력한다. • 입력값 범위는 아래와 같다.

구분	항목	설명
		◦ IP: 1.0.0.1 ~ 254.255.255.254 ◦ 도메인: 모든 문자열로 입력할 수 있다. (1~255자)
	포트 번호**(*)**	• 연동할 SG-KMS의 포트 번호를 입력한다. • 숫자로만 입력할 수 있다. (1~65535) • 기본값: 2525

표 1-11 SG-KMS 연동 설정_Agent 설정

구분	항목	설명	
Agent 설정	Agent 아이디 **(*)**	• Agent 아이디를 입력한다. • 모든 문자열로 입력할 수 있다. (1~255자)	
	PKD**(*)**	• SG-KMS와 통신할 때 사용할 데이터 요청 버전을 설정한다. • 기본값: 109	
		102	SG-KMS v3.0.1.4 이하일 경우에만 사용한다.
		103	SG-KMS v3.0.2.0 이하일 경우에만 사용한다.
		104	SG-KMS v3.0.2.4 이하일 경우에만 사용한다. (FPE 치환 사용 가능)
		105	SG-KMS v3.0.4.0 이하일 경우에만 사용한다. (패딩 및 IV 데이터 사용 가능)
		106	SG-KMS v3.0.7.1 이하일 경우에만 사용한다.
		107	SG-KMS v3.0.16.1 이하일 경우에만 사용한다.
		109	• SG-KMS v3.0.17.0 이상일 경우에만 사용한다.
	사이트 인증서 파일**(*)**	• 사이트 인증서의 절대 경로를 입력한다. 예) D:₩dbms_api₩key₩damo_agt_site.cer • 모든 문자열로 입력할 수 있다. (1~255자)	
	Agent 인증서 파일**(*)**	• Agent 인증서의 절대 경로를 입력한다. 예) D:₩dbms_api₩key₩damo_agt.cer • 모든 문자열로 입력할 수 있다. (1~255자)	
	Agent 키 파일 **(*)**	• Agent 키 파일의 절대 경로를 입력한다. 예) D:₩dbms_api₩key₩damo_agt.key • 모든 문자열로 입력할 수 있다. (1~255자)	
	SPIN**(*)**	해당 Agent 키의 SPIN 값을 입력한다.	
SG-KMS 타임아웃 설정	공통	• 연동할 SG-KMS의 타임아웃을 설정한다. • 설정 값을 초과할 경우, 오류로 처리된다. • 숫자로만 입력할 수 있다. (1~600초) • 기본값: 2초	
	연결 타임아웃 (초)(*)	SG-KMS 연결 시 소요되는 시간을 설정한다.	
	송신 타임아웃 (초)(*)	SG-KMS 연결 후, 요청을 보내는데 소요되는 시간을 설정한다.	
	수신 타임아웃	SG-KMS 연결 후 요청을 보내는데 성공할 경우, SG-KMS에서 보내는 메시지를 수신하는	

구분	항목	설명
	(초)(*)	데 소요되는 시간을 설정한다.

1.4.1.5 운영 설정

DA-MYQ 서버 운영 시 필요한 로그, 라이선스 및 이중 암호화 방지를 설정한다.

DA-MYQ 설정 파일(scpdb_agent.ini)을 수정할 경우, 반드시 D'Amo Control Center 관리도구의 '**새로 고침**' 기능을 사용하여 관리도구에 설정 값을 적용한다.

표 1-12 운영 설정_로그 설정/라이선스 설정/이중 암호화방지 설정

구분	항목		설명
로그 설정	로그 레벨**(*)**	No	로그를 남기지 않는다.
		오류	오류 및 경로 로그만 기록한다.
		정보	정보/오류/경고 로그만 기록한다.
		디버그	디버그/정보/오류/경고 로그를 모두 기록한다.
	로그 카운트 주기**(*)**		• 로그를 출력하는 주기를 설정한다. 예) 10000으로 설정할 경우, 그 이후 기록된 로그(10,001번째 로그)부터 출력 • 숫자로만 입력할 수 있다. (1~2147483647) • 기본값: 10000
	로그 경로**(*)**		• 로그를 기록할 디렉터리의 절대 경로를 입력한다. • 모든 문자열로 입력할 수 있다. (1~255자)
라이선스 설정	라이선스 파일 경로		라이선스 파일이 설치된 경로를 표시한다.
이중 암호화 방지 설정	이중 암호화 방지 유형**(*)**	All OFF	암호화 서비스 구분 없이, 이중 암호화 방지 기능을 사용하지 않는다. (기본값)
		All ON	암호화 서비스 구분 없이, 이중 암호화 방지 기능을 사용한다.
		SG-KMS ON	SG-KMS에서 설정한 서비스 아이디 및 키 파일에서만, 이중 암호화 방지 기능을 사용한다.
	암호화 식별값**(*)**		• 암호화 식별에 사용할 문자열을 설정한다. • 암호화 식별 값을 길게 설정할 경우, 암호화 데이터가 늘어나기 때문에 '**최대 3자리**'로 설정할 것을 권장한다. • 기본값: @^
	이중 암복호화 감지 시, 성공으로 처리		• 암호화 식별 기능을 사용할 경우, 이중 암호화를 방지하기 위한 암호화 식별 과정에서 오류가 발생할 수 있다. • 이 경우, 이중 암복호화를 감지할 때 성공으로 처리할 수 있도록 해당 기능을 설정한다.

1.4.1.6 암호화 설정

DA-MYQ 암호화 기능에 필요한 KEYINFO 섹션을 설정한다.

DA-MYQ 설정 파일(scpdb_agent.ini)을 수정할 경우, 반드시 D'Amo Control Center 관리도구의 '**새로 고침**' 기능을 사용하여 관리도구에 설정 값을 적용한다.

표 1-13 암호화 설정_KEYINFO 설정

항목	설명
KEYINFO	• 통합 함수에서 사용하는 [KEYINFO] 섹션을 설정할 수 있다. • 다음을 주의해서 [KEYINFO] 섹션을 설정한다. ◦ 여러 개의 암호화 정책을 사용할 경우, 키 이름은 중복할 수 없다. ◦ 하나의 KEY는 동일한 정책에서만 사용할 수 있다. ◦ 암호화 키 개수에 따라 KEY1, KEY2, KEY3 등 항목을 추가할 수 있다. • 아래의 예시를 참고해서 [KEYINFO] 섹션을 설정한다.

```
[KEYINFO] 설정 예시

# SG-KMS와 연동하여 암호화 키를 사용하는 경우
KEY1=ServiceID

# SCP 키 파일로 내보내기한 암호화 키를 사용하는 경우
KEY1=/home/scptest/AES_128_E_FIXED_IV_CBC.SCPS

# SG-KMS 연동 실패 시 SCP 키 파일을 사용할 경우
KEY1=ServiceID,/home/scptest/AES_128_E_FIXED_IV_CBC.SCPS

# SCP 키 파일 오류 시 SG-KMS와 연동할 경우
KEY1=/home/scptest/AES_128_E_FIXED_IV_CBC.SCPS,ServiceID
```

1.4.1.7 암복호화 권한 설정

DA-MYQ 암호화 기능에 필요한 암복호화 권한을 설정한다.

DA-MYQ 설정 파일(scpdb_agent.ini)을 수정할 경우, 반드시 D'Amo Control Center 관리도구의 '**새로 고침**' 기능을 사용하여 관리도구에 설정 값을 적용한다.

표 1-14 암호화 설정_암복호화 권한

구분	항목	설명
암복호화 권한	공통	• OS 계정 단위로 암복호화 권한을 설정한다. • 암복호화 권한 설정이 가능한 라이선스를 사용할 경우에만 설정할 수 있다.
	사용자명(*)	• 권한을 적용하고자 하는 DB의 계정명을 입력한다. • DB에 저장된 DB USER의 대소문자 여부를 확인하고 동일하게 입력해야 한다.
	서비스명/SCPS 파일 경로(*)	• 정책에 할당할 ServiceID나 SCP 키 파일명을 입력한다. • SG-KMS의 ServiceID에 대한 정책을 추가할 경우, SG-KMS의 암호화 서비스를 입력한다. 예) SP1 • SCP 키 파일 관련 정책을 추가할 경우, SCP 키 파일(애플리케이션에서 입력되는 절대 경로)를 입력한다. 예) /dbms_api/key/SP1.SCPS
	암호화 권한(*)	암호화 권한을 설정한다. • 체크박스 선택: 암호화 가능 • 체크박스 미선택: 암호화 불가 (기본값)
	복호화 권한(*)	복호화 권한을 설정한다. • 체크박스 선택: 복호화 가능 • 체크박스 미선택: 복호화 불가 (기본값)

1.4.2 서버 목록 수정

등록한 서버의 기본 정보를 수정할 수 있다.

표 1-15 서버 기본 정보

항목	설명	항목	설명
서버명	DA-MYQ 서버의 아이디를 표시한다.	설치 제품	설치한 서버의 제품 유형을 보여준다.
IP 주소	DCA가 설치된 DA-MYQ 서버의 IP 주소를 표시한다.	제품 버전	DA-MYQ 서버의 버전 정보를 표시한다.
포트 번호	DA-MYQ 서버의 DCA 포트 번호를 표시한다.	상태	DA-MYQ 서버의 상태를 '정상/비정상'으로 표시한다.
설치 경로(*)	• DA-MYQ 서버가 설치된 절대 경로를 표시하며, 수정할 수 있다. • 수정 시, 모든 문자열로 입력할 수 있다. (1~255자)		
설정 라이브러리 경로(*)	• DA-MYQ 서버의 라이브러리가 설치된 폴더의 절대 경로를 표시하며, 수정할 수 있다. • 수정 시, 모든 문자열로 입력할 수 있다. (1~255자)		
설명	• DA-MYQ 서버에 대한 추가 정보를 입력한다. • 수정 시, 모든 문자열로 입력할 수 있다. (0~255자)		

1.5 템플릿

템플릿 기능을 통해, DA-MYQ 제품별로 동일한 설정 정보를 일괄 적용할 수 있다.

템플릿을 통해 적용한 설정 정보는, 서버가 아닌 **DA-MYQ 제품별로 적용**된다.

1.5.1 템플릿 생성

DA-MYQ에 일괄적으로 적용할 설정 정보 템플릿을 생성한다.

그림 1-3 서버 관리_템플릿 생성

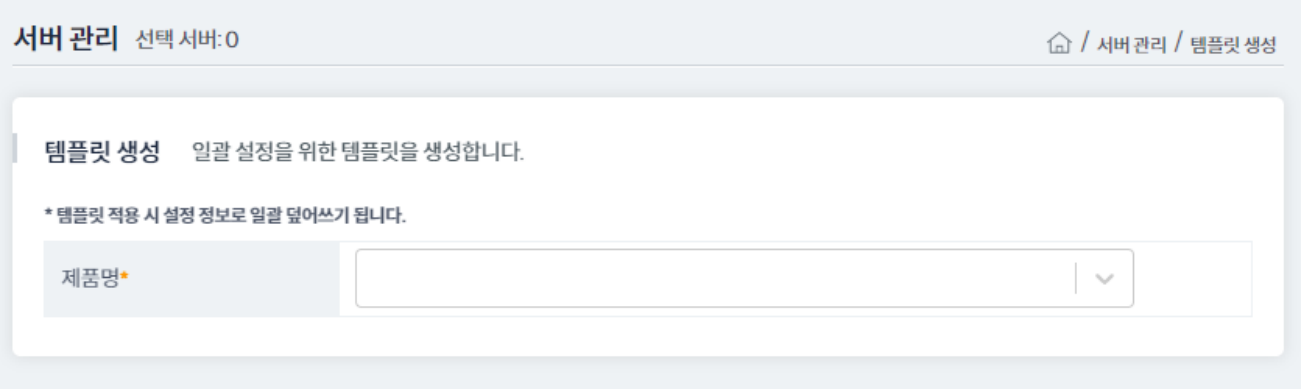


표 1-16 서버 관리_서버 등록

항목		설명
제품명(*)		• 등록할 서버의 제품 유형인 DA-MYQ 를 선택한다. • 선택한 제품 유형에 따라, 설정 항목이 출력된다.
서버명(*)		• 등록할 DA-MYQ 서버 아이디를 입력한다. • 특수문자(#'") 제외, 모든 문자열로 입력할 수 있다. (1~128자)
DCA(*)	IP 주소	• 등록할 DA-MYQ 서버의 DCA IP 주소를 입력한다. • 모든 문자열로 입력할 수 있다. (1~2000자)
	포트 번호	• 등록할 DA-MYQ 서버의 DCA 포트 번호를 입력한다. • 숫자만 입력할 수 있다. (0~65535)
설치 경로(*)		• DA-MYQ 서버가 설치된 절대 경로를 입력한다. • 모든 문자열로 입력할 수 있다. (1~255자)
설치 라이브러리 경로(*)		• DA-MYQ 서버의 라이브러리가 설치된 폴더의 절대 경로를 입력한다. • 모든 문자열로 입력할 수 있다. (1~255자)
설명		• 등록할 서버에 대한 추가 정보를 입력한다. • 한글, 영문자, 숫자, 특수문자 (!,@,$,&,(,),_,+,-,=,:,',,,.)만 입력할 수 있다. (0~512자)

1.5.2 템플릿 목록

등록한 DA-MYQ 템플릿을 목록 형태로 제공하여, 템플릿 조회 및 서버 적용을 진행할 수 있다.

표 1-17 템플릿 목록과 관리

항목	설명
상세	등록된 템플릿 항목을 조회하고 관리한다. 항목은 제품별로 다르므로, 자세한 설명은 해당 제품의 매뉴얼을 참고한다.
수정	'제품명'과 '템플릿명'을 제외한 모든 항목을 수정할 수 있다.
템플릿명	등록된 템플릿의 템플릿명을 표시한다.
-	• [적용] 버튼을 클릭하면 해당 템플릿의 제품 유형과 동일한 유형의 서버에 설정 템플릿을 적용할 수 있는 팝업이 노출된다. • 템플릿 목록 화면 왼쪽 상단> 라디오 버튼 설정에 따라 적용 범위가 달라진다. ◦ [전체 서버 적용]: 전체 서버 중 해당 템플릿의 제품 유형과 동일한 유형의 서버에 적용 ◦ [선택 서버 적용]: 서버 패널에서 선택한 서버 중 해당 템플릿의 제품 유형과 동일 서버에 적용

2.

서버 운영 설명서

2.1 시작하기 전에

본 설명서는 **DA-MYQ v5.0**을 기준으로 본 제품을 운영하는데 필요한 **DA-MYQ 설정 파일, SG-KMS Agent 접근 제어** 등에 대해 설명한다.

2.2 DA-MYQ 설정 파일

DA-MYQ를 운영하는데 필요한 설정 파일(scpdb_agent.ini)의 각 섹션에 대해 설명한다.

제품 운영 중 scpdb_agent.ini 파일을 수정할 경우, '**CONFIG_REINIT() 함수**'를 호출해야 변경된 내용이 적용된다.

2.2.1 KEYINFO 섹션

KEYINFO 섹션을 구성하고 있는 항목에 대한 설명은 다음과 같다.

표 2-1 KEYINFO 섹션

항목	설명
공통	• KEY1, KEY2, KEY3 등 사용하는 암호화 키 개수에 따라, 항목을 추가할 수 있다. • **주석(#)을 삭제**한 후, 사용한다.
KEY1=ServiceID**(*)**	• SG-KMS와 통신을 하여 '**암호화 키**'를 가져와 데이터를 암복호화 한다. • SG-KMS에서 생성한 서비스 ID 를 입력한다.

항목	설명
#KEY2=SCP_FilePath	• SG-KMS 통신 없이 SCP 키 파일에서 '**암호화 키**'를 가져와 데이터를 암복호화 한다. • SCP 키 파일의 절대 경로, 파일명 및 확장자를 입력한다.
#KEY3=ServiceID,SCP_FilePath	• SG-KMS 통신에 실패할 경우, SCP 키 파일로 내보내기한 '**암호화 키**'를 사용한다. • SG-KMS에서 생성한 서비스 ID와 SCP 키 파일의 절대 경로, 파일명 및 확장자를 함께 입력한다. • 서비스 ID와 SCP 키 파일 정보를 모두 입력할 경우, **공백 없이** 입력한다.

DB를 재시작해야 변경된 KEYINFO 값이 적용된다.

2.2.2 SERVER 섹션

SERVER 섹션을 구성하고 있는 항목에 대한 설명은 다음과 같다.

표 2-2 SERVER 섹션

항목	설명	
Server**(*)**	ServerIP	• SG-KMS의 IP를 입력한다. • 입력 가능한 IP 수: 최대 10개
	ServerPort	• SG-KMS의 포트를 입력한다. • 기본값: 2525
Server2	ServerIP	• HA 대상인 Slave SG-KMS의 IP를 입력한다.
	ServerPort	• HA 대상인 Slave SG-KMS의 포트를 입력한다. • 기본값: 2525

2.2.3 TIMEOUT 섹션

TIMEOUT 섹션을 구성하고 있는 항목에 대한 설명은 다음과 같다.

표 2-3 TIMEOUT 섹션

항목	설명
ConnectTimeout	• SG-KMS와 연동하는데 걸리는 시간을 제한하는 기능이다. • 설정한 시간 내에 연동이 안 될 경우, 오류로 처리된다. • 기본값: 2초
SendTimeout	• SG-KMS와 연동 후 요청 신호를 송신하는데 걸리는 시간을 제한하는 기능이다. • 설정한 시간 내에 SG-KMS가 요청을 받지 않을 경우, 오류로 처리된다. • 기본값: 2초

항목	설명
RecvTimeout	• SG-KMS와 연동 후 요청을 보내고 성공 시 SG-KMS에서 보내는 메시지를 받는데 걸리는 시간을 제한하는 기능이다. • 설정한 시간 내에 메시지를 못 받을 경우, 오류로 처리된다. • 기본값: 2초

2.2.4 AGENT 섹션

AGENT 섹션을 구성하고 있는 항목에 대한 설명은 다음과 같다.

표 2-4 AGENT 섹션 #1

항목	설명	
AgentID	SG-KMS에서 등록한 [Agent ID(CN)]를 입력한다.	
LogDir	DA-MYQ 로그 파일을 저장할 경로를 입력한다.	
LogLevel	DA-MYQ 로그 파일에 남기는 로그 레벨을 설정한다.	
	0	로그 파일을 남기지 않는다. (기본값)
	4	오류 로그 및 경고 로그를 파일에 기록한다.
	6	정보 로그, 오류 로그, 경고 로그를 파일에 기록한다.
	8	디버그 로그, 정보 로그, 오류 로그, 경고 로그를 파일에 기록한다.
LogCount	• DA-MYQ의 로그 생성 시 로그의 양을 조절할 수 있는 숫자를 입력한다. 예) 10,000으로 설정했을 경우, 첫 번째 로그를 1회 남기고 다음 10000 번이 지난 10001번째에 로그를 남김 • 입력값 범위: 1~2,147,483,647 (기본값: 10,000)	
LogCountType	SG-KMS에 암복호화 로그를 남길 수 있도록 설정한다. • 0: SG-KMS에 암복호화 로그 남김 (기본값) • 그 외: SG-KMS에 암복호화 로그 남기지 않음	
LogCountTime	• SG-KMS에 암복호화 로그를 특정 시간마다 1회씩 남기도록 설정한다. ◦ 0: SG-KMS에 암복호화 로그를 매번 남김 (기본값) ◦ 10: 10초가 초과되면 SG-KMS에 암복호화 로그 남김 • 해당 옵션은 [LogCountType]이 0일 경우에만 동작	
SiteCertFilePath	SG-KMS에서 발급한 사이트 인증서 파일의 경로를 입력한다.	
CertFilePath	SG-KMS에서 발급한 Agent 키의 인증서 파일 경로를 입력한다.	
KeyFilePath	SG-KMS에서 발급한 Agent 키의 키 파일 경로를 입력한다.	
SPIN	SG-KMS에서 발급한 Agent 키의 .spin 파일을 열어 값을 붙여 넣는다.	
CharSet	• 부분 암호화할 경우에 입력된 데이터의 CharSet을 지정한다. • 암복호화시 입력한 데이터를 통해 CharSet을 판단할 수 없기 때문에, 설정된 옵션에 맞춰 부분 암호화를 지원한다.	
	0	입력 받은 데이터를 바이트 단위로 처리한다. (기본값)
	1	EUC-KR로 설정하여, 입력 받은 데이터 중 멀티 바이트일 경우에는 2 Byte 단위로 처리한다.

항목	설명	
	2	• UTF-8로 설정하여, 입력 받은 데이터 중 멀티 바이트일 경우에는 3 Byte 단위로 처리한다. • 암호화 정책이 특성 유지 암복호화일 경우 지원하지 않는다.
PartialEncType	0	암호화 데이터에 암호화된 길이 정보(예. 024, 032)를 3byte 형태로 표시한다.
	1	• 암호화 데이터에 암호화된 길이 정보(예. 024, 032)를 표시하지 않는다. • 글자 단위 암호화 및 입력값 중간부터 부분 암호화를 진행할 경우, 해당 모드는 지원하지 않는다.

표 2-5 AGENT 섹션 #2

항목	설명	
PKP	SG-KMS와 통신 시에 사용하는 프로토콜 버전이다.	
	100	공개키 암호화, 공개키 서명 검증, 세션키를 매번 생성하는 방식 (기본값)
	102	대칭키 암호화, HMAC 무결성 검증, 세션키를 매번 생성하는 방식
AclPKP	• SG-KMS와 접근 제어 항목을 통신할 때에 사용하는 프로토콜 버전이다. • 내용은 PKP 항목과 동일하다. • 기본값: 102	
PKD	• SG-KMS와 통신할 경우 사용하는 데이터 요청 버전을 의미한다. • SG-KMS 버전에 맞추어 설정해야 한다.	
	102	SG-KMS v3.0.1.4 이하일 경우에만 사용
	103	SG-KMS v3.0.2.0 이하일 경우에만 사용
	104	• SG-KMS v3.0.2.4 이하일 경우에만 사용 • FPE 치환 기능 사용 가능
	105	• SG-KMS v3.0.4.0 이하일 경우에만 사용 • 패딩 및 IV 데이터 사용 가능
	106	SG-KMS v3.0.7.1 이하일 경우에만 사용
	107	SG-KMS v3.0.16.1 이하일 경우에만 사용
	109	• SG-KMS v3.0.17.0 이상일 경우에만 사용 (기본값) • 키 그룹 기능 사용 가능

표 2-6 AGENT 섹션 #3

항목	설명	
DiscernMode	• 암호화 식별 기능을 사용할 때 설정한다. • Base64 타입 문자열 암호화만 지원한다.	
	0	암호화 식별 기능을 사용하지 않음 (기본값)
	1	암호화 서비스 구분 없이 모든 정책에 암호화 식별 기능 사용
	2	SG-KMS에서 암호화 식별 기능을 설정한 암호화 정책 및 키 파일만 암호화 식별 기능 사용

항목	설명	
DiscernChar	• 암호화 식별 기능을 사용하기 위해 암호문에 추가적으로 입력되는 문자열이다. • 기본값: @^ • 'DiscernMode'가 1일 경우에만 정상 동작한다.	
DiscernAfter	암호화 식별 기능을 사용할 때 설정한다.	
	0	암호화 식별 될 경우, 오류를 리턴한다. (기본값)
	1	• 암호화 식별 기능이 동작하는 경우에도 오류로 처리되지 않고 성공으로 리턴하며, 암호화 데이터 입력값을 그대로 반환한다. • 특성 암호화의 경우, DiscernMode 값이 1 또는 2일 때 암호화 데이터 입력값을 그대로 반환한다.
ZeroLengthMode	• DP-MSQ와 호환하기 위해서 DA-MSQ에서 입력 데이터가 없는 경우에도 암호화를 진행할 때 설정한다. • DA-MSQ에서만 정상 동작한다.	
	0	입력 데이터가 빈 값인 경우에는 암호화 하지 않고 빈 값을 리턴한다. (기본값)
	1	양방향 암호화, CBC 모드일 경우에만 동작한다.
IniBackupDir	D'Amo Control Center 연동시 scpdb_agent.ini 백업 파일을 저장하는 디렉터리이다.	

2.3 DA-MYQ acl_cli 설정

acl_cli을 실행하여 DB 계정별로 암복호화 권한의 정책을 설정한다. 설정된 정책에 따라, 암복호화를 제어한다.

2.3.1 DA-MYQ acl_cli 실행

acl_cli 파일을 실행하여 암복호화 권한을 설정한다.

DA-MYQ acl_cli 실행 시 권한 정보가 변경되기 때문에, 현재 폴더를 포함한 하위 폴더 모두 '**쓰기 권한**'을 가지고 있어야 한다.

Windows(Windows Server)의 경우

```
cd %DA_INST_HOME%
acl_cli.exe -start
```

Linux(Unix)의 경우

```
cd $DA_INST_HOME
./acl_cli -start
```

Agent 등록하기

acl_cli 파일을 최초로 실행한 경우, acl_cli 파일 실행과 함께 Agent 키의 비밀번호를 입력하는 명령어가 출력된다.

```
Enter the PIN of CLI-Key : <Agent 키 비밀번호 입력>
```

CLI 명령어에 대한 자세한 설명은, *help* 명령어를 통해 확인할 수 있다.

2.3.2 DA-MYQ acl_cli 설정

${DA_INST_HOME} 디렉토리에서 DA-MYQ acl_cli 파일을 실행하여 DB 계정 단위로 암복호화 권한을 설정한다.

정책 추가

DA-MYQ acl_cli에 정책을 추가한다.

```
SET PRIV ENC <USER>"<KEY_NAME>"<ENC>"<DEC>
```

표 2-7 DA-MYQ acl_cli 정책 추가

파라미터	설명
USER(*)	• 권한을 적용하고자 하는 DB의 계정명을 입력한다. • DB에 저장된 DB USER의 대소문자 여부를 확인하고 동일하게 입력해야 한다.
KEY_NAME(*)	• 정책에 할당할 암호화 키명을 입력한다. • 암호화 키명은 scpdb_agent.ini 파일 [KEYINFO] 섹션의 KEY1, KEY2, KEY3과 같은 값을 의미한다. 예) SET PRIV ENC SCP"KEY1"1"1
ENC(*)	해당 계정에 암호화 권한을 부여할지 여부를 설정한다. • 0: 암호화 권한 미부여 • 1: 암호화 권한 부여
DEC(*)	해당 계정에 복호화 권한을 부여할지 여부를 설정한다. • 0: 복호화 권한 미부여 • 1: 복호화 권한 부여

정책 삭제

DA-MYQ acl_cli에 설정된 정책을 삭제한다.

```
DEL PRIV ENC <USER>"<KEY_NAME>
```

표 2-8 DA-MYQ acl_cli 정책 삭제

파라미터	설명
USER(*)	적용했던 권한을 삭제하려는 DB의 계정명을 입력한다.
KEY_NAME(*)	• 암복호화 권한을 삭제할 암호화 키명을 입력한다. 예) DEL PRIV ENC SCP"KEY1

정책 조회

DA-MYQ acl_cli에 추가된 정책을 유저별로 조회한다.

```
SHOW PRIV ENC <USER>
```

표 2-9 DA-MYQ acl_cli 정책 조회

파라미터	설명
USER(*)	• DA-MYQ acl_cli에 추가된 특정 DB 사용자의 정책을 조회한다. • 권한이 적용된 DB의 계정명을 입력한다. 예) SHOW PRIV ENC SCP

DA-MYQ acl_cli에 추가된 정책을 전체 조회한다.

```
SHOW ALL
```

권한 조회

DA-MYQ acl_cli에 추가된 권한을 cli 명령어 형태로 조회한다.

```
SHOW PRIV COMMAND
```

표 2-10 DA-MYQ acl_cli 권한 조회

구분	설명
SHOW PRIV COMMAND	DA-MYQ acl-cli에 기록된 권한을 명령어 형태로 조회한다.

정책 저장

DA-MYQ acl_cli에 설정한 정책을 저장한다.

```
SAVE ALL
```

표 2-11 DA-MYQ acl_cli 정책 저장

구분	설명
SAVE ALL	• 정책 추가·삭제 후 *SAVE ALL*을 입력하면, 설정한 정책이 저장된다. • 설정한 정책을 저장하지 않을 경우, acl_cli에 적용되지 않는다.

로그 조회

DA-MYQ acl_cli의 로그를 조회한다.

```
SHOW LOG POLICY
```

표 2-12 DA-MYQ acl_cli 로그 조회

구분	설명
SHOW LOG POLICY	• DA-MYQ acl-cli에 기록된 로그를 조회한다. • 조회할 로그 파일 날짜를 공백 없이 '**yyyymmdd**' 형태로 입력한다. 예) 20210525

날짜 조회

DA-MYQ acl_cli 서버의 현재 날자를 조회한다.

```
SHOW DATE
```

2.4 SG-KMS Agent 접근 제어 설정

SG-KMS를 연동할 경우, DA-MYQ는 SG-KMS에서 설정한 Agent 접근 허용 항목에 따라 암호화 정책에 대한 접근 제어를 설정할 수 있다.

아래의 표를 참고하여, 접근 제어 항목을 설정해야 한다. 일치하지 않는 항목이 있을 경우, 암호화 정책 가져오기에 실패한다.

표 2-13 SG-KMS Agent 접근 제어 설정

항목	설명
공통	접근 제어 관련 항목을 설정하지 않을 경우, '**모두 허용**'으로 설정된다.
Agent IP	Agent IP를 설정한 경우, Agent IP 허용 범위에 DA-MYQ가 설치된 IP가 포함되어야 한다.
접근 허용 Agent 설치 경로	접근 허용 Agent 설치 경로를 설정한 경우, DA-MYQ를 적용한 애플리케이션 실행 경로와 동일해야 한다.
접근 허용 가능 기간	접근 허용 가능 기간(기간, 요일, 시간)을 설정한 경우, 설정한 기간에만 접근할 수 있다.
접근 허용 가능 계정	접근 허용 가능 계정을 설정한 경우, DA-MYQ를 적용한 애플리케이션의 계정과 동일해야 한다.

접근 제어 관련 항목에 대한 자세한 설명은, <**SG-KMS 사용자 설명서**>를 참고한다.

2.5 DA-MYQ 운영 함수

여기에서는 DA-MYQ 운영에 필요한 함수에 대해 설명한다.

2.5.1 DA-MYQ 함수

DA-MYQ에서는 다음과 같은 함수를 사용한다.

표 2-14 DA-MYQ 함수

함수명	파라미터	입력값	출력값
ENC_STR	I_KEY	IN 문자열	Hex String 암호문
	I_DATA	IN 문자열 (평문)	
ENC_B64	I_KEY	IN 문자열	Base64 Encoding 암호문
	I_DATA	IN 문자열 (평문)	
DEC_STR	I_KEY	IN 문자열	평문
	I_DATA	IN 문자열 (Hex String 암호문)	
DEC_B64	I_KEY	IN 문자열	
	I_DATA	IN 문자열 (Base64 String 암호문)	
INDEX_STR	I_KEY	IN 문자열	Hex String 암호문
	I_DATA	IN 문자열 (평문)	
	I_TYPE	'' 또는 (Plug-IN 연동 시) 'IX'	
	I_KEY	IN 문자열 (Hex String 암호문)	

함수명	파라미터	입력값		출력값
DEC_INDEX_STR	I_DATA	IN 문자열 (암호문)		OPE 데이터
	I_TYPE	'' 또는 (Plug-IN 연동 시) 'IX'		
DEC_INDEX_B64	I_KEY	IN 문자열 (Base64 Encoding 암호문)		
	I_DATA	IN 문자열 (암호문)		
	I_TYPE	'' 또는 (Plug-IN 연동 시) 'IX'		
HASH_STR	I_ALOG	IN 숫자	SHA1 =70	Hex String 해시 암호문
			SHA256 =71	
			SHA384 =72	
			SHA512 =73	
			HAS160 =74	
	I_DATA	IN 문자열		
HASH_B64	I_ALOG	IN 숫자	SHA1 =70	Base64 String 해시 암호문
			SHA256 =71	
			SHA384 =72	
			SHA512 =73	
			HAS160 =74	
	I_DATA	IN 문자열		
HEXTOB64	I_DATA	IN 문자열 (Hex String 암호문)		Base64 Encoding 암호문
B64TOHEX	I_DATA	IN 문자열 (Base64 Encoding 암호문)		Hex String 암호문
CONFIG_REINIT	-			• SUCCESS: 성공 • 그 외: 오류

Hex String 은 1byte 데이터를 16진수 2byte의 아스키 코드로 표현하는 방식이다.
따라서 입력값이 Hex String인 경우 포맷에 맞게 *2의 배수* 글자 수를 입력하도록 한다.

다음 함수 파라미터를 참고하여, 함수를 사용한다.

표 2-15 함수 파라미터

파라미터	설명
I_KEY	• 암복호화 시 사용하는 암호화 키명 • 암호화 키명은 scpdb_agent.ini 파일의 [KEYINFO] 섹션에서 KEY1, KEY2, KEY3와 같은 값
I_DATA	평문(암호화 함수일 경우) 또는 암호문(복호화 함수일 경우)

2.5.2 함수 파라미터

다음 함수 파라미터를 참고하여, 함수를 사용한다.

표 2-16 함수 파라미터

파라미터	설명
I_KEY	• 암복호화 시 사용하는 암호화 키명 • 암호화 키명은 scpdb_agent.ini 파일의 [KEYINFO] 섹션에서 KEY1, KEY2, KEY3와 같은 값
I_DATA	평문(암호화 함수일 경우) 또는 암호문(복호화 함수일 경우)

```
예시
SELEC ENC_STR('KEY1', 'abc');
SELEC DEC_STR('KEY1', ENC_STR('KEY1', 'abc'));
```

DA-MYQ는 성능 향상을 위해 암호화 키명으로 **캐시된 암호화 정책을 사용**한다. 암호화 키명은 동일하나 다른 암호화 정책을 사용할 경우, 이전에 캐시된 암호화 키로 복호화를 시도하여 오류가 발생한다. 이 경우, **DB 서버를 재시작하여 함수를 재호출**한다.

2.5.3 함수 호출 예제

1. ENC_STR

```
SELECT ENC_STR('KEY1', 'abc');
```

2. ENC_B64

```
SELECT ENC_B64('KEY1', 'abc');
```

3. DEC_STR

```
SELECT DEC_STR('KEY1', ENC_STR('KEY1', 'abc'));
```

4. DEC_B64

```
SELECT DEC_B64('KEY1', ENC_B64('KEY1', 'abc'));
```

5. INDEX_STR

```
DP 제품에 연동 하지 않을 경우
SELECT INDEX_STR('KEY1', 'abc', '');

DP 제품에 연동 할 경우
SELECT INDEX_STR('KEY1', 'abc', 'IX');
```

6. DEC_INDEX_STR, DEC_INDEX_B64

```
DP 제품에 연동 하지 않을 경우
SELECT DEC_INDEX_STR('KEY1', ENC_STR('KEY1', 'abc'), '');
SELECT DEC_INDEX_B64('KEY1', ENC_B64('KEY1', 'abc'), '');

DP 제품에 연동 할 경우
SELECT DEC_INDEX_STR('KEY1', ENC_STR('KEY1', 'abc'), 'IX');
SELECT DEC_INDEX_B64('KEY1', ENC_B64('KEY1', 'abc'), 'IX');
```

7. HASH_STR

```
SELECT HASH_STR( 71, 'abc' );
```

8. HASH_B64

```
SELECT HASH_B64( 71, 'abc' );
```

9. HEXTOB64

```
SELECT HEXTOB64('A305378D8F974F1C1537ED7CB0CB959245D1AC31');
```

10. B64TOHEX

```
SELECT B64TOHEX('owU3jY+XTxwVN+18sMuVkkXRrDE=');
```

11. CONFIG_REINIT

```
SELECT CONFIG_REINIT();
```

2.6 DA-MYQ 제품 버전 확인

acl_cli 파일을 실행하여 제품 버전 정보를 확인한다.

Windows(Windows Server)의 경우

```
cd %DA_INST_HOME%
acl_cli.exe -v
```

Unix(Linux)의 경우

```
cd $DA_INST_HOME
./acl_cli -v
```

파트 III.

운영 안내서

여기에서는, 제품 설치 및 설정 완료 후 여러 상황 별 운영 방법에 대해 기술한다.

제품에는 하드웨어와 소프트웨어를 모두 포함한다.

1.

암호화 키 설정 안내서

1.1 시작하기 전에

본 안내서는 **DA-MYQ 5.0**을 기반으로, **암호화 키를 설정하는 방법**에 대해 설명한다.

1.2 암호화 키 설정하기

DA-MYQ 에서 암호화 키를 설정하는 방법은 다음과 같다.

1.2.1 SG-KMS 연동하기

DA-MYQ는 SG-KMS[1]에서 만든 '암호화 키'를 이용해 데이터를 암복호화 할 수 있다.

표 1-1 SG-KMS의 암호화 키 사용하는 방법

방법	설명
SG-KMS와 연동하기	SG-KMS와 연동하여, SG-KMS에서 만든 암호화 키를 호환하여 사용한다.
SG-KMS의 암호화 키 내보내기	SG-KMS에서 생성한 암호화 키를 '**SCP 키 파일**[a]'로 내보내기 한 후, 사용한다.

a **SCP 키 파일**: .scp 및 .scps 키 파일을 의미함

여기에서는 SG-KMS와 연동하기 위해, SG-KMS에서 DA-MYQ 정보를 등록하고 연동에 필요한 키를 내보내기 하는

1. **SG-KMS**: 암호화 키·암호화 정책 등을 생성 및 관리할 수 있는, 펜타시큐리티(주)의 DB 보안 솔루션

방법에 대해 설명한다.

사전 준비

SG-KMS 연동을 진행하기 전, 다음 사항을 확인한다.

표 1-2 준비 항목

준비 항목	설명	
연동 가능한 SG-KMS 버전 정보	SG-KMS v3.0	v3.0.9.0 이상 지원
	SG-KMS v4.0	• v4.0.104.5 이상 지원 • v4.0.302.0 이상 지원
SG-KMS	• SG-KMS 관리도구 • SG-KMS 관리도구에 접속할 수 있는 아이디 및 비밀번호 • SG-KMS 사용자 설명서	

본 안내서에서는 SG-KMS의 키 종류 및 SG-KMS 관리도구 사용법에 대한 내용은 다루지 않는다. 자세한 사항은 <**SG-KMS 사용자 설명서(SL4)**>를 참고한다.

SG-KMS 버전별 연동 방법

SG-KMS는 버전에 따라 연동하는 방법이 다르다.
연동할 SG-KMS의 버전을 확인한 후, 다음 안내서를 참고하여 연동을 진행한다.

표 1-3 SG-KMS 버전별 연동 방법

SG-KMS 버전	참고 자료
SG-KMS v3.0.9 이상	• <관리도구 사용 설명서>를 참고하여, SG-KMS 연동을 진행한다. • 해당 안내서는 **SG-KMS v3.0.25** 기준으로 작성되었다.
SG-KMS v4.0.104.5 이상	• <D'Amo Agent 연동 안내서>를 참고하여, SG-KMS 연동을 진행한다. • 해당 안내서는 **SG-KMS v4.0.176** 기준으로 작성되었다.
SG-KMS v4.0.302 이상	• <Agent 연동 안내서>를 참고하여, SG-KMS 연동을 진행한다. • 해당 안내서는 **SG-KMS v4.0.302** 기준으로 작성되었다.

1.2.2 라이선스 발급 및 등록하기

DA-MYQ를 사용하기 위해, ICS^{2}에서 라이선스를 발급 받아 등록한다.

1. 환경에 따라, 라이선스를 발급 받는다.
2. 발급 받은 라이선스 파일을 아래의 디렉터리에 복사한다.

표 1-4 환경별 디렉터리 위치

환경	디렉터리 위치
Windows(Windows Server)	%DA_INST_HOME%
Linux(Unix)	$DA_INST_HOME

3. 복사한 라이선스 파일명을 '**damo_lic.cer**'로 변경하여, 라이선스 등록을 완료한다.

1.2.3 설정 파일 수정하기

여기에서는 DA-MYQ 운영을 위해, 설정 파일을 수정하는 방법에 대해 설명한다. 설정 이외 항목에 대한 자세한 설명은 <DA-MYQ 운영 설명서>의 '**DA-MYQ 설정 파일**'을 참고한다.

1.2.3.1 암호화 키 설정하기

SG-KMS와 연동 또는 키 내보내기를 통해 DA-MYQ에서 사용할 **'암호화 키'**를 가져오기 한다.

해당 키를 사용하기 위해서는, 다음과 같이 설정한다.

1. DA-MYQ의 '**scpdb_agent.ini**' 설정 파일에서 [KEYINFO] 섹션으로 이동한다.
2. 아래의 표를 참고하여, 암호화 키 정보를 입력한다.

표 1-5 KEYINFO 섹션

항목	설명
공통	• KEY1, KEY2, KEY3 등 사용하는 암호화 키 개수에 따라, 항목을 추가할 수 있다. • **주석(#)을 삭제**한 후, 사용한다.
KEY1=ServiceID**(*)**	• SG-KMS와 통신을 하여 '**암호화 키**'를 가져와 데이터를 암복호화 한다. • SG-KMS에서 생성한 서비스 ID 를 입력한다.
#KEY2=SCP_FilePath	• SG-KMS 통신 없이 SCP 키 파일에서 '**암호화 키**'를 가져와 데이터를 암복호화 한다. • SCP 키 파일의 절대 경로, 파일명 및 확장자를 입력한다.
#KEY3=ServiceID,SCP_FilePath	• SG-KMS 통신에 실패할 경우, SCP 키 파일로 내보내기한 '**암호화 키**'를 사용한다. • SG-KMS에서 생성한 서비스 ID와 SCP 키 파일의 절대 경로, 파일명 및 확장자를 함께 입력한다. • 서비스 ID와 SCP 키 파일 정보를 모두 입력할 경우, **공백 없이** 입력한다.

2. **ICS(Intelligent Customer Support)**: 펜타시큐리티(주) 제품의 라이선스를 관리하는 포털 사이트

Windows(Windows Server)의 경우

```
[KEYINFO] 예시

KEY1=DA_AES256
KEY2=D:\dbms_api\key\DA_AES256.SCPS
KEY3=DA_AES256,D:\dbms_api\key\DA_AES256.SCPS
```

Linux(Unix)의 경우

```
[KEYINFO] 예시

KEY1=DA_AES256
KEY2=/dbms_api/key/DA_AES256.SCPS
KEY3=DA_AES256,/dbms_api/key/DA_AES256.SCPS
```

3. SG-KMS와 연동한 경우, 설정 파일의 [Server]과 [Server2]를 추가적으로 수정한다.

표 1-6 SERVER 섹션

항목	설명	
Server(*)	ServerIP	• SG-KMS의 IP를 입력한다. • 입력 가능한 IP 수: 최대 10개
	ServerPort	• SG-KMS의 포트를 입력한다. • 기본값: 2525
Server2	ServerIP	• HA 대상인 Slave SG-KMS의 IP를 입력한다.
	ServerPort	• HA 대상인 Slave SG-KMS의 포트를 입력한다. • 기본값: 2525

```
[Server] 예시

ServerIP=192.168.22.25
ServerPort=2525
```

4. 설정 파일의 [AGENT] 섹션을 설정한다.

표 1-7 AGENT 섹션

항목	설명
AgentID(*)	SG-KMS 관리도구에서 설정한 D'Amo Agent의 Agent ID를 입력한다.

항목	설명
SiteCertFilePath(*)	SG-KMS 장비에서 설정한 사이트 공개키(.cer)의 절대 경로 및 파일명을 입력한다.
CertFilePath(*)	SG-KMS 관리도구에서 설정한 D'Amo Agent의 공개키(.cer)의 절대 경로 및 파일명을 입력한다.
KeyFilePath(*)	SG-KMS 관리도구에서 설정한 D'Amo Agent의 개인키(.key)의 절대 경로 및 파일명을 입력한다.
SPIN(*)	• SG-KMS 관리도구에서 설정한 D'Amo Agent의 SPIN 값을 입력한다. • 파일명: damo-scp_PENTA-{Agent명}.spin

Windows(Windows Server)의 경우

```
[AGENT] 예시

AgentID=DA
SiteCertFilePath=D:\dbms_api\key\kms\damo-site_PENTA.cer
CertFilePath=D:\dbms_api\key\kms\damo-scp_PENTA-SA_TEST.cer
KeyFilePath=D:\dbms_api\key\kms\damo-scp_PENTA-SA_TEST.key
SPIN=Tstg3bmj4He6ZnaPxnlF
```

Linux(Unix)의 경우

```
[AGENT] 예시

AgentID=DA
SiteCertFilePath=/dbms_api/key/kms/damo-site_PENTA.cer
CertFilePath=/dbms_api/key/kms/damo-scp_PENTA-SA_TEST.cer
KeyFilePath=/dbms_api/key/kms/damo-scp_PENTA-SA_TEST.key
SPIN=Tstg3bmj4He6ZnaPxnlF
```

키 파일을 DA-MYQ 설치 폴더 하위의 '**key/kms 경로**'에 업로드할 것을 권장한다.

5. 모든 항목을 수정한 후, 설정 파일을 저장한다.

1.2.3.2 로그 설정하기

DA-MYQ에서 사용할 로그 생성 경로 및 로그 레벨을 설정한다.

로그 설정을 하는 방법은 다음과 같다.

1. DA-MYQ의 '**scpdb_agent.ini**' 설정 파일에서 [AGENT] 섹션으로 이동한다.
2. 아래의 표를 참고하여, 암호화 키 정보를 입력한다.

표 1-8 [AGENT] 설정

항목	설명
LogDir**(*)**	DA-MYQ의 각종 로그를 생성 할 절대 경로를 입력한다.
LogLevel**(*)**	DA-MYQ의 로그 수준을 입력한다. • 0: NO • 4: LEVEL4_ERROR(기본 값) • 6: LEVEL6_NOTICE • 8: LEVEL8_DEBUG

Windows(Windows Server)의 경우

```
[AGENT] 예시

LogDir=D:\dbms_api\log
LogLevel=4
```

Linux(Unix)의 경우

```
[AGENT] 예시

LogDir=/dbms_api/log
LogLevel=4
```

3. 모든 항목을 수정한 후, 설정 파일을 저장한다.

2.

암복호화 권한 설정 안내서

2.1 시작하기 전에

본 설명서는 **DA-MYQ 5.0**을 기반으로, **DA-MYQ 암복호화 권한을 설정하는 방법**에 대해 설명한다.

이때, DB 유저명은 'SCP', 권한을 부여하는 정책 이름은'KEY1'이라는 가정하에 설명한다.

2.2 CLI에서 암복호화 권한 설정하기

$DA_INST_HOME 디렉토리에서 DA-MYQ acl_cli 파일을 실행하여 DB 계정 단위로 암복호화 권한을 설정한다.

1. $DA_INST_HOME 디렉토리에서 DA-MYQ acl_cli 파일을 실행한다.
2. 다음을 참고하여 DA-MYQ acl_cli에 암복호화 권한 정책을 추가한다.
    a. **DB에 저장된 DB USER의 대소문자 여부를 확인하고 동일하게 입력해야 한다.**

```
SET PRIV ENC SCP"KEY1"1"1
```

3. 다음과 같이 DA-MYQ acl_cli에 설정한 암복호화 권한 정책을 저장한다.

```
SAVE ALL
```

4. 암복호화 권한 정책이 제대로 적용되었는지 조회해서 확인한다.

```
SHOW PRIV ENC SCP
```

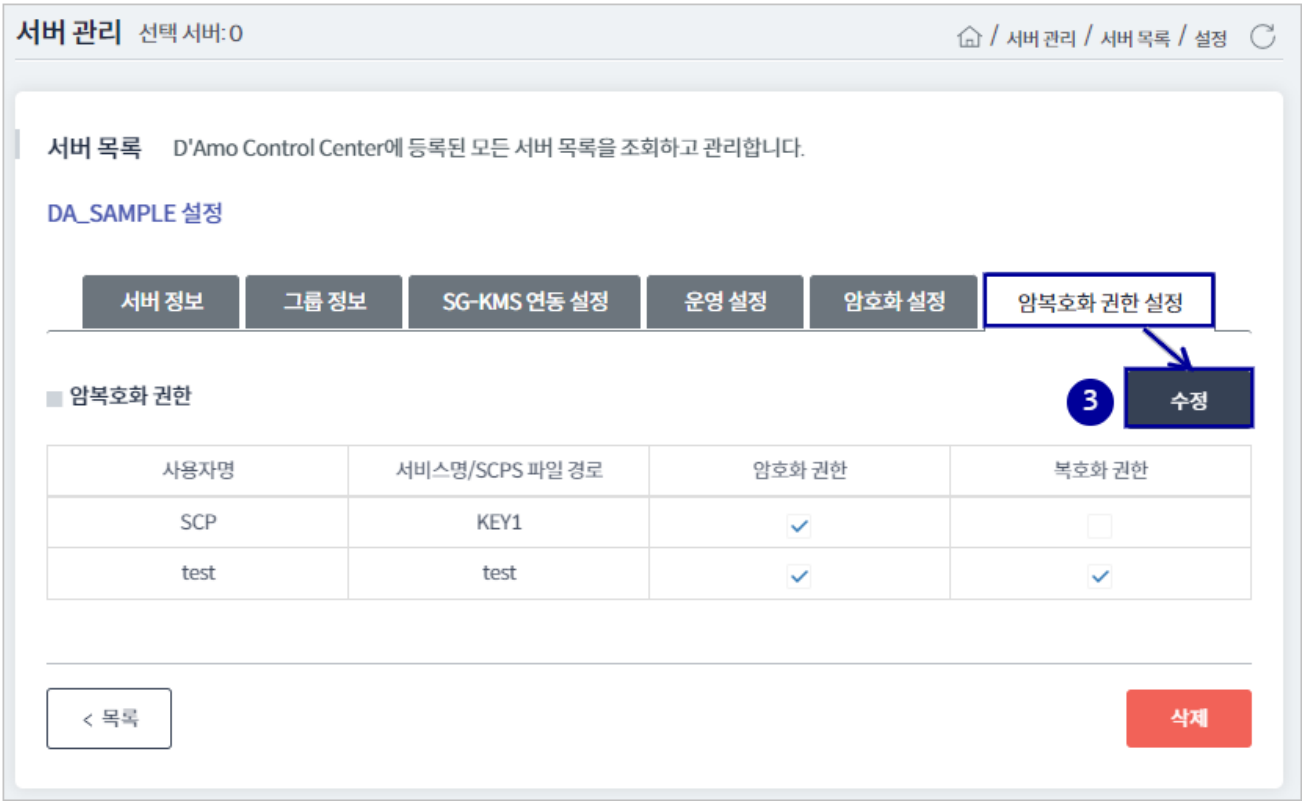
DA-MYQ acl_cli에 대한 자세한 설명은, <DA-MYQ 운영 설명서>를 참고한다.

2.3 D'Amo Control Center에서 암복호화 권한 설정하기

D'Amo Control Center 관리도구에서 DA-MYQ 의 암복호화 권한을 설정할 수 있다.

1. D'Amo Control Center 관리도구에서 [서버 관리] - [서버 목록]으로 이동한다.
2. 암복호화 권한을 설정할 DA-MYQ 서버의 을 클릭한다.
3. [암복호화 권한 설정] 탭을 클릭한 후, [수정]을 클릭한다.

그림 2-1 암복호화 권한 설정 화면

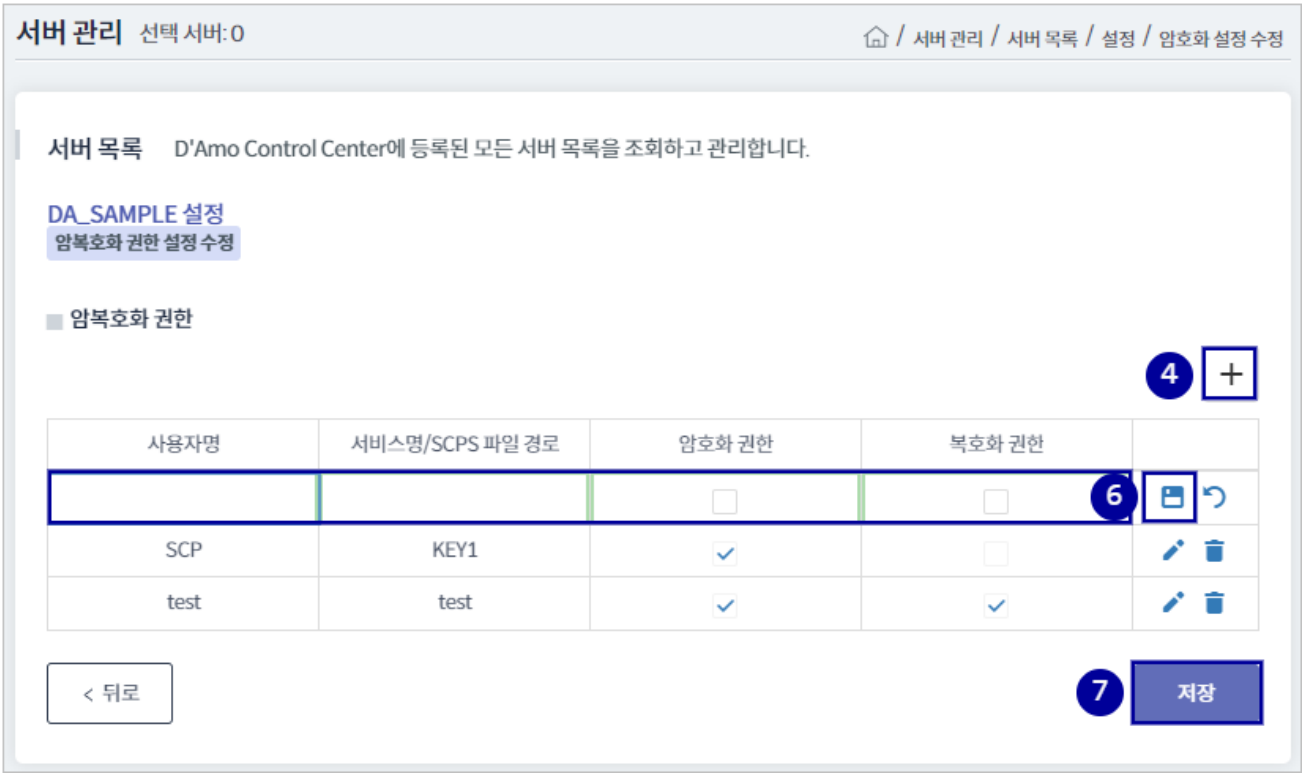


4. 암복호화 권한에서 + 아이콘을 클릭하여 권한을 추가한다.
5. 아래의 표를 참고하여, 각 항목에 알맞은 값을 입력한다.

표 2-1 암호화 설정_암복호화 권한

구분	항목	설명
암복호화 권한	공통	• OS 계정 단위로 암복호화 권한을 설정한다. • 암복호화 권한 설정이 가능한 라이선스를 사용할 경우에만 설정할 수 있다.
	사용자명(*)	• 권한을 적용하고자 하는 DB의 계정명을 입력한다. • DB에 저장된 DB USER의 대소문자 여부를 확인하고 동일하게 입력해야 한다.
	서비스명/SCPS 파일 경로(*)	• 정책에 할당할 ServiceID나 SCP 키 파일명을 입력한다. • SG-KMS의 ServiceID에 대한 정책을 추가할 경우, SG-KMS의 암호화 서비스를 입력한다. 예) SP1 • SCP 키 파일 관련 정책을 추가할 경우, SCP 키 파일(애플리케이션에서 입력되는 절대 경로)를 입력한다. 예) /dbms_api/key/SP1.SCPS
	암호화 권한(*)	암호화 권한을 설정한다. • 체크박스 선택: 암호화 가능 • 체크박스 미선택: 암호화 불가 (기본값)
	복호화 권한(*)	복호화 권한을 설정한다. • 체크박스 선택: 복호화 가능 • 체크박스 미선택: 복호화 불가 (기본값)

그림 2-2 암복호화 권한 설정하기



6. 아이콘을 클릭하여 입력한 값을 저장한다.
7. [저장]을 클릭하여 암복호화 권한을 설정한다.

8. 설정한 권한이 적용되었는지 서버 목록 설정의 [암복호화 권한]에서 확인한다.

3.

ACL CLI 키쌍 변경 안내서

3.1 시작하기 전에

본 설명서는 **DA-MYQ 5.0**을 기반으로, **DA-MYQ CLI 키쌍을 변경하는 방법**에 대해 설명한다.

3.2 CLI 키쌍 변경하기

$DA_INST_HOME 디렉터리에서 *DA-MYQ acl_cli -change*를 실행하여 CLI 키쌍을 변경할 수 있다.

기존에 등록한 key를 경로상에서 제거하지 않고 유지한 상태에서 진행한다.

Windows(Windows Server)에서 CLI 키쌍 변경하기

1. DA_INST_HOME 디렉터리에서 다음 파일을 백업한다.
   - key
   - log
   - privilege.damo
   - privilege.damo.backup
2. %DA_INST_HOME%₩key 경로로 이동한다.

```
cd %DA_INST_HOME%\key
```

3. CLI 키쌍의 이름을 다음과 같이 변경하여, %DA_INST_HOME%₩key 경로에 업로드한다.

```
damo_agt_new.cer
damo_agt_new.key
damo_agt_new.spin
```

4. DA_INST_HOME 경로로 이동한다.

```
cd %DA_INST_HOME%
```

5. CLI 키를 교체한다.

```
acl_cli.exe -change
```

6. 기존에 사용하던 CLI 키 비밀번호를 입력한다.

```
Enter the PIN of CLI-key. : <기존 CLI 키 비밀번호>
```

7. 변경할 CLI 키 비밀번호를 입력한다.

```
Enter the PIN of NEW CLI-key. : <새로운 CLI 키 비밀번호>
```

8. CLI 키를 변경한 후, 백업된 파일을 확인한다.

```
Success to Change Agent key. [backupDir : .\backup\20230110-100506]
```

표 3-1 백업 폴더 및 파일

패키지/키 파일명	설명
backup₩YYYYMMDD-HHMISS₩key	%DA_INST_HOME%₩key₩damo_agt.* 기존 CLI 키 쌍 복사
backup₩YYYYMMDD-HHMISS₩log	*.policy.log CLI 로그 복사
backup₩YYYYMMDD-HHMISS₩privilege.damo	권한 파일 복사
backup₩YYYYMMDD-HHMISS₩privilege.damo.backup	권한 백업 파일 복사

backupDir은 CLI 키쌍이 교체되는 시점에 생성된다.

Linux(Unix)에서 CLI 키쌍 변경하기

1. $DA_INST_HOME 디렉터리에서 다음 파일을 백업한다.
   - key
   - log

- privilege.damo
- privilege.damo.backup

2. $DA_INST_HOME/key 경로로 이동한다.

```
cd $DA_INST_HOME/key
```

3. CLI 키쌍의 이름을 다음과 같이 변경하여, $DA_INST_HOME/key 경로에 업로드한다.

```
damo_agt_new.cer
damo_agt_new.key
damo_agt_new.spin
```

4. $DA_INST_HOME 경로로 이동한다.

```
cd $DA_INST_HOME
```

5. CLI 키를 교체한다.

```
./acl_cli -change
```

6. 기존 사용하던 CLI 키 비밀번호를 입력한다.

```
Enter the PIN of CLI-key. : 〈기존 CLI 키 비밀번호〉
```

7. 변경할 CLI 키 비밀번호를 입력한다.

```
Enter the PIN of NEW CLI-key. : 〈새로운 CLI 키 비밀번호〉
```

8. CLI 키를 변경한 후, 백업된 파일을 확인한다.

```
Success to Change Agent key. [backupDir : ./backup/20230110-100506]
```

표 3-2 백업 폴더 및 파일

패키지/키 파일명	설명
backup/YYYYMMDD-HHMISS/key	$DA_INST_HOME/key/damo_agt.* 기존 CLI 키 쌍 복사
backup/YYYYMMDD-HHMISS/log	*.policy.log CLI 로그 복사
backup/YYYYMMDD-HHMISS/privilege.damo	권한 파일 복사
backup/YYYYMMDD-HHMISS/privilege.damo.backup	권한 백업 파일 복사

backupDir은 CLI 키쌍이 교체되는 시점에 생성된다.

파트 IV.

부록

여기에서는 제품 사용 시 필요한 추가 정보에 대해 기술한다.

1.

D'Amo 용어 정의

여기에서는 IT 일반 용어를 포함하여 D'Amo 제품에서 사용되는 용어에 대해 정의한다.

1.1 D'Amo 공통

D'Amo 제품 공통으로 사용되는 용어 중, 크게 일반적인 개념과 특정 키로 분류하여 정의한다.

1.1.1 개념 및 일반

표 1-1 D'Amo 공통 개념 및 일반

용어	정의
CLI (Command Line Interface)	제품의 운용을 위한 설정 작업을 할 수 있는 명령어 입력 기반의 관리도구이다.
관리도구	제품의 운용을 위한 설정 작업을 할 수 있는 GUI(Graphical User Interface) 입력 기반의 관리도구이다.
DCA (D'Amo Control Agent)	관리도구와 각 제품을 연결하는 서버이다.
서버	데이터 암복호화를 수행하는 D'Amo의 Agent 제품들을 통칭한다. • DP-ORA/DP-MSQ/DE-MYQ/DE-PGS/BA-SCP/KE-LNX 등
Security Library	DBMS에 탑재되는 제품의 구성 요소 중 하나로, 실제 암복호화를 수행한다.
Agent	D'Amo SG-KMS와 연동하여 데이터 암복호화를 수행하는 SA(Security Agent)를 포함한 Agent를 통칭한다.
암호화 컬럼	데이터가 암호화되어 있는 DB의 컬럼이다.
정책	암복호화에 필요한 키와 알고리즘의 정보(암호 알고리즘 ID, IV, 부분 암호화 범위)로 구성되며, '보안 정책'이라고도 말한다.
	• 회사·조직 내의 DB 보안 책임자, 또는 제품의 운용을 책임지는 담당자를 의미한다.

용어	정의
보안관리자	• 사이트 키 및 관리자 키를 생성·관리하고, 하위 운용자에게 관리자 키를 배포한다.

1.1.2 키

D'Amo 제품 공통으로 사용되는 각종 키에 대해 정의한다.

표 1-2 D'Amo 공통 키

용어	정의
컬럼 키	테이블의 컬럼을 암호화 할 때 사용하는 대칭키이다.
DB 키	• 비공개키와 공개키로 구성된 PKI 기반의 암호화 키이다. • 컬럼 키를 안전하게 보관하기 위한 암호화에 사용한다.
관리자 키	• CLI를 통한 로그인 시에 사용된다. • '*공개키 쌍*'으로 구성되어 있다. ◦ PKI 인증서 형식(x.509)의 '*공개키*' ◦ 암호화된 '*개인키*' • 보안 관리자가 관리도구에서 '생성·관리' 한다.
사이트 키	• CLI를 통해 모든 공개키 기반의 키 생성 시에 사용된다. • '*공개키 쌍*'으로 구성되어 있다. ◦ PKI 인증서 형식(x.509)의 '*공개키*' ◦ 암호화 된 '*개인 키*' • 보안 관리자가 CLI를 통해 생성(1회에 한함)하고 사용한다.
라이선스 키	• 제품에서 사용할 수 있는 기능과 기간을 설정하는데 사용한다. • 당사에서 운영하는 '라이선스 서버'를 통해 해당 키 발급을 신청하여 사용한다. ◦ 라이선스 서버는 별도 문의
사이트 공개키	사이트 공개키(사이트 인증서) 쌍의 일부로 암호화 주체끼리 공유하는 키이다.
사이트 비공개키	사이트 공개키 쌍의 일부로 암호화 시에 비공개로 사용된다.
DB 공개키	DB 키 쌍의 일부로 암호화 주체끼리 공유하는 키이다.
DB 비공개키	DB 키 쌍의 일부로 암호화 시에 비공개로 사용된다.

1.2 D'Amo 제품별

여기에서는 펜타시큐리티에서 정의한 D'Amo 제품 고유의 용어에 대해 정의한다.

1.2.1 D'Amo Control Center

Web UI로 제공되는 D'Amo Control Center에서 정의한 용어는 다음과 같다.

표 1-3 D'Amo Control Center

용어	정의
D'Amo Control Center 관리도구	D'Amo 제품 운영을 위해, 웹에서 사용 가능한 D'Amo Control Center 관리도구이다.
D'Amo Control Center 공개키	D'Amo Control Center 관리도구 공개키 쌍의 일부로 암호화 주체끼리 공유한다.
D'Amo Control Center 비공개키	D'Amo Control Center 관리도구 공개키 쌍의 일부로 암호화 시 비공개로 사용한다.
D'Amo Control Center 키 쌍	• 보안관리자 인증서로 D'Amo Control Center 관리도구를 사용하기 위한 키이다. • 공개키와 비공개키가 한 쌍을 이룬다.
보안관리자	• 관리도구 최초 로그인 시 등록하는 계정이다. • 관리도구에서 제공하는 모든 기능을 사용할 수 있다.
일반 사용자	• 보안관리자가 생성한 일반 계정이다. • 보안관리자가 부여한 사용 권한만 가진다.

1.2.2 SG-KMS 권한

웹 UI로 제공되는 SG-KMS에서는 권한을 다음과 같이 정의하고 있다.

표 1-4 SG-KMS 권한 관련 용어 정의

용어	정의
관리자	• 회사·조직 내의 DB 보안 책임자, 또는 제품의 운용을 책임지는 담당자를 의미한다. • '관리도구 최초 생성되는 계정'을 의미한다. • 관리도구를 통해, 보조 관리자를 '추가/변경/삭제' 가능하다. • 관리도구를 통해, 각종 키 및 암호화 정책 등에 대한 '추가/변경/삭제'가 가능하다.
로컬 보안 관리자	CLI를 통해, 제품의 내부 설정을 변경할 수 있는 권한을 가진다.
보조 관리자	• 관리자에 의해 생성된 계정을 의미한다. • 관리도구를 통해, 각종 키 및 암호화 정책 등에 대한 '추가/변경/삭제'가 가능하다.

1.2.3 SG-KMS 키

SG-KMS 중 각종 키에 대해 정의한 용어는 다음과 같다.

표 1-5 SG-KMS 키 관련 용어 정의

용어	정의
암호화 키	• 데이터 암호화 및 데이터 HMAC에 사용한다. • 대칭키 형태로 구성되어 있다. • 관리도구에서 '생성·관리' 한다.
비대칭키	• 데이터를 암호화 한다. • 관리도구에서 '생성·관리' 한다.
Agent 키	D'Amo SG-KMS와 제품을 포함한 Agent를 연동할 때 사용되는 키를 의미한다.
사이트 키	• CLI를 통해 모든 공개키 기반의 키 생성 시에 사용된다. • '*공개키 쌍*'으로 구성되어 있다. ◦ PKI 인증서 형식(x.509)의 '*공개키*' ◦ 암호화 된 '*개인 키*' • 보안관리자가 CLI를 통해 생성(1회에 한함)하고 사용한다.
라이선스 키	• 제품에서 사용할 수 있는 기능과 기간을 설정하는데 사용한다. • 당사에서 운영하는 '라이선스 서버'를 통해 해당 키 발급을 신청하여 사용한다. ◦ 라이선스 서버는 별도 문의
SPIN	• Secure Personal Identification Number의 약자로, 보안 개인 식별 번호를 의미한다. • SG-KMS에서는 인증서의 비밀번호를 암호화한다.

1.3 DB 암호 제품

DB 암호화 제품 내에서 공통으로 사용되는 용어를 정의한다.

1.3.1 암호화 알고리즘의 종류

본 제품에서 사용하는 암호화 알고리즘은 한국 표준(KS)을 포함하여, 아래의 표준 규격에 근거하여 사용한다.

표 1-6 암호화 알고리즘의 종류

표준 규격	알고리즘	설명
NIST[a]	DES (Data Encryption Standard)	• 평문을 64비트로 나눠 56비트의 키를 이용해 다시 64비트의 암호문을 만들어 내는 알고리즘 • 블록 암호(Block Cipher)의 일종으로 1977년 미국 NBS[b]에서 국가 표준으로 정한 대칭키 암호이다. • 현재, DES 보다 Triple-DES가 더 안전한 것으로 알려져 있으며 AES가 새 표준으로 정해져 있다.
	TDES	3DES라고도 하며, DES의 키 길이 단점을 보완하기 위해 각 데이터 블록에 DES를 3

표준 규격	알고리즘	설명
	(Triple Data Encryption Standard)	번 반복하는 암호화 알고리즘
	AES (Advanced Encryption Standard)	• 고급 암호화 표준이라고 불리며, 암복호화 과정에서 동일한 키를 사용하는 대칭키 알고리즘 • DES를 대체하기 위해 2001년 NIST에 채택되었다.
ISO[c] KS[d]	SEED	• 미국에서 수출되는 웹 브러우저 보안 수준이 40비트로 제한됨에 따라 128비트 보안을 위해 별도로 개발된 알고리즘 • 1999년 TTA에서 발표한 한국 표준(KS)으로 지정되었다.
	ARIA	• 경량 환경 및 하드웨어 구현을 위해 최적화 된 Involutional SPN 구조 • ISO 표준인 SEED와 함께 사용되는 국가 표준 128비트의 범용 블록 암호 알고리즘

a NIST(National Institute of Standards and Technology): 미국표준기술연구소
b NBS(National Bureau of Standards): 미국표준규격국, 현재의 NIST
c ISO(International Organization for Standardization): 국제표준화기구
d KS(Korean (Industrial) Standards): 한국공업표준규격

1.3.2 블록 암호(Block Cipher) 운영 모드의 종류

블록 암호는 TDES, SEED, AES 등 대칭 키 블록 암호 알고리즘을 사용할 때 암호화 할 정보가 블록 길이와 다를 경우에 사용하며, 운영 모드의 종류는 아래와 같다.

표 1-7 블록 암호(Block Cipher) 운영 모드의 종류

운영 모드	설명
초기화 벡터 (IV: Initialization Vector)	블록 암호화 시 첫 블록(128비트)을 암호화할 때 사용하는 데이터를 의미한다.
ECB Mode (Electric CodeBook)	• 전자 코드북 방식으로 블록 암호 운영 모드 중 가장 간단한 구조를 가진다. • 각 블록을 독립적으로 암호화 하며 초기화 벡터가 필요 없다.
CBC Mode (Cipher-Block Chaining)	• 암호 블록 체인 방식으로 1976년 IBM에 의해 개발되었다. • 블록의 평문과 앞 블록 암호문과의 배타적 논리합으로 암호화 한다. 블록 간의 의존 관계를 갖는 모드로서 보안적 특성이 뛰어남
CFB Mode (Cipher FeedBack)	• 암호 피드백 방식으로 CBC를 변형한 모드이다. • 고정 길이의 평문을 고정 길이의 암호문으로 변환하는 비밀 키 암호 방식을 사용하여 송수신에서 같은 길이의 비트 수 단위로 암호화한다. • 암호화 데이터 길이가 늘어나지 않는 것이 장점이다. • 단, 짧은 길이의 데이터에서 고정된 초기화 벡터(IV)를 사용할 경우 보안적 특성이 떨어질 수 있다.
OFB Mode (Output FeedBack)	평문이 직접 암호화 되지 않는 것은 CFB와 동일하지만 평문 블록과 암호 알고리즘의 출력을 XOR하여 암호문을 생성한다.
CTR (CounTeR)	블록 암호를 스트림 암호로 바꾸는 구조를 가진다.

운영 모드	설명
CFB_BYTE	CFB를 블록 길이 단위가 아닌, 바이트 단위로 처리한 운영 모드이다.

1.3.3 기타 DB 암호 제품의 용어 정의

표 1-8 기타 DB 암호 제품의 용어 정의

용어	설명
BASE64	• 바이너리 데이터(2진수)를 문자 코드의 영향을 받지 않는 공통 아스키(ASCII) 문자로 표현하기 위해 만들어진 인코딩 방식 중 하나이다. • 8비트짜리 바이트 3개를 6비트씩 4개로 쪼개서 Base64 코드 4개로 바꾸어 표현한다. • 메일에서 이미지, 오디오 파일을 보낼 때 이용하는 코딩으로 모든 플랫폼에서 안 보이거나 해독할 수 없는 현상이 발생하지 않도록 공통으로 64개 아스키 코드를 이용하여 2진 데이터를 변환하기 위해 베이스 64를 이용한다. • 따라서 BASE64로 인코딩하면 크기가 원문에서 대략 33% 커진다.
HEXSTRING	• 바이너리 데이터(2진수)를 문자 코드에 영향을 받지 않는 공통 아스키(ASCII) 문자로 표현하기 위해 만들어진 인코딩 방식 중 하나이다. • 1byte 데이터를 16진수 2byte의 아스키 코드로 표현하는 방식으로, HEXSTRING으로 인코딩하면 크기가 2배로 커진다.
Hash	• 임의의 데이터로부터 일종의 짧은 '전자 지문'을 만들어 내는 방법이다. • 해시 함수는 데이터를 자르고 치환하거나 위치를 바꾸는 등의 방법을 사용해 결과를 만들어 내며, 이 결과를 흔히 해시 값(hash value)이라 한다. • 두 개의 데이터를 각각 해시한 후, 그 결과값이 다르다면 그 해시 값에 대한 원본 데이터도 다름을 보장한다. • 대표적인 Hash 함수로는 MD5, SHA1, SHA256, HAS-160 등이 있다.
HMAC	• MAC[a] 을 연산하는 특정 구조로 Hash 함수와 비밀 키의 조합으로 연산 된다. • 송신자와 수신자만 공유하고 있는 키와 데이터(메시지)를 혼합하여 해시값을 만든다. • MAC과 마찬가지로 메시지의 무결성 확인 뿐만 아니라 인증 기능으로도 사용된다.
SHA	• 미국 국가 안전 보장국(NSA)이 1993년에 처음으로 설계했으며 미국 표준 기술 연구소(NIST)에 의해 미국 국가 표준으로 지정된 Hash 함수이다. • SHA 함수군에 속하는 최초의 함수는 공식적으로 SHA라고 불리지만, 나중에 설계된 함수들과 구별하기 위하여 SHA-0이라고도 불린다.
BLOWFISH	• 1993년 브루스 슈나이어(Bruce Schneier)가 설계한 키(key)방식의 대칭형 블록 암호이다. • DES의 대안으로서 다른 알고리즘에 관련된 제약과 문제를 해결하기 위해 고안되었다. • BLOWFISH는 64비트 블록 크기, 또 32비트에서 최대 448비트에 이르는 가변 키 길이를 갖추고 있다. • 16라운드 파이스텔 암호로서 대형 키 의존 S박스를 이용한다. 구조는 수정된 S박스를 사용하는 CAST-128과 비슷하다.
RC4	• 로널드 라이베스트(Ron Rivest)가 만든 스트림 암호로, 전송 계층 보안(TLS)이나 WEP등의 여러 프로토콜에 사용되어 왔다. • 이후 여러 연구를 통해 취약한 것으로 밝혀졌으며, RC4를 사용한 WEP의 경우 해당 프로

용어	설명
	토콜의 사용을 권장하지 않는다.
PENTA_FFX	• NIST_FFX를 보완하여 펜타시큐리티의 자체 기술로 개발된 알고리즘 • 평문과 암호문에서 제외될 문자열의 타입을 사용자가 직접 지정한다.
PADDING	• 블록의 고정된 길이를 사용하기 위해 블록의 길이를 고정된 값으로 맞춤 • CBC, ECB 모드인 경우만 선택 가능 • NON-PADDING: 블록의 고정된 길이를 사용하지 않음

a MAC: Message Authentication Code

1.3.4 FPE 알고리즘의 암호화 규칙

FPE(Format Preserving Encryption)란 암호화 알고리즘 중 암호문과 평문의 형태(Format)를 그대로 보존하기 위한 암호 기술 중 하나이다.

아래의 문자 정의를 토대로, 각 알고리즘의 암호화 규칙을 설명한다.

- **대·소문자**: 영 대문자, 영 소문자
- **2바이트 문자열**: 한글, 일본어, 한자 등

표 1-9 FPE 알고리즘의 암호화 규칙

알고리즘	설명
FPE_NUM2SYMBOL	• 숫자가 포함된 문자열을 숫자가 없는 문자열로 암호화한다. • 숫자를 지정된 특수 문자의 형태로 암호화 하고, 그 외의 나머지 문자는 암호화에서 제외된다. ◦ 단, 입력 값에 지정된 특수 문자가 있는 경우에는 오류가 발생한다. ◦ 지정된 특수 문자: # $ % ^ = 〈 〉 ? ~ ;
FPE_NUM2SYMBOL2	• 숫자가 포함된 문자열을 숫자가 없는 문자열로 암호화한다. • 숫자를 지정된 특수 문자의 형태로 암호화 하고, 그 외의 나머지 문자들은 암호화 제외된다. ◦ 단, 입력 값에 지정된 특수 문자가 있는 경우에는 오류가 발생한다. ◦ 지정된 특수 문자: # $; ? [ ] ^ { } 〈
FPE_CHAR2CHAR	특수 문자를 포함하는 문자를, 특수 문자를 포함하는 문자로 암호화한다. ◦ 숫자, 영 대/소문자, 특수 문자 - 숫자, 영 대/소문자, 특수 문자
FPE_CHAR2CHAR_S	• FPE_CHAR2CHAR 운영 모드와 동일하지만 공백은 암호화하지 않는다. • 암호화 대상에 * | 과 같은 특수 문자는 포함할 수 없다. ◦ 숫자, 영문 대·소문자, 특수 문자 - 숫자, 영문 대·소문자, 특수문자
FPE_UCHAR2UCHAR	• 특수문자를 포함하는 영문 대문자를, 특수문자를 포함하는 영문 대문자로 암호화한다. ◦ 숫자, 영문 대문자, 특수문자 - 숫자, 영문 대문자, 특수문자
FPE_UCHAR2UCHAR_S	• FPE_UCHAR2UCHAR 운영 모드와 동일하지만 공백은 암호화하지 않는다. • 암호화 대상에 * | 과 같은 특수문자는 포함할 수 없다.

알고리즘	설명
	◦ 숫자, 영문 대문자, 특수문자 - 숫자, 영문 대문자, 특수문자
FPE_NUM2CHAR	• 숫자와 지정된 특수문자(- 공백)를, 특수문자를 포함하는 문자로 암호화한다. ◦ 숫자, 지정된 특수문자(- 공백) - 숫자, 영문 대/소문자, 특수문자
FPE_NUM2RRN	• 주민등록번호 형태의 숫자를 주민등록번호 형태가 아닌 숫자로 암호화한다. ◦ 숫자 - 숫자, 암호화 대상은 숫자만 입력 가능 • 주의 사항 ◦ 암호화 조건: 길이가 3이고 세 번째 자릿수가 0 또는 1인 경우만 ◦ 그 외는 입력된 평문 값을 그대로 결과 값으로 내보내고 성공을 리턴
FPE_KOR2KOR	• 특수 문자를 포함하는 한글을, 특수문자를 포함하는 한글로 암호화한다. ◦ 숫자, 영문 대·소문자, 특수문자, 2바이트 문자열 - 숫자, 영문 대·소문자, 특수문자, 2바이트 문자열
FPE_KOR2KOR_S	• FPE_KOR2KOR 운영 모드와 동일하지만 공백은 암호화하지 않는다. • 암호화 대상에 * | 과 같은 특수 문자는 포함할 수 없다. ◦ 숫자, 영문 대·소문자, 특수문자, 2바이트 문자열 - 숫자, 영문 대·소문자, 특수문자, 2바이트 문자열
FPE_PASSPORTID	• 여권 번호 형식의 데이터를 암호화한다. • 여권 번호는 아래의 두 형식 모두 지원한다. ◦ 숫자, 영문 대문자 - 숫자, 영문 대문자, 지정된 특수문자(! @ # $ % - ? = +)) ◦ 구 여권 번호: 공관 부호(2자리) + 여권 번호(7자리) ◦ 신 여권 번호: 여권의 종류(1자리) + 여권 번호(8자리)
FPE_NUM2CHAR_SYMBOL	• FPE_NUM2CHAR 운영 모드와 동일하며, 숫자를 문자로 암호화한다. • 공백, 특수문자는 암호화 하지 않는다. ◦ 숫자 - 숫자, 영문 대·소문자
FPE_CHAR2CHAR_SYMBOL	• FPE_CHAR2CHAR 운영 모드와 동일하며 공백, 특수문자는 암호화하지 않는다. ◦ 숫자, 영문 대·소문자 - 숫자, 영문 대·소문자
FPE_UCHAR2UCHAR_SYMBOL	• FPE_UCHAR2UCHAR 운영 모드와 동일하며, 공백, 특수문자는 암호화하지 않는다. ◦ 숫자, 영문 대문자 - 숫자, 영문 대문자
FPE_KOR2KOR_SYMBOL	• FPE_KOR2KOR 운영 모드와 동일하며 공백, 특수문자는 암호화하지 않는다. ◦ 숫자, 영문 대·소문자, 2바이트 문자열 - 숫자, 영문 대·소문자, 2바이트 문자열
FPE_KOR2UCHARKOR_SYMBOL	• 한글을 영문 대문자, 한글로 암호화하며 공백, 특수문자는 암호화하지 않는다. ◦ 숫자, 영 대문자, 2바이트 문자열 - 숫자, 영 대문자, 2바이트 문자열
FPE_ACCOUNT_SYMBOL	• 계좌번호 형식의 데이터를 암호화한다. • 숫자, 영문 대문자, 지정된 특수문자를 제외한 모든 문자는 암호화하지 않는다. ◦ 숫자, 영문 대문자 - 영문 대문자, 지정된 특수문자 ◦ 지정된 특수문자: # $ % ^ = 〈 〉 ? ~ ;

2.

함수 지원표

2.1 시작하기 전에

본 지원표는 **DA-MYQ 5.0**을 기준으로 **암호화 종류별 지원하는 함수**를 설명한다.

DA-MYQ의 함수마다 지원하는 기능이 다르므로, 반드시 지원하는 함수를 확인한 후 사용해야 한다.

2.2 양방향 암호화

양방향 암호화란, 평문을 암호화하여 복호화가 가능한 암호화 방식을 의미한다.

양방향 암호화는 다음과 같이 3가지로 분류할 수 있다.

표 2-1 양방향 암호화 종류

종류	설명
일반 암호화	평문 전체를 암호화하는 방식
부분 암호화	평문 중 일부를 암호화하는 방식
FPE 암호화	평문과 동일한 형식으로 암호화하는 방식

DA-MYQ의 함수별 양방향 암호화 지원 여부는 다음과 같다.

표 2-2 함수별 양방향 암호화 지원 여부

함수명	양방향 암호화		
	일반	부분	FPE
(ENC)DEC_STR	O	O	O
(ENC)DEC_B64	O	O	O(Str과 동일)

2.3 단방향 암호화

단방향 암호화란, 평문 암호화만 가능하고 복호화는 불가한 암호화 방식을 의미한다.

단방향 암호화는 일반적으로 2가지 방식으로 구분된다.

표 2-3 단방향 암호화 종류

종류	설명
HASH	일반적인 단방향 암호화 방식으로, 임의의 길이의 데이터를 고정된 길이의 데이터로 반환시켜 주는 암호화 방식
HMAC	암호화 키를 사용한 HASH 암호화 방식

DA-MYQ의 함수별 단방향 암호화 지원 여부는 다음과 같다.

표 2-4 함수별 단방향 암호화 지원 여부

함수명	단방향 암호화	
	HASH	HMAC
ENC_STR	X	O
ENC_B64	X	O
HASH_STR	O	X
HASH_B64	O	X

2.4 INDEX 함수

INDEX 함수란, DA-MYQ에서 암호화한 칼럼에 인덱스를 생성하거나 범위 검색 및 SELECT 성능을 향상시키기 위해 제공하는 암호화 함수를 의미한다.

INDEX 함수는 일반적으로 2가지 방식으로 구분된다.

표 2-5 INDEX 함수 종류

구분	INDEX 함수 예시
평문을 INDEX 형태로 정렬하는 함수	INDEX_STR, DEC_INDEX_STR
암호문을 INDEX 형태로 정렬하는 함수	DEC_INDEX_B64

3.

D'Amo_DA 오류코드 일람표

D'Amo 통합 오류코드는 제품 운용 시에 발생할 수 있는 오류코드를 정리한 문서로, 사용자가 해당 문제를 해결할 수 있는 **적절한 대응 방법을 안내**하기 위해 작성되었습니다.

다음 안내 방법으로 해결하지 못할 경우, 펜타시큐리티(주) 담당자에게 문의주십시오.

PDF 파일에 넣을 수 없는 내용이 있습니다. 웹 뷰어에서 확인할 수 있습니다.