시작하기

작업 흐름

다음 절차에서는 Firepower 4100/9300 새시 구성 시 완료해야 하는 기본 작업을 보여줍니다.

프로시저

단계 **1**	Firepower 4100/9300 새시 하드웨어를 구성합니다(*Cisco Firepower Security Appliance* 하드웨어 설치 가이드 참조).
단계 **2**	초기 구성을 완료합니다(초기 구성, 2 페이지 참고).
단계 **3**	Firepower Chassis Manager에 로그인합니다(로그인 또는 로그아웃 Firepower Chassis Manager, 9 페이지 참조).
단계 **4**	날짜 및 시간을 설정합니다(날짜 및 시간 설정 참고).
단계 **5**	DNS 서버를 구성합니다(DNS 서버 구성 참고).
단계 **6**	제품 라이선스를 등록합니다(ASA의 라이선스 관리 참고).
단계 **7**	사용자를 구성합니다(사용자 관리 참고).
단계 **8**	필요 시 소프트웨어 업데이트를 수행합니다(이미지 관리 참고).
단계 **9**	추가 플랫폼 설정을 구성합니다(플랫폼 설정 참고).
단계 **10**	인터페이스를 구성합니다(인터페이스 관리 참고).
단계 **11**	논리적 디바이스를 생성합니다(논리적 디바이스 참고).

초기 구성

Firepower Chassis Manager 또는 FXOS CLI를 사용하여 시스템을 구성하고 관리할 수 있으려면 먼저 몇 가지 초기 구성 작업을 수행해야 합니다. 콘솔 포트를 통해 액세스되는 FXOS CLI를 사용하거나 관리 포트를 통해 액세스하는 SSH, HTTPS 또는 REST API를 사용하여 초기 구성을 수행할 수 있습니다(이 절차를 로우 터치(low-touch) 프로비저닝이라고도 함).

콘솔 포트를 사용한 초기 구성

FXOS CLI를 사용하여 처음으로 Firepower 4100/9300 섀시에 액세스할 때 시스템을 구성하는 데 사용할 수 있는 설정 마법사가 나타납니다.

참고 초기 설정을 반복하려면 다음 명령을 사용하여 기존 구성을 지워야 합니다.

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

Firepower 4100/9300 섀시의 단일 관리 포트에는 IPv4 주소, 게이트웨이 및 서브넷 마스크 하나만, 또는 IPv6 주소, 게이트웨이 및 네트워크 접두사 하나만 지정해야 합니다. 관리 포트 IP 주소로 IPv4 또는 IPv6 주소 중 하나를 구성할 수 있습니다.

시작하기 전에

1. Firepower 4100/9300 섀시에서 다음의 물리적 연결을 확인합니다.
   - 콘솔 포트는 컴퓨터 터미널 또는 콘솔 서버에 물리적으로 연결됩니다.
   - 1Gbps 이더넷 관리 포트는 외부 허브, 스위치 또는 라우터에 연결됩니다.

   자세한 내용은 하드웨어 설치 가이드를 참조하십시오.
2. 콘솔 포트에 연결된 컴퓨터 터미널(또는 콘솔 서버)의 콘솔 포트 파라미터가 다음과 같은지 확인합니다.
   - 9600보드
   - 8 데이터 비트
   - 패리티 없음
   - 1 스톱 비트
3. 설정 스크립트에 사용할 다음 정보를 수집합니다.
   - 새 관리자 비밀번호
   - 관리 IP 주소 및 서브넷 마스크

- 게이트웨이 IP 주소
- HTTPS 및 SSH 액세스를 허용할 서브넷
- 호스트 이름 및 도메인 이름
- DNS 서버 IP 주소

프로시저

단계 **1** 새시 전원을 켭니다.

단계 **2** 터미널 에뮬레이터를 사용하여 시리얼 콘솔 포트에 연결합니다.

Firepower 4100/9300에는 RS-232-to-RJ-45 시리얼 콘솔 케이블이 포함되어 있습니다. 연결을 설정하려면 서드파티 시리얼-USB 케이블을 사용해야 할 수도 있습니다. 다음 시리얼 매개변수를 사용합니다.

- 9600보드
- 8 데이터 비트
- 패리티 없음
- 1 스톱 비트

단계 **3** 표시되는 화면 컨피그레이션을 완료합니다.

참고 초기 구성 중에 언제든지 선택적으로 debug(디버그) 메뉴에 진입하여 설정 문제를 디버깅하거나 구성을 중단하고 시스템을 리부팅할 수 있습니다. 디버그 메뉴를 시작하려면 Ctrl-C를 누릅니다. 디버그 메뉴를 종료하려면 Ctrl-D를 두 번 누릅니다. Ctrl-D를 처음 누른 후 두 번째 키를 누르는 동안 중간에 입력하는 모든 내용은 Ctrl-D를 두 번째 누른 후에 실행됩니다.

예제:

```
          ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the FXOS Supervisor is performed through these steps.

Type Ctrl-C at any time for more options or to abort configuration
and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.


You have chosen to setup a new Security Appliance.
      Continue? (yes/no): y

Enforce strong password? (yes/no) [y]: n

Enter the password for "admin": Farscape&32
```

```
  Confirm the password for "admin": Farscape&32
  Enter the system name:  firepower-9300

  Supervisor Mgmt IP address : 10.80.6.12

  Supervisor Mgmt IPv4 netmask : 255.255.255.0

  IPv4 address of the default gateway : 10.80.6.1

  The system cannot be accessed via SSH if SSH Mgmt Access is not configured.

  Do you want to configure SSH Mgmt Access? (yes/no) [y]: y

  SSH Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

  SSH Mgmt Access IPv4 netmask: 255.0.0.0

  Firepower Chassis Manager cannot be accessed if HTTPS Mgmt Access is not configured.

  Do you want to configure HTTPS Mgmt Access? (yes/no) [y]: y

  HTTPS Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

  HTTPS Mgmt Access IPv4 netmask: 255.0.0.0

  Configure the DNS Server IP address? (yes/no) [n]: y

    DNS IP address : 10.164.47.13

  Configure the default domain name? (yes/no) [n]: y

    Default domain name : cisco.com

  Following configurations will be applied:

    Switch Fabric=A
    System Name=firepower-9300
    Enforced Strong Password=no
    Supervisor Mgmt IP Address=10.89.5.14
    Supervisor Mgmt IP Netmask=255.255.255.192
    Default Gateway=10.89.5.1
    SSH Access Configured=yes
        SSH IP Address=10.0.0.0
        SSH IP Netmask=255.0.0.0
    HTTPS Access Configured=yes
        HTTPS IP Address=10.0.0.0
        HTTPS IP Netmask=255.0.0.0
    DNS Server=72.163.47.11
    Domain Name=cisco.com

  Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y
  Applying configuration. Please wait...  Configuration file – Ok
.....

Cisco FPR Series Security Appliance
firepower-9300 login:  admin
Password: Farscape&32
Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.

[...]
```

```
firepower-chassis#
```

관리 포트를 사용한 로우 터치(Low-Touch) 프로비저닝

Firepower 4100/9300 섀시이 부팅 시 시작 구성을 찾을 수 없는 경우, 디바이스는 Low-Touch 프로비저닝 모드를 시작하여, DHCP(Dynamic Host Control Protocol) 서버를 찾은 다음 관리 인터페이스 IP 주소를 사용하여 자체적으로 부트스트랩합니다. 그런 다음 관리 인터페이스를 통해 연결하여 SSH, HTTPS 또는 FXOS REST API를 사용하여 시스템을 구성할 수 있습니다.

참고 초기 설정을 반복하려면 다음 명령을 사용하여 기존 구성을 지워야 합니다.

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

Firepower 4100/9300 섀시의 단일 관리 포트에는 IPv4 주소, 게이트웨이 및 서브넷 마스크 하나만, 또는 IPv6 주소, 게이트웨이 및 네트워크 접두사 하나만 지정해야 합니다. 관리 포트 IP 주소로 IPv4 또는 IPv6 주소 중 하나를 구성할 수 있습니다.

시작하기 전에

설정 스크립트에 사용할 다음 정보를 수집합니다.

- 새 관리자 비밀번호
- 관리 IP 주소 및 서브넷 마스크
- 게이트웨이 IP 주소
- HTTPS 및 SSH 액세스를 허용할 서브넷
- 호스트 이름 및 도메인 이름
- DNS 서버 IP 주소

프로시저

단계 **1** Firepower 4100/9300 섀시의 관리 포트에 IP 주소를 할당하도록 DHCP 서버를 구성합니다.

Firepower 4100/9300 섀시의 DHCP 클라이언트 요청에는 다음이 포함됩니다.

- 관리 인터페이스의 MAC 주소입니다.
- DHCP 옵션 60(vendor-class-identifier) - "FPR9300" 또는 "FPR4100"으로 설정합니다.

- DHCP 옵션 61(dhcp-client-identifier) - Firepower 4100/9300 섀시 일련 번호로 설정합니다. 이 일련 번호는 섀시의 풀아웃 탭에서 확인할 수 있습니다.

단계 **2** Firepower 4100/9300 섀시의 전원을 켭니다.
섀시가 부팅될 때 시작 구성을 찾을 수 없는 경우, 디바이스는 Low-Touch 프로비저닝 모드를 시작합니다.

단계 **3** HTTPS를 사용하여 시스템을 구성하려면 다음을 수행합니다.

a) 지원되는 브라우저를 사용하여 주소 표시줄에 다음 URL을 입력합니다.

https://<*ip_address*>/api

여기서<*ip_address*>는 DHCP 서버에 의해 할당된 Firepower 4100/9300 섀시에 있는 관리 포트의 IP 주소입니다.

참고 지원되는 브라우저에 대한 정보는 사용 중인 버전에 대한 릴리스 노트를 참고하십시오 (http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html 참고).

b) 메시지가 표시되면 사용자 이름 **install** 및 비밀번호 <*chassis_serial_number*> 를 사용하여 로그인합니다.

<*chassis_serial_number*>는 섀시의 태그를 검사하여 얻을 수 있습니다.

c) 표시되는 화면 컨피그레이션을 완료합니다.

- 강력한 비밀번호 시행 정책(강력한 비밀번호 지침에 대해서는 사용자 계정 참고).
- 관리자 계정의 비밀번호.
- 시스템 이름
- 관리자 관리 IPv4 주소 및 서브넷 마스크, 또는 IPv6 주소 및 프리픽스.
- 기본 게이트웨이 IPv4 또는 IPv6 주소
- SSH 액세스가 허용되는 호스트/네트워크 주소 및 넷마스크/프리픽스.
- HTTPS 액세스가 허용되는 호스트/네트워크 주소 및 넷마스크/프리픽스.
- DNS 서버 IPv4 또는 IPv6 주소.
- 기본 도메인 이름

d) **Submit(**제출**)**을 클릭합니다.

단계 **4** SSH를 사용하여 시스템을 구성하려면 다음을 수행합니다.

a) 다음 명령을 사용하여 관리 포트에 연결합니다.

ssh install@<*ip_address*>

여기서 <*ip_address*>는 DHCP 서버에 의해 할당된 Firepower 4100/9300 섀시에 있는 관리 포트의 IP 주소입니다.

b) 메시지가 표시되면 비밀번호 **Admin123**을 사용하여 로그인합니다.

c) 표시되는 화면 컨피그레이션을 완료합니다.

참고 초기 구성 중에 언제든지 선택적으로 debug(디버그) 메뉴에 진입하여 설정 문제를 디버깅하거나 구성을 중단하고 시스템을 리부팅할 수 있습니다. 디버그 메뉴를 시작하려면 Ctrl-C를 누릅니다. 디버그 메뉴를 종료하려면 Ctrl-D를 두 번 누릅니다. Ctrl-D를 처음 누른 후 두 번째 키를 누르는 동안 중간에 입력하는 모든 내용은 Ctrl-D를 두 번째 누른 후에 실행됩니다.

예제:

```
          ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the FXOS Supervisor is performed through these steps.

Type Ctrl-C at any time for more options or to abort configuration
and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.


You have chosen to setup a new Security Appliance.
      Continue? (yes/no): y

Enforce strong password? (yes/no) [y]: n

Enter the password for "admin": Farscape&32
Confirm the password for "admin": Farscape&32
Enter the system name:  firepower-9300

Supervisor Mgmt IP address : 10.80.6.12

Supervisor Mgmt IPv4 netmask : 255.255.255.0

IPv4 address of the default gateway : 10.80.6.1

The system cannot be accessed via SSH if SSH Mgmt Access is not configured.

Do you want to configure SSH Mgmt Access? (yes/no) [y]: y

SSH Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

SSH Mgmt Access IPv4 netmask: 255.0.0.0

Firepower Chassis Manager cannot be accessed if HTTPS Mgmt Access is not configured.

Do you want to configure HTTPS Mgmt Access? (yes/no) [y]: y

HTTPS Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

HTTPS Mgmt Access IPv4 netmask: 255.0.0.0

Configure the DNS Server IP address? (yes/no) [n]: y

  DNS IP address : 10.164.47.13

Configure the default domain name? (yes/no) [n]: y
```

```
    Default domain name : cisco.com

  Following configurations will be applied:

    Switch Fabric=A
    System Name=firepower-9300
    Enforced Strong Password=no
    Supervisor Mgmt IP Address=10.89.5.14
    Supervisor Mgmt IP Netmask=255.255.255.192
    Default Gateway=10.89.5.1
    SSH Access Configured=yes
        SSH IP Address=10.0.0.0
        SSH IP Netmask=255.0.0.0
    HTTPS Access Configured=yes
        HTTPS IP Address=10.0.0.0
        HTTPS IP Netmask=255.0.0.0
    DNS Server=72.163.47.11
    Domain Name=cisco.com

  Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y
  Applying configuration. Please wait...  Configuration file - Ok
.....

Initial Setup complete, Terminating sessions
.Connection to <ip_address> closed.
```

단계 **5** FXOS REST API를 사용하여 시스템을 구성하려면 다음을 수행합니다.

REST API를 사용하여 시스템을 구성하려면 다음 예를 사용합니다. 자세한 내용은 https://developer.cisco.com/site/ssp/firepower/를 참고하십시오.

참고 dns, domain_name, https_net, https_mask, ssh_net 및 ssh_mask 속성은 선택 사항입니다. 다른 모든 속성은 REST API 구성에 필수입니다.

```
IPv4 REST API example:

{
    "fxosBootstrap": {
        "dns": "1.1.1.1",
        "domain_name": "cisco.com",
        "mgmt_gw": "192.168.0.1",
        "mgmt_ip": "192.168.93.3",
        "mgmt_mask": "255.255.0.0",
        "password1": "admin123",
        "password2": "admin123",
        "strong_password": "yes",
        "system_name": "firepower-9300",
        "https_mask": "2",
        "https_net": "::",
        "ssh_mask": "0",
        "ssh_net": "::"
    }
}


IPV6 REST API example

{
    "fxosBootstrap": {
        "dns": "2001::3434:4343",
        "domain_name": "cisco.com",
        "https_mask": "2",
```

```
        "https_net": "::",
        "mgmt_gw": "2001::1",
        "mgmt_ip": "2001::2001",
        "mgmt_mask": "64",
        "password1": "admin123",
        "password2": "admin123",
        "ssh_mask": "0",
        "ssh_net": "::",
        "strong_password": "yes",
        "system_name": "firepower-9300"
    }
}
```

로그인 또는 로그아웃 Firepower Chassis Manager

Firepower Chassis Manager를 사용하여 Firepower 4100/9300 섀시를 구성하려면 유효한 사용자 어카운트를 사용하여 로그인해야 합니다. 사용자 어카운트에 대한 자세한 내용은 사용자 관리 섹션을 참조하십시오.

일정 기간 동안 아무 작업도 하지 않으면 시스템에서 자동으로 로그아웃됩니다. 기본적으로는 10분 동안 작업을 하지 않으면 시스템에서 로그아웃됩니다. 이 시간 초과 설정을 구성하려면 세션 시간 초과 구성 섹션을 참조하십시오. 세션이 활성 상태이더라도 일정 기간이 지나면 사용자가 시스템에서 로그아웃되는 절대 시간 초과 설정을 구성할 수도 있습니다. 절대 시간 초과 설정을 구성하려면 절대 세션 시간 초과 구성 섹션을 참조하십시오.

Firepower Chassis Manager에서 자동으로 로그아웃하게 하는 모든 시스템 변경 사항 목록은 Firepower Chassis Manager 세션을 종료시키는 시스템 변경 사항 섹션을 참조하십시오.

참고 선택적으로, 로그인 시도 실패를 특정 횟수만큼만 허용하고 그 이후에는 지정된 시간 동안 사용자가 잠기도록 Firepower Chassis Manager를 구성할 수 있습니다. 자세한 내용은 최대 로그인 시도 횟수 설정를 참고하십시오.

프로시저

단계 **1** Firepower Chassis Manager에 로그인하려면 다음 작업을 수행하십시오.

a) 지원되는 브라우저를 사용하여 주소 표시줄에 다음 URL을 입력합니다.

https://<*chassis_mgmt_ip_address*>

여기서 <*chassis_mgmt_ip_address*>는 초기 구성을 설정하는 동안 입력한 Firepower 4100/9300 섀시의 IP 주소 또는 호스트 이름입니다.

참고 지원되는 브라우저에 대한 정보는 사용 중인 버전에 대한 릴리스 노트를 참고하십시오 (http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html 참고).

b) 사용자 이름 및 비밀번호를 입력합니다.

c) **Login(**로그인**)**을 클릭합니다.

로그인하면 Firepower Chassis Manager가 열리고 요약 페이지가 표시됩니다.

단계 **2** Firepower Chassis Manager에서 로그아웃하려면 네비게이션 바에서 사용자 이름을 가리킨 다음 **Logout(**로그아웃**)**을 선택합니다.
Firepower Chassis Manager에서 로그아웃되고 로그인 화면으로 돌아갑니다.

액세스 - FXOS CLI

콘솔 포트에 전원이 연결된 터미널을 사용하여 FXOS CLI에 연결할 수 있습니다. 콘솔 포트에 연결된 컴퓨터 터미널(또는 콘솔 서버)의 콘솔 포트 파라미터가 다음과 같은지 확인합니다.

- 9600보드
- 8 데이터 비트
- 패리티 없음
- 1 스톱 비트

또한 SSH 및 텔넷을 사용하여 FXOS CLI에 연결할 수 있습니다. FXOS는 최대 8개의 동시 SSH 연결을 지원합니다. SSH를 사용하여 연결하려면 Firepower 4100/9300 섀시의 IP 주소 또는 호스트 이름을 알아야 합니다.

다음 구문 예시 중에서 하나를 사용하여 SSH, 텔넷 또는 Putty를 통해 로그인할 수 있습니다.

참고 SSH 로그인은 대/소문자를 구분합니다.

SSH를 사용하는 Linux 터미널에서 다음 구문을 사용합니다.

- **ssh ucs-***auth-domain**username*@{*UCSM-ip-address* | *UCMS-ipv6-address*}

```
ssh ucs-example\\jsmith@192.0.20.11
ssh ucs-example\\jsmith@2001::1
```

- **ssh -l ucs-***auth-domain**username* {*UCSM-ip-address*| *UCSM-ipv6-address*| *UCSM-host-name*}

```
ssh -l ucs-example\\jsmith 192.0.20.11
ssh -l ucs-example\\jsmith 2001::1
```

- **ssh** {*UCSM-ip-address* | *UCSM-ipv6-address* | *UCSM-host-name*} **-l ucs-***auth-domain**username*

```
ssh 192.0.20.11 -l ucs-example\\jsmith
ssh 2001::1 -l ucs-example\\jsmith
```

- **ssh ucs-***auth-domain**username*@{*UCSM-ip-address* | *UCSM-ipv6-address*}

```
ssh ucs-ldap23\\jsmith@192.0.20.11
```

```
ssh ucs-ldap23\\jsmith@2001::1
```

텔넷을 사용하는 Linux 터미널에서 다음 구문을 사용합니다.

참고 텔넷은 기본적으로 비활성화되어 있습니다. 텔넷 활성화에 대한 지침은 텔넷 구성를 참고하십시오.

- **telnet ucs-***UCSM-host-name* **ucs-***auth-domain**username*

```
telnet ucs-qa-10
login: ucs-ldap23\blradmin
```

- **telnet ucs-**{*UCSM-ip-address* | *UCSM-ipv6-address*}*ucs-auth-domain**username*

```
telnet 10.106.19.12 2052
ucs-qa-10-A login: ucs-ldap23\blradmin
```

Putty 클라이언트에서 다음 구문을 사용합니다.

- 다음으로 로그인: **ucs-***auth-domain**username*

```
Login as: ucs-example\jsmith
```

참고 기본 인증이 로컬로 설정되어 있고 콘솔 인증이 LDAP으로 설정된 경우, **ucs-local\admin**을 사용하여 Putty 클라이언트에서 패브릭 인터커넥트에 로그인할 수 있으며 이때 admin은 로컬 어카운트의 이름입니다.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.