

外部認証用のLDAPを使用したFirepower Management CenterおよびFTDの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ネットワーク図](#)

[設定](#)

[FMC GUIでの基本的なLDAP設定](#)

[外部ユーザのシエルアクセス](#)

[FTDへの外部認証](#)

[ユーザ ロール](#)

[SSLまたはTLS](#)

[確認](#)

[テスト検索ベース](#)

[LDAP統合のテスト](#)

[トラブルシューティング](#)

[FMC/FTDとLDAPはどのように相互作用してユーザをダウンロードしますか。](#)

[ユーザログイン要求を認証するためにFMC/FTDとLDAPはどのように相互作用しますか。](#)

[SSLまたはTLSが期待どおりに機能しない](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco Authentication Management Center(FMC)およびFirepower Threat Defense(FTD)でMicrosoft Lightweight Directory Access Protocol(LDAP)外部Firepowerを有効にする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- シスコFTD
- Cisco FMC
- Microsoft LDAP

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- FTD6.5.0-123
- FMC 6.5.0-115
- Microsoft Server 2012

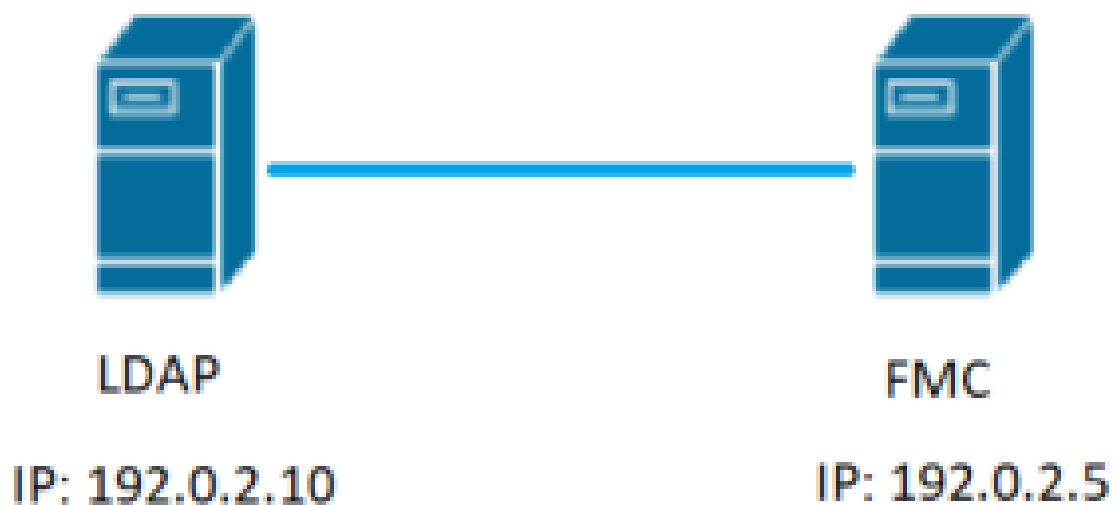
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

FMCと管理対象デバイスには、管理アクセス用のデフォルトの管理者アカウントが含まれています。FMCおよび管理対象デバイス上に、内部ユーザとして、またはモデルでサポートされている場合はLDAPまたはRADIUSサーバ上の外部ユーザとして、カスタムユーザアカウントを追加できます。外部ユーザ認証は、FMCとFTDでサポートされます。

- ・ 内部ユーザ：FMC/FTDデバイスは、ユーザ認証のためにローカルデータベースをチェックします。
- ・ 外部ユーザ：ユーザがローカルデータベースに存在しない場合、外部LDAPまたはRADIUS認証サーバからのシステム情報がユーザデータベースに入力されます。

ネットワーク図



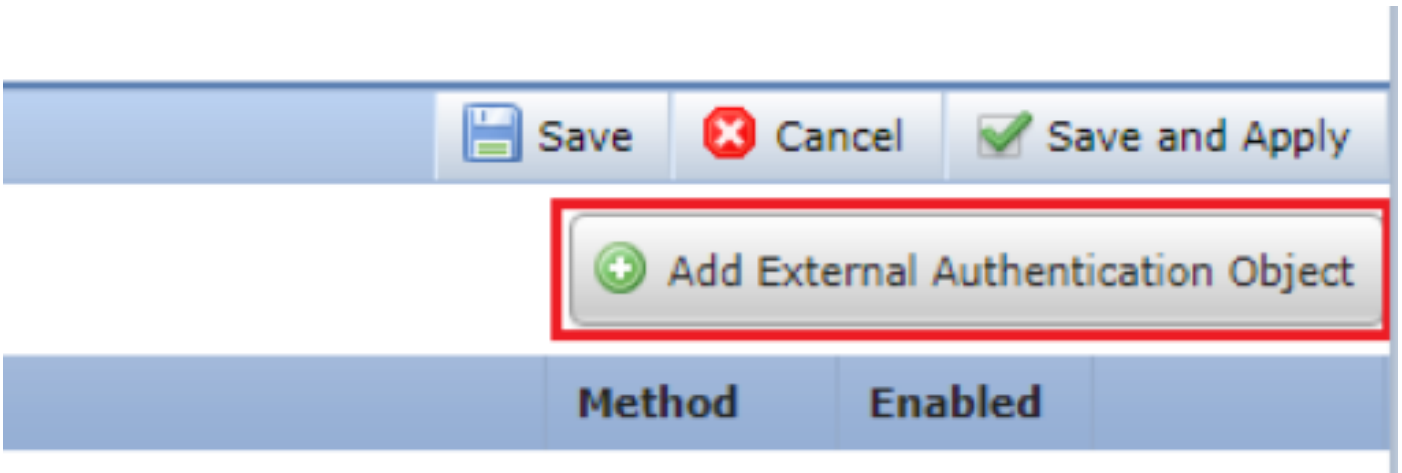
設定

FMC GUIでの基本的なLDAP設定

ステップ 1：移動先 System > Users > External Authentication：を入力します。



ステップ 2：選択 Add External Authentication Object：を入力します。



ステップ 3：次の必須フィールドに入力します。

External Authentication Object

Authentication Method: Use for CAC authentication and authorization

Name: Name the External Authentication Object

Description:

Server Type: Choose MS Active Directory and click 'Set Defaults'

Primary Server

Host Name/IP Address: ex. IP or hostname

Port: Default port is 389 or 636 for SSL

Backup Server (Optional)

Host Name/IP Address:

Port:

LDAP-Specific Parameters

*Base DN specifies where users will be found

Base DN: ex. dc=sourcefire,dc=com

Base Filter:

User Name: Username of LDAP Server admin

Password:

Confirm Password:

Show Advanced Options:

Attribute Mapping

*Default when 'Set Defaults' option is clicked

UI Access Attribute:

Shell Access Attribute:

Group Controlled Access Roles (Optional) ▼

Access Admin

Administrator

Discovery Admin

External Database User

Intrusion Admin

Maintenance User

Network Admin

Security Analyst

Security Analyst (Read Only)

Security Approver

Threat Intelligence Director (TID) User

View-Only-User (Read Only)

Default User Role To specify the default user role if user is not found in any group

Group Member Attribute

Group Member URL Attribute

Shell Access Filter

Shell Access Filter Same as Base Filter ex. (cn=jsmith), (cn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith*)))

(Mandatory for FTD devices)

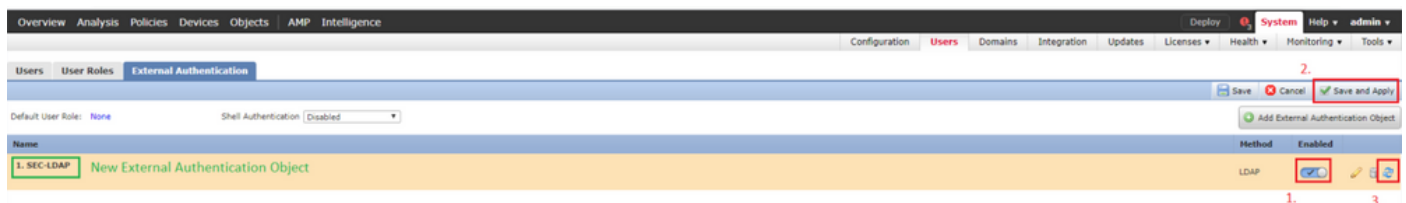
Additional Test Parameters

User Name

Password

*Required Field

ステップ 4：次を有効にします。 External Authentication オブジェクトと保存：



外部ユーザのシェルアクセス

FMCでは、Webインターフェイス用とCLIアクセス用の2つの異なる内部管理者ユーザがサポートされています。つまり、誰がGUIにアクセスできるのか、誰がCLIにアクセスできるのかということははっきりと区別されます。インストール時に、デフォルトの管理者ユーザのパスワードは、GUIとCLIの両方で同じになるように同期されますが、これらは異なる内部メカニズムによって追跡され、最終的には異なる場合があります。

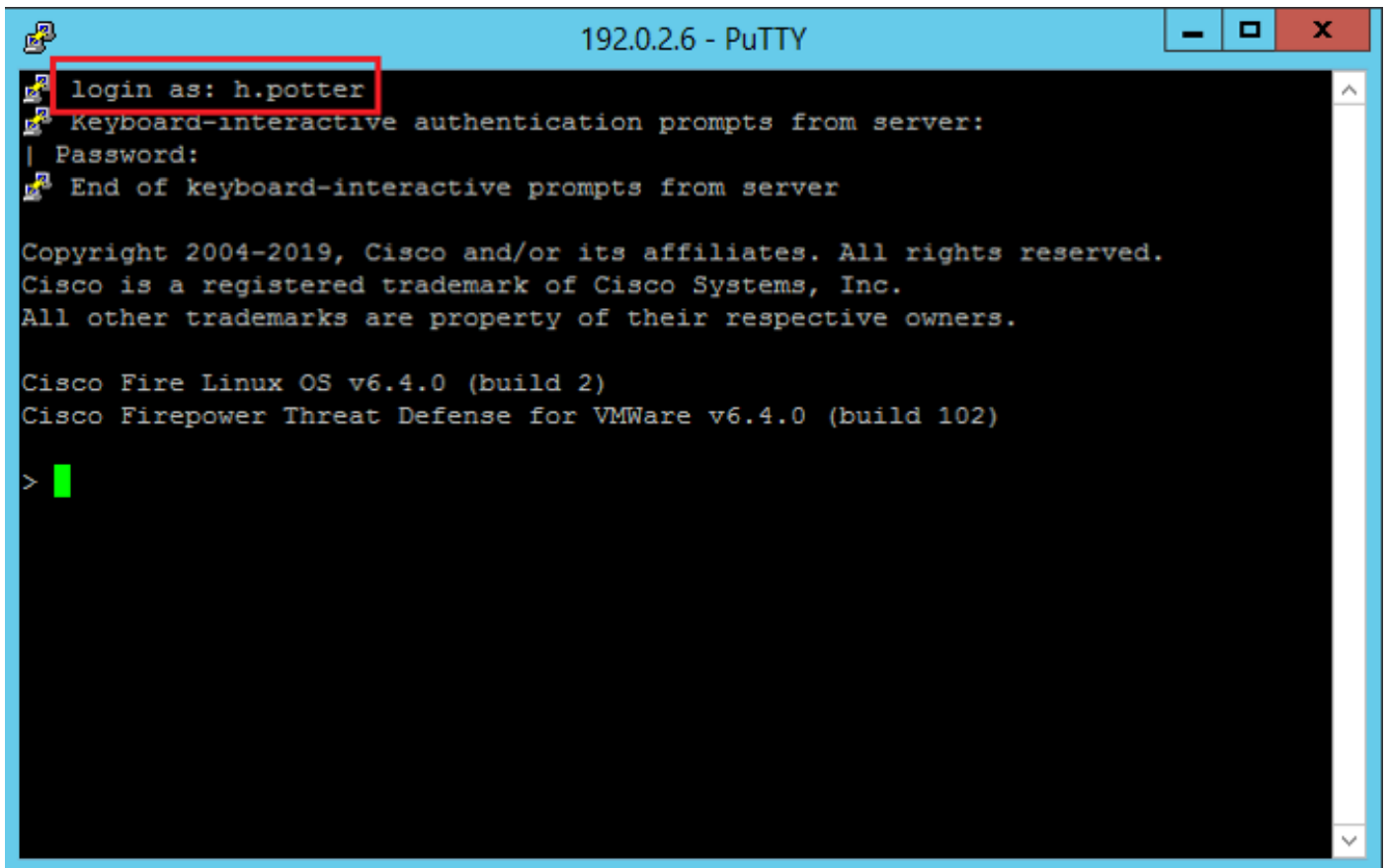
LDAP外部ユーザにもシェルアクセスを許可する必要があります。

ステップ 1：移動先 System > Users > External Authentication をクリックして Shell Authentication 図に示すドロップダウンボックスを使用して保存します。



ステップ 2 : FMCで変更を展開します。

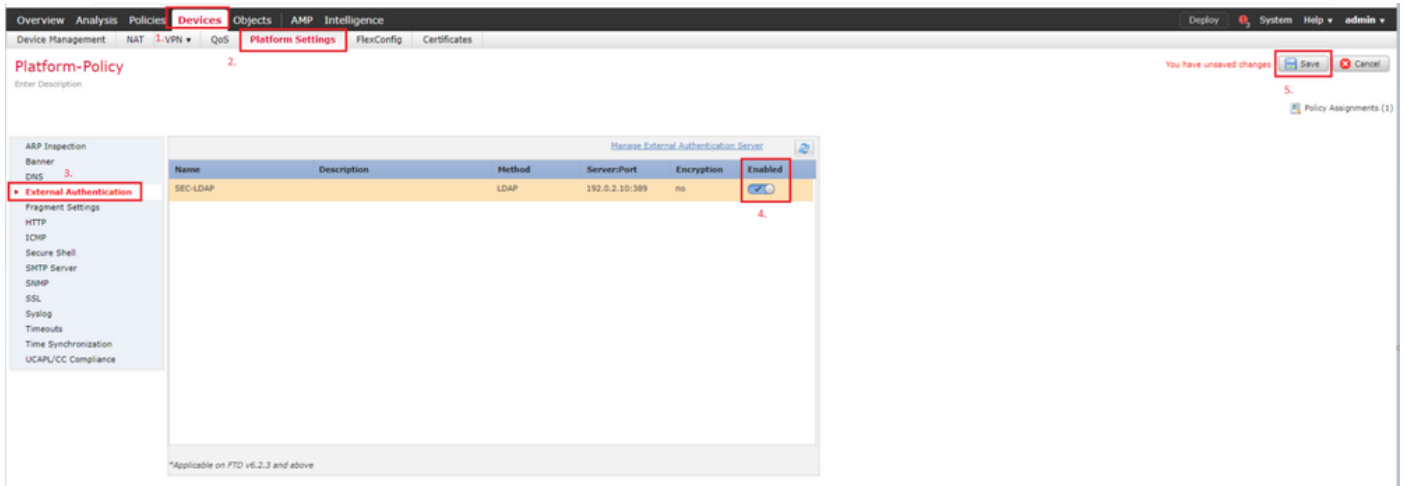
外部ユーザのシェルアクセスが設定されると、次の図に示すように、SSH経由のログインが有効になります。



FTDへの外部認証

外部認証はFTDでイネーブルにできます。

ステップ 1 : 移動先 [Devices > Platform Settings > External Authentication](#) を参照。クリック **Enabled** 保存します。



ユーザ ロール

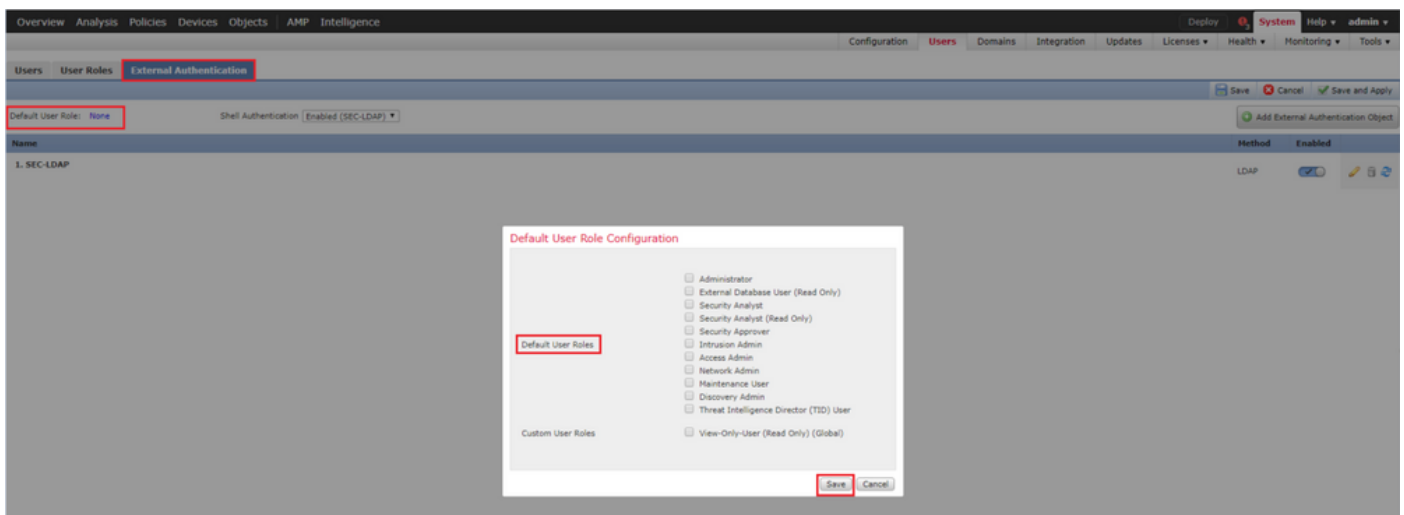
ユーザ権限は、割り当てられたユーザロールに基づきます。また、組織のニーズに合わせてアクセス権限を持つカスタムユーザロールを作成したり、セキュリティアナリストやディスクバリ管理者などの事前定義されたロールを使用することもできます。

ユーザロールには、次の2つのタイプがあります。

1. Webインターフェイスユーザロール
2. CLIユーザロール

事前定義されたロールの完全なリストと詳細については、「[ユーザロール](#)」を参照してください。

すべての外部認証オブジェクトのデフォルトユーザロールを設定するには、System > Users > External Authentication > Default User Roleを参照。割り当てるデフォルトのユーザロールを選択し、Saveを参照。



デフォルトのユーザロールを選択したり、特定のオブジェクトグループ内の特定のユーザに特定のロールを割り当てたりするには、オブジェクトを選択し、Group Controlled Access Roles 次の図に示すように、

Group Controlled Access Roles (Optional) ▾


Access Admin	<input type="text"/>
Administrator	<input type="text" value="h.potter@SEC-LAB"/>
Discovery Admin	<input type="text"/>
External Database User	<input type="text" value="s.rogers@SEC-LAB"/>
Intrusion Admin	<input type="text"/>
Maintenance User	<input type="text"/>
Network Admin	<input type="text" value="h.simpson@SEC-LAB"/>
Security Analyst	<input type="text" value="r.weasley@SEC-LAB"/>
Security Analyst (Read Only)	<input type="text"/>
Security Approver	<input type="text"/>
Threat Intelligence Director (TID) User	<input type="text"/>
View-Only-User (Read Only)	<input type="text" value="ma.simpson@SEC-LAB"/>

Default User Role

SSLまたはTLS

DNSはFMCで設定する必要があります。これは、証明書のサブジェクト値が `Authentication Object Primary Server Hostname` を参照。セキュアLDAPが設定されると、パケットキャプチャでクリアテキストのバインド要求が表示されなくなります。

SSLではデフォルトポートが636に変更され、TLSでは389のままになります。

 注: TLS暗号化では、すべてのプラットフォームで証明書が必要です。SSLの場合、FTDにも証明書が必要です。その他のプラットフォームでは、SSLに証明書は不要です。ただし、中間者攻撃を防ぐために、常にSSL用の証明書をアップロードすることをお勧めします。

ステップ 1: 移動先 `Devices > Platform Settings > External Authentication > External Authentication Object` SSL/TLSの詳細オプション情報を入力します。

LDAP-Specific Parameters

Base DN * ex. dc=sourcefire,dc=com

Base Filter ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)(!(cn=bsmith)(cn=csmith*)))

User Name * ex. cn=jsmith,dc=sourcefire,dc=com

Password *

Confirm Password *

Show Advanced Options ▼

Encryption SSL TLS None

SSL Certificate Upload Path No file chosen ex. PEM Format (base64 encoded version of DER)

User Name Template ex. cn=%s,dc=sourcefire,dc=com

Timeout (Seconds)

ステップ 2：サーバの証明書に署名したCAの証明書をアップロードします。証明書はPEM形式である必要があります。

LDAP-Specific Parameters

Base DN * ex. dc=sourcefire,dc=com

Base Filter ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)(!(cn=bsmith)(cn=csmith*)))

User Name * ex. cn=jsmith,dc=sourcefire,dc=com

Password *

Confirm Password *

Show Advanced Options ▼

Encryption SSL TLS None

SSL Certificate Upload Path CA-Cert-base64.cer ex. PEM Format (base64 encoded version of DER)

Certificate has been loaded (Select to clear loaded certificate)

User Name Template ex. cn=%s,dc=sourcefire,dc=com

Timeout (Seconds)

ステップ 3：設定を保存します。

確認

テスト検索ベース

LDAPが設定されているWindowsコマンドプロンプトまたはPowerShellを開き、次のコマンドを入力します。 `dsquery user -name`

を参照。

例：

```
PS C:\Users\Administrator> dsquery user -name harry*
PS C:\Users\Administrator> dsquery user -name *
```



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> dsquery user -name harr*
"CN=Harry Potter,CN=Users,DC=SEC-LAB
PS C:\Users\Administrator>
PS C:\Users\Administrator> dsquery user -name *
"CN=Administrator,CN=Users,DC=SEC-LAB
"CN=Guest,CN=Users,DC=SEC-LAB
"CN=krbtgt,CN=Users,DC=SEC-LAB
"CN=Anthony E. Stark,CN=Users,DC=SEC-LAB
"CN=Bart Simpson,CN=Users,DC=SEC-LAB
"CN=Dr. Robert B. Banner,CN=Users,DC=SEC-LAB
"CN=Ginny Weasley,CN=Users,DC=SEC-LAB
"CN=Harry Potter,CN=Users,DC=SEC-LAB
"CN=Hermione Granger,CN=Users,DC=SEC-LAB
"CN=Homer Simpson,CN=Users,DC=SEC-LAB
"CN=Lisa Simpson,CN=Users,DC=SEC-LAB
"CN=Maggie Simpson,CN=Users,DC=SEC-LAB
"CN=Marge Simpson,CN=Users,DC=SEC-LAB
"CN=Matthew Murdock,CN=Users,DC=SEC-LAB
"CN=Neville Longbottom,CN=Users,DC=SEC-LAB
"CN=Peter B. Parker,CN=Users,DC=SEC-LAB
"CN=Ron Weasley,CN=Users,DC=SEC-LAB
"CN=Steven Rogers,CN=Users,DC=SEC-LAB
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
```

LDAP統合のテスト

移動先 System > Users > External Authentication > External Authentication Object を参照。ページの下部に、Additional Test Parameters 図に示すセクション：

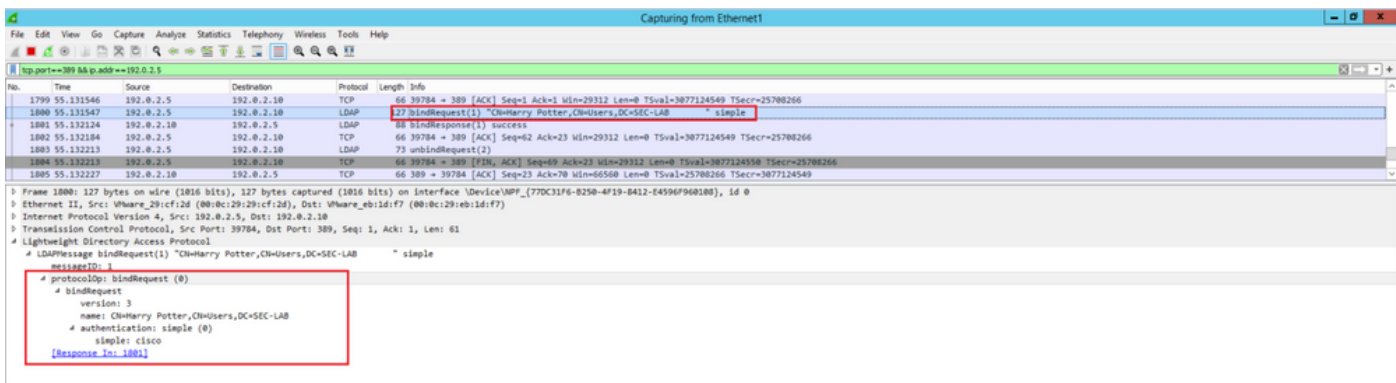
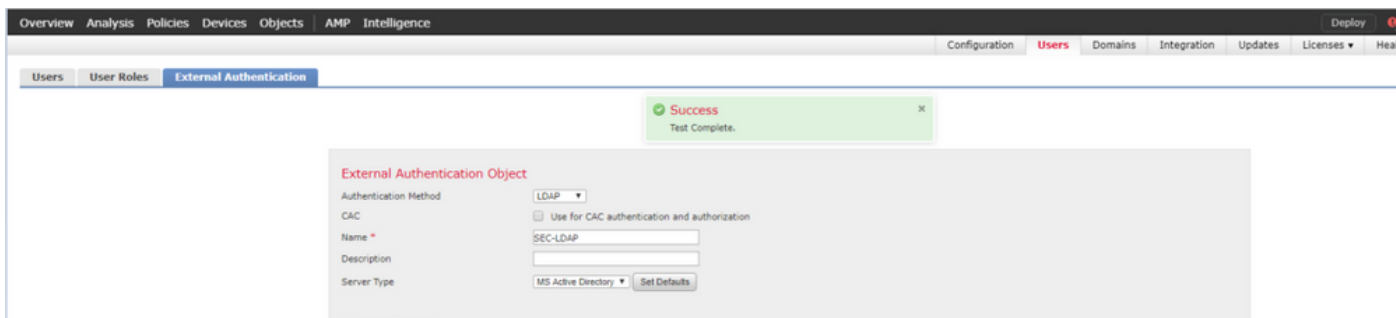
Additional Test Parameters

User Name

Password

*Required Field

結果を表示するには、Testを選択します。



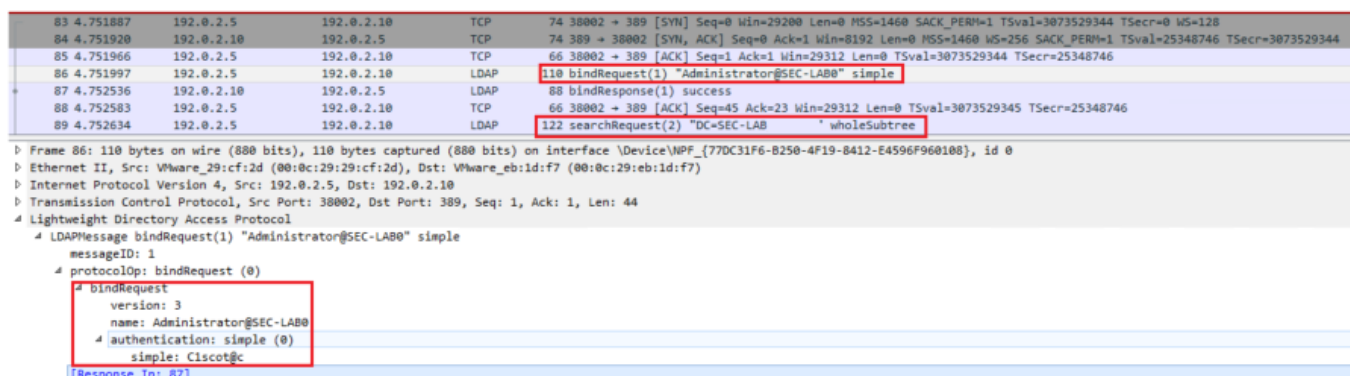
トラブルシューティング

FMC/FTDとLDAPはどのように相互作用してユーザをダウンロードしますか。

FMCがMicrosoft LDAPサーバからユーザをプルできるようにするには、FMCは最初に、LDAP管理者クレデンシャルを使用して、ポート389(SSL)または636(SSL)でバインド要求を送信する必要があります。LDAPサーバがFMCを認証できるようになると、成功メッセージで応答します。最後に、FMCは次の図に示すように、検索要求メッセージを使用して要求を行うことができます。

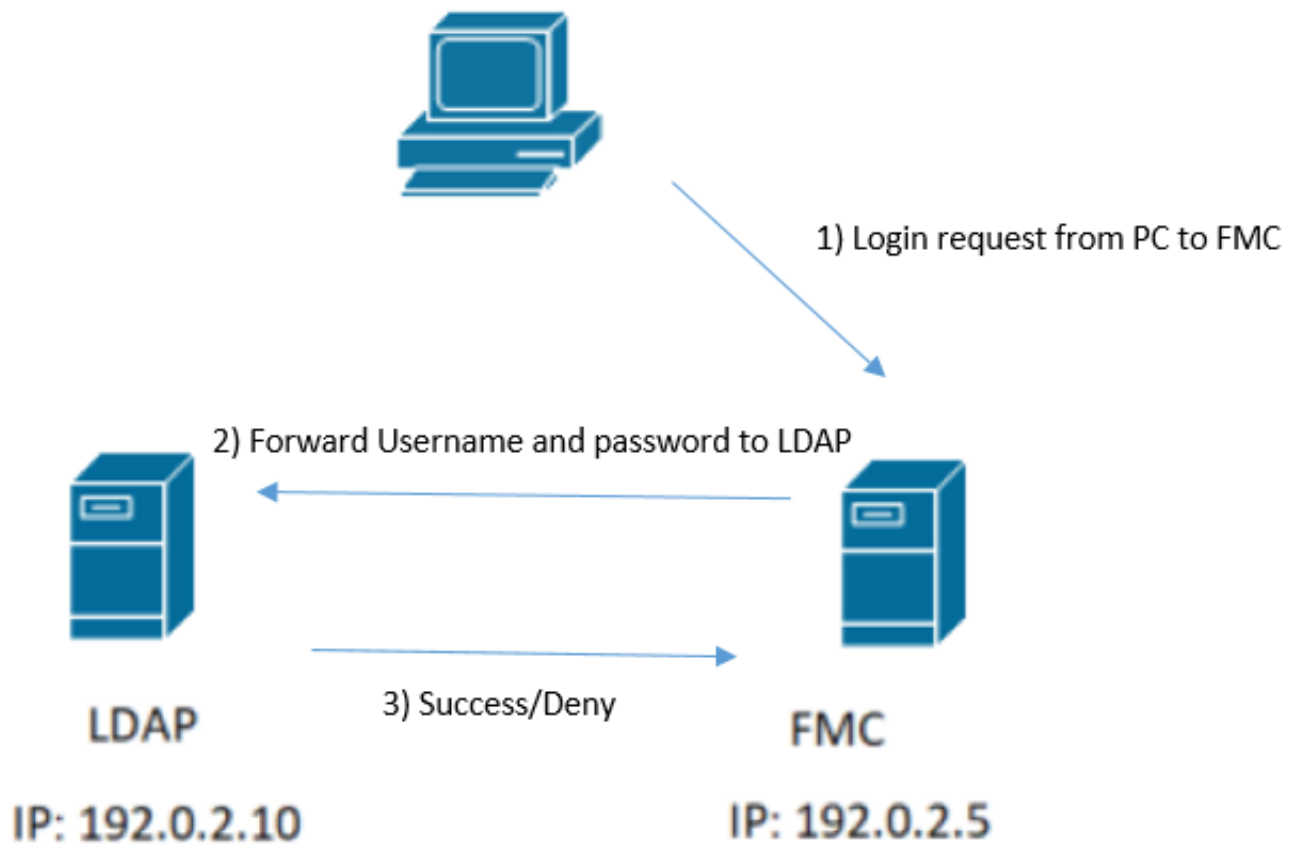
<< --- FMC sends: bindRequest(1) "Administrator@SEC-LAB0" simple LDAP must respond with: bindResponse(1) success --- >> << ---
 FMC sends: searchRequest(2) "DC=SEC-LAB,DC=NET" wholeSubtree

デフォルトでは、認証はクリアテキストでパスワードを送信することに注意してください。



ユーザログイン要求を認証するためにFMC/FTDとLDAPはどのように相互作用しますか。

LDAP認証が有効な状態でユーザがFMCまたはFTDにログインできるように、最初のログイン要求がFirepowerに送信されます。ただし、ユーザ名とパスワードはLDAPに転送され、成功/拒否応答が返されます。つまり、FMCとFTDはパスワード情報をデータベース内にローカルに保持せず、代わりに続行する方法に関するLDAPからの確認を待ちます。



No.	Time	Source	Destination	Protocol	Length	Info
58	13:11:59.695671	192.0.2.5	192.0.2.10	LDAP	110	bindRequest(1) "Administrator@SEC-LAB0" simple
59	13:11:59.697473	192.0.2.10	192.0.2.5	LDAP	88	bindResponse(1) success
67	13:11:59.697773	192.0.2.5	192.0.2.10	LDAP	110	bindRequest(1) "Administrator@SEC-LAB0" simple
69	13:11:59.699474	192.0.2.10	192.0.2.5	LDAP	88	bindResponse(1) success
97	13:11:59.729988	192.0.2.5	192.0.2.10	LDAP	127	bindRequest(1) "CN=Harry Potter,CN=Users,DC=SEC-LAB" simple
98	13:11:59.730698	192.0.2.10	192.0.2.5	LDAP	88	bindResponse(1) success

ユーザ名とパスワードが受け入れられると、次の図に示すようにWeb GUIにエントリが追加されます。

Username	Roles	Authentication Method	Password Lifetime
admin	Administrator	Internal	Unlimited
h.potter	Administrator	External	

ユーザ情報を確認するには、FMC CLISHでshow userコマンドを実行します。 > show user

コマンドは、指定したユーザの詳細な設定情報を表示します。次の値が表示されます。

Login : ログイン名

UID : 数値のユーザID

Auth (ローカルまたはリモート) : ユーザの認証方法

Access (BasicまたはConfig) : ユーザの特権レベル

有効 (有効または無効) : ユーザがアクティブかどうか

Reset (YesまたはNo) : ユーザが次回ログイン時にパスワードを変更する必要があるかどうか

Exp (NeverまたはNumber) : ユーザのパスワードを変更するまでの日数

Warn (N/Aまたは数値) : パスワードの有効期限が切れるまでにパスワードを変更するためにユーザに与えられる日数

Str (YesまたはNo) : ユーザのパスワードが強度チェックの基準を満たす必要があるかどうか

ロック (YesまたはNo) : ログインの失敗回数が多すぎるためにユーザーのアカウントがロックされているかどうか

Max (N/Aまたは数値) : ログインに失敗した回数の上限。この回数を超えると、ユーザのアカウントがロックされます。

SSLまたはTLSが期待どおりに機能しない

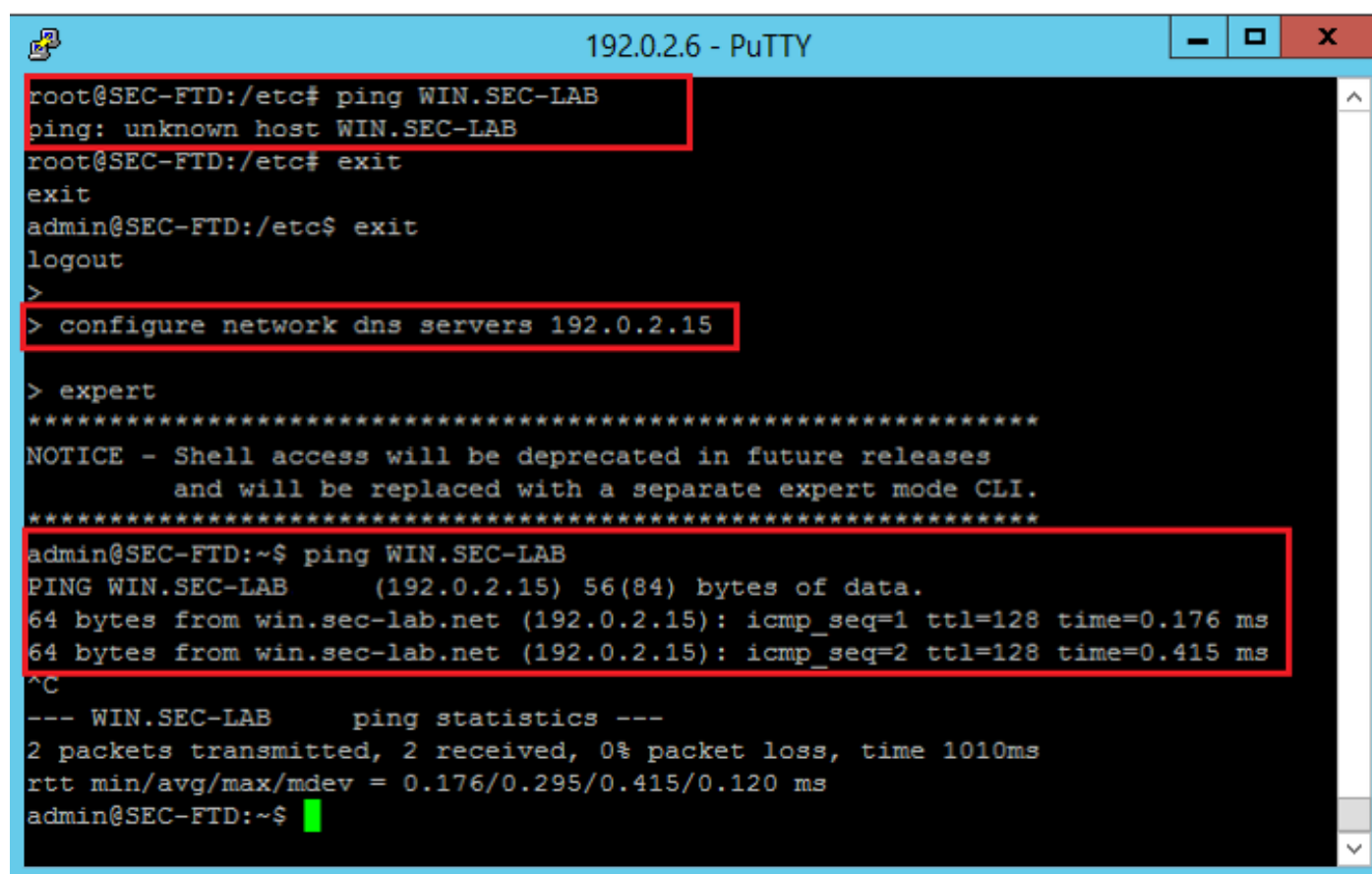
FTDでDNSを有効にしないと、ピグテールログにLDAPが到達不能であることを示すエラーが表示される場合があります。

```
root@SEC-FMC:/$ sudo cd /var/common
root@SEC-FMC:/var/common$ sudo pigtail
```

```
MSGs: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_unix(sshd:auth): authentication failure; logname= uid=0 e
MSGs: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_ldap: ldap_starttls_s: Can't contact LDAP server
MSGs: 03-05 14:35:33 SEC-FTD sshd[10138]: error: PAM: Authentication failure for h.potter from 192.0.2.
MSGs: 03-05 14:35:33 SEC-FTD sshd[10138]: Failed keyboard-interactive/pam for h.potter from 192.0.2.15
MSGs: 03-05 14:35:33 SEC-FTD sshd[10138]: error: maximum authentication attempts exceeded for h.potter
MSGs: 03-05 14:35:33 SEC-FTD sshd[10138]: Disconnecting authenticating user h.potter 192.0.2.15 port 61
```

firepowerがLDAPサーバのFQDNを解決できることを確認します。そうでない場合は、図に示すように正しいDNSを追加します。

FTD:FTD CLISHにアクセスし、次のコマンドを実行します。 > configure network dns servers



```
192.0.2.6 - PuTTY
root@SEC-FTD:/etc# ping WIN.SEC-LAB
ping: unknown host WIN.SEC-LAB
root@SEC-FTD:/etc# exit
exit
admin@SEC-FTD:/etc$ exit
logout
>
> configure network dns servers 192.0.2.15

> expert
*****
NOTICE - Shell access will be deprecated in future releases
         and will be replaced with a separate expert mode CLI.
*****
admin@SEC-FTD:~$ ping WIN.SEC-LAB
PING WIN.SEC-LAB (192.0.2.15) 56(84) bytes of data.
64 bytes from win.sec-lab.net (192.0.2.15): icmp_seq=1 ttl=128 time=0.176 ms
64 bytes from win.sec-lab.net (192.0.2.15): icmp_seq=2 ttl=128 time=0.415 ms
^C
--- WIN.SEC-LAB ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.176/0.295/0.415/0.120 ms
admin@SEC-FTD:~$
```

FMC : 選択 System > Configuration を選択し、次の図に示すように Management Interfaces を選択します

。

- Access List
- Access Control Preferences
- Audit Log
- Audit Log Certificate
- Change Reconciliation
- DNS Cache
- Dashboard
- Database
- Email Notification
- External Database Access
- HTTPS Certificate
- Information
- Intrusion Policy Preferences
- Language
- Login Banner
- Management Interfaces**
- Network Analysis Policy Preferences
- Process
- REST API Preferences
- Remote Storage Device
- SNMP
- Shell Timeout
- Time
- Time Synchronization
- UCAPL/CC Compliance
- User Configuration
- VMware Tools
- Vulnerability Mapping
- Web Analytics

Interfaces

Link	Name	Channels	MAC Address	IP Address	
<input checked="" type="checkbox"/>	eth0	Management Traffic Event Traffic	00:0C:29:29:CF:2D	192.0.2.5	

Routes

IPv4 Routes

Destination	Netmask	Interface	Gateway	
*			192.0.2.1	

IPv6 Routes

Destination	Prefix Length	Interface	Gateway	
-------------	---------------	-----------	---------	--

Shared Settings

Hostname: SEC-FMC

Domains:

Primary DNS Server: 192.0.2.10

Secondary DNS Server:

Tertiary DNS Server:

Remote Management Port: 8305

ICMPv6

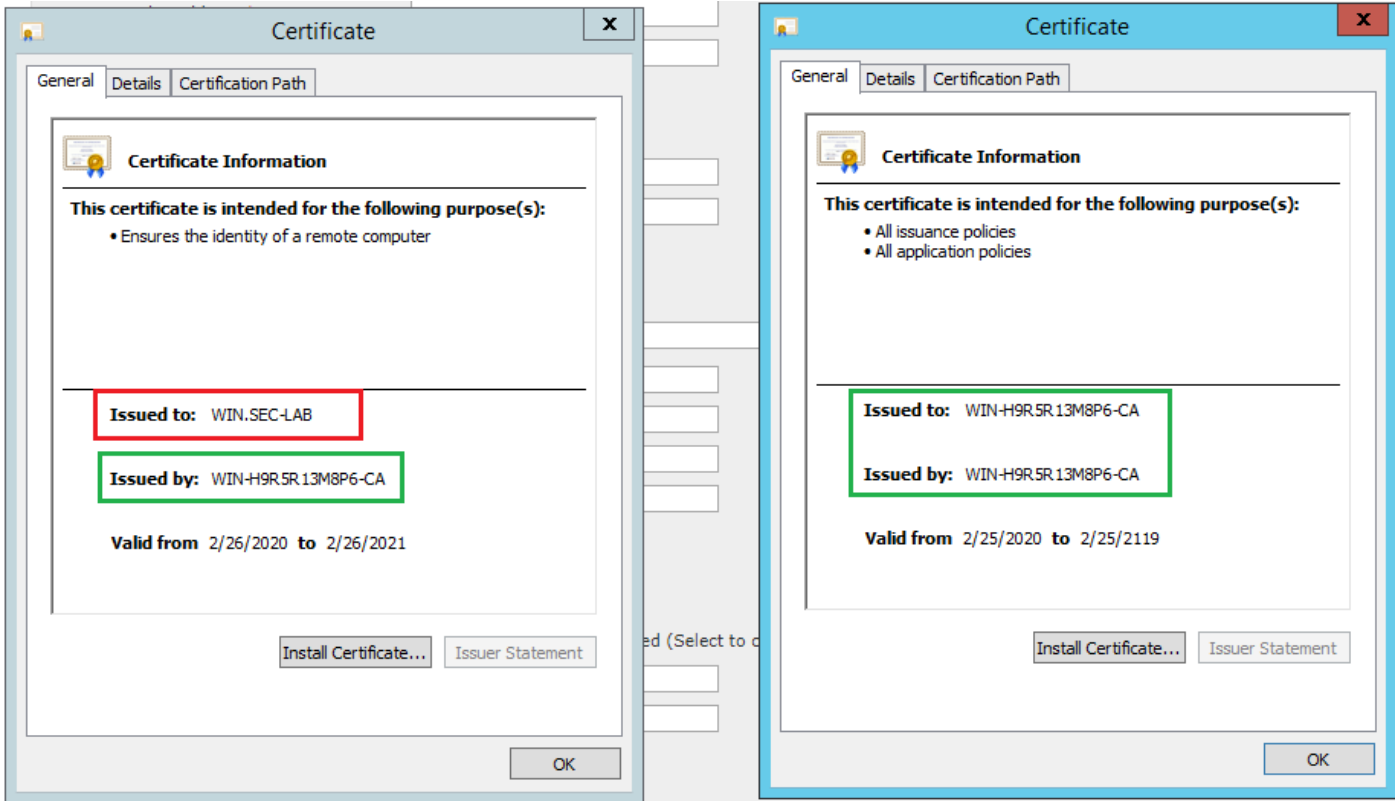
Allow Sending Echo Reply Packets:

Allow Sending Destination Unreachable Packets:

Proxy

Enabled:

次の図に示すように、FMCにアップロードされた証明書が、LDAPのサーバ証明書に署名したCAの証明書であることを確認します。



パケットキャプチャを使用して、LDAPサーバが正しい情報を送信していることを確認します。

The network capture shows the following details for the highlighted frame:

- Frame 33: 1515 bytes on wire (12120 bits), 1515 bytes captured (12120 bits) on interface \Device\NPF_{3EAD5E9F-B6CB-4EB4-A462-217C1A10A8FE}, id 0
- Ethernet II, Src: VMware_69:c8:c6 (00:0c:29:69:c8:c6), Dst: VMware_29:cf:2d (00:0c:29:29:cf:2d)
- Internet Protocol Version 4, Src: 192.0.2.15, Dst: 192.0.2.5
- Transmission Control Protocol, Src Port: 389, Dst Port: 52384, Seq: 47, Ack: 279, Len: 1449
- Transport Layer Security
 - Handshake Protocol: Multiple Handshake Messages
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 1444
 - Handshake Protocol: Server Hello
 - Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 1124
 - Certificates Length: 1121
 - Certificates (1121 bytes)
 - Certificate Length: 1118
 - Certificate: 3082045a30820342a0030201020213320000000456c380c8... id-at-commonName=WIN.SEC-LAB id-
 - signedCertificate
 - algorithmIdentifier (sha256WithRSAEncryption)
 - padding: 0
 - encrypted: 3645eb1128788982e7a5178f36022fa303e77bad1043bbdd...
 - Handshake Protocol: Server Key Exchange
 - Handshake Protocol: Certificate Request
 - Handshake Protocol: Server Hello Done
 - Handshake Type: Server Hello Done (14)
 - Length: 0

関連情報

- [管理アクセスのユーザーアカウント](#)

- [Cisco Firepower Management Center Lightweight Directory Access Protocol 認証バイパスの脆弱性](#)
- [FireSIGHT システムでの LDAP 認証オブジェクトの設定](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。