set コマンド

set absolute-session-timeout

絶対セッション タイムアウトを設定するには、**set absolute-session-timeout** コマンドを使用します。

set absolute-session-timeout *seconds*

構文の説明

seconds	Web、SSH、および Telnet セッションの絶対セッション タイムアウト。値は 0 ～ 3600 秒で指定できます。このタイムアウトを無効にするには、値を 0 に設定します。

コマンド モード

デフォルト認証（/security/default-auth）モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

セッションの使用状況に関係なく、指定したタイムアウト期間が経過すると、絶対セッション タイムアウトによってユーザ セッションは閉じられます。この絶対タイムアウトは、シリアル コンソール、SSH、HTTPS を含むすべての形式のアクセスに対してグローバルに適用されます。

例

次の例は、デフォルトの認証モードを開始し、すべてのセッションの絶対タイムアウトを 4 分に設定する方法を示しています。

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set absolute-session-timeout 240
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

関連コマンド

コマンド	説明
set refresh-period	Web セッション更新期間を設定します。
show detail	現在のセッションおよび絶対セッション タイムアウト設定を表示します。

set account-status

ローカル ユーザ アカウントをアクティブ化するか非アクティブ化するかを指定するには、**set account-status** コマンドを使用します。

set account-status {**active** | **inactive**}

構文の説明

active	ローカル ユーザ アカウントが有効になるように指定します。
inactive	ローカル ユーザ アカウントが無効になるように指定します。

コマンド モード

ローカル ユーザ（/security/local-user）モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、admin または AAA 権限を持つユーザである必要があります。

admin ユーザ アカウントは常にアクティブに設定されます。変更はできません。

例

次の例は、ローカルユーザモードを開始し、ローカルユーザアカウントを非アクティブ化する方法を示しています。

```
FP9300-A # scope security
FP9300-A /security # scope local-user test_user
FP9300-A /security/local-user # set account-status inactive
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

関連コマンド

コマンド	説明
set expiration	ユーザ アカウントが期限切れになる日付を指定します。

set address

Smart Call Home またはスマート ライセンスの宛先の電子メール アドレスまたは URL アドレスを設定するには、**set address** コマンドを使用します。

set address *address*

構文の説明

address	Smart Call Home またはスマート ライセンスの宛先の電子メール アドレスまたは URL。

コマンド モード

scope monitoring/scope callhome/scope profile/scope destination/

コマンド履歴

リリース	変更内容
1.4(1)	コマンドが追加されました。

使用上のガイドライン

各 Firepower 4100/9300 シャーシは、Smart Call Home ライセンス認証局またはスマート ライセンス サテライト サーバに登録する必要があります。このコマンドを使用して、電子メールまたは HTTP/HTTPS の URL アドレスをライセンスの宛先として設定します。

ライセンス認証局例: `https://tools.cisco.com/its/service/oddce/services/DDCEService`

サテライト サーバ例：`https://ip_address/Transportgateway/services/DeviceRequestHandler`

例

次の例は、Smart Call Home の宛先を作成する方法を示しています。

```
firepower # scope monitoring
firepower /monitoring # scope callhome
firepower /monitoring/callhome # scope profile SLProfile
firepower /monitoring/callhome/profile # scope destination SLDest
firepower /monitoring/callhome/profile/destination # set address
https://tools.cisco.com/its/service/oddce/services/DDCEService
firepower /monitoring/callhome/profile/destination* # commit-buffer
firepower /monitoring/callhome/profile/destination #
```

関連コマンド

コマンド	説明
create destination	新しい Smart Call Home の宛先を作成します。
delete destination	既存の Smart Call Home 宛先を削除します。
set protocol	Smart Call Home 宛先のトランスポート プロトコルを設定します。

set admin-state

Smart Call Home ポリシーの管理状態を有効または無効にするには、**set admin-state** コマンドを使用します。

set admin-state {**disabled** | **enabled**}

構文の説明

disabled	ポリシーの管理状態を無効に設定します。
enabled	ポリシーの管理状態を有効に設定します。

コマンド モード

scope monitoring/scope callhome/policy/

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、関連付けられた原因と一致する障害またはシステムイベントが発生した場合に、Call Home ポリシーをイネーブルまたはディセーブルにします。

例

次の例は、link-down イベントに対し Call Home ポリシーを開始し、イネーブルにする方法を示します。

```
firepower /monitoring/callhome # enter policy link-down
firepower /monitoring/callhome/policy* # set admin-state enabled
firepower /monitoring/callhome/policy* # commit-buffer
firepower /monitoring/callhome/policy #
```

関連コマンド

コマンド	説明
enter policy	Smart Call Home ポリシーを入力します。
delete policy	既存の Smart Call Home ポリシーを削除します。
scope policy	Smart Call Home ポリシーを有効にします。
show	Call Home の設定またはポリシーに関する情報を表示します。

set auth-server-group

デフォルトの認証サーバ グループを指定するには、**set auth-server-group** コマンドを使用します。

set auth-server-group *admin*

構文の説明

admin	認証サーバ グループの名前。

コマンド モード

デフォルト認証モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

例

次の例は、デフォルトの認証サーバ グループを指定する方法を示しています。

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set auth-server-group admin_server
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

関連コマンド

コマンド	説明
set realm	デフォルトの認証サービスを指定します。

set authentication

ログインする際およびコンソールポート経由で FXOS CLI に接続する際のユーザーのデフォルト認証方式を設定するには、 **set authentication** コマンドを使用します。

set authentication

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

scope security

コマンド履歴

リリース	変更内容
2.10(1)	コマンドが追加されました。

使用上のガイドライン

ログインする際およびコンソールポート経由で FXOS CLI に接続する際のユーザーのデフォルト認証方式を設定できます。

例

次の例は、セキュリティモードを開始し、デフォルト認証方式を設定する方法を示しています。

```
firepower# scope security
firepower /security # set authentication
  console  Console authentication
  default  Default authentication
```

関連コマンド

コマンド	説明
show authentication	既存の認証サービスを表示します。

set auto-negotiation

インターフェイスの自動ネゴシエーションを有効または無効にするには、**set auto-negotiation** コマンドを使用します。

set auto-negotiation {**on** | **off**}

構文の説明

on	（任意）自動ネゴシエーションがオンになります。
off	（任意）自動ネゴシエーションがオフになります。

コマンド モード

scope eth-uplink/scope fabric a/scope interface/

コマンド履歴

リリース	変更内容
2.1.1	コマンドが追加されました。

使用上のガイドライン

このコマンドは特定のポート タイプのみで機能します。

例

次の例は、自動ネゴシエーションを有効または無効にする方法を示しています。

```
Firepower-9300 # scope eth-uplink
Firepower-9300 /eth-uplink # scope fabric a
Firepower-9300 /eth-uplink #/fabric # scope interface Ethernet2/1
Firepower-9300 /eth-uplink/fabric/interface* # set auto-negotiation on
Firepower-9300 /eth-uplink/fabric/interface* # commit-buffer
Firepower-9300 /eth-uplink/fabric/interface #
```

関連コマンド

コマンド	説明
scope interface	インターフェイスのイーサネットインターフェイスの情報を表示します。

set cert

RSA 証明書をキーリングに追加するには、**set cert** コマンドを使用します。

set cert

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

キーリング モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

コマンドを入力すると、証明書のテキストを入力するように求められます。この末尾には **ENDOFBUF** を入力する必要があります。

例

次の例は、証明書のテキストをキーリングに入力する方法を示しています。

```
FP9300-A /security/keyring # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
>-----BEGIN CERTIFICATE-----
MIIFqDCCA5CgAwIBAgIBBDANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBAcMA1NKQzEOMAwGA1UECgwFQ2lzY28xDTALBgNV
BAsMBFNUQlUxCzAJBgNVBAMMAkNBMRowGAYJKoZIhvcNAQkBFgtzc3BAc3NwLm5l
dDAeFw0xNjEyMTUyMTM0NTRaFw>0yNjEyMTMyMTM0NTRaMHwxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJDQTEPMA0GA1UECgwGbmV3c3RnMRAwDgYDVQQLDAduZXdzdGJ1
MRMwEQYDVQQDDAppbnRlcm0xLWNhMSgwJgYJKoZIhvcNAQkBFhlpbnRlcm0xLWNh
QGludGVybTEtY2EubmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA
wLpNnyEx5I4P8uDoW>KWF3IZsegjhLANsodxuAUmhmwKekd0OpZZxHMw1wSO4IBX5
4itJS0xyXFzPmeptG3OXvNqCcsT+4BXl3DoGgPMULccc4NesHeg2z8+q3SPA6uZh
iseWNvKfnUjixbQEBtcrWBiSKnZuOz1cpuBn34gtgeFFoCEXN+EZVpPESiancDVh
8pCPlipc/08ZJ3o9GW2j0eHJN84sguIEDL812ROejQvpmfqGUq11stkIIuh+wB+V
VRhUBVG7p>V57I6DHeeRp6cDMLXaM3iMTelhdShyo5YUaRJMak/t8kCqhtGXfuLlI
E2AkxKXeeveR9n6cpQd5JiNzCT/t9IQL/T/CCqMICRXLFpLCS9o5S5O2B6QFgcTZ
yKR6hsmwe22wpK8QI7/5oWNXlolb96hHJ7RPbG7RXYqmcLiXY/d2j9/RuNoPJawI
hLkfhoIdPA28xlnfIB1azCmMmdPcBO6cbUQfCj5hSmk3StVQKgJCjaujz55TGGd1
G>jnxDMX9twwz7Ee51895Xmtr24qqaCXJoW/dPhcIIXRdJPMsTJ4yPG0BieuRwd0p
i8w/rFwbHzv4C9Fthw1JrRxH1yeHJHrLlZgJ5txSaVUIgrgVCJaf6/jrRRWoRJwt
AzvnzYql2dZPCcEAYgP7JcaQpvdpuDgq++NgBtygiqECAwEAAaNBMD8wDAYDVR0T
BAUwAwEB/zAvBgNVHR8EKDAmMCSgIqAghh5odHRwOi8vMTkyLjE2OC40LjI5>L2lu
dGVybS5jcmwwDQYJKoZIhvcNAQELBQADggIBAG/XujJh5G5UWo+cwTSitAezWbJA
h1dAiXZ/OYWZSxkFRliErKdupLqL0ThjnX/wRFfEXbrBQwm5kWAUUDr97D1Uz+2A
8LC5I8SWKXmyf0jUtsnEQbDZb33oVL7yXJk/A0SF0jihpPheMA+YRazalT9xj9KH
PE7nHCJMbb2ptrHUyvBrKSYrSeEqOpQU2+otnFyV3rS9aelgV>juaWyaWOc3lZ1Oi
CC2tJvY3NnM56j5iesxUCeY/SZ2/ECXN7RRBViLHmA3gFKmWf3xeNiKkxmJCxOaa
UWPC1x2V66I8DG9uUzlWyd79O2dy52aAphAHC6hqlzb6v+gw1Tld7UxaqVd8CD5W
ATjNs+ifkJS1h5ERxHjgcurZXOpR+NWpwF+UDzbMXxx+KAAXCI6ltCd8Pb3wOUC3
PKvwEXaIcCcxGx71eRLpWPZFyEoi4N2NGE9OXRjz0>K/KERZgNhsIW3bQMjcw3aX6
OXskEuKgsayctnWyxVqNnqvpuz06kqyubh4+ZgGKZ5LNEXYmGNz3oED1rUN636Tw
SjGAPHgeROzyTFDixCei6aROlGdP/Hwvb0/+uThIe89g8WZ0djTKFUM8uBO3f+II
```

```
/cbuyBO1+JrDMq8NkAjxKlJlp1c3WbfCue/qcwtcfUBYZ4i53a56UNF5Ef0rpy/8
B/+07Me/p2y9Luqa
-----END CERTIFICATE-----
ENDOFBUF
FP9300-A /security/keyring* #
```

関連コマンド

コマンド	説明
set modulus	RSA キー係数（SSL キーの長さ）をビット単位で指定します。
set regenerate	デフォルト キー リングで RSA キーを再生成します。
set trustpoint	キーリング証明書を再生成できるかどうかを指定します。

set certchain

現在のトラストポイントの証明書のリスト（またはチェーン）を入力するには、**set certchain** コマンドを使用します。

set certchain ［*cert_chain*］

構文の説明

cert_chain	（任意）認証局から取得した証明書チェーン。 この変数を省略すると、証明書情報を手動で入力するように求められます。

コマンド モード

トラストポイント モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

証明書は、Base64 エンコード X.509（CER）フォーマットである必要があります。

コマンドで証明書チェーンを指定しない場合、ルート認証局（CA）への認証パスを定義するトラストポイントのリストまたは証明書を入力するように求められます。入力を完了するには ENDOFBUF と入力します。

信頼証明書の取得については、『*Cisco FXOS CLI Configuration Guide*』の「Certificates, Key Rings, and Trusted Points」を参照してください。

例

次の例は、新しいトラストポイントを作成して入力し、このトラストポイントに証明書チェーンを貼り付ける方法を示しています。

```
FP9300-A # scope security
FP9300-A /security # enter trustpoint tPoint4
FP9300-A /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
```

```
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
FP9300-A /security/trustpoint* # commit-buffer
FP9300-A /security/trustpoint #
```

関連コマンド

コマンド	説明
enter trustpoint	トラストポイントを入力します。
show trustpoint	現在のトラストポイント情報を表示します。

set (certreq)

キーリング認証要求パラメータを指定するには、認証要求モードで**set**コマンドを使用します。

set {*country* | *dns* | *e-mail* | *fi-a-ip* | *fi-a-ipv6* | *fi-b-ip* | *fi-b-ipv6* | *ip* | *ipv6* | *locality* | *org-name* | *org-unit-name* | *password* | *state* | *subject-name* }

構文の説明

country	（任意）要求に2文字の国コードを指定します。文字は大文字で指定する必要があります。
dns	（任意）ネットワークに割り当てられるドメイン名（すべてのホスト名に共通）を指定します。これは *subject-name* の代わりです。
e-mail	（任意）要求に関連付けられた電子メールアドレスを指定します。
fi-a-ip	未使用。
fi-a-ipv6	未使用。
fi-b-ip	未使用。ファブリック インターコネクト B はありません。
fi-b-ipv6	未使用。ファブリック インターコネクト B はありません。
ip	（任意）デバイス ドメインの IPv4 アドレスを指定します。
ipv6	（任意）デバイス ドメインの IPv6 アドレスを指定します。
locality	（任意）証明書を要求している会社の本社が存在する市または町を指定します。 最大 64 文字まで入力できます。任意の文字、数字、スペース、および次の特殊文字を使用できます：,（カンマ）、.（ピリオド）、@（アット マーク）、^（キャラット）、(（開き括弧）、)（閉じ括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）。
org-name	（任意）証明書を要求している組織を指定します。 最大 64 文字まで入力できます。任意の文字、数字、スペース、および次の特殊文字を使用できます：,（カンマ）、.（ピリオド）、@（アット マーク）、^（キャラット）、(（開き括弧）、)（閉じ括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）。

org-unit-name	（任意）組織内の部門名を指定します。 最大 64 文字まで入力できます。任意の文字、数字、スペース、および次の特殊文字を使用できます：,（カンマ）、.（ピリオド）、@（アット マーク）、^（キャラット）、(（開き括弧）、)（閉じ括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）。
password	（任意）要求のパスワードを入力して確認するように求められます。
state	（任意）証明書を要求している会社の本社が存在する州または行政区分を指定します。 最大 64 文字まで入力できます。任意の文字、数字、スペース、および次の特殊文字を使用できます：,（カンマ）、.（ピリオド）、@（アット マーク）、^（キャラット）、(（開き括弧）、)（閉じ括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）。
subject-name	（任意）ローカル ファブリック インターコネクトの完全修飾ドメイン名を指定します。

コマンド モード

scope security/enter keyring/scope certreq/

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

認証要求を作成または入力した後は、次のオプションを使用して要求に関する情報を指定します。

例

次の例は、認証要求に関する情報を指定する方法を示しています。

```
firepower /security/keyring # enter certreq
firepower /security/keyring/certreq # set subject-name FP9300-1.testnet.com
firepower /security/keyring/certreq* # set password
Certificate request password:
Confirm certificate request password:
firepower /security/keyring/certreq* #
```

関連コマンド

コマンド	説明
create certreq	新しいキーリング認証要求を作成します。
delete certreq	既存のキーリング認証要求を削除します。

コマンド	説明
enter certreq	キーリング認証要求を入力します。
set (keyring)	モジュールとトラストポイントなど、キーリング関連の情報を設定します。

set (cfg-export-policy)

既存の設定エクスポート ポリシーのパラメータを指定または編集するには、configuration-export-policy モードで **set** コマンドを使用します。

set {**adminstate** | **descr** | **hostname** | **password** | **port** | **protocol** | **remote-file** | **schedule** | **user**}

構文の説明

adminstate {**disable** | **enable**	ポリシー管理を有効または無効にします。無効にすると、設定のバックアップがポリシー スケジュールに従ってエクスポートされません。
descr *description*	（任意）設定オブジェクトに説明を追加できます。説明は 1 ～ 256 文字で指定できます。ダッシュやアンダースコアのようにほとんどの英数字を使用できます。文字列の末尾には、セミコロン、ピリオド（終止符）、および感嘆符などの句読点を使用できますが、説明にはこれらの文字を埋め込むことはできません。
hostname *host_ID*	（任意）設定のバックアップのエクスポート先であるリモート サーバの IP アドレスまたはホスト名を指定します。このホストには、サーバ、ストレージアレイ、ローカル ドライブ、またはネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどを指定できます。 （注） 実際のホスト名を使用するには、設定された DNS サーバが利用可能である必要があります。
password	（任意）リモート サーバへの接続に使用するパスワードを指定します。パスワードを入力して確認するように求められます。
port {*number* | **default**}	（任意）リモート サーバとの通信に使用されるポートを変更できます。このオプションが指定されていない場合は、プロトコルのデフォルト ポートが使用されます。 オプションは、0 ～ 4294967295 のポート ID 番号です。現在のプロトコルのデフォルト ポートは **default** です。
protocol *name*	（任意）使用するファイル転送プロトコルを指定します。使用可能なオプションは次のとおりです。 • **ftp** • **scp** • **sftp** • **tftp**

remote-file *name*	（任意）エクスポートされた設定のファイル名を含むフルパスを指定します。1 ～ 128 文字で指定できます。
schedule {**bi-weekly** | **daily** | **weekly**}	（任意）設定が自動的にエクスポートされる頻度を指定します。 • **bi-weekly** ：2 週間ごとにエクスポートが実行されます。 • **daily** ：毎日エクスポートが実行されます。 • **weekly** ：1 週間に 1 回エクスポートが実行されます。
user *name*	（任意）リモート ホストへの接続に使用されるユーザ アカウント名を指定します。0 ～ 510 文字で指定できます。

コマンド モード

scope org/scope cfg-export-policy/

コマンド履歴

リリース	変更内容
1.1.1	コマンドが追加されました。

使用上のガイドライン

`set adminstate` を `enable` に変更し、`commit-buffer` コマンドをすぐに発行すると、設定のエクスポートがトリガーされます。

例

次の例は、デフォルトの設定エクスポート ポリシーを設定し、ポリシー パラメータを確認する方法を示しています。

```
firepower # scope org
firepower /org # scope cfg-export-policy default
firepower /org/cfg-export-policy # set protocol scp
firepower /org/cfg-export-policy* # set hostname 192.168.1.2
firepower /org/cfg-export-policy* # set remote-file /export/cfg-backup.xml
firepower /org/cfg-export-policy* # set user user1
firepower /org/cfg-export-policy* # set password
Enter a password:
Confirm the password:
firepower /org/cfg-export-policy* # set schedule weekly
firepower /org/cfg-export-policy* # set adminstate enable
firepower /org/cfg-export-policy* # commit-buffer
firepower /org/cfg-export-policy # show detail
Config Export policy:
    Name: default
    Description: Configuration Export Policy
    Admin State: Enable
    Protocol: Scp
    Hostname: 192.168.1.2
    User: user1
    Remote File: /export/cfg-backup.xml
    Schedule: Weekly
    Port: Default
    Current Task:
firepower /org/cfg-export-policy #
```

関連コマンド

コマンド	説明
export-config	現在のシステム設定をリモートサーバに XML ファイルとしてエクスポートします。エクスポート設定オブジェクトを作成します。
import-config	以前にエクスポートした XML コンフィギュレーション ファイルをこのアプライアンスにコピーします。
set password-encryption-key	設定のエクスポート中に機密情報を暗号化するときに使用されるキーを指定します。

set (cfg-export-reminder)

設定エクスポート通知オブジェクトのパラメータを指定または編集するには、configuration-export-reminder モードで **set** コマンドを使用します。

set {**adminstate** | **frequency**}

構文の説明

adminstate {**disable** | **enable**	エクスポートの通知を有効または無効にします。無効にすると、設定のバックアップ通知エラーは生成されません。
frequency *number_of_days*	設定をバックアップせずに経過する日数を指定します。この期間が経過すると、システムによって通知エラーが生成されます。この値は 1 ～ 365 日で指定できます。

コマンド モード

scope org/scope cfg-export-reminder/

コマンド履歴

リリース	変更内容
1.1.3	コマンドが追加されました。

使用上のガイドライン

通知が有効になっている場合は、設定のエクスポートが指定された日数だけ経過すると、システムによってエラーが生成されます。

例

次の例は、エクスポート通知オブジェクトを入力して有効にし、バックアップを実行する頻度を指定し、設定を表示する方法を示しています。

```
firepower # scope org
firepower /org # scope cfg-export-reminder
firepower /org/cfg-export-reminder # set adminstate enable
firepower /org/cfg-export-reminder* # set frequency 30
firepower /org/cfg-export-policy* # commit-buffer
firepower /org/cfg-export-reminder # show

Config Export Reminder:
    Config Export Reminder (Days): 30
    AdminState: Enable
firepower /org/cfg-export-reminder #
```

関連コマンド

コマンド	説明
scope cfg-export-policy	設定エクスポート ポリシーを入力します。
show	設定エクスポートの通知モードでは、現在の通知オブジェクトの設定が表示されます。

set cli

ターミナル ウィンドウの幅に合うようにコマンド出力行を折り返すまたは切り詰めるかどうか、テーブルヘッダーを表示するかどうか、コマンド出力テーブルのフィールドを区切るためにカンマまたはスペースを使用するかどうかを指定するには、**set cli** コマンドを使用します。

set cli {**suppress-field-spillover** {**off** | **on**} | **suppress-headers** {**off** | **on**} | **table-field-delimiter** {**comma** | **none** } }

構文の説明

suppress-field-spillover {**off** | **on**}	**off** を使用すると、ターミナル ウィンドウで出力行が折り返されます。 **on** を使用すると、ターミナル ウィンドウの端で出力行を切り詰められます。
suppress-headers {**off** | **on**}	**off** を使用すると、テーブル ヘッダーを表示します。 **on** を使用すると、テーブル ヘッダーを非表示にします。
table-field-delimiter {**comma** | **none**}	**comma** を使用すると、コマンド出力テーブルのフィールドがカンマで区切られます。 **none** を使用すると、コマンド出力テーブルのフィールドがスペースで区切られます。

コマンド デフォルト

ターミナル ウィンドウでコマンド出力の行を折り返します。

テーブル ヘッダーは表示されます。

コマンド出力テーブルのフィールドを区切るためにスペースを使用します。

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、ターミナル ウィンドウの幅に合うようにコマンド出力行を折り返すまたは切り詰めるかどうか、テーブルヘッダーを表示するかどうか、コマンド出力テーブルのフィールドを区切るためにカンマまたはスペースを使用するかどうかを指定できます。

例

次の例は、コマンド出力行が切り詰められるように指定してから、折り返すようにリセットする方法を示しています。

```
FP9300-A# set cli suppress-field-spillover on
FP9300-A# show fault
```

```
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Warning   F16520   2010-01-21T18:33:22.065   5785755 [FSM:STAGE:RETRY:]: detect
mezz cards in 1/6(FSM-STAGE:sam:dme:ComputeBladeDiscover:NicPresence)
Condition F77960   2010-01-21T18:32:31.255   1089623 [FSM:STAGE:REMOTE-ERROR]: R
esult: end-point-unavailable Code: unspecified Message: sendSamDmeAdapterInfo: i
dentify failed

FP9300-A# set cli suppress-field-spillover off
FP9300-A# show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Warning   F16520   2010-01-21T18:33:22.065   5785755 [FSM:STAGE:RETRY:]: detect
Condition F77960   2010-01-21T18:32:31.255   1089623 [FSM:STAGE:REMOTE-ERROR]: R

FP9300-A#
```

関連コマンド

コマンド	説明
show cli	現在の CLI 設定を表示します。
terminal	ターミナル ウィンドウに表示される行数および行の幅を設定します。

set clock

FXOS でクロックを手動で設定するには、 **set clock** コマンドを使用します。

set clock

構文の説明

set clock	FXOS でクロックを手動で設定するために **set clock** を使用します。

コマンド モード

scope system/scope services

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

例

次の例は、FXOS でクロックを設定する方法を示しています。

```
firepower# scope system
firepower /system# scope services
firepower /system/services # set clock aug 23 2021 12 00 00
firepower /system/services* # commit
firepower /system/services # show clock
Tue Aug 24 12:00:02 UTC 2021
```

set cluster-control-link network

Threat Defense および ASA のクラスタ ブートストラップ設定でクラスタ制御リンク IP ネットワークを設定するには、**set cluster-control-link network** コマンドを使用します。

set cluster-control-link network *a.b*.**0.0**

構文の説明

a.b.**0.0**	ループバック（127.0.0.0/8）およびマルチキャスト（224.0.0.0/4）のアドレスは除いて、任意の/16 ネットワーク アドレスを指定します。値を 0.0.0.0 に設定すると、デフォルトのネットワーク（127.2.0.0）が使用されます。

コマンド デフォルト

デフォルト ネットワークは 127.2.0.0 です。

コマンド モード

scope ssa/create logical-device/create cluster-bootstrap/

コマンド履歴

リリース	変更内容
2.4(1)	コマンドが追加されました。

使用上のガイドライン

シャーシは、シャーシ ID とスロット ID（*a.b.chassis_id.slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイスの IP アドレスを自動生成します。

ブートストラップの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、アプリケーション CLI の設定でほとんどの値を変更できます。

例

次に、モードをルーテッドに設定する例を示します。

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 clustered
Firepower /ssa/logical-device* # create cluster-bootstrap
firepower /ssa/logical-device/cluster-bootstrap* # set cluster-control-link network
10.10.0.0
firepower /ssa/logical-device/cluster-bootstrap* #
```

関連コマンド

コマンド	説明
create logical-device	論理デバイスを作成します。
create cluster-bootstrap	アプリケーションのクラスタ ブートストラップ設定を作成します。

set collection-interval

モニタ対象の統計情報を収集する頻度を定義するには、**set collection-interval** コマンドを使用します。

set collection-interval *interval*

構文の説明

interval	統計情報収集間隔を定義する時間の長さ。使用可能な値は次のとおりです。 • `1minute`：1 分間隔 • `2minutes`：2 分間隔 • `30seconds`：30 秒間隔 • `5minutes`：5 分間隔

コマンド モード

scope monitoring/scope stats-collection-policy/

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

set collection-interval コマンドを使用して、統計情報を収集する頻度を定義し、**set reporting-interval** コマンドを使用して、統計情報を報告する頻度を定義します。これらの間隔で統計情報収集ポリシーが定義されます。

報告インターバル中に複数の統計データ ポイントが収集できるように、報告インターバルは収集インターバルよりも長くなります。これにより、最小値、最大値、平均値を計算して報告するために十分なデータが提供されます。

統計情報は、Firepower システムの次の機能領域ごとに収集して報告することができます。特定の収集ポリシーにアクセスするには、**scope stats-collection-policy** コマンドを使用します。

- `Adapter`：アダプタに関連した統計情報。
- `Chassis`：ブレード シャーシに関連した統計情報。
- `Fex`：設定されたファブリック エクステンダに関連した統計情報。
- `Host`：このポリシーは今後サポートされる機能のプレースホルダです。
- `Port`：サーバ ポート、アップリンク イーサネット ポート、およびアップリンク ファイバ チャネル ポートを含むポートに関連した統計情報。
- `Server`：サーバに関連した統計情報。

（注） 機能エリアごとにデフォルト統計情報収集ポリシーが 1 つずつあります。追加で統計情報収集ポリシーを作成できません。また、既存のデフォルトポリシーを削除できません。デフォルト ポリシーを変更することだけが可能です。

例

次の例は、ポートの統計情報収集ポリシーを入力し、収集間隔を1分に設定し、レポート間隔を 30 分に設定し、トランザクションをコミットする方法を示しています。

```
firepower # scope monitoring
firepower /monitoring # scope stats-collection-policy port
firepower /monitoring/stats-collection-policy # set collection-interval 1minute
firepower /monitoring/stats-collection-policy* # set reporting-interval 30minute
firepower /monitoring/stats-collection-policy* # commit-buffer
firepower /monitoring/stats-collection-policy #
```

関連コマンド

コマンド	説明
scope stats-collection-policy	stats-collection-policy モードを開始します。ここでは、統計情報の収集と報告の間隔を管理できます。
set reporting-interval	統計情報の報告頻度を指定します。

set con-absolute-session-timeout

シリアル コンソールの絶対セッション タイムアウトを設定するには、**set con-absolute-session-timeout** コマンドを使用します。

set con-absolute-session-timeout *seconds*

構文の説明

seconds	シリアルコンソールの絶対セッションタイムアウト。値は0～3600秒で指定できます。このタイムアウトを無効にするには、値を0に設定します。

コマンド モード

デフォルト認証モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

シリアル コンソール セッションの絶対セッション タイムアウトを個別に設定できます。つまり、デバッグ用にシリアル コンソールの絶対セッション タイムアウトは無効にしながら、他の形式のアクセスの絶対タイムアウトは維持することができます。

例

次の例は、デフォルトの認証モードを開始し、シリアル コンソールの絶対タイムアウトを 4 分に設定する方法を示しています。

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set con-absolute-session-timeout 240
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

関連コマンド

コマンド	説明
set refresh-period	Web セッション更新期間を設定します。
show detail	現在のセッションおよび絶対セッション タイムアウト設定を表示します。

set con-session-timeout

シリアルコンソールのアイドルセッションタイムアウトを設定するには、**set con-session-timeout** コマンドを使用します。

set con-session-timeout *seconds*

構文の説明

seconds	シリアル コンソールのアイドル セッション タイムアウト。値は 0 ～ 3600 秒で指定できます。このタイムアウトを無効にするには、値を 0 に設定します。

コマンド モード

デフォルト認証モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、シリアル コンソール セッションのアイドル セッション タイムアウトを指定します。

例

次の例は、デフォルトの認証モードを開始し、シリアルコンソールのアイドルタイムアウトを 4 分に設定する方法を示しています。

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set con-session-timeout 240
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

関連コマンド

コマンド	説明
set refresh-period	Web セッション更新期間を設定します。
show detail	現在のセッションおよび絶対セッション タイムアウト設定を表示します。

set cpu-core-count

コンテナ インスタンスで使用するリソース プロファイルの CPU コア数を設定するには、**set cpu-core-count** コマンドを使用します。

set cpu-core-count *cores*

構文の説明

cores	シャーシに応じて、プロファイルのコア数を 6 ～最大数（偶数）で設定します。8 コアを指定することはできません。

コマンド モード

scope ssa/create resource-profile/

コマンド履歴

リリース	変更内容
2.4(1)	コマンドが追加されました。

使用上のガイドライン

コンテナインスタンスごとにリソース使用率を指定するには、1 つまたは複数のリソース プロファイルを作成します。論理デバイス/アプリケーション インスタンスを展開するときに、使用するリソース プロファイルを指定します。リソース プロファイルは CPU コアの数を設定します。RAM はコアの数に従って動的に割り当てられ、ディスク容量はインスタンスごとに 40 GB に設定されます。

- コアの最小数は 6 です。
- 内部アーキテクチャにより 8 コアを指定することはできません。
- コアを偶数（6、10、12、14 など）で最大値まで割り当てることができます。
- 利用可能な最大コア数は、セキュリティ モジュール / シャーシ モデルによって異なります。

シャーシには、「Default-Small」と呼ばれるデフォルト リソース プロファイルが含まれています。このコア数は最小です。このプロファイルの定義を変更したり、使用されていない場合には削除することもできます。シャーシをリロードし、システムに他のプロファイルが存在しない場合は、このプロファイルが作成されます。

使用中のリソースプロファイルの設定を変更することはできません。そのリソースプロファイルを使用しているすべてのインスタンスを無効にしてから、リソースプロファイルを変更し、最後にインスタンスを再度有効にする必要があります。確立されたハイ アベイラビリティ ペア内のインスタンスのサイズを変更する場合、できるだけ早くすべてのメンバを同じサイズにする必要があります。

Threat Defense インスタンスを Management Center に追加した後にリソース プロファイル設定を変更する場合は、**[Devices]** > **[Device Management]** > **[Device]** > **[System]** > **[Inventory]** ダイアログボックスで各ユニットのインベントリを更新します。

例

次の例では、3 つのリソース プロファイルを追加します。

```
firepower# scope ssa
firepower /ssa # enter resource-profile basic
firepower /ssa/resource-profile* # set description "lowest level"
firepower /ssa/resource-profile* # set cpu-core-count 6
firepower /ssa/resource-profile* # exit
firepower /ssa # enter resource-profile standard
firepower /ssa/resource-profile* # set description "middle level"
firepower /ssa/resource-profile* # set cpu-core-count 10
firepower /ssa/resource-profile* # exit
firepower /ssa # enter resource-profile advanced
firepower /ssa/resource-profile* # set description "highest level"
firepower /ssa/resource-profile* # set cpu-core-count 12
firepower /ssa/resource-profile* # commit-buffer
firepower /ssa/resource-profile #
```

関連コマンド

コマンド	説明
create resource-profile	コンテナ インスタンスで使用するリソース プロファイルを追加します。
set resource-profile-name	リソース プロファイルがアプリケーション インスタンスに割り当てられました。
show monitor detail	セキュリティ モジュール / エンジン スロットのリソース使用率を表示します。
show resource detail	アプリケーション インスタンスのリソース割り当てを表示します。
show resource-profile user-defined	リソース プロファイルの割り当てを表示します。

set deploy-type

ネイティブまたはコンテナのいずれかのアプリケーションインスタンスの展開タイプを設定するには、**set deploy-type** コマンドを使用します。

set deploy-type {**native** | **container**}

構文の説明

container	アプリケーション インスタンスをコンテナ タイプに設定します。
native	アプリケーションインスタンスをネイティブタイプに設定します。

コマンド デフォルト

デフォルトのタイプは native です。

コマンド モード

scope ssa/scope slot/create app-instance/

コマンド履歴

リリース	変更内容
2.4(1)	Threat Defense にコマンドが追加されました。

使用上のガイドライン

アプリケーション インスタンスは次の展開タイプで実行します。

- ネイティブ インスタンス：ネイティブ インスタンスはセキュリティモジュール/エンジンのすべてのリソース（CPU、RAM、およびディスク容量）を使用するため、ネイティブインスタンスを 1 つだけインストールできます。
- コンテナ インスタンス：コンテナ インスタンスでは、セキュリティモジュール/エンジンのリソースのサブセットを使用するため、複数のコンテナインスタンスをインストールできます。マルチインスタンス機能は、Threat Defense でのみサポートされています。ASA ではサポートされていません。

（注） マルチインスタンス機能は、実装は異なりますが、ASA マルチ コンテキスト モードに似ています。マルチ コンテキスト モードでは、単一のアプリケーションインスタンスがパーティション化されますが、マルチインスタンス機能では、独立したコンテナ インスタンスを使用できます。コンテナインスタンスでは、ハードリソースの分離、個別の構成管理、個別のリロード、個別のソフトウェアアップデート、および Threat Defense のフル機能のサポートが可能です。マルチ コンテキスト モードでは、共有リソースのおかげで、特定のプラットフォームでより多くのコンテキストをサポートできます。Threat Defense ではマルチコンテキストモードは使用できません。

Firepower 9300 の場合、一部のモジュールでネイティブ インスタンスを使用し、他のモジュールではコンテナ インスタンスを使用することができます。

例

次の例は、Threat Defense のアプリケーション インスタンスを追加し、コンテナ タイプに設定する方法を示しています。

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

関連コマンド

コマンド	説明
show app-attri	現在のアプリケーション属性を表示します。
create resource-profile	コンテナ インスタンスで使用するリソース プロファイルを作成します。
show resource-profile-name	利用可能なリソース プロファイルを表示します。

set descr

ポートチャネルに説明を設定するには、**set descr** コマンドを使用します。

set descr *description*

構文の説明

description	（任意）説明。256 文字以下で入力します。

コマンド モード

scope eth-uplink/scope fabric a/port-channel/

コマンド履歴

リリース	変更内容
2.0.1	コマンドが追加されました。

使用上のガイドライン

説明にスペース、特殊文字、または句読点が含まれている場合、説明の前後に引用符を付ける必要があります。引用符は、show コマンド出力イーサネットの説明フィールドには表示されません。

例

次に、説明を設定する例を示します。

```
firepower-9300 # scope eth-uplink
firepower-9300 /eth-uplink # scope fabric a
firepower-9300 /eth-uplink/fabric # create port-channel id
firepower-9300 /eth-uplink/fabric/port-channel* # enable
firepower-9300 /eth-uplink/fabric/port-channel* # set descr "link"
firepower-9300 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

関連コマンド

コマンド	説明
show interface	duplex パラメータを含むインターフェイスの情報を表示します。

set duplex

ポートチャネルのすべてのメンバーのデュプレックスを設定するには、**set duplex** コマンドを使用します。

set duplex {**fullduplex** | **halfduplex**}

構文の説明

fullduplex	（任意）デュプレックス モードを全二重に指定します。
halfduplex	（任意）デュプレックス モードを半二重に指定します。

コマンド モード

scope eth-uplink/scope fabric a/port-channel/

コマンド履歴

リリース	変更内容
2.0.1	コマンドが追加されました。

使用上のガイドライン

デュプレックス モードを設定する前に速度を設定する必要があります。速度を 10 または 100 Mbps に指定すると、ポートでは半二重モードを使用するように自動的に設定されますが、全二重モードを指定することもできます。ギガビット イーサネットには全二重だけ指定できます。ギガビットイーサネットまたはギガビットイーサネットに設定されている 10/100/1000-Mbps ポートのデュプレックス モードは変更できません。

例

次の例は、インターフェイスのデュプレックス モードを設定する方法を示しています。

```
firepower-9300# scope eth-uplink
firepower-9300 /eth-uplink # scope fabric a
firepower-9300 /eth-uplink/fabric # create port-channel id
firepower-9300 /eth-uplink/fabric/port-channel* # enable
firepower-9300 /eth-uplink/fabric/port-channel* # set duplex halfduplex
firepower-9300 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

関連コマンド

コマンド	説明
show interface	duplex パラメータを含むインターフェイスの情報を表示します。

set email

ユーザ アカウントの連絡先電子メール アドレスを設定するには、**set email** コマンドを使用します。

set email *email_address*

構文の説明

email_address	ユーザ アカウント用の電子メール アドレス。電子メール アドレスを *user_name@domain_name* という形式で指定します。

コマンド モード

Callhome（/monitoring/callhome）モード：Call Home メッセージに含めるプライマリ連絡先の電子メール アドレスを指定します。

ローカル ユーザ（/security/local-user）モード：現在のローカル ユーザの連絡先電子メール アドレスを指定します。

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

電子メール アドレスに #（ハッシュ記号）、スペース、&（アンパサンド）などの特殊文字が含まれていると、電子メール サーバが電子メール メッセージをそのアドレスに配信できないことがあります。RFC2821 および RFC2822 に準拠し、7 ビット ASCII 文字のみを含む電子メール アドレスを使用することをお勧めします。

Callhome モードでは、電子メール アドレスに最大 2083 文字を使用できます。

ローカル ユーザ モードでは、電子メール アドレスに最大 510 文字を使用できます。

例

次の例は、現在のローカルユーザの電子メールアドレスを指定する方法を示しています。

```
FP9300-A /security/local-user # set email admin@example.com
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

関連コマンド

コマンド	説明
create local-user	新規のローカル ユーザ アカウントを作成します。
set phone-contact	Smart Call Home アカウントの電話連絡先番号を指定します。

set enforce-strong-password

強力なパスワードの適用を有効または無効するには、**set enforce-strong-password** コマンドを使用します。

set enforce-strong-password {**no** | **yes**}

構文の説明

no	強力なパスワードの適用を無効にします。
yes	強力なパスワードの適用を有効にします。

コマンド モード

セキュリティ モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

ローカル認証された各ユーザ アカウントにパスワードが必要です。admin 権限または AAA 権限を持つユーザは、すべてのユーザ パスワードのパスワード強度チェックを実行するようにシステムを設定できます。パスワード強度チェックが有効になると、各ユーザが強力なパスワードを使用する必要があります。

各ユーザが強力なパスワードを設定することを推奨します。ローカル認証ユーザのパスワード強度チェックを有効にすると、FXOS は次の要件を満たしていないパスワードを拒否します。

- 8 ～ 80 文字の長さであること。（set min-password-length （65 ページ） コマンドを使用すると、必要な最小文字数を指定できます。）
- アルファベットの大文字を少なくとも 1 文字含む。
- アルファベットの小文字を少なくとも 1 文字含む。
- 英数字以外の文字（特殊文字）を少なくとも 1 文字含む。
- aaabbb など連続して 3 回を超えて繰り返す文字を含まない。
- passwordABC や password321 などの 3 つの連続した数字や文字をどのような順序であっても含まない。
- ユーザ名またはユーザ名を逆にしたものではない。
- パスワード ディクショナリ チェックに合格する。たとえば、辞書に記載されている標準的な単語に基づくパスワードを指定することはできません。
- 次の記号を含まない。$（ドル記号）、?（疑問符）、=（等号）。
- ローカル ユーザ アカウントおよび admin アカウントの場合は空白にしない。

例

次の例は、セキュリティ モードを開始し、強力なパスワードの適用を有効にする方法を示しています。

```
FP9300-A# scope security
FP9300-A /security # set enforce-strong-password yes
FP9300-A /security* # commit-buffer
FP9300-A /security #
```

関連コマンド

コマンド	説明
set min-password-length	パスワードの最小の長さを指定します。

set expiration

ローカルユーザアカウントの有効期限を設定するには、**set expiration** コマンドを使用します。

set expiration {{**apr** | **aug** | **dec** | **feb** | **jan** | **jul** | **jun** | **mar** | **may** | **nov** | **oct** | **sep**} *day* *year*}

構文の説明

{**apr** | **aug** | **dec** | **feb** | **jan** | **jul** | **jun** | **mar** | **may** | **nov** | **oct** | **sep**}	3 文字の月名の略称。
day	月の日付（数字）。有効な値は 1 ～ 31 です。
year	有効期限の年（数字）。最大値は 2037 です。

コマンド モード

ローカル ユーザ モード：現在のローカル ユーザの有効期限を指定します。

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

ユーザ アカウントに有効期限を設定した後、「有効期限なし」に再設定することはできません。ただし、別の有効期限を使用してアカウントを再設定することはできます。

例

次の例は、セキュリティ モードを開始し、新しいローカル ユーザ アカウントを作成し、そのアカウントの有効期限を指定する方法を示しています。

```
FP9300-A# scope security
FP9300-A /security # create local-user test_user
FP9300-A /security/local-user* # set expiration dec 31 2019
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

関連コマンド

コマンド	説明
create local-user	新規のローカル ユーザ アカウントを作成します。
set password	ユーザ アカウントのパスワードを指定します。

set (export-config)

既存のエクスポート設定オブジェクトのパラメータを編集するには、export-configuration モードで **set** コマンドを使用します。

set {**descr** | **password** | **port** | **protocol** | **remote-file** | **user**}

構文の説明

descr *description*	（任意）設定オブジェクトに説明を追加できます。説明は 1 ～ 256 文字で指定できます。ダッシュやアンダースコアのようにほとんどの英数字を使用できます。文字列の末尾には、セミコロン、ピリオド（終止符）、および感嘆符などの句読点を使用できますが、説明にはこれらの文字を埋め込むことはできません。
password	（任意）リモート サーバへの接続に使用するパスワードを変更できます。パスワードを入力して確認するように求められます。
port {*number* | **default**}	（任意）リモート サーバとの通信が行われるポートを変更できます。オプションは、0 ～ 4294967295 のポート ID 番号です。現在のプロトコルのデフォルト ポートは **default** です。
protocol *name*	（任意）設定のバックアップをリモート サーバに送信するために使用されるファイル転送プロトコルを変更できます。使用可能なオプションは次のとおりです。 • **ftp** • **scp** • **sftp** • **tftp**
remote-file *name*	（任意）バックアップ コンフィギュレーション ファイルの名前を変更できます。1 ～ 128 文字で指定できます。
user *name*	（任意）リモート ホストへの接続に使用されるユーザ アカウント名を変更できます。0 ～ 510 文字で指定できます。

コマンド モード

scope system/scope export-config/

コマンド履歴

リリース	変更内容
1.1.3	コマンドが追加されました。

使用上のガイドライン

このオプションを使用して、既存のエクスポート設定オブジェクトのバックアップ オプションを変更します。

現在の論理デバイスとプラットフォーム設定のバックアップに**export-config** コマンドを発行する場合に、エクスポート設定オブジェクトが作成されます。**scope export-config** を使用すると、オブジェクトを入力し、そのパラメータを編集できます。

次の点に注意してください。

- FXOS 2.6.1 以降、設定のエクスポート中にパスワードやその他の秘密キーなどの機密情報を暗号化する際に使用するキーを指定する必要があります。設定をエクスポートする前に、パスワードやその他の秘密キーを指定しておく必要があります。

  また、ファイルが 2.6.1 より前の FXOS リリースからファイルがエクスポートされない限り、エクスポートされた設定をインポートする場合にターゲット システムで、エクスポート時に同じキーが使用されるように設定する必要もあります。この場合、ターゲット システムは暗号化キーをチェックせず、インポートできます。

- コンフィギュレーション ファイルの内容は、修正しないでください。コンフィギュレーション ファイルが変更されると、そのファイルを使用するコンフィギュレーション インポートが失敗する可能性があります。

- 既存のバックアップ ファイルが上書きされるのを回避するには、エクスポート操作時にファイル名を変更するか、既存のファイルを別の場所にコピーしてください。

例

次の例は、既存のエクスポート設定オブジェクトに説明を追加する方法を示しています。

```
firepower # scope system
firepower /system # scope export-config 192.168.1.2
firepower /system/export-config # set descr one-time_back-up_be_sure_to_change_file_name
firepower /system/export-config* # commit-buffer
firepower /system/export-config #
```

関連コマンド

コマンド	説明
cfg-export-policy	設定のエクスポート ポリシーを指定します。
export-config	現在のシステム設定をリモート サーバに XML ファイルとしてエクスポートします。エクスポート設定オブジェクトを作成します。
import-config	以前にエクスポートした XML コンフィギュレーション ファイルをこのアプライアンスにコピーします。
set password-encryption-key	設定のエクスポート中に機密情報を暗号化するときに使用されるキーを指定します。

set firstname

ローカル ユーザの名を指定するには、**set firstname** コマンドを使用します。

set firstname *name*

構文の説明

name	ユーザの名。0 ～ 32 文字で指定できます。

コマンド モード

ローカル ユーザ モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

例

次の例は、セキュリティ モードを開始し、新しいローカル ユーザ アカウントを作成し、そのユーザの名と姓を指定する方法を示しています。

```
FP9300-A# scope security
FP9300-A /security # create local-user test_user
FP9300-A /security/local-user* # set firstname john
FP9300-A /security/local-user* # set lastname doe
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

コマンド	説明
create local-user	新規のローカル ユーザ アカウントを作成します。
set lastname	ローカル ユーザ アカウントの姓を指定します。

set flow-control-policy

フロー制御ポリシーをインターフェイスまたはポートチャネルに割り当てるには、**set flow-control-policy** コマンドを使用します。

set flow-control-policy *name*

構文の説明

name	フロー制御ポリシーの名前。最大 16 文字です。

コマンド モード

scope eth-uplink/scope fabric a/scope interface/

scope eth-uplink/scope fabric a/scope port-channel/

コマンド履歴

リリース	変更内容
2.0.1	コマンドが追加されました。

使用上のガイドライン

新しいフロー制御ポリシーを作成すると、新しいポリシーがまだコミットされていないことを示すアスタリスクが付いた flow-control/policy モード（eth-uplink/flow-control/policy）が自動的に開始されます。ポリシープロパティ値を設定し、新しいポリシーをコミットすることができます。フロー制御ポリシーを作成した後は、ポリシー名を変更することはできません。ポリシーを削除し、新しいポリシーを作成する必要があります。

例

次の例は、フロー制御ポリシーをインターフェイスに割り当てる方法を示しています。

```
firepower-9300 # scope eth-uplink
firepower-9300 /eth-uplink # scope fabric
firepower-9300 /eth-uplink #/fabric # scope interface Ethernet1/8
firepower-9300 /eth-uplink/fabric/interface* # set flow-control-policy eth1-8flowcontrol
firepower-9300 /eth-uplink/fabric/interface* # commit-buffer
firepower-9300 /eth-uplink/fabric/interface #
```

関連コマンド

コマンド	説明
create policy (flow control)	新しいフロー制御ポリシーを作成します。
show interface	インターフェイス ステータスを表示します。速度パラメータもあわせて表示します。
show port-channel	ポート チャネル情報を表示します。

set (flow-control policy)

既存のフロー制御ポリシーのパラメータを指定または編集するには、フロー制御/ポリシーモードで **set** コマンドを使用します。

set {**prio** | **receive** | **send**}

構文の説明

prio {**auto** | **on**	フロー制御優先順位オプションを設定します。 • **auto**：このデバイスとネットワークが、このファブリックでポイントツーポイントプロトコル（PPP）が使用されているかどうかをネゴシエートします。 • **on**：このファブリックで PPP が有効になります。
receive off	ネットワークからのポーズ要求が無視され、トラフィックフローが通常どおり継続することを指定します。
send off | **on**	フロー制御送信パラメータを設定します。 • **off**：パケット負荷に関係なくトラフィックが通常どおり流れます。 • **on**：着信パケットバッファがいっぱいになると、このデバイスからポーズ要求がネットワークに送信されます。ポーズは、トラフィックが通常のレベルに戻っている間も、数ミリ秒間は有効のままになります。

コマンド モード

scope eth-uplink/scope flow-control/policy/

コマンド履歴

リリース	変更内容
1.1.1	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、フロー制御受信オプションを指定します。off を指定すると、ネットワークからのポーズ要求が無視されて、トラフィック フローが通常どおり継続します。on を指定すると、ポーズ要求に従って、ネットワークがポーズ要求を取り消すまですべてのトラフィックがそのアップリンク ポートで停止されます。

このコマンドを使用して、フロー制御送信オプションを指定します。**off** を指定すると、パケット負荷に関係なくポート上のトラフィックが通常どおり流れます。**on** に指定すると、着信パケット レートが非常に高くなる場合に、FXOS がポーズ要求をネットワークに送信します。ポーズは数ミリ秒有効になった後、通常のレベルにリセットされます。

例

次の例は、フロー制御の名前付きポリシーを作成し、開始してから、ポリシーパラメータを設定する方法を示しています。

```
firepower # scope eth-uplink
firepower /eth-uplink # scope flow-control
firepower /eth-uplink/flow-control # enter policy FCpolicy1
firepower /eth-uplink/flow-control/policy* # set prio auto
firepower /eth-uplink/flow-control/policy* # set send on
firepower /eth-uplink/flow-control/policy* # commit-buffer
firepower /eth-uplink/flow-control/policy #
```

関連コマンド

コマンド	説明
show policy	フロー制御/ポリシーモードでは、現在のフロー制御ポリシーのプロパティ値が表示されます。 フロー制御モードでは、現在定義されているすべてのフロー制御ポリシーのプロパティ値が表示されます。

set frequency

設定のエクスポートが特定の日数実行されない場合にエラーを生成するには、**set frequency** コマンドを使用します。

set frequency *days*

構文の説明

days	エクスポート通知の設定 (日数)。

コマンド モード

scope org/scope cfg-export-reminder/

コマンド履歴

リリース	変更内容
2.0.1	コマンドが追加されました。

例

次の例は、エクスポート通知の設定頻度の日数を設定する方法を示しています。

```
firepower-9300* # scope org
firepower-9300 /org* # scope cfg-export-reminder
firepower-9300 /org/scope cfg-export-reminder* # set frequency 2
firepower-9300 /org/scope cfg-export-reminder* # commit-buffer
firepower-9300 /org/scope cfg-export-reminder* # show detail
Config Export Reminder:
Config Export Reminder (Days): 10
AdminState: Enable
```

関連コマンド

コマンド	説明
set adminstate	エクスポート通知の管理状態を指定します。

set http-proxy-server-enable

スマート ソフトウェア ライセンスおよび Smart Call Home の HTTP/HTTPS プロキシを有効または無効にするには、**set http-proxy-server-enable** コマンドを使用します。

set http-proxy-server-enable {**off** | **on**}

構文の説明

off	Smart Call Home の HTTP/HTTPS プロキシを無効にします。
on	Smart Call Home の HTTP/HTTPS プロキシを有効にします。

コマンド デフォルト

HTTP/HTTPS プロキシはデフォルトで無効になっています。

コマンド モード

Callhome モード

使用上のガイドライン

ネットワークでインターネット アクセスに HTTP プロキシを使用する場合、スマート ソフトウェア ライセンスのプロキシを有効にしてアドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

例

次の例は、HTTP プロキシを有効にする方法を示しています。

```
FP9300-A# scope monitoring
FP9300-A /monitoring # scope callhome
FP9300-A /monitoring/callhome # set http-proxy-server-enable on
FP9300-A /monitoring/callhome #
```

関連コマンド

コマンド	説明
set http-proxy-server-url	プロキシ サーバの HTTP または HTTPS アドレスを設定します。
set http-proxy-server-port	プロキシ サーバの通信ポートを設定します。

set http-proxy-server-port

スマート ソフトウェア ライセンスおよび Smart Call Home の HTTP/HTTPS プロキシ サーバ ポートを設定するには、**set http-proxy-server-port** コマンドを使用します。

set http-proxy-server-port *port_number*

構文の説明

port_number	HTTP または HTTPS プロキシ サーバのポート。範囲は 1 ～ 65535 です。

コマンド デフォルト

HTTP/HTTPS プロキシはデフォルトで無効になっています。サーバ アドレスとポート番号を入力する前にプロキシを有効にする必要があります。

コマンド モード

Callhome モード

使用上のガイドライン

ネットワークでインターネット アクセスに HTTP プロキシを使用する場合、スマート ソフトウェア ライセンスのプロキシを有効にしてアドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

例

次の例は、HTTP/HTTPS プロキシ サーバのポート番号を入力する方法を示しています。

```
FP9300-A# scope monitoring
FP9300-A /monitoring # scope callhome
FP9300-A /monitoring/callhome # set http-proxy-server-port 443
FP9300-A /monitoring/callhome #
```

関連コマンド

コマンド	説明
set http-proxy-server-enable	スマート ソフトウェア ライセンスおよび Smart Call Home の HTTP/HTTPS プロキシを有効または無効にします。
set http-proxy-server-url	プロキシ サーバの HTTP/HTTPS アドレスを設定します。

set http-proxy-server-url

スマート ソフトウェア ライセンスおよび Smart Call Home の HTTP/HTTPS プロキシ サーバ アドレスを設定するには、**set http-proxy-server-url** コマンドを使用します。

set http-proxy-server-url *url*

構文の説明

url	プロキシ サーバの HTTP または HTTPS アドレス。最大 2083 文字を指定できます。

コマンド デフォルト

HTTP/HTTPS プロキシはデフォルトで無効になっています。サーバ アドレスを入力する前にプロキシを有効にする必要があります。

コマンド モード

Callhome モード

使用上のガイドライン

ネットワークでインターネット アクセスに HTTP プロキシを使用する場合、スマート ソフトウェア ライセンスのプロキシを有効にしてアドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

例

次の例は、HTTPS プロキシ サーバ アドレスを入力する方法を示しています。

```
FP9300-A# scope monitoring
FP9300-A /monitoring # scope callhome
FP9300-A /monitoring/callhome # set http-proxy-server-url https://209.165.201.10
FP9300-A /monitoring/callhome #
```

関連コマンド

コマンド	説明
set http-proxy-server-enable	スマート ソフトウェア ライセンスおよび Smart Call Home の HTTP/HTTPS プロキシを有効または無効にします。
set http-proxy-server-port	プロキシ サーバの通信ポートを設定します。

set https

HTTPS サービス パラメータを指定するには、**set https** コマンドを使用します。

set https {**auth-type** {**cert-auth** | **cred-auth**} | **cipher-suite** *cipher_string* | **cipher-suite-mode** {**custom** | **high-strength** | **low-strength** | **medium-strength**} | **crl-mode** {**relaxed** | **strict**} | **keyring** *keyring_name* | **port** *port_number*}

構文の説明

auth-type {**cert-auth** | **cred-auth**}	（任意）HTTPS アクセスで使用する認証タイプを指定します。 • **cert-auth**：HTTPS アクセスのユーザを認証するために、クライアント証明書と LDAP を一緒に使用するようにシステムを設定します。 • **cred-auth**：HTTPS アクセスにクレデンシャルベースのユーザ認証を使用するようにシステムを設定します。
cipher-suite *cipher_string*	（任意）カスタム **cipher-suite-mode** で使用する暗号スイートの定義文字列を指定します。 仕様の文字列は最大 256 文字まで使用できますが、OpenSSL 暗号スイート仕様に準拠する必要があります。次の場合を除き、スペースや特殊文字は使用できません。！（感嘆符）、+（プラス記号）、-（ハイフン）、および :（コロン）。詳細については、http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuiteを参照してください。 （注） **cipher-suite-mode** が **custom** に設定されている場合を除いて、この文字列は無視されます。

cipher-suite-mode {**custom** | **high-strength** | **low-strength**	（任意）使用する暗号スイート セキュリティのレベルを設定します。 • **custom**：**cipher-suite** オプションを使用して、カスタム暗号スイートのセキュリティ仕様の文字列を定義できます。 • **high-strength**：ALL:!EDH-RSA-DES-CBC3-SHA: !EDH-DSS-DES-CBC3-SHA: !DES-CBC3-SHA:!ADH:!3DES: !EXPORT40:!EXPORT56:!LOW:!MEDIUM:!eNULL:!RC4:!MD5: !IDEA:+HIGH:+EXP • **low-strength**：ALL:!EDH-RSA-DES-CBC3-SHA: !EDH-DSS-DES-CBC3-SHA: !DES-CBC3-SHA:!ADH:!3DES: !EXPORT40:!EXPORT56:RC4+RSA: !IDEA:+HIGH:+MEDIUM:+LOW:+EXP:+eNULL • **medium-strength**：ALL:!EDH-RSA-DES-CBC3-SHA: !EDH-DSS-DES-CBC3-SHA: !DES-CBC3-SHA:!ADH:!3DES:!EXPORT40:!EXPORT56: !LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM:+EXP:+eNULL 通常、暗号強度はセキュリティのビット（または対称キーサイズ）に基づいていることがほとんどで、「low」は 128 ビット未満のセキュリティ、「medium」は 128 ビット、「high」は 128 ビットを超えるセキュリティを示しています。
crl-mode {**relaxed** | **strict**}	（任意）HTTPS接続の証明書失効リスト（CRL）チェックのレベルを定義します。 • **relaxed**：証明書が CRL にリストされていても、証明書のリスト理由に応じて HTTPS 認証の許可に使用される場合があります。発生するたびに警告メッセージが記録されます。基本的には、CRL チェックを無効にします。 • **strict**：CRL の証明書の接続認証は失敗します。発生するたびに警告メッセージが記録されます。また、CRLは最新の状態に維持する必要があります。
keyring *keyring_name*	（任意）HTTPS 接続に使用する RSA キーリングの名前を指定します。
port *port_number*	（任意）HTTPS接続に使用するポートを指定します。1 ～ 65535 で指定できます。デフォルトは 443 です。

コマンド デフォルト

Firepower 4100/9300 シャーシ上でのデフォルトの HTTPS 認証設定はクレデンシャルベースです。

デフォルトの暗号スイートのセキュリティ レベルは中程度の強度です。

コマンド モード

サービス モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

証明書認証が有効である場合、これは HTTPS に許可されている唯一の認証形式です。

この機能を使用するには、クライアント証明書が次の要件を満たしている必要があります。

- ユーザ名が X509 属性 [Subject Alternative Name - Email] に含まれている必要があります。
- クライアント証明書は、その証明書をスーパーバイザ上のトラストポイントにインポートしているルート CA により署名されている必要があります。

注意 これらの設定パラメータの大部分（特に keyring、port、cipher-suite、custom cipher-suite-mode）をコミットすると、現在のすべての HTTP および HTTPS セッションがユーザ警告なしで終了します。

例

次の例は、HTTPSアクセスの証明書ベースの認証を有効にする方法を示しています。

```
FP9300-A# scope system
FP9300-A /system # scope services
FP9300-A /system/services # set https auth-type cert-auth
FP9300-A /system/services* # commit-buffer
FP9300-A /system/services #
```

関連コマンド

コマンド	説明
enable https	HTTPS サービスを有効にします。
show https	現在の HTTPS サービス設定を表示します。

set (interface)

インターフェイスのパラメータを指定または変更するには、インターフェイス モードで **set** コマンドを使用します。

set
{**admin-duplex** | **admin-speed** | **auto-negotiation** | **descr** | **eth-link-profile** | **flow-control-policy** | **nw-ctrl-policy** | **port-type** | **user-label**}

構文の説明

admin-duplex {**fullduplex** | **halfduplex**}	インターフェイスのデュプレックス モードを定義します。 • **fullduplex** ：双方向の同時通信を指定します。 • **halfduplex** ：一方向通信を指定します。
admin-speed {**100gbps** | **100mbps** | **10gbps** | **10mbps** | **1gbps** | **40gbps**}	インターフェイスのデータ転送速度を指定します。 • **100gbps** ：100 ギガビット/秒。 • **100mbps** ：100 メガビット/秒。 • **10gbps** ：10 ギガビット/秒。 • **10mbps** ：10 メガビット/秒。 • **1gbps** ：1 ギガビット/秒。 • **40gbps** ：40 ギガビット/秒。
auto-negotiation {**no** | **yes**}	速度、デュプレックス、フロー制御など、一般的な伝送パラメータの自動ネゴシエーションを有効または無効にします。 • **no** ：自動ネゴシエーションを無効にします。 • **yes** ：自動ネゴシエーションを有効にします。
descr *description*	インターフェイスに説明を追加できます。説明は 0 ～ 256 文字で指定できます。ダッシュやアンダースコアのようにほとんどの英数字を使用できます。スペースは使用できません。文字列の末尾には、セミコロン、ピリオド（終止符）、および感嘆符などの句読点を使用できますが、説明にはこれらの文字を埋め込むことはできません。
eth-link-profile *name*	インターフェイスにイーサネット リンク プロファイルを割り当てると、プロファイルパラメータに従ってインターフェイスを自動的に設定できます。プロファイルの名前を指定します。名前には最大 16 文字の英数字を使用できます。

flow-control-policy *name*	フロー制御ポリシーをインターフェイスに割り当てることができます。ポリシー名を指定します。最大 16 文字の英数字を使用できます。
nw-ctrl-policy *name*	ネットワーク制御ポリシーをインターフェイスに割り当てることができます。ポリシー名を指定します。最大 16 文字の英数字を使用できます。
port-type {**cluster** | **data** | **data-sharing** | **firepower-eventing** | **mgmt**}	インターフェイスのタイプまたは機能を指定します。 • **cluster**：このインターフェイスをクラスタ制御リンクとして使用する場合のみ、**cluster** を指定します。 • **data**：通常のデータ伝送に使用します。これがデフォルトのタイプです。 • **data-sharing**：通常のデータに使用します。コンテナインスタンスでのみサポートされます。 • **firepower-eventing**：このインターフェイスは、Threat Defense デバイスのセカンダリ管理インターフェイスとして使用します。firepower-eventing インターフェイスを使用すると、firepower-eventing インターフェイスは、すべてのイベントのトラフィック（Web イベントなど）を運べます。 • **mgmt**：アプリケーションインスタンスの管理に使用します。各論理デバイスには、管理インターフェイスを 1 つだけ割り当てることができます。 このコマンドの詳細については、set port-type （82 ページ）を参照してください。
user-label *label*	このインターフェイスには説明ラベルを適用できます。0 ～ 16 文字の英数字を使用できます。

コマンド モード

scope eth-uplink/scope fabric a/interface/

コマンド履歴

リリース	変更内容
2.4(1)	**data-sharing** タイプが追加されました。
1.1(4)	**firepower-eventing** タイプが追加されました。
1.1(1)	コマンドが追加されました。

使用上のガイドライン

タイプ `cluster` はクラスタ化された論理デバイスに使用する特別なインターフェイスです。このタイプは、ユニット間のクラスタ通信用にクラスタ制御リンクに自動的に割り当てられます。デフォルトでは、クラスタ制御リンクは 48 番のポートチャネル上に自動的に作成されます。

データ インターフェイスは論理デバイス間で共有できません。

タイプ data-sharing はコンテナ インスタンスでのみサポートされ、これらのデータ インターフェイスは 1 つまたは複数の論理デバイス/コンテナ インスタンス（Threat Defense のみ）で共有できます。各コンテナインスタンスは、このインターフェイスを共有する他のすべてのインスタンスと、バック プレーン経由で通信できます。共有インターフェイスは、展開可能なコンテナインスタンスの数に影響することがあります。共有インターフェイスは、ブリッジグループ メンバインターフェイス（トランスペアレント モードまたはルーテッド モード）、インライン セット、パッシブ インターフェイス、またはフェールオーバー リンクではサポートされません。

firepower-eventing インターフェイスは Threat Defense デバイスのセカンダリ管理インターフェイスです。このインターフェイスを使用するには、Threat Defense CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Web イベントなど）から管理トラフィックを分類できます。『Management Center configuration guide』の「*System Configuration*」の章にある「Management Interfaces」のセクションを参照してください。Firepower イベント インターフェイスは、外部ホストにアクセスするために 1 つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介してインターフェイスを共有する他の倫理デバイスと通信することはできません。

mgmt インターフェイスを使用してアプリケーション インスタンスを管理します。外部ホストにアクセスするために 1 つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介して、インターフェイスを共有する他の倫理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを 1 つだけ割り当てることができます。

指定するインターフェイス速度はインターフェイスで使用するデュプレックス モードに影響を与えます。このため、デュプレックス モードを設定する前に速度を設定する必要があります。速度を 10 または 100 Mbps に指定すると、ポートでは半二重モードを使用するように自動的に設定されますが、全二重モードを指定することもできます。1000 Mbps（1 Gbps）以上の速度に設定すると、自動的に全二重モードが使用されます。

デフォルトのフロー制御ポリシーを編集した場合は、インターフェイスにすでに適用されています。新しいポリシーを作成した場合は、そのポリシーをインターフェイスに適用できます。

例

次の例は、インターフェイス速度を 10 Gbps に設定し、ポート タイプをデータに設定する方法を示しています。

```
firepower # scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # enter interface Ethernet1/8
firepower /eth-uplink/fabric/interface # enable
firepower /eth-uplink/fabric/interface* # set admin-speed 10gbps
firepower /eth-uplink/fabric/interface* # set port-type data
firepower /eth-uplink/fabric/interface* # commit-buffer
firepower /eth-uplink/fabric/interface
```

関連コマンド

コマンド	説明
enter interface	インターフェイス設定を指定および管理できるようにインターフェイスを入力します。
scope interface	インターフェイス設定を指定および管理できるようにインターフェイスを有効にします。
show interface	インターフェイスの設定とステータスに関する情報を表示します。

set keyring-name

IPSec 接続にキーリングを割り当てるには、**set keyring-name** コマンドを使用します。

set keyring-name *name*

構文の説明

name	IPSec 接続に割り当てるキーリングの名前。最大 16 文字。

コマンド モード

接続（/security/ipsec/connection）モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、IPSec 接続にキーリングを追加します。

例

次の例は、現在の IPSec 接続にキーリングを追加する方法を示しています。

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set keyring-name kr22
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

コマンド	説明
create connection	新しい IPSec 接続を作成します。
set keyring-passwd	IPSec 接続に割り当てられるキーリングのパスフレーズを指定します。

set lastname

ローカル ユーザの姓を指定するには、**set lastname** コマンドを使用します。

set lastname *name*

構文の説明

name	ユーザの姓。0 ～ 32 文字で指定できます。

コマンド モード

ローカル ユーザ モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

例

次の例は、セキュリティ モードを開始し、新しいローカル ユーザ アカウントを作成し、そのユーザの名と姓を指定する方法を示しています。

```
FP9300-A# scope security
FP9300-A /security # create local-user test_user
FP9300-A /security/local-user* # set firstname john
FP9300-A /security/local-user* # set lastname doe
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

コマンド	説明
create local-user	新規のローカル ユーザ アカウントを作成します。
set firstname	ローカル ユーザ アカウントの名を指定します。

set link-state-sync

サービス状態を使用して動作リンク状態をデータインターフェイスの物理リンク状態と同期させるには、 **set link-state-sync** コマンドを使用します。

set link-state-sync

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

scope ssa

コマンド履歴

リリース	変更内容
2.9(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、FTD動作リンク状態をデータインターフェイスの物理リンク状態と同期させることができます。

例

次の例は、scope ssa モードを開始し、link-state-sync を設定する方法を示しています。

```
firepower# scope ssa
firepower /ssa # scope logical-device <logical device identifier>
firepower /ssa/logical-device # set link-state-sync ?
  disabled  Disabled
  enabled   Enabled
```

set local-address

IPSec 接続のローカル IP アドレスを指定するには、**set local-address** コマンドを使用します。

set local-address *ip_address*

構文の説明

ip_address	IPSec 接続の IPv4 または IPv6 ローカル ゲートウェイ アドレスを入力します。最大 510 文字。

コマンド モード

Connection mode

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドと **set remote-address** コマンドを使用して、IPSec 接続のエンドポイントを定義します。

例

次の例は、IPSec 接続のローカル アドレスを設定する方法を示しています。

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set local-address 209.165.201.12
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

コマンド	説明
create connection	新しい IPSec 接続を作成します。
set remote-addr	IPSec 接続のリモート IP アドレスを設定します。

set log-level

IPSec ロギング レベルを指定するには、**set log-level** コマンドを使用します。

set log-level *log_level*

構文の説明

log_level	0 ～ 4 の値を入力して、IPSec ログの詳細を指定します。デフォルトは 1 です。 **0**：SA アップ/ダウンなどの基本的な監査情報。 **1**：：エラーのある一般的な制御フロー情報。 **2**：デバッグ情報などの詳細な制御フロー情報。 **3**：raw データ ダンプ（16 進数）が含まれます。 **4**：SA キーなど、データ ダンプに機密情報が含まれます。

コマンド モード

IPsec モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

show ipsec-log コマンドを使用してログを表示します。

例

次の例は、IPSec ロギング レベルを 2 に設定する方法を示しています。

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # set log-level 2
FP9300-A /security/ipsec* # commit-buffer
FP9300-A /security/ipsec #
```

関連コマンド

コマンド	説明
show ipsec-log	IPSec ログ ファイルを表示します。

set max-login-attempts

ログイン試行の失敗が許可される最大回数を指定するには、**set max-login-attempts** コマンドを使用します。

set max-login-attempts *max_attempts*

構文の説明

max_attempts	ユーザがシステムからロックアウトされるまでにログイン試行を失敗できる回数。指定できる値は0～10です。デフォルトは0です。

コマンド モード

セキュリティ モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

ユーザ（管理者ユーザを含む）がこのログイン試行最高回数を超えると、ユーザはシステムからロックアウトされるため、ログインが再び許可されるまで、指定された時間待機する必要があります。ユーザがロックアウトされたことを示す通知は表示されません。

例

次の例は、セキュリティ モードを開始し、ログインの最大試行回数を指定する方法を示しています。

```
FP9300-A# scope security
FP9300-A /security # set max-login-attempts 4
FP9300-A /security* # commit-buffer
FP9300-A /security #
```

関連コマンド

コマンド	説明
clear lock-status	ユーザのロックアウト ステータスをクリアします。
set user-account-unlock-time	ログイン試行の最高回数に達した後、ユーザがシステムからロックアウトされる時間を指定します。

set message

ログイン前バナーとして表示されるテキストの行を追加または置き換えるには、**set message** コマンドを使用します。

set message

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

scope security/scope banner/scope pre-login-banner/

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

コマンドを入力すると、バナー テキストの行数を入力するように求められます。バナー テキストを終了するには、ENDOFBUF（すべて大文字）と入力する必要があります。

（注） ログイン前バナー オブジェクトがすでに存在している必要があります。create pre-login-bannerを参照してください。

例

次の例は、ログイン前バナーを作成および指定し、コミットおよび表示する方法を示します。

```
firepower # scope security
firepower /security # scope banner
firepower /security/banner # create pre-login-banner
firepower /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Firepower-9300-2
>Western Data Center
>ENDOFBUF
firepower /security/banner/pre-login-banner* # commit
firepower /security/banner/pre-login-banner # show

Pre login banner:
    Message
    -------
    Firepower-9300-2
Western Data Center

firepower /security/banner/pre-login-banner #
```

関連コマンド

コマンド	説明
clear message	既存のログイン前バナーからテキストを削除します。実際のバナーオブジェクト自体は削除されません。
create pre-login-banner	ログイン画面の前に表示されるバナーを作成します。初期のバナーオブジェクトは空です。

set min-password-length

ユーザ パスワードの最小長を指定するには、**set min-password-length** コマンドを使用します。

set min-password-length *num_chars*

構文の説明

num_chars	ユーザ パスワードに必要な最小文字数。値の範囲は 8 ～ 80 です。

コマンド モード

セキュリティ モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

有効にした場合、ユーザは指定された最小文字数以上のパスワードを作成する必要があります。たとえば、*num_chars* が 15 に設定されている場合、パスワードの長さは 15 文字以上で指定する必要があります。

例

次の例は、セキュリティ モードを開始し、パスワードの最小長を 15 文字に指定する方法を示しています。

```
FP9300-A# scope security
FP9300-A /security # set min-password-length 15
FP9300-A /security* # commit-buffer
FP9300-A /security #
```

関連コマンド

コマンド	説明
set enforce-strong-password	強力なパスワードの適用を有効または無効にします。

set mode

IPSec 接続モードを指定するには、**set mode** コマンドを使用します。

set mode {**transport** | **tunnel**}

構文の説明

transport	接続モードを **transport** に設定します。
tunnel	接続モードを **tunnel** に設定します。

コマンド モード

Connection mode

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

トランスポート モードでは、IP パケットのペイロードのみが暗号化されます。トンネル モードでは、パケット全体が暗号化されます。通常、トランスポート モードはエンドツーエンド セッションに使用され、トンネルモードは他のすべての接続タイプ（ゲートウェイ間など）に使用されます。

例

次の例は、IPSec 接続モードをトンネルに設定する方法を示しています。

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set mode tunnel
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

コマンド	説明
create connection	新しい IPSec 接続を作成します。
set local-addr	IPSec 接続のローカル IP アドレスを設定します。
set remote-addr	IPSec 接続のリモート IP アドレスを設定します。

set modulus

RSA キー係数（SSL キーの長さ）をビット単位で指定するには、**set modulus** コマンドを使用します。

set modulus {**mod1536** | **mod2048** | **mod2560** | **mod3072** | **mod3584** | **mod4096**}

構文の説明

ビット単位の RSA キー係数（SSL キー長）	有効なオプションは次のとおりです。 • **mod1536**：係数は 1536 ビットです • **mod2048**：係数は 2048 ビットです • **mod2560**：係数は 2560 ビットです • **mod3072**：係数は 3072 ビットです • **mod3584**：係数は 3584 ビットです • **mod4096**：係数は 4096 ビットです

コマンド モード

キーリング モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、キーリングのキーの長さを指定します。

例

次の例は、キーリングのキーの長さとして 2048 ビットを指定する方法を示します。

```
FP9300-A# scope security
FP9300-A /security # scope keyring test-ring
FP9300-A /security/keyring # set modulus 2048
FP9300-A /security/keyring* # commit-buffer
switch-A /security/keyring #
```

関連コマンド

コマンド	説明
set cert	キー リングの RSA 証明書を入力します。
set regenerate	デフォルト キー リングで RSA キーを再生成します。
set trustpoint	キーリング証明書を再生成できるかどうかを指定します。

set out-of-band

デバイスの管理 IP アドレスを変更するには、**set out-of-band** コマンドを使用します。

IPv4 アドレスの場合：

set out-of-band {**gw** *gateway_address* | **ip** *ip_address* | **netmask** *network_mask*}

IPv6 アドレスの場合：

set out-of-band {**ipv6** *ipv6_address* | **ipv6-gw** *ipv6_gateway* | **ipv6-prefix** *ipv6_prefix*}

構文の説明

gw *gateway_address*	IPv4 ゲートウェイ アドレスを入力します。
ip *ip_address*	デバイス管理アクセスの IPv4 アドレスを指定します。
netmask *network_mask*	IPv4 アドレスのネットマスクを指定します。
ipv6 *ipv6_address*	デバイス管理アクセスの IPv6 アドレスを指定します。
ipv6-gw *ipv6_gateway*	IPv6 ゲートウェイ アドレスを入力します。
prefix *ipv6_prefix*	IPv6 アドレスのプレフィックス長を入力します。 （注） シャーシの IPv6 管理アドレスとしてサポートされるのは、IPv6 グローバル ユニキャスト アドレスのみです。

コマンド モード

IPv4 アドレス：ファブリック インターコネクト モード

IPv6 アドレス：IPv6 設定（fabric-interconnect/ipv6-config）モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

管理 IP アドレスを変更した後、新しいアドレスを使用して既存の接続を再確立する必要があります。

あるコマンド ラインで IP アドレス タイプに 3 つのキーワードと変数を任意の順序で入力できます。次の例を参照してください。

（注） シャーシの IPv6 管理アドレスとしてサポートされるのは、IPv6 グローバル ユニキャスト アドレスのみです。

例

次の例は、現在のIPv4管理インターフェイスおよびゲートウェイアドレスを表示し、新しいアドレスを指定する方法を示しています。

```
FP9300-A # scope fabric-interconnect a
FP9300-A /fabric-interconnect # show

Fabric Interconnect:
ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
Prefix Operability
---- --------------- --------------- --------------- ---------------- ----------------
------ -----------
A    192.0.2.112     192.0.2.1       255.255.255.0   ::               ::
64     Operable
FP9300-A /fabric-interconnect # set out-of-band ip 192.0.2.111 netmask 255.255.255.0 gw
 192.0.2.1
Warning: When committed, this change may disconnect the current CLI session
FP9300-A /fabric-interconnect* # commit-buffer
FP9300-A /fabric-interconnect #
```

次の例は、現在のIPv6管理インターフェイスおよびゲートウェイアドレスを表示し、新しいアドレスを指定する方法を示しています。

```
FP9300-A # scope fabric-interconnect a
FP9300-A /fabric-interconnect # scope ipv6-config
FP9300-A /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
IPv6 Address                       Prefix     IPv6 Gateway
---------------------------------- ---------- ------------
2001::8998                         64         2001::1
FP9300-A /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999 ipv6-prefix
 64 ipv6-gw 2001::1
FP9300-A /fabric-interconnect/ipv6-config* # commit-buffer
FP9300-A /fabric-interconnect/ipv6-config #
```

コマンド	説明
show	現在のデバイス管理 IP アドレスを表示します。
show ipv6-if	現在のデバイス管理 IPv6 アドレスを表示します。

set password

ユーザ アカウントのパスワードを指定するには、**set password** コマンドを使用します。

set password

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

`scope security/`：現在ログインしているユーザのパスワードを変更します

`scope security/scope local-user/`：現在のローカル ユーザのパスワードを指定します

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

set password コマンドを入力すると、パスワードの入力と確認を求めるプロンプトが表示されます。セキュリティ上の理由から、入力したパスワードは CLI ウィンドウには表示されません。

このパスワードの最小文字数は 8 文字、最大文字数は 80 文字です。特定の最小文字数を定義するには、set min-password-length （65 ページ）を使用します。「強力な」パスワードを使用する必要があるには、set enforce-strong-password （37 ページ）を使用します。

例

次の例は、セキュリティ モードを開始し、新しいローカル ユーザ アカウントを作成し、そのユーザのパスワードを指定する方法を示しています。

```
firepower# scope security
firepower /security # create local-user test_user
firepower /security/local-user* # set password
Enter a password:
Confirm the password:
firepower /security/local-user* # commit-buffer
firepower /security/local-user #
```

コマンド	説明
create local-user	新規のローカル ユーザ アカウントを作成します。
set expiration	ユーザ アカウントが期限切れになる日付を指定します。

set password-encryption-key

設定のエクスポート中に機密情報を暗号化するときに使用されるキーを指定するには、**set password-encryption-key** コマンドを使用します。

set password-encryption-key

構文の説明

このコマンドには引数またはキーワードはありません。コマンドを入力すると、暗号キーを入力して確認するように求められます。

キーの長さは 4 ～ 40 文字です。入力したキーは 128 ビットの MD5 ハッシュ値を生成するために使用されます。

コマンド モード

scope security/

コマンド履歴

リリース	変更内容
2.6.1	コマンドが追加されました。

使用上のガイドライン

設定エクスポート機能を使用すると、Firepower 4100/9300 シャーシの論理デバイスとプラットフォーム構成設定を含む XML ファイルをリモート サーバにエクスポートできます。このコンフィギュレーション ファイルを後でインポートして Firepower 4100/9300 に迅速に構成設定を適用し、既知の構成に戻したり、システム障害から回復させたりすることができます。

FXOS 2.6.1 以降、設定のエクスポート中にパスワードやその他の秘密キーなどの機密情報を暗号化する際に使用するキーを指定する必要があります。設定をエクスポートする前に、パスワードやその他の秘密キーを指定しておく必要があります。

また、ファイルが 2.6.1 より前の FXOS リリースからファイルがエクスポートされない限り、エクスポートされた設定をインポートする場合にターゲット システムで、エクスポート時に同じキーが使用されるように設定する必要もあります。この場合、ターゲット システムはインポートを許可します。

パスワード暗号キーが設定されると、factory-reset または password-recovery を実行しない限り、変更または削除することはできません。factory-reset または password-recovery はキーをクリアして、キーが設定されていない状態にします。

例

次の例は、現在の設定をエクスポートする前にパスワード暗号キーを指定する方法を示しています。

```
firepower # scope security
firepower /security # set password-encryption-key
Enter a key:
Confirm the key:
Warning: Please make note of the encryption key configured. If you change the key,
importing configurations that were exported with the previous key will fail, because
```

```
Import and Export requires the same encryption key on the system.
firepower /security* # commit-buffer
firepower /security #
```

関連コマンド

コマンド	説明
cfg-export-policy	エクスポート ポリシーを設定します。
export-config	現在のシステム設定をリモート サーバに XML ファイルとしてエクスポートします。
import-config	以前にエクスポートした XML コンフィギュレーション ファイルをこのアプライアンスにコピーします。

set (password-profile)

ローカルユーザー パスワードプロファイル パラメータを指定または変更するには、パスワード プロファイル モードで **set** コマンドを使用します。

set {**change-count** | **change-during-interval** | **change-interval** | **history-count** | **no-change-interval**}

構文の説明

change-count *count*	ユーザーが自分のパスワードを変更できる最大回数（**set change-interval** で指定された期間中）。値は 0 ～ 10 で指定できます。
change-during-interval {**disable** | **enable**}	ローカル認証されたユーザーがパスワードを変更できる回数に対する制限を有効または無効にします。 • `disable`：パスワード変更回数に対する制限を無効にします。 • `enable`：パスワード変更回数に対する制限を有効にします。 このオプションは、ローカル認証されたユーザが自分のパスワードを変更できる最大回数を指定し、パスワードの変更回数を実行できる時間を指定する前に有効にする必要があります。
change-interval *interval*	ユーザのパスワード変更間隔は、**set change-count** コマンドで指定された最大回数を超えないように設定します。時間は 1 ～ 745 で指定できます。 この間隔を指定する前に **set change-during-interval** オプションを有効にしておく必要があります。
history-count *count*	ローカル認証されたユーザーが、以前に使用したパスワードを再利用できるようになるまでに、作成する必要がある一意のパスワードの数。0 ～ 15 の値を指定できます。 デフォルトの *count* 値はゼロのため、パスワード履歴カウントが無効になり、ユーザーは以前使用したパスワードをいつでも再利用できます。
no-change-interval *hours*	ユーザーが自分のパスワードを再度変更できない時間。1 ～ 745 の値を指定できます。 **set change-during-interval** オプションは、この時間を設定するまで無効にしておく必要があります。そうしないと、この値は無視されます。

コマンド モード

scope security/scope password-profile/

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

set change-during-interval オプションは、ローカル認証されたユーザーが自分のパスワードを変更できる最大回数を指定し、パスワードの変更回数を実行できる時間を指定する前に有効にする必要があります。

デフォルトの **set history-count** 値はゼロのため、パスワード履歴カウントが無効になり、ユーザーは以前使用したパスワードをいつでも再利用できます。

例

次の例は、パスワードプロファイルモードを開始し、パスワード変更の制限を有効にして、ユーザーが48時間に2回だけ自分のパスワードを変更できるように指定してから、現在の設定を表示する方法を示しています。

```
firepower # scope security
firepower /security # scope password-profile
firepower /security/password-profile # set change-during-interval enable
firepower /security/password-profile* # set change-count 2
firepower /security/password-profile* # set change-interval 48
firepower /security/password-profile* # commit-buffer
firepower /security/password-profile # show detail

Password profile:
    Password history count: 5
    No password changes allowed (in Hours): 24
    Password change during interval: Enable
    Password change interval (in Hours): 48
    Password change count: 2
firepower /security/password-profile #
```

関連コマンド

コマンド	説明
show detail	現在のパスワードプロファイル設定を表示します。

set phone

ユーザ アカウントの連絡先電話番号を設定するには、**set phone** コマンドを使用します。

set phone *tel_number*

構文の説明

tel_number	ユーザ アカウントの連絡先電話番号。最大 20 文字。

コマンド モード

ローカル ユーザ モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

例

次の例は、現在のローカル ユーザの電話番号を指定する方法を示しています。

```
FP9300-A /security/local-user # set phone +1-408-555-1212
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

関連コマンド

コマンド	説明
create local-user	新規のローカル ユーザ アカウントを作成します。
set phone-contact	Smart Call Home アカウントの連絡先電話番号を指定します。

set (port-channel)

既存のポートチャネルのパラメータを指定または編集するには、ポートチャネル モードで **set** コマンドを使用します。

set {**auto-negotiation** | **descr** | **duplex** | **flow-control-policy** | **lacp-policy-name** | **nw-ctrl-policy** | **port-channel-mode** | **port-type** | **speed**}

構文の説明

auto-negotiation {**no** | **yes**}	速度、デュプレックス、フロー制御など、一般的な伝送パラメータの自動ネゴシエーションを有効または無効にします。 • **no** ：自動ネゴシエーションを無効にします。 • **yes** ：自動ネゴシエーションを有効にします。
descr *description*	ポートチャネルに説明を追加できます。説明は 0 ～ 256 文字で指定できます。ダッシュやアンダースコアのようにほとんどの英数字を使用できます。スペースは使用できません。文字列の末尾には、セミコロン、ピリオド（終止符）、および感嘆符などの句読点を使用できますが、説明にはこれらの文字を埋め込むことはできません。
duplex {**fullduplex** | **halfduplex**}	ポートチャネルのデュプレックス モードを定義します。 • **fullduplex** ：双方向の同時通信を指定します。 • **halfduplex** ：一方向通信を指定します。
flow-control-policy *name*	フロー制御ポリシーをポートチャネルに割り当てることができます。ポリシー名を指定します。最大 16 文字の英数字を使用できます。
lacp-policy-name *name*	LACP ポリシーをポートチャネルに割り当てることができます。ポリシー名を指定します。最大 16 文字の英数字を使用できます。
nw-ctrl-policy *name*	ネットワーク制御ポリシーをポートチャネルに割り当てることができます。ポリシー名を指定します。最大 16 文字の英数字を使用できます。

port-channel-mode {**active** | **on**}	ポートチャネルの物理データまたはデータ共有インターフェイスのモードを定義します。 • **active**：LACP アップデートを送信および受信します。アクティブ ポートチャネルは、アクティブまたはパッシブ ポートチャネルのいずれかと接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。これはデフォルトです。 • **on**：ポートチャネルは常にオンであり、LACP は使用されません。「オン」ポートチャネルは、別の「オン」ポートチャネルとの接続のみを確立できます。 非データ インターフェイスはアクティブ モードのみをサポートします。
port-type {**cluster** | **data** | **data-sharing** | **firepower-eventing** | **mgmt**}	ポートチャネル タイプまたは機能を指定します。 • **cluster**：このポートチャネルをクラスタ制御リンクとして使用する場合のみ、**cluster** を指定します。 • **data**：通常のデータ伝送に使用します。これがデフォルトのタイプです。 • **data-sharing**：通常のデータに使用します。コンテナ インスタンスでのみサポートされます。 • **firepower-eventing**：このポートチャネルを Threat Defense デバイスのセカンダリ管理インターフェイスとして使用します。firepower-eventing ポートチャネルを使用すると、すべてのイベントのトラフィック（Web イベントなど）を運べます。 • **mgmt**：アプリケーション インスタンスの管理に使用します。各論理デバイスには、管理インターフェイスを 1 つだけ割り当てることができます。 このコマンドの詳細については、set port-type （82 ページ）を参照してください。
speed {**100gbps** | **100mbps** | **10gbps** | **10mbps** | **1gbps** | **40gbps**}	ポート データ転送速度を指定します。 • **100gbps**：100 ギガビット/秒。 • **100mbps**：100 メガビット/秒。 • **10gbps**：10 ギガビット/秒。 • **10mbps**：10 メガビット/秒。 • **1gbps**：1 ギガビット/秒。 • **40gbps**：40 ギガビット/秒。

コマンド モード

scope eth-uplink/scope fabric a/port-channel/

コマンド履歴

リリース	変更内容
2.4(1)	**data-sharing** タイプが追加されました。
1.1(4)	**firepower-eventing** タイプが追加されました。
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用してパラメータを設定する前に、メンバーインターフェイスをポートチャネルに割り当てます。

LACPポートチャネルモードはデータとデータ共有インターフェイスにのみ適用されます。非データまたは非データ共有インターフェイスの場合、モードは常に `active` です。

タイプ `cluster` はクラスタ化された論理デバイスに使用する特別なインターフェイスです。このタイプは、ユニット間のクラスタ通信用にクラスタ制御リンクに自動的に割り当てられます。デフォルトでは、クラスタ制御リンクは 48 番のポートチャネル上に自動的に作成されます。

データ インターフェイスは論理デバイス間で共有できません。

タイプ `data-sharing` はコンテナ インスタンスでのみサポートされ、これらのデータ インターフェイスは 1 つまたは複数の論理デバイス/コンテナ インスタンス（Threat Defense のみ）で共有できます。各コンテナインスタンスは、このインターフェイスを共有する他のすべてのインスタンスと、バック プレーン経由で通信できます。共有インターフェイスは、展開可能なコンテナインスタンスの数に影響することがあります。共有インターフェイスは、ブリッジグループ メンバインターフェイス（トランスペアレント モードまたはルーテッド モード）、インライン セット、パッシブ インターフェイス、またはフェールオーバー リンクではサポートされません。

`firepower-eventing` インターフェイスは Threat Defense デバイスのセカンダリ管理インターフェイスです。このインターフェイスを使用するには、Threat Defense CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Webイベントなど）から管理トラフィックを分類できます。『Management Center configuration guide』の「*System Configuration*」の章にある「Management Interfaces」のセクションを参照してください。Firepower イベントインターフェイスは、外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介してインターフェイスを共有する他の倫理デバイスと通信することはできません。

`mgmt` インターフェイスを使用してアプリケーション インスタンスを管理します。外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介して、インターフェイスを共有する他の倫理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを 1 つだけ割り当てることができます。

指定するインターフェイス速度はインターフェイスで使用するデュプレックス モードに影響を与えます。このため、デュプレックス モードを設定する前に速度を設定する必要があります。速度を 10 または 100 Mbps に指定すると、ポートでは半二重モードを使用するように自動的に

設定されますが、全二重モードを指定することもできます。1000 Mbps（1 Gbps）以上の速度に設定すると、自動的に全二重モードが使用されます。

デフォルトのフロー制御ポリシーを編集した場合は、インターフェイスにすでに適用されています。新しいポリシーを作成した場合は、そのポリシーをポートチャネルに適用できます。

例

次の例は、4 つのメンバー インターフェイスでポートチャネル 1 を作成し、タイプをデータに設定し、EtherChannel を On モードに設定する方法を示しています。

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # create port-channel 1
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # set port-type data
firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
firepower /eth-uplink/fabric/port-channel* # commit-buffer
firepower /eth-uplink/fabric/port-channel #
```

関連コマンド

コマンド	説明
create port-channel	EtherChannel インターフェイスを追加します。
scope interface	インターフェイス設定を指定および管理できるように物理インターフェイスを入力します。

set port-channel-mode

EtherChannel のポート チャネル モードを設定するには、**set port-channel-mode** コマンドを使用します。

set port-channel-mode {**active** | **on**}

構文の説明

active	EtherChannel 内のインターフェイスをアクティブに設定します。
on	EtherChannel 内のインターフェイスをオンに設定します。データまたはデータ共有インターフェイスでのみサポートされます。

コマンド デフォルト

デフォルト モードは、active です。

コマンド モード

scope eth-uplink/scope fabric a/create port-channel/

コマンド履歴

リリース	変更内容
2.4(1)	コマンドが追加されました。

使用上のガイドライン

EtherChannel内の各物理データまたはデータ共有インターフェイスを次のように設定できます。

- アクティブ：LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- オン：EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

非データ インターフェイスのみがアクティブ モードをサポートしています。

例

次の例は、4 つのメンバー インターフェイスでポートチャネル 1 を追加し、タイプをデータに設定し、EtherChannel を On モードに設定する方法を示しています。

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # create port-channel 1
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # set port-type data
```

```
firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

関連コマンド

コマンド	説明
create port-channel	EtherChannel インターフェイスを追加します。
create member-port	EtherChannel にメンバーを割り当てます。
set port-type	インターフェイス タイプを設定します。

set port-type

インターフェイスのポート タイプを設定するには、**set port-type** コマンドを使用します。

set port-type {**cluster** | **data** | **data-sharing** | **firepower-eventing** | **mgmt**}

構文の説明

cluster	クラスタ化された論理デバイスに使用する特別なインターフェイス タイプです。このタイプは、ユニット間のクラスタ通信用にクラスタ制御リンクに自動的に割り当てられます。デフォルトでは、クラスタ制御リンクは 48 番のポートチャネル上に自動的に作成されます。 マルチインスタンス クラスタリングの場合、デバイス間でクラスタタイプのインターフェイスを共有することはできません。各クラスタが別個のクラスタ制御リンクを使用でできるように、クラスタ EtherChannel に VLAN サブインターフェイスを追加できます。クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタには使用できません。Device Manager ではクラスタリングはサポートされません。
data	データ インターフェイスは論理デバイス間で共有できません。
data-sharing	コンテナ インスタンスでのみサポートされ、これらのデータ インターフェイスは 1 つまたは複数の論理デバイス/コンテナ インスタンス（Threat Defense 専用）で共有できます。各コンテナ インスタンスは、このインターフェイスを共有する他のすべてのインスタンスと、バックプレーン経由で通信できます。共有インターフェイスは、展開可能なコンテナインスタンスの数に影響することがあります。共有インターフェイスは、ブリッジグループ メンバーインターフェイス（トランスペアレントモードまたはルーテッドモード）、インラインセット、パッシブインターフェイス、クラスタ、またはフェールオーバーリンクではサポートされません。
firepower-eventing	このインターフェイスは、Threat Defense デバイスのセカンダリ管理インターフェイスです。このインターフェイスを使用するには、Threat Defense CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Web イベントなど）から管理トラフィックを分類できます。『Management Center configuration guide』の「*System Configuration*」の章にある「Management Interfaces」のセクションを参照してください。Firepower イベント インターフェイスは、外部ホストにアクセスするために 1 つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介してインターフェイスを共有する他の倫理デバイスと通信することはできません。

mgmt	管理インターフェイスを使用してアプリケーションインスタンスを管理します。外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介して、インターフェイスを共有する他の倫理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを 1 つだけ割り当てることができます。

コマンド デフォルト

デフォルトのタイプは data です。

コマンド モード

scope eth-uplink/scope fabric a/scope interface/

scope eth-uplink/scope fabric a/scope interface/create subinterface/

scope eth-uplink/scope fabric a/create port-channel/

scope eth-uplink/scope fabric a/create port-channel/create subinterface/

コマンド履歴

リリース	変更内容
2.8(1)	マルチインスタンス クラスタリングで使用する VLAN サブインターフェイスの **cluster** タイプを設定できます。
2.4(1)	**data-sharing** タイプが追加されました。
1.1(4)	**firepower-eventing** タイプが追加されました。
1.1(1)	コマンドが追加されました。

使用上のガイドライン

コンテナ インスタンスは、data-sharing タイプのインターフェイスを共有できます。この機能を使用して、物理インターフェイスの使用率を節約し、柔軟なネットワークの導入をサポートできます。インターフェイスを共有すると、シャーシは一意の MAC アドレスを使用して、正しいインスタンスにトラフィックを転送します。ただし、共有インターフェイスでは、シャーシ内にフルメッシュトポロジが必要になるため、転送テーブルが大きくなることがあります（すべてのインスタンスが、同じインターフェイスを共有するその他すべてのインスタンスと通信できる必要があります）。そのため、共有できるインターフェイスの数には制限があります。

転送テーブルに加えて、シャーシは VLAN サブインターフェイスの転送用に VLAN グループテーブルも保持します。親インターフェイスの数とその他の導入決定に応じて、最大500個の VLAN サブインターフェイスを作成できます。

共有インターフェイスの割り当てに次の制限を参照してください。

- 共有インターフェイスごとの最大インスタンス数：14。たとえば、Instance1 ～ Instance14 に Ethernet1/1 を割り当てることができます。
- インスタンスごとの最大共有インターフェイス数：10 たとえば、Ethernet1/1.10 を介して Instance1 に Ethernet1/1.1 を割り当てることができます。

スタンドアロン展開とクラスタ展開での FTD および ASA アプリケーションのインターフェイスタイプのサポートについては、次の表を参照してください。

表 *1*：インターフェイスタイプのサポート

アプリケーション		データ	データ：サブインターフェイス	データ共有	データ共有：サブインターフェイス	管理	Firepower イベント	クラスタ（EtherChannel のみ）	クラスタ：サブインターフェイス
FTD	スタンドアロン ネイティブ インスタンス	対応	—	—	—	対応	対応	—	—
	スタンドアロン コンテナ インスタンス	対応	対応	対応	対応	対応	対応	—	—
	クラスタ ネイティブ インスタンス	対応（シャーシ間クラスタ専用の EtherChannel）	—	—	—	対応	対応	対応	—
	クラスタ コンテナ インスタンス	対応（シャーシ間クラスタ専用の EtherChannel）	—	—	—	対応	対応	対応	対応

アプリケーション		データ	データ：サブインターフェイス	データ共有	データ共有：サブインターフェイス	管理	Firepower イベント	クラスタ（EtherChannel のみ）	クラスタ：サブインターフェイス
ASA	スタンドアロン ネイティブ インスタンス	対応	—	—	—	対応	—	対応	—
	クラスタ ネイティブ インスタンス	対応（シャーシ間クラスタ専用の EtherChannel）	—	—	—	対応	—	対応	—

例

次の例は、4 つのメンバー インターフェイスでポートチャネル 1 を追加し、タイプをデータに設定し、EtherChannel を On モードに設定する方法を示しています。

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # create port-channel 1
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # set port-type data
firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

次の例は、3 つのサブインターフェイスを追加し、ポート タイプを data-sharing に設定する方法を示しています。

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # enter interface Ethernet1/1
firepower /eth-uplink/fabric/interface # enter subinterface 10
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 10
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # enter subinterface 11
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 11
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
```

```
firepower /eth-uplink/fabric/interface # enter subinterface 12
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 12
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
firepower /eth-uplink/fabric/interface/subinterface #
```

関連コマンド

コマンド	説明
create port-channel	EtherChannel インターフェイスを追加します。
scope interface	インターフェイス設定を指定および管理できるように物理インターフェイスを入力します。

set port-type (aggr-interface)

インターフェイスのポート タイプを設定するには、**set port-type** コマンドを使用します。

set port-type { *data* | *data-sharing* | *mgmt* | *firepower-eventing* | *cluster* }

構文の説明

data	（オプション）データインターフェイスは論理デバイス間で共有できません。
data-sharing	（オプション）コンテナインスタンスでのみサポートされ、これらのデータ インターフェイスは 1 つまたは複数の論理デバイス/コンテナ インスタンス（FTD 専用）で共有できます。各コンテナ インスタンスは、このインターフェイスを共有する他のすべてのインスタンスと、バック プレーン経由で通信できます。共有インターフェイスは、展開可能なコンテナインスタンスの数に影響することがあります。共有インターフェイスは、ブリッジ グループ メンバ インターフェイス（トランスペアレント モードまたはルーテッド モード）、インライン セット、パッシブ インターフェイス、またはフェールオーバー リンクではサポートされません。
mgmt	（オプション）管理インターフェイスを使用してアプリケーション インスタンスを管理します。外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介して、インターフェイスを共有する他の倫理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを 1 つだけ割り当てることができます。
firepower-eventing	（オプション）このインターフェイスは、FTDデバイスのセカンダリ管理インターフェイスです。このインターフェイスを使用するには、FTD CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Web イベントなど）から管理トラフィックを分類できます。Management Center 構成ガイドのシステム設定の章にある「管理インターフェイス」のセクションを参照してください。Firepower イベント インターフェイスは、外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介してインターフェイスを共有する他の倫理デバイスと通信することはできません。
cluster	（オプション）クラスタ化された論理デバイスに使用する特別なインターフェイスタイプです。このタイプのインターフェイスは、ユニットクラスタ間通信用のクラスタ制御リンクに自動的に割り当てられます。デフォルトでは、クラスタ制御リンクはポートチャネル 48 に自動的に作成されます。

コマンド モード

scope cabling/scope fabric a/

コマンド履歴

リリース	変更内容
2.4(1)	**data-sharing** タイプが追加されました。
1.1(4)	**firepower-eventing** タイプが追加されました。
1.1(1)	コマンドが追加されました。

使用上のガイドライン

コンテナ インスタンスは、data-sharing タイプのインターフェイスを共有できます。この機能を使用して、物理インターフェイスの使用率を節約し、柔軟なネットワークの導入をサポートできます。インターフェイスを共有すると、シャーシは一意の MAC アドレスを使用して、正しいインスタンスにトラフィックを転送します。ただし、共有インターフェイスでは、シャーシ内にフルメッシュトポロジが必要になるため、転送テーブルが大きくなることがあります（すべてのインスタンスが、同じインターフェイスを共有するその他すべてのインスタンスと通信できる必要があります）。そのため、共有できるインターフェイスの数には制限があります。

例

次の例では、インターフェイスのポート タイプを設定し、利用可能なコマンドをリストする方法を示します。

```
firepower-9300* # scope cabling
firepower-9300 /cabling* # scope fabric a
firepower-9300 /cabling/fabric* # create breakout port breakout 2 1
firepower-9300 /cabling/fabric* # show config
 scope fabric a
+    enter breakout 2 3
+    exit
 exit
firepower-9300 /cabling/fabric* # exit
firepower-9300 /cabling* # exit
```

commit-buffer コマンドを使用すると、システムが再起動します。

```
firepower-9300* # scope eth-uplink
firepower-9300 /eth-uplink* # scope fabric a
firepower-9300 /eth-uplink/fabric* # show

Fabric:
    Fabric ID
    ---------
    Afirepower-9300 /eth-uplink/fabric* # show
  <CR>
  >               Redirect it to a file
  >>              Redirect it to a file in append mode
  aggr-interface  Aggregate Interface
  detail          Detail
  event           Event Management
  expand          Expand
  fault           Fault
  fsm             Fsm
  interface       Interface
  port-channel    Port Channel
  stats           statistics
```

```
  |              Pipe command output to filter

firepower-9300 /eth-uplink/fabric* # show aggr-interface expand
firepower-9300 /eth-uplink/fabric* # show aggr-interface
  1-4     Slot
  <CR>
  >       Redirect it to a file
  >>      Redirect it to a file in append mode
  detail  Detail
  expand  Expand
  n/n     Ethernet<Slot Id>/<Aggregate Port Id>
  |       Pipe command output to filter
firepower-9300 /eth-uplink/fabric* # show aggr-interface expand
firepower-9300 /eth-uplink/fabric* #
  acknowledge  Acknowledge
  create       Create managed objects
  delete       Delete managed objects
  enter        Enters a managed object
  scope        Changes the current mode
  show         Show system information

firepower-9300 /eth-uplink/fabric* # scope aggr-interface
  1-4  Slot
  n/n  Ethernet<Slot Id>/<Aggregate Port Id>

firepower-9300 /eth-uplink/fabric* # scope port-channel 2
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface* # create member-port
Ethernet2/1/1
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* # show config
+enter member-port 2 1
+exit
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* #
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* # exit
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface* # exit
firepower-9300 /eth-uplink/fabric/port-channel* # show config
 enter port-channel 2
     enable
+    enter aggr-interface 2 1
+        enter member-port 2 1
+        exit
+    exit
     enter member-port 1 6
         enable
     exit
     set auto-negotiation no
     set descr ""
     set duplex fullduplex
     set flow-control-policy default
     set lacp-policy-name default
     set nw-ctrl-policy default
     set port-channel-mode active
     set port-type data
     set speed 1gbps
 exit

firepower-9300 /eth-uplink/fabric/port-channel* # set port-type
  cluster            Cluster
  data               Data
  data-sharing       Data Sharing
  firepower-eventing  Firepower Eventing
  mgmt               Mgmt

firepower-9300 /eth-uplink/fabric/port-channel* # set port-type cluster
```

```
firepower-9300 /eth-uplink/fabric/port-channel* commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

関連コマンド

コマンド	説明
create port-channel	EtherChannel インターフェイスを追加します
scope interface	物理インターフェイスを編集します。

set prefix

コンテナ インスタンス インターフェイスの MAC アドレスの自動生成時に使用される MAC アドレス プレフィックスを設定するには、**set prefix** コマンドを使用します。

set prefix *prefix*

構文の説明

prefix	1 ～ 65535 の 10 進数を指定します。このプレフィックスは 4 桁の 16 進数値に変換され、MAC アドレスの一部として使用されます。

コマンド モード

scope ssa/scope auto-macpool/

コマンド履歴

リリース	変更内容
2.4(1)	コマンドが追加されました。

使用上のガイドライン

FXOS シャーシは、各インスタンスの共有インターフェイスが一意の MAC アドレスを使用するように、コンテナインスタンスインターフェイスのMACアドレスを自動的に生成します。

アプリケーション内の共有インターフェイスに MAC アドレスを手動で割り当てると、手動で割り当てられた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます。生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、アプリケーション内のインターフェイスの MAC アドレスを手動で設定してください。

自動生成されたアドレスは A2 で始まるため、アドレスが重複するリスクがあることから手動 MAC アドレスを A2 で始めることはできません。

（注） MAC アドレスを手動で設定すると、サブインターフェイスを共有していない場合でも、分類が正しく行われるように、同じ親インターフェイス上のすべてのサブインターフェイスで一意の MAC アドレスを使用します。

FXOS シャーシは、次の形式を使用して MAC アドレスを生成します。

A2*xx.yyzz.zzzz*

xx.yy はユーザ定義のプレフィックスまたはシステム定義のプレフィックスであり、*zz.zzzz* はシャーシが生成した内部カウンタです。システム定義のプレフィックスは、IDPROMにプログラムされている Burned-in MAC アドレス内の最初の MAC アドレスの下部 2 バイトと一致します。**connect fxos**を使用し、次に**show module**を使用して、MACアドレスプールを表示します。たとえば、モジュール 1 について示されている MAC アドレスの範囲が b0aa.772f.f0b0 ～ b0aa.772f.f0bf の場合、システム プレフィックスは f0b0 になります。

ユーザ定義のプレフィックスは、16進数に変換される整数です。ユーザ定義のプレフィックスの使用方法を示す例を挙げます。プレフィックスとして 77 を指定すると、シャーシは 77 を 16

進数値 004D（*yyxx*）に変換します。MAC アドレスで使用すると、プレフィックスはシャーシネイティブ形式に一致するように逆にされます（*xxyy*）。

A2**4D**.**00***zz*.*zzzz*

プレフィックス 1009（03F1）の場合、MAC アドレスは次のようになります。

A2**F1**.**03***zz*.*zzzz*

例

次の例では、MAC プレフィックスを 33 に設定しています。

```
firepower# scope ssa
firepower /ssa # scope auto-macpool
firepower /ssa/auto-macpool # set prefix 33
firepower /ssa/auto-macpool* # commit-buffer
firepower /ssa/auto-macpool
```

関連コマンド

コマンド	説明
scope ssa	ssa モードを開始します。
scope auto-macpool	auto-macpool モードを開始します。
show mac-address	指定された MAC アドレスを表示します。

set protocol

エクスポート ポリシーのリモート サーバと通信する場合に使用されるプロトコルを指定するには、**set protocol** コマンドを使用します。

set protocol {**ftp** | **scp** | **sftp** | **tfp**}

構文の説明

ftp	ファイル転送用のファイル転送プロトコル（FTP）を指定します。
scp	ファイル転送用のセキュア コピー プロトコル（SCP）を指定します。
sftp	ファイル転送用のセキュア ファイル転送プロトコル（SFTP）を指定します。
tfp	ファイル転送用の簡易ファイル転送プロトコル（TFTP）を指定します。

コマンド モード

設定のエクスポート ポリシー（/org/cfg-export-policy）

コマンド履歴

リリース	変更内容
2.0.1	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、ファイル転送プロトコルを設定します。

例

次の例は、エクスポート ポリシーのポート番号を設定する方法を示しています。

```
firepower-9300* # scope org
firepower-9300 /org* # scope cfg-export-policy default
firepower-9300 /org/cfg-export-policy* # set protocol scp
firepower-9300 /org/cfg-export-policy* # commit-buffer
firepower-9300 /org/cfg-export-policy #
```

関連コマンド

コマンド	説明
set adminstate (/org)	エクスポート ポリシーを有効にします。
set hostname (/org)	バックアップ ファイルを格納する場所のホスト名を指定します。
set password (/org)	リモート サーバのユーザ名のパスワードを指定します。
set port (/org)	ポート番号を指定します。
set protocol (/org)	リモート サーバとの通信時に使用するプロトコルを指定します。

コマンド	説明
set remote-file (/org)	ファイル名を含むコンフィギュレーション ファイルをエクスポートする場所のフル パスを指定します。
set schedule (/org)	設定を自動的にエクスポートするスケジュールを指定します。
set user (/org)	システムがリモート サーバへのログインに使用する必要のあるユーザ名を指定します。

set realm

デフォルトの認証サービスを指定するには、**set realm** コマンドを使用します。

set realm {**ldap** | **local** | **none** | **radius** | **tacacs**}

構文の説明

ldap	LDAP 認証を指定します。
local	ローカル認証を指定します。
none	ローカル ユーザはパスワードを指定せずにログインできます。
radius	RADIUS 認証を指定します。
tacacs	TACACS+ 認証を指定します。

コマンド モード

デフォルト認証モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

例

次の例は、security/default-auth モードを開始し、デフォルトの認証サービスを Radius に設定する方法を示しています。

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set realm radius
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

関連コマンド

コマンド	説明
set auth-server-group	関連する認証プロバイダー グループを指定します。
set use-2-factor	認証方式を Radius または TACACS+ レルムの二要素認証に設定します。

set refresh-period

Webセッションの更新期間（このドメインのユーザに許可された更新要求間の最大時間）を設定するには、**set refresh-period** コマンドを使用します。

set refresh-period *seconds*

構文の説明

seconds	Webセッションが非アクティブと見なされるまでの秒数。値は0～3600秒です。デフォルトは600秒です。

コマンドモード

デフォルト認証モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

この時間制限を超えると、FXOSはWebセッションを非アクティブと見なしますが、そのセッションを終了することはありません。

例

次の例は、デフォルトの認証モードを開始し、セッションの更新間隔を設定する方法を示しています。

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set refresh-period 800
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

関連コマンド

コマンド	説明
set タイムアウト値	**set absolute-session-timeout**、**set con-absolute-session-timeout**、**set con-session-timeout**、および **set session-timeout** コマンドを使用してさまざまなタイムアウト値を設定します。

set regenerate

デフォルトのキーリング内のキーを再生成するには、**set regenerate** コマンドを使用します。

set regenerate {**no** | **yes**}

構文の説明

no	キーを再生成しません。
yes	キーを再生成します。

コマンド モード

キーリング モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、デフォルトのキーリング内の RSA キーを再生成します。このコマンドは、デフォルトのキーリング内だけに適用されます。

例

次に、デフォルトのキーリング内のキーを再生成する例を示します。

```
FP9300-A# scope security
FP9300-A /security # scope keyring default
FP9300-A /security/keyring # set regenerate yes
FP9300-A /security/keyring* # commit-buffer
switch-A /security/keyring #
```

関連コマンド

コマンド	説明
set cert	キー リングの RSA 証明書を入力します。
set modulus	RSA キー係数（SSL キーの長さ）をビット単位で指定します。
set trustpoint	キーリング証明書を再生成できるかどうかを指定します。

set remote-address

IPSec 接続のリモート IP アドレスを指定するには、**set remote-address** コマンドを使用します。

set remote-address *ip_address*

構文の説明

ip_address	IPSec 接続の IPv4 または IPv6 リモート ゲートウェイ アドレスを入力します。最大 510 文字。

コマンド モード

接続（/security/ipsec/connection）モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドと **set local-address** コマンドを使用して、IPSec 接続のエンドポイントを定義します。

例

次の例は、IPSec 接続のリモート アドレスを設定する方法を示しています。

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set local-address 209.165.202.129
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

コマンド	説明
create connection	新しい IPSec 接続を作成します。
set local-addr	IPSec 接続のローカル IP アドレスを設定します。

set remote-ike-ident

IPSec トンネル接続のリモート ピア IKE ID を指定するには、**set remote-ike-ident** コマンドを使用します。

set remote-ike-ident *remote_ID*

構文の説明

remote_ID	リモート ピアの IKE ID。最大 510 文字。

コマンド モード

接続（/security/ipsec/connection）モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、IPSec 接続のリモート ピアの IKE ID を指定します。この ID は、IKE ネゴシエーション中のピアの検証に使用されます。

例

次の例は、IPSec 接続のリモート IKE ID を指定する方法を示しています。

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set remote-ike-ident 203.0.113.12
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

コマンド	説明
create connection	新しい IPSec 接続を作成します。
set remote-addr	IPSec 接続のリモート IP アドレスを設定します。

set remote-subnet

IPSec トンネル接続のリモート サブネットを指定するには、**set remote-subnet** コマンドを使用します。

set remote-subnet *ip_address/mask_bits*

構文の説明

ip_address/mask_bits	IPSec 接続の IPv4 または IPv6 リモート サブネット アドレス/マスクを入力します。最大 510 文字。

コマンド モード

接続（/security/ipsec/connection）モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、IPSec 接続のリモート サブネットの IP アドレス/マスクを指定します。

例

次の例は、IPSec 接続のリモート サブネットを設定する方法を示しています。

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set remote-subnet 209.165.202.128/27
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

コマンド	説明
create connection	新しい IPSec 接続を作成します。
set remote-addr	IPSec 接続のリモート IP アドレスを設定します。

set remote-user

確立されたユーザ ロールに一致するユーザへのアクセスを制限するには、**set remote-user** コマンドを使用します。

set remote-user default-role {**assign-default-role** | **no-login**}

構文の説明

assign-default-role	ユーザがログインを試みたときに、リモート認証プロバイダーがユーザの認証情報を含むユーザ ロールを提供しないと、ユーザは読み取り専用ユーザ ロールでログインすることができます。
no-login	ユーザがログインを試みたときに、リモート認証プロバイダーがユーザの認証情報を含むユーザ ロールを提供しないと、アクセスは拒否されます。

コマンド モード

セキュリティ モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

assign-default-role デフォルトの動作です。

例

次の例は、セキュリティ モードを開始し、ユーザ ロールが指定されていないユーザのアクセスを拒否する方法を示しています。

```
FP9300-A# scope security
FP9300-A /security # set remote-user default-role no-login
FP9300-A /security* # commit-buffer
FP9300-A /security #
```

関連コマンド

コマンド	説明
set authentication	デフォルトの認証サービスを指定します。

set reporting-interval

モニタ対象の統計情報を報告する頻度を定義するには、**set reporting-interval** コマンドを使用します。

set reporting-interval *interval*

構文の説明

interval	統計情報報告間隔を定義する時間の長さ。使用可能な値は次のとおりです。 • `15minutes`：15 分間隔 • `2hours`：2 時間（120 分）間隔 • `2minutes`：2 分間隔 • `30minutes`：30 分間隔 • `4hours`：4 時間（240 分）間隔 • `60minutes`：60 分（1 時間）間隔 • `8hours`：8 時間（480 分）間隔

コマンド モード

scope monitoring/scope stats-collection-policy/

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

set collection-interval コマンドを使用して、統計情報を収集する頻度を定義し、**set reporting-interval** コマンドを使用して、統計情報を報告する頻度を定義します。これらの間隔で統計情報収集ポリシーが定義されます。

報告インターバル中に複数の統計データ ポイントが収集できるように、報告インターバルは収集インターバルよりも長くなります。これにより、最小値、最大値、平均値を計算して報告するために十分なデータが提供されます。

統計情報は、Firepower システムの次の機能領域ごとに収集して報告することができます。特定の収集ポリシーにアクセスするには、**scope stats-collection-policy** コマンドを使用します。

- `Adapter`：アダプタに関連した統計情報。
- `Chassis`：ブレード シャーシに関連した統計情報。
- `Fex`：設定されたファブリック エクステンダに関連した統計情報。
- `Host`：このポリシーは今後サポートされる機能のプレースホルダです。

- Port：サーバ ポート、アップリンク イーサネット ポート、およびアップリンク ファイバ チャネル ポートを含むポートに関連した統計情報。
- Server：サーバに関連した統計情報。

（注） 機能エリアごとにデフォルト統計情報収集ポリシーが 1 つずつあります。追加で統計情報収集ポリシーを作成できません。また、既存のデフォルト ポリシーを削除できません。デフォルト ポリシーを変更することだけが可能です。

例

次の例は、ポートの統計情報収集ポリシーを入力し、収集間隔を1分に設定し、レポート間隔を 30 分に設定し、トランザクションをコミットする方法を示しています。

```
firepower # scope monitoring
firepower /monitoring # scope stats-collection-policy port
firepower /monitoring/stats-collection-policy # set collection-interval 1minute
firepower /monitoring/stats-collection-policy* # set reporting-interval 30minute
firepower /monitoring/stats-collection-policy* # commit-buffer
firepower /monitoring/stats-collection-policy #
```

関連コマンド

コマンド	説明
scope stats-collection-policy	stats-collection-policy モードを開始します。ここでは、統計情報の収集と報告の間隔を管理できます。
set collection-interval	統計情報の収集頻度を指定します。

set resource-profile-name

アプリケーション インスタンスのリソース プロファイルを設定するには、**set resource-profile-name** コマンドを使用します。

set resource-profile-name *profile_name*

構文の説明

profile_name	このアプリケーション インスタンスのリソース プロファイル名を設定します。

コマンド モード

scope ssa/scope slot/create app-instance/

コマンド履歴

リリース	変更内容
2.4(1)	コンテナ インスタンスで使用できるようになりました。
1.1(1)	vDP で使用するコマンドが追加されました。

使用上のガイドライン

vDP の場合、リソース プロファイルは、vDP イメージのダウンロード時に FXOS 設定で事前に作成されます。コンテナ インスタンスの場合、**create resource-profile** コマンドを使用してリソース プロファイルを作成します。**show resource-profile system** コマンドを使用して、利用可能なプロファイルを表示します。

実行中のアプリケーション インスタンスのリソース プロファイルを変更すると、インスタンスが再起動します。

例

次の例は、vDPアプリケーションインスタンスのリソースプロファイルを設定する方法を示しています。

```
firepower# scope ssa
firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default
 App
   ---------- --------------- ---------- ---------------------- ----------- --------------

    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
    vdp        8.13.01.09-2    radware    Vm                     Application Yes

firepower /ssa # show resource-profile system
Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical Core
Count RAM Size (MB)  Default Profile Profile Type Description
------------------ ---------- ------------ ---------- ---------------
---------------------- -------------- --------------- ------------ -----------
DEFAULT-4110-RESOURCE
                   vdp        8.13.01.09-2 No         FPR4K-SM-12
    4          16384 Yes             System
DEFAULT-RESOURCE   vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44,
```

```
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

    6          24576 Yes              System
VDP-10-CORES       vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

   10          40960 No               System
VDP-2-CORES        vdp        8.13.01.09-2 No         all
    2           8192 No               System
VDP-4-CORES        vdp        8.13.01.09-2 No         all
    4          16384 No               System
VDP-8-CORES        vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

    8          32768 No               System
firepower /ssa/app # exit
firepower /ssa # scope slot 1
firepower /ssa/slot # create app-instance vdp VDP1
firepower /ssa/slot/app-instance* # set resource-profile-name VDP-10-CORES
firepower /ssa/slot/app-instance* #
```

例

次の例は、Threat Defense コンテナ インスタンスのリソース プロファイルを設定する方法を示しています。

```
firepower# scope ssa
firepower /ssa # show resource-profile

Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical Core
Count RAM Size (MB)  Default Profile Profile Type Description
------------------ ---------- ------------ ---------- ---------------
---------------------- -------------- --------------- ------------ -----------
bronze             N/A        N/A          No         all
    6            N/A No              Custom       low end device
silver             N/A        N/A          No         all
    8            N/A No              Custom       mid-level

firepower /ssa # scope slot 1
firepower /ssa/slot # create app-instance ftd FTD1
firepower /ssa/slot/app-instance* # set resource-profile-name silver
firepower /ssa/slot/app-instance* #
```

関連コマンド

コマンド	説明
show app-attri	現在のアプリケーション属性を表示します。
create resource-profile	コンテナ インスタンスで使用するリソース プロファイルを作成します。
show resource-profile-name	利用可能なリソース プロファイルを表示します。

set session-timeout

Web、SSH、および Telnet セッションのアイドル セッション タイムアウトを設定するには、**set session-timeout** コマンドを使用します。

set session-timeout *seconds*

構文の説明

seconds	Web、SSH、および Telnet セッションのアイドル セッション タイムアウト。値は 0 ～ 3600 秒で指定できます。

コマンド モード

デフォルト認証モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、Web、SSH、および Telnet セッションのアイドル セッション タイムアウトを指定します。

例

次の例は、デフォルトの認証モードを開始し、アイドル セッション タイムアウトを 4 分に設定する方法を示しています。

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set session-timeout 240
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

関連コマンド

コマンド	説明
set refresh-period	Web セッション更新期間を設定します。
show detail	現在のセッションおよび絶対セッション タイムアウト設定を表示します。

set snmp

Simple Network Management Protocol（SNMP）の設定パラメータを設定するには、**set snmp** コマンドを使用します。

set snmp {**community** | **syscontact** | **syslocation**}

構文の説明

community	このコマンドを入力すると、1 ～ 32 文字の英数字の SNMP コミュニティ名を入力するように求められます。入力したコミュニティ名は表示されませんが、**Enter** キーを押すと、バッファをコミットする必要があることを示すアスタリスクがプロンプト表示されます。
syscontact *name*	このシステム上の SNMP に関して連絡する担当者の名前を入力します。0 ～ 255 文字の英数字を指定できます。
syslocation *location*	このシステムの場所を入力します。0 ～ 510 文字の英数字を指定できます。

コマンド モード

scope monitoring/

コマンド履歴

リリース	変更内容
1.1.1	コマンドが追加されました。

使用上のガイドライン

シスコでは、他のネットワーク アプリケーションとのやり取りに必要なコミュニケーション サービスだけを有効にすることを推奨しています。

このシステムで SNMP を設定する前に SNMP エージェント（**enable snmp**）を有効にする必要があります。

set snmp community を使用して、SNMP トラップの宛先へのアクセスを許可するために使用されるコミュニティ アクセス ストリングを指定します。SNMPv1 または SNMPv2c が SNMP バージョンとして設定されている場合は、コミュニティ引数がコミュニティストリングとして使用されます。SNMPv3 が設定されている場合は、コミュニティ引数がトラップメッセージを送信するための SNMP ユーザー名として使用されます。

SNMP コミュニティ名を指定すると、SNMP リモートマネージャからのポーリング要求に対して SNMP バージョン 1 および 2c も自動的に有効になります。

（注） SNMP バージョン 1 および 2c には、重大な既知のセキュリティ問題があるので注意してください。これらのバージョンでは、すべての情報が暗号化されずに送信されます。これらのバージョンで唯一の認証形式として機能するコミュニティストリングも含まれます。

コミュニティ名は 1 つだけです。ただし、**set snmp community** を使用して既存の名前を上書きすることができます。既存のコミュニティ名を削除するには、**set snmp community** を入力します。ただし、コミュニティストリングは入力しないでください。つまり、もう一度**Enter**キーを押します。バッファをコミットすると、**show snmp** の出力に `Is Community Set: No` という行が含まれます。

例

次の例は、モニタリング モードを開始し、SNMP 処理を有効にし、SNMP コミュニティ文字列とシステム連絡先を設定し、変更をコミットし、**show snmp** コマンドを使用して変更を確認する方法を示しています。

```
firepower # scope monitoring
firepower /monitoring # enable snmp
firepower /monitoring* # set snmp community
Enter a snmp community:
firepower /monitoring* # set snmp syscontact R_Admin
firepower /monitoring* # commit-buffer
firepower /monitoring # show snmp
Name: snmp
    Admin State: Enabled
    Port: 161
    Is Community Set: Yes
    Sys Contact: R_Admin
    Sys Location:
firepower /monitoring #
```

関連コマンド

コマンド	説明
disable snmp	SNMP をディセーブルにします。
enable snmp	SNMP を有効にします。
show snmp	現在の SNMP 設定を表示します。

set (snmp-trap)

Simple Network Management Protocol（SNMP）トラップパラメータを指定するには、snmp-trap モードで **set** コマンドを使用します。

set {**community** | **notificationtype** | **port** | **v3privilege** | **version**}

構文の説明

community	トラップの宛先へのアクセスを許可するために必要な SNMPv1/v2c コミュニティストリングまたは SNMPv3 ユーザ名を指定します。このコマンドを入力すると、コミュニティ名が照会されます。名前は最大 32 文字で、スペースは使用できません。名前は入力しても表示されません。
notificationtype {**informs** | **traps**}	このエージェントによって生成される SNMP 通知のタイプを指定します。 • **informs**：これらは、重要なローカルイベントをマネージャに通知するために送信される非要請通知です。これらのメッセージは確認応答されます。このオプションは、**version** が **vc2** に設定されている場合にのみ使用できます。 • **traps**：これらは、重要なローカルイベントをマネージャに通知するために送信される非要請通知です。これらのメッセージは確認応答されません。
port *port_num*	エージェントが SNMP 要求を受信するポートを変更するには、このコマンドを使用います。デフォルトのポートは 161 です。
v3privilege {**auth** | **noauth** | **priv**}	このコマンドを使用して、送信された SNMP トラップの Simple Network Management Protocol バージョン 3（SNMPv3）セキュリティレベルを指定します。 • **auth**：キー付きハッシュ認証を指定しますが、暗号化は指定しません。 • **noauth**：認証または暗号化を指定しません。これを指定することはできますが、FXOS は SNMPv3 でこのセキュリティレベルをサポートしていないことに注意してください。 • **priv**：キー付きハッシュ認証とデータの暗号化（プライバシー）を指定します。

version {**v1** | **v2c** | **v3**}	トラップ通知を送信するときに使用するSNMPセキュリティモデルを指定するには、このコマンドを使用します。 • **v1**：SNMP バージョン 1 を指定します。 • **v2c**：SNMP バージョン 2c を指定します。 • **v3**：SNMP バージョン 3 を指定します。 （注） SNMP バージョン 1 および 2c には、重大な既知のセキュリティ問題があるので注意してください。これらのバージョンでは、すべての情報が暗号化されずに送信されます。これらのバージョンで唯一の認証形式として機能するコミュニティストリングも含まれます。

コマンド モード

scope monitoring/snmp-trap

コマンド履歴

リリース	変更内容
1.1.1	コマンドが追加されました。

使用上のガイドライン

SNMP（**enable snmp**）を有効にするには、SNMP トラップを作成してこれらのパラメータを設定する前に、SNMP コミュニティ（**set snmp community**）を作成する必要があります。

新しいSNMPトラップを作成すると、新しいトラップがまだコミットされていないことを示すアスタリスクが付いた monitoring/snmp-trap モードが自動的に開始されます。

（注） 最大 8 つの SNMP トラップを作成できます。

set version を使用して SNMPv1 または SNMPv2c が設定されている場合、**set community** 引数がコミュニティストリングとして使用されます。SNMPv3 が設定されている場合は、その引数が、通知を送信するためのユーザー名として使用されます。

SNMPv3 では、トラップの **v3privilege** 設定が、関連する SNMPv3 ユーザーのセキュリティレベルと互換性がある必要があります。つまり、関連付けられたユーザーのセキュリティ設定は、少なくともトラップの設定と同じくらいセキュアである必要があります。たとえば、認証がSNMPv3ユーザーに対して有効になっている場合（認証は行われるが、プライバシー暗号化は行われない）、ユーザーのpriv-passwordは設定されません。一方、プライバシーを有効にして（つまり、認証が行われ、プライバシー暗号化も行われる）通知を送信する場合は、ユーザーの priv-password が設定されます。SNMPv3 ユーザーに関連付けられたパスワードは、トラップ/通知の送信時にユーザーを認証するために使用されます。

例

次の例は、SNMP を有効にし、IPv4 アドレスを使用して SNMP トラップを作成し、バージョンを v3 に設定し、v3 権限レベルをプライバシーに設定し、トランザクションをコミットします。

```
firepower # scope monitoring
firepower /monitoring/ # enable snmp
firepower /monitoring/ # create snmp-trap 192.168.100.112
firepower /monitoring/snmp-trap* # set notificationtype traps
firepower /monitoring/snmp-trap* # set version v3
firepower /monitoring/snmp-trap* # set v3privilege priv
firepower /monitoring/snmp-trap* # commit-buffer
firepower /monitoring/snmp-trap #
```

関連コマンド

コマンド	説明
create snmp-trap	新しい SNMP トラップ宛先を作成します。
enable snmp	SNMP をイネーブルにします。

set (snmp-user)

既存の Simple Network Management Protocol（SNMP）v3 ユーザーのパラメータを指定するには、`snmp-user` モードで **set** コマンドを使用します。

set {**aes-128** | **auth** | **password** | **priv-password**}

構文の説明

aes-128 {**no** | **yes**}	Advanced Encryption Standard（AES）-128 暗号化の使用を無効または有効にします。`no` または `yes` を入力してください。 デフォルトでは、AES-128 暗号化は無効になっています。
auth sha	HMAC Secure Hash Algorithm（SHA）に基づく SNMPv3 ユーザーの認証を有効にします。
password	このユーザーのパスワードを指定します。このコマンドを入力すると、パスワードの入力と確認を求められるようになります。
priv-password	ユーザー プライバシー パスワードを指定します。このコマンドを入力すると、パスワードの入力と確認を求められるようになります。AES プライバシーパスワードは 8 文字以上である必要があります。

コマンド モード

scope monitoring/snmp-user

コマンド履歴

リリース	変更内容
1.1.1	コマンドが追加されました。

使用上のガイドライン

SNMP ユーザーを作成してこれらのパラメータを設定する前に、SNMP を有能にする（**enable snmp**）必要があります。

新しいSNMPユーザを作成すると、新しいユーザがまだコミットされていないことを示すアスタリスクが付いた monitoring/snmp-user モードが自動的に開始されます。

プライバシーパスワード（priv オプション）では、SNMP セキュリティ暗号化方式として DES または 128 ビット AES を選択できます。AES-128 の設定を有効にして、SNMPv3 ユーザ用のプライバシー パスワードを含めると、Firepower シャーシはそのプライバシー パスワードを使用して 128 ビット AES キーを生成します。

例

次の例では、`snmp-user14` という名前の SNMPv3 ユーザーを作成し、AES-128 暗号化を有効化し、パスワードおよびプライバシーパスワードを設定し、トランザクションをコミットします。

```
firepower # scope monitoring
firepower /monitoring/ # enable snmp
firepower /monitoring/ # create snmp-user snmp-user14
Password:
firepower /monitoring/snmp-user* # set aes-128 yes
firepower /monitoring/snmp-user* # set priv-password
Enter a password:
Confirm the password:
firepower /monitoring/snmp-user* # commit-buffer
firepower /monitoring/snmp-user #
```

関連コマンド

コマンド	説明
create snmp-user	新しい SNMPv3 ユーザーを作成します。
enable snmp	SNMP をイネーブルにします。

set speed

インターフェイスの速度を設定するには、**set speed** コマンドを使用します。

（注） このコマンドは、ポートチャネル範囲でのみ使用できます。

set speed { **10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps** }

構文の説明

10mbps	（任意）速度を 10 Mbps に設定します。
100mbps	（任意）速度を 100 Mbps に設定します。
1gbps	（任意）速度を 1 Gbps に設定します。
10gbps	（任意）速度を 10 Gbps に設定します。
40gbps	（任意）速度を 40 Gbps に設定します。
100gbps	（任意）速度を 100 Gbps に設定します。

コマンド モード

scope eth-uplink/scope fabric a/port-channel/

コマンド履歴

リリース	変更内容
2.4.1(1)	コマンドが追加されました。

使用上のガイドライン

指定するインターフェイス速度はインターフェイスで使用するデュプレックス モードに影響を与えます。このため、デュプレックス モードを設定する前に速度を設定する必要があります。速度を 10 または 100 Mbps に指定すると、ポートでは半二重モードを使用するように自動的に設定されますが、全二重モードを指定することもできます。1000 Mbps（1 Gbps）以上の速度に設定すると、自動的に全二重モードが使用されます。

例

次の例は、インターフェイスの速度を設定する方法を示しています。

```
firepower-9300 # scope eth-uplink
firepower-9300 /eth-uplink # scope fabric a
firepower-9300 /eth-uplink/fabric # create port-channel id
firepower-9300 /eth-uplink/fabric/port-channel* # enable
firepower-9300 /eth-uplink/fabric/port-channel* # set speed
firepower-9300 /eth-uplink/fabric/port-channel* # set speed 1gbps
firepower-9300 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

関連コマンド

コマンド	説明
duplex	デュプレックス モードを全二重または半二重に指定します。
show interface	インターフェイス ステータスを表示します。速度パラメータもあわせて表示します。

set speed (aggr-interface)

インターフェイスの速度を設定するには、**set speed** コマンドを使用します。

set speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

構文の説明

10mbps	（任意）速度を 10 Mbps に設定します。
100mbps	（任意）速度を 100 Mbps に設定します。
1gbps	（任意）速度を 1 Gbps に設定します。
10gbps	（任意）速度を 10 Gbps に設定します。
40gbps	（任意）速度を 40 Gbps に設定します。
100gbps	（任意）速度を 100 Gbps に設定します。

コマンド モード

scope eth-uplink/scope fabric a/port-channel/

コマンド履歴

リリース	変更内容
2.4.1(1)	コマンドが追加されました。

使用上のガイドライン

指定するインターフェイス速度はインターフェイスで使用するデュプレックス モードに影響を与えます。このため、デュプレックス モードを設定する前に速度を設定する必要があります。速度を 10 または 100 Mbps に指定すると、ポートでは半二重モードを使用するように自動的に設定されますが、全二重モードを指定することもできます。1000 Mbps（1 Gbps）以上の速度に設定すると、自動的に全二重モードが使用されます。

次の例は、インターフェイスの速度を設定する方法を示しています。

```
firepower-9300* # scope cabling
firepower-9300 /cabling* # scope fabric a
firepower-9300 /cabling/fabric* # create breakout port breakout 2 1
firepower-9300 /cabling/fabric* # show config
 scope fabric a
+    enter breakout 2 3
+    exit
 exit
firepower-9300 /cabling/fabric* # exit
firepower-9300 /cabling* # exit
firepower-9300* # scope eth-uplink
firepower-9300 /eth-uplink* # scope fabric a
firepower-9300 /eth-uplink/fabric* # show

Fabric:
    Fabric ID
    ---------
    A
firepower-9300 /eth-uplink/fabric* # show
```

```
  <CR>
  >               Redirect it to a file
  >>              Redirect it to a file in append mode
  aggr-interface  Aggregate Interface
  detail          Detail
  event           Event Management
  expand          Expand
  fault           Fault
  fsm             Fsm
  interface       Interface
  port-channel    Port Channel
  stats           statistics
  |               Pipe command output to filter

firepower-9300 /eth-uplink/fabric* # show aggr-interface expand
firepower-9300 /eth-uplink/fabric* # show aggr-interface
  1-4     Slot
  <CR>
  >       Redirect it to a file
  >>      Redirect it to a file in append mode
  detail  Detail
  expand  Expand
  n/n     Ethernet<Slot Id>/<Aggregate Port Id>
  |       Pipe command output to filter
firepower-9300 /eth-uplink/fabric* # show aggr-interface expand
firepower-9300 /eth-uplink/fabric* #
  acknowledge  Acknowledge
  create       Create managed objects
  delete       Delete managed objects
  enter        Enters a managed object
  scope        Changes the current mode
  show         Show system information

firepower-9300 /eth-uplink/fabric* # scope aggr-interface
  1-4  Slot
  n/n  Ethernet<Slot Id>/<Aggregate Port Id>

firepower-9300 /eth-uplink/fabric* # scope port-channel 2
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface* # create member-port
Ethernet2/1/1
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* # show config
+enter member-port 2 1
+exit
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* # exit
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface* # exit
firepower-9300 /eth-uplink/fabric/port-channel* # show config
 enter port-channel 2
     enable
+    enter aggr-interface 2 1
+        enter member-port 2 1
+        exit
+    exit
     enter member-port 1 6
         enable
     exit
     set auto-negotiation no
     set descr ""
     set duplex fullduplex
     set flow-control-policy default
     set lacp-policy-name default
     set nw-ctrl-policy default
     set port-channel-mode active
     set port-type data
     set speed 1gbps
```

```
 exit
firepower-9300 /eth-uplink/fabric/port-channel* # set speed
  100gbps  100 Gbps
  100mbps  100 Mbps
  10gbps   10 Gbps
  10mbps   10 Mbps
  1gbps    1 Gbps
  40gbps   40 Gbps

firepower-9300 /eth-uplink/fabric/port-channel* # set speed 1gbps
firepower-9300 /eth-uplink/fabric/port-channel* commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

関連コマンド

コマンド	説明
duplex	デュプレックス モードを全二重または半二重に指定します。
show interface	インターフェイス ステータスを表示します。速度パラメータもあわせて表示します。

set ssh-server

SSH ホスト キーのサイズを設定するには、**set ssh-server** コマンドを使用します。

set ssh-server host-key rsa *key_size*

構文の説明

rsa	ホスト キーのタイプを指定します。
key-size	ホスト キーのサイズ。

コマンド モード

サービス モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、SSH ホスト キーのサイズを設定します。

例

次の例は、SSH ホスト キーのサイズを 2048 ビットに設定する方法を示しています。

```
FP9300-A # scope system
FP9300-A /system # scope services
FP9300-A /system/services # set ssh-server host-key rsa 2048
FP9300-A /system/services* # commit-buffer
FP9300-A /system/services #
```

関連コマンド

コマンド	説明
create ssh-server	新しい SSH サーバのホスト キーを作成します。
delete ssh-server	既存の SSH ホスト キーを削除します。
show ssh-server	ホスト キーのサイズを表示します。

set sshkey

パスワードなしのアクセスを許可する SSH キーを指定するには、**set sshkey** コマンドを使用します。

set sshkey ［**none** | *user_ssh_key*］

構文の説明

none	（任意）ユーザの SSH 公開キーをクリアするには、**none** キーワードを入力します。
user_ssh_key	（任意）ユーザの SSH 公開キーを入力または貼り付けます。

コマンド モード

ローカル ユーザ モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

set sshkey の入力後に **Enter** キーを押すと、SSH キーを 1 行ずつ入力するようにプロンプトが表示されます。完了するには、ENDOFBUF と入力します。中止するには、Ctrl-C キーを押します。

例

次の例は、現在のローカル ユーザの SSH 公開キーを指定する方法を示しています。

```
FP9300-A /security/local-user # set sshkey
"ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw85lkdQqap+NFuNmHcb4K

iaQB8X/PDdmtlxQQcawclj+k8f4VcOelBxlsGk5luq5ls1ob1VOIEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpD
 m8HPh2LOgyH7Ei1MI8="
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

関連コマンド

コマンド	説明
create local-user	新規のローカル ユーザ アカウントを作成します。
set password	ユーザ アカウントのパスワードを指定します。

set startup-version

アプリケーションのスタートアップバージョンを指定するには、 **set startup-version** コマンドを使用します。

set startup-version

構文の説明

startup-version	アプリケーションインスタンスのスタートアップ ソフトウェア バージョン

コマンド モード

scope ssa

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

scope app-instance ftd ftd1 の後に **Enter** キーを押すと、スタートアップバージョンを設定するように求められます。

例

次の例は、FTD アプリケーションのスタートアップバージョンを設定する方法を示しています。

```
FPR# scope ssa
FPR /ssa # scope slot 1
FPR /ssa/slot # scope app-instance ftd ftd1
FPR /ssa/slot/app-instance # set startup-version 6.6.1.91
Warning: Upgrade of ftd through FXOS is not supported. The specified version of ftd
will be installed. Please reinitialize or reinstall ftd.
```

set timezone

FXOS でタイムゾーンを設定するには、 **set timezone** コマンドを使用します。

set timezone

構文の説明		
	set timezone	コマンド set timezone を使用して、FXOS のタイムゾーンを設定します。

コマンド モード

scope system/scope services

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、FXOS のタイムゾーンを設定します。

例

次の例は、FXOS でタイムゾーンを設定する方法を示しています。

```
firepower# scope system
firepower /system# scope services
firepower /system/services # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean


#? 8 <====== Europe


Please select a country.
 1) Aaland Islands        18) Greece               35) Norway
 2) Albania               19) Guernsey             36) Poland
 3) Andorra               20) Hungary              37) Portugal
 4) Austria               21) Ireland              38) Romania
 5) Belarus               22) Isle of Man          39) Russia
 6) Belgium               23) Italy                40) San Marino
 7) Bosnia & Herzegovina  24) Jersey               41) Serbia
 8) Britain (UK)          25) Latvia               42) Slovakia
 9) Bulgaria              26) Liechtenstein        43) Slovenia
10) Croatia               27) Lithuania            44) Spain
11) Czech Republic        28) Luxembourg           45) Sweden
12) Denmark               29) Macedonia            46) Switzerland
13) Estonia               30) Malta                47) Turkey
14) Finland               31) Moldova              48) Ukraine
15) France                32) Monaco               49) Vatican City
16) Germany               33) Montenegro
17) Gibraltar             34) Netherlands

#? 36 <======Poland
```

```
The following information has been given:

        Poland

Therefore timezone 'Europe/Warsaw' will be set.
Local time is now:      Sun Oct 24 08:51:04 CEST 2021.
Universal Time is now:  Sun Oct 24 06:51:04 UTC 2021.
Is the above information OK?
1) Yes
2) No


#? 1 <======== Yes

firepower /system/services* # commit
firepower /system/services # show timezone
Timezone: Europe/Warsaw <======= Timezone is set

To set the timezone to UTC:

firepower /system/services* # set timezone UTC
firepower /system/services* # commit
```

set trustpoint

キーリングの証明書トラストポイントを指定するには、**set trustpoint** コマンドを使用します。

set trustpoint *trustpoint_name*

構文の説明

trustpoint_name	定義されたトラストポイントの名前。 この名前には、1 ～ 32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。

コマンド モード

scope security/scope keyring/

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、このキーリングの証明書に署名したトラストポイントを指定します。

例

次に、デフォルトのキーリング内のキーを再生成する例を示します。

```
firepower# scope security
firepower /security # scope keyring test-ring
firepower /security/keyring # set trustpoint CiscoCA5
firepower /security/keyring* # commit-buffer
firepower /security/keyring #
```

コマンド	説明
set cert	キー リングの RSA 証明書を入力します。
set modulus	RSA キー係数（SSL キーの長さ）をビット単位で指定します。
set regenerate	デフォルト キー リングで RSA キーを再生成します。

set use-2-factor

認証レルムの二要素認証を有効または無効にするには、**set use-2-factor** コマンドを使用します。

（注） 二要素認証は、RADIUS および TACACS+ レルムにのみ適用されます。

set use-2-factor {**no** | **yes**}

構文の説明

no	レルムの二要素認証を無効にします。
yes	レルムの二要素認証を有効にします。

コマンド モード

デフォルト認証モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

RADIUS または TACACS+ レルムに二要素認証を設定する場合は、リモート ユーザが頻繁に再認証する必要がないよう、セッションの更新時間およびセッションのタイムアウト時間を増やすことを検討してください。

例

次の例は、デフォルトの認証モードを開始し、二要素認証を有効にする方法を示しています。

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set use-2-factor yes
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

関連コマンド

コマンド	説明
set authentication	デフォルトの認証サービスを指定します。
set タイムアウト値	**set absolute-session-timeout**、**set con-absolute-session-timeout**、**set con-session-timeout**、および **set session-timeout** コマンドを使用してさまざまなタイムアウト値を設定します。

set user-account-unlock-time

ログイン試行の最高回数に達した後、ユーザがシステムからロックアウトされる時間を指定するには、**set user-account-unlock-time** コマンドを使用します。

set user-account-unlock-time *unlock_time*

構文の説明

unlock_time	ユーザがシステムからロックアウトされた状態を維持する時間（秒単位）。値の範囲は600～36000です。デフォルト値は1800秒（30分）です。

コマンド モード

セキュリティ モード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

ユーザ（管理者ユーザを含む）が指定されたログイン試行最高回数を超えると、ユーザはシステムからロックアウトされるため、ログインが再び許可されるまで、この時間待機する必要があります。ユーザがロックアウトされたことを示す通知は表示されません。

例

次の例では、セキュリティ モードを開始し、ロックアウトされたユーザが再びログインできるまでに経過する時間を指定する方法を示します。

```
FP9300-A # scope security
FP9300-A /security # set user-account-unlock-time 900
FP9300-A /security* # commit-buffer
FP9300-A /security #
```

関連コマンド

コマンド	説明
clear lock-status	ユーザのロックアウト ステータスをクリアします。
set max-login-attempts	ユーザがシステムからロックアウトされるまで、ログイン試行を失敗できる回数を指定します。

set user-label

アプリケーション シャーシにユーザ定義識別子を割り当てるには、chassis/ モード **set user-label** コマンドを使用します。

インストール済みサーバのいずれかにユーザ定義識別子を割り当てるには、server/ モードで **set user-label** コマンドを使用します。

set user-label *user_label*

構文の説明

user_label	アプライアンスまたはサーバに割り当てるラベル。最大 32 文字。

コマンド モード

scope chassis/

scope chassis/scope server

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

chassis/ モードで **show detail** コマンドを使用すると、シャーシに現在割り当てられているユーザ ラベルを表示できます。

chassis/server/ モードで **show detail** コマンドを使用すると、接続されたサーバに現在割り当てられているユーザ ラベルを表示できます。

例

次の例は、アプライアンス シャーシにユーザ定義ラベルを割り当てる方法を示しています。

```
firepower # scope chassis 1
firepower /chassis # set user-label FP9300-4
firepower /chassis* # commit-buffer
firepower /chassis # show detail

Chassis:
    Chassis: 1
    User Label: FP9300-4
    Overall Status: Operable
    Oper qualifier: N/A
    Operability: Operable
    Conf State: Ok
    Admin State: Acknowledged
    Conn Path: A
    Conn Status: A
    Managing Instance: A
    Product Name: Cisco Firepower 9300 Security Appliance AC
    PID: FPR-C9300-AC
    VID: V02
    Part Number: 68-100280-04
    Vendor: Cisco Systems Inc
```

```
    Model: FPR-C9300-AC
    Serial (SN): JMX1950196H
    HW Revision: 0
    Mfg Date: 2015-12-16T00:00:00.000
    Power State: Ok
    Thermal Status: Ok
    SEEPROM operability status: Operable
    Dynamic Reallocation: Chassis
    Reserved Power Budget (W): 600
    PSU Capacity (W): 0
    PSU Line Mode: High Line
    PSU State: Ok
    Current Task:
firepower /chassis #
```

関連コマンド

コマンド	説明
show detail	`chassis/` モードでは、シャーシの現在のユーザ ラベルなど、詳細なシャーシ情報を表示します。 `chassis/server/` モードでは、接続サーバのユーザ ラベルなど、詳細なサーバ情報を表示します。

set value (create bootstrap-key FIREWALL_MODE)

Threat Defense と ASA のブートストラップ コンフィギュレーションでファイアウォール モードをルーテッドまたはトランスペアレントに指定するには、**set value** コマンドを指定します。

set value {**routed** | **transparent**}

構文の説明

routed	ファイアウォール モードをルーテッド ファイアウォール モードに設定します。
transparent	ファイアウォール モードをトランスペアレント ファイアウォールに設定します。

コマンド モード

scope ssa/create logical-device/create mgmt-bootstrap/create bootstrap-key FIREWALL_MODE/

コマンド デフォルト

デフォルト モードはルーテッドです。

コマンド履歴

リリース	変更内容
2.4(1)	ASA のサポートが追加されました。
1.1(4)	FTD に対してコマンドが追加されました。

使用上のガイドライン

ブートストラップの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、アプリケーション CLI の設定でほとんどの値を変更できます。

例

次に、モードをルーテッドに設定する例を示します。

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

関連コマンド

コマンド	説明
create bootstrap-key FIREWALL_MODE	アプリケーションのファイアウォール モードを設定します。
create logical-device	論理デバイスを作成します。

コマンド	説明
create mgmt-bootstrap	アプリケーションのブートストラップコンフィギュレーションを作成します。

set value (create bootstrap-key MANAGEMENT_TYPE)

Threat Defense のブートストラップ設定でマネージャ（FMC または FDM）を指定するには、**set value** コマンドを使用します。

set value {**FMC** | **LOCALLY_MANAGED**}

構文の説明

FMC	マネージャを FDM に設定します。
LOCALLY_MANAGED	マネージャを FMC に設定します。

コマンド モード

scope ssa/create logical-device/create mgmt-bootstrap/create bootstrap-key LOCALLY_MANAGED/

コマンド デフォルト

デフォルトのマネージャは FMC です。

コマンド履歴

リリース	変更内容
2.7(1)	FTD に対してコマンドが追加されました。

使用上のガイドライン

ブートストラップの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、アプリケーション CLI の設定でほとんどの値を変更できます。

例

次の例は、マネージャを FDM に設定する方法を示しています。

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key MANAGEMENT_TYPE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value LOCALLY_MANAGED
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

関連コマンド

コマンド	説明
create bootstrap-key FIREWALL_MODE	アプリケーションのファイアウォール モードを設定します。
create logical-device	論理デバイスを作成します。
create mgmt-bootstrap	アプリケーションのブートストラップ コンフィギュレーションを作成します。

set value (create bootstrap-key PERMIT_EXPERT_MODE)

Threat Defense の FTD SSH セッションでエキスパート モードを許可するには、 **set value** コマンドを使用します。

set value {**yes** | **no**}

構文の説明

no	SSH セッションから Threat Defense へのエキスパート モードを禁止します。
yes	SSH セッションから Threat Defense へのエキスパート モードを許可します。

コマンド モード

scope ssa/create logical-device/create mgmt-bootstrap/create bootstrap-key PERMIT_EXPERT_MODE/

コマンド デフォルト

デフォルトは no です。

コマンド履歴

リリース	変更内容
2.4(1)	コマンドが追加されました。

使用上のガイドライン

エキスパート モードでは、高度なトラブルシューティングに FTD シェルからアクセスできます。デフォルトでは、コンテナ インスタンスの場合、エキスパート モードを使用できるのは FXOS CLI から FTD CLI にアクセスするユーザだけです。この制限は、インスタンス間の分離を増やす場合、コンテナインスタンスのみに適用されます。マニュアルの手順で求められた場合、または Cisco Technical Assistance Center から求められた場合のみ、エキスパート モードを使用します。このモードを開始するには、FTD CLI で expert コマンドを使用します。

例

次に、SSH でエキスパート モードを有効にする例を示します。

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key PERMIT_EXPERT_MODE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value yes
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

関連コマンド

コマンド	説明
create bootstrap-key FIREWALL_MODE	アプリケーションのファイアウォール モードを設定します。

コマンド	説明
create logical-device	論理デバイスを作成します。
create mgmt-bootstrap	アプリケーションのブートストラップ コンフィギュレーションを作成します。

set vlan

コンテナ インスタンスで使用するサブインターフェイスの VLAN ID を設定するには、**set vlan** コマンドを使用します。

set vlan *id*

構文の説明

id	1 ～ 4095 の間で VLAN ID を設定します。

コマンド モード

scope eth-uplink/scope fabric a/scope interface/create subinterface/

scope eth-uplink/scope fabric a/create port-channel/create subinterface/

コマンド履歴

リリース	変更内容
2.4(1)	コマンドが追加されました。

使用上のガイドライン

ネットワーク配置に応じて、250 ～ 500 の VLAN サブインターフェイスをシャーシに追加できます。

インターフェイスごとの VLAN ID は一意である必要があります。コンテナ インスタンス内では、VLAN ID は割り当てられたすべてのインターフェイス全体で一意である必要があります。異なるコンテナ インターフェイスに割り当てられている限り、VLAN ID を別のインターフェイス上で再利用できます。ただし、同じ ID を使用していても、各サブインターフェイスが制限のカウント対象になります。

例

次に、イーサネット 1/1 上の 3 つのサブインターフェイスを作成し、データ共有インターフェイスに設定する例を示します。

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # scope interface Ethernet1/1
firepower /eth-uplink/fabric/interface # create subinterface 10
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 10
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # create subinterface 11
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 11
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # create subinterface 12
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 12
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
firepower /eth-uplink/fabric/interface/subinterface #
```

関連コマンド

コマンド	説明
create port-channel	EtherChannel（ポート チャネル）を作成します。
create subinterface	サブインターフェイスを追加します。
scope interface	物理インターフェイス オブジェクトを入力します。
set port-type	インターフェイス タイプを設定します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。