

# ISEサーバを使用したUCS ManagerでのTACACS+認証ドメインの設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[コンフィギュレーション](#)

[ISEでのTACACS+の設定](#)

[ISEでのTACACS+の設定](#)

[ISEでの属性とルールの設定](#)

[UCSMでのTACACS+の設定](#)

[ユーザのロールの作成](#)

[TACACS+プロバイダーの作成](#)

[TACAC+プロバイダーグループの作成](#)

[認証ドメインの作成](#)

[トラブルシュート](#)

[UCSMでの一般的なTACACS+の問題](#)

[UCSMレビュー](#)

[ISEでの一般的なTACACの問題](#)

[ISEのレビュー](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、Unified Compute System Manager(UCSM)でのTerminal Access Controller Access-Control System Plus(TACACS+)認証の設定について説明します。 TACACS+は、認証、許可、およびアカウンタビリティサービス(AAA)に使用されるネットワークプロトコルで、サーバを介してルールを管理および作成できるネットワークアクセステバイス(NAD)を管理するための集中方式を提供します。この使用例では、Identity Services Engine(ISE)を使用します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco UCS Manager(UCSM)
- Terminal Access Controller Access-Control System Plus(TACACS+)
- Identity Services Engine ( ISE )

## 使用するコンポーネント

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

- UCSM 4.2(3d)
- Cisco Identity Services Engine(ISE)バージョン3.2

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

## コンフィギュレーション

### ISEでのTACACS+の設定

#### ISEでのTACACS+の設定

ステップ 1：最初の作業は、ISEにTACACS+認証を処理する正しい機能があるかどうかを確認することです。このような場合、ポリシーサービスノード(PSN)内にDevice Admin Serviceの機能が必要かどうかを確認し、メニューAdministration > System > Deploymentを参照して、ISEがTACACS+を実行するノードを選択し、Editボタンを選択します。



The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes links for Cisco ISE, Evaluation Mode 90 Days, and various system management options. The main menu has tabs for Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, and Settings. The 'Deployment' tab is selected. On the left, a sidebar shows a tree view with 'Deployment' expanded, and 'PAN Failover' listed under it. The main content area is titled 'Deployment Nodes'. It displays a table with one row for 'Ise32'. The columns are 'Hostname' (Ise32), 'Personas' (Administration, Monitoring, Policy Service), 'Role(s)' (STANDALONE), 'Services' (SESSION, PROFILER), and 'Node Status' (green checkmark). Below the table, there are buttons for 'Edit', 'Register', 'Syncup', and 'Deregister'. A status bar at the bottom indicates 'Selected 0 Total 1'.

ステップ 2 Device Administration Serviceという対応する機能が表示されるまで下にスクロールします（この機能を有効にするには、まずポリシーサーバのペルソナをノードで有効にし、さらにTACACS+のライセンスを展開環境で有効にする必要があります）。このチェックボックスをオンにして、設定を保存します。

The screenshot shows the 'Administration - System' section of the Cisco ISE web interface. A node named 'Other Monitoring Node' is selected. Under 'Policy Service', 'Enable Session Services' is checked. In the 'Include Node in Node Group' dropdown, 'None' is selected. Under 'Enable Profiling Service', 'Enable Threat Centric NAC Service' is checked. A 'Personas' tab is visible. The 'Enable Device Admin Service' checkbox is highlighted with a red box. Other options like 'Enable SXP Service' and 'Enable Passive Identity Service' are present but not checked. At the bottom right, there are 'Reset' and 'Save' buttons, with 'Save' being highlighted with a red box.

ステップ3 ISEをTACACS+としてサーバとして使用するNetwork Access Device(NAD)を設定し、Administration > Network Resources > Network Devicesの順にメニューに移動して、+Addボタンを選択します。

The screenshot shows the 'Administration - Network Resources' section with the 'Network Devices' tab selected. The main area displays a table with columns: Name, IP/Mask, Profile Name, Location, Type, and Description. A message 'No data available' is shown. At the top of the table, there are several buttons: Edit, + Add (highlighted with a red box), Duplicate, Import, Export, Generate PAC, and Delete. On the left sidebar, there are links for Network Devices, Default Device, and Device Security Settings.

ステップ4このセクションでは、次のように設定します。

- TACACS+クライアントにするUCSMの名前。
- UCSMがISEに要求を送信するために使用するIPアドレス。
- TACACS+ Shared Secret。これは、UCSMとISE間のパケットの暗号化に使用されるパスワードです。

Network Devices    Network Device Groups    Network Device Profiles    External RADIUS Servers    RADIUS Server Sequences    NAC Managers    External MDM    pxGrid Direct Connectors    Location Services

Network Devices

Default Device

Device Security Settings

Network Devices List > USCM

Network Devices

Name	USCM
Description	
IP Address	* IP: 10.31.123.9 / 32
IP Address	* IP: 10.31.123.8 / 32

Device Profile: Cisco

Model Name:

Software Version:

Network Device Group

Location: All Locations

IPSEC: No

Device Type: All Device Types

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret: ..... Show Retire

Enable Single Connect Mode

Legacy Cisco Device



注：クラスタ構成の場合は、両方のFabric Interconnectに管理ポートのIPアドレスを追加します。この設定により、1番目のFabric Interconnectに障害が発生してシステムが2番目のFabric Interconnectにフェールオーバーした場合に、リモートユーザが引き続きログインできることが保証されます。すべてのログイン要求はこれらのIPアドレスから送信され、Cisco UCS Managerで使用される仮想IPアドレスからは送信されません。

## ISEでの属性とルールの設定

ステップ1：TACACS+プロファイルを作成し、メニューWork Centers > Device Administration > Policy Elements > Results > TACACS Profilesに移動して、Addを選択します。

Cisco ISE

Work Centers - Device Administration

Overview    Identities    User Identity Groups    Ext Id Sources    Network Resources    Policy Elements    Device Admin Policy Sets    Reports    Settings

Conditions    >

Network Conditions    >

Results    >

Allowed Protocols

TACACS Command Sets

TACACS Profiles

TACACS Profiles

Add    Duplicate    Trash    Edit

Name	Type	Description
Default Shell Profile	Shell	Default Shell Profile

Rows/Page: 5

ステップ2このセクションでは、プロファイルを名前で設定し、Custom AttributesセクションでAddを選択し、次に特性MANDATORYの1つの属性を作成し、cisco-av-pairと名前を付け、値でUCSM内で使用可能なロールの1つを選択してシェルロールとして入力します。この例ではロール

adminを使用しており、入力はshell:roles="admin"である必要があります。

Cisco ISE

Work Centers - Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

Conditions > Name UCSM PROFILE ADMIN

Network Conditions >

Results > Description

Allowed Protocols

TACACS Command Sets

TACACS Profiles

Task Attribute View Raw View

Common Tasks

Common Task Type Shell

Default Privilege (Select 0 to 15)

Maximum Privilege (Select 0 to 15)

Access Control List

Auto Command

No Escape (Select true or false)

Timeout Minutes (0-9999)

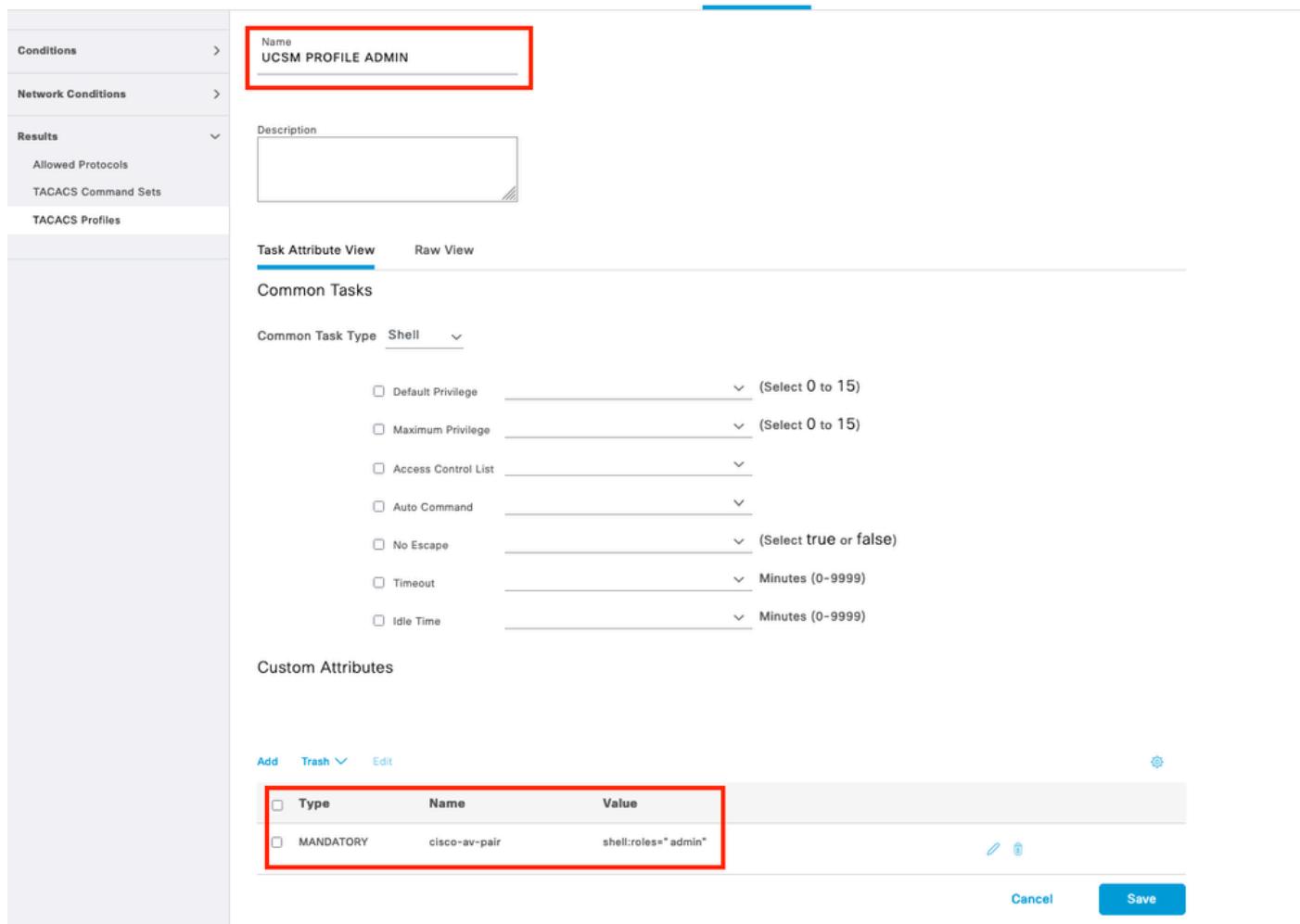
Idle Time Minutes (0-9999)

Custom Attributes

Add Trash Edit

Type	Name	Value
MANDATORY	cisco-av-pair	shell:roles="admin"

Cancel Save



同じメニューで、TACACSプロファイルに対してRaw Viewを選択すると、ISEを介して送信される属性の対応する設定を確認できます。

Cisco ISE

Work Centers - Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

Conditions > TACACS Profiles > UCSM PROFILE ADMIN

Network Conditions >

Results > Name UCSM PROFILE ADMIN

Allowed Protocols

TACACS Command Sets

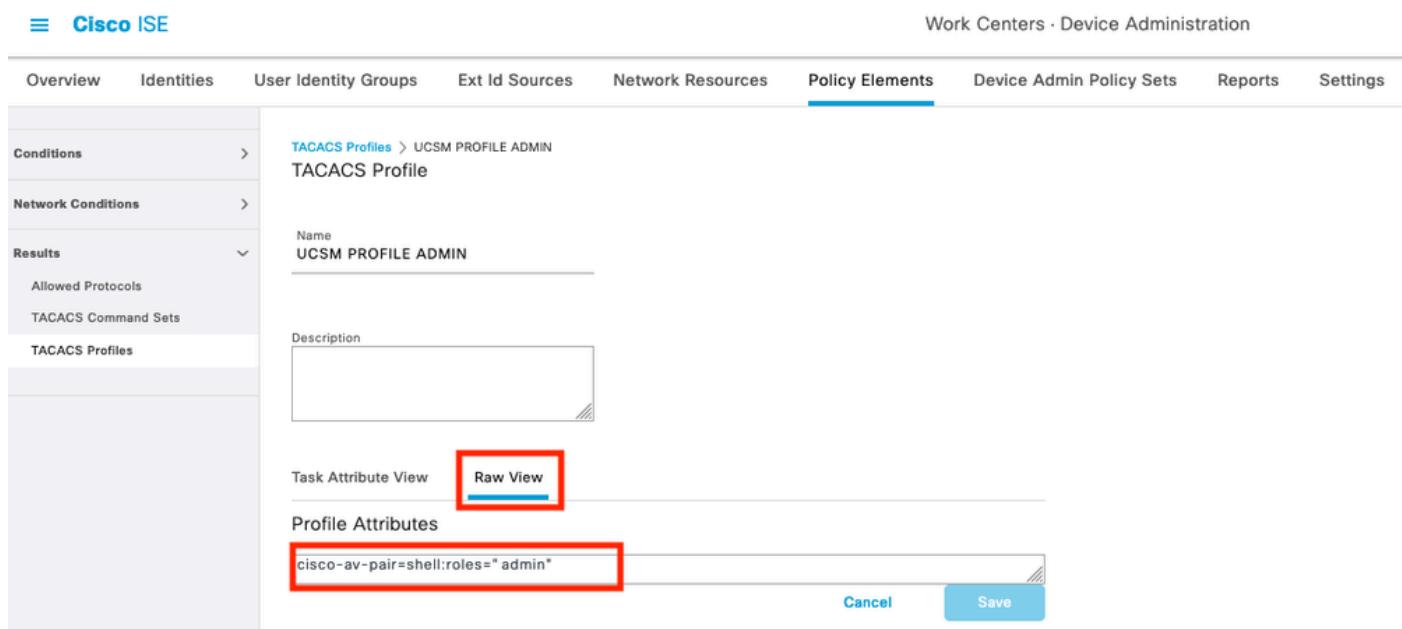
TACACS Profiles

Task Attribute View Raw View

Profile Attributes

cisco-av-pair=shell:roles="admin"

Cancel Save





注:cisco-av-pair nameは、TACACS+プロバイダーの属性IDを提供する文字列です。

ステップ3 チェックマークを選択して、設定を保存します。

ステップ4 UCSMで使用するデバイス管理ポリシーセットを作成し、メニューWork Centers > Device Administration > Device Admin Policy Setsに移動し、既存のポリシーセットから歯車アイコンを選択してInsert new rowを選択します

The screenshot shows the Cisco ISE Device Admin Policy Sets page. A new policy set named 'Tacacs Default policy set' has been created. The 'Default Device Admin' section is visible, with a button labeled 'Insert new now above' highlighted.

ステップ5 この新しいポリシーセットに名前を付け、UCSMサーバから実行されているTACACS+認証の特性に応じて条件を追加し、Allowed Protocols > Default Device Adminの順に選択して、設定を保存します。

The screenshot shows the Cisco ISE Device Admin Policy Sets page. A condition 'DEVICE Device Type EQUALS All Device Types' has been added to the 'USCM ACCESS' policy set. The 'Default Device Admin' section is visible, with a button labeled 'Insert new now above' highlighted.

ステップ6 >表示オプションで選択し、Authentication Policyセクションで、ISEがUCSMに入力されるユーザ名とクレデンシャルを照会する外部アイデンティティソースを選択します。この例では、クレデンシャルはISE内に保存されている内部ユーザに対応します。

The screenshot shows the Cisco ISE Authentication Policy configuration page. It displays an authentication rule for 'USCM ACCESS' with a condition 'DEVICE Device Type EQUALS All Device Types'. In the 'Options' section, a red box highlights the 'Internal Users' dropdown menu, which is currently set to 'Internal Users'.

ステップ7 Authorization Policyというセクションまでスクロールダウンして、Default policyまでスクロールし、歯車のアイコンを選択して、ルールを1つ挿入します。

ステップ8 新しい認可ルールに名前を付け、グループメンバーシップとして認証済みのユーザに

関する条件を追加します。次に、Shell Profilesセクションで、以前に設定したTACACSプロファイルを保存します。

The screenshot shows the 'Authorization Policy (2)' configuration screen. A new rule is being added for 'USCM ADMIN'. The 'Conditions' section contains a condition 'InternalUser IdentityGroup EQUALS User Identity Groups:Employee'. The 'Actions' section includes 'UCSM PROFILE ADMIN' and 'DenyAllCommands'. The 'Results' section lists 'Deny All Shell Profile'. The 'Save' button at the bottom right is highlighted with a red box.

## UCSMでのTACACS+の設定

管理者権限を持つユーザでCisco UCS Manager GUIにログインします。

### ユーザのロールの作成

ステップ1：ナビゲーションペインで Admin タブを選択します。

ステップ2 Adminタブで、All > User Management > User Services > Roles の順に展開します。

ステップ3 作業ペインで、General tabを選択します。

ステップ4 カスタムロールの場合は、Addを選択します。このサンプルでは、デフォルトのロールを使用します。

ステップ5 名前のロールが、TACACSプロファイルで前に設定した名前と一致することを確認します。

The screenshot shows the 'User Services - Roles' page. The 'Roles' tab is selected. A list of roles is displayed, including 'aaa', 'admin', 'facility-manager', 'network', 'operations', 'read-only', 'read-onlyTest', 'server-compute', 'server-equipment', 'server-profile', 'server-security', 'stats', and 'storage'. The 'Add' button at the bottom is highlighted with a red box.

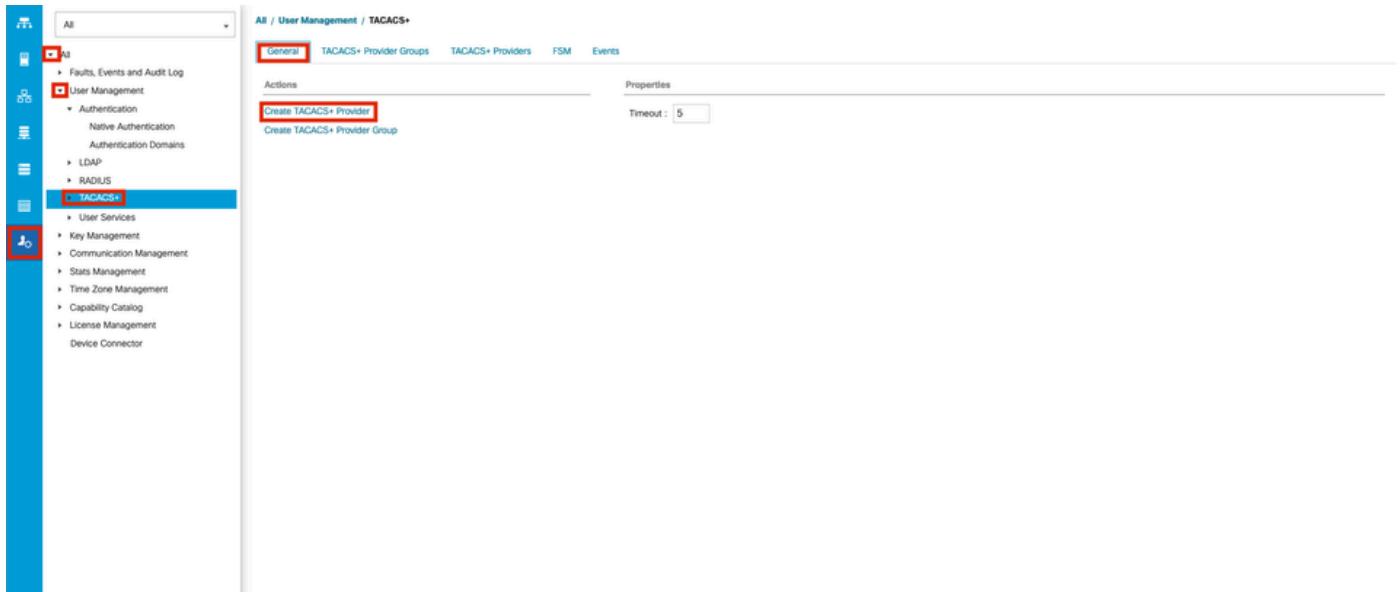
### TACACS+プロバイダーの作成

ステップ1：ナビゲーションペインで Admin タブを選択します。

ステップ2 Adminタブで、All > User Management > TACACS+ の順に展開します。

ステップ3 作業ペインで、Generalタブを選択します。

ステップ4 Actionsで、Create TACACS+ Providerを選択します。



ステップ5 Create TACACS+ Providerwizardに、適切な情報を入力します。

- Hostnameフィールドに、TACACS+サーバのIPアドレスまたはホスト名を入力します。
- Orderフィールドで、Cisco UCSがユーザの認証にこのプロバイダーを使用する順序。

1 ~ 16の整数を入力するか、このCisco UCSインスタンスで定義されている他のプロバイダーに基づいてCisco UCSで次に使用可能な順序を割り当てる場合は、使用可能な最小値または0(ゼロ)を入力します。

- Keyフィールドに、データベースのSSL暗号化キーを入力します。
- Confirm Keyフィールドで、確認のためにSSL暗号キーを再入力します。
- Portフィールドで、Cisco UCSがTACACS+データベースと通信するために使用するポート(ポート49のデフォルトポート)。
- Timeoutフィールドには、タイムアウトが発生する前にTACACS+データベースへの問い合わせが試行される時間(秒単位)です。

Create TACACS+ Provider

Hostname/FQDN (or IP Address) :

Order :

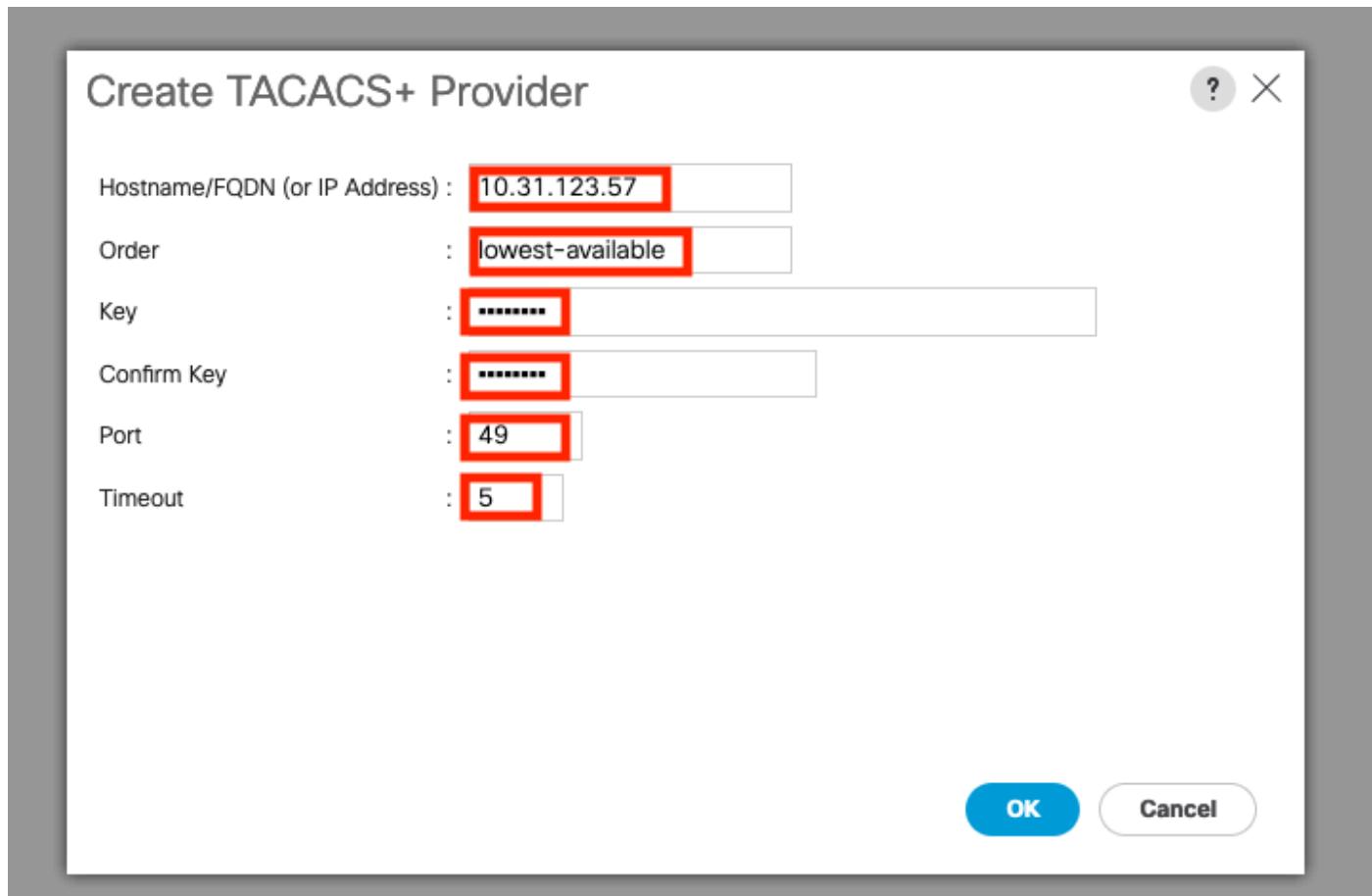
Key :

Confirm Key :

Port :

Timeout :

**OK** **Cancel**



ステップ 6 Okを選択します。



注:IPアドレスではなくホスト名を使用する場合、Cisco UCS ManagerでDNSサーバを設定する必要があります。

#### TACAC+プロバイダーグループの作成

ステップ1：ナビゲーションペインでAdminタブを選択します。

ステップ2 Admintabで、All > User Management > TACACS+の順に展開します。

ステップ3 作業ペインでGeneralタブを選択します。

ステップ4 Actionsaで、Create TACACS+ ProviderGroupを選択します。

The screenshot shows the Juniper Network Manager interface. On the left, there's a navigation tree with various service icons. The 'TACACS+' icon is highlighted with a red box. The main pane shows the 'User Management / TACACS+' section. A red box highlights the 'General' tab. Below it, under 'Actions', two options are listed: 'Create TACACS+ Provider' and 'Create TACACS+ Provider Group'. A red box highlights the 'Create TACACS+ Provider Group' option.

ステップ 5 Create TACACS+ Provider Groupダイアログボックスで、必要な情報を入力します。

- Name フィールドに、グループの一意の名前を入力します。
- TACACS+ Providers テーブルで、グループに含めるプロバイダーを選択します。
- >> ボタンを選択して、含まれるプロバイダーの表にプロバイダーを追加します。

The dialog box is titled 'Create TACACS+ Provider Group'. It has a 'Name' field containing 'TACACSGr' with a red box around it. To the right are two tables: 'TACACS+ Providers' and 'Included Providers'. The 'TACACS+ Providers' table shows a row with 'Hostname' '10.31.123.57' and 'Port' '49', also with a red box around it. A red box highlights the '>>' button between the provider and included provider tables. The 'Included Providers' table currently shows 'No data available'. At the bottom are 'OK' and 'Cancel' buttons, with 'OK' highlighted by a red box.

ステップ 6 Okを選択します。

## 認証ドメインの作成

ステップ1：ナビゲーションペインで Admin タブを選択します。

ステップ2 Adminタブで、All > User Management > Authentication の順に展開します

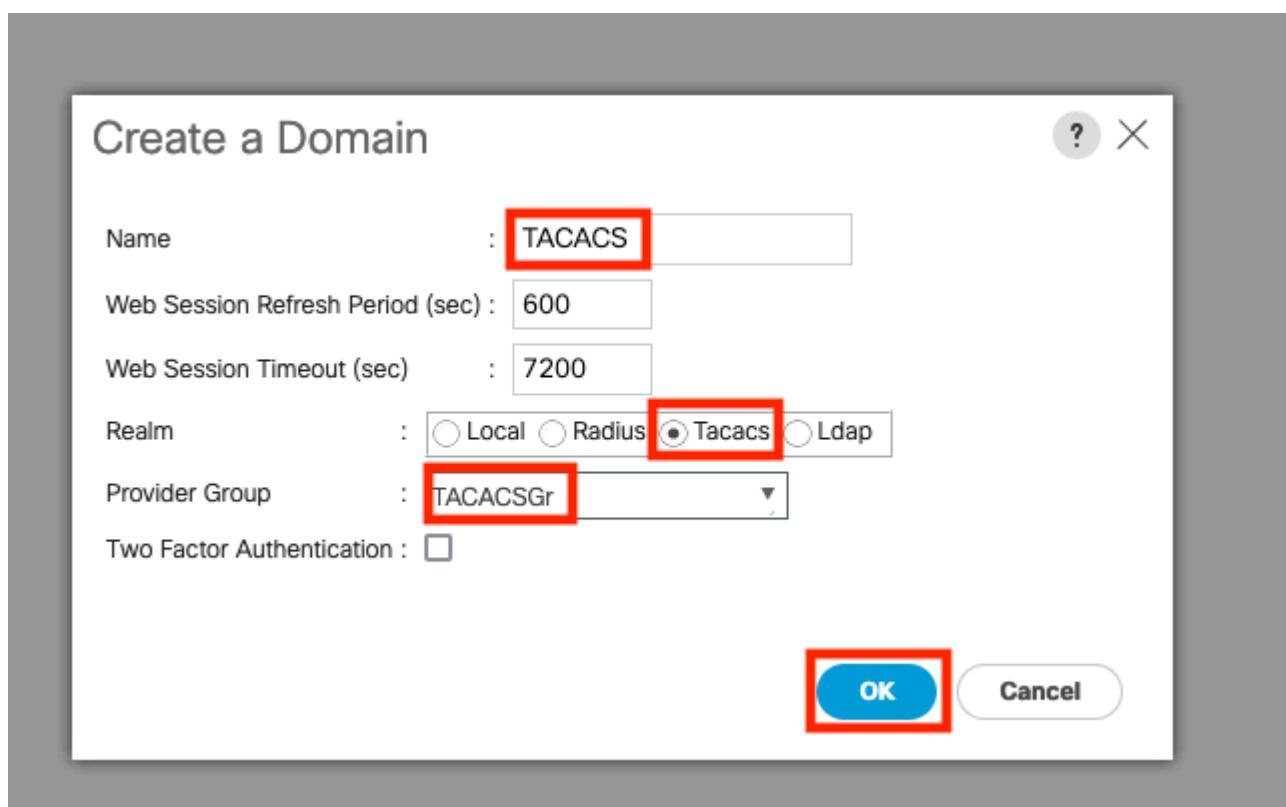
ステップ3 作業ペインで General タブを選択します。

ステップ4 ActionAreaで、Create a Domain を選択します。



ステップ5 Create Domainダイアログボックスで、要求された情報を入力します。

- Name フィールドに、ドメインの一意の名前を入力します。
- Realm で、Tacacsオプションを選択します。
- Provider Group ドロップダウンリストから、先に作成したTACACS+プロバイダーグループを選択し、OKを選択します



## トラブルシュート

## UCSMでの一般的なTACACS+の問題

- キーが正しくないか、無効な文字です。
- ポートが正しくない。
- ファイアウォールまたはプロキシルールが原因で、プロバイダーとの通信が行われません。
- FSMは100 %ではありません。

UCSM TACACS+の設定を確認します。

有限状態マシン(FSM)のステータスをチェックする設定が、100 %完了としてUCSMに実装されていることを確認する必要があります。

UCSMコマンドラインから設定を確認する

```
<#root>

UCS-A#
scope security

UCS-A /security #
scope tacacs

UCS-A /security/tacacs #
show configuration
```

```
[UCS-AS-MXC-P25-02-A# scope security
[UCS-AS-MXC-P25-02-A /security # scope tacacs
[UCS-AS-MXC-P25-02-A /security/tacacs # show configuration
  scope tacacs
    enter auth-server-group TACACSGr
      enter server-ref 10.31.123.57
        set order 1
      exit
    exit
    enter server 10.31.123.57
      set order 1
      set port 49
      set timeout 5
    !
    !       set key
    exit
    set timeout 5
exit
```

```
<#root>
```

```
UCS-A /security/tacacs #
show fsm status
```

```
[UCS-AS-MXC-P25-02-A /security/tacacs # show fsm status
```

```
FSM 1:
  Status: Nop
  Previous Status: Update Ep Success
  Timestamp: 2023-06-24T20:54:05.021
  Try: 0
  Progress (%): 100
  Current Task:
```

NXOSからTACACS設定を確認します。

```
<#root>
UCS-A#
connect nxos

UCS-A(nx-os)#
show tacacs-server

UCS-A(nx-os)#
show tacacs-server groups
```

```
[UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, Cisco and/or its affiliates.
All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.

A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

[UCS-AS-MXC-P25-02-A(nx-os)# show tacacs-server
timeout value:5
deadtime value:0
source interface:any available
Global Test Username:test
Global Test Password:*****
total number of servers:1

following TACACS+ servers are configured:
  10.31.123.57:
    available on port:49
    TACACS+ shared secret:*****
    timeout:5

[UCS-AS-MXC-P25-02-A(nx-os)# show tacacs-server groups
total number of groups:2

following TACACS+ server groups are configured:
  group tacacs:
    server 10.31.123.57 on port 49
    deadtime is 0
    vrf is management
  group TACACSGr:
    server 10.31.123.57 on port 49
    deadtime is 0
    vrf is management
```

NX-OSから認証をテストするには、`test`コマンドを使用します（NXOSからのみ使用可能）。

サーバの設定を検証します。

```
<#root>

UCS-A(nx-os)#
test aaa server tacacs+
<TACACS+-server-IP-address or FQDN> <username> <password>
```

```
[UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, Cisco and/or its affiliates.
All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/libraryv.txt.

[UCS-AS-MXC-P25-02-A(nx-os)# test aaa server tacacs+ 10.31.123.57 operator Cisc0123
```

## UCSMレビュー

### 到達可能性の検証

```
<#root>

UCS-A#
connect local-mgmt

UCS-A(local-mgmt)#
ping
<TACACS+-server-IP-address or FQDN>
```

```
[UCS-AS-MXC-P25-02-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

[UCS-AS-MXC-P25-02-A(local-mgmt)# ping 10.31.123.57
PING 10.31.123.57 (10.31.123.57) from 10.31.123.8 : 56(84) bytes of data.
64 bytes from 10.31.123.57: icmp_seq=1 ttl=64 time=0.347 ms
64 bytes from 10.31.123.57: icmp_seq=2 ttl=64 time=0.309 ms
```

### ポートの検証

```
<#root>
UCS-A#
connect local-mgmt

UCS-A(local-mgmt)#
telnet
<TACACS+-server-IP-address or FQDN> <Port>
```

```
[UCS-AS-MXC-P25-02-A# connect local-mgmt]
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

[UCS-AS-MXC-P25-02-A(local-mgmt)# telnet 10.31.123.57 49]
Trying 10.31.123.57...
Connected to 10.31.123.57.
Escape character is '^]'.
```

エラーを確認する最も効果的な方法は、NXOSデバッグを有効にすることです。この出力では、グループ、接続、および誤通信を引き起こすエラーメッセージを確認できます。

- UCSMへのSSHセッションを開き、管理者権限を持つ任意の特権ユーザ（できればローカルユーザ）でログインし、NX-OS CLIコンテキストに変更して端末モニタを起動します。

```
<#root>
UCS-A#
connect nxos

UCS-A(nx-os)#
terminal monitor
```

- デバッグフラグを有効にし、ログファイルへのSSHセッション出力を確認します。

```
<#root>
UCS-A(nx-os)#
debug aaa all

UCS-A(nx-os)#

```

```

debug aaa aaa-request

UCS-A(nx-os)#
debug tacacs+ aaa-request

UCS-A(nx-os)#
debug tacacs+ aaa-request-lowlevel

UCS-A(nx-os)#
debug tacacs+ all

```

```

[UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, Cisco and/or its affiliates.
All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

[UCS-AS-MXC-P25-02-A(nx-os)# terminal monitor
[UCS-AS-MXC-P25-02-A(nx-os)# debug tacacs+ all
2023 Jun 26 04:42:22.104286 tacacs: event_loop(): calling process_rd_fd_set
2023 Jun 26 04:42:22.104311 tacacs: process_rd_fd_set: calling callback for fd 6
2023 Jun 26 04:42:22.104341 tacacs: fsrv didnt consume 182 opcode
2023 Jun 26 04:42:22.104994 tacacs: mts_message_handler: sdwrap_process_msg
2023 Jun 26 04:42:22.105011 tacacs: process_rd_fd_set: callback returned for fd 6
[UCS-AS-MXC-P25-02-A(nx-os)# debug aaa all]

```

- 次に、新しいGUIまたはCLIセッションを開き、リモートユーザ(TACACS+)としてログインします。
- ログイン失敗メッセージを受信したら、セッションを閉じるデバッグをオフにするか、このコマンドを使用します。

```
UCS-A(nx-os)# undebug all
```

## ISEでの一般的なTACACの問題

- ISEでは、UCSMがadminまたはその他のロールに対応するロールを割り当てるために必要な属性でTACACSプロファイルを設定する際に、この動作が表示されます。保存ボタンをク

リックすると、この動作が表示されます（次の図を参照）。

The screenshot shows the Cisco ISE interface under 'Work Centers - Device Administration'. In the 'Policy Elements' section, there is a 'TACACS Profiles' sub-section. A 'TACACS Profile' named 'UCSM Profile User' is selected. An 'Error' dialog box is displayed, stating 'You have entered an invalid character'. The 'OK' button is visible at the bottom right of the dialog.

このエラーは、次の不具合<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwc91917>（登録ユーザ専用）が原因で発生します。この不具合に対処できる場所を確認してください。

## ISEのレビュー

ステップ1：TACACS+サービスアビリティが実行されているかどうかを確認します。これは次のようにチェックインできます。

- GUI: Administration > System > Deploymentで、サービスDEVICE ADMINとともにノードが表示されているかどうかを確認します。
- CLI : コマンドshow ports | include 49を実行して、TACACS+に属するTCPポートに接続があることを確認します

<#root>

```
ise32/admin#
show ports | include 49
```

```
tcp: 169.254.4.1:49, 169.254.2.1:49, 169.254.4.1:49, 10.31.123.57:49
```

ステップ2 TACACS+認証試行に関して livelogsがあるかどうかを確認します。これは、Operations > TACACS > Live logsの順にメニューで確認できます。

障害の原因に応じて、設定を調整したり、障害の原因に対処したりできます。

The screenshot shows the Cisco ISE interface under 'Operations - TACACS'. The 'Live Logs' tab is selected. The table displays log entries for TACACS+ authentication attempts. The columns include Logged Time, Status, Details, Identity, Type, Authentication Policy, Authorization Policy, Ise Node, Network Device N, Network Device V, Device Type, Location, Device P., Failure Reason, and Remote Address. The first entry shows an 'INVALID' identity and a failure reason related to a subject not found in the application. The second and third entries show successful authentication attempts.

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device N	Network Device V	Device Type	Location	Device P.	Failure Reason	Remote Address
Jun 25, 2023 12:30:16.8...	●	○	INVALID	Authentic...	Default > Default	Authorization Policy	ise32	USCM	10.31.123.8	Device Type>All ...	Location>All Loc...		22056 Subject not found in the ap...	10.99.183.4
Jun 25, 2023 12:20:38.7...	●	○		Authentic...			ise32		10.31.123.9				13017 Received TACACS+ packet f...	
Jun 25, 2023 12:20:02.2...	●	○		Authentic...			ise32		10.31.123.9				13017 Received TACACS+ packet f...	

ステップ3livelogが表示されない場合は、パケットキャプチャを実行し、Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dumpの順にメニューに移動し、on addを選択します。

The screenshot shows the Cisco ISE Operations - Troubleshoot interface. In the left sidebar, under Diagnostic Tools, 'TCP Dump' is selected. The main area is titled 'TCP Dump' and contains a sub-section titled 'The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear.' Below this is a table header with columns: Host Name, Network Interface, Filter, File Name, Repository, File S..., Number of ..., Time Limit, Promiscuous M..., and Status. A red box highlights the 'Add' button at the top left of the table area.

UCSMが認証を送信しているポリシーサービスノードを選択し、フィルタで、認証が送信されているUCSMのIPに対応する入力ip host X.X.X.Xに進み、キャプチャに名前を付けて下にスクロールして保存し、キャプチャを実行してUCSMからログインします（図1の矢印Bを参照）。

The screenshot shows the 'Add TCP Dump' configuration page. Under 'Host Name', 'ise32' is entered. Under 'Network Interface', 'GigabitEthernet 0 [Up, Running]' is selected. In the 'Filter' field, 'ip host 10.31.123.7' is typed. Under 'File Name', 'tacccap' is entered. At the bottom right, the 'Save and Run' button is highlighted with a red box.

ステップ4認証が実行されるPSN内のデバッグのコンポーネントruntime-AAAを、Operations > Troubleshoot > Debug Wizard > Debug log configurationで有効にし、PSNノード（ノードID）を選択してから、editボタンでnextを選択します。

[Diagnostic Tools](#) [Download Logs](#) [Debug Wizard](#)

Debug Profile Configuration

Debug Log Configuration

## Node List

[Edit](#) [Reset to Default](#)

Node Name	Replication Role
-----------	------------------

<input type="radio"/> ise32	STANDALONE
-----------------------------	------------

コンポーネントruntime-AAAを探し、そのレベルをdebugに変更して問題を再度再現し、ログの分析に進みます（次の出力例を参照）。

[Diagnostic Tools](#) [Download Logs](#) [Debug Wizard](#)

Debug Profile Configuration

Debug Log Configuration

Node List &gt; ise32.example.com

## Debug Level Configuration

[Edit](#) [Reset to Default](#)

Component Name	Log Level	Description	Log file Name
----------------	-----------	-------------	---------------

runtime-AAA	X		
-------------	---	--	--

<input type="radio"/> runtime-AAA	DEBUG	AAA runtime messages (prrt)	prrt-server.log
-----------------------------------	-------	-----------------------------	-----------------

 注：詳細については、Cisco YoutubeのチャンネルHow to Enable Deubgs on ISE 3.x Versions <https://www.youtube.com/watch?v=E3USz8B76c8>のビデオを参照してください。

## 関連情報

[Cisco UCS Managerアドミニストレーションマネジメントガイド](#)[Cisco UCS CIMCコンフィギュレーションガイドTACACS+](#)

## 翻訳について

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