

# 在ISE 2.2上配置最大併發使用者會話

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

### [背景資訊](#)

### [網路圖表](#)

### [案例](#)

#### [每個使用者的最大會話數](#)

##### [組態](#)

##### [範例](#)

#### [組的最大會話數](#)

##### [設定](#)

##### [範例](#)

##### [角部案例](#)

#### [組中使用者的最大會話數](#)

##### [設定](#)

##### [範例](#)

#### [組的最大會話和該組中的使用者的最大會話數](#)

##### [設定](#)

##### [範例](#)

#### [計數器時間限制](#)

##### [設定](#)

##### [範例](#)

#### [最大會話功能和訪客訪問許可權](#)

##### [中央 Web 驗證](#)

##### [本地 Web 驗證](#)

### [疑難排解](#)

#### [Radius即時日誌](#)

#### [ISE調試](#)

---

## 簡介

本文檔介紹如何配置身份服務引擎(ISE)2.2中引入的最大會話功能。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- RADIUS通訊協定
- 無線LAN控制器(WLC)上的802.1x組態
- ISE及其角色 ( 角色 )

## 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎版本2.2
- 無線LAN控制器8.0.100.0
- Cisco Catalyst交換器3750 15.2(3)E2
- Windows 7電腦
- 運行6.0.1的Android電話
- 運行5.0的Android電話
- Apple iPad iOS 9.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

「最大會話數」功能提供了一種方法，可針對每個使用者或每個身份組控制和強制執行即時會話。本檔案是用於RADIUS作業階段，但也可以用於TACACS作業階段。

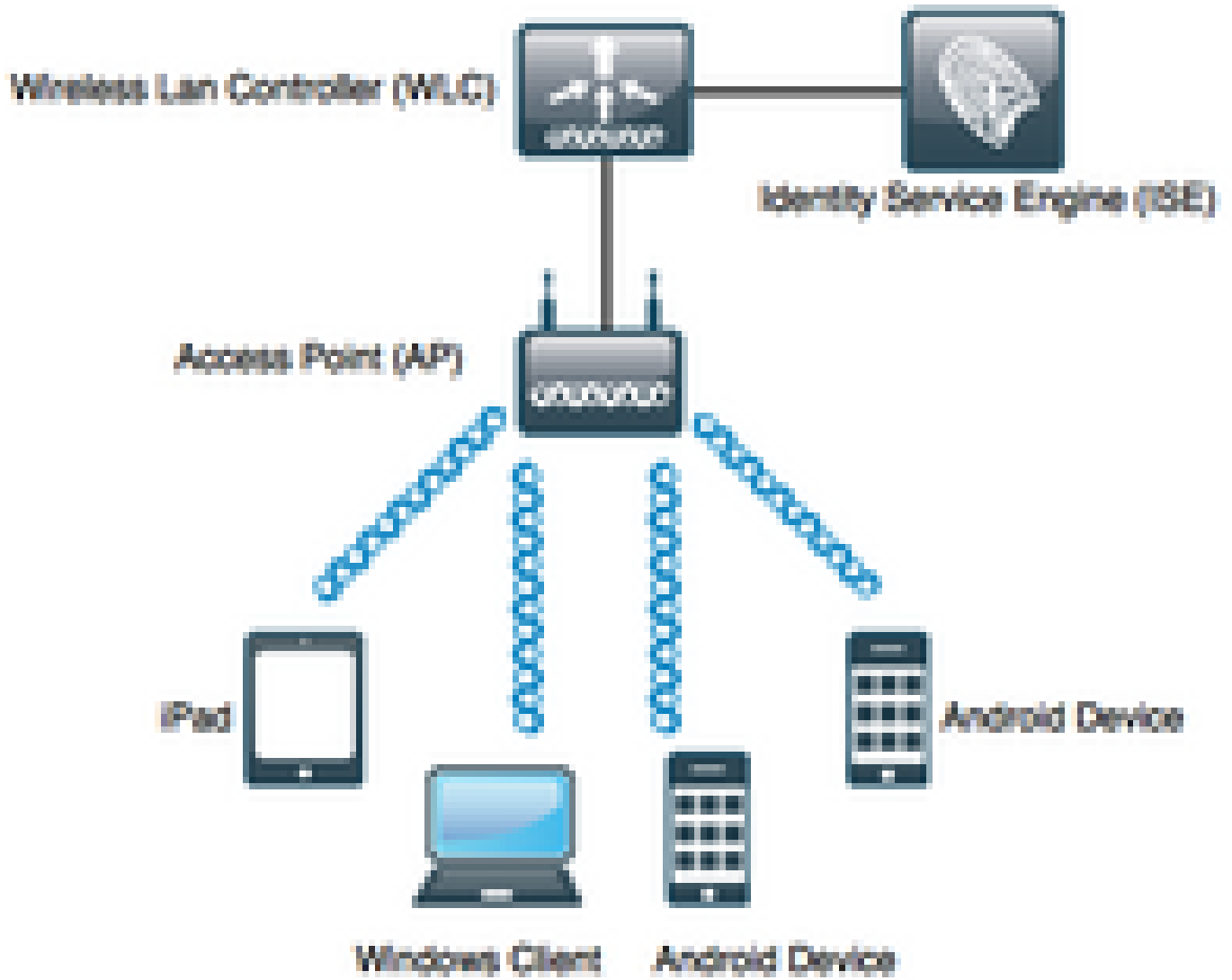
ISE版本2.2可以基於以下併發會話檢測和構建實施策略：

- User Identity — 限制每個特定使用者的會話數
- Identity Group — 限制每個特定組的會話數
- 組中的使用者 — 限制每個使用者屬於特定組的會話數

併發會話的強制和計數是唯一的，由每個策略服務節點(PSN)管理。PSN之間沒有會話計數方面的同步。併發會話功能在運行時進程中實現，資料僅儲存在記憶體中。在PSN重新啟動的情況下，MaxSessions計數器將重置。

使用者會話計數對使用者名稱不區分大小寫，並且獨立於使用的網路訪問裝置 ( 只要使用相同的PSN節點 )。

## 網路圖表

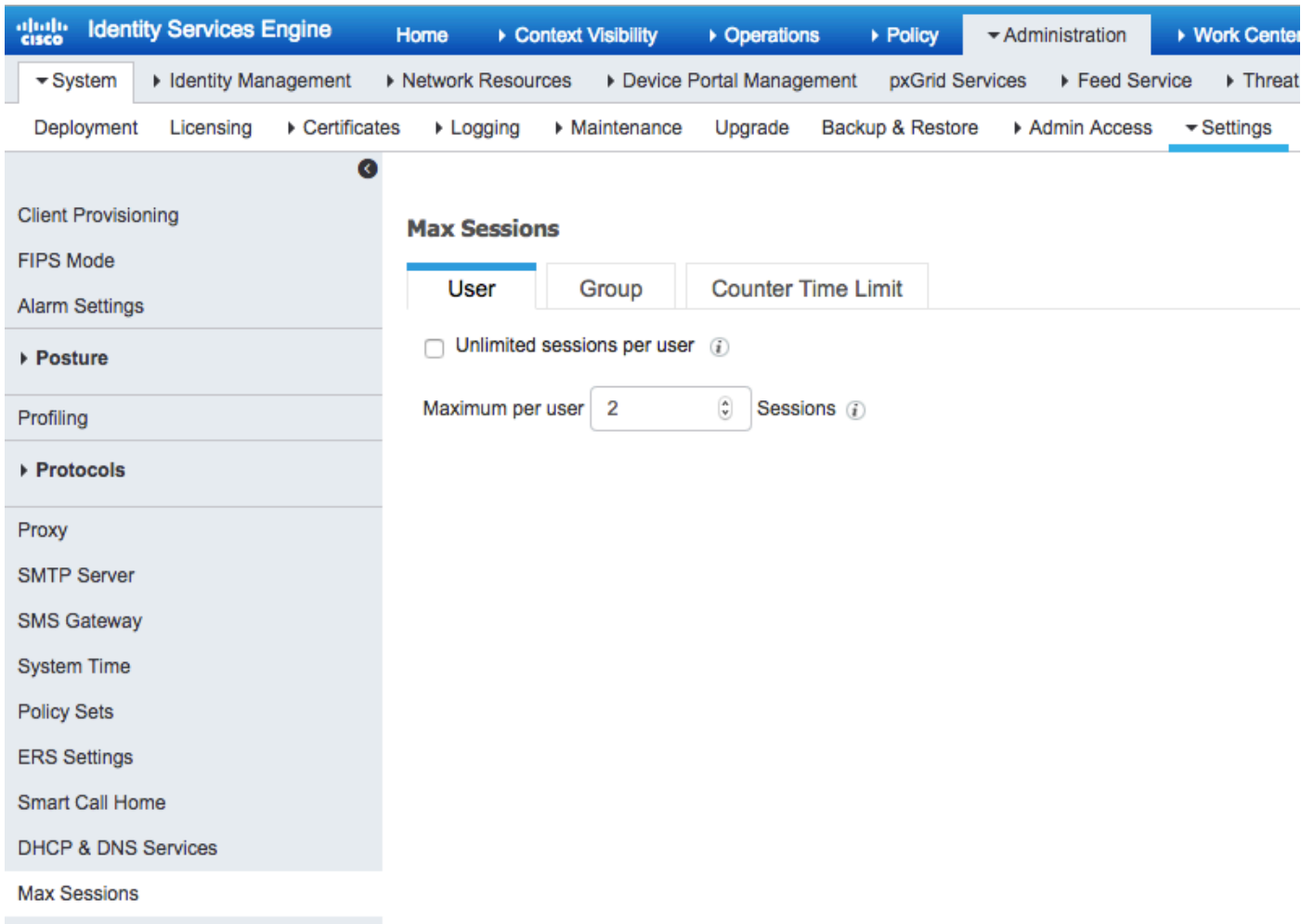


## 案例

每個使用者的最大會話數

組態

導覽至Administration > System > Settings > Max Sessions，如下圖所示：



要啟用該功能，請取消選中Unlimited session per user覈取方塊，該覈取方塊預設處於選中狀態。在Maximum per user Sessions欄位中，配置特定使用者在每個PSN上可以擁有的會話數。在本例中，它設定為2。

來自外部身份源（例如Active Directory）的使用者也受此配置的影響。

### 範例

Bob是來自Active Directory域的帳戶的使用者名稱，該帳戶已連線並加入ISE伺服器。「使用者最大會話」配置為值2，這表示不允許對同一使用者超過此數量的任何會話（每個PSN）。

如圖所示，使用者Bob使用相同的憑證連線Android Phone和Windows電腦：

Jan 29, 2017 08:34:51.137 AM	✓	🔒	Bob	CC:FA:00:B4:D5:0F	LG-Device	Profiled	Default >> Dot1X >> Default	Default >> MaxSession_Test
Jan 29, 2017 08:32:17.776 AM	✓	🔒	Bob	C0:4A:00:14:56:F4	TP-LINK-Device	Profiled	Default >> Dot1X >> Default	Default >> MaxSession_Test

由於未超過最大作業階段上限，因此允許兩個作業階段。請參閱詳細的Radius Live日誌，如下圖所示：

## Overview

Event 5200 Authentication succeeded

Username Bob

Endpoint Id CC:FA:00:B4:D5:0F ⓘ

Endpoint Profile LG-Device

Authentication Policy Default >> Dot1X >> Default

Authorization Policy Default >> MaxSession\_Test

Authorization Result PermitAccess

15036 Evaluating Authorization Policy

15048 Queried PIP - EndPoints.LogicalProfile

15048 Queried PIP - Network Access.AuthenticationStatus

15004 Matched rule - MaxSession\_Test

15016 Selected Authorization Profile - PermitAccess

22081 Max sessions policy passed

22080 New accounting session created in Session cache

12306 PEAP authentication succeeded

11503 Prepared EAP-Success

24432 Looking up user in Active Directory - pgruszczad.example.com

24355 LDAP fetch succeeded - pgruszczad.example.com

24416 User's Groups retrieval from Active Directory succeeded - pgruszczad.example.com

11002 Returned RADIUS Access-Accept

22081 Max sessions policy passed 步驟提供最大併發會話檢查成功的資訊。

啟動與另一裝置的第三個連線並啟動相同的憑證後，Bob會收到PermitAccess，但Access-Reject會傳送到身份驗證器：

Jan 29, 2017 08:35:35.293 AM	✖	🔒	Bob	34:AB:37:60:63:88	Apple-Device	Profiled	Default >> Dot1X >> Default	Default >> MaxSession_Test
Jan 29, 2017 08:34:51.137 AM	✔	🔒	Bob	CC:FA:00:B4:D5:0F	LG-Device	Profiled	Default >> Dot1X >> Default	Default >> MaxSession_Test
Jan 29, 2017 08:32:17.776 AM	✔	🔒	Bob	C0:4A:00:14:56:F4	TP-LINK-Device	Profiled	Default >> Dot1X >> Default	Default >> MaxSession_Test

## Overview

**Event** 5400 Authentication failed

**Username** Bob

**Endpoint Id** 34:AB:37:60:63:88

**Endpoint Profile** Apple-Device

**Authentication Policy** Default >> Dot1X >> Default

**Authorization Policy** Default >> MaxSession\_Test

**Authorization Result** PermitAccess

## Authentication Details

**Source Timestamp** 2017-01-29 08:36:28.882

**Received Timestamp** 2017-01-29 08:35:35.293

**Policy Server** pgruszczise22

**Event** 5400 Authentication failed

**Failure Reason** 22089 Max sessions policy failed. Max sessions user limit exceeded.

**Username** Bob

**Endpoint Id** 34:AB:37:60:63:88

```

15008 Evaluating Authorization Policy
15048 Queried PIP - EndPoints.LogicalProfile
15048 Queried PIP - Network Access.AuthenticationStatus
15004 Matched rule - MaxSession_Test
15018 Selected Authorization Profile - PermitAccess
22088 Max sessions policy failed. Max sessions user limit exceeded.
12308 PEAP authentication succeeded
11503 Prepared EAP-Success
11503 Returned RADIUS Access-Reject

```

不允許進行作業階段，即使在Radius即時記錄中，您會看到它命中正確的授權設定檔。若要檢查活動會話，請導航到操作> Radius >活動會話：

Session Status	Action	Endpoint ID	Identity	IP Address	Endpoint Profile
Started	Show CoA Actions	CC:FA:00:B4:D5:0F	Bob	10.62.148.145	LG-Device
Started	Show CoA Actions	C0:4A:00:14:56:F4	Bob	10.62.148.141	TP-LINK-Device

在這種情況下，兩個會話的狀態都是Started，這表示會話的Accounting Start到達ISE。必須收到Radius Accounting for Max Session才能正常工作，在會話計數期間不會考慮已驗證狀態（允許會話，但沒有記帳）：

Session Status	Action	Endpoint ID	Identity	IP Address	Endpoint Profile	Posture Status	Security Group
Authenticated	Show CoA Actions	C0:4A:00:14:56:A7	Bob				
Authenticated	Show CoA Actions	C0:4A:00:14:56:F4	Bob		TP-LINK-Device		
Authenticated	Show CoA Actions	34:AB:37:60:63:88	Bob		Apple-Device		
Authenticated	Show CoA Actions	CC:FA:00:B4:D5:0F	Bob		LG-Device		

## 組的最大會話數

設定

導航到管理>System>設定>最大會話數>組:

### Max Sessions

User	Group	Counter Time Limit		
Expand All Collapse All Filter Settings				
Name	Description	Max Sessions for Group	Max Sessions for User in Group	
ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (defau...	Unlimited	Unlimited	🔗
Employee	Default Employee User Group	Unlimited	Unlimited	🔗
GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (d...	Unlimited	Unlimited	🔗
GroupTest1	MaxSession Test	Unlimited	Unlimited	🔗
<b>GroupTest2</b>	<b>MaxSession Test</b>	<b>2</b>	Unlimited	🔗
GroupTest3	MaxSession Test	Unlimited	Unlimited	🔗
GuestType_Contractor (default)	Identity group mirroring the gues...	Unlimited	Unlimited	🔗
GuestType_Daily (default)	Identity group mirroring the gues...	Unlimited	Unlimited	🔗
GuestType_StandardGuest	Identity group mirroring the gues...	Unlimited	Unlimited	🔗
GuestType_Weekly (default)	Identity group mirroring the gues...	Unlimited	Unlimited	🔗
OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (def...	Unlimited	Unlimited	🔗
				Reset Save

此配置最多為內部身份組GroupTest2實施2個會話：您只能為內部組為每個組配置實施。

### 範例

Alice、Pablo和Peter是內部ISE使用者儲存的使用者。它們都是名為GroupTest2的組的成員。根據本示例中的配置，根據組成員身份，會話的最大值設定為2。

### Network Access Users

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups
<input type="checkbox"/> Enabled	alice					GroupTest2
<input type="checkbox"/> Enabled	pablo					GroupTest2
<input type="checkbox"/> Enabled	peter					GroupTest2

Pablo和Peter使用來自名為GroupTest2的內部組的憑證連線到網路：


Jan 29, 2017 09:25:54.554 AM	✔	🔗	Pablo	C0:4A:00:14:56:F4	TP-LINK-Device	User Identity Groups:GroupTest2 Default >> MaxSession_Test
Jan 29, 2017 09:25:34.984 AM	✔	🔗	Peter	34:AB:37:60:63:88	Apple-Device	User Identity Groups:GroupTest2 Default >> MaxSession_Test

Alice嘗試連線後，將強制每個組的MaxSessions限制：

Jan 29, 2017 09:26:17.812 AM	✘	🔗	Alice	CC:FA:00:B4:D5:0F	LG-Device	User Identity Groups:GroupTest2 Default >> MaxSession_Test
Jan 29, 2017 09:25:54.554 AM	✔	🔗	Pablo	C0:4A:00:14:56:F4	TP-LINK-Device	User Identity Groups:GroupTest2 Default >> MaxSession_Test
Jan 29, 2017 09:25:34.984 AM	✔	🔗	Peter	34:AB:37:60:63:88	Apple-Device	User Identity Groups:GroupTest2 Default >> MaxSession_Test



## Overview

Event	5400 Authentication failed
Username	Alice
Endpoint Id	CC:FA:00:B4:D5:0F 
Endpoint Profile	LG-Device
Authentication Policy	Default >> Dot1X >> Default
Authorization Policy	Default >> MaxSession_Test
Authorization Result	PermitAccess

由於Peter和Pablo已用盡最大會話組限制，因此Alice不允許連線到網路：

## Authentication Details

Source Timestamp	2017-01-29 09:27:11.504
Received Timestamp	2017-01-29 09:26:17.812
Policy Server	pgruszczise22
Event	5400 Authentication failed
Failure Reason	22097 Max sessions policy failed. Max sessions group limit exceeded.
Username	Alice

## 角部案例

如果配置了User Maximum Sessions，則兩個功能獨立工作。在此示例中，使用者最大會話數設定為1，組的最大會話數設定為2。

## Max Sessions

**User** | Group | Counter Time Limit

Unlimited sessions per user ⓘ

Maximum per user  Sessions ⓘ

基於組的最大會話（2個會話）允許Peter，但由於使用者最大會話配置（一個會話）導致他無法連線到網路：

Jan 29, 2017 09:34:18.169 AM			Peter	C0:4A:00:14:56:F4	TP-LINK-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test
Jan 29, 2017 09:33:54.792 AM			Peter	34:AB:37:60:63:88	Apple-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test

如果使用者同時是一個以上組的成員，並且為其配置了Max Sessions for Group，則一旦連線，ISE會針對使用者所屬的每個組增加Max Session for Group cache的計數器。

在本示例中，Alice和Pablo都是GroupTest1和GroupTest2的成員。Veronica僅屬於GroupTest1，Peter屬於GroupTest2

## Network Access Users

Edit Add Change Status Import Export Delete Duplicate

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/> Enabled	alice					GroupTest1,GroupTest2	
<input type="checkbox"/> Enabled	pablo					GroupTest1,GroupTest2	
<input type="checkbox"/> Enabled	peter					GroupTest2	
<input type="checkbox"/> Enabled	veronica					GroupTest1	

GroupTest1和GroupTest2的Max Session設定為2:

## Max Sessions

User	Group	Counter Time Limit		
Expand All Collapse All Filter Settings				
Name	Description	Max Sessions for Group	Max Sessions for User in Group	
ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (defau...	Unlimited	Unlimited	🗑️
Employee	Default Employee User Group	Unlimited	Unlimited	🗑️
GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (d...	Unlimited	Unlimited	🗑️
GroupTest1		2	Unlimited	🗑️
GroupTest2		2	Unlimited	🗑️
GroupTest3		Unlimited	Unlimited	🗑️
GuestType_Contractor (default)	Identity group mirroring the gues...	Unlimited	Unlimited	🗑️
GuestType_Daily (default)	Identity group mirroring the gues...	Unlimited	Unlimited	🗑️
GuestType_Weekly (default)	Identity group mirroring the gues...	Unlimited	Unlimited	🗑️
OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (def...	Unlimited	Unlimited	🗑️
				Reset Save

當Alice和Pablo連線到網路時，它們超過了兩個組的會話限制。Veronica ( 僅屬於GroupTest1和Peter )，GroupTest2的成員無法連線，因為組的Max Session已達到最大配置值：

Icon	Name	MAC Address	Device Type	User Identity Groups	Default >> D...	Default >> MaxSession_Test
🔴	Veronica	10:A5:D0:98:B8:E2	Unknown	User Identity Groups:GroupTest1,Unknown	Default >> D...	Default >> MaxSession_Test
🔴	Peter	34:AB:37:60:63:88	Apple-Device	User Identity Groups:GroupTest2,Profiled	Default >> D...	Default >> MaxSession_Test
🟡	Pablo	CC:FA:00:B4:D5:0F	LG-Device		Default >> D...	Default >> MaxSession_Test
🟢	Pablo	CC:FA:00:B4:D5:0F	LG-Device	User Identity Groups:GroupTest1,User Identity Groups:GroupTest2,f	Default >> D...	Default >> MaxSession_Test
🟡	Alice	C0:4A:00:14:56:F4	TP-LINK-Device		Default >> D...	Default >> MaxSession_Test
🟢	Alice	C0:4A:00:14:56:F4	TP-LINK-Device	User Identity Groups:GroupTest1,User Identity Groups:GroupTest2,f	Default >> D...	Default >> MaxSession_Test

## 組中使用者的最大會話數

設定

導航到Administration > System > Settings > Max Sessions > Group。

## Max Sessions

User	Group	Counter Time Limit		
Expand All Collapse All Filter Settings				
Name	Description	Max Sessions for Group	Max Sessions for User in Group	
ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (defau...	Unlimited	Unlimited	🔗
Employee	Default Employee User Group	Unlimited	Unlimited	🔗
GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (d...	Unlimited	Unlimited	🔗
GroupTest1	MaxSession Test	Unlimited	Unlimited	🔗
GroupTest2	MaxSession Test	Unlimited	2	🔗
GroupTest3	MaxSession Test	Unlimited	Unlimited	🔗
GuestType_Contractor (default)	Identity group mirroring the gues...	Unlimited	Unlimited	🔗
GuestType_Daily (default)	Identity group mirroring the gues...	Unlimited	Unlimited	🔗
GuestType_StandardGuest	Identity group mirroring the gues...	Unlimited	Unlimited	🔗
GuestType_Weekly (default)	Identity group mirroring the gues...	Unlimited	Unlimited	🔗
OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (def...	Unlimited	Unlimited	🔗
				Reset Save

此配置最多為內部身份組GroupTest2實施2個會話。

## 範例

Alice是GroupTest2的成員：

## Network Access Users

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups
<input checked="" type="checkbox"/> Enabled	alice					GroupTest2

此功能的工作方式與使用者最大會話(User Maximum Session)類似 — ISE限制指定內部組內使用者可擁有的併發會話數。此配置僅影響屬於已配置組的使用者。

Alice作為GroupTest2的成員，可以有2個同時會話。連線到第三台裝置後，ISE根據超過組內使用者最大會話數返回PermitAccess和Access-Reject:

Jan 29, 2017 10:00:17.666 AM	❌	🔒	Alice	34:AB:37:60:63:88	Apple-Device	User Identity Groups:GroupTest2 Default >> MaxSession_Test
Jan 29, 2017 09:59:56.723 AM	✅	🔒	Alice	CC:FA:00:B4:D5:0F	LG-Device	User Identity Groups:GroupTest2 Default >> MaxSession_Test
Jan 29, 2017 09:59:00.008 AM	✅	🔒	Alice	C0:4A:00:14:56:F4	TP-LINK-Device	User Identity Groups:GroupTest2 Default >> MaxSession_Test

詳細的Radius-Live日誌：

## Overview

Event **5400 Authentication failed**

Username Alice

Endpoint Id 34:AB:37:60:63:88 

Endpoint Profile Apple-Device

Authentication Policy Default >> Dot1X >> Default

Authorization Policy Default >> MaxSession\_Test

Authorization Result PermitAccess

15036 Evaluating Authorization Policy

15048 Queried PIP - EndPoints.LogicalProfile

15048 Queried PIP - Network Access.AuthenticationStatus

15004 Matched rule - MaxSession\_Test

15016 Selected Authorization Profile - PermitAccess

**22098 Max sessions policy failed. Max sessions user in group limit exceeded.**

12306 PEAP authentication succeeded


11503 Prepared EAP-Success

11003 Returned RADIUS Access-Reject

如果同時啟用「使用者最大會話數」，則兩個功能獨立工作。如果使用者Alice是組GroupTest2的成員，且組Maximum Session for User in Group配置為2，同時User Max Sessions配置為每個使用者只允許一個會話，則User Max Sessions優先：

### Max Sessions

User Group Counter Time Limit

Unlimited sessions per user 

Maximum per user  Sessions 

Reset

Save

當Alice嘗試連線到第二個裝置時，ISE根據超過最大會話使用者限制返回訪問拒絕：

Jan 29, 2017 10:06:00.852 AM	✖	🔗	Alice	CC:FA:00:B4:D5:0F	LG-Device	User Identity Groups:GroupTest2 Default >> MaxSession_Test
Jan 29, 2017 10:05:28.903 AM	✔	🔗	Alice	C0:4A:00:14:56:F4	TP-LINK-Device	User Identity Groups:GroupTest2 Default >> MaxSession_Test

拒絕的原因可以在詳細的Radius即時日誌下檢查。最大會話使用者限制是失敗的原因：

### Authentication Details

Source Timestamp	2017-01-29 10:06:54.616
Received Timestamp	2017-01-29 10:06:00.852
Policy Server	pgruszczise22
Event	5400 Authentication failed
Failure Reason	22089 Max sessions policy failed. Max sessions user limit exceeded.
Username	Alice

```
15008 Evaluating Authorization Policy
15048 Queried PIP - EndPoints.LogicalProfile
15048 Queried PIP - Network Access.AuthenticationStatus
15004 Matched rule - MaxSession_Test
15018 Selected Authorization Profile - PermitAccess
22089 Max sessions policy failed. Max sessions user limit exceeded.
12308 PEAP authentication succeeded
11503 Prepared EAP-Success
11003 Returned RADIUS Access-Reject
```

組的最大會話和該組中的使用者的最大會話數

設定

導航到Administration > System > Settings > Max Sessions > Group。

## Max Sessions

User	Group	Counter Time Limit		
Expand All Collapse All Filter Settings				
Name	Description	Max Sessions for Group	Max Sessions for User in Group	
ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (defau...	Unlimited	Unlimited	🗑️
Employee	Default Employee User Group	Unlimited	Unlimited	🗑️
GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (d...	Unlimited	Unlimited	🗑️
GroupTest1		Unlimited	Unlimited	🗑️
GroupTest2		3	2	🗑️
GroupTest3		Unlimited	Unlimited	🗑️
GuestType_Contractor (default)	Identity group mirroring the gues...	Unlimited	Unlimited	🗑️
GuestType_Daily (default)	Identity group mirroring the gues...	Unlimited	Unlimited	🗑️
GuestType_Weekly (default)	Identity group mirroring the gues...	Unlimited	Unlimited	🗑️
OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (def...	Unlimited	Unlimited	🗑️
				Reset Save

此配置在內部身份組GroupTest2中實施最多3個會話，在該組中為使用者實施最多2個會話。

## 範例

Alice和Pablo是GroupTest2的成員。根據本示例中的配置，GroupTest2中最多允許3個會話。ISE確保單個使用者在此組中最多可以有2個會話。

## Network Access Users

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups
<input type="checkbox"/> Enabled	alice					GroupTest2
<input type="checkbox"/> Enabled	pablo					GroupTest2

Alice通過兩個裝置連線。兩個終端均連線到網路：

Jan 29, 2017 10:27:04.543 AM	✔	📄	Alice	34:AB:37:60:63:88	Apple-Device	User Identity Groups:GroupTest2 Default >> MaxSession_Test
Jan 29, 2017 10:26:50.664 AM	✔	📄	Alice	C0:4A:00:14:56:F4	TP-LINK-Device	User Identity Groups:GroupTest2 Default >> MaxSession_Test

當Alice嘗試通過第三台裝置連線時，訪問被拒絕，並且超過組內使用者的最大會話數限制：

Jan 29, 2017 10:28:34.503 AM	✘	🔒	Alice	CC:FA:00:B4:D5:0F	LG-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test
Jan 29, 2017 10:27:04.543 AM	✔	🔒	Alice	34:AB:37:60:63:88	Apple-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test
Jan 29, 2017 10:26:50.664 AM	✔	🔒	Alice	C0:4A:00:14:56:F4	TP-LINK-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test

## Authentication Details

Source Timestamp	2017-01-29 10:29:28.309
Received Timestamp	2017-01-29 10:28:34.503
Policy Server	pgruszczise22
Event	5400 Authentication failed
Failure Reason	22098 Max sessions policy failed. Max sessions user in group limit exceeded.
Username	Alice

如果Pablo嘗試訪問網路，他能夠這樣做，因為Group的Max Session for GroupTest2尚未滿：

Jan 29, 2017 10:31:22.128 AM	✔	🔒	Pablo	CC:FA:00:B4:D5:0F	LG-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test
Jan 29, 2017 10:28:34.503 AM	✘	🔒	Alice	CC:FA:00:B4:D5:0F	LG-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test
Jan 29, 2017 10:27:04.543 AM	✔	🔒	Alice	34:AB:37:60:63:88	Apple-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test
Jan 29, 2017 10:26:50.664 AM	✔	🔒	Alice	C0:4A:00:14:56:F4	TP-LINK-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test

當Pablo嘗試從第二台裝置訪問網路時，他因超過組的最大會話限制而失敗（即使他只有1個會話）：

Jan 29, 2017 10:55:24.389 AM	✘	🔒	Pablo	CC:FA:00:B4:D5:0F	LG-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test
Jan 29, 2017 10:54:11.860 AM	✔	🔒	Pablo	10:A5:D0:98:B8:E2	Unknown	User Identity Groups:GroupTest2	Default >> MaxSession_Test
Jan 29, 2017 10:53:36.734 AM	✔	🔒	Alice	C0:4A:00:14:56:F4	TP-LINK-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test
Jan 29, 2017 10:52:42.285 AM	✔	🔒	Alice	34:AB:37:60:63:88	Apple-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test



### Authentication Details

Source Timestamp	2017-01-29 10:56:18.248
Received Timestamp	2017-01-29 10:55:24.389
Policy Server	pgruszczise22
Event	5400 Authentication failed
Failure Reason	22097 Max sessions policy failed. Max sessions group limit exceeded.
Username	Pablo

如前面的示例所示，如果啟用User Maximum Sessions，它將獨立工作。

## 計數器時間限制

設定

導航到管理>系統>設定>最大會話>計數器時間限制。

### Max Sessions

User Group Counter Time Limit

Unlimited - no time limit

Delete sessions after 0 Days 0 Hour/s 5 Minutes

Reset Save

計數器時間限制是指定按照最大會話快取對會話計數的時間間隔的功能。此功能允許您指定PSN從計數器刪除會話的時間以及允許新的會話。

要啟用該功能，需要取消選中Unlimited - no time limitcheckbox (預設情況下選中)。在可編輯欄位中，可以設定MaxSession的計數器考慮會話的時間長度。

請記住，配置時間後的會話不會斷開連線，也不會從會話資料庫中刪除。在設定時間後沒有終止授權鏈結(CoA)。

範例

User Max Session設定為使用者只允許一個會話：

### Max Sessions

User Group Counter Time Limit

Unlimited sessions per user ⓘ

Maximum per user  Sessions ⓘ

Reset Save

Alice在11:00:34使用IPad連線到網路，第二次身份驗證在11:07進行，即使超過使用者最大會話值，仍允許訪問。由於計數器時間限制，兩個身份驗證均成功。

Jan 29, 2017 11:07:29.192 AM	✓	🔒	Alice	C0:4A:00:14:56:F4	TP-LINK-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test
Jan 29, 2017 11:00:34.938 AM	✓	🔒	Alice	34:AB:37:60:63:88	Apple-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test

Alice嘗試在上次成功連線通過5分鐘之前連線到另一台裝置，ISE拒絕身份驗證：

Jan 29, 2017 11:08:51.051 AM	✗	🔒	Alice	CC:FA:00:B4:D5:0F	LG-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test
Jan 29, 2017 11:07:29.192 AM	✓	🔒	Alice	C0:4A:00:14:56:F4	TP-LINK-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test
Jan 29, 2017 11:00:34.938 AM	✓	🔒	Alice	34:AB:37:60:63:88	Apple-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test

在上次身份驗證後5分鐘後，Alice可以使用其他裝置連線到網路。

Jan 29, 2017 11:12:51.216 AM	✓	🔒	Alice	CC:FA:00:B4:D5:0F	LG-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test
Jan 29, 2017 11:08:51.051 AM	✗	🔒	Alice	CC:FA:00:B4:D5:0F	LG-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test
Jan 29, 2017 11:07:29.192 AM	✓	🔒	Alice	C0:4A:00:14:56:F4	TP-LINK-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test
Jan 29, 2017 11:00:34.938 AM	✓	🔒	Alice	34:AB:37:60:63:88	Apple-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test

在即時會話中，您可以看到處於已啟動狀態的所有三個會話：

11:12:51.577 AM	Started	Show CoA Actions ⚙	CC:FA:00:B4:D5:0F ⚙	Alice ⚙	10.62.148.145 ⚙	LG-Device
11:07:29.365 AM	Started	Show CoA Actions	C0:4A:00:14:56:F4	Alice	10.62.148.141	TP-LINK-Device
11:00:35.028 AM	Started	Show CoA Actions	34:AB:37:60:63:88	Alice	10.62.148.144	Apple-Device

## 最大會話功能和訪客訪問許可權

### 中央 Web 驗證

在User Maximum Session feature下配置了一個會話後，您仍然能夠使用兩個會話的Guest1帳戶進

行連線：

Jan 29, 2017 12:02:41.587 PM	<input checked="" type="checkbox"/>		guest1	CC:FA:00:B4:D5:0F	Unknown	Any, GuestEndpoints	Default >> Wi-Fi_Guest_Access
Jan 29, 2017 12:02:41.575 PM	<input checked="" type="checkbox"/>			CC:FA:00:B4:D5:0F			
Jan 29, 2017 12:02:39.982 PM	<input checked="" type="checkbox"/>		guest1	CC:FA:00:B4:D5:0F		Any	
Jan 29, 2017 12:01:51.408 PM	<input checked="" type="checkbox"/>			CC:FA:00:B4:D5:0F	LG-Device	Profiled	Default >> Wi-Fi_Redirect_to_Guest_Login
Jan 29, 2017 12:01:37.682 PM	<input checked="" type="checkbox"/>		guest1	34:AB:37:60:63:88	Unknown	Any, GuestEndpoints	Default >> Wi-Fi_Guest_Access
Jan 29, 2017 12:01:37.645 PM	<input checked="" type="checkbox"/>			34:AB:37:60:63:88			
Jan 29, 2017 12:01:13.402 PM	<input checked="" type="checkbox"/>		guest1	34:AB:37:60:63:88		Any	
Jan 29, 2017 12:00:35.970 PM	<input checked="" type="checkbox"/>			34:AB:37:60:63:88	Apple-Device	Profiled	Default >> Wi-Fi_Redirect_to_Guest_Login

為了限制訪客訪問，您可以在Guest Type配置中指定Maximum simultaneous logins。

導覽至Work Centers > Guest Access > Portal & Components > Guest Types，然後變更Maximum simultaneous logins選項，如下圖所示：

### Guest Type

Guest type name: \*

Description:

▾

Collect Additional Data

#### Maximum Access Time

Account duration starts

- From first login
- From sponsor-specified date (or date of self-registration, if applicable)

Maximum account duration

Default  (1-999)

Allow access only on these days and times:

From  To   Sun  Mon  Tue  Wed  Thu  Fri  Sat

Configure guest Account Purge Policy at:  
[Work Centers > Guest Access > Settings > Guest Account Purge Policy](#)

#### Login Options

Maximum simultaneous logins  (1-999)

When guest exceeds limit:

- Disconnect the oldest connection
- Disconnect the newest connection
- Redirect user to a portal page showing an error message ⓘ  
*This requires the creation of an authorization policy rule*

### 本地Web驗證

在User Maximum Session (使用者最大會話) 下配置一個會話後，您將無法連線：

Jan 29, 2017 12:13:22.598 PM	✘	🔒	Guest1	CC:FA:00:B4:D5:0F	Unknown	GuestEndpoints	Default >> MaxSession_Test
Jan 29, 2017 12:13:17.505 PM	✔	🔒	guest1			Any	
Jan 29, 2017 12:12:25.560 PM	✔	🔒	Guest1	34:AB:37:60:63:88	Unknown	GuestEndpoints	Default >> MaxSession_Test
Jan 29, 2017 12:12:19.629 PM	✔	🔒	guest1			Any	

根據Radius Live-logs，訪客1一律會根據入口驗證進行正確驗證。一旦WLC通過第二個會話為Guest1傳送RADIUS請求，ISE就會因為超過使用者限制而拒絕訪問：

## Authentication Details

Source Timestamp	2017-01-29 12:14:16.603
Received Timestamp	2017-01-29 12:13:22.598
Policy Server	pgruszczise22
Event	5400 Authentication failed
Failure Reason	22089 Max sessions policy failed. Max sessions user limit exceeded.

## 疑難排解

### Radius即時日誌

詳細的Radius報告是排除MaxSession功能故障的首要位置。

## Authentication Details

Source Timestamp	2017-01-29 11:09:44.931
Received Timestamp	2017-01-29 11:08:51.051
Policy Server	pgruszczise22
Event	5400 Authentication failed
Failure Reason	22089 Max sessions policy failed. Max sessions user limit exceeded.

此失敗原因表示已超過此會話/使用者的全域性最大使用者會話限制，如下圖所示：

## Authentication Details

Source Timestamp	2017-01-29 10:42:38.819
Received Timestamp	2017-01-29 10:41:44.988
Policy Server	pgruszczise22
Event	5400 Authentication failed
Failure Reason	22097 Max sessions policy failed. Max sessions group limit exceeded.

此失敗原因表示已超過此會話/使用者的組最大會話限制，如下圖所示：

## Authentication Details

Source Timestamp	2017-01-29 10:29:28.309
Received Timestamp	2017-01-29 10:28:34.503
Policy Server	pgruszczise22
Event	5400 Authentication failed
Failure Reason	22098 Max sessions policy failed. Max sessions user in group limit exceeded.

此失敗原因表示已超過此會話/使用者的組使用者最大會話數限制。

在選擇授權配置檔案後檢查MaxSession快取：

成功：

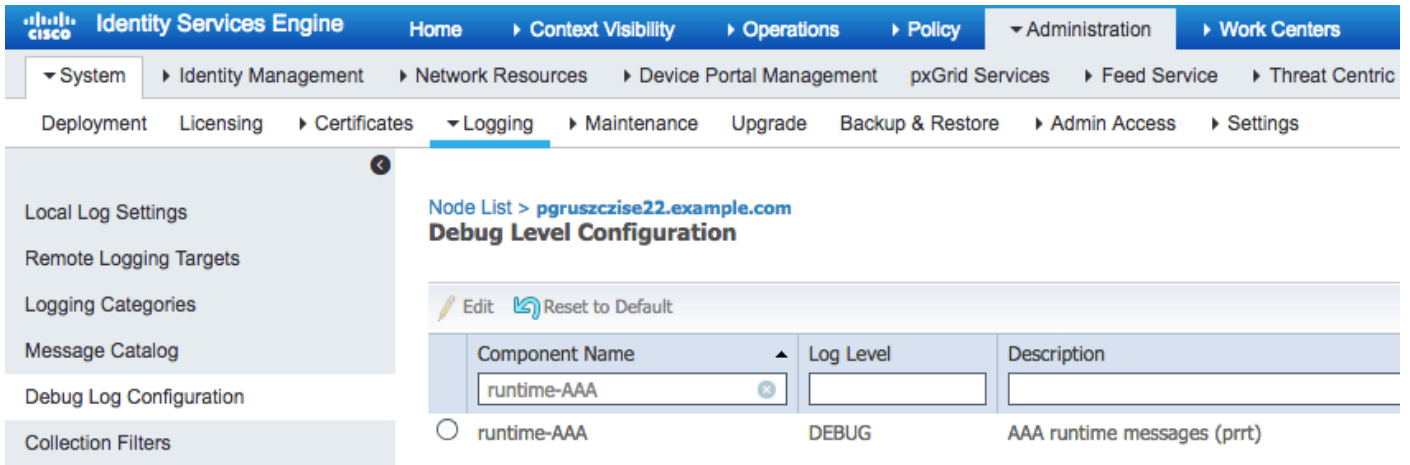
15016 Selected Authorization Profile - PermitAccess  
22081 Max sessions policy passed  
22080 New accounting session created in Session cache  
12306 PEAP authentication succeeded  
11503 Prepared EAP-Success  
11002 Returned RADIUS Access-Accept

失敗：

15016 Selected Authorization Profile - PermitAccess  
22089 Max sessions policy failed. Max sessions user limit exceeded.  
12306 PEAP authentication succeeded  
11503 Prepared EAP-Success  
11003 Returned RADIUS Access-Reject

ISE調試

最大會話日誌位於prrt-server.log中。若要收集這些內容，請將runtime-AAA元件設定為DEBUG級別(導航到Administration > System > Logging > Debug Log Configuration > PSN)，如下圖所示：



若要獲取File prtt-server.log，請導覽至Operations > Troubleshoot > Download Logs > PSN > Debug Logs。最大會話日誌也收集在端點調試中(操作>故障排除>診斷工具>常規工具>端點調試)。

使用者最大會話檢查已正確通過：

<#root>

```
2017-01-29 08:33:11,310 INFO [Thread-83][] cisco.cpm.prrt.impl.PrRTLoggerImpl -:::::- SessionCache,IN
maxUserSessions=[2]
,SessionCache.cpp:283
2017-01-29 08:33:11,311 INFO [Thread-83][] cisco.cpm.prrt.impl.PrRTLoggerImpl -:::::- SessionCache,IN
user=[Bob] not found in cache due to first time authorization
,SessionCache.cpp:1025
2017-01-29 08:33:11,311 DEBUG [Thread-83][] cisco.cpm.prrt.impl.PrRTLoggerImpl -:::::- SessionCache,DE
checkMaxSessions passed
,SessionCache.cpp:360
2017-01-29 08:33:11,311 INFO [Thread-83][] cisco.cpm.prrt.impl.PrRTLoggerImpl -:::::- SessionCache,IN
```

ISE僅在收到SessionCounter會話的Accounting Start後增加SessionCounter:

<#root>

```
2017-01-29 08:33:11,619 DEBUG [Thread-90][] cisco.cpm.prrt.impl.PrRTLoggerImpl -:::::- Radius,DEBUG,0x
[1] User-Name - value: [Bob]
[4] NAS-IP-Address - value: [10.62.148.79]
[5] NAS-Port - value: [1]
[8] Framed-IP-Address - value: [10.62.148.141]
[25] Class - value: [****]
[30] Called-Station-ID - value: [80-e0-1d-8b-72-00]
[31] Calling-Station-ID - value: [c0-4a-00-14-56-f4]
[32] NAS-Identifier - value: [WLC7]
[40] Acct-Status-Type - value: [
Start
```

```
]
[44] Acct-Session-Id - value: [588da8a0/c0:4a:00:14:56:f4/3789]
[45] Acct-Authentic - value: [RADIUS]
[55] Event-Timestamp - value: [1485678753]
[61] NAS-Port-Type - value: [Wireless - IEEE 802.11]
[64] Tunnel-Type - value: [(tag=0) VLAN]
[65] Tunnel-Medium-Type - value: [(tag=0) 802]
[81] Tunnel-Private-Group-ID - value: [(tag=0) 481]
[26] cisco-av-pair - value: [audit-session-id=0a3e944f00000e7d588da8a0]
[26] Airespace-Wlan-Id - value: [4] ,RADIUSHandler.cpp:2003
```

(...)

```
2017-01-29 08:33:11,654 DEBUG [Thread-83][] cisco.cpm.prvt.impl.PrRTLoggerImpl -:::::- SessionCache,DE
2017-01-29 08:33:11,655 DEBUG [Thread-83][] cisco.cpm.prvt.impl.PrRTLoggerImpl -:::::- SessionCache,DE
```

```
user=[Bob] current user session count=[1]
```

```
,SessionCache.cpp:862
```

使用者最大會話檢查失敗：

<#root>

```
2017-01-29 08:37:00,534 INFO [Thread-75][] cisco.cpm.prvt.impl.PrRTLoggerImpl -:::::- SessionCache,IN
2017-01-29 08:37:00,535 INFO [Thread-75][] cisco.cpm.prvt.impl.PrRTLoggerImpl -:::::- SessionCache,IN
```

```
user=[Bob] is not authorized because current active user sessions=[2] >= max-user-sessions=[2]
```

```
,SessionCache.cpp:1010
```

```
2017-01-29 08:37:00,535 DEBUG [Thread-75][] cisco.cpm.prvt.impl.PrRTLoggerImpl -:::::- SessionCache,DE
2017-01-29 08:37:00,535 DEBUG [Thread-75][] cisco.cpm.prvt.impl.PrRTLoggerImpl -:::::- RadiusAuthoriza
```



## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。