

Configurazione del numero massimo di sessioni utente simultanee su ISE 2.2

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio di rete](#)

[Scenari](#)

[Numero massimo di sessioni per utente](#)

[Configurazione](#)

[Esempio](#)

[Sessione massima per il gruppo](#)

[Configurazione](#)

[Esempio](#)

[Bordi](#)

[Numero massimo di sessioni per utente nel gruppo](#)

[Configurazione](#)

[Esempio](#)

[Sessione massima per il gruppo e Sessione massima per l'utente nel gruppo](#)

[Configurazione](#)

[Esempio](#)

[Limite di tempo contatore](#)

[Configurazione](#)

[Esempio](#)

[Funzionalità sessione massima e accesso guest](#)

[Autenticazione Web centrale](#)

[Autenticazione Web locale](#)

[Risoluzione dei problemi](#)

[Registri attivi Radius](#)

[Debug ISE](#)

Introduzione

In questo documento viene descritto come configurare la funzionalità Maximum Sessions introdotta in Identity Services Engine (ISE) 2.2.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Protocollo RADIUS
- Configurazione 802.1x su controller WLC
- ISE e il suo personale (ruoli)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Identity Service Engine versione 2.2
- Controller LAN wireless 8.0.100.0
- Cisco Catalyst Switch 3750 15.2(3)E2
- Computer Windows 7
- Android Phone con versione 6.0.1
- Android Phone con versione 5.0
- Apple iPad iOS 9.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La funzionalità Sessioni massime consente di controllare e applicare le sessioni in tempo reale per utente o per gruppo di identità. Questo documento è destinato alle sessioni RADIUS, ma può essere usato anche per le sessioni TACACS.

ISE versione 2.2 è in grado di rilevare e creare regole di applicazione basate sulla sessione simultanea di:

- Identità utente: limita il numero di sessioni per utente specifico
- Gruppo di identità - limita il numero di sessioni per gruppo specifico
- Utente in un gruppo - limita il numero di sessioni per utente, appartenente a un gruppo specifico

L'applicazione e il conteggio di una sessione concorrente sono univoci e gestiti da ogni PSN (Policy Service Node). Nessuna sincronizzazione tra i PSN in termini di numero di sessioni. La funzione Sessione concorrente viene implementata nel processo di runtime e i dati vengono memorizzati solo nella memoria. In caso di riavvio del PSN, i contatori MaxSessions vengono reimpostati.

Per il numero di sessioni utente non viene fatta distinzione tra maiuscole e minuscole in relazione ai nomi utente e non viene utilizzata la periferica di accesso alla rete (purché si utilizzi lo stesso nodo PSN).

Esempio di rete



Scenari

Numero massimo di sessioni per utente

Configurazione

Passare a Amministrazione > Sistema > Impostazioni > Sessioni massime come mostrato nell'immagine:

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is Administration > Settings > Max Sessions. The 'User' tab is selected. The configuration shows that the 'Unlimited sessions per user' checkbox is unchecked. The 'Maximum per user' field is set to 2. The left sidebar contains various configuration categories such as Client Provisioning, FIPS Mode, Alarm Settings, Posture, Profiling, Protocols, Proxy, SMTP Server, SMS Gateway, System Time, Policy Sets, ERS Settings, Smart Call Home, DHCP & DNS Services, and Max Sessions.

Per attivare la funzione, deselezionare la casella di controllo Sessione illimitata per utente, che è selezionata per impostazione predefinita. Nel campo Numero massimo di sessioni per utente configurare il numero di sessioni che un utente specifico può avere su ogni PSN. In questo esempio viene impostato su 2.

Questa configurazione interessa anche gli utenti di origini di identità esterne, ad esempio Active Directory.

Esempio

Bob è il nome utente di un account del dominio di Active Directory connesso e collegato al server ISE. User Maximum Sessions è configurato con il valore 2, ovvero non è consentita alcuna sessione per lo stesso utente oltre questo numero (per PSN).

Come mostrato nell'immagine, l'utente Bob si connette con Android Phone e il computer Windows

con le stesse credenziali:

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

Entrambe le sessioni sono consentite perché non viene superato il limite massimo di sessioni. Vedere il registro dettagliato di Radius Live, mostrato nell'immagine:

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

Il passaggio 22081 del criterio Numero massimo di sessioni passato fornisce informazioni sull'esito positivo del controllo del numero massimo di sessioni simultanee.

Una volta avviata la terza connessione con un altro dispositivo e le stesse credenziali, Bob riceve PermitAccess, ma Access-Reject viene inviato all'autenticatore:

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

```

La sessione non è consentita, anche se nel registro Radius Live è presente il profilo di autorizzazione corretto. Per controllare le sessioni attive, selezionare Operazioni > Raggio > Sessioni attive:

Session Status	Action	Endpoint ID	Identity	IP Address	Endpoint Profile
<input type="text" value=""/>		<input type="text" value="Endpoint ID"/>	<input type="text" value="Identity"/>	<input type="text" value="IP Address"/>	<input type="text" value="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

In questo caso, entrambe le sessioni hanno lo stato Started (Avviato), che indica che l'Accounting Start è arrivato su ISE per la sessione. È necessario ricevere l'accounting Radius affinché Max Session funzioni correttamente. Lo stato Authenticated (Session consentita, ma nessun accounting) non viene preso in considerazione durante il conteggio delle sessioni:

Session Status	Action	Endpoint ID	Identity	IP Address	Endpoint Profile	Posture Status	Security Group
<input type="text" value=""/>		<input type="text" value="Endpoint ID"/>	<input type="text" value="Identity"/>	<input type="text" value="IP Address"/>	<input type="text" value="Endpoint Profile"/>	<input type="text" value="Posture Status"/>	<input type="text" value="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		

Sessione massima per il gruppo

Configurazione

Selezionare Amministrazione > Sistema > Impostazioni > Sessioni massime > Gruppo:

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	2	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

Questa configurazione impone un massimo di 2 sessioni per il gruppo di identità interno GroupTest2: è possibile configurare l'imposizione per gruppo solo per i gruppi interni.

Esempio

Alice, Pablo e Peter sono gli utenti del Negozio Interno ISE. Tutti sono membri del gruppo denominato GroupTest2. In base alla configurazione di questo esempio, il valore massimo delle sessioni è impostato su 2 in base all'appartenenza al gruppo.

Network Access Users

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

Pablo e Peter si connettono alla rete con le credenziali del gruppo interno denominato GroupTest2:

Jan 29, 2017 09:25:54.554 AM	<input checked="" type="checkbox"/>		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	<input checked="" type="checkbox"/>		Peter	34:AB:37:60:63:88	Apple-Device	User Identity Groups:GroupTest2	Default >> MaxSession_Test

Quando Alice tenta di connettersi, viene applicato il limite MaxSessions per gruppo:

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

Alice non è autorizzata a connettersi alla rete perché il limite massimo di gruppi di sessioni è utilizzato da Peter e Pablo:

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

Se è stato configurato User Maximum Sessions, entrambe le funzionalità funzioneranno in modo indipendente. In questo esempio, User Max Sessions è impostato su 1 e Maximum Session for Group è impostato su 2.

Max Sessions

User
 Group
 Counter Time Limit

Unlimited sessions per user ⓘ

Maximum per user Sessions ⓘ

Peter è autorizzato in base alla sessione massima per il gruppo (2 sessioni), ma a causa della configurazione delle sessioni massime dell'utente (una sessione) non riesce a connettersi alla rete:

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

Se l'utente è membro di più gruppi contemporaneamente e il numero massimo di sessioni per il gruppo è configurato per tali utenti, dopo la connessione ISE aumenta il contatore del numero massimo di sessioni per la cache del gruppo per ogni gruppo a cui l'utente appartiene.

In questo esempio, Alice e Paolo sono membri di GroupTest1 e GroupTest2. Veronica appartiene solo a GroupTest1 e Peter a GroupTest2

Network Access Users

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	

Max Session for Group è impostato su 2 per GroupTest1 e GroupTest2:

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

Quando Alice e Pablo sono connessi alla rete, superano i limiti di sessione per entrambi i gruppi. Veronica, che appartiene solo a GroupTest1 e Peter, membro di GroupTest2, non è in grado di connettersi perché Max Session per Group ha raggiunto il valore configurato massimo:

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

Numero massimo di sessioni per utente nel gruppo

Configurazione

Passare a Amministrazione > Sistema > Impostazioni > Sessioni massime > Gruppo.

Max Sessions

User	Group	Counter Time Limit		
Expand All Collapse All Filter				
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

Questa configurazione impone un massimo di 2 sessioni per il GroupTest2 del gruppo di identità interno.

Esempio

Alice è membro di GroupTest2:

Network Access Users

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

Questa funzione funziona in modo simile a User Maximum Session - ISE limita il numero di sessioni simultanee che un utente all'interno del gruppo interno specificato può avere. Questa configurazione ha effetto solo sull'utente che appartiene al gruppo configurato.

Alice, in qualità di membro di GroupTest2, può avere due sessioni simultanee. Una volta connessa al terzo dispositivo, ISE restituisce PermitAccess e Access-Reject in base al superamento del valore di Maximum Session for User in Group:

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

Log dettagliati Radius-Live:

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

Se è attivata anche l'opzione Sessioni massime utente, entrambe le funzionalità funzionano in modo indipendente. Se un utente Alice è membro del gruppo GroupTest2 con la sessione massima per l'utente nel gruppo configurato per 2 e contemporaneamente la configurazione di User Max Sessions consente solo una sessione per utente, la priorità sarà User Max Sessions:

Max Sessions

User Group Counter Time Limit

Unlimited sessions per user 

Maximum per user Sessions 

Reset

Save

Quando Alice tenta di connettersi con il secondo dispositivo, ISE restituisce Access-Reject in base al superamento del limite massimo di utenti per sessione:

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

Il motivo del rifiuto può essere controllato nel dettagliato Raggio Live-Log. Il limite massimo di sessioni utente è la causa dell'errore:

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.
12306 PEAP authentication succeeded
11503 Prepared EAP-Success
11503 Returned RADIUS Access-Reject
```

Sessione massima per il gruppo e Sessione massima per l'utente nel gruppo
Configurazione

Passare a Amministrazione > Sistema > Impostazioni > Sessioni massime > Gruppo.

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

Questa configurazione impone un numero massimo di sessioni pari a 3 nel gruppo di identità interno GroupTest2 e un numero massimo di sessioni pari a 2 per l'utente in tale gruppo.

Esempio

Alice e Pablo sono membri di GroupTest2. In base alla configurazione di questo esempio, in GroupTest2 è consentito un massimo di 3 sessioni. ISE garantisce che un singolo utente possa avere al massimo 2 sessioni all'interno di questo gruppo.

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 si connette tramite due dispositivi. Entrambi gli endpoint sono connessi alla rete:

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

Quando Alice tenta di connettersi tramite un terzo dispositivo, l'accesso viene negato e viene

superato il limite massimo di sessioni per l'utente nel gruppo:

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

Se Pablo tenta di accedere alla rete, è in grado di farlo poiché Max Session for Group, GroupTest2, non è ancora pieno:

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

Quando Pablo tenta di accedere alla rete da un secondo dispositivo, non riesce perché ha superato il limite massimo di sessioni per il gruppo (anche se ha solo 1 sessione):

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

Come negli esempi precedenti, se si abilita Sessioni massime utente, questa funzione viene eseguita in modo indipendente.

Limite di tempo contatore

Configurazione

Passare a Amministrazione > Sistema > Impostazioni > Sessioni massime > Limite di tempo contatore.

Max Sessions

User Group Counter Time Limit

Unlimited - no time limit

Delete sessions after 0 Days 0 Hour/s 5 Minutes

Reset Save

Il limite di tempo del contatore è la funzione che specifica l'intervallo di tempo durante il quale la sessione viene conteggiata in termini di cache sessione massima. Questa funzionalità consente di specificare il tempo trascorso il quale il PSN elimina la sessione dal contatore e consente nuove sessioni.

Per attivare la funzione, è necessario deselezionare la casella di controllo Illimitato - nessun limite di tempo che è selezionata per impostazione predefinita. Nel campo modificabile, è possibile impostare il tempo durante il quale la sessione viene presa in considerazione nei contatori di MaxSession.

Tenere presente che le sessioni dopo il tempo configurato non vengono disconnesse o rimosse dal database delle sessioni. Dopo l'ora configurata non è presente alcun CoA (Terminate Chain of Authorization).

Esempio

User Max Session è impostato per consentire una sola sessione per l'utente:

Max Sessions

User | Group | Counter Time Limit

Unlimited sessions per user ⓘ

Maximum per user Sessions ⓘ

Reset Save

Alice si connette alla rete utilizzando l'indirizzo IP alle 11:00:34, la seconda autenticazione avviene alle 11:07 e l'accesso è consentito anche se viene superato il valore User Maximum Session. Entrambe le autenticazioni hanno esito positivo a causa del limite di tempo del contatore.

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 cerca di collegarsi a un altro dispositivo prima che siano trascorsi 5 minuti dall'ultimo passaggio di connessione riuscito. ISE rifiuta l'autenticazione:

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

Dopo 5 minuti dall'ultima autenticazione, Alice è riuscita a connettersi alla rete con un dispositivo aggiuntivo.

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

Nelle sessioni in diretta, è possibile vedere tutte e tre le sessioni nello stato Avviato:

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

Funzionalità sessione massima e accesso guest

Autenticazione Web centrale

Con una sessione configurata in Sessione massima utente, è ancora possibile connettersi con l'account Guest1 per entrambe le sessioni:

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

Per limitare l'accesso guest, è possibile specificare il numero massimo di accessi simultanei nella configurazione Guest Type.

Passare a Centri di lavoro > Accesso guest > Portale e componenti > Tipi guest e modificare l'opzione Numero massimo di accessi simultanei, come mostrato nell'immagine:

Guest Type

Save Close

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

Autenticazione Web locale

Se in Sessione massima utente è configurata una sessione, non è possibile connettersi:

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	

Come per i Live Log Radius, il Guest1 è sempre correttamente autenticato in termini di autenticazione del portale. Dopo che WLC ha inviato la richiesta RADIUS con la seconda sessione per Guest1, ISE nega l'accesso a causa del superamento del limite di utenti:

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.

Risoluzione dei problemi

Registri attivi Radius

Il report dettagliato sul raggio è il primo strumento per la risoluzione dei problemi relativi alla feature MaxSession.

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.

Questo motivo di errore indica che il limite massimo globale di sessioni utente è stato superato per questa sessione/utente, come mostrato nell'immagine:

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.

Questo motivo di errore indica che il limite massimo di sessioni del gruppo è stato superato per questa sessione/utente, come mostrato nell'immagine:

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.

Questo motivo di errore indica che per la sessione o l'utente corrente è stato superato il limite massimo di sessioni per gli utenti del gruppo.

Il controllo della cache MaxSession avviene dopo la selezione del profilo di autorizzazione:

Operazione completata:

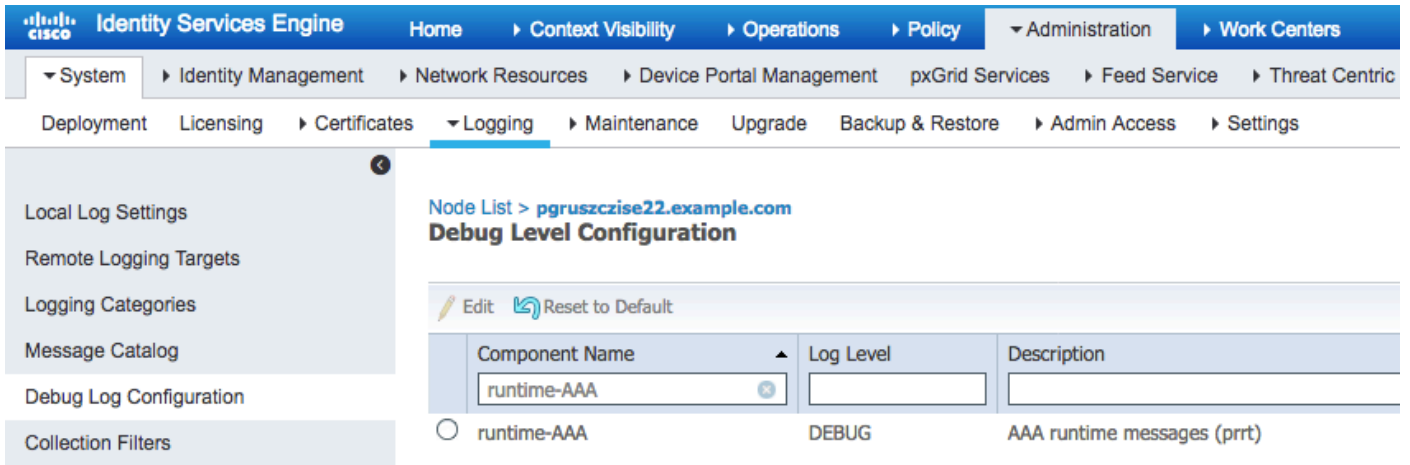
15016 Selected Authorization Profile - PermitAccess
22081 Max sessions policy passed
22080 New accounting session created in Session cache
12306 PEAP authentication succeeded
11503 Prepared EAP-Success
11002 Returned RADIUS Access-Accept

Errore:

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

Debug ISE

Il numero massimo di registri di sessione si trova nel file prrt-server.log. Per raccogliarli, impostare il componente runtime-AAA sul livello DEBUG (selezionare Amministrazione > Sistema > Log > Configurazione log di debug > PSN), come mostrato nell'immagine:



Per ottenere il file port-server.log, selezionare Operazioni > Risoluzione dei problemi > Log di download > PSN > Log di debug. I log sessione max vengono raccolti anche nei debug degli endpoint (Operazioni > Risoluzione dei problemi > Strumenti diagnostici > Strumenti generali > Debug degli endpoint).

Controllo sessione massima utente superato correttamente:

<#root>

```
2017-01-29 08:33:11,310 INFO [Thread-83][] cisco.cpm.prtt.impl.PrRTLoggerImpl -:::::- SessionCache,IN
maxUserSessions=[2]
,SessionCache.cpp:283
2017-01-29 08:33:11,311 INFO [Thread-83][] cisco.cpm.prtt.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.prtt.impl.PrRTLoggerImpl -:::::- SessionCache,DE
checkMaxSessions passed
,SessionCache.cpp:360
2017-01-29 08:33:11,311 INFO [Thread-83][] cisco.cpm.prtt.impl.PrRTLoggerImpl -:::::- SessionCache,IN
```

ISE incrementa SessionCounter solo dopo aver ricevuto l'avvio accounting per la sessione:

<#root>

```
2017-01-29 08:33:11,619 DEBUG [Thread-90][] cisco.cpm.prtt.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
```

Errore di controllo della sessione massima utente:

```
<#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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).