

# Configure Maximum Concurrent User Sessions on ISE 2.2

## Contents

- [Introduction](#)
- [Prerequisites](#)
- [Requirements](#)
- [Components Used](#)
- [Background Information](#)
- [Network Diagram](#)
- [Scenarios](#)
- [Maximum Sessions per User](#)
- [Configuration](#)
- [Example](#)
- [Maximum Session for Group](#)
- [Configure](#)
- [Example](#)
- [Corner Cases](#)
- [Maximum Sessions for User in Group](#)
- [Configure](#)
- [Example](#)
- [Maximum Session for Group and Maximum Session for User in that Group](#)
- [Configure](#)
- [Example](#)
- [Counter Time limit](#)
- [Configure](#)
- [Example](#)
- [Maximum Session Feature and Guest Access](#)
- [Central Web Authentication](#)
- [Local Web Authentication](#)
- [Troubleshoot](#)
- [Radius live logs](#)
- [ISE Debugs](#)

## Introduction

This document describes how to configure the Maximum Sessions feature introduced in the Identity Services Engine (ISE) 2.2.

## Prerequisites

## Requirements

Cisco recommends that you have knowledge of these topics:

- RADIUS Protocol
- 802.1x configuration on Wireless LAN Controller (WLC)
- ISE and its personas (roles)

## Components Used

The information in this document is based on these software and hardware versions:

- Cisco Identity Service Engine version 2.2
- Wireless LAN Controller 8.0.100.0
- Cisco Catalyst Switch 3750 15.2(3)E2
- Windows 7 Machine
- Android Phone running 6.0.1
- Android Phone running 5.0
- Apple iPad iOS 9.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

The Maximum Sessions feature provides a way to control and enforce live sessions per user or per identity group. This document is for RADIUS sessions, but it could be used as well for the TACACS sessions.

ISE version 2.2 can detect and build enforcement policy based on the concurrent session of:

- User Identity - limit number of sessions per specific user
- Identity Group - limit number of sessions per specific group
- User in a Group - limit number of sessions per user, that belongs to specific group

Enforcement and count of a concurrent session is unique and managed by each Policy Service Node (PSN). There is no synchronization between the PSNs in terms of session count. The Concurrent Session feature is implemented in the runtime process, and data is stored only in memory. In case of PSN restart, MaxSessions counters reset.

User session count is case insensitive with regard to usernames, and independent of Network Access Device used (as long as you use the same PSN node).

## Network Diagram



## Scenarios

### Maximum Sessions per User

### Configuration

Navigate to **Administration > System > Settings > Max Sessions** as shown in the image:

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', and 'Administration'. The 'Administration' menu is expanded, showing 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', and 'Feed Service'. The 'System' menu is further expanded to show 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Backup & Restore', and 'Admin Access'. The 'Max Sessions' configuration page is displayed, with the 'User' tab selected. The configuration includes a checkbox for 'Unlimited sessions per user' (unchecked) and a 'Maximum per user' field set to '2' Sessions.

To enable the feature, uncheck **Unlimited session per user** checkbox, which is checked by default. In the **Maximum per user Sessions** field, configure number of sessions specific user can have on each PSN. In this example, it is set to 2.

Users from External Identity Sources (for example, Active Directory) are affected by this configuration as well.

### Example

Bob is the username of an account from the Active Directory Domain which is connected and joined to ISE server. User Maximum Sessions is configured with value 2, which means that any session for same user beyond this number is not permitted (per PSN).

As shown in the image, user Bob connects with Android Phone and Windows machine with the same credentials:

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

Both sessions are permitted because maximum sessions limit is not exceeded. See detailed Radius Live log, shown in the image:

## Overview

<b>Event</b>	5200 Authentication succeeded
<b>Username</b>	Bob
<b>Endpoint Id</b>	CC:FA:00:B4:D5:0F
<b>Endpoint Profile</b>	LG-Device
<b>Authentication Policy</b>	Default >> Dot1X >> Default
<b>Authorization Policy</b>	Default >> MaxSession_Test
<b>Authorization Result</b>	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 step provides information that Maximum Concurrent Session check is successful.

Once third connection with another device and same credentials is initiated, Bob receives PermitAccess, but Access-Reject is sent to authenticator:

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

## Overview

<b>Event</b>	5400 Authentication failed
<b>Username</b>	Bob
<b>Endpoint Id</b>	34:AB:37:60:63:88 
<b>Endpoint Profile</b>	Apple-Device
<b>Authentication Policy</b>	Default >> Dot1X >> Default
<b>Authorization Policy</b>	Default >> MaxSession_Test
<b>Authorization Result</b>	PermitAccess

## Authentication Details

<b>Source Timestamp</b>	2017-01-29 08:36:28.882
<b>Received Timestamp</b>	2017-01-29 08:35:35.293
<b>Policy Server</b>	pgruszczise22
<b>Event</b>	5400 Authentication failed
<b>Failure Reason</b>	22089 Max sessions policy failed. Max sessions user li
<b>Username</b>	Bob
<b>Endpoint Id</b>	34:AB:37:60:63:88

```

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

```

Session is not permitted, even though in the Radius live log you can see that it hits the correct Authorization Profile. In order to check the live sessions, navigate to **Operations > Radius > Live Sessions**:

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

In this case, both of the sessions have status Started, which indicates Accounting Start arrived on ISE for the session. It is necessary to receive the Radius Accounting for Max Session to work properly, status Authenticated (Session permitted, but no accounting) is not taken into consideration during session count:

Session Status	Action	Endpoint ID	Identity	IP Address	Endpoint Profile
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

## Maximum Session for Group

### Configure

Navigate to **Administration > System>Settings > Max Sessions > Group**:

## Max Sessions

User **Group** Counter Time Limit

Expand All Collapse All

Name	Description	Max Sessions for Group	Max Sessions for User
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




This configuration enforces 2 sessions as a maximum for internal identity group GroupTest2: You are able to configure the enforcement per Group only for the Internal Groups.

### Example

Alice, Pablo and Peter are the users from the Internal ISE User Store. All of them are members of group named GroupTest2. As per the configuration in this example, maximum value of sessions is set to 2 based on the Group membership.

## Network Access Users

Edit Add Change Status Import Export Delete Duplicate

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

Pablo and Peter connect to the network with their credentials from the Internal Group named GroupTest2:



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

Once Alice tries to connect, MaxSessions limit per Group is enforced:

Jan 29, 2017 09:26:17.812 AM	✗		Alice	CC:FA:00:B4:D5:0F	LG-Device	User Identity C
Jan 29, 2017 09:25:54.554 AM	✓		Pablo	C0:4A:00:14:56:F4	TP-LINK-Device	User Identity C
Jan 29, 2017 09:25:34.984 AM	✓		Peter	34:AB:37:60:63:88	Apple-Device	User Identity C

## 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 is not allowed to connect to the network because Max Session group limit is used up by Peter and 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

## Corner Cases

If User Maximum Sessions is configured, both features work independently. In this example, User Max Sessions is set to 1 and Maximum Session for Group is set to 2.

## Max Sessions

**User** | Group | Counter Time Limit

Unlimited sessions per user ⓘ

Maximum per user  Sessions ⓘ

Peter is permitted based on the Maximum Session for Group (2 sessions), but because of User Max Sessions configuration (one session) he fails to connect to the network:

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

If the user is a member of more than one group at the same time, and the Max Sessions for Group is configured for them, once connected, ISE increases the counter of Max Session for Group cache for every group the user belongs to.

In this example, Alice and Pablo are members of both GroupTest1 and GroupTest2. Veronica belongs only to GroupTest1 and Peter to GroupTest2

### Network Access Users

Status	Name	Description	First Name	Last Name	Email Address
<input type="checkbox"/> Enabled	alice				
<input type="checkbox"/> Enabled	pablo				
<input type="checkbox"/> Enabled	peter				
<input type="checkbox"/> Enabled	veronica				

Max Session for Group is set to 2 for GroupTest1 and GroupTest2:

### Max Sessions

User	Group	Counter Time Limit
<input type="checkbox"/> Expand All <input type="checkbox"/> Collapse All		
Name	Description	Max Sessions for Group
ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (defau...	Unlimited
Employee	Default Employee User Group	Unlimited
GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (d...	Unlimited
GroupTest1		2
GroupTest2		2
GroupTest3		Unlimited
GuestType_Contractor (default)	Identity group mirroring the gues...	Unlimited
GuestType_Daily (default)	Identity group mirroring the gues...	Unlimited
GuestType_Weekly (default)	Identity group mirroring the gues...	Unlimited
OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (def...	Unlimited

When Alice and Pablo are connected to the network, they exceed the session limits for both groups. Veronica, who belongs only to GroupTest1 and Peter, member of GroupTest2 are unable to connect because of Max Session for Group reached the maximum configured value:

✖	🔒		Veronica	10:A5:D0:98:B8:E2	Unknown	User Identity Groups:GroupTest1,Unknown
✖	🔒		Peter	34:AB:37:60:63:88	Apple-Device	User Identity Groups:GroupTest2,Profiled
🟡	🔒	0	Pablo	CC:FA:00:B4:D5:0F	LG-Device	
✅	🔒	+	Pablo	CC:FA:00:B4:D5:0F	LG-Device	User Identity Groups:GroupTest1,User Identity Groups:Gro
🟡	🔒	0	Alice	C0:4A:00:14:56:F4	TP-LINK-Device	
✅	🔒		Alice	C0:4A:00:14:56:F4	TP-LINK-Device	User Identity Groups:GroupTest1,User Identity Groups:Gro

## Maximum Sessions for User in Group

### Configure

Navigate to **Administration > System > Settings > Max Sessions > Group**.

#### Max Sessions

User
  Group
  Counter Time Limit

Expand All
  Collapse All


Name	Description	Max Sessions for Group	Max Sessions
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

This configuration enforces 2 sessions maximum for Internal Identity group GroupTest2.

## Example

Alice is member of GroupTest2:

### Network Access Users

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

This feature works similar to User Maximum Session - ISE limits the number of concurrent sessions User within specified Internal Group can have. This configuration affects only User, who belongs to the configured group.

Alice, as a member of the GroupTest2, can have 2 simultaneous sessions. Once connected with the third device, ISE returns PermitAccess and Access-Reject based on exceeded 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 C
Jan 29, 2017 09:59:56.723 AM			Alice	CC:FA:00:B4:D5:0F	LG-Device	User Identity C
Jan 29, 2017 09:59:00.008 AM			Alice	C0:4A:00:14:56:F4	TP-LINK-Device	User Identity C

Detailed Radius-Live logs:

## 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

If User Maximum Sessions is enabled as well, then both features work independently. If a user Alice is member of the group GroupTest2 with Maximum Session for User in Group configured for 2, and in the same time User Max Sessions is configured to allow only one session per user, User Max Sessions take precedence:

## Max Sessions

User | Group | Counter Time Limit

Unlimited sessions per user 

Maximum per user  Sessions 

When Alice tries to connect with the second device, ISE returns Access-Reject based on Max Session User limit exceeded:

Jan 29, 2017 10:06:00.852 AM			Alice	CC:FA:00:B4:D5:0F	LG-Device	User Identity G
Jan 29, 2017 10:05:28.903 AM			Alice	C0:4A:00:14:56:F4	TP-LINK-Device	User Identity G

The reason for denial could be checked under the detailed Radius Live-Log. Max sessions user limit is the reason for failure:

## 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

```
15036 Evaluating Authorization Policy
15048 Queried PIP - EndPoints.LogicalProfile
15048 Queried PIP - Network Access.AuthenticationStatus
15004 Matched rule - MaxSession_Test
15016 Selected Authorization Profile - PermAccess
22089 Max sessions policy failed. Max sessions user limit exceeded.
12306 PEAP authentication succeeded
11503 Prepared EAP-Success
11003 Returned RADIUS Access-Reject
```

## Maximum Session for Group and Maximum Session for User in that Group

### Configure

Navigate to **Administration > System > Settings > Max Sessions > Group**.

#### Max Sessions

User	Group	Counter Time Limit
------	-------	--------------------

↗ Expand All   ↘ Collapse All

Name	Description	Max Sessions for Group	Max Sessions for User
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

This configuration enforces maximum session of 3 in Internal identity group GroupTest2, and 2 maximum session for User in that group.

### Example

Alice and Pablo are members of GroupTest2. As per configuration in this example, maximum of 3 sessions is allowed in GroupTest2. ISE ensures that single user can have Maximum 2 sessions within this group.



## Network Access Users

Edit	Add	Change Status ▾	Import	Export ▾	Delete ▾	Duplicate
Status	Name	Description	First Name	Last Name	Email Address	
<input type="checkbox"/> Enabled	alice					
<input type="checkbox"/> Enabled	pablo					

Alice connects via two devices. Both endpoints are connected to the network:

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

When Alice is trying to connect via third device, access is denied with Maximum Session for User in Group limit exceeded:

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

### 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

Username Alice

If Pablo tries to access the network, he is able to do so since Max Session for Group, GroupTest2, is not yet full:

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

When Pablo tries to access the network from second device, he fails because he exceeded the Max Session limit for Group (even though he has only 1 session):

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

## 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 l

Username Pablo

As in previous examples, if you enable User Maximum Sessions, it works independently.

## Counter Time limit

### Configure

Navigate to **Administration > System > Settings > Max Sessions > Counter Time Limit**.

### Max Sessions

**User** | **Group** | **Counter Time Limit**

Unlimited - no time limit

Delete sessions after  Days  Hour/s  Minutes ⓘ

Counter Time limit is the feature which specifies the time interval during which session is counted in terms of the Maximum Session cache. This feature allows you to specify the time after which PSN deletes the session from the counter, and allows new sessions.

To enable the feature, you need to uncheck **Unlimited - no time limit** checkbox which is checked by default. In the editable field, you can set the time for how long the session is taken into consideration in the counters of MaxSession.

Keep in mind that sessions after configured time are not disconnected or removed from the session database. There is no Terminate Chain of Authorization (CoA) after configured time.

### Example

User Max Session is set to allow only one session for user:

### Max Sessions

**User** | **Group** | **Counter Time Limit**

Unlimited sessions per user ⓘ

Maximum per user  Sessions ⓘ

Alice connects to the network using the iPad at 11:00:34, the second authentication happens at 11:07, and even though User Maximum Session value is exceeded, access is permitted. Both authentications are successful because of Counter Time limit.

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

Alice tries to connect with another device before 5 minutes from the last successful connection passes, ISE rejects authentication:

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

After 5 minutes from the last authentication, Alice could connect to the network with additional device.

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

On the live sessions, you could see all three sessions in the state Started:

11:12:51.577 AM	Started	Show CoA Actions	CC:FA:00:B4:D5:0F	Alice	10.62.148.14
11:07:29.365 AM	Started	Show CoA Actions	C0:4A:00:14:56:F4	Alice	10.62.148.14
11:00:35.028 AM	Started	Show CoA Actions	34:AB:37:60:63:88	Alice	10.62.148.14

## Maximum Session Feature and Guest Access

### Central Web Authentication

With one session configured under User Maximum Session feature, you are still able to connect with the Guest1 account for both of the sessions:

Jan 29, 2017 12:02:41.587 PM	✓		guest1	CC:FA:00:B4:D5:0F	Unknown	Any,GuestEndp
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
Jan 29, 2017 12:01:37.682 PM	✓		guest1	34:AB:37:60:63:88	Unknown	Any,GuestEndp
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

In order to limit the Guest Access, you can specify the Maximum simultaneous logins in the Guest Type configuration.

Navigate to **Work Centers > Guest Access > Portal & Components > Guest Types** and change **Maximum simultaneous logins** option, as shown in the image:

### 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*

### Local Web Authentication

With one session configured under User Maximum Session, you are unable to connect:

Jan 29, 2017 12:13:22.598 PM	✘		Guest1	CC:FA:00:B4:D5:0F	Unknown	Gue
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	Gue
Jan 29, 2017 12:12:19.629 PM	✔		guest1			Any

As per the Radius Live-logs, the Guest1 is always correctly authenticated in terms of the portal authentication. Once WLC sends the RADIUS request with the second session for the Guest1, ISE denies the access because of exceed user limit:

### 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.

## Troubleshoot

### Radius live logs

Detailed Radius Report is the very first place for troubleshooting the MaxSession Feature.

### 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.

This failure reason indicates that Global Max User Session Limit is exceeded for this session/user, as shown in the image:

## 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.

This failure reason indicates that Group Max Sessions limit is exceeded for this session/user, as shown in the image:

## 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.

This failure reason indicates that Group User Max Sessions limit is exceeded for this session/user.

The check of MaxSession cache happens after Authorization Profile selection:

Success:

```
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
```

Failure:

```

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 Debugs

Max Session logs are located in the prrt-server.log. In order to collect those, set **runtime-AAA** component to DEBUG level ( navigate to **Administration > System > Logging > Debug Log Configuration > PSN**), as shown in the image:

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Administration > System > Logging > Debug Log Configuration > PSN. The page title is "Node List > pgruszczise22.example.com Debug Level Configuration". There are "Edit" and "Reset to Default" buttons. A table shows the configuration for the "runtime-AAA" component.

Component Name	Log Level	Description
runtime-AAA	DEBUG	AAA runtime messages (p

In order to obtain **File prrt-server.log**, navigate to **Operations > Troubleshoot > Download Logs > PSN > Debug Logs**. Max Session logs are collected in the Endpoint Debugs as well (**Operations > Troubleshoot > Diagnostic Tools > General Tools > EndPoint Debug**).

User Maximum Session check correctly passed:

```

<#root>
2017-01-29 08:33:11,310 INFO [Thread-83][] cisco.cpm.prrt.impl.PrRTLoggerImpl -:::::- SessionCache,INF
maxUserSessions=[2]
,SessionCache.cpp:283
2017-01-29 08:33:11,311 INFO [Thread-83][] cisco.cpm.prrt.impl.PrRTLoggerImpl -:::::- SessionCache,INF
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,DEE
checkMaxSessions passed
,SessionCache.cpp:360

```



2017-01-29 08:33:11,311 INFO [Thread-83][] cisco.cpm.prprt.impl.PrRTLoggerImpl -:::::- SessionCache,INF

ISE increments the SessionCounter only after it receives Accounting Start for the session:

<#root>

```
2017-01-29 08:33:11,619 DEBUG [Thread-90][] cisco.cpm.prprt.impl.PrRTLoggerImpl -:::::- Radius,DEBUG,0x7
[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.prprt.impl.PrRTLoggerImpl -:::::- SessionCache,DEE
2017-01-29 08:33:11,655 DEBUG [Thread-83][] cisco.cpm.prprt.impl.PrRTLoggerImpl -:::::- SessionCache,DEE
```

```
user=[Bob] current user session count=[1]
,SessionCache.cpp:862
```

User Maximum Session check failure:

<#root>

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

```
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.prprt.impl.PrRTLoggerImpl -:::::- SessionCache,DEE
2017-01-29 08:37:00,535 DEBUG [Thread-75][] cisco.cpm.prprt.impl.PrRTLoggerImpl -:::::- RadiusAuthorizat
```