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 Maximum Sessions feature introduced in the Identity Services Engine (ISE) 2.2. 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.

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, make sure that you understand the potential impact of any command.

Background information

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. 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:
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:

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Username</th>
<th>MAC Address</th>
<th>Device</th>
<th>Profile</th>
<th>Policy</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 29, 2017 08:34:51.137 AM</td>
<td>02 Bob</td>
<td>C0:FA:0D:45:35:9F</td>
<td>LG-Device</td>
<td>Profiled</td>
<td>Default &gt;&gt; Dot1X &gt;&gt; Default</td>
<td>Default &gt;&gt; MaxSession_Test</td>
</tr>
<tr>
<td>Jan 29, 2017 08:32:17.778 AM</td>
<td>02 Bob</td>
<td>C0:FA:0D:14:56:F4</td>
<td>TP-LINK-Device</td>
<td>Profiled</td>
<td>Default &gt;&gt; Dot1X &gt;&gt; Default</td>
<td>Default &gt;&gt; MaxSession_Test</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Event</th>
<th>5400 Authentication failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Bob</td>
</tr>
<tr>
<td>Endpoint Id</td>
<td>34:AB:37:60:63:88</td>
</tr>
<tr>
<td>Endpoint Profile</td>
<td>Apple-Device</td>
</tr>
<tr>
<td>Authentication Policy</td>
<td>Default &gt;&gt; Dot1X &gt;&gt; Default</td>
</tr>
<tr>
<td>Authorization Policy</td>
<td>Default &gt;&gt; MaxSession_Test</td>
</tr>
<tr>
<td>Authorization Result</td>
<td>PermitAccess</td>
</tr>
</tbody>
</table>

**Authentication Details**

<table>
<thead>
<tr>
<th>Source Timestamp</th>
<th>2017-01-29 08:36:28.882</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received Timestamp</td>
<td>2017-01-29 08:35:35.293</td>
</tr>
<tr>
<td>Policy Server</td>
<td>pgruszc2ise22</td>
</tr>
<tr>
<td>Event</td>
<td>5400 Authentication failed</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>22089 Max sessions policy failed. Max sessions user limit exceeded.</td>
</tr>
<tr>
<td>Username</td>
<td>Bob</td>
</tr>
<tr>
<td>Endpoint Id</td>
<td>34:AB:37:60:63:88</td>
</tr>
</tbody>
</table>

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**:

<table>
<thead>
<tr>
<th>Session Status</th>
<th>Action</th>
<th>Endpoint ID</th>
<th>Identity</th>
<th>IP Address</th>
<th>Endpoint Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Started</td>
<td>Show CoA Actions</td>
<td>CC:FA:00:B4:D5:0F</td>
<td>Bob</td>
<td>10.62.148.145</td>
<td>LG-Device</td>
</tr>
<tr>
<td>Started</td>
<td>Show CoA Actions</td>
<td>C0:4A:00:14:58:F4</td>
<td>Bob</td>
<td>10.62.148.141</td>
<td>TP-LINK-Device</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Session Status</th>
<th>Action</th>
<th>Endpoint ID</th>
<th>Identity</th>
<th>IP Address</th>
<th>Endpoint Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticated</td>
<td>Show CoA Actions</td>
<td>C0:4A:00:14:58:F4</td>
<td>Bob</td>
<td>TP-LINK-Device</td>
<td></td>
</tr>
<tr>
<td>Authenticated</td>
<td>Show CoA Actions</td>
<td>54:AB37:50:53:88</td>
<td>Bob</td>
<td>Apple-Device</td>
<td></td>
</tr>
<tr>
<td>Authenticated</td>
<td>Show CoA Actions</td>
<td>CC:FA:00:B4:D5:0F</td>
<td>Bob</td>
<td>LG-Device</td>
<td></td>
</tr>
</tbody>
</table>

**Maximum Session for Group**

**Configure**

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

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

Once Alice tries to connect, MaxSessions limit per Group is enforced:
Alice is not allowed to connect to the network because Max Session group limit is used up by Peter and Pablo:

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.
Peter should be 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:

If the user is 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

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

Maximum Sessions for User in Group

**Configure**

Navigate to **Administration > System > Settings > Max Sessions > Group**.
This configuration enforces 2 sessions maximum for Internal Identity group **GroupTest2**.

**Example**

Alice is member of GroupTest2:

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 connect with the third device, ISE returns PermitAccess and Access-Reject based on exceeded Maximum Session for User in Group:

Detailed Radius-Live logs:
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:

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:

When Alice tries to connect with the second device, ISE returns Access-Reject based on Max Session User limit exceeded:
The reason for deny could be checked under the detailed Radius Live-Log. Max sessions user limit is the reason of failure:

![Authentication Details](image)

**Maximum Session for Group and Maximum session for User in that Group**

**Configure**

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

Alice connects via two devices, both endpoints are connected to the network:

When Alice is trying to connect via third device, access is denied with Maximum Session for User in Group limit exceeded:
If Pablo tries to access the network, he is able to do so, since Max Session for Group **GroupTest2** is not yet full:

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):

```
Authentication Details

<table>
<thead>
<tr>
<th>Source Timestamp</th>
<th>2017-01-29 10:56:18.248</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received Timestamp</td>
<td>2017-01-29 10:55:24.389</td>
</tr>
<tr>
<td>Policy Server</td>
<td>pgruszczise22</td>
</tr>
<tr>
<td>Event</td>
<td>5400 Authentication failed</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>22097 Max sessions policy failed. Max sessions group limit exceeded.</td>
</tr>
<tr>
<td>Username</td>
<td>Pablo</td>
</tr>
</tbody>
</table>
```

```
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**.

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 delete 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 should be taken into consideration in the counters of MaxSession.

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

#### Example

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

Alice connects to the network using the IPad at 11:00:34, the second authentication happens at 11:07 and even User Maximum Session value is exceeded access is permitted. Both authentications are successful because of Counter Time limit.
Alice tries to connect with another device, before 5 minutes from the last successful connection passes, ISE rejects authentication:

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

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

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:

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:
Local Web Authentication

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

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

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

**Authentication Details**

<table>
<thead>
<tr>
<th>Source Timestamp</th>
<th>2017-01-29 11:09:44.931</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received Timestamp</td>
<td>2017-01-29 11:08:51.051</td>
</tr>
<tr>
<td>Policy Server</td>
<td>pgruszczise22</td>
</tr>
<tr>
<td>Event</td>
<td>5400 Authentication failed</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>22089 Max sessions policy failed. Max sessions user limit exceeded.</td>
</tr>
</tbody>
</table>

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

**Authentication Details**

<table>
<thead>
<tr>
<th>Source Timestamp</th>
<th>2017-01-29 10:42:38.819</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received Timestamp</td>
<td>2017-01-29 10:41:44.988</td>
</tr>
<tr>
<td>Policy Server</td>
<td>pgruszczise22</td>
</tr>
<tr>
<td>Event</td>
<td>5400 Authentication failed</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>22097 Max sessions policy failed. Max sessions group limit exceeded.</td>
</tr>
</tbody>
</table>
This failure reason indicates that Group Max Sessions limit is exceeded for this session/user, as shown in the image:

<table>
<thead>
<tr>
<th>Authentication Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received Timestamp</td>
</tr>
<tr>
<td>Policy Server</td>
</tr>
<tr>
<td>Event</td>
</tr>
<tr>
<td>Failure Reason</td>
</tr>
</tbody>
</table>

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)
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:

```
2017-01-29 08:33:11,310 INFO [Thread-83][] cisco.cpm.prrt.impl.PrRTLoggerImpl -- SessionCache,INFO ,0x7f885e867700,cntx=0000001335,sesn=pgruszczise22/275051099/8,CPMSessionID=0a3e944f00000e7d588da8a0,user=Bob,CallingStationID=c0-4a-00-14-56-f4,SessionCache::onMaxSessionsAznEvent: current global configuration data: auditSessionTtl=[3600], maxUserSessions=[2],SessionCache.cpp:283 2017-01-29 08:33:11,311 INFO [Thread-83][] cisco.cpm.prrt.impl.PrRTLoggerImpl -- SessionCache,INFO ,0x7f885e867700,cntx=0000001335,sesn=pgruszczise22/275051099/8,CPMSessionID=0a3e944f00000e7d588da8a0,user=Bob,CallingStationID=c0-4a-00-14-56-f4,SessionCache::checkMaxSessions: 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,DEBUG,0x7f885e867700,cntx=0000001335,sesn=pgruszczise22/275051099/8,CPMSessionID=0a3e944f00000e7d588da8a0,user=Bob,CallingStationID=c0-4a-00-14-56-f4,SessionCache::onMaxSessionsAznEvent: current global configuration data: auditSessionTtl=[3600], maxUserSessions=[2],SessionCache.cpp:283 2017-01-29 08:33:11,311 INFO [Thread-83][] cisco.cpm.prrt.impl.PrRTLoggerImpl -- SessionCache,INFO ,0x7f885e867700,cntx=0000001335,sesn=pgruszczise22/275051099/8,CPMSessionID=0a3e944f00000e7d588da8a0,user=Bob,CallingStationID=c0-4a-00-14-56-f4,SessionCache::checkMaxSessions passed,SessionCache.cpp:360 2017-01-29 08:33:11,311 INFO [Thread-83][] cisco.cpm.prrt.impl.PrRTLoggerImpl -- SessionCache,INFO ,0x7f885e867700,cntx=0000001335,sesn=pgruszczise22/275051099/8,CPMSessionID=0a3e944f00000e7d588da8a0,user=Bob,CallingStationID=c0-4a-00-14-56-f4,SessionCache::onMaxSessionsAznEvent: create a new session object sessionID=[0a3e944f00000e7d588da8a0]; user=[Bob],SessionCache.cpp:375
```

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

```
User Maximum Session check failure:

```plaintext
2017-01-29 08:37:00,534 INFO [Thread-75][] cisco.cpm.prrt.impl.PrRTLoggerImpl :::::-SessionCache,INFO,0x7fe858a69700,cntx=0000005011,sesn=pgruszczise22/275051099/15,CPMSessionID=0a3e944f00000e7f588da966,user=Bob,CallingStationID=34-ab-37-60-63-88,SessionCache::onMaxSessionsAznEvent: current global configuration data: auditSessionTtl=[3600], maxUserSessions=[2],SessionCache.cpp:283
```

```plaintext
2017-01-29 08:37:00,535 INFO [Thread-75][] cisco.cpm.prrt.impl.PrRTLoggerImpl :::::-SessionCache,INFO,0x7fe858a69700,cntx=0000005011,sesn=pgruszczise22/275051099/15,CPMSessionID=0a3e944f00000e7f588da966,user=Bob,CallingStationID=34-ab-37-60-63-88,SessionCache::checkMaxSessions: user=[Bob] is not authorized because current active user sessions=[2] >= max-user-sessions=[2],SessionCache.cpp:341 2017-01-29 08:37:00,535 DEBUG [Thread-75][] cisco.cpm.prrt.impl.PrRTLoggerImpl :::::-RadiusAuthorization,DEBUG,0x7fe858a69700,cntx=0000005011,sesn=pgruszczise22/275051099/15,CPMSessionID=0a3e944f00000e7f588da966,user=Bob,CallingStationID=34-ab-37-60-63-88,RadiusAuthorization:::onResponseMaxSessionsAznEvent return from SessionCache,RadiusAuthorization.cpp:371
```