## Error A required privilege is not held by the client when building Windows PE

Windows PE rescue media creation fails and the following may be seen the the Windows PE log file:

ImageX Tool for Windows Copyright (C) Microsoft Corp. All rights reserved. Version: 6.2.9200.16384 Mounting: [C:\boot\macrium\WADKFiles\media\sources\boot.wim, 1] -> [C:\boot\macrium\WADKFiles\mount]... [ 0% ] Mounting progress Error mounting image. A required privilege is not held by the client.

This error may indicate that default Windows security settings have been to be modified. Typically, this is caused by Anti-Virus/Security software or by incorrect 'Administrator' group assignments.

Note: To view the Windows PE log file click the 'View Log' button in the 'Prepare Windows PE Image' wizard page:

Rescue Media	a Wizard	
Prepare	Windows PE Ir	nage
Select you	r architecture and WIM	Type, then press next
Use the W	indows Assessment and	Deployment Kit to prepare the Reflect PE image
Build the	PE Environment	
	PE Architecture:	64Bit 🗸
61.2	Include optional cor	mponents - required for iSCSI and BitLocker support unlock BitLocker encrypted drives
	Default base WIM (Recommended)	C:\ProgramData\Macrium\Reflect\Windows Kits\8.0\\winpe.wim
	○ Custom base WIM	
For adva	anced users, a custom W	IM enables you to prepare your own Windows PE environment.
Mounting t	he Windows Image File	
View Lo	g	Please press the <b>Next</b> button to continue.
	Help	< Back Next > Cancel Finish
To resolve follo	w the steps below:	

## Ensure that your Windows User Account is a member of the Administrators Group

1. Start the Windows 'Computer Management' console by running 'compmgmt.msc'

In Windows 10 type **compmgmt.msc** in the search box:

	📕 My s	stuff		Q	Web
-	compmg	mt.msc			
In Window	vs 7 and Vista o pmgmt.msc	click 'Start' an	nd type cor	npmg	jmt.msc:
<b>@</b>	6		0		

2. Navigate to 'Local Users and Groups' > 'Groups', then right click on 'Administrators' and select 'Add to group'.

Somputer Management (Local	Name	Description
V 🙀 System Tools	Access Control Assist	Members of this group can remot
> ( Task Scheduler	Administrators	Add to Group
> 🛃 Event Viewer	🗿 Backup Operators	rride se
> 👸 Shared Folders	A Cryptographic Ope	All Tasks > perfor
<ul> <li>Local Users and Groups</li> </ul>	A Distributed COM U	Unch, a
Groups	Not the Readers	n read e
> ( Performance	A Guests	Rename ess as m
A Device Manager	🜆 Hyper-V Administra	Properties ve com
✓ <a>Array</a>	A IIS_IUSRS	ernet Inf
🔤 Disk Management	👰 Network Configura	Help have s
> 🛃 Services and Applications	A Performance Log Users	Members of this group may sche
	nterformance Monitor	Members of this group can acces
	A Power Users	Power Users are included for back
I I	1 All 1 1 1 1 1 1	A.A. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1.

3. If your user account isn't in the list then <b>click the Add bu</b>
--

Administrators Properties	?	×	
General			
Administrators			
Description: Administrators have complete a to the computer/domain	nd unrestricted a	iccess	
Members:			
Add Remove Changes to a u are not effectiv user logs on.	iser's group mem e until the next ti	bership me the	
	Apply	Help	
UK Cancel			
ter your account name and click 'OK'.			
Iter your account name and click 'OK': Select Users			
ter your account name and click 'OK': Select Users			
Select this object type: Users or Built-in security principals		Object	Types
The second secon		Object	Types
Inter your account name and click 'OK': Select Users Select this object type: Users or Built-in security principals From this location:		Object	Types
the point of		Object Loca	Types
OK     Cancel       Inter your account name and click 'OK':       Select Users       Select this object type:       Users or Built-in security principals       From this location:       Image: Enter the object names to select (examples):       John		Object Loca Check	Types tions

## Ensure that the 'Administrators' Group is assigned to the 'Auditing and Security log'

1. Start the 'Local Group Policy Editor' by running 'gpedit.msc'.



The above example shows Windows 10. For other versions of Windows click the 'Start' button or press the Windows key and type 'gpedit.msc'

2. Navigate to 'Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment' and select 'Manage audit and security log'':

I Local Group Policy Editor	_		×	
File Action View Help				
<ul> <li>Cocal Computer Policy</li> <li>Computer Configuration</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Windows Settings</li> <li>Mame Resolution Policy</li> <li>Scripts (Startup/Shutdown)</li> <li>Security Settings</li> <li>Security Settings</li> <li>Security Settings</li> <li>Security Settings</li> <li>Security Settings</li> <li>Security Optices</li> <li>Security Options</li> <li>Windows Firewall with Advanced Security and security log</li> <li>Modify an object label</li> <li>Modify an object label</li> <li>Modify an object label</li> <li>Modify firmware environment values</li> <li>Sefurity Policies</li> <li>Software Restriction Policies</li> <li>Software Restriction Policies</li> <li>Software Restriction Policies</li> <li>Modify an object label</li> <li>Modify firmware environment values</li> <li>Perform volume maintenance tasks</li> <li>Profile single process</li> <li>Profile single process</li> <li>Profile single process</li> <li>Profile softe and directories</li> <li>Advanitistative Templates</li> <li>Churd aver the protive</li> <li>Churd aver the protive</li> <li>Churd aver the protive</li> <li>Churd aver the protive</li> <li>Software Restriction Policies</li> <li>Software Restriction Policies</li> <li>Software Restriction Policies</li> <li>Software Restriction Policies</li> <li>Churd aver the protive</li> <li>Churd aver the protive</li> <li>Churd aver the protive</li> </ul>	ega	Security Adminis LOCAL S LOCAL S Users, Sy Adminis Adminis NETWO Adminis Adminis Adminis Adminis Adminis Adminis Adminis	Sett stratc SERV SERV sterr stratc stratc stratc stratc stratc stratc stratc stratc stratc stratc stratc	
			>	

3. Double click on 'Manage audit and security log' to display the Properties dialog:

Manage auditing and security log Properties	?	$\times$
Local Security Setting Explain		
Manage auditing and security log		
Add User or Group Remove		
OK Cancel	Ap	ply

4. Ensure that the 'Administrators' user group is shown, if not then click 'Add User or Group' then click the 'Object Types' button and s elect 'Groups'.



5. Enter 'Administrators' and click	'OK':		
Select Users or Groups			×
Select this object type:			
Users, Groups or Built-in security	y principals		Object Types
From this location:			
			Locations
Enter the object names to select	: ( <u>examples</u> ):		
Administrators			Check Names
Advanced		OK	Cancel
		OIN	
6. Finally <b>click 'OK'</b> to save the chan	ges:		2 ~
Manage auditing and security	roperties		· ^ ·
Local Security Setting Explain	1		
Manage auditing an	nd security log		
Administrators			
Administrators			
Add User or Group	Remove		
	ОК	Cancel	Apply