

## Ldap error - not permitted to logon at this workstation

2022/05/09 17:45 - Admin Redmine

<b>ステータス:</b>	New	<b>開始日:</b>	2022/05/09
<b>優先度:</b>	通常	<b>期日:</b>	
<b>担当者:</b>		<b>進捗率:</b>	0%
<b>カテゴリ:</b>	LDAP_28	<b>予定工数:</b>	0.00時間
<b>対象バージョン:</b>		<b>作業時間:</b>	0.00時間
Redmineorg_URL:	https://www.redmine.org/issues/20699	status_id:	1
category_id:	28	tracker_id:	1
version_id:	0	plus1:	0
issue_org_id:	20699	affected_version:	
author_id:	111839	closed_on:	
assigned_to_id:	0	affected_version_id:	90
comments:	4		

**説明**

I configured "LDAP authentication" for our Active Directory.  
On Windows 2003 server x68 and Windows 2012 server x64 login attempts ends with the error (logged using WireShark):

```
LDAPMessage bindResponse(1) invalidCredentials (80090308: LdapErr: DSID-0C090334, comment: AcceptSecurityContext error, data 531, vece)
```

which means "not permitted to logon at this workstation". The solution is to add AD server to "userWorkstations" list of each domain user, and it works. But it is a bad solution and our administrators does not accept this.  
This behavior was commented a year ago:  
#1913#note-29

journals

I had the same problem with you. Have you solved this problem without adding AD server to "userWorkstations" list of each domain user?

xuezhi li wrote:

I had the same problem with you. Have you solved this problem without adding AD server to "userWorkstations" list of each domain user?

No, currently I`m using solution with Apache + sspi mod :(  
<http://www.redmine.org/boards/2/topics/127?page=2>

I used this patch for auth\_source\_ldap to enable ldap authentication in my situation.  
The idea is based on this description of "error 531" and confirmed with my tests:

```
80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 531, v893
HEX: 0x531 - not permitted to logon from this workstation
DEC: 1329 - ERROR_INVALID_WORKSTATION (Logon failure: user not allowed to log on to this computer.)
LDAP[userWorkstations: ]
NOTE: Returns only when presented with valid username and password/credential.
```

So, if this error was returned - username / password are ok, and I return "true" as a authenticate\_dn result.

I understand that searching in error text is not very good solution, but I don`t have any

other, and it works.

---

#### 履歴

---

#1 - 2022/05/10 17:08 - Admin Redmine

- カテゴリをLDAP\_28 にセット