Account Lockout – How to unlock user AD account

KB0013378  -  [v7.0](javascript:void(0))

7 views

**Administrative Reference for KB:**Account Lockout – How to unlock user AD account

**Audience:** Verint IT

**KB Content:**Account Lockout, Disabled / Inactive

User contact helpdesk stating that they are unable to login to machine or connect to VPN or access any application or resources, GSD analyst should verify if the users AD account is locked.

**Account lockout:**

Account lockout policies are used by OS / administrators to lock out an account when someone tries to logon unsuccessfully several times in a row.

**Verint account lockout policy:**

1. Account Lockout Duration:  60 minutes (the duration that a locked-out account remains locked out before automatically getting unlocked)
2. Account lockout threshold:  5 invalid logon attempts (Number of invalid logon attempts that will cause a user account to get locked)
3. Reset account lockout counter after 60 minutes (Number of minutes that must elapse from the time the user fails to login before the failed logon attempt counter is reset to 0).

GSD could unlock any account which is locked out in Active Directory.

* User AD account (Ex: Username)
* System/Domain Admin accounts (Ex: Sa\_username)
* Service Account (Splunk user / F5 account etc)
* Shared Mailbox

**Note:**

* **GSD will never change password or enable** any System/domain admin account or Service Account.
* **GSD will never unlock a disabled / inactive account.**
* In cases where user account is Terminated / disabled, **GSD will never inform the user that the account is TERMINATED**or the **reason for Termination**. In such scenarios, team will inform the user that the account is disabled and the ticket should be transferred to the respective region based T2\_Services team as **hot transfer.**
* User account disablement issues which is due to any Change/ Automation/ Scripts (as a part of offboarding/ clean up changes or any other related activities), the ticket should be **Hot transferred to the respective T2 Services team** immediately with detailed documentation on our investigation and user inputs. These tickets should not be transferred to HR team or user should not be directed to HR.
* Enabling a disabled user account would be processed strictly as per defined SOC compliance protocol - **KB0012982 - Handling of SOC disabled accounts.**
* Password reset for any of the user account would be processed based on Verint password policy - **KB0012759 - Verint - Password Expiry and Reset Process**
* Whenever a user reports account lockout, ensure to check ticket history from **Service Now** next to username in ticket.
* Probe and understand if the issue reoccurred within last 30 days and document on the ticket.
* If it is a frequent account lockout, refer **KB0012753** - Frequent Account Lockout

**Process to unlock a user account:**

Verify if user account is active in Active Directory, **do not unlock an inactive/disabled** user account. Refer the section below **“If the user account is inactive / disabled”** to verify.

**Preferred method: KB0013290 - Self-Service Password Reset (SSPR)**

* Guide user to login to **ServiceNow Self Service portal** and access SSPR process **(Self-Service Password Reset (SSPR))** by searching the KB number **KB0013290.**
* If user is unable to access ServiceNow self-service page, guide user to open the below url from a browser from PC/ laptop/ mobile device/ tablet to access Microsoft password reset portal:

[**https://passwordreset.microsoftonline.com/**](https://passwordreset.microsoftonline.com/)

* If user doesn’t have access to any devices to perform Account unlock, follow the below steps:

* **From Active Directory Users and Computers**, click on Search Object icon to search an object (User / Computer)

* Click on **Find Users** to search for user from **Contacts and Groups** dialog box
* Enter the username in **Name: Textbox**and click**Find Now**

**If the user account is inactive / disabled**

* When you search for the user in Active directory, if the user icon is marked with a down arrow as shown in the below image, the respective user account is inactive (Account disabled).
* Account inactive status is applicable only for **User account (Type: User)**in Active Directory and it’s not applicable for Mailboxes.
* Mailboxes which are migrated to cloud from on-premises would be in inactive status in AD but active in Exchange admin center.
* If user account is disabled, verify if it is disabled by SOC by referring the comments in the description field in AD user account properties. If yes, follow the **KB0012982 - Handling of SOC disabled accounts.**

* If the user account is disabled, due to any other reasons (incorrect account end date in Oracle and AD or by referencing any other tickets), move the ticket to respective region T2\_Services queue in Service Now following **hot transfer.**
* If user is a contractor and rejoining the company, the account enablement process would be handled by HR based on the request from user’s manager as part of onboarding process. For such scenarios, GSD analyst could raise a TCKT for General inquiry updating the detailed log and inform the user to contact their managers for guidance.

**User Account disablement via UiPath Automation:**

Some user accounts have been disabled via UiPath Automation. These accounts have been disabled based on HR request.

Please suggest the users to contact their Manager or regional HR partners to get the issue fixed, since IT cannot help on this issue.

**If the user account is active**

* Right Click on the Object (Username) and select properties.

* Account tab would display the information if the account is locked.

* If the account is locked, the error message would be displayed.
* To unlock click on the highlighted check box.
* Click Apply and Ok

* This would unlock the user account and user would be able to access the account.

If user is unable to login to machine or any applications, check for password expiry by following **KB0012759 - Verint - Password Expiry and Reset Process.**