SAMT Administrator Notifications Explained

EDCS-23343735

SAMT Administrator Notifications & Emails

Cisco provides SAMT Administrators two methods to receive information and updates regarding user access:

To view notifications, click the 🔔 Icon located at the top right corner in SAMT. Notifications are also delivered via email.
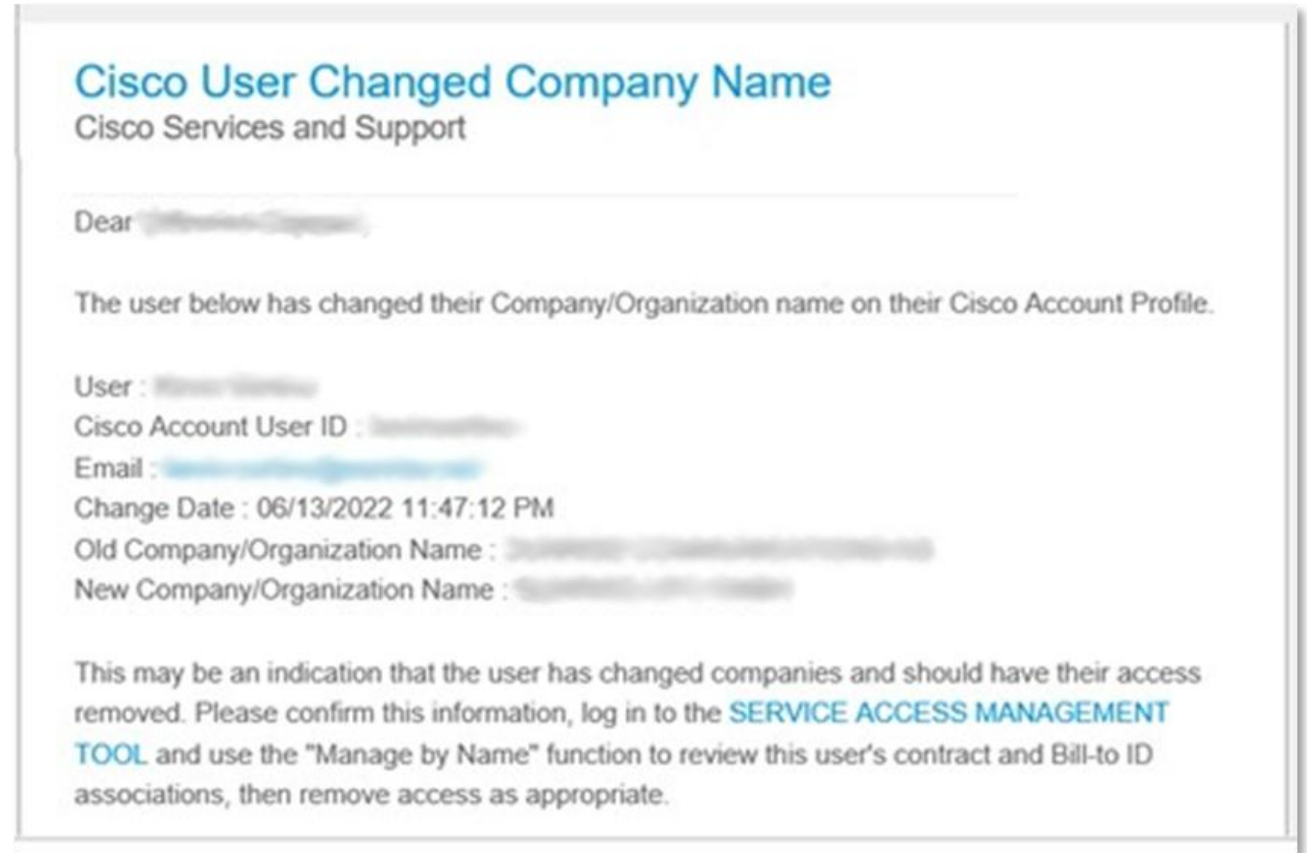
SAMT notifications and email notifications can be adjusted from "Preferences" which is symbolized by a wheel ⚙ icon at the top right corner in SAMT

User Profile Updates

SAMT provides a notification when a user who has access to contract(s) changes their company name.

This change may indicate that the user has changed companies and should no longer have access to one or more contracts or Bill to IDs.

SAMT Admins should review these notifications and take appropriate action to remove or adjust support access, as needed.

Cisco User Changed Company Name
Cisco Services and Support

Dear

The user below has changed their Company/Organization name on their Cisco Account Profile.

User :
Cisco Account User ID :
Email :
Change Date : 06/13/2022 11:47:12 PM
Old Company/Organization Name :
New Company/Organization Name :

This may be an indication that the user has changed companies and should have their access removed. Please confirm this information, log in to the SERVICE ACCESS MANAGEMENT TOOL and use the "Manage by Name" function to review this user's contract and Bill-to ID associations, then remove access as appropriate.
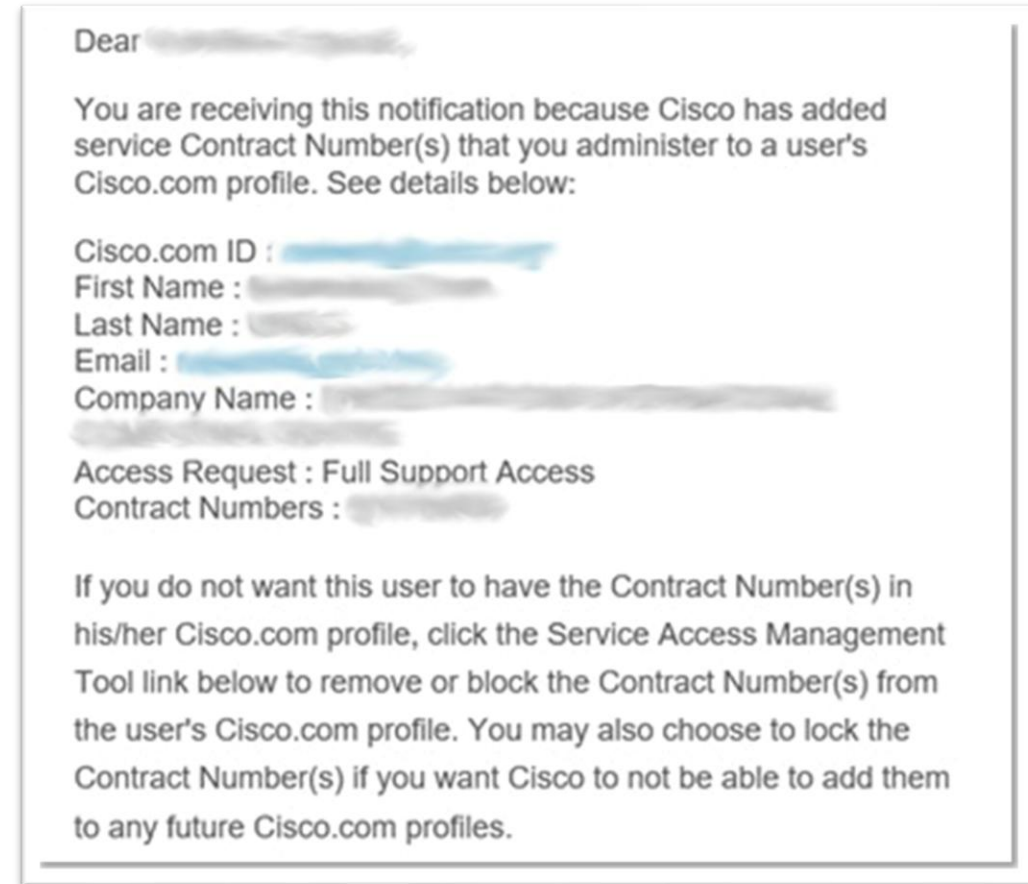
Updates Made by Cisco Support

SAMT provides a notification to SAMT Admins when Cisco makes any of the following changes related to a Bill to ID or contract :
- Attempt to Associate a Blocked Contract
- Contract Access Added or Removed
- Bill to ID Access Added or Removed
- Additional SAMT Admins Onboarded

SAMT Admins should review these notifications and take appropriate action to remove or reinstate support access, as needed.

Dear

You are receiving this notification because Cisco has added service Contract Number(s) that you administer to a user's Cisco.com profile. See details below:

Cisco.com ID :
First Name :
Last Name :
Email :
Company Name :

Access Request : Full Support Access
Contract Numbers :

If you do not want this user to have the Contract Number(s) in his/her Cisco.com profile, click the Service Access Management Tool link below to remove or block the Contract Number(s) from the user's Cisco.com profile. You may also choose to lock the Contract Number(s) if you want Cisco to not be able to add them to any future Cisco.com profiles.
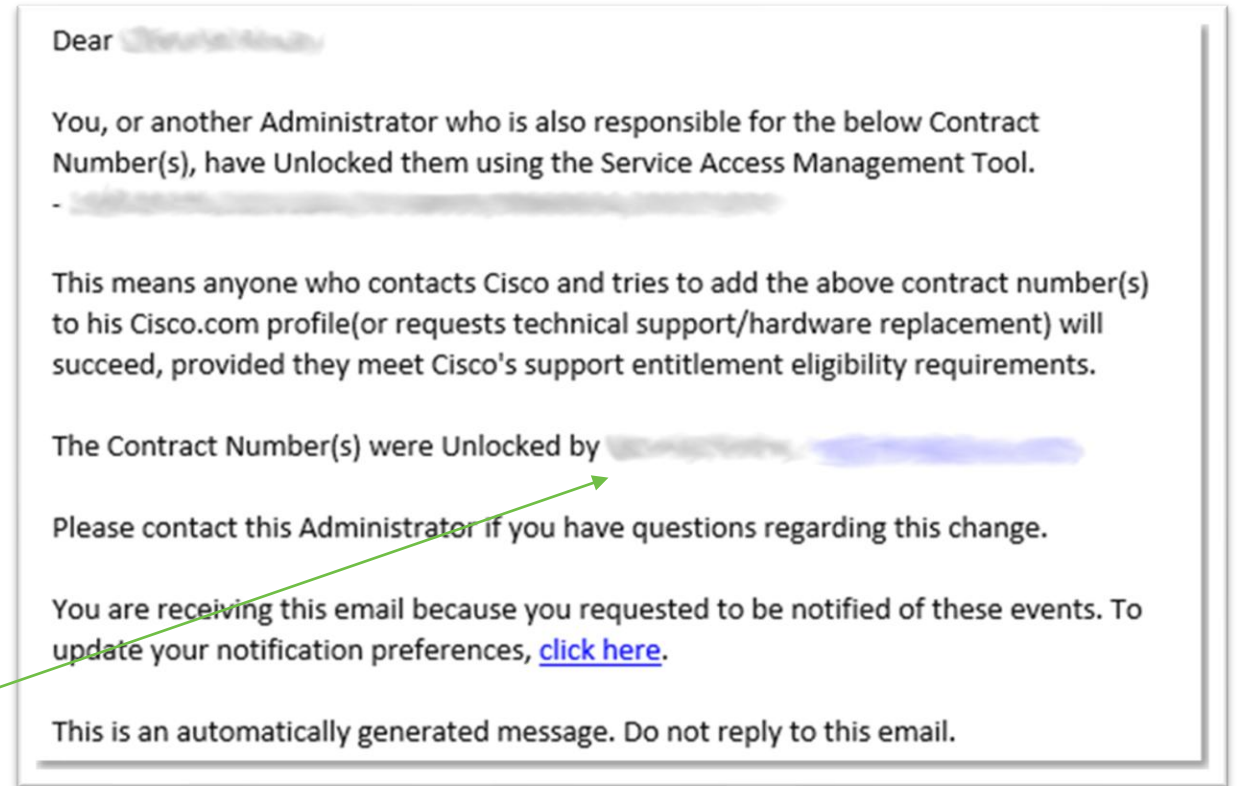
Peer SAMT Administrator Notifications

SAMT provides notifications when a peer SAMT Administrator performs any of the following related to a Bill to ID or contract:

- Contract Locked or Unlocked
- Bill to ID Locked or Unlocked
- Contract Blocked or Unblocked (from a User)
- Bill to ID Blocked or Unblocked (from a User)
- Peer Admin Onboarded
- Administrator has set up a Proxy SAMT Admin
- A Group you manage has been shared/ unshared by a Peer Admin

SAMT Admins should review these notifications and take appropriate or contact their peer SAMT Admin to discuss.

Dear

You, or another Administrator who is also responsible for the below Contract Number(s), have Unlocked them using the Service Access Management Tool.
-

This means anyone who contacts Cisco and tries to add the above contract number(s) to his Cisco.com profile(or requests technical support/hardware replacement) will succeed, provided they meet Cisco's support entitlement eligibility requirements.

The Contract Number(s) were Unlocked by

Please contact this Administrator if you have questions regarding this change.

You are receiving this email because you requested to be notified of these events. To update your notification preferences, click here.

This is an automatically generated message. Do not reply to this email.

Peer Administrator User Access Association notifications

SAMT provides notifications when a peer SAMT Admin of a contract or Bill-to ID makes any of the following changes:

- Contract Added or Removed from a User Profile
- Bill to ID Enabled or Disabled for Support for a User Profile

SAMT Admins should review these notifications and take appropriate or contact their peer SAMT Admin to discuss.

Dear ~~[redacted]~~,

You, or another Administrator who is also responsible for the below Contract Number(s), have Deleted them from Cisco.com profile(s) - ~~[redacted]~~ using the Service Access Management Tool.

The Contract Number(s) were Deleted by ~~[redacted]~~

Please contact this Administrator if you have questions regarding this change.

This is an automatically generated message. Do not reply to this email.

Contract Change Notifications

SAMT provides notifications when an additional end customer company is added or removed from a contract.

SAMT Admins should review the changes and manage user access, as needed. Questions about the change should be sent to the company's purchasing representative or a case can be opened with Cisco commerce operations support (cs-support@cisco.com).

New Install-at Parent Company added to Contract

Dear ▓▓▓▓▓▓▓,

The following new Install-at Parent Companies have been added to contract ▓▓▓▓▓, that you manage:

- ▓▓▓▓▓▓

Please use SAMT to onboard or update users or admins, as needed.

If you have any questions or believe this contract change was made in error, please contact your service seller, purchasing contract administrator, or Cisco commerce support cs-support@cisco.com.

This is an automatically generated message. Do not reply to this email.

Bill-to ID User Access Revalidations

SAMT Bill to ID Admins are required to revalidate users who have access to support via a Bill to ID every 6 months.

- SAMT sends a notification 30 days prior to the revalidation due date.
- If revalidation of Bill-to ID user(s) does not occur, a 15-day notice is issued.
- If the Bill to ID user(s) are still not revalidated, a one-day notice is issued before the Bill to ID(s) are put into "Overdue" revalidation status.

SAMT Admins should follow the directions to review the users with access to the Bill-to ID. Then, remove any users who should no longer have access and certify revalidation is complete.

Users Authorized for Service Using Bill to ID(s) Require Validation - 1 Day Notice
Cisco Services and Support

Dear ▓▓▓▓▓▓▓▓,

The revalidation of users' access to Cisco services is imperative to ensuring that only authorized people have access. Cisco requires a 6-month revalidation of users granted access through Bill-to IDs. The following Bill to ID(s) that you manage are due for revalidation before 03/31/2022.

Total No of Bill to IDs to be revalidated: 1

Bill to IDs requiring user revalidation include the following. Please log into SAMT to view all: ▓▓

How to Revalidate:

1. Log into the Service Access Management Tool ("SAMT")
2. Click here for step by step instruction for re-validating Bill-To ID users.

When the revalidation date passes without action by a SAMT Bill-to ID Admin, the Bill to ID revalidation will be considered overdue. Once overdue, additional users cannot be granted access to the Bill-to ID within SAMT, and any current user with access to the Bill-to ID whose stated parent company does not relate to the Bill-to company will have their access ID revoked. Users whose access has been revoked may re-request access through profile. However, if the Bill-to ID revalidation is still overdue, SAMT Bill-to ID Admins able to process the request in SAMT. Any Bill-to ID user whose parent company rel Bill-to parent company will keep access, as granted, even when the Bill-to ID reval overdue status. Once a SAMT Admin has indicated within SAMT that revalidation is the next revalidation will be due in 6 months. Revalidation may be performed at any longer than 6 months from the prior revalidation completion date.

You will not receive any other reminders before the revalidation is considered overd

MANDATORY NOTIFICATION

Cisco User Bill to ID Support Access Removed
Cisco Services and Support

Dear ▓▓▓▓▓▓▓▓,

The following Bill to ID support access has been removed from the user listed below. Cisco was unable to confirm the user's association with the Bill-to company and support access was not revalidated by a SAMT Bill to ID Administrator. The user will be notified. Bill-to user revalidation is required before support access may be granted to any users.

Requestor's Name : ▓▓▓▓▓
Cisco Account User ID : ▓▓▓▓▓▓▓
Email : ▓▓▓▓▓▓▓
Company/Organization : ▓▓▓▓▓▓▓

Bill to ID : ▓▓▓▓▓
Bill to ID Company : ▓▓▓▓▓

Contract Access Revalidations

Contract Bill-to and Install-at Admins are required to revalidate users who have access to support via a contract every 6 months.
SAMT sends a notification 30 days prior to the 6-month due date.
If revalidation of Bill-to ID user(s) does not occur, a 15-day notice is issued.
If the Bill to ID user(s) are still not revalidated, a one-day notice is issued before the Bill to ID(s) are put into "Overdue" revalidation status.
SAMT BID Admins cannot associate users to Bill-to IDs in "Overdue" status but can remove users.

SAMT Admins should log into SAMT and follow the directions to review the users with access to the contract(s). Then, remove any users who should no longer have access and certify revalidation is complete

Users Authorized for Service Require Validation - 15 Day Notice
Cisco Services and Support

Dear ████████,

You must revalidate the users authorized to obtain service for the following contracts by 06/17/2022.

Total No of contracts to be revalidated : 1

Contract(s) requiring validation include the following. Please log into SAMT to view all:
████████

How to Revalidate:

1. Log into the Service Access Management Tool ("SAMT")
2. Click here for the step-by-step instructions for revalidating the contract(s).

If you do not revalidate the contracts, you will not be able to associate new users because the contract will be in Overdue Revalidation Status.

You will receive 1 more reminder before the contracts become overdue.

MANDATORY NOTIFICATION

User Access Messages, Reminders, & Cancellations

SAMT sends a notification when a user sends a message regarding access to a contract or Bill to ID to the SAMT Administrator.

Additionally, SAMT sends reminders when requests are pending in the Admin's inbox for at least 1 week and action is required. If action is not taken, requests are cancelled after about 30 days.

SAMT Admins should review the notifications and act, if needed.

MANDATORY NOTIFICATION

Access requests pending for your review

Dear ▓▓▓▓,

You currently have requests pending your review and action for over a week in SAMT. Any requests that are not processed within 4 weeks of the request date will be cancelled and removed from the pending requests queue. Upon cancellation, a message will be sent to the SAMT Administrators and requestor.

Please log into SAMT as soon as possible to review and take action on your pending access requests.

Thank you,
Cisco Account Support.

Cisco Contract Access Request Cancelled
Cisco Services and Support

Dear ▓▓▓▓,

The following access request submitted to you on Request Date : 04/14/2022 07:03:02 AM has been cancelled due to no response by an Administrator. The request will no longer be accessible within SAMT. The requestor will be notified.

Requestor's Name : ▓▓▓▓
Cisco Account User ID : ▓▓▓▓
Email : ▓▓▓▓
Company/Organization : Cisco Systems, Inc.
Access Request : Full Support Access
Contract : ▓▓▓▓
Status : CANCELLED
Request Date : 04/14/2022 07:03:02 AM
Cancelled Date : 05/14/2022 10:37:05 PM

Thank you,
Cisco Account Support