Service Access Management Tool

"SAMT"

Overview & Guide for Contract Administrators

(Bill-To and Install-At)

Table of Contents

Welcome

The Services Access Management Tool (“SAMT”) enables Cisco’s customers and partners to self-administer and manage user access to contracted Cisco services that may include technical support services, advanced hardware replacement, software upgrades and/or Cisco.com access. SAMT provides proactive self-service access management, allowing Cisco customers and partners to run their business more efficiently. This guide has been created to aid SAMT Administrators and assist with understanding service contract access management and how to effectively use SAMT to grant and control user access.

Cisco.com User Profile (“User Profile”)

All individuals that interact with Cisco’s services, tools, and other information, must create, and maintain a Cisco.com User Profile account on Cisco.com. Prior to receiving technical support services from Cisco, individuals need to visit Cisco.com to create a User Profile or to log into their existing Cisco.com User Profile and request contract access.

Every Cisco.com User Profile is associated with an individual person, dictates entitlement to services from Cisco and may include, among other things, the person's contact information, the customer organization that the person represents, the Contract Numbers and/or Bill-To IDs under which the person is entitled to receive Cisco services, and other appropriate information provided by the user and/or collected by Cisco regarding the user's history and interactions with Cisco.

Cisco uses the information provided within a Cisco.com User Profile, such as email address and company information, to associate the User Profile to a Parent Company (also referred to as a Global Ultimate.) A Parent Company/ Global Ultimate (“GU”) is the top-level of a company hierarchy. Every Parent Company/ GU has an associated identification number designation known as the GU ID. Within a company hierarchy may be one or more Bill-To accounts, each with their own assigned Bill-To ID (“BID”.) Cisco creates a Bill-To and Bill-To ID when a company buys services directly from Cisco. One or more Bill-To IDs may roll up to a Parent Company/ GU hierarchy.

Contract Entitlement

All Cisco service contracts contain a Bill-To Company/Bill-To ID and Install-At GU IDs, Entitled Party, as well as other important information. The “Entitled Party” of a contract is Bill-To or Install-At, depending on the service levels within the contract. The “Entitled Party” of a contract dictates which company(s), and their associated Cisco.com users, may be entitled to the services on the contract.

Bill-To Entitlement

When the "Entitled Party" of a contract is Bill-To, only users who work for, or on behalf of, the contract’s Bill-To company are eligible to obtain full support for all the products in the

support contract. Bill-To companies are those companies that purchase services from Cisco directly for their own consumption and/or through Channel Partner resale to end customers. Bill-To entitlement is typical for contracts that contain partner-branded services (such as Partner Support Services "PSS") where a Cisco partner (not Cisco) has the responsibility to provide technical support to end customers (Install-At parties) or for service contracts that contain products purchased and consumed by the contract's Bill-To company. Users of Bill-To entitled services work for, or on behalf of, the contract's Bill-To party and may be entitled to access the services when the contract's BID is in their User Profile and is enabled for support (via SAMT), or when the contract number is in the individual's User Profile. Full support access to Bill-To entitled PSS contracts is only available for Bill-To users (BID or contract number is in the User Profile.) However, some PSS contracts offer users of Install-At parties (end customers) the capability to download operating system software for Cisco products. This is referred to as Partner Software Download ("PSD") enablement. PSD entitlement, when enabled, is only available for Install-At users on Bill-To entitled PSS contracts.

Install-At Entitlement

Cisco services (such as SmartNet) that Cisco provides directly to end customers are considered "Install-At" entitled services. Access to these services may be granted to employees of the end customers (Install-At parties) on the contract. Additionally, to encourage Partners to assist end customers with post-sales technical support, by default, Cisco entitles Partner users to access technical support on the Install-At services they purchase for their end customers. User access to Install-At entitled services may be managed by representatives of the Install-At customer and/or representatives of the Bill-To (Partner) company.

User Access to Service Entitlements			
	Contract Service Lines		
User's Company Affiliation	**"Bill-To Entitled" Services (no PSD)**	**"Bill-To Entitled" PSS w/ PSD**	**"Install-At Entitled" Services**
Install-at Company GU ID (Does not match contract Bill-To/BID)	No Access	SW Downloads Only for matching Install-At GUID service lines in the Contract	Full Support Access for all matching Install-At GU ID service lines in the Contract
Contract's Bill-To GU ID	Full Support Access to All Service Lines in the Contract	Full Support Access to All Service Lines in the Contract	Full Support Access to All Service Lines in the Contract

Contract's Bill-To GU ID with BID Enabled for Support (Enabled for Support in SAMT)	Full Support Access to All Service Lines in All Contracts sold under that BID	Full Support Access to All Service Lines in All Contracts sold under that BID	Full Support Access to All Service Lines in All Contracts sold under that BID

Contract Service Request Access Levels

"Service Request Management" is the level of access to Cisco services a contract will provide to an individual, if the contract is associated with an individual's User Profile. It is the level of access a user will have to view, open, or update service requests related to a specific contract. Levels include: "Query/Update/Open," "Query & Update," "Query Only," or "No Access."

"Query/Update/Open" indicates users associated to the contract can perform all service request functions. This is the most common setting for service contracts.

"Query & Update" indicates users associated to the contract can view and change a service request but cannot open them.

"Query Only" indicates that users associated to the contract can view service requests but cannot open or update them.

"No Access" indicates that users associated to the contract have no access to view, open, or update service requests.

The Service Request Access information is displayed in various areas within SAMT.

Requesting Access to Service Contracts

Any individual with a Cisco.com User Profile may request access to contracted technical support services from Cisco once logged into their existing Cisco.com User Profile on Cisco.com. End users who have purchased Cisco-branded services (such as SMARTnet) through a partner, employees of direct Cisco customers, and partner employees who need access to specific service contracts may request access by entering a contract number or serial number of any product covered by a contract. On the Profile Management page, there is an "Add Access" button within "Access Management" and "Access - Services & Support" tab. The requestor selects access for either a) software download, support tools, and entitled content on Cisco.com or b) TAC and RMA case creation, software download, support tools and entitled content on Cisco.com. If option a (software download, support tools and entitled content on Cisco.com) is selected, up to 10 contract numbers or one serial number may be entered for the request to be processed. If option b (TAC and RMA case creation, software download, support tools and entitled content on Cisco.com) is selected, up to 10 Bill-To IDs, 10 contract numbers, or one serial number may be entered for the request to be processed.

Cisco's Support Case Manager application provides a "real-time onboarding" function that allows an unentitled user to submit a request for access while opening a support case.

Access Advisor ("AA") Request Review

All contract access requests are reviewed by Cisco's Access Advisor. Access Advisor provides a systematic evaluation of access requests including, but not limited to, the user, the user's company details, the contract details, and the access requested by the user. If AA recommends "Add", the system adds the contract to the requestor's profile. In the case of "Deny" or "Review," AA sends a notification to the requestor and SAMT Admin(s) with an explanation of the decision and no changes are made to the User Profile. If a contract has been locked from AA automation by a SAMT Admin, the request is routed directly to the SAMT Admin(s) for review. If no SAMT Admin is assigned to an unlocked contract, a Cisco Agent reviews the AA recommendation and other user/contract details and grants or denies the access.

Service Access Management Tool Administrator ("SAMT Admin")

SAMT Admins are a limited number of individuals who have been granted the authority to determine which individuals employed or working on behalf of a customer entity GU ID (Bill-To company and/or Install-At company) are authorized to obtain technical support from Cisco under support contract(s), and use SAMT functionality to Add, Enable Support Access, Remove Support Access, and Delete, Block, Unblock, Lock and Unlock Contract Numbers and/or Bill-To IDs. Depending on service contract entitlements, a SAMT Admin may be authorized to manage user access for Install-At users only or both Bill-To party users and the Install-At party users. These SAMT Admins that manage user access at a contract-level may be referred to as a contract-level SAMT Admin (of an Install-At party or Bill-To party) or a Bill-To level SAMT Admin ("BID Admin"). Therefore, any service contract may have BID SAMT Admin(s) AND a contract-level SAMT Admin(s) managing user access to the contract at the same time.

User Access Administration

Contract-level SAMT Administrators manage user access to individual contracts. Cisco resellers of Install-at entitled Cisco-branded support contracts, such as SMARTnet, may nominate a customer employee as a SAMT Admin to manage access of users to their contracts. After the customer confirms to their partner, who at their company is their elected contract SAMT Admin(s), an existing Partner SAMT Admin should use the Peer Admin Onboarding function in SAMT Administration tab to enable the customer user(s) as SAMT Admin for those contract(s). When the SAMT Admin role is granted, the customer SAMT Admin can log into SAMT and manage their users' access to the contracts that they were granted the ability to manage. Note that a contract SAMT Admin might only be

granted a portion of their company's contracts to manage. There may be multiple contract SAMT Admins from one company assigned to manage different (or the same) contracts for their company. Cisco partners and resellers also may choose to manage customers' access to contracts on behalf of their customers or in addition to their customers. They may do so as contract-level Admins or they may manage contract access as BID-level SAMT Admins. BID-level SAMT Admins may be assigned to direct purchasing Cisco customers and partners to provide access to their employees to all BID company contracts. The following table describes the types of SAMT Administrators that can manage user access, the company affiliation of the Admins and the type of services the Admin can manage depending on their company affiliation.

User Access Administration				
SAMT Admin Type	**SAMT Admin Manages**	**Install-At Entitled Services**	**Bill-To Entitled Services (no PSD)**	**Bill-To Entitled Services PSS w PSD**
Install-At GU ID Contract-level Admin	Each Contract/GU ID nominated to manage	Install-At Users of matching GU ID only	-	-
Bill-To GU-ID Contract-level Admin	Each Contract nominated to manage	Bill-To Users and All Install-At Users	All Bill-To Users	All Bill-To Users & All Install-At Users to PSD
BID BID level Admin	All BIDs in Profile & All Contracts Under BIDs	All Bill-To Users and All Install-At Users	All Bill-To Users	All Bill-To Users & All Install-At Users to PSD

Using the Service Access Management Tool ("SAMT") to Manage User Access

Accepting the SAMT Terms & Conditions

SAMT may only be accessed by users who are SAMT Administrators (Bill-To/BID SAMT Admins or Install-At SAMT Admins.) The first time that a SAMT Admin opens the application, the Terms & Conditions must be accepted. By clicking on the "Accept" button, the SAMT Admin acknowledges reading and agreeing to the "Service Access Management Administrator Agreement" in its entirety and commits their organization to this Agreement.

SAMT Management Tabs

There are six tabs within SAMT to manage user access. They are "Requests," "Manage by Number," "Manage by Name," "Manage by Group," "Lock/Unlock" and "Administration."

The “Requests,” “Manage by Number,” “Manage by Name,” and “Manage by Group,” tabs appear by default. The “Lock/Unlock” and “Administration” tabs are displayed only after clicking the “>>” tab.

Requests

The “Requests” tab and the “Pending Requests” sub-tab are the default SAMT homepage upon login. All submitted requests for access that require SAMT Admin review/action are listed in the “Pending Requests” sub-tab. Cisco’s automated access system, Access Advisor, will direct any access requests to the SAMT Admin for review when it is unable to automatically validate a user’s request. Additionally, when the SAMT Admin has locked a contract from Cisco (Access Advisor and Cisco Agents), access requests appear in the queue and require SAMT Admin approval. Clicking on a hyperlinked contract number opens a pop-up screen with contract details including the contract’s entitlement, service level(s), start/end dates, Bill-To information, company GUID(s) within the contract and the quantity of unique contract GUIDs. A click on the “show sites” button on the pop-up, provides the contract’s Install-At site information.

Contracts with Multiple End Customers

On the pending requests screen, the requesting user’s Parent Company is displayed in the column labeled, “User’s Company (Parent Company Name).” The list of Parent Companies with services on that contract is accessible by clicking the “View” link under the type of approval request within the “Request Type Details” column. If the user’s request to access the contract is approved by the SAMT Admin but the current Parent Company of the user does not match a Parent Company within the contract (such as a third-party), upon approval submission, a pop-up screen appears. On this screen, the SAMT Admin must select the Parent Company within the contract for which the user is to be associated. See “Assigning a Parent Company” for more information. Users associated to an Install-At GU ID only have access to the lines on the contract that belong to that Install-At GU ID.

Approving or Denying Requests

To approve a request, click the radio button next to “Approve” and provide additional information to be shared with other SAMT Administrators (optional). To deny a request, click the radio button next to “Deny” and select a required reason for the denial: unrecognized user, unrecognized company, or other (explanation to the requester is required). After the request is approved or denied, it is removed from the “Pending Requests” sub-tab and moves to the “History” sub-tab. SAMT also provides the option to approve or deny all pending requests at the same time within the “Pending Requests” tab by clicking on the radio button next to “Approve All” or “Deny All” in the “Actions” column.

Access Advisor for Pending Requests

The Access Advisor function provides advice for contract requests based on systematic evaluation of the user and the access requested by the user. Access advice within SAMT is available for requests for full support and software download access to a contract. Advice is determined dynamically based on the latest information available to Cisco. To view the access advice available, click the “?” button appearing on the request line. A spinning

wheel may appear when the question mark icon is clicked while the system is deciding what advice to provide. Once advice is available, it is displayed, along with a link to the details. After Access Advisor is employed by the SAMT Admin in the Requests tab, the "Approve" option could be grayed out and no longer available to the SAMT Admin, if Access Advisor determines a "deny" recommendation due to failed critical criteria. More detail is available when "Details," "View," or the contract number hyperlinks are chosen in SAMT.

Notifications

SAMT keeps Admins informed about access requests and important transaction events using the notifications sub-tab. Being aware of pending user requests and account changes can help keep business running smoothly. SAMT tracks many types of transactions that may impact users, so appropriate action may be taken to keep users happy and information safe. Valuable information may be listed on the "Notifications" sub-tab. Notifications may include User Profile changes that may affect continued access to a contract, access changes processed by other SAMT Admins, or reminders. Actions do not need to be taken in response to notifications. Notification preferences can be adjusted within the Administration tab.

History

After a pending request is approved or denied, it is removed from the "Pending Requests" sub-tab and moves to the "History" sub-tab. History line items may be filtered to view only the requests for full support to contracts or software downloads to contracts. Search is also available within the following elements: name, user's organizational entity (OE), contract number, Bill-To ID, Parent Company name, request date or User ID. The "Request Type Details" column displays a hyperlink to view the details of the request and steps taken for each line item. Clicking on the hyperlinked contract number opens a pop-up screen with contract details including the contract entitlement, service level(s), start/end dates, Bill-To information, company GU IDs within the contract and the quantity of unique contract GU IDs. Click on "show sites" button on the pop-up to view Install-At site information. History will also contain requests processed by other SAMT Admins for the contract(s) the SAMT Admin manages.

Manage by Number/ Manage by Name - Contracts

SAMT Contract Admins may use the "Manage by Number" or "Manage by Name" tabs to proactively manage user access to a specific contract or contracts. The SAMT Admin must first choose the type of access being managed, either Support Access or Software Access (available only for some Partner-Branded contracts).

Support Access (aka Full Contract Access)

Support Access provides access to all service entitlements contained in a contract. This may be access to Cisco's technical assistance, hardware replacements, and/or software downloads. Users granted support access to a contract will be entitled to consume the

services that the contract offers for the user's parent company(s). When choosing "Support Access" on the "Manage by Number" tab or on the "Manage by Name" tab (after choosing a user,) all contracts the SAMT Admin manages are listed. The Admin may choose a contract listed or enter the contract number, if known, in the "Enter Contract Number" field.

Software-Only Access (aka Indirect Access)

Cisco partners managing end customer networks using a Partner-branded support contract ("PSS") may choose to allow end customers to download software for products on the PSS contract. Software Download Access is only available for PSS contracts that are Bill-To entitled and enabled for Partner Software Delivery ("PSD"). When the "Software Access" radio-button on the "Manage by Number" tab or on the "Manage by Name" tab (after choosing a user) is chosen, only those contracts eligible for Software Download Access are listed. Software Only Access is not available for Install-At entitled contracts or for contracts that are not enabled for Partner Software Delivery.

When software access is granted, the software downloads available are only for the customer-owned hardware of the customer user's Parent Company GU ID and active within that contract. This "indirect" contract association does not grant access to Cisco technical support or advanced hardware replacements.

Add Contract or Software Download Access to a Cisco.com Profile

Manage by Number

In the "Manage by Number" tab, after choosing "Support Access" or "Software Access," enter or choose a single contract number listed and select "Add Contract to a Cisco.com Profile" or "Grant Software Access" option from the "Action" dropdown list. A pop-up screen may appear after choosing the option to add a contract to a User Profile. This pop-up appears when a contract has multiple end customers AND the SAMT Admin manages more than one Parent Company present on the contract. Identify the customer(s) for which the user is authorized to obtain support when granting user access to this contract. See "Assigning a Parent Company" for more information. After the action is submitted, indicate or choose the user to receive access. The list of existing users already associated to one of the Administrator's other managed contracts is displayed and may be searched, or a new user may be added. To add a new user, click "Add New User" button. On the next screen, enter up to 10 Cisco.com IDs or Email IDs separated by commas. Click search. Search results do not include inactive/invalid users. Users who are grayed out (unable to be chosen), do not have a complete and validated email address in their User Profile. These users must update their email address in their profiles before they can be granted access. Select the user to have the contract added to their profile and click the "Submit" button. Click the radio button next to the appropriate User Profile and select "Add Contract to a Cisco.com Profile" or "Grant Software Access" option from the "Action" dropdown list. See Revalidation, if a revalidation pop-up screen appears when attempting to add a contract to a Cisco.com Profile or there is a revalidation message present on the top of the screen.

Manage by Name

In the “Manage by Name” tab, after choosing “Support Access” or “Software Access,” search for users or view a list of existing users associated to the contracts available to administer access by clicking on the “click here” hyperlink. This hyperlink provides a list of users that have already been associated to contracts the SAMT Admin manages. To search for a user. Select a search attribute from the drop-down list. Enter the information to search for and click the “Search” button. A list of individuals who match the search attribute and criteria entered appears. Click radio button next to the appropriate User Profile and select an action from the list. To enter a Cisco.com ID for an individual not found in provided list, click "Add Names". Add an individual by entering their Cisco.com ID or their email address in the boxes provided. Choose the user and “Add Contract to a Cisco.com Profile” or “Grant Software Access” from the action dropdown on the bottom of the page.

Assigning a Parent Company

A pop-up screen may appear after choosing the option to add a contract to a User Profile. This pop-up appears when the user’s current Parent Company does not match any Parent Company on the contract, or when a contract has multiple end customers and the SAMT Admin manages more than one Parent Company present on the contract. The list of Parent Companies with services on that contract appears on the pop-up screen. The SAMT Admin must select the Parent Company(s) on the contract to which the user is being granted access. If the contract contains services for multiple end customers (with different GUIDs,) users may only access the services within the contract that are associated with their own Parent Company GU ID. Therefore, if Install-At sites within a contract belong to different Parent Company GUIDs, a user will only be entitled to support for the products in the contract that belong to the user’s Parent Company GU ID. If the user belongs to the Parent Company that is the contract’s Bill-To company, the user is entitled to receive support on all items in the contract, even if Install-at sites in the contract are different than the Bill-To company. Only the Parent Companies on the contract that the Admin has rights to manage appear. *Granting user access to a company when the user is not authorized to obtain support on behalf of that company could expose protected customer data and render the SAMT Admin and/or SAMT Admin’s company liable for the exposure.*

When adding a contract to a User Profile, the SAMT Admin may set an expiration date for user access to a contract. This is recommended for third-party integrator access and temporary assignments to ensure access is automatically terminated when it is no longer needed.

Delete Contract or Software Download Access from Cisco.com Profile

This action removes a contract from a Cisco.com User Profile and disables support access for the user to contract entitlements. In the “Manage by Number” tab, after choosing “Support Access” or “Software Access,” choose a single contract number listed and select “Delete Contract to a Cisco.com Profile” or “Revoke Software Access” option from the “Action” dropdown list. After the action is submitted, search for or choose from the list of

individuals who currently have access to the Contract Number and whose access is to be removed.
In the “Manage by Name” tab, after choosing “Support Access” or “Software Access,” search for a user or view a list of existing users associated to the contracts available to manage by clicking on the “click here” hyperlink. Choose the appropriate user and “Delete Contract to a Cisco.com Profile” or “Revoke Software Access” from the action dropdown on the bottom of the page. Choose the appropriate contract number from the list of contracts in the individual’s profile that can be used for support. Click “Submit.”

Removing a Parent Company

When choosing the option to delete contract from Cisco.com Profile, a pop-screen appears, if the user currently has access to more than one end customer Parent Company on the contract. Remove the check mark to remove the user’s access to one or more end customer Parent Company(s) on the contract. If the user was originally given access to the contract through a group, an informational pop-up appears, and the user is removed from the group.

Block Contract Addition to a Cisco.com Profile

The block action prevents a user from requesting access to a contract and restricts that contract from being associated to that specific Cisco.com User Profile. When a contract is blocked from a user, it is no longer associated with the individual's User Profile and the blocked contract cannot be associated with that individual's User Profile until a SAMT BID Admin or Contract Admin for the contract unblocks it from the user's Profile. Blocking a contract removes the user's ability to utilize all services and support granted by that contract.
In the “Manage by Number” tab, after choosing “Support Access,” choose a single contract number listed and select “Block Contract Addition to a Cisco.com Profile” option from the “Action” dropdown list. After the action is submitted, search for or choose from the list of individuals who currently have access to the Contract Number and whose access is to be blocked. Once submitted, the contract will be deleted from the individual’s User Profile, support access is removed, and Cisco’s Access Advisor or Cisco Agents will be unable to add the blocked contract number to the individual’s User Profile.
In the “Manage by Name” tab, after choosing “Support Access,” search for a user or view a list of existing users currently associated to the contracts available to manage, by clicking on the “click here” hyperlink. Choose the appropriate user and “Block Contract Addition to a Cisco.com Profile” from the action dropdown on the bottom of the page. Choose the appropriate contract number(s) from the list of contracts in the individual’s profile that can be used for support. Click “Submit.” Once submitted, the contract(s) will be deleted from the individual’s User Profile, support access is removed, and Cisco’s Access Advisor or Cisco Agents will be unable to add the blocked contract number(s) to the individual’s User Profile. Note that block is not an action option for “Software Access” only users to a PSS contract with Partner Software Download enabled.

Unblock Contract to Allow Addition to Cisco.com Profile

This action removes the current block of a contract to a specific Cisco.com User Profile. An unblocked user may then have the contract added to their User Profile by a SAMT BID Admin or Contract Admin proactively using SAMT “Manage by Name” “Manage by Number” “Manage by Group” or when requested by the user through Profile Manager or a Cisco Agent.

Modify Expiry Date to Access Contract

This action allows the SAMT Admin to set, remove or modify a previously set expiration date for user access to a contract. This is recommended for third-party integrator access and temporary assignments to ensure access is automatically terminated when it is no longer needed.

Manage by Group

Organizing access by contract groups simplifies the process of managing access to multiple users and/or multiple contracts. By creating a group and then adding multiple users and/or contracts to the group, all users in the group will have access to all contracts in the group. To onboard a new user and grant them access to all contracts, add the user to the group. Or, when a new contract needs to be granted to all the users, just add the contract to the group. Create a new group or revise an existing group by selecting the “Manage by Group” tab.

Create New Contract Group

Prior to creating a new contract group in SAMT, choose the type of group access being granted, either Support Access or Software Access. Then click “Create New Group” button. Provide a name for the group and a description for future reference. Select the contract(s) from the list to add to the group. Once contracts are added to the group, SAMT provides a message that the group was successfully added. To allow other company SAMT Administrators to access to this group, click "Continue to share", otherwise click "Done".

Share/ Unshare Contract Group Access

Administrators may share the groups they have created with other Administrators. After creating a new contract group, click the option “Continue to share.” Groups can only be shared with someone who is also a SAMT Administrator for at least one contract in the group. After clicking “Continue to Share,” enter the Cisco.com ID of the Admin. Other contract Admins can be found in the “Administration” page using the Locate Other Administrators report. In addition, Groups may also be shared using the Share Access Groups hyperlink within the “Administration” tab in SAMT.

Add Contract to Group

Once a new group is created or to add contracts to a previously created group, select a group appearing in the list and choose “Add Contract to group” in the action dropdown list. SAMT provides a list of contracts the SAMT Admin manages that are not currently in the

group. Specific contract numbers may also be found using the search option. Select the contracts displayed to be added to the group.
If a contract contains multiple end customers (multiple Parent Company GU IDs), the contracted GU ID(s) to be added to the group must be chosen. Click on the "Show More" button to see the contract details and list of all GU IDs on the contract. Choose the GU ID(s) to add and submit. See Revalidation, if a revalidation pop-up screen appears when attempting to associate a contract to a group or there is a revalidation message present on the top of the screen.

Add Name to Contract Group

Users may be added to a new group or new users may be added to an existing group. Search for users that currently access managed contracts or click "Add Name" button to add a new user(s). If a contract contains multiple end customers (multiple Parent Company GU IDs), the GU ID(s) to which the new user in the group will be associated must also be identified. Choose the user's Parent Company GU ID(s) and press "Submit." *Please, note that granting a user from one company access to another company's contract could create a data protection exposure, for which you and your company may be found legally and financially liable.*
If a contract group already exists with more than one contract and one the contracts in the group needs to be revalidated, new users to the group will not be added to the contract that needs revalidation. Before adding new users to a group, ensure all contracts in the group are up to date on revalidations.

Delete Contract from Group

Select "Delete Contract from Group" action from dropdown to delete a contract from a group, and press "Submit." Choose the contract(s) listed to remove from the group. This action deletes the selected contract number(s) from all individuals in the group. Note, if an individual is in more than one group with the same removed contract number(s), the contract number(s) are still deleted from their profile. To re-associate the contract(s) to those individuals, remove the contract from the other contract group(s) containing the contract number(s) and then add them back to the group(s.)

Delete Name from Contract Group

Select a group from the on-screen list of previously created groups and choose "Delete name from group" action from the dropdown to delete an individual from a group. Choose from the individual(s) listed. This action removes the user from the group and deletes the group's contract number(s) from the selected individual's User Profile. If an individual is associated with other groups containing the same contract number(s) of the group that the individual was just removed from, the contract number(s) are still deleted from the individual. To re-associate the user to the contract(s), the user may be removed from the other contract group(s) containing the contract number(s) and returned to the group(s) to re-apply the contract number(s) to User Profile.

Rename Contract Group

Select a group from the on-screen list of previously created groups and choose “Rename group” action from the dropdown to rename a group. Enter a new group name and description and press “Submit.” Group names must be unique and cannot be duplicated.

Delete Contract Group

Select a group from the on-screen list of previously created groups and choose “Delete group” action from the dropdown to delete a group. Deleting a group does not delete the contract number(s) from the individuals in the group. It only removes the group container of contracts/users. It is recommended that prior to deleting a group, all users and contracts should be removed from the group. Otherwise, once the group is deleted, “Manage by Number” or “Manage by Name” functions may be used to remove the contracts from each user that was in the now deleted contract group.

Lock/Unlock Tab

The “Lock/Unlock” tab provides Admins the ability to implement rules to further restrict access or make access management more efficient. SAMT provides Administrators the option to turn-off Cisco’s automated processing of user requests via Access Advisor or through Cisco Agents. Email domain matching rules may be implemented to make the approval process faster and more efficient via Access Advisor or through Cisco Agents.

Lock Contract Number

Locking access to a contract prevents Cisco from reviewing submitted requests and automatically granting user access to the locked contract. When a contract is locked, all valid requests are routed to the SAMT Administrator for manual review. Users requesting access to a locked contract will receive the message that the request is “Pending Your Company Contract Administrator Review.”

Enter a contract number or select the contract number(s) from the displayed list to invoke a lock. Note the “Locked” column on the display for the contract(s) listed. It displays if a contract is currently in a locked status. Access Advisor is enabled on all contracts by default and, therefore, a “No” is the default display. Select the “Lock Contract Number” action from the dropdown list. Note that if a contract-level SAMT Admin locks a contract, only Cisco Agents and Cisco’s Access Advisor are prevented from approving user access requests. All other SAMT Administrators of the contract will be able to approve user access requests. For example, if the contract is an Install-At entitled contract purchased by a different Bill-To than the Install-At parties (such as through a Cisco partner), there may be a BID SAMT Admin with user access management privileges to the contract. Access requests may still be processed by the BID SAMT Admin. Locking a contract does not lock out a Partner (contract Bill-To) from managing end user access to the contract.

LOCKING CONTRACTS WITH MULTIPLE END CUSTOMERS

When the contract being locked contains multiple end customers (Install-At sites of different Parent Company GU IDs) and the SAMT Admin manages multiple Parent Company GU IDs within the contract, a pop-screen appears listing the contract's Install-At GU IDs. The SAMT Admin must choose which GU IDs on the contract should receive the lock status. Once set, access requests for the contract from users associated to the locked Parent Company GU IDs are routed to the SAMT Admin for review. The locked column within SAMT displays "Partial," if the Admin manages multiple contract GU IDs and locked one or more of those GU IDs but not all. When the Admin manages only one of the multiple GU IDs on the contract and that one GU ID is locked, the display reflects a "Yes" that the contract is locked. The history view only displays the lock history for the GU IDs that the Admin manages.

Unlock Contract Number

Unlocking a contract removes the restriction preventing Cisco from approving an access request when it is received and processed. When a contract is in a locked state, any SAMT Admin (contract-level or BID level) of the contract may remove the lock. Unlock a contract on the "Lock/Unlock" tab by entering the contract number or choosing from the list of contracts displayed and choose the "Unlock Contract Number" from the action dropdown list. Press the "Submit" button. Note the "Locked" column on the display for the listed contract(s). It indicates if a contract is in an unlocked status with a "No". Access Advisor is enabled for all contracts by default and, therefore, a "No" is the default display.

Restrict Contract from BID level Users

A contract-level SAMT Admin may desire to prevent their partner users (who have been granted support access to a contract at the BID level) from viewing or opening support cases for the products on their contract(s). On the "Lock/Unlock" tab, the list of contracts is displayed including a column showing the "BID Level Access" settings for each contract. The default BID level access for all contracts is "Enabled." To restrict a contract so that BID level users cannot obtain service from Cisco or access service-related data pertaining to the contract (such as viewing TAC cases), enter the contract number or select a contract from the list displayed. Select the action "Restrict Contract from BID-level users" from the dropdown and press submit. All Administrators are notified of the restriction according to their individual notification and email preferences. If a specific individual from the partner's company needs access to support to the contract, the contract-level SAMT Admin may add that person's User Profile to the contract using "Manage by Name", "Manage by Number" or "Manage by Group" tabs. Note that when "BID Level Access" restriction is enacted, any BID level users with individual contract access in their User Profile continues to receive Cisco support and view service-related data for the BID restricted contract.

Enable contract for BID level Users

By default, BID level users are enabled to receive Cisco support and view service-related data pertaining to all contracts under the BID. If a contract-level SAMT Admin had restricted BID level user access to a contract, it may be disabled within the "Lock/Unlock" tab. The list of contracts is displayed including a column showing the "BID Level Access" settings for each contract. The default BID level access for all contracts is "Enabled." When a contract is restricted the column displays "Restricted." To remove a restriction, enter the contract number or select a contract from the list displayed. Select the action "Enable Contract from BID-level users" from the dropdown and press submit. Once processed, the "BID Level Access" displayed for the contract shows "Enabled."

Email Domain Matching for Contract Access

Email domain matching can help reduce SAMT Admin workload and improve data access and security. A SAMT Admin may enable automatic approval of contract association requests from users that match specific company email domain address(es) and/or enable automatic denial of contract association requests from users that don't match the set auto-approve company email domain address(es). A SAMT Admin may also perform bulk downloads and uploads of domain matching rules. Refer to Bulk Transactions for more information about bulk transactions. On the "Lock/Unlock" tab all contracts are listed that can be managed by the SAMT Admin. A column labeled "Email Domain Matching Enabled" is available to view for each contract listed, if domain matching is enabled or disabled. By default, email domain matching is not enabled. *Note: When a contract is locked, all valid requests are routed to the SAMT Admin for review, even when email matching settings are enabled.*

AUTO APPROVE DOMAINS

To establish email domain settings for a contract from the "Lock/Unlock" tab, select a contract from the list and choose "Enable Email Domain Matching" from the action list or click the "Add" hyperlink that appears in the "Email Domain Matching Enabled" status column. In the next "Contract Email Domain Settings" screen, choose the Parent Company name in the dropdown to which the settings should be applied upon receiving requests for access. In the AUTO APPROVE section, enter the company's email domain(s) that should be approved. This option should only be chosen when all company employees with the email domain should have access to all services on the contract. There may be circumstances when a company has multiple email domains such as after an acquisition or company merger. To assist with indicating all appropriate domains, a summarized list of email domains of users currently associated to the contract may be viewed by pressing the hyperlink "Suggested email domains for this Contract Number." A listed email domain may be chosen to add to the auto approval textbox. Public email domains are not eligible for domain matching and are not selectable. If unrecognized email domains appear on the "Suggested email domains for this Contract Number" list, those user(s) may have changed

companies and need their contract access removed. Check the box in the AUTO APPROVE section to automatically approve contract association requests.

"REVIEW" & "AUTO DENY" USING DOMAINS

To prevent users from unknown email domains from requesting access and require manual review of users from known domains, enter the *known* email domains in the "REVIEW" text box. This is an option when not all users with the same company email domain in their User Profile and only certain individuals at a company should have access to a contract. Note, all requests are DENIED from users with domains that do not match the "AUTO APPROVE" domains and/or the "REVIEW" domains when the "REVIEW" box is checked (if domains are listed in the textbox or not). This saves the effort of reviewing all other domains and then having to deny them. Since any domain NOT entered in either box is auto denied (when "review" box is checked), this option should be reviewed carefully before choosing and enabling the "REVIEW" functionality.

After entries are complete, set the dropdown next to "Email Domain Validation for Access Automation" to "Enable" or "Disable." When set to "Enable," the email settings take effect immediately upon saving. When disabled, the settings entered are saved but are not enforced. Saving the email domain rules, but not enabling them, provides time for further review of the settings.

SAMT returns to the "Lock/Unlock" tab after the domain settings are saved. The column "Email Domain Matching Enabled" is updated within the displayed list of contracts. When settings are enabled, that contract's row displays "Yes" with an "Edit" link to adjust settings when needed. When settings are disabled, the column displays "No" with an "Edit" link to adjust settings and enable when desired. To enable or disable existing email match settings (with no edits to the current rules), enter a contract number in the text box after "Enter Contract Number" or check the box of the contract(s) in the displayed list and choose "Enable" or "Disable" in the action dropdown.

Partner-branded support contracts that enable Partner Software Delivery (PSD) may have separate email domain matching rules for customer users to access software downloads. The top of the screen displays a "YES" next to "Partner Software Delivery Enabled" to indicate that the contract-level SAMT Admin may create domain matching rules for their own partner company users to have full access to the contract, and separate rules to apply for end customer users to receive software download access within the PSD enabled contract.

Revalidation

The revalidation of users is imperative to ensuring that only authorized people obtain the services provided by partner/customer contracts. This revalidation is required to be completed by SAMT Admins on a yearly basis. Regularly reconfirming and validating access maximizes the value that the contracts provide to users and protects confidential

data. Any SAMT Admin may revalidate users associated with contracts at any time from the "Administration" tab or "Manage by Name" or "Manage by Number" tabs. When contracts are due for revalidation, an alert appears at the top of "Manage by Name," "Manage by Number," "Manage Group" and "Lock/Unlock" tabs in SAMT. When a SAMT Admin completes the required revalidation for all due or overdue contracts, the messages no longer appear.

Prior to initiating an action to add a contract to a User Profile within "Manage by Number", "Manage by Name", "Manage by Group" tabs, a pop-up message appears that states a contract cannot be added to the User Profile because the contract has a revalidation status of "Overdue." The contract(s) must be revalidated before the contract can be added to a User Profile. Note that Access Advisor can add contracts in "revalidation overdue" status to a User Profile when the contract is not locked.

There are different avenues in SAMT to revalidate users of a contract.

From the hyperlink appearing in an alert appearing at the top of "Manage by Name," "Manage by Number," or "Manage by Group" tabs, SAMT moves to the "Contracts Revalidation" screen within "Administration" management.

From within a pop-up message click the revalidate hyperlink. SAMT moves to the "Contracts Revalidation" screen within "Administration" management.

From within the "Administration" tab, choose the "Revalidate that users are authorized for service by contract" hyperlink to be brought to the "Contracts Revalidation" screen.

In the "Contracts Revalidation" screen, select one or many contracts listed or search for contracts based on one or more attributes provided. Select contract(s) to revalidate and click on button at bottom of page to generate a user report for the selected contract(s).

After receiving the notification or email that the report has been generated, visit the "View Generated Reports" on the "Administration" tab and download the report. An Excel file opens with a list of users who can currently utilize the contract to obtain service. Review the report and remove access from any unauthorized users. After adjusting user access, generate a new report to ensure changes were made successfully. Return to the "Administration" tab and click the "Revalidate that Users are authorized for service by contract" hyperlink to revalidate contracts and accept the Terms of Revalidation Agreement checkbox certifying that report(s) have been reviewed, necessary changes are made, and only appropriate individuals have access to the services.

An annual notification of revalidation is issued 30 days prior to the annual date coming due. If revalidation does not occur, a 14-day notice is issued. If the contract(s) are still not revalidated, a one-day notice is issued before the contract(s) are put into "Overdue" revalidation status. SAMT Admins cannot associate users to contracts in "Overdue" status but can remove users. User access already established is not affected.

Administration Tab

Administration tab provides capabilities for a SAMT Admin to obtain reports, update their own User Profile, inform Cisco about individuals who have left the company, inform Cisco about individuals who are not authorized to obtain support and register a new individual for a Cisco.com User Profile.

Generate Reports

The generation of reports makes managing user access easier and more efficient.

Contract & Bill-To ID Reports

An Admin may visit the Administration tab and generate reports via the hyperlinks "Contracts by User Name", "Contracts by Number" or "Contracts by Group". Cisco processes the report(s) offline and notifies the Admin when the reports are ready for viewing at the "View Generated Reports" hyperlink on the "Administration" tab.

The "Contracts by Name" report may be used to view user support access to contracts managed by the SAMT Admin. Users can be searched for by last name, first name, company name, email address or Cisco.com ID.

The "Contracts by Number" report page displays all the contracts that are managed by the logged-in SAMT Admin. The SAMT Admin may choose one or more of the listed contracts to generate a report of the individuals who have support access to the contract(s).

The "Contracts by Group" report page displays all group(s) available to the SAMT Admin. One or more groups may be chosen to generate a report of individuals who have access to the contract(s) within the group(s).

Software Download Activity Reports

The software download activity reports provide the Admin with the details of user's who have access to software downloads for products on PSS contracts that are Bill-To entitled and enabled for Partner Software Delivery ("PSD") contracts. User access to the software may be queried by user or by group.

View Generated Reports

Clicking the "View Generated Reports" hyperlink displays all pending and completed reports, the date of submission and the current status of the report. When the reports are generated and available for viewing, the download hyperlink will open a CSV file for the SAMT Admin to review and save. Reports are available for two weeks after generation.

Bulk Transactions

Batch Upload Contract Associations

SAMT Admins that need to associate large numbers of users and contracts may use the batch upload feature on the Administration page to upload a .csv file containing up to 500 unique user-contract associations. SAMT provides a file template to be used as a guide to populate with the users and contracts to be uploaded. The data required for upload

includes User ID, Contract Number and Parent Company to be associated. To ensure the correct Parent Company(s) are provided in the upload file, the SAMT Admin may first download the contract's Parent Company details. The Parent Company information can be copied and pasted to the correct users to the batch upload file in the same and correct format. When the batch upload .csv file is ready for upload, process the file using the "Validate and Generate Report Only" option. This will provide the SAMT with the opportunity to resolve any issues before uploading the file using the "Validate, Associate and Generate Report" option. The "Validate, Associate and Generate Report" will perform the mass association. A report will be returned with results and further action may be taken, if necessary. All validation rules that exist in the "Manage by Name" and "Manage by Number" tabs are enforced during the batch upload process. Associations will be made even if the contract is "Locked" status.

Batch Upload/download Email Domain matching settings

A SAMT Admin may perform bulk downloads and uploads of domain matching rules. This is especially helpful to Admins of a large numbers of contracts. A blank template can be downloaded or a file containing existing domain matching settings can be downloaded to use for the upload file. When "Download Existing Settings" file is chosen, select the contracts to be included in the downloaded file. There is also an option to include the email domain recommendations in the file. Those recommended values may be copied from the "recommendations" column to the "domains" column in the file. Once completed, upload the file for processing. If the upload file contains multiple rows for the same contract, only the values from the first row is saved. The file is processed offline and notification is issues when the job is completes. A batch upload report is generated, containing success or failures of settings. Peer SAMT Admins are notified of edits according to their SAMT notification preferences.

Revalidate that users are authorized for service by contract

Revalidation of users is imperative to ensuring that only authorized people obtain the services provided by partner/customer contracts. This revalidation is required to be completed by SAMT Admins on a yearly basis. Regularly reconfirming and validating access maximizes the value that the contracts provide to users and protects confidential data. Any SAMT Admin may revalidate users associated with contracts at any time from the "Administration" tab or "Manage by Name" or "Manage by Number" tabs. When contracts are due for revalidation, an alert appears at the top of "Manage by Name," "Manage by Number," "Manage Group" and "Lock/Unlock" tabs in SAMT. When a SAMT Admin completes the required revalidation for all due or overdue contracts, the messages no longer appear.

When on the Administration tab, click the "Revalidate that users are authorized for service by contract" hyperlink to be brought to the "Contracts Revalidation" screen. Select one or many contracts listed or search for contracts based on one or more attributes provided. Select contract(s) to revalidate and click on button at bottom of page to generate a user

report for the selected contract(s). After receiving the notification or email that the report has been generated, visit the “View Generated Reports” on the “Administration” tab and download the report. An Excel file opens with a list of users who can currently utilize the contract to obtain service. Review the report and remove access from any unauthorized users. After adjusting user access, generate a new report to ensure changes were made successfully. Return to the “Administration” tab and click the “Revalidate that Users are authorized for service by contract” hyperlink to revalidate contracts and accept the Terms of Revalidation Agreement checkbox certifying that report(s) have been reviewed, necessary changes are made, and only appropriate individuals have access to the services. An annual notification of revalidation is issued 30 days prior to the annual date coming due. If revalidation does not occur, a 14-day notice is issued. If the contract(s) are still not revalidated, a one-day notice is issued before the contract(s) are put into “Overdue” revalidation status. SAMT Admins cannot associate users to contracts in “Overdue” status but can remove users. User access already established is not affected.

Grant Access to Other Administrators

Onboard Peer SAMT Admins

Existing SAMT Administrators may onboard peers as additional administrators. Peer administrators can manage user access to any subset of the contracts that the original administrator manages. Note that Access Advisor is available here, too. The advice is based on the same rules as contract associations for service access. Peer Administrator access must only be granted to people from the same organization. If contract administrator access is granted to a customer, there must not be other customers on that same contract. Doing so would expose one customer’s data to another! Enter the Cisco.com ID or email of the person to onboard and click “Search.” The email address on the profile must be a business address. Public domain email addresses are not allowed for SAMT Admins. Enter or choose the contract(s) to assign. If a contract has an existing Contract Admin, click on “Yes” to display their information. To display contract details, click on the contract number.

Grant Proxy Access

When a SAMT Admin plans to be out of the office and needs to grant temporary access to a colleague during their absence, the “Grant Proxy Access” functionality may be employed. Proxy Access can only be granted by the SAMT Admin. The Cisco.com User ID must be provided, and the feature enabled. An expiration date setting is suggested, if known in advance. If no expiration date is set, after Proxy Access is enabled and no longer needed, the SAMT Admin can disable the proxy access when logging into SAMT and clicking on the “Grant Proxy Access” hyperlink.

Share Access Groups

When a contract group is created or existing within “Manage by Group” tab and the contract(s) within the group have more than one SAMT Admin assigned, the SAMT Admins

may share the group. A group can only be shared with someone who is already a SAMT Administrator for at least one contract in the group. To grant SAMT Administrator access, use the "Onboard Peer SAMT Admins" function on the Administration tab. On the "Share Admin Groups" page, enter the Cisco ID or email address of an existing administrator to share one or more access groups.

Locate Other Administrators

Often, user access to service contracts is managed by more than one SAMT Admin. Additionally, a contract's SAMT Admins may be contract Admins or a BID Admins. "Locate Other Administrators for Contract Number" provides a list of SAMT Admins for a given contract. The list will display the Admin's name, company/organization affiliation, email address and Admin type (contract or BID Admin.)

Update My Profile

Notification Preferences

A SAMT Admin may choose which notifications appear in the "Notifications" subtab within the "Pending Requests" tab. On the "Administration" tab, view transaction notification options by selecting "Change My Notification Preferences." By default, new SAMT Administrators will receive all notification types. Uncheck the box next to a listed transaction type to stop receiving those types of notifications. To view detailed explanations of the different notification types, hover over the information icons. In addition to choosing which transactions and pending requests appear on the "Notifications" tab, SAMT Admins can also how frequently to receive email notifications for the notification types with marked checkboxes. Note that all SAMT Admins will receive notifications of contract revalidations needed and messages/reminders related to contracts the SAMT Admin manages. These notifications cannot be disabled.

a. Real Time: Immediately receive a separate email for each request or transaction
b. Hourly / Daily: Receive a summary email with counts of each transaction and a link to SAMT to view the details. *(If there are no transactions during that time, no email is sent.)*
c. Never: No emails are sent, but notifications are still visible in SAMT. (Recommended for backup administrators only.)

In addition to providing pending access requests within SAMT, emails are sent to SAMT Admins for the pending requests. A SAMT Admin may choose how frequently to receive email notifications of pending requests. SAMT automatically sends emails to users when access is granted or removed, but there is an option to temporarily discontinue sending these emails to users such as when correcting access errors. Check the box next to "Temporarily suppress emails to users when performing any transactions in this SAMT session" to prevent SAMT's automatic emails from notifying users of transactions performed. Emails are not sent to users until the box is unchecked, SAMT is closed, or the browser is closed.

Request User Administration Access to Additional Contracts

The SAMT Admin may click on the "Request User Administration Access to Additional Contracts" and enter up to 10 contract numbers separated by commas to request the ability to manage user access to technical support. A request will be sent to all current SAMT Admins for each contract submitted.

Request User Administration Access to Additional Bill-to IDs

The SAMT Admin may click on the "Request User Administration Access to Additional Bill-to IDs" to be brought to the Cisco.com Profile Management page where the SAMT Admin may request access to BIDs or, if already a BID Admin, request to manage user access to additional BIDs. A request will be sent to all current SAMT BID Admins for the requested BID.

Edit My Cisco Account Profile

The SAMT Admin may click on the "Edit My Cisco Account Profile" to be brought to the Cisco.com Profile Management page to review and edit their company and access details.

Request Support-only Access to Additional Contracts

The SAMT Admin may click on the "Edit My Cisco Account Profile" to be brought to the Cisco.com Profile Management page. On the Profile Management page, there is an "Add Access" button within "Access Management" and "Access - Services & Support" tab. The SAMT Admin may select access for either a) software download, support tools, and entitled content on Cisco.com or b) TAC and RMA case creation, software download, support tools and entitled content on Cisco.com. If option a (software download, support tools and entitled content on Cisco.com) is selected, up to 10 contract numbers or one serial number may be entered for the request to be processed. If option b (TAC and RMA case creation, software download, support tools and entitled content on Cisco.com) is selected, up to 10 Bill-To IDs, 10 contract numbers, or one serial number may be entered for the request to be processed.

Contact Cisco

Tell Cisco that an Individual has Left My Company

When an individual's employment for a company terminates, all access to that company's support contracts should be removed to prevent company data and fraud. A SAMT Admin may only manage access to a portion of their company's contracts. Therefore, after removing access, a notification should be sent by the SAMT Admin to Cisco via the "Tell Cisco that an Individual has Left My Company" link. Cisco Agents will receive the notification and review the user's access and adjust accordingly.

Tell Cisco about Unauthorized Support Access/Usage

If ever a SAMT Admin has reason to believe that an individual is completing or attempting unauthorized actions, they may submit this information and all relevant details to Cisco. We will review the information and act as necessary.