



Secure Endpoint MSSP Console Guide

Last Updated: September 23, 2022

Overview

This document is a guide to the Secure Endpoint Managed Security Services Partner (MSSP) Console. This guide is only intended for setting up and managing user and customer accounts. For day-to-day operation of Secure Endpoint, see the Secure Endpoint User Guide.

Terminology

The **MSSP Partner** refers to the company that is providing and administering Secure Endpoint on behalf of the **Customer** company in whose environments the endpoints are deployed.

The **customer** is the **MSSP Customer** whose environment the MSSP user will be managing via Secure Endpoint MSSP Console.

The MSSP Partner performs two functions: managing its customers (MSSP Customers) and managing its customers' Secure Endpoint environments. An MSSP Partner can add **user** accounts for its own organization to manage its customers.

Users Page

The **Users** page lists all the users, including their login email address and the time and date of their last login. You can access the Users page by clicking on **Users** in the **Accounts** drop-down menu.

Users [View All Changes](#) [+ New User](#)

Filters no filters applied

	Name	Email Address	Last Login	
🔍	Aly MSSP Partner User	@cisco.com	2018-04-23 19:58:39 UTC	⌵ 🗑
🔍	Desmond O'Leary	@cisco.com	Never	⌵ 🗑
🔍	donna gh	@cisco.com	Never	⌵ 🗑
🔍	Kapila MSSP	@cisco.com	2017-06-12 21:36:20 UTC	⌵ 🗑

You can narrow down the list of users with filters. Clicking the **+** button next to **Filters** expands the Filters configuration.

Filters

Last Login	Any Date	User	Name or Email
Two-Step Verification	Any	Command Line	Any
Remote File Fetch	Any		

[Clear Filters](#) [Apply Filters](#)

Users Page

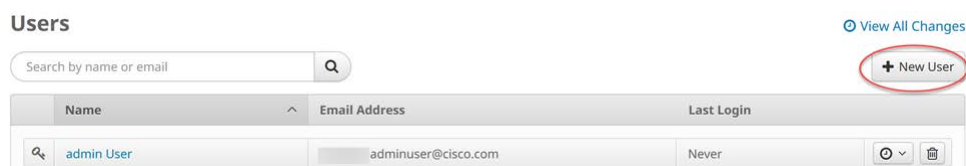
You can filter the user list by various fields and settings. **Last Login** allows you to view users who have logged in during various time frames or never. **User** lets you search by username or email address. The **Two-Step Verification**, **Remote File**, and **Command Line** filters allow you to filter by whether users have those features enabled or not on their accounts.

The **key icon** beside the user's name indicates that the user has administrator privileges. You can click the **clock button** by the user's name to track logins by the user, failed login attempts, view activity by the user, and view changes to the user. The search box in the upper left-hand corner of the page allows you to search for users by name or email.

You can click on a user's name to view the user's information, such as account status, login email, notification email, last login and the user's account settings. You can click on **Reset Password** to change the user's password.

Creating New Users

You can create new users by clicking the **New User** button on the **Users** page.



When you do, a **Create User** dialog will appear. Enter the user's information, including the login email and the notification email. Note that the **User** field includes separate login and notification emails. This is because many users will manage numerous accounts, each of which requires a separate login email. Having one notification email will streamline this process.

The screenshot shows a 'Create User' dialog box. It has a title bar with a close button (X). Inside the dialog, there are four input fields: 'First Name', 'Last Name', 'Login Email', and 'Notification Email'. The 'Notification Email' field has a hint text that says 'Leave blank if same as Login Email'. At the bottom of the dialog are two buttons: 'Cancel' and 'Create'.

Administrator privileges are granted to a new user by default on creation of the new user. They are indicated by the presence of the **key icon** next to the user's name on the Users page.

IMPORTANT! Administrator privileges give the user full control over your Secure Endpoint deployment.



Users Page

You can view the new user's page by clicking on the user's name on the User page. You can configure or revise the user's permissions after creating the user account by clicking **Revoke Administrator Privileges** on the user's account page.

Test User

Account Status	Normal
Login Email	test_user_1@company.com
Notification Email	
Last Login	2017-06-06 17:22:46 UTC
Locale	Not Set
Edit	

Settings

Two-Step Verification	Enabled
Remote File Fetch	Enabled
Command Line	Enabled
Time Zone	UTC
Email Announcements	Disabled

Privileges

[Revoke Administrator Privileges](#)

[Administrator](#)

- All Groups
- All Policies
- All Outbreak Control Lists

When you click **Revoke Administrator Privileges**, a dialog box will appear confirming that you want to proceed with revoking privileges.

Revoke Administrator Privileges ×

If you revoke administrator privileges for Joe Smith, they will only be able to view groups and edit policies and lists that you assign to them. Are you sure you want to proceed?

[Cancel](#) [Revoke Administrator Privileges](#)

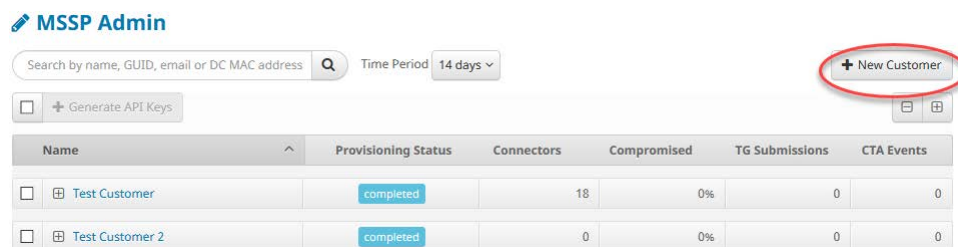
When a user first logs onto the Secure Endpoint MSSP Console, the user will land on the **Customer** page with a prompt to enable **TSV (two-step verification)** or **SSO (single sign-on)**.

[MSSP Admin](#)

Need to enable **TSV** or **SSO** before accessing MSSP Partner Portal

Creating New Customers

When you first log in, the Customers page will be empty. To create a customer, click the **New Customer** button to open the New Customer page.



On the New Customer page, the **Name** is the name that you choose to identify the customer, such as the company name or the business unit within the company. **User** refers to the user who is setting up the new customer and managing the customer's MSSP environment. As the person who is setting up the new customer, you will be automatically granted administrator rights.

Each new customer must be provisioned with a unique login email, otherwise provisioning will not complete successfully. To leverage a common email address, we recommend using SMTP plus addressing or subaddressing.

For example: bob@mssp.edu would like to provision multiple customers. Bob provisions customer 1 with the login email bob+cust1@mssp.edu, and repeats this method for subsequent customers, e.g. bob+cust2@mssp.edu, etc."

In the "Send email to" field, the MSSP partner should send confirmation emails to the partner user. The MSSP partner will be notified once the provision is complete. No further activation is required.

The form is titled "New Customer" and contains several sections. The first section is "Organization Name" with a text input field. The second section is "USER" and includes "First Name", "Last Name", "Login Email", and "Notification Email" (with a hint "Leave blank if same as Login Email"). The third section is "CONFIRMATION EMAILS" and includes a "Send email to" section with radio buttons for "Partner user" (selected) and "Customer". Below this are two dropdown menus: "Payment State" (with the text "Select payment state") and "Tier" (with the text "Select organization tier"). At the bottom right is a green "Create" button.

The **Payment State** drop-down menu allows the user to set the current payment status of the account. The payment state will determine some of the parameters of the customer account.

Payment state refers to one of these states. They are:

- **Licensed** means that the company has a fully paid license, with the number of Connectors and the term of the license being dependent on the license agreement.
- **Evaluation** indicates that the user has been granted a limited number of licenses for a limited term.

Customers Page

The **Tier** drop-down menu allows you to choose between Essentials and Advantage packages. See [Cisco Secure Endpoint License Comparison](#) for more information.

Once you are satisfied that the new customer setup is complete, you can create the customer by clicking **Create**. When the customer has been created, it will be submitted for provisioning. Once the provisioning is completed, the user responsible for the account will receive a message at the notification email address indicating that the account has been provisioned.

Customers Page

After initial login, you will land on the **Customers** page by default. You can also access the **Customers** page by clicking on the **Customers** tab.

Test MSSP Partner org

+ New Customer

Search by name, GUID, email or DC MAC address

Q

Tier

All v

Time Period

30 days v

☐

+ Generate API Keys

Name	Provisioning Status	Connectors	Compromised	TG Submissions	Global Threat Alerts Events	Payment State
<input type="checkbox"/> Organization	pending completion	0	0%	0	0	Licensed
Totals	-	0	-	0	0	-

1 record

<

1

of 1

>

Export to CSV

Clicking the user name at the top of the page will open the **Organization Settings** page. (See [Organization Page, page 11](#))

Each month, MSSP Partner usage is automatically billed. To view details, click the “View Usage Reports” button. You can either download a csv file containing the aggregate number of connectors that was billed, or a detailed report containing a breakdown of what was billed for on a per customer basis for that month.

IMPORTANT! Connectors are counted as installed in the License Report if they have been installed for more than 16 days of the billing month.

Search allows you to search by name (user name or customer name), GUID, email or DC MAC address. When you enter a search criterion, the data that appears on the customer page will be filtered according until you return to the customer page.

Tier allows you to filter customers by Essentials or Advantage packages.

Time Period allows you to filter Secure Endpoint MSSP data by time period: 14 days, 7 days, 1 day, and (approximately) one hour. If a time period is selected, all data shown on your MSSP console will be restricted to that time period until the time period is changed.

Time Period 14 days v

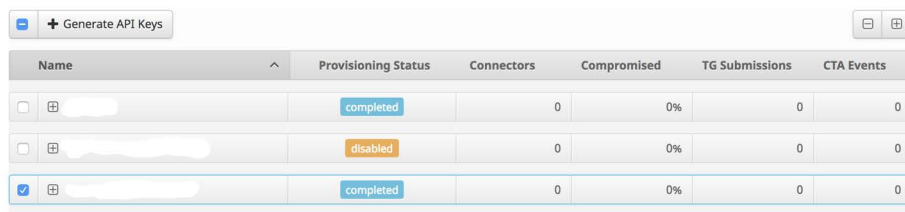
✓ 14 days

7 days

1 day

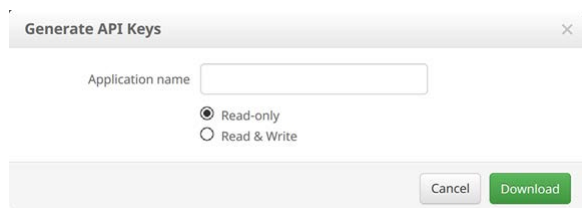
About 1 hour

The **Secure Endpoint API** allows you to send requests for information so you can retrieve data from Secure Endpoint servers without accessing the Secure Endpoint console. You can generate API keys for users by filling the checkbox next to the customer's name and clicking **Generate API Keys**.



Name	Provisioning Status	Connectors	Compromised	TG Submissions	CTA Events
<input type="checkbox"/> [Name]	completed	0	0%	0	0
<input type="checkbox"/> [Name]	disabled	0	0%	0	0
<input checked="" type="checkbox"/> [Name]	completed	0	0%	0	0

Click the **Generate API Keys** button to open this dialog.



Enter the name of the application that you will be using and select **Read-only** or **Read & Write**:

- Read-only gives you only read access to the Secure Endpoint API.
- Read & Write gives both read and write access to the Secure Endpoint API.

WARNING! An API credential with read and write scope can make changes to your Secure Endpoint configuration that may cause significant problems with your endpoints. Some of the input protections built into the Secure Endpoint console do not apply to the API.

Click **Download** to generate the API key. Be sure to store your API key in a safe place: it is only shown to you once.

Connectors displays how many Secure Endpoint Connectors each customer has installed.

Compromised displays the percentage of Connectors that have been compromised, where malware has been detected but for which no action has been taken to remove the threat from system. The compromise percentage indicates the percentage of Connectors that have detected compromises during the selected time period. It does not indicate the number of malware files that have compromised affected computers.

Secure Endpoint automatically uploads malicious files to the **Cisco Secure Malware Analytics** (formerly Threat Grid) sandbox environment for analysis. **Secure Malware Analytics submissions** represents the number of malicious files that have been detected in the customer's environment and uploaded to Secure Malware Analytics during the selected time period.

Global threat alerts events are events recorded by **global threat alerts** (formerly Cognitive Threat Analytics) in the customer's environment. These are incidents that occur on computers that don't have an Secure Endpoint Connector installed.

- Your customer must have **Global Threat Alerts Integration** enabled on the **Organization Settings** page and at least one enabled device like a Cisco Secure Web Appliance (formerly Web Security Appliance) configured to send logs to global threat alerts for events to populate this page.
- You should download and install an **Secure Endpoint Connector** on any computers that appear in the **Agentless Global Threat Alerts** list if possible. This can help to detect and quarantine threats at an earlier stage and surface the full range of an incident through **Device Trajectory**.

Totals shows the total number of each item (Connectors, TG Submissions, Global Threat Alerts Events) for all customers in the user's environment for the selected time period. If the time period is selected, or filters are applied through the **Search** feature, the totals will reflect those considerations.

Detailed Customer View

Export to CSV allows you to export a summary of your customer information to a CSV file. This summary will include: customer name, number of Connectors, percentage of Connectors compromised, and provisioning status for the selected time period.

Detailed Customer View

The MSSP Console allows you to see an expanded view with details about Secure Endpoint Connector deployment information for each customer. On the **Customers** page, each customer entry can be expanded to provide a detailed view of the account. Click the **+** button beside each customer to expand the detailed view for that customer or click on the **+** button below the **New Customer** button to expand detailed views for all customers.

In addition to data related to Connectors, compromises and provisioning status, the detailed customer view allows you to track the following:

- **Installs** displays the number of Connector installs that took place during the selected time period.
- **Install Failures** displays the number of Connector installs that failed during the selected time period.
- **Recent Users** displays which users have logged on during the selected time period. If the Recent Users field is blank, no users have logged in during the period.
- **Tier** shows if the customer has the Essentials or Advantage package.

The detailed customer view also allows you to perform several administrator functions that are specific to the customer's account. **Disable** allows you to disable a customer's account so that the customer cannot log in.

IMPORTANT! You cannot delete customer's accounts from your Secure Endpoint MSSP Console, but **Disable** will allow you to remove it from active use.

Identity Sync looks for host names of Connectors that have been removed or disabled, and re-installed or re-enabled, and updates the data associated with that Connector. Click **Enable Identity Sync** to restore data that may have been lost or missed while a customer's account was disabled and has since been re-enabled.

WARNING! Identity Sync is an advanced feature that can generate significant amounts of data. It should only be enabled in certain situations.

Click **Edit** to change the Organization Name, Payment State, or Tier.

Organization Switcher

The organization switcher allows you to quickly change between Secure Endpoint organizations. You must have accounts in each organization to switch between them. The organization switcher will only be visible if you have accounts in multiple organizations. The name of the current organization is displayed in the ribbon. The ribbon displays the number of connectors in the organization, the number of compromises in the organization, and the number of threat detected events.

To switch to another organization:

1. Click the Switch button to display the list of organizations.
2. Select the organization you want to access.

IMPORTANT! The organization switcher is a great feature of Secure Endpoint that allows a user belong to multiple organizations and switch between them. However, there can be some unexpected behavior related to this. When you first log in to Orbital or SecureX, you are assigned a session for the Secure Endpoint organization that you are logged in to. If you switch organizations in Secure Endpoint, the organization is NOT switched in Orbital or SecureX. To switch organizations in Orbital or SecureX, you must log out of those systems, then log in again and select the organization you want to use.

Customer Summary Page

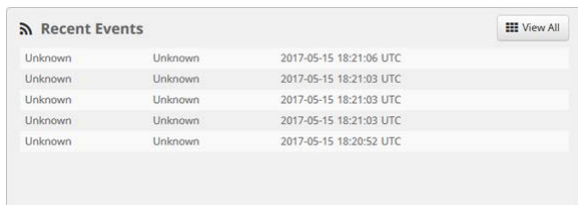
To view a summary of recent activity in the customer's environment, click on the user's name. This will allow you to impersonate the customer and will take you to the customer's account summary page.

Customer Company

The screenshot displays the Customer Summary Page with several panels:

- Recent Events:** A table showing five events, all with status 'Unknown' and timestamps from 2017-05-15 18:21:06 UTC to 18:20:52 UTC.
- Recent Computers:** A table listing five Windows 7, SP 1.0 computers with version 5.1.1.10393. Hostnames include Demo_Zoot, Demo_Dyre, Demo_Ramnit, Demo_Tinba, and Demo_Upatre. Groups are Audit, Protect, Audit, Triage, and Audit.
- Recent Audit Logs:** A table showing six audit log entries for user impersonation and logout, all from @cisco.c, with timestamps from 2017-06-07 21:11:31 UTC to 17:04:04 UTC.
- Recent Outbreak Control Lists:** Two lists: 'File List' (File Blacklist) and 'Exclusion Set' (Workstation Exclusions), both from 2017-05-15 18:41:41 UTC and 18:41:42 UTC respectively.
- Recent Policies:** A table showing five policies: Protect, Audit, Triage, Protect, and Audit, all from 2017-05-15 18:42:16 UTC.
- Applications:** A section stating 'No applications found'.

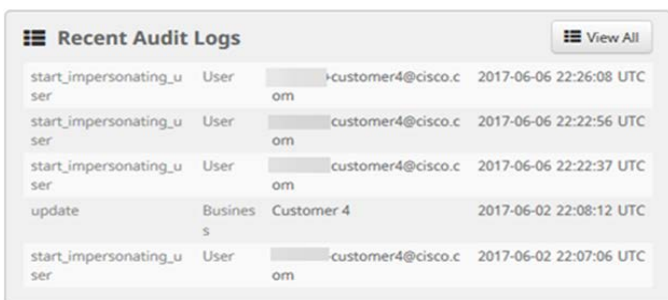
Recent Events display events that have been detected on the customer's organization in the selected time period. Event types include malware, compromises, quarantined files, scans, remote file fetches, installs/uninstalls and so on. Clicking on **View All** will take you to the **Events** tab of the customer's Secure Endpoint console. For more information about the Events tab, see the Secure Endpoint User Guide.



The screenshot shows a table titled "Recent Events" with a "View All" button. The table contains five rows of event data.

Event Type	User	Timestamp
Unknown	Unknown	2017-05-15 18:21:06 UTC
Unknown	Unknown	2017-05-15 18:21:03 UTC
Unknown	Unknown	2017-05-15 18:21:03 UTC
Unknown	Unknown	2017-05-15 18:21:03 UTC
Unknown	Unknown	2017-05-15 18:20:52 UTC

Audit logs display administrative events that have taken place within the customer's account, such as impersonating customers, updating policies, creating and/or disabling customers and users. **Recent Audit Logs** shows the most recent audit logs for the user's customers.

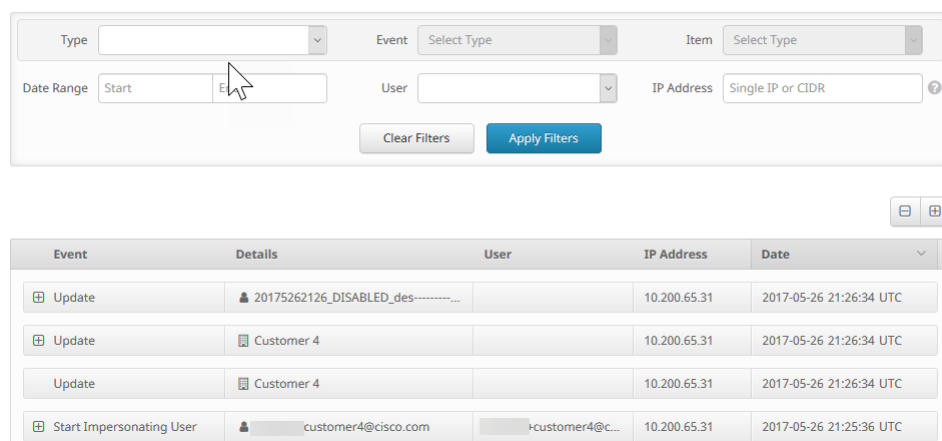


The screenshot shows a table titled "Recent Audit Logs" with a "View All" button. The table contains five rows of audit log data.

Event Type	User	Item	Timestamp
start_impersonating_user	User	customer4@cisco.com	2017-06-06 22:26:08 UTC
start_impersonating_user	User	customer4@cisco.com	2017-06-06 22:22:56 UTC
start_impersonating_user	User	customer4@cisco.com	2017-06-06 22:22:37 UTC
update	Business	Customer 4	2017-06-02 22:08:12 UTC
start_impersonating_user	User	customer4@cisco.com	2017-06-02 22:07:06 UTC

Clicking **View All** on the Recent Audit Log page will display the audit log for all activity on the customer's account. For more information about the Audit Log, see the Secure Endpoint User Guide.

Audit Log



The screenshot shows the Audit Log interface. At the top, there are filter controls for Type, Event, Item, Date Range, User, and IP Address. Below the filters are "Clear Filters" and "Apply Filters" buttons. The main part of the screenshot shows a table with columns: Event, Details, User, IP Address, and Date. The table contains four rows of audit log data.

Event	Details	User	IP Address	Date
Update	20175262126_DISABLED_des-----		10.200.65.31	2017-05-26 21:26:34 UTC
Update	Customer 4		10.200.65.31	2017-05-26 21:26:34 UTC
Update	Customer 4		10.200.65.31	2017-05-26 21:26:34 UTC
Start Impersonating User	customer4@cisco.com	customer4@c...	10.200.65.31	2017-05-26 21:25:36 UTC

Secure Endpoint policies allow you to define Cisco Secure Endpoint Connector behavior for different groups. You can assign Outbreak Control and Exclusion lists to groups through policies. For more information about Secure Endpoint policies, see the Secure Endpoint User Guide.

Customer Summary Page

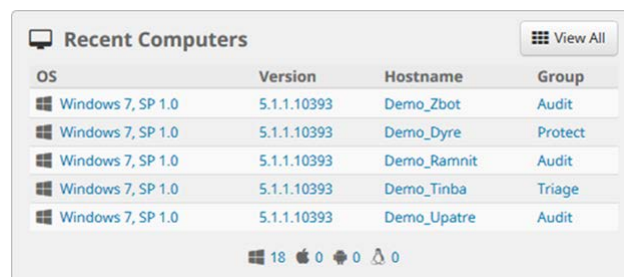
Recent policies displays the policies that have been deployed in the customer's environment during the selected time period. Clicking on a specific policy will take you to the **Edit Policy** page. Click **View All** to see all of the policies that are deployed in the customer's Secure Endpoint Console. Clicking on a policy will show to which groups the policy has been assigned and a summary of the settings for that policy. You can also create, edit, and delete policies from this screen.



The screenshot shows a table titled "Recent Policies" with a "View All" button. The table lists five policies, all deployed on 2017-04-19 at 17:09:02 UTC. The policies are: Protect Policy for Linux, Audit Policy for Linux, Triage Policy for Mac, Protect Policy for Mac, and Audit Policy for Mac.

Policy Name	Deployment Date
Protect Policy for Linux	2017-04-19 17:09:02 UTC
Audit Policy for Linux	2017-04-19 17:09:02 UTC
Triage Policy for Mac	2017-04-19 17:09:02 UTC
Protect Policy for Mac	2017-04-19 17:09:02 UTC
Audit Policy for Mac	2017-04-19 17:09:02 UTC

Recent Computers displays computers that have recently been active in the customer's organization. It lists the operating system, version, and hostname of each computer. It also lists the Secure Endpoint group to which the computer belongs, such as **Audit**, **Protect**, or **Triage**. For more information on Secure Endpoint groups, see the Secure Endpoint User Guide.

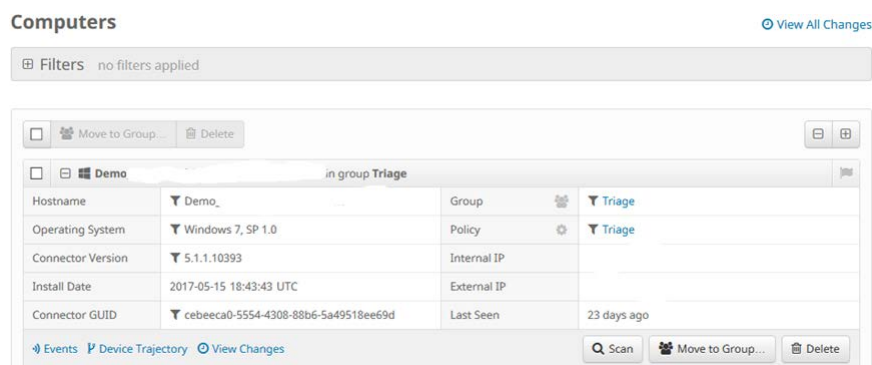


The screenshot shows a table titled "Recent Computers" with a "View All" button. The table lists five Windows 7 computers, all with version 5.1.1.10393. The computers are: Demo_Zbot (Audit), Demo_Dyre (Protect), Demo_Ramnit (Audit), Demo_Tinba (Triage), and Demo_Upatre (Audit). At the bottom, there is a breakdown of the number of recent computers by operating system: 18 Windows, 0 Mac, 0 Linux, and 0 Solaris.

OS	Version	Hostname	Group
Windows 7, SP 1.0	5.1.1.10393	Demo_Zbot	Audit
Windows 7, SP 1.0	5.1.1.10393	Demo_Dyre	Protect
Windows 7, SP 1.0	5.1.1.10393	Demo_Ramnit	Audit
Windows 7, SP 1.0	5.1.1.10393	Demo_Tinba	Triage
Windows 7, SP 1.0	5.1.1.10393	Demo_Upatre	Audit

OS Breakdown: 18 Windows, 0 Mac, 0 Linux, 0 Solaris

At the bottom of the Recent Computers window is a breakdown of the number of recent computers by operating system. You can click on the number next to the icon representing each operating system to view the computers running the respective operating system. You also can click the **View All** button to open the Computers page, which shows a list of all of the customer's computers. On the Computers page, you can click the **+** beside the computer names to expand the detailed view of each computer.



The screenshot shows the "Computers" page. At the top, there is a "Filters" section with "no filters applied" and a "View All Changes" link. Below this is a table showing details for a computer named "Demo" in the "Triage" group. The table includes fields for Hostname, Operating System, Connector Version, Install Date, and Connector GUID. At the bottom, there are links for "Events", "Device Trajectory", and "View Changes", along with buttons for "Scan", "Move to Group...", and "Delete".

Field	Value
Hostname	Demo_...
Operating System	Windows 7, SP 1.0
Connector Version	5.1.1.10393
Install Date	2017-05-15 18:43:43 UTC
Connector GUID	cebeeca0-5554-4308-88b6-5a49518ee69d

Buttons: Events, Device Trajectory, View Changes, Scan, Move to Group..., Delete

Organization Page

Recent Outbreak Control Lists displays the outbreak control lists that have been applied in a customer's environment during the selected time period. You can click on a list or the **View All** button to view and configure details of the list. For more information on outbreak control lists, see the Secure Endpoint User Guide.

File List	Quick SCD	2017-04-03 22:23:59 UTC	View All
Exclusion Set	Workstation Exclusions For Windows	2017-04-03 22:24:00 UTC	View All

Applications displays the applications external to Secure Endpoint that you have authorized to access your organization's data. When you select the name of an application from your list, you will see the current settings for that application, as well as the type of application, its authorizations, and the groups it is receiving events for. From this view, you can also deauthorize any data streams the device is receiving. For more information about applications, see the Secure Endpoint User Guide.

Organization Page

The **Organization Settings** page under the **Accounts** drop-down allows you to manage the account settings for the MSSP Partner Organization.

You can edit the organization by clicking the **Edit** button. From here, you can edit the organization name and Support Email/URL, as well as configure TSV by clicking **Two Step Verification**. You can also click **Configure Single Sign-On** to access your SSO settings.

< Edit Business

Business Name

Support Email/URL

[Cancel](#)

[Update](#)

Features

Requires [Two Step Verification](#)

Single Sign-On

[Disabled](#)

[Configure Single Sign-On](#)

MSSP API

You can use the MSSP API to create customers and retrieve the status for all customers using the MSSP customer creation, customer status, list customer, and disable customer API. The api_endpoint for these API calls depend on your region:

- North America: api.amp.cisco.com
- Europe: api.eu.amp.cisco.com
- Asia: api.apjc.amp.cisco.com

The MSSP-specific APIs are under <api_endpoint>/v1/mssp.

MSSP API

Go to Accounts -> API Credentials to generate your API Client ID and API Key.

1. Click **+New Credentials**.
2. Enter a name in the Application Name field.
3. Select the Read & Write scope.
4. Click **Create**.
5. Note the 3rd Party API Client ID and API Key that are generated.

IMPORTANT! This information cannot be displayed again after you leave this page so if you forget the credentials or need to change them you will have to delete the credentials and create new ones.

You can also authenticate to this API by making calls such as:

```
https://<your_client_id>:<your_api_key>@<api_endpoint>
```

You can also use Basic HTTP Authentication:

1. Base64 encode the 3rd Party API Client ID, the colon (":"), and the API Key together.
2. Prepend the string "Basic" as the Authorization header.
3. Send that header with your API call.

For example, if your 3rd Party API Client ID was "1234" and your API Key was "atest", then your base64 encoded string would be "MTIzNDphdGVzdA==". The header that you would send would be:

```
Authorization: Basic MTIzNDphdGVzdA==
```

IMPORTANT! Be careful not to encode a newline in the base64 string. For more information see [RFC 1945](#).

You should also have the Headers "Accept: application/json" and "Content-type: application/json" included in your requests.

Create New MSSP Customer

You can create a new customer by sending a POST to <base_url>/v1/mssp/customers. The data must have the following attributes:

Table 1 New MSSP Customer Attributes

Attribute	Description
email	Email address of the first user being created.
password	Password used for the first user's Cisco Security Account. This will be removed in the future.
first_name	First name of the first user being created.
last_name	Last name of the first user being created.
business_name	Name of the organization being created.
payment_state_id	1 = licensed, 2 = Evaluation

If no payment_state_id value is passed, then the payment state will default to the same value as the MSSP partner account. You should use Evaluation for testing purposes.

MSSP API

Example:

```
curl -X POST https://<api_endpoint>/v1/mssp/customers -d '{
  "email": "testuser@test.com",
  "password": "Passw0rd!",
  "first_name": "John",
  "last_name": "MSSP Test Customer",
  "payment_state_id": 2,
  "business_name": "mssp_customer_business"
}' -H 'Authorization: Basic MTIzNDphdGVzdA==' -H 'Accept: application/json' -H
'Content-type: application/json'
```

Will return:

```
{
  "version": "v1.2.0",
  "metadata": {
    "links": {
      "self": " https://<api_endpoint>/v1/mssp/customers"
    }
  },
  "data": {
    "business_name": "mssp_customer_business",
    "email": " testuser@test.com",
    "status": "Customer business creation is scheduled"
  }
}
```

Upon completion you will be presented with an HTTP Response.

Table 2 HTTP Response Codes

HTTP Status Code	Description
200	Successfully created.
202	Email already exists.
400	Error in your JSON.
401	Error in authentication or Unauthorized. You should confirm you are using Read & Write API Credentials.
429	Rate limit has been exceeded.

Check MSSP Customer Creation Status

The creation of an MSSP customer runs as a batch process, so the first POST queues the creation of the account. You can check on the status of that customer by creating a GET to <base_url>/v1/mssp/customers/status with the following parameters:

Table 3 MSSP Customer Status Attributes

Attribute	Description
email	Email address of the first user being created.

MSSP API

Example:

```
curl -X GET https://<api_endpoint>/v1/mssp/customers/status -d '{"email":  
"mssp+customer+test9@cisco.com"}' -H 'Authorization: Basic MTIzNDphdGVzdA==' -H 'Accept:  
application/json' -H 'Content-type: application/json'
```

Will return:

```
{  
  "version": "v1.2.0",  
  "metadata": {  
    "links": {  
      "self": "https://<api_endpoint>/v1/mssp/customers/status"  
    }  
  },  
  "data": {  
    "business_name": "mssp_customer_business",  
    "email": "testuser@test.com",  
    "status": "completed"  
  }  
}
```

Upon completion you will be presented with an HTTP Response.

Table 4 HTTP Response Codes

HTTP Status Code	Description
200	Successfully created.
400	Error in your JSON.
401	Error in authentication or Unauthorized. You should confirm you are using Read & Write API Credentials.
404	Email address does not exist in the list of MSSP customers.
429	Rate limit has been exceeded.

Then you will receive a status.

Table 5 MSSP Customer Status

Status	Description
completed	Successfully created.
processing	Provisioning in process.
not found	Email address does not exist in the list of MSSP customers.

List Status of all MSSP Customers

Use this to display the status of an MSSP customer. Create a GET to <base_url>/v1/mssp/customers with no parameters.

Example:

```
curl -X GET https://<api_endpoint>/v1/mssp/customers -H 'Authorization: Basic  
MTIzNDphdGVzdA==' -H 'Accept: application/json' -H 'Content-type: application/json'
```

MSSP API

Will return:

```
{
  "version": "v1.2.0",
  "metadata": {
    "links": {
      "self": "https://<api_endpoint>/v1/mssp/customers"
    }
  },
  "data": [
    {
      "customer_name": "mssp_customer_business",
      "provisioning_status": "completed",
      "connector_count": 0,
      "percent_compromised": 0
    }
  ]
}
```

Upon completion you will be presented with an HTTP Response.

Table 6 HTTP Response Codes

HTTP Status Code	Description
200	Successfully created.
400	Error in your JSON.
401	Error in authentication or unauthorized. You should confirm you are using Read & Write API Credentials.
429	Rate limit has been exceeded.

Fetch MSSP Total Monthly Usage

Use this to fetch the total monthly usage of an MSSP partner for the previous month. Create a GET to <base_url>/v1/mssp/customer_usage_reports/total_monthly_usage with no parameters.

Example:

```
curl -X GET https://<api_endpoint>/v1/mssp/customer_usage_reports/total_monthly_usage -H 'Authorization: Basic MTIzNDphdGVzdA==' -H 'Accept: application/json' -H 'Content-Type: application/json'
```

MSSP API

Will return:

```
{
  "version": "v1.2.0",
  "metadata": {
    "links": {
      "self": "http://test.host/v1/mssp/customer_usage_reports/total_monthly_usage"
    }
  },
  "data": {
    "External_Ref_ID": "111",
    "Usage_Type": "SPLA-AMP4E",
    "Category": "",
    "Location": "",
    "Start_Time": "07/01/2021 00:00",
    "End_Time": "07/31/2021 23:59",
    "Quantity": "0",
    "UoM": "Nodes",
    "usage_attr_1": "",
    "usage_attr_2": "",
    "usage_desc": "",
    "Customer_Name": "",
    "Customer_Addr": "",
    "Customer_City": "",
    "Customer_State": "",
    "Customer_Zip": "",
    "Customer_Country": ""
  }
}
```

Upon completion you will be presented with an HTTP Response.

Table 7 HTTP Response Codes

HTTP Status Code	Description
200	Success.
401	Authentication error or unauthorized. Confirm you are using API credentials with read and write permission.
404	MSSP partner business not found.

Disable MSSP Customer

Use this to disable an MSSP customer for any reason. Send a DELETE to <base_url>/v1/mssp/customers with the following parameters:

Table 8 Disable MSSP Customer Attributes

Attribute	Description
email	Email address of the first user created.

MSSP Detailed Monthly Usage API endpoint

Example:

```
curl -X DELETE <base_url>/v1/mssp/customers -d '{"email":  
"mssp+customer+test9@cisco.com"}' -H 'Authorization: Basic MTIzNDphdGVzdA==' -H  
'Accept: application/json' -H 'Content-type: application/json'
```

Will return:

```
{  
  "version": "v1.2.0",  
  "metadata": {  
    "links": {  
      "self": "https://api-qa-ext.immunet.com/v1/mssp/customers"  
    }  
  },  
  "data": {  
    "business_name": "mssp_customer_business",  
    "email": " testuser@test.com ",  
    "status": "Customer business is destroyed"  
  }  
}
```

Upon completion you will be presented with an HTTP Response.

Table 9 HTTP Response Codes

HTTP Status Code	Description
200	Successfully created.
400	Error in your JSON.
401	Error in authentication or unauthorized. You should confirm you are using Read & Write API Credentials.
404	Email address does not exist in the list of MSSP Customers.
429	Rate limit has been exceeded.

MSSP Detailed Monthly Usage API endpoint

This endpoint provides detailed billing information. As an authenticated API endpoint, it requires API credentials (Client ID & API Key).

API client_id:api_key Base64 encoded as \$BASIC_AUTH

Request sample:

```
GET /v1/mssp/customer_usage_reports/detailed_monthly_usage
```

```
curl http://test.host/v1/mssp/customer_usage_reports/detailed_monthly_usage  
-X GET  
-H 'Accept: application/json'  
-H 'Content-Type: application/json'  
-H 'Authorization: Basic $BASIC_AUTH'
```

MSSP Detailed Monthly Usage API endpoint

Success - 200 response sample:

```
{
  "version": "v1.2.0",
  "metadata": {
    "links": {
      "self": "http://test.host/v1/mssp/customer_usage_reports/detailed_monthly_usage"
    }
  },
  "data": {
    "partner_name": "Partner business",
    "partner_sple_sub_ref": "Sub1234",
    "start_time": "07/01/2021 00:00",
    "end_time": "07/31/2021 23:59",
    "billed_connector_usage": "0",
    "customers": [
      {
        "customer_name": "Customer business",
        "billed_connector_usage": "0"
      },
      {
        "customer_name": "Customer business 2",
        "billed_connector_usage": "0"
      }
    ]
  }
}
```

Not Found - 404 response sample:

```
{
  "version": "v1.2.0",
  "metadata": {
    "links": {
      "self": "http://test.host/v1/mssp/customer_usage_reports/detailed_monthly_usage"
    }
  },
  "data": {},
  "errors": [
    {
      "error_code": 404,
      "description": "Not Found",
      "details": "Not Found"
    }
  ]
}
```

MSSP Detailed Monthly Usage API endpoint

Unauthorized - 401 response sample:

```
{
  "version": null,
  "data": {},
  "errors": [
    {
      "error_code": 401,
      "description": "Unauthorized",
      "details": [
        "Unknown API key or Client ID"
      ]
    }
  ]
}
```

Fetch MSSP Detailed Monthly Usage

Use this to fetch the MSSP detailed monthly usage of an MSSP Partner for the previous month. Create a GET to /v1/mssp/customer_usage_reports/detailed_monthly_usage with no parameters.

Example:

```
curl -X GET https://<api_endpoint>/v1/mssp/customer_usage_reports/detailed_monthly_usage -H
'Authorization: Basic MTIzNDphdGVzdA==' -H 'Accept: application/json' -H 'Content-Type:
application/json'
```

MSSP Detailed Monthly Usage API endpoint

Will return:

```
{
  "version": "v1.2.0",
  "metadata": {
    "links": {
      "self": "http://test.host/v1/mssp/customer_usage_reports/detailed_monthly_usage"
    }
  },
  "data": {
    "partner_name": "Partner business",
    "partner_sple_sub_ref": "Sub1234",
    "start_time": "07/01/2021 00:00",
    "end_time": "07/31/2021 23:59",
    "billed_connector_usage": "0",
    "customers": [
      {
        "customer_name": "Customer business",
        "billed_connector_usage": "0"
      },
      {
        "customer_name": "Customer business 2",
        "billed_connector_usage": "0"
      }
    ]
  }
}
```

Upon completion you will be presented with an HTTP Response.

Table 10 HTTP Response Codes

HTTP Status Code	Description
200	Successfully completed.
401	Error in authentication or unauthorized. You should confirm you are using Read & Write API Credentials.
404	MSSP partner business was not found.