opentext™

ArcSight ESM

Software Version: 7.8

ESM Best Practices: Multitenancy and Managed Security Service Providers

Document Release Date: August 2024
Software Release Date: August 2024

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Trademark Notices

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

Chapter 1: Introduction

ArcSight Enterprise Security Management (ESM) consolidates and normalizes data from disparate devices across your enterprise network in a centralized view. ESM provides a holistic view on the security status of all relevant IT systems, and integrates security into your existing management processes and workflows.

Multitenancy is an ESM architecture in which ESM is set up to support threat detection for multiple, completely separate tenants. A tenant is a group of users sharing the same view on the software they are using. With a multitenant architecture, ArcSight ESM is designed to provide every tenant a dedicated share of the instance, including its data, configuration, user management, tenant-specific functionality, and other properties.

If you are a managed security service provider (MSSP) or serve multiple end users within the organization, these multitenancy best practices are for you.

After reading this guide, you will have an understanding of:

- ArcSight deployment architectures
- Network modeling
- ESM content building
- ESM provisioning
- Troubleshooting tips

This section includes the following topics:

Who Should Read this Guide

This guide is intended for all levels of ESM users interested in learning how to deploy ESM in MSSP or large enterprise with MSSP architectures. You should have a basic understanding of the following topics:

- Networks and network security
- Internet and software application browsing conventions

In this guide, the terms tenant and customer may be used interchangeably.

Prerequisites

The guidelines in this document are based on ESM 6.8 and later. OpenText releases new features and enhancements that may affect functionality described here. For such updates, the document will specify the applicable ESM version.

This guide assumes that you have a strong background in ArcSight concepts.

- You should have a basic understanding of ESM operations, networks, and network security. A good starting point would be to read (missing or bad snippet).
- You must be familiar with the ArcSight Console and ArcSight Command Center user interface for building ESM content and configuration.
- You should have completed courses on ArcSight security products.

Chapter 2: ESM Architectures for MSSPs

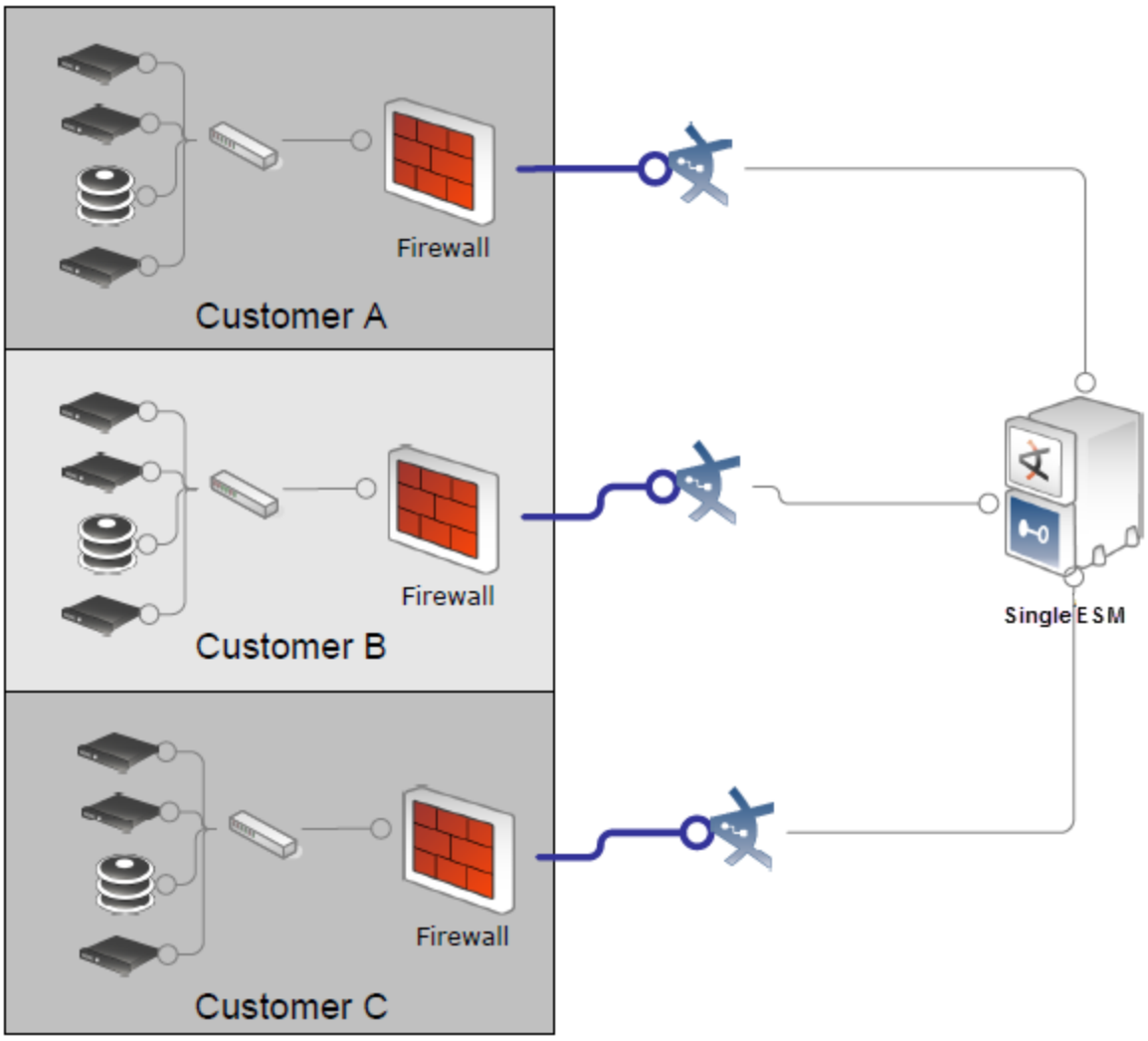
ESM consists of several separately installable components that work together to process event data from your network. These components connect to your network through sensors that report to SmartConnectors. SmartConnectors translate a multitude of device output into a normalized ESM schema that becomes the starting point for ESM's correlation capabilities.

Topics in this section:

Single ESM Server

ESM is most often deployed in a single configuration. That means you are using a single Manager instance. In this configuration, all events coming from end devices such as firewalls and IDSs are collected and processed by ArcSight SmartConnectors, which then send the events to a single ArcSight Manager.

In an MSSP environment, this also means that data collected from multiple tenants are processed centrally by one Manager. Physical separation of client data is not possible in this configuration. However, ESM provides very granular access controls that will prevent tenants from seeing each other's data.



Advantages

A single ArcSight Console can control and view all customers (tenants) and events. Patches, upgrades, ArcSight Update Packs (AUPs), and system updates are easy to maintain. ESM configuration is also easy to manage because you update rules and content in only one place.

Disadvantages

In a single-ESM environment, physical separation of client data is not possible. Scalability is limited to the capability of the Manager (its CPU) and storage configurations.

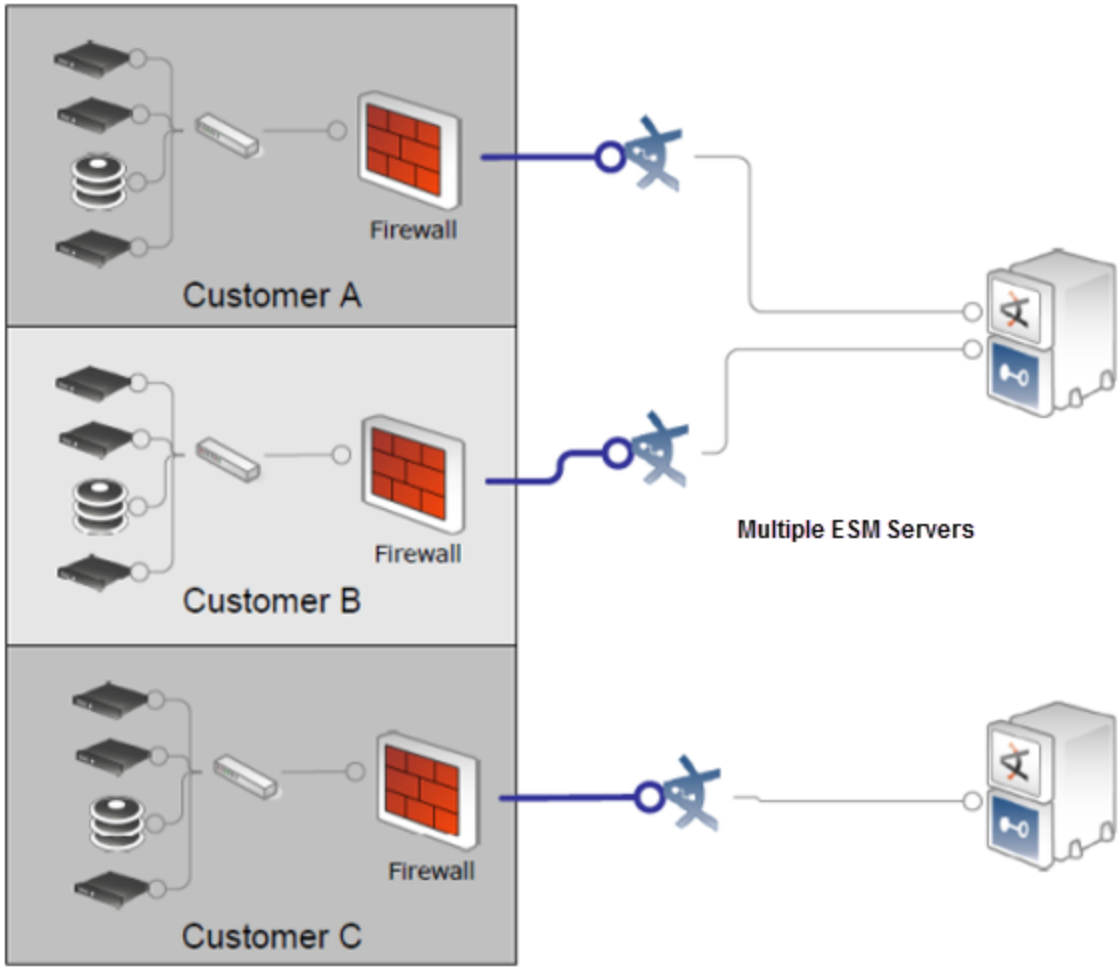
Multiple ESM Servers

In a multiple-ESM architecture, you have more than one ArcSight Manager. The decision for using multiple Managers can be both technical and business driven. The technical reasons are typically for scalability or physically separate environments. If the sheer volume of data is too much for one Manager, then you can install an additional Manager. If parts of a network are not physically connected, then a separate Manager is required. There may be non-technical reasons for distributing across multiple Managers. For instance, the collection and processing may be broken up to match business units or region.

In an MSSP environment, you can use multiple ArcSight Managers to address both technical and business needs. As the customer base increases, so does the volume of events a single Manager must handle. When a Manager reaches its processing threshold, deploy a new Manager to handle the new volumes of events.

The threshold of each Manager can be predetermined by running a series of performance tests. These tests show the theoretical limit in terms of events per second (EPS) for that Manager configuration. Then, as you add new tenants, and volume increases and approaches that limit, it is time to deploy a new Manager.

Depending on the service levels or business design, the MSSP may provide an optional service where a tenant pays for a dedicated ESM instance.



Advantage

You can easily achieve physical separation of client data and the architecture is easier to scale.

Disadvantages

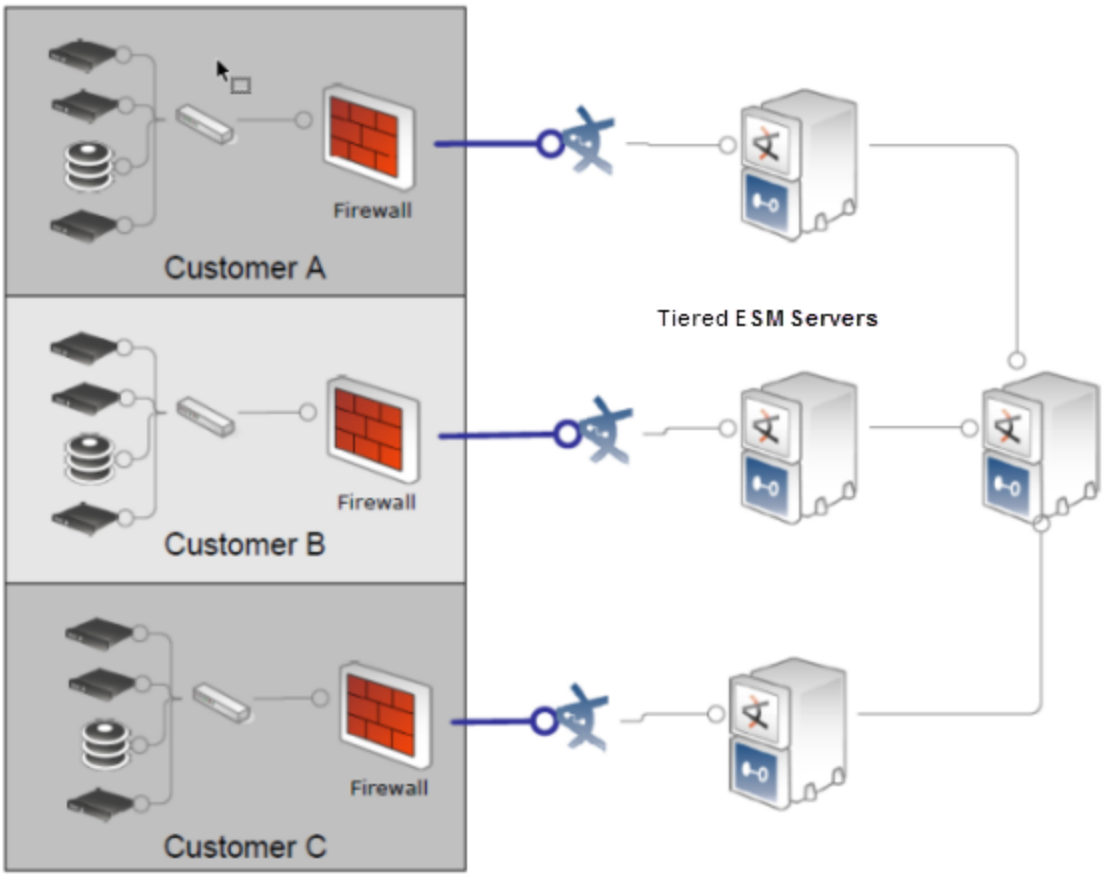
- There is no cross correlation across all tenants or sharing of data between Managers.
- SOC workflow, including stages, annotations, and case management is done in separate Console instances.
- Configuration management is done at each Manager instance.

Tiered ESM Servers

Tiered ESM deployments combine many of the benefits from single and multiple ESM deployment options.

In a tiered environment, there is more than one ArcSight Manager. In this case, the lower-tiered Managers are configured to send their critical events and correlation events up to a single primary Manager. The primary Manager typically will be the single location for operators and analysts to perform their duties.

In a typical MSSP environment, the primary Manager provides a key service such as correlation and trend monitoring across the customer base. Tenants would only view the data at the first tier. The MSSP SOC would typically only have access to the primary Manager.



Advantages

A tiered ESM deployment:

- Simplifies the segregation of accessibility because tenants have access only to their dedicated machines.
- Provides high level of data separation as each tenant data is stored on a dedicated system. In events that are forwarded to the primary Manager, sensitive information can be obfuscated.
- Allows selective cross-correlation between different tenants' events.
- Allows the MSSP SOC operators to monitor tenants' events from a single Console.

Disadvantages

Managing multiple servers can be complex, but the content management feature introduced in ESM 6.5 may help simplify some tasks.

See also:

- "Content Management" in the (missing or bad snippet)
- "Creating or Editing Packages," which includes information for package format to use in content synchronization, in the (missing or bad snippet)

SmartConnector Location

One of the critical decisions to make is the location of SmartConnectors. This decision can be driven by the device logging technology, reliability of transport, location of tenant security management systems, and central IDS management system. In general, the connectors can be located either at the individual tenant's site or at a central MSSP site.

Caution: Do not grant tenants Write (W) access to `/All Connectors` to prevent unauthorized users from executing ESM commands using the API connector services.

See "Permissions to Resources" on page 26 for related discussion.

At the Tenant Site

Placing a connector on the tenant's site increases the reliability of data collection. After a connector collects the data locally at the tenant site, this data is then securely and reliably

transmitted to a Manager. If the link between the MSSP and the tenant goes down, whether the link is physical or through VPN, the connector caches data until the link is restored.

Filtering occurs at the tenant site, therefore reducing WAN bandwidth consumption. Obfuscation of sensitive information occurs at the tenant's premise, ensuring that sensitive information stays there.

Note: Deploying the connector hosting appliance simplifies connector deployment without using tenant IT resources.

At the MSSP Site

If the MSSP provides the security end devices such as firewalls or IDSs to its tenants as part of its service, then the MSSP most likely uses that technology's centralized management system. In this case the connector is on the MSSP site next to the central management systems. This configuration presents a challenge because typically, in this configuration, the central management system is collecting from multiple tenants at the same time. The key is to differentiate each client's data from each other. Fortunately, ESM can model each tenant and differentiate client data through its network modeling capability (see "Using the Network Model in an MSSP Environment" on page 15).

Chapter 3: Using the Network Model in an MSSP Environment

This chapter assumes you are familiar with the fundamentals of network modeling in ArcSight or have read the section, "The Network Model," in *ESM 101*. This chapter reviews the network model topic and reiterates key rules in building assets within ArcSight. Then we will cover three main network and ArcSight scenarios that an MSSP might have to address when modeling their environment.

The networking modeling scenarios are

- Dedicated connectors per tenant
- Centralized connectors with multiple tenants, non-overlapping address space
- Centralized connectors with multiple tenants, overlapping address space

Topics in this section:

Network Model Terminology and Rules

ESM uses the following resources to model the network.

Assets represent individual nodes on the network, such as servers, routers, and laptops.

- Physical asset
- Mutually exclusive, collectively exhaustive (MECE); meaning, there can be no overlaps on any two assets in the entire network.
- Assigned to different zones for the same address
- Inherits categories from asset ranges
- Example: 192.0.2.0

Asset ranges represent a set of network nodes addressable by a contiguous block of IP addresses.

- Physical network
- Mutually exclusive, collectively exhaustive (MECE); meaning, there can be no overlaps on any two asset ranges in the entire network
- Assigned to different zones for the same address space
- Example: 192.0.2.0 through 192.0.2.255

Zones represent portions of the network itself and are also characterized by a contiguous block of addresses.

- Zone is a segment of the global logical network
- Mutually exclusive, collectively exhaustive (MECE); meaning, there can be no overlaps on any two zones in the entire network
- Only one network per zone
- Example: USA West DMZ, Hong Kong Internal

Networks are helpful when disambiguating two private address spaces.

- Define the global logical network
- Contain one or more zones
- Example: USA, Hong Kong, Europe
- Configure Connector(s) with Networks

Locations describe the geographic location of assets, asset groups, or zones.

Customers describe the internal or external cost centers, separate business units, or tenants associated with networks, if applicable to your business environment.

- Define owners of the network
- One network belongs to only one customer

Vulnerabilities describe any attributes of an asset that leave it open to exploits.

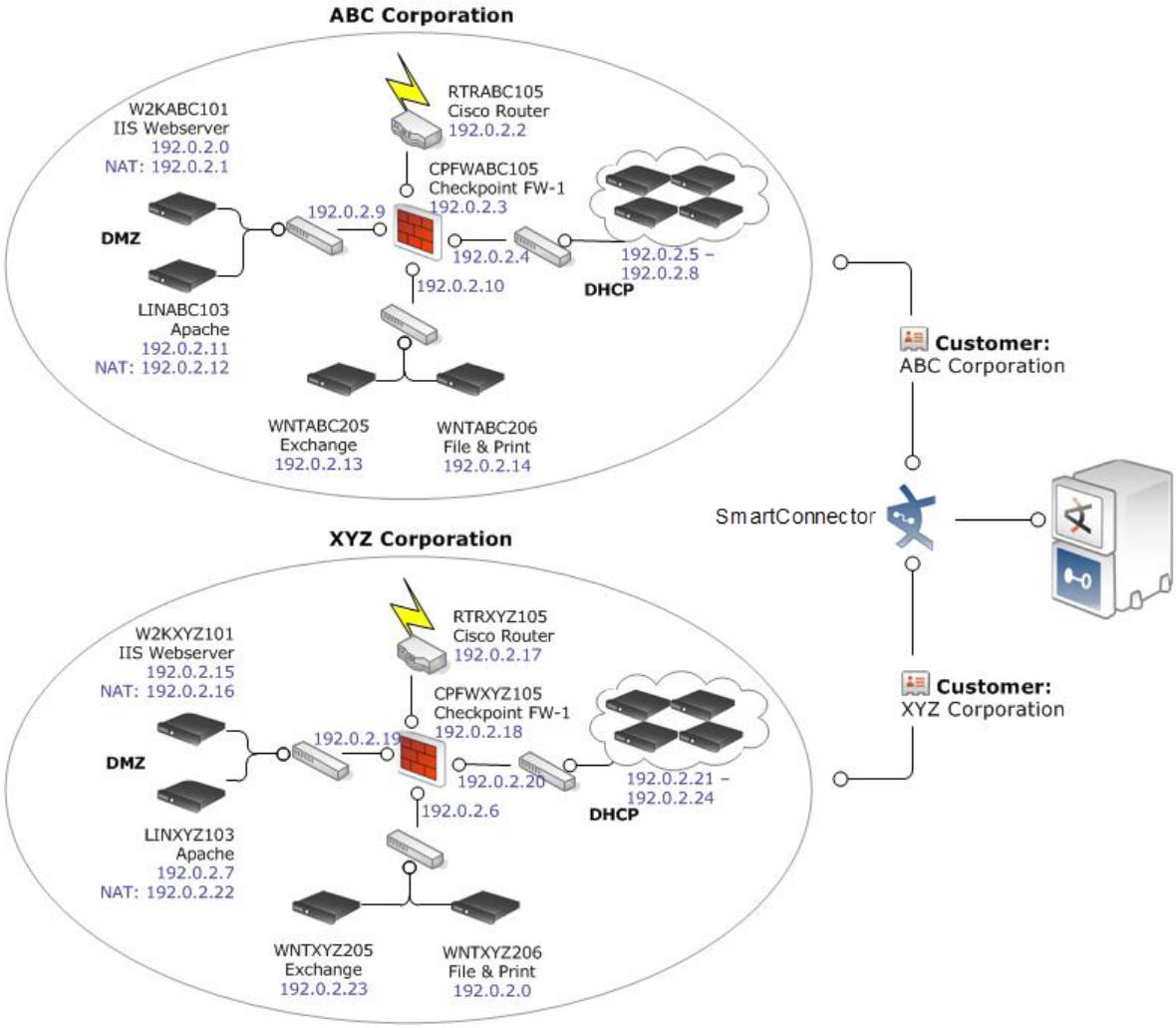
Customer Tagging

Customer tagging is a feature developed mainly to support MSSP environments, although private organizations can use the technique to denote cost centers, internal groups, or business units.

A `Customer` is not a source or target of an event, but it can be thought of as the owner of an event. Content developers can also use the `Customer` tag to develop customer-aware content.

Why is customer tagging critical in MSSP environments? The `Customer` designation identifies who owns the events. This ensures each customer (tenant) can view only its own events.

Consider this scenario: The customer tag is usually assigned based on the reporting device IP address. In an MSSP environment, different customers can have overlapping networks. This requires an elaborate mechanism for assigning a customer attribute to events, described later in "Setting Customer Tags to Events" on page 20.



The MSSP Network Model Challenge

Since most organizations use private address spaces (see https://en.wikipedia.org/wiki/Private_network), addresses included in events from different customers may contain identical addresses but referring to different assets. For example, two tenants may use the private address space 192.0.2.x, and therefore the address 192.0.2.1 may be used by both tenants to refer to a local system.

Make sure you have the proper network information model, which includes zone information, and the asset model, which requires correct zone information. When a connector enriches an

event with asset information derived from the ESM asset model, the event uses the asset address as key for locating asset information. The ESM asset model would therefore need a mechanism to differentiate between assets with the same address but belonging to different customers.

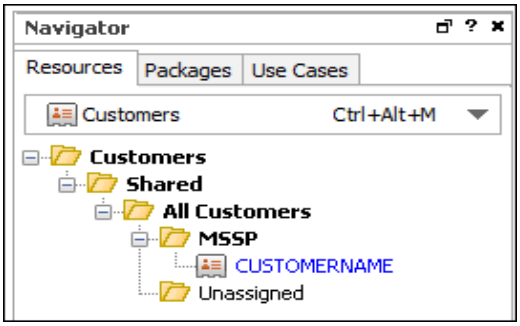
Setting Up the Network Model

This procedure assumes you are familiar with the ArcSight Console and have worked with ESM resources.

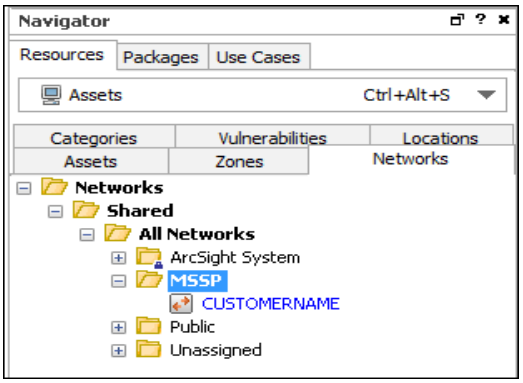
Where: ArcSight Console > Navigator > Resources

Procedure:

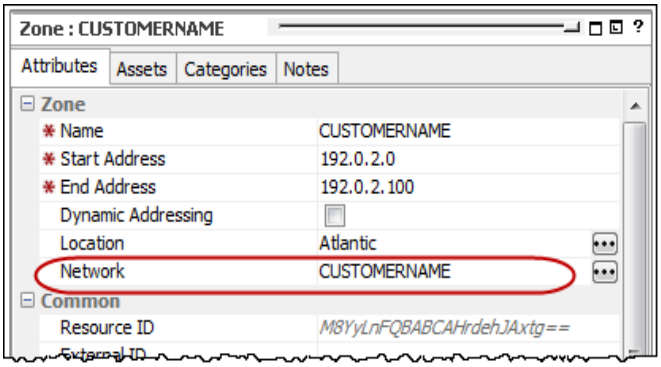
1. Log into the Console with administrator privileges.
2. Select the **Customers** resource and create customers. For example:



3. Create a Network resource for each customer. Use descriptive names to help you distinguish customer networks.

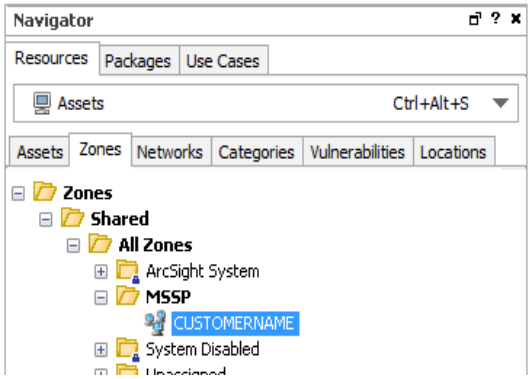


4. Create Zone resources for each customer. For each zone, specify the corresponding network from the previous step:

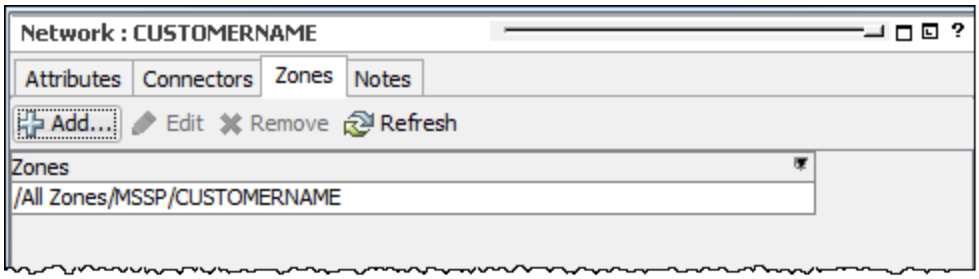


Note: If you save the zone without assigning a network, ESM automatically assigns the zone to `\All Networks\ArcSight System\Local`.

- Even if the address space overlaps between two customers, you must define distinct zones for each customer.
- The Zone resource itself does not refer to a customer, so use descriptive names to help you distinguish customer zones.



Following is an example of a customer zone assigned to a network:



Setting Customer Tags to Events

Setting events with customer tags is done by the connectors. Tagging can be either static or dynamic. There are three possible deployment modes, each one with specific procedures.

- A dedicated connector for a single customer, in which case both static and dynamic assignment of customers apply.

  Note: If you have ESM 6.11.0 or later and are using MSSP Reports, a dedicated connector per customer is the required configuration. See "Using MSSP Reports" on page 44.

- A shared connector that serves multiple customers *without* overlapping IP addresses. This requires dynamic customer assignment.

  Caution: While it is possible to have a shared connector serving customers with overlapping addresses, this setup is risky and can potentially send events to the wrong customer.

Related topics:

- "Using Static Customer Tags" below
- "Using Dynamic Customer Tags" on the next page

Using Static Customer Tags

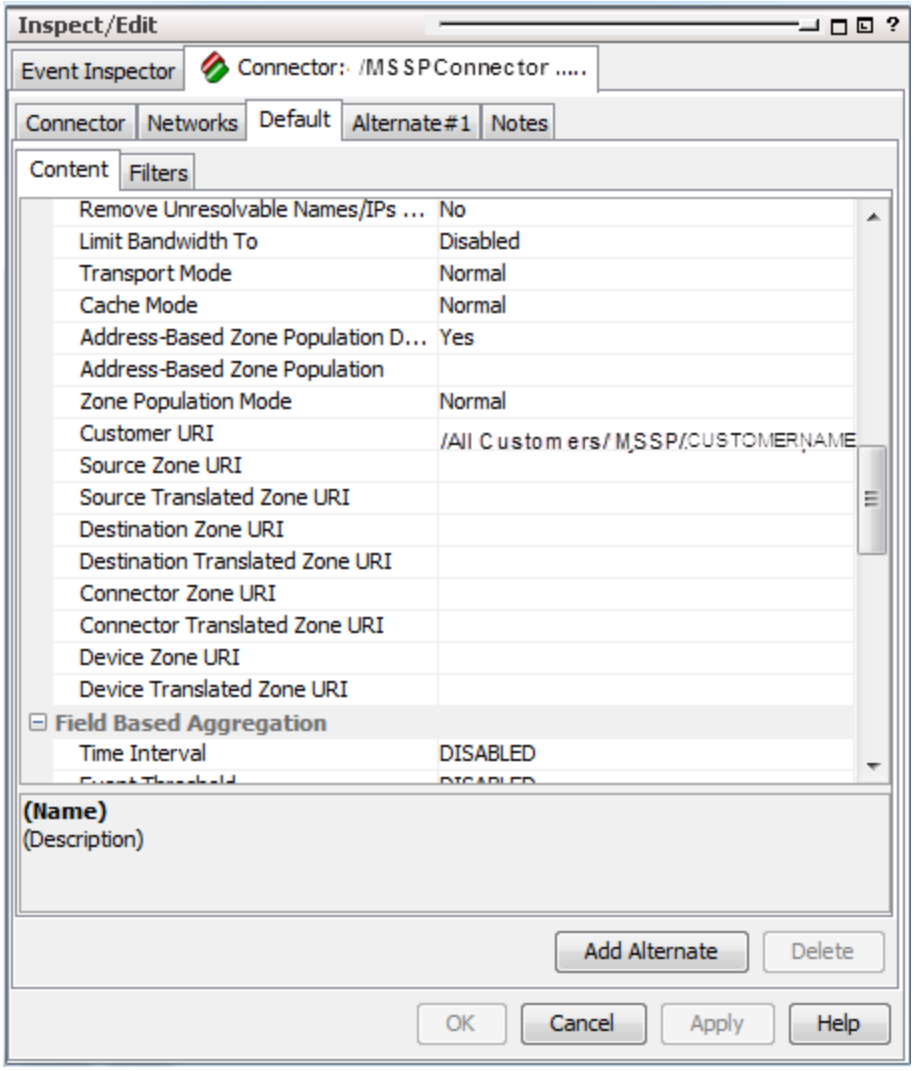
This applies if a registered connector is dedicated to a single customer.

Purpose: To ensure that all events from the single connector are tagged with a specific customer.

Where: Navigator > Connectors

1. Open the connector's editor.
2. Go to the **Default > Content** tab.
3. Under the Network section, set the **Customer URI** field to the customer resource. For example:

```
/All Customers/MSSP/CUSTOMERNAME
```



Using Dynamic Customer Tags

This applies if one registered connector is used for multiple customers with non-overlapping IP addresses.

Purpose: To ensure that all events from the single connector are dynamically tagged so that event fields correctly identify which customer should see those events.

Velocity template or connector map file

You can perform dynamic tagging in one of two ways:

- Through a Velocity template variable
- Through a connector map file

Map files and Velocity templates use different operators that might factor in specific mapping situations.

What are the differences?

- Map files allow multiple mappings with different transformation functions, including static mapping. You can only use one Velocity template for every connector.
- Velocity expressions are set in the ArcSight Console, are part of the resource, are safely persisted in the database, and can be backed up. Map files, on the other hand, are external files. Map files are placed in the connector installation directory. They require manual updates. While not that easy to set up, map files are more flexible and ready for automation.
- Overall, map files offer more power and flexibility. However, for simple setups, Velocity templates might be faster to setup. They do not require access to the connector server.

Using Velocity Templates

You enter a Velocity expression in the connector editor's **Default > Content** tab in the **Customer URI** field. For example:

```
$company_name
```

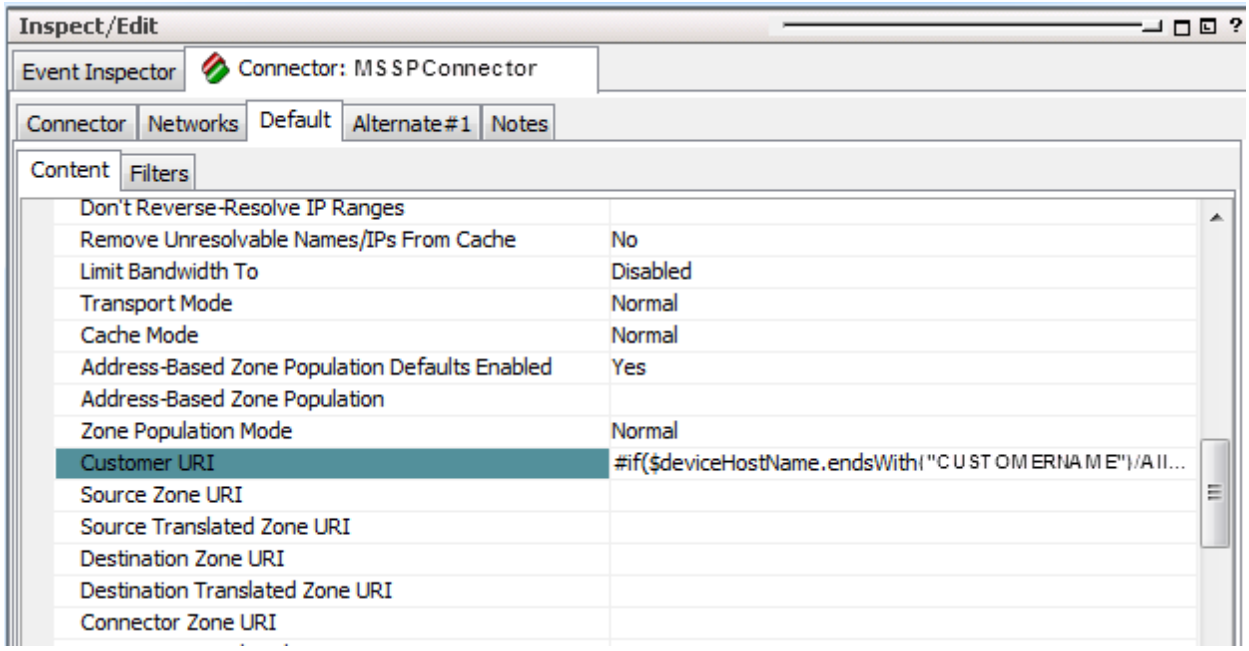
Note: You should be experienced in using Velocity templates. OpenText does not provide error checking or error messaging for user-created expressions.

Where: Navigator > Connectors

To set up the Customer URI with a Velocity template:

1. Right-click the connector and select **Configure**.
2. Go to the **Default** tab. The Content subtab is displayed.
3. In the Content subtab, locate the **Network > Customer URI** setting. Ignore the popup for customer resource selection. You should still be in the Customer URI text field.
4. Enter the Velocity template text into this text field. For example:

   ```
   #if($deviceHostName.endsWith("CUSTOMERNAME"))/All
   Customers/MSSP/CUSTOMERNAME#elseif($deviceHostName.endsWith
   ("CUSTOMERNAME2"))/All Customers/MSSP/CUSTOMERNAME2#end
   ```
5. Click **Apply** or **OK**.



More information:

- "Velocity Examples" on page 52
- http://velocity.apache.org/engine/devel/user-guide.html
- The topic "Velocity Templates" and all subtopics in the Reference section of the (missing or bad snippet)

Using Map Files

Map files can include entries with the following mappings:

Mapping entry	Example
Value mapping	If field A has a value X, assign value Y to field B.
Range mapping	If field A is in the range N-M, assign value Y to field B.
Regular expression mapping	If field A matches regular expression RE, assign value Y to field B.
Expression mapping	Use any of the conditions above, but instead of assigning the constant value Y, assign the result of an expression using any valid connector parser field mapping expression.

Using different techniques, you can set the customer tag based on existing fields in the event, which in turn will indicate the customer "owner."

Value Mapping Using deviceAddress

This example applies to customers with set of distinct IP addresses.

```
event.deviceAddress,set.event.customerURI
192.0.2.0,/All Customers/XYZ Corp
198.51.100.0,/All Customers/ABC Corp
```

Range Mapping Using deviceAddress

This example applies to customers with set of distinct IP addresses.

```
range.event.deviceAddress,set.event.customerURI
192.0.2.0-192.0.2.25,/All Customers/MSSP/CUSTOMERNAME
198.51.100.0-198.51.100.70,/All Customers/MSSP/CUSTOMERNAME2
```

Regular Expression Mapping Using requestURL

```
regex.event.requestURL,set.event.customerURI
http:\/\/www.CUSTOMERNAME.com\/.*, /All Customers/MSSP/CUSTOMERNAME
```

To use a map file:

Store the files on the server where the connector is running. Use the following directory:

`$ARCSIGHT_HOME/user/agent/map/map.`***X***`.properties`

where ***X*** is the next sequential number following any other existing map file in that directory. Updating this file does not require any connector restarts.

More information:

- "Troubleshooting" on page 50 for information related to map file installation
- The section "Map Files" in the (missing or bad snippet)

Chapter 4: Managing Permissions in the MSSP Environment

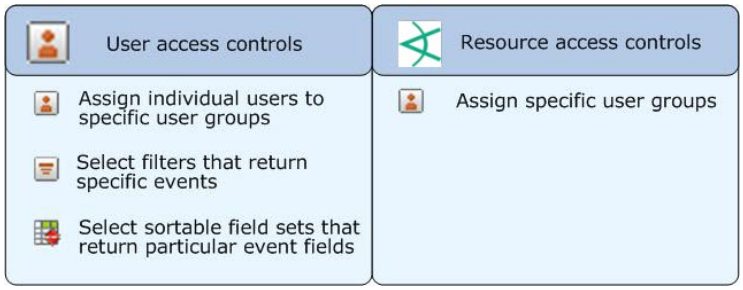
Correct settings of permissions to ESM resources, operations, and events ensure that customers are restricted to their own ESM content, and not any other customers' content.

Topics in this section:

Note: The provisioning section contains links to permissions topics, as required.

Access Control Lists (ACLs)

ESM manages user access to resources using Access Control Lists (ACLs). ACLs are applied to user groups, which allows the users in that group to have read/write access to the resources specified by the ACL.



You can further refine access to individual resources by specifying what user groups can have read/write access to it.

Subgroups inherit the ACL settings of their parent groups. If a resource is assigned to more than one user group, the ACL is the combined list of those two groups.

Users and user groups and the ACLs to which they have access are managed in both the ArcSight Console and the ArcSight Command Center.

There are no explicit "denies" in the ESM ACL implementation. This means that Read and Write are implicitly denied until you explicitly grant permissions.

Note: ACLs in the MSSP environment are discussed further in "The Provisioning Process" on page 29.

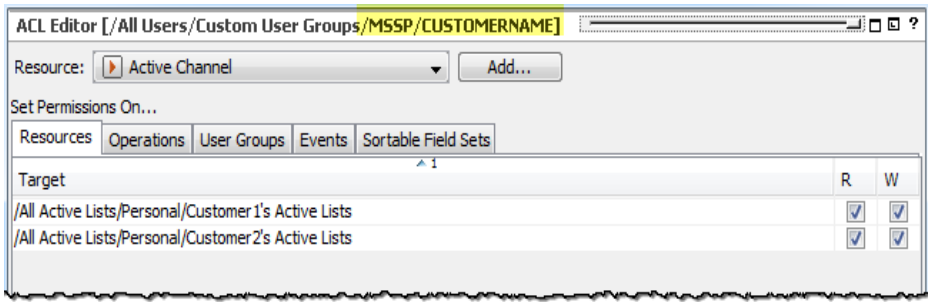
For more about ACLs, see also:

- "Managing Permissions" in the (missing or bad snippet)
- "User Management" in the (missing or bad snippet)

Permissions to Resources

Resource permissions indicate whether a user group has inspect (**R**ead) or edit (**W**rite) permissions to certain ESM resources. Refer to the topic, "Managing Permissions" > "Granting or Removing Resource Permissions" in the (missing or bad snippet).

Following is an example of the ACL Editor on the Resources tab. It shows the resources manually configured for a customer user group:



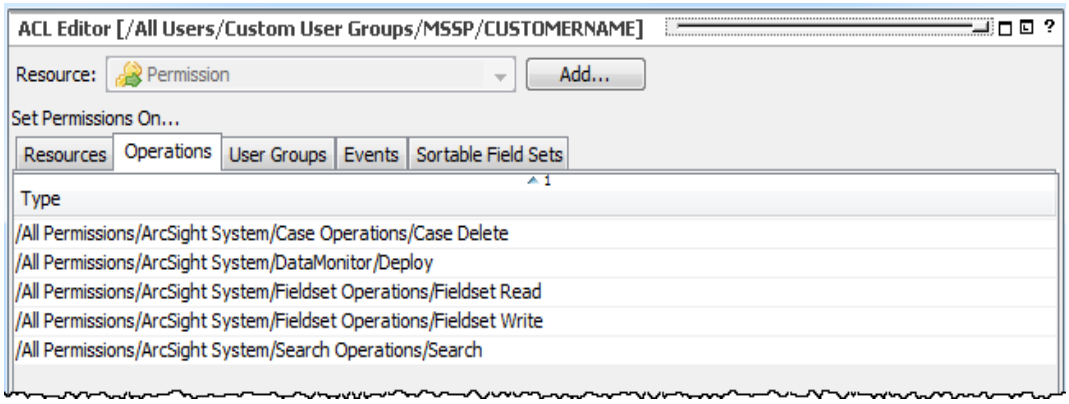
Caution: Do not grant tenants Write (W) access to `/All Connectors` to prevent unauthorized users from executing ESM commands using the API connector services.

Permissions to Operations

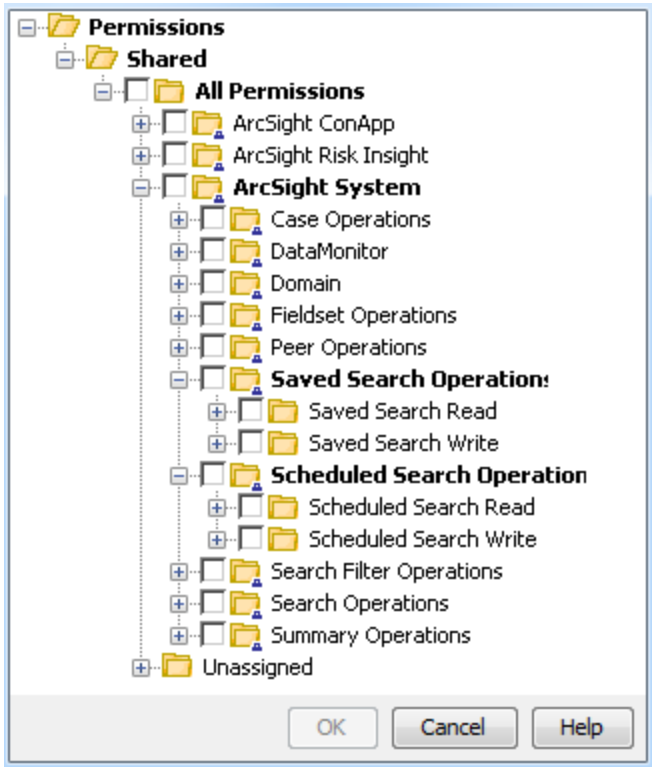
Examples of operations are deleting cases, reading and writing fieldsets, and deploying data monitors, among others. Users under Default User Groups and their subgroups have their own set of operations permissions.

Refer to the topics, "Managing Permissions" > "Granting or Removing Operations Permissions" in the (missing or bad snippet).

Following is an example of the ACL Editor on the Operations tab. It shows the operations manually configured for the user group, /MSSP/CUSTOMERNAME:

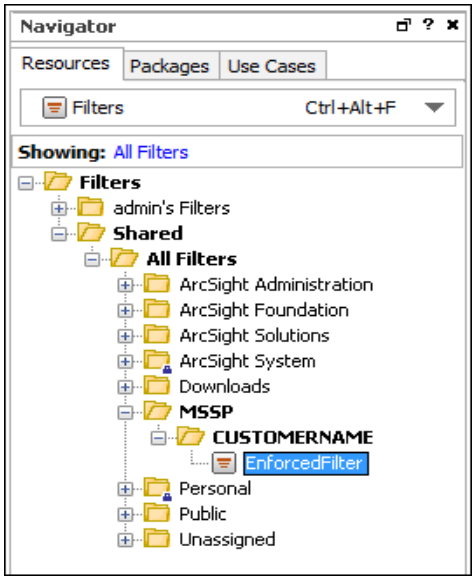


Following is a list of available permissions for Operations. This Permission Selector pop-up appears if you click **Add** on the ACL Editor's Operations tab:



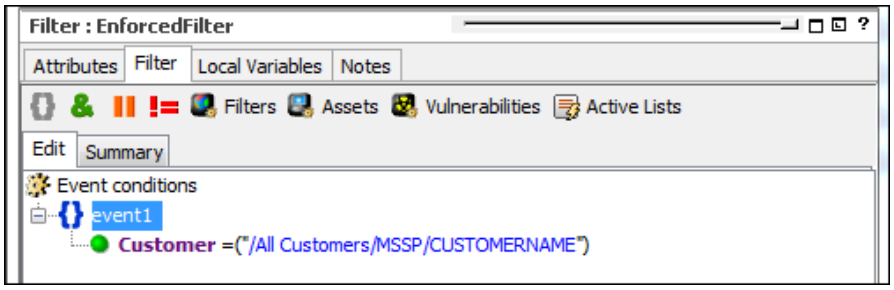
Permissions to Events Using Enforced Filters

Each customer should have a separate set of enforced filters for their needs. The best practice is to set an enforced filter that limits a customer to view only their data. Do this by creating a filter that matches a customer to the Customer resource:



Add the required filters to the Access Control List editor's Events tab as enforced filters, which dynamically limit the events viewed in active channels and reports. You can then create a series of specific filters for rules and dashboards.

As a best practice, If you want to restrict the events a user can see, be sure to use the correct enforced filters. For filters, apply a filter condition using the Customer field:



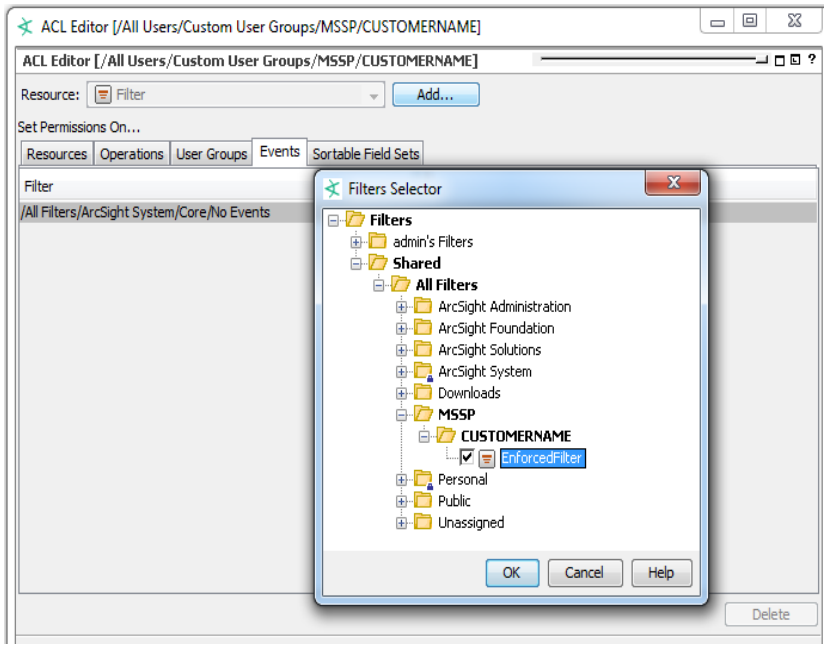
As described in the topic "Managing Permissions" in the (missing or bad snippet), a user group has associated access control lists (ACLs) .

Important notes about enforced filters:

- *Enforced filters* are filters added to the ACL Editor's Events tab. These filters restrict the events a user group (a customer in this case) can see.
- Always create filters in their appropriate filter groups assigned to specific tenants.
- Active channels, when launched, use the enforced filters associated with the user who launched the channels.
- Reports and query viewers use the enforced filters to return and display data.
- Trends and data monitors use the enforced filters of the user who created these resources. This is the user described in Setting Up Administrator Users.

- ESM evaluates the enforced filters with an OR operator. Evaluating events with an OR becomes relevant especially if different filters are applied to a hierarchy of user groups, or if a user is linked to multiple user groups. You should keep these relationships in mind, to determine the ultimate set of events that a user sees.
- Users have the ability to annotate events that match any one of their enforced filters.

In the following example, the CUSTOMERNAME user group is assigned an enforced filter exclusively for that tenant:



Note: Saved searches and search filters conform to the event filters you add here.

The Provisioning Process

This topic outlines ArcSight features designed to help provision your customers.

Below are high level steps for the provisioning process:

1. Create a customer tag `CUSTOMERNAME`. This is part of "Setting Up the Network Model" on page 18.
2. Create user groups. Recommended format:

   `/All Users/Custom User Groups/MSSP/CUSTOMERNAME`
3. Follow the instructions in "Setting Up Administrator Users" on page 32.
4. Define a filter as described in "Permissions to Events Using Enforced Filters" on page 27.
5. Define a group for the user in each one of the following resource trees:

```
/All Archived Reports/MSSP/CUSTOMERNAME
```

```
/All Assets/MSSP/CUSTOMERNAME
```

```
/All Cases/MSSP/CUSTOMERNAME
```

```
/All Customers/MSSP/CUSTOMERNAME-Customer
```

```
/All Destinations/CUSTOMERNAME
```

```
/All Files/MSSP/CUSTOMERNAME
```

```
/All Locations/MSSP/CUSTOMERNAME
```

```
/All Rules/Real-time Rules/MSSP/CUSTOMERNAME
```

```
/All Zones/MSSP/CUSTOMERNAME (This is part of "Setting Up the Network Model" on page 18.)
```

```
/All Networks/MSSP/CUSTOMERNAME (This is part of "Setting Up the Network Model" on page 18.)
```

6. Set the ACL for the customer user group to:
   - Allow either read or read/write access to the above groups:
     - Read if customer users are only content consumers.
     - Read/write if customer users are expected to create or modify content.
   - Allow access only to the filter above.

   See "Managing Permissions in the MSSP Environment" on page 25.
7. Assign "Permissions to Operations" on page 26.
8. Create a package, recommended under `/All Packages/MSSP/CUSTOMERNAME`, and include in this package all the resource groups above.

   See the topic, "Managing Packages" in the (missing or bad snippet).

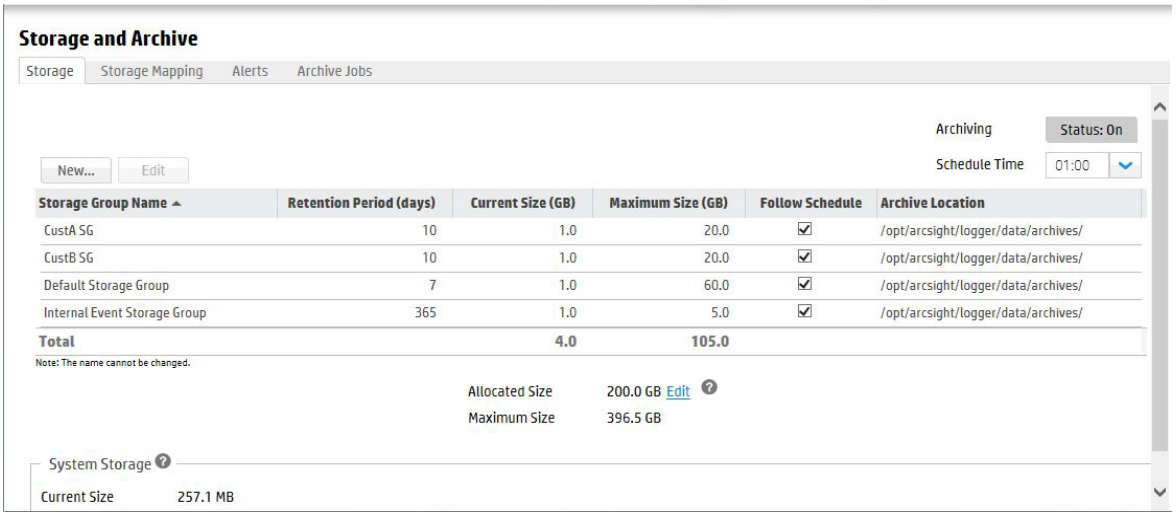
Managing Storage Groups

ESM provides a mechanism for you to segregate tenants' data by storing their events in a limited number of different storage groups. These are then stored in different physical locations on the system. This technique applies to deployments where each connector is associated with a single tenant, because ESM storage groups are mapped to connectors.

Storage groups are defined using the ArcSight Command Center. Refer to the topics, "Storage" and "Storage Mapping" in the (missing or bad snippet).

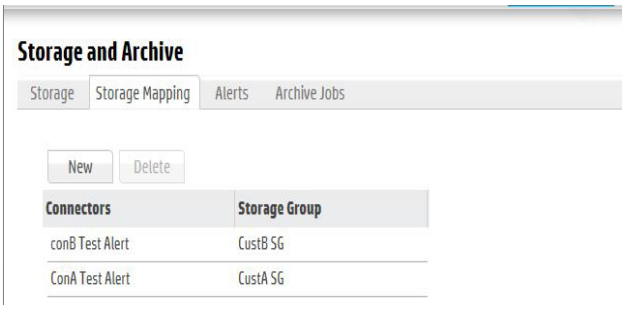
The following examples illustrate the process of defining a storage group per customer.

Step 1: Create a Storage Group per Customer



Step 2: Assign a Connector per Storage Group

This ensures all events from a connector go to the designated storage group.



Chapter 5: Configuration

This section provides instructions to set up ESM for the MSSP environment.

Setting Up Administrator Users

To set up administrator users for each customer:

1. Create an administrator user group under the customer's name.
2. To this group, assign all ACL privileges, including the enforced filters, for that customer.

   This ensures that customer-specific content is displayed appropriately.
3. Create a customer-specific administrator user under this user group.

   Caution: Restrict the knowledge and use of this administrator user only to you, the provider. Do not share this information with the customer to prevent unauthorized access to other customers' data.
4. Log in as this customer administrator to create ESM content, such as data monitors, for that customer.
5. Repeat the process for each customer.

This ensures that customer-specific content gets the correct permissions, filters, and so on.

Setting Searches

The ArcSight Command Center includes a search feature, described in the topic "About Searching for Events" in the (missing or bad snippet). That guide describes how to create search filters and saved searches. These resources conform to the enforced filters defined in the ACL Editor's Events tab for the customer. While there are no additional content-related tasks to searches, you need to perform configuration tasks.

To prevent unintentional exposure of other tenants' events on the Command Center, configure the property settings described here. Note that this requires a services restart, see Tip below.

Tip:

- Refer to the topic "Managing and Changing Properties File Settings" in the (missing or bad snippet) for general information on editing properties files. Enter all the settings described here, then restart all services.
- Changing properties files requires restarting services. For our purposes, use the command

```
/sbin/service arcsight_services restart all
```

Property filename:

`logger.properties`

File location in ESM's directory:

`/opt/arcsight/logger/userdata/logger/user/logger/`

Property settings:

Settings for Searches in the ArcSight Command Center

Property Setting	Purpose
`complete.fulltext.enabled=false`	This setting disables the search auto-complete feature. If not disabled, the auto-complete feature can potentially include data from other tenants.
`search.export.saveToServer.enabled=false`	This setting removes the ability to save exported search results using the **Save to ArcSight Command Center** option. This option is removed from the user interface. If not disabled, the results are saved to a directory that is accessible to all users regardless of permissions. **Note:** This property setting is available with ESM 6.8c Patch 3. The property setting will not affect saved searches that have been exported previous to the patch.

Chapter 6: Building ESM Content

Now that the Network Modeling framework is complete, you are ready to create ESM content that allows customers to view their own data.

Configuring ESM resources correctly is critical to MSSP provisioning. Make sure the ESM resources used to monitor and investigate events are carefully designed so that customers see only their data.

Before creating customer content, make sure you have created an administrator user for each customer, as described in "Setting Up Administrator Users" on page 32.

Topics in this section:

MSSP SOC and Customer Interaction Modes

There are several options for how the MSSP SOC interacts with customers. The choice of mode influences the methodology used to create ESM content for the SOC. Some key guidelines are common to all the models presented below:

- **Only the MSSP creates content.** The MSSP model calls for the service provider to provide the security know-how and the security operations. Providing ArcSight as a SaaS, in which the customer fully operates the system even if deployed by the service provider, is beyond the scope of this document.
- **The MSSP does real time monitoring using active channels.** Active channels are a core part of the SOC which is operated by the MSSP. The customer may have a need to view events, but the recommended method for that would be search, or in some cases, a query viewer as part of a dashboard.

- **If at all, the customer uses only the ArcSight Command Center.** All the features required by the operational models below are supported by the ArcSight Command Center. The customer does not need to use the ArcSight Console.

With those general guidelines in mind, the following are possible interaction modes for an MSSP SOC and customers. Except for the first option, the interaction can be a combination of the options described below:

- **No customer access.** The customer does not use the ArcSight Console or the ArcSight Command Center. The interaction with the customer is carried out by other means outside of the ArcSight solution, such as an external ticketing system or the MSSP portal which either integrates with ArcSight or is operated independently.
- **Provide reports to the customer.** For example, the reports are for compliance purposes. Reports are provided by e-mail or through the ArcSight Command Center.
- **View dashboards.** The customer views dashboards using the ArcSight Command Center. This enables the MSSP to provide managerial level visibility to the customer.
- **Send notifications.** Notifications are sent to the customer.
- **View and update cases.** Cases often serve as the communication mechanism between the MSSP and the customer, especially when the customer is in charge of the actual remediation process.
- **Use search.** The single most useful interactive function for customers is search, which enables them to look up past events. It has a lower learning curve than active monitoring and is more suitable for occasional use of the system.

MSSP Content Management Guidelines

The operational models described in "MSSP SOC and Customer Interaction Modes" on the previous page require that the customer has access to some of, but not limited to, the following, as required:

- Events
- Cases
- Reports
- Data Monitors
- Dashboards
- Notifications
- Rules

These resources in turn may need to rely on a large variety of additional resources. In this document we will focus on event-based content and therefore also discuss:

- Trends
- Query viewers - described in Reports and Dashboards
- Active Lists

Events

Since an MSSP system is using enforced filters, the customer tag for events must be set. This ensures that reports and search results include only events belonging to the customer.

For base events, this is ensured at the connector level as described in "Setting Customer Tags to Events" on page 20. For correlation events the guiding principle is that the generating rule must set the customer tag. An example of implementing this for a rule based only on events is shown in "Common Set of Rules" on page 40.

Cases

To ensure that customers have access only to their own cases, make sure that analysts open cases for a customer only under that customer's cases folder,

```
/All Cases/MSSP/CUSTOMERNAME
```

where `CUSTOMERNAME` is the customer name.

Refer to the following topics in the (missing or bad snippet):

- Case Management and Queries
- Rule Actions Reference, specifically the Case action

Reports

In an MSSP environment, the provider designs the reports. This topic refers to reports on events: either based directly on event queries, or reports based on trends generated using event-based queries. For reports based on non-event based queries, the query itself and its data source must ensure data is segregated by customer.

Reports can use data from active lists. Make sure that the active lists used in reports are segregated by customer, as described in "Active Lists" on page 41.

Note: If you have ESM 6.11.0 or later, you can also use a set of reports designed specifically for MSSP use. See "Using MSSP Reports" on page 44 for details.

Defining Reports

Reports derive their data through queries or trends. Queries run during report generation. As the method for running reports on a schedule (next topic) takes advantage of enforced filters, the output automatically uses only the customer events.

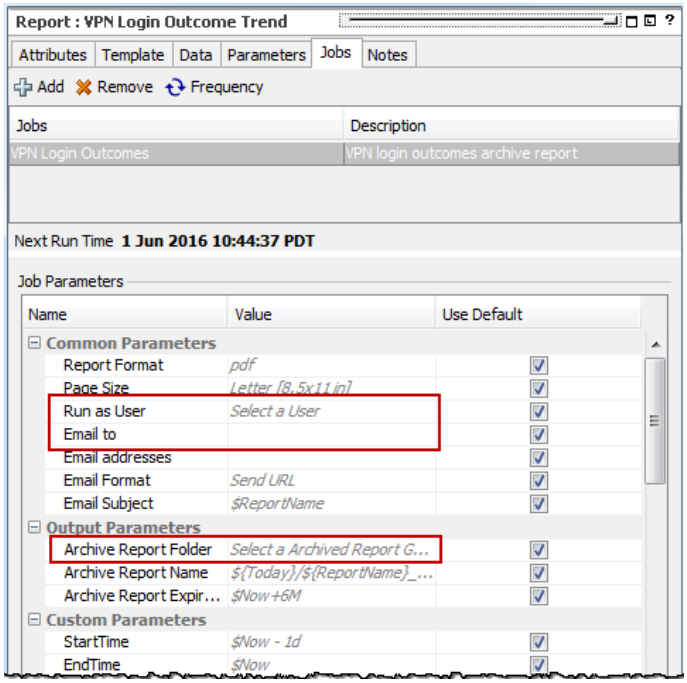
To report on trends, either use per-customer reports and trends; or follow the guidelines in the Trends topic.

Scheduling Reports

Schedule reports for customers, then provide the reports by email or as archived reports in the ArcSight Command Center. To accomplish this, configure a report job for each report for the customer.

When scheduling reports:

- Set `Run as User` to the customer administrator ("Setting Up Administrator Users" on page 32).
- If the report is to be sent by email, set `Email` to a single recipient's email address; or `Email addresses` to multiple email addresses.
- If the report is available on the ArcSight Command Center, set `Archive Report Folder` to `/All Archived Reports/MSSP/CUSTOMERNAME` where `CUSTOMERNAME` is the customer.



If you have a large number of reports, you can use group scheduling. See the topic, "Scheduling Report Archiving by Resource Group" in the (missing or bad snippet).

Common Reports

Since an MSSP system strictly tags each event with a customer tag, any report run under a tenant user will include only the events that are viewable by the tenant. Therefore, a common report can be used for multiple tenants. If the report requires trends, follow the guidelines for common trends in the Trends topic.

Tenant-Specific Reports

If the report template includes tenant-specific elements such as company name or logo; or if the report requires a non-common trend, the report has to be specific to the customer. As a best practice, store the report in

```
/All Reports Archive/MSSP/CUSTOMERNAME
```

and the associated template in

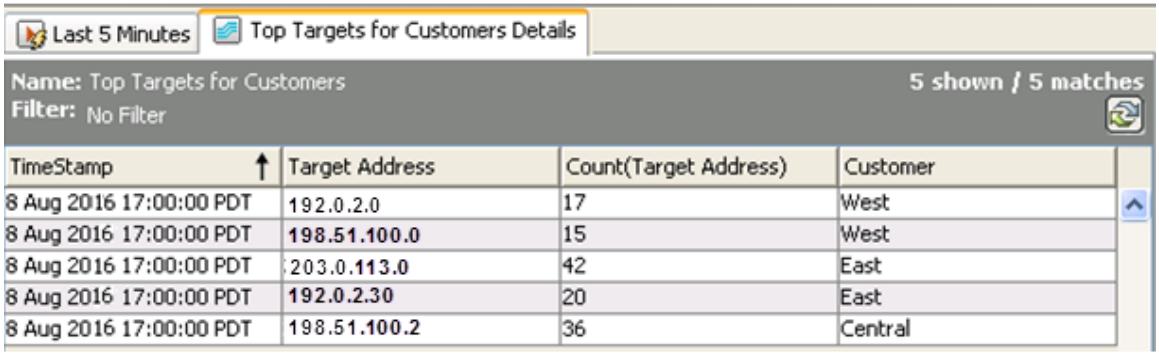
```
/All Report Templates/MSSP/CUSTOMERNAME
```

where `CUSTOMERNAME` is the relevant customer.

Trends

To use a common trend for multiple customers:

- Include a Customer field in the trend schema which the trend populates from the events it queries.



TimeStamp	Target Address	Count(Target Address)	Customer
8 Aug 2016 17:00:00 PDT	192.0.2.0	17	West
8 Aug 2016 17:00:00 PDT	198.51.100.0	15	West
8 Aug 2016 17:00:00 PDT	203.0.113.0	42	East
8 Aug 2016 17:00:00 PDT	192.0.2.30	20	East
8 Aug 2016 17:00:00 PDT	198.51.100.2	36	Central

- In the trend query (query used to fetch data from the trend for a report), use a Customer custom parameter to be used as a condition on the trend's Customer field. Set this custom parameter to the customer name when scheduling the reports.

- If you are using a separate trend per customer, log in as the customer administrator user (Setting Up Administrator Users) to create each customer's trend.

Dashboards

You can add two types of resources on dashboards: query viewers and data monitors. Event-based query viewers honor enforced filters; therefore you can add common query viewers in dashboards.

While data monitors also honor enforced filters, they are executed in the context of the user who created them rather than the user viewing the dashboard. As a result, you must create a separate data monitor for each customer (see "Data Monitors" on page 42). Therefore, dashboards displaying data monitors **must** be customer specific.

Notifications

The ESM notification rule action does not support dynamic destinations based on the customer name.

To implement e-mail based alerts:

1. Prepare an active list containing customer names and associated e-mail addresses to become recipients of notifications.
2. Use a variable in the rule to fetch the e-mail address from the list based on the customer name.
3. Use the execute command rule action with the e-mail address as the parameter to send the alert.

Rules

Topics in this section:

Refer also to these topics in the (missing or bad snippet):

- Filtering Events > Creating Filters
- Rules Authoring
  - Specifying Rule Conditions > Adding Filter Conditions

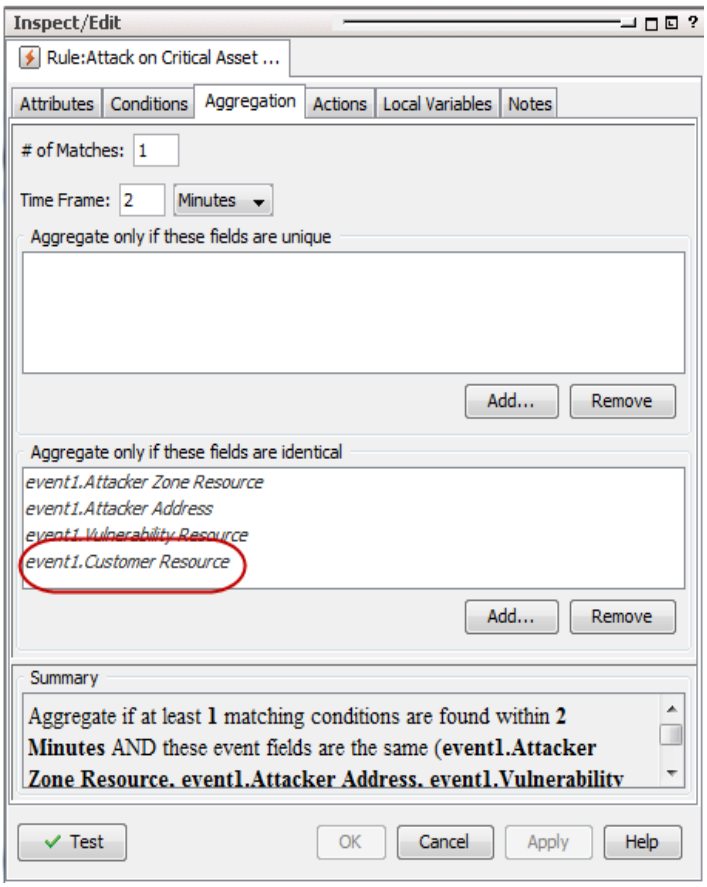
- Optimizing the Evaluation of Event Conditions
- Rule Actions Reference (see the Case rule action)

Common Set of Rules

Rules do not use enforced filters.

To create a rule that is common to multiple customers based on the customer tag in the base events:

1. Aggregate based on the customer tag or the customer field in an active list.

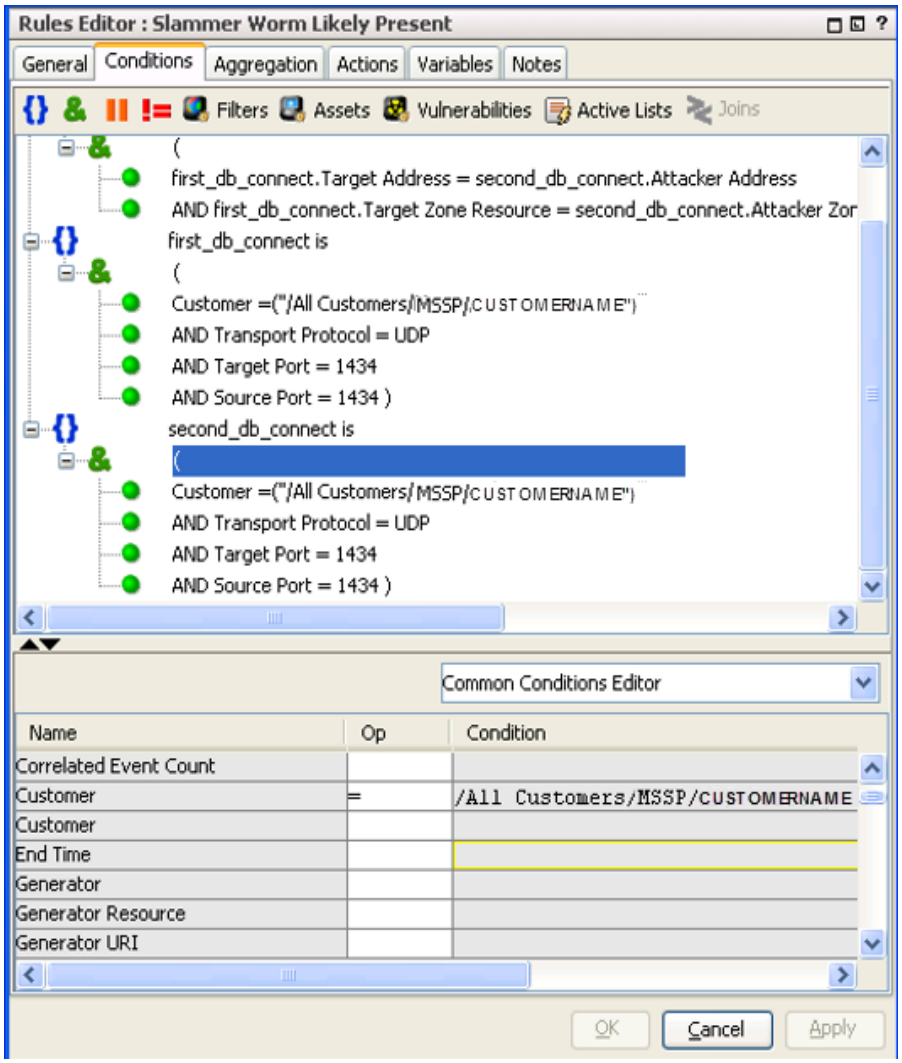


2. Set the correlation event customer tag to the customer value.

Tenant-Specific Rules

To ensure that the rule matches only those events specific to the tenant, make sure the rule condition specifies the `Customer` field in a filter condition.

If a tenant requires more than the standard service rules, then define a set of rules where the condition for the rule refers to `Customer = "CUSTOMERNAME"` as shown in the following example:

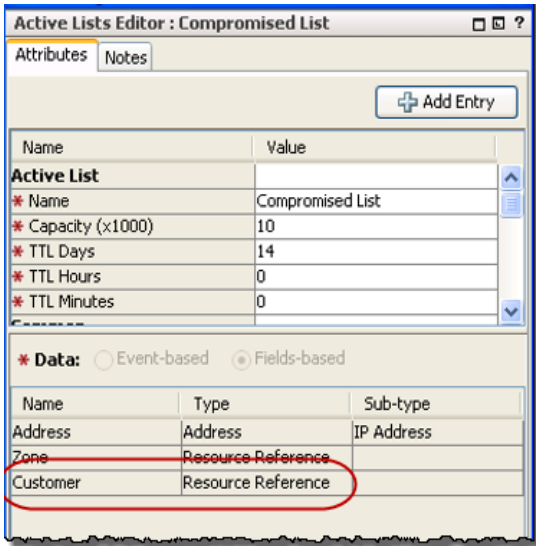


Active Lists

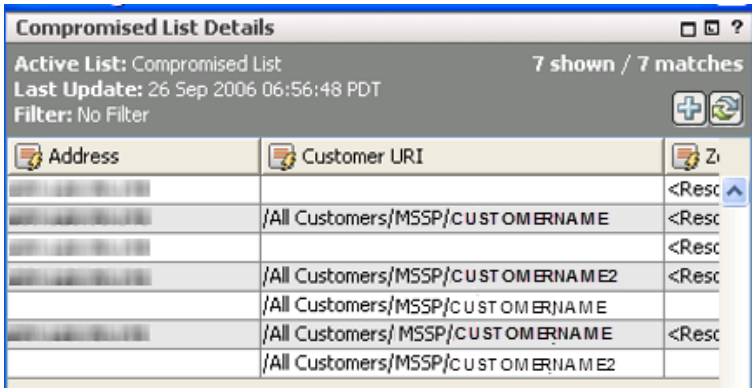
To create active lists common to all customers:

- Restrict access rights to these lists so that tenants will not see the entries, their own or other customers'. Store these common active lists in a non-tenant active list folder.
- Use the *Customer Resource Reference* data type. This will indicate to which customer a list entry belongs.

Tip: Aggregate based on the Customer resource when building rules for shared active lists.



By using *Customer Resource Reference* as an option, the *Customer ID*, *Customer URI*, *Customer Reference ID*, and *Customer Name* are populated automatically on the resulting list:



Data Monitors

Data monitors (DMs) are views within dashboards you can use to report on events, filters, and rules. Examples of information being collected are information on top events, most recent event activity, partial rule occurrences, hourly event counts, and so on.

Satistical data monitors (moving average data monitors are a subset) perform calculations that should also be restricted by enforced filters. An example would be one that monitors spikes in port activity, where the same level of activity may be normal for one customer but not for another. Correlation events generated from statistical DMs can be consumed by other DMs and rules.

As with ESM's other event monitoring resources, viewing events on data monitors require permissions. These events are specified through enforced filters - ESM filters that are added to a user group's ACL editor on the Events tab.

To ensure that the tenant's data monitor displays only the tenant's events:

1. Log in as the administrator user of a tenant (see "Setting Up Administrator Users" on page 32).
2. Create data monitors for the tenant being represented by the logged-in administrator. The data monitors will automatically use the enforced filters when displaying customer events.
3. Create a separate dashboard for the tenant. Add the customer-specific data monitors to the customer-specific dashboard.
4. Repeat the process, each time logging in as the administrator for another tenant.

Chapter 7: Using MSSP Reports

If you have ESM 6.11.0 or later, you can leverage predefined reports designed specifically for providers. The reports help you monitor your customers' EPS usage. These reports and other supporting resources are available from the ArcSight Marketplace.

Prerequisites:

- Your MSSP setup must be one dedicated connector to a customer.
- The Customer URI value in the connector configuration must be set so that the rule triggers.

See "Setting Customer Tags to Events" on page 20 for related information.

To download and install the free MSSP report package:

1. Sign in to the ArcSight Marketplace.
2. From the top menu, select the **Categories > Utilities and Tools**.
3. Locate and click **MSSP Usage Report** to download the zip file, **MSSP_Usage_Report_1.0.zip**, on the system where the ArcSight Console is installed.

   Extract these files:

   - MSSP_Usage_Report_1.0.arb
   - MSSP_Usage_Report_1.0_ReadMe.txt
4. Log into the Console as administrator.
5. Follow the instructions in the topic, "Importing Packages" in the (missing or bad snippet) to import and install the `.arb` package.

The package includes:

Package Contents

Resource Type	Description	Resources
Active Lists	Active lists store event count information.	• Events Count • Total Event Count
Queries	Queries get the data to populate the report. Each query has a local variable, MyESMInstance, which represents your Manager hostname. You can edit that variable so that your actual hostname is used in the report.	• Daily Aggregated EPS • Daily Average EPS • Total Average EPS

Package Contents, continued

Resource Type	Description	Resources
Reports	Reports track daily EPS usage and provide aggregated license information. EPS usage history is tracked from the beginning of the current month till the day you run the report ($Today).	• Daily EPS Usage for All Customers • MSSP Aggregated License Report
Rule	The rule tracks the event usage and adds information to the active lists.	Event Counts Detected

The reports are installed in `/All Reports/ArcSight Solutions/MSSP Usage Report`. See also "MSSP Reports by Resource Type" on page 53 for a list of other resources used by the reports.

Customizing the MSSP Reports

This information applies to ESM 6.11.0 or later.

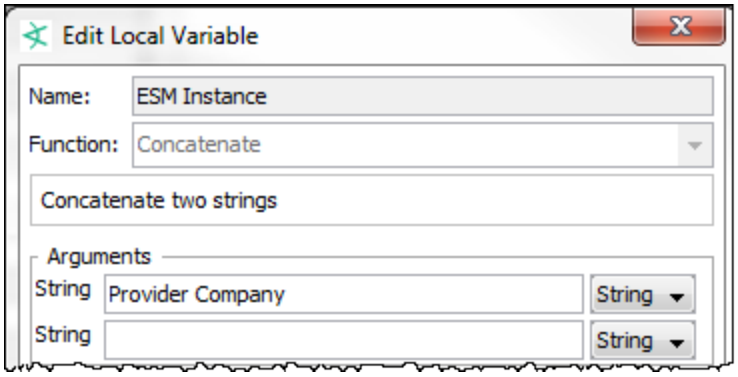
You can customize the local variable that supplies the string, `MyESMInstance`, to represent the Manager hostname. This string is output in all MSSP reports and supplied by the underlying queries. To know which queries are providing the report data, get them from the report's Edit panel, Data tab. Check each subtab if applicable, to see if the report is using different queries.

Where: Navigator > Resources > Reports > Queries tab

For each report you want to change, you change the underlying query.

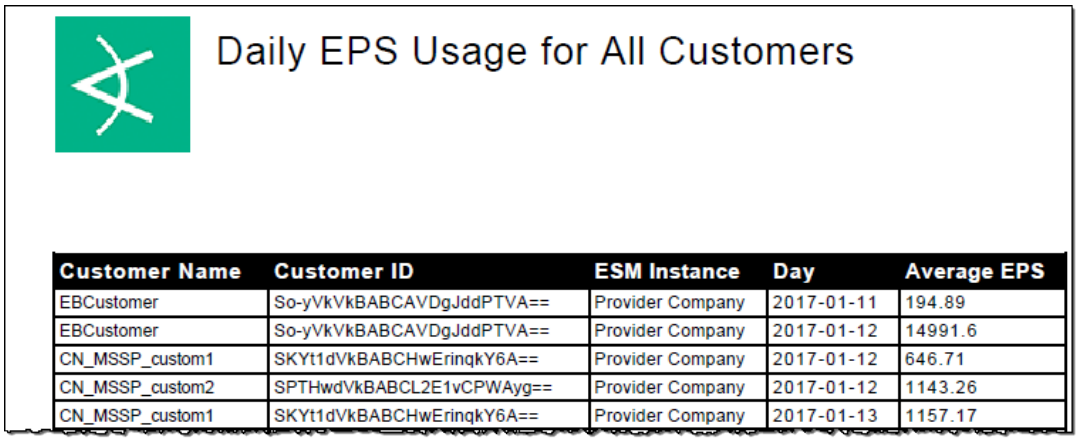
To change the string value for MyESMInstance:

1. On the Queries tab, expand /All Queries/ArcSight Solutions/MSSP Usage Report.
2. Right-click the query, for example, **Daily Average EPS** and select **Edit Query**.
3. On the Edit panel, go to the **Local Variables** tab.
4. Select the row for **ESM Instance** and click **Edit**.
5. In the Arguments field, change the string value MyESMInstance to your preferred string (Provider Company is the example here):



6. Click **OK** to save the variable, then click **OK** to save the query.

The next time you run the report that uses the modified query, the ESM Instance column will be populated with the new string value:



Daily EPS Usage for All Customers

Customer Name	Customer ID	ESM Instance	Day	Average EPS
EBCustomer	So-yVkVkBABCAVDgJddPTVA==	Provider Company	2017-01-11	194.89
EBCustomer	So-yVkVkBABCAVDgJddPTVA==	Provider Company	2017-01-12	14991.6
CN_MSSP_custom1	SKYt1dVkBABCHwEringkY6A==	Provider Company	2017-01-12	646.71
CN_MSSP_custom2	SPTHwdVkBABCL2E1vCPWAyg==	Provider Company	2017-01-12	1143.26
CN_MSSP_custom1	SKYt1dVkBABCHwEringkY6A==	Provider Company	2017-01-13	1157.17

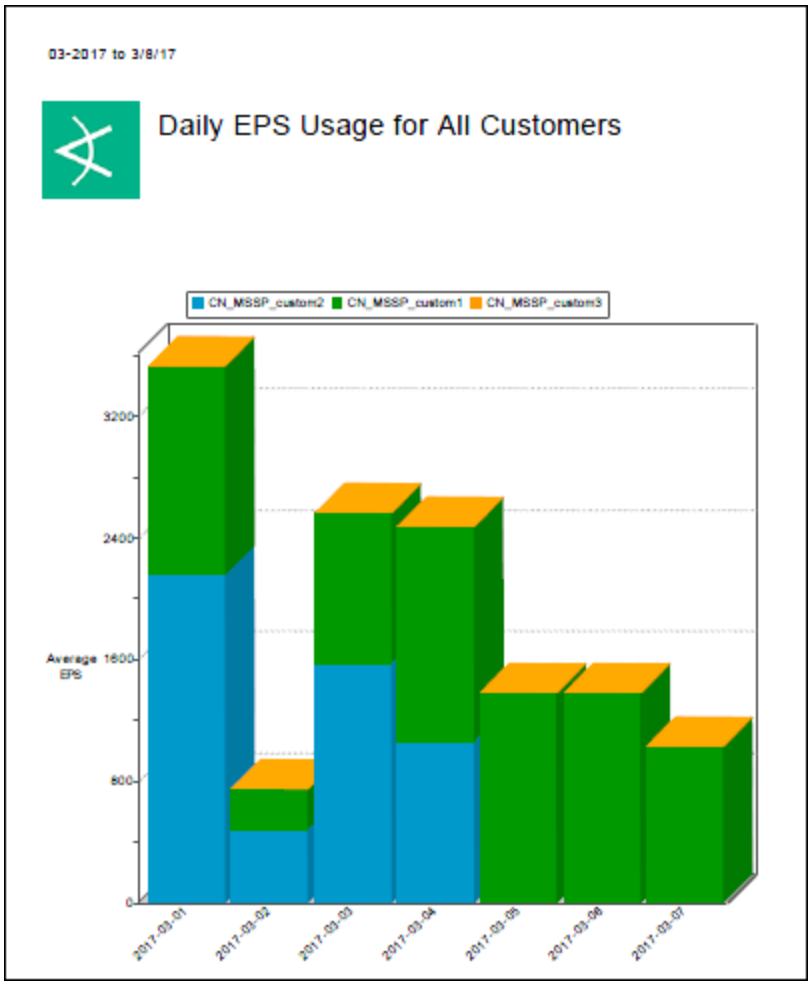
Running the MSSP Reports

This information applies to ESM 6.11.0 or later.

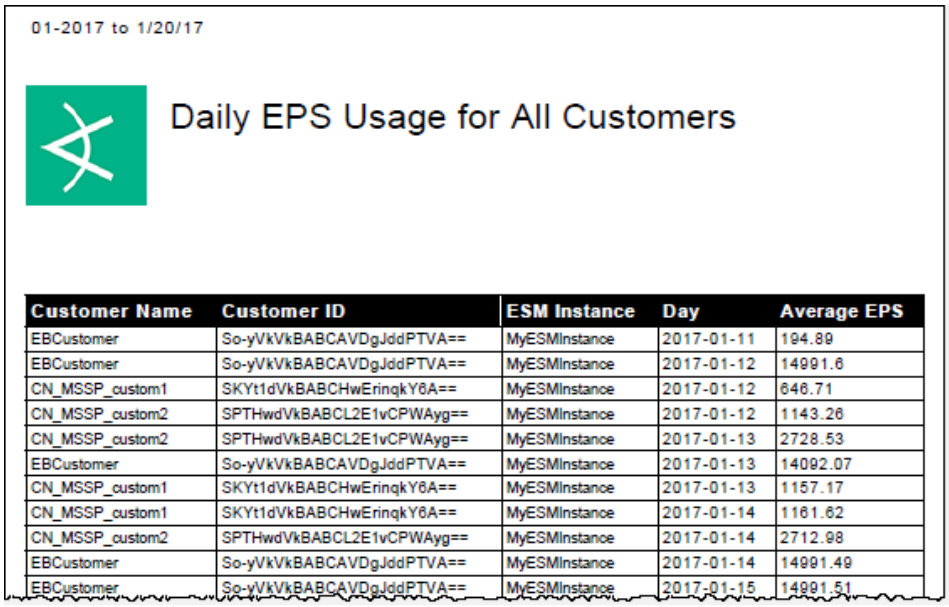
Where: Navigator > Resources > Reports > /All Reports/ArcSight Solutions/MSSP Usage Report

- Right-click **Daily EPS Usage for All Customers** and select **Run > Report with defaults**. This report is populated by a query that populates data for a chart and a table. Following is an example of the result.

Page 1 is a chart of all customers' daily average EPS usage per day:



Page 2 is a table. The report provides a list of all your customers, the corresponding customer ID, your ESM instance hostname, the date from the beginning of the month till the date you run the report, and the customer's average EPS consumption for the day.



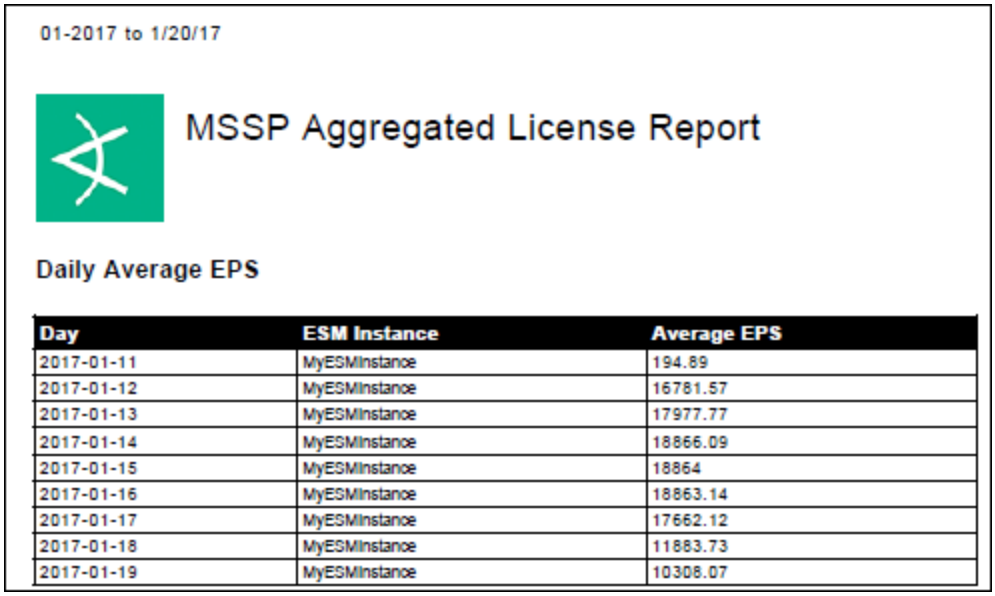
01-2017 to 1/20/17

Daily EPS Usage for All Customers

Customer Name	Customer ID	ESM Instance	Day	Average EPS
EBCustomer	So-yVkVkBABCAVDgJddPTVA==	MyESMInstance	2017-01-11	194.89
EBCustomer	So-yVkVkBABCAVDgJddPTVA==	MyESMInstance	2017-01-12	14991.6
CN_MSSP_custom1	SKYt1dVkBABCHwEringkY6A==	MyESMInstance	2017-01-12	646.71
CN_MSSP_custom2	SPTHwdVkBABCL2E1vCPWAyg==	MyESMInstance	2017-01-12	1143.26
CN_MSSP_custom2	SPTHwdVkBABCL2E1vCPWAyg==	MyESMInstance	2017-01-13	2728.53
EBCustomer	So-yVkVkBABCAVDgJddPTVA==	MyESMInstance	2017-01-13	14092.07
CN_MSSP_custom1	SKYt1dVkBABCHwEringkY6A==	MyESMInstance	2017-01-13	1157.17
CN_MSSP_custom1	SKYt1dVkBABCHwEringkY6A==	MyESMInstance	2017-01-14	1161.62
CN_MSSP_custom2	SPTHwdVkBABCL2E1vCPWAyg==	MyESMInstance	2017-01-14	2712.98
EBCustomer	So-yVkVkBABCAVDgJddPTVA==	MyESMInstance	2017-01-14	14991.49
EBCustomer	So-yVkVkBABCAVDgJddPTVA==	MyESMInstance	2017-01-15	14991.51

- Right-click **MSSP Aggregated License Report** and select **Run > Report with defaults**. This report is populated by two queries. Following is an example of the result.

  Page 1 of the report provides the average EPS consumption of all customers per day:



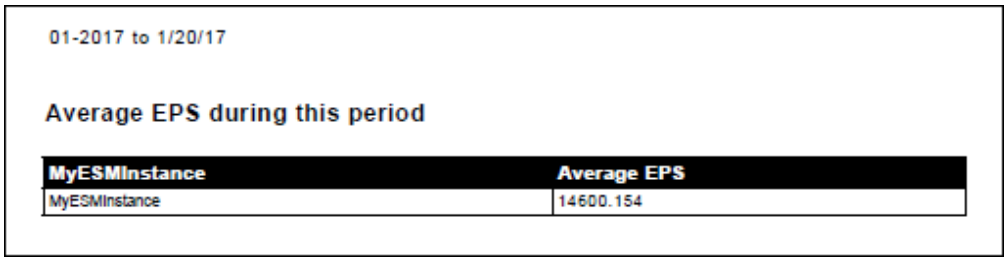
01-2017 to 1/20/17

MSSP Aggregated License Report

Daily Average EPS

Day	ESM Instance	Average EPS
2017-01-11	MyESMInstance	194.89
2017-01-12	MyESMInstance	16781.57
2017-01-13	MyESMInstance	17977.77
2017-01-14	MyESMInstance	18866.09
2017-01-15	MyESMInstance	18864
2017-01-16	MyESMInstance	18863.14
2017-01-17	MyESMInstance	17662.12
2017-01-18	MyESMInstance	11883.73
2017-01-19	MyESMInstance	10308.07

Page 2 of the report provides the total average EPS consumption for the period specified in the query:



01-2017 to 1/20/17

Average EPS during this period

MyESMInstance	Average EPS
MyESMInstance	14600.154

Chapter 8: Troubleshooting

This section describes error conditions that you might encounter, and provides recommendations for workarounds.

Map file does not work.

See the discussion,"Using Map Files" on page 23. If your map file does not seem to work, verify the following:

1. Make sure that your map file, `map.x.properties`, has entries. The two map files, `map.0.properties` and `map.1.properties`, that come with the SmartConnector does not have any valid entries.
2. If your `map.x.properties` has no entries, rename it to **map.0.properties**.
3. Restart the SmartConnector.

Other tenants' data appear on the active channel.

If an active channel intended for a tenant shows other tenants' data, verify the permissions set for the tenant's user group. Permissions are inherited from the parent group, so eliminate the broader permissions at the parent group and restrict the event filters at the individual user group.

Customer URI is not being set correctly

The significance of Customer URI is described in "Customer Tagging" on page 16.

1. Verify that the CustomerURI setting in the map file or the velocity template is correctly set.
2. Verify that the network model, network assignment, and zone configurations are configured correctly in the SmartConnector.
3. Test using a simple network setup.

Tenant cannot import another tenant's package

When resources are exported, the associated ACL settings are exported. When that package is then imported, the associated ACLs are enforced. This is the reason why the import does not succeed.

Velocity expression is not evaluated

If the Customer URI field is set to with a Velocity expression but it is not evaluated properly, verify if your Velocity expression has a syntax error. Follow instructions in "Using Velocity Templates" on page 22.

Correlated events (CFC feature) are not forwarded

If you are forwarding correlated events in a tiered architecture, make sure that the ESM version you are using supports such feature. This feature is available from ESM 6.8 onward.

Optimizing performance

Here are useful tips:

- **Rules.** A badly written rule can affect system performance and can block the flow of events not only for one tenant but all tenants in the same ESM server.
- **Lists.**The capacity of active and session lists is critical. View the status of this capacity to avoid overflowing and degrading of performance.
- **Performance troubleshooting.** Refer to this KB article:

  https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result/-/facetsearch/document/KM02203065

  Run the script in this article and open a ticket with Micro Focus ArcSight support.

Appendix A: Velocity Examples

```
#if($sourceHostName.endsWith("abc.com"))/All Customers/MY MSSP/ABC Corp#end
#if($sourceHostName.endsWith("xyz.com"))/All Customers/MY MSSP/XYZ Corp#end
```

IF Statements

```
#if( $foo < 10 )
    <strong>Go North</strong>
#elseif( $foo == 10 )
    <strong>Go East</strong>
#elseif( $bar == 6 )
    <strong>Go South</strong>
#else
    <strong>Go West</strong>
#end
```

Loops

```
#foreach( $product in $allProducts )
    <li>$product</li>
#end
```

Appendix B: MSSP Reports by Resource Type

This section applies to ESM 6.11.0 or later, and lists the resources by type.

Active Lists

The following table lists all the active lists found in `/All Active Lists/ArcSight Solutions/MSSP Usage Report`.

This table applies to ESM 6.11.0 or later.

Active List Resources

Resource	Description
Events Count	This active list retrieves event count per day per customer, when the Event Counts Detected rule triggers.
Total Event Count	This active list retrieves total event count per day, when the Event Counts Detected rule triggers.

Queries

The following table lists all the queries found in `/All Queries/ArcSight Solutions/MSSP Usage Report`.

This table applies to ESM 6.11.0 or later.

Query Resources

Resource	Description
Daily Aggregated EPS	This query calculates the sum of daily average Events Per Second (EPS) based on Events Count active list.
Daily Average EPS	This query calculates the daily average Events Per Second (EPS) for all customers based on the Events Count active list.
Total Average EPS	This query calculates total average Events Per Second (EPS) during this period based on the Total Event Count active list.

Reports

The following table lists all the reports found in `/All Reports/ArcSight Solutions/MSSP Usage Report`.

This table applies to ESM 6.11.0 or later.

Report Resources

Resource	Description
Daily EPS Usage for All Customers	This report shows the daily average Events Per Second (EPS) history for all customers. By default, the EPS history is for current month from beginning of the month till Today. This report is useful for Managed Security Services Provider (MSSP).
MSSP Aggregated License Report	This report shows two tables: 1) The aggregated daily average Events Per Second (EPS) 2) Total average Events Per Second (EPS) By default, the EPS history is for current month; from beginning of the month till Today. This report is useful for Managed Security Services Provider (MSSP).

Rule

The following table lists the rule found in `/All Rules/ArcSight Solutions/MSSP Usage Report`.

This table applies to ESM 6.11.0 or later.

Note: This rule is enabled, therefore automatically added to Real-Time Rules. Make sure you have set the Customer URI value in the customer's dedicated connector for report accuracy. The rule requires that Customer URI must not be null.

Rule Resource

Resource	Description
Event Counts Detected	This rule triggers when an `agent:050` audit event is detected. The rule adds the customer resource, day of month, and the event count to the Events Count active list. This rule also adds the day of month, sum of event count to the Total Event Count active list.

Publication Status

Released: August 2024

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on ESM Best Practices: Multitenancy and Managed Security Service Providers (ESM 7.8)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!