Micro Focus Security ArcSight ESM

Software Version: 7.5

Configuration Guide for ESM MSSP Multitenancy Environments

Document Release Date: April 2022
Software Release Date: April 2022

Legal Notices

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://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Introduction

ArcSight Enterprise Security Manager (ESM) consolidates and normalizes data from disparate devices across your enterprise network in a centralized view. ESM provides a holistic view of 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 you configure ESM to support threat detection for multiple, completely separate tenants. A tenant is a group of users sharing the same view of the software they are using. With a multitenant architecture, ESM provides every tenant a dedicated share of the instance, including its data, configuration, user management, tenant-specific functionality, and other properties.

This guide provides the information required for managed security service providers (MSSPs) to configure the MSSP environment for multitenancy and adopt SOAR into the environment.

After you configure your ESM MSSP environment for multitenancy, if SOAR is integrated with ESM, you can adopt SOAR into your multitenancy solution for real-time detection and response capabilities.

ArcSight SOAR is a Security Orchestration, Automation, and Response (SOAR) platform. SOAR provides a single unified pane of glass for automation of recurrent security events. SOAR ensures end-to-end mapping of all cybersecurity incidents of the organization, thereby increasing agility and responsiveness in addressing these incidents. SOAR also provides the flexibility to modify or add customized security tools as required and provide a robust security shield for your organization. For more information about SOAR capabilities, see the SOAR documentation.

While ESM real-time analytics allows you to analyze events from multiple customers and detect threats, SOAR lets you manage customer cases and automated response activities such as case enrichments, attack mitigation, and notifications.

Note: When you adopt SOAR into your multitenancy solution, SOAR is only available to MSSP employees that have access to all tenants' data. End customers cannot directly access SOAR.

SOAR does not provide data segregation or tenant isolation. It provides tenant-based filtering capabilities so that you can differentiate the cases per tenant and perform response activities.

Prerequisites

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

- You must have a basic understanding of ESM operations, networks, and network security.
- You must be familiar with the ArcSight Console and ArcSight Command Center for building ESM content and completing configuration tasks.
- You should have completed courses on ArcSight security products.

The following prerequisites apply to adopting SOAR into your multitenancy solution:

- The MSSP environment must already be configured for multitenancy, as described in this guide.
- SOAR must already be deployed within the ArcSight Platform version 21.1 or 22.1 and integrated with ESM version 7.5 or 7.6.

Deploying and Configuring ESM in Multitenancy Mode

Deploying ESM in multitenancy mode involves the following activities:

	Task	See
❑	1. Understand the advantages and disadvantages of the ESM architectures for MSSPs and choose what is best for you.	Understanding ESM Architectures for MSSPs Single ESM Server Multiple ESM Servers Tiered ESM Servers
❑	2. Decide whether to locate SmartConnectors at the individual tenant's site or at a central MSSP site.	Understanding Options for SmartConnector Location
❑	3. Understand the network model, decide which scenario applies to you, and set up the network model.	Using the Network Model in an MSSP Environment Understanding Network Model Resources Understanding Customer Tagging Understanding the MSSP Network Model Challenge Setting Up the Network Model Setting Customer Tags to Events
❑	4. Set permissions to ESM resources, operations, and events so that customers are restricted to their own ESM content.	Managing Permissions in the MSSP Environment Using Access Control Lists (ACLs) to Manage User Access to Resources Setting Permissions to Operations Using Enforced Filters to Set Permissions to Events
❑	5. Provision your customers.	Understanding the Provisioning Process
❑	6. Configure storage groups to segregate tenants' data.	Using Storage Groups to Segregate Data

❑	7. Configure ESM for the MSSP environment.	Configuring ESM for the MSSP Environment
❑	8. Configure ESM content for data segragation.	Managing ESM Content Understanding MSSP SOC and Customer Interaction Modes Configuring Content
❑	9. Install predefined reports designed specifically for providers.	Installing MSSP Reports

Understanding 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.

The following topics describe the architectures for MSSPs, along with the advantages and disadvantages of each:

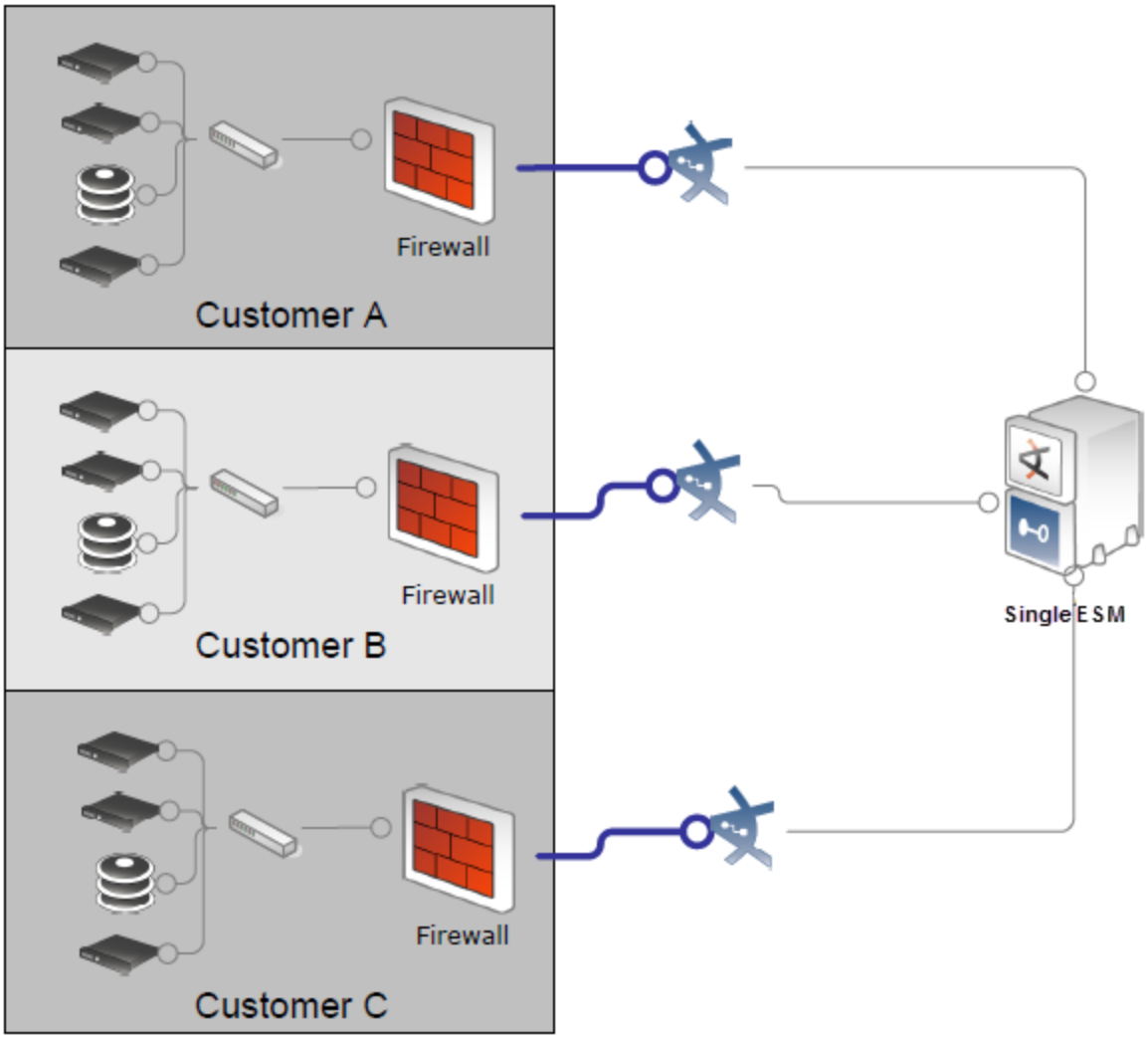
- Single ESM Server
- Multiple ESM Servers
- Tiered ESM Servers

In addition to choosing the architecture that is appropriate for you, it is also important to choose the appropriate location for SmartConnectors. The SmartConnectors can be located on the individual tenant's site or on a central MSSP site.

Single ESM Server

ESM is most often deployed with a single ArcSight 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 Manager.

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



Advantages

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

Disadvantages

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

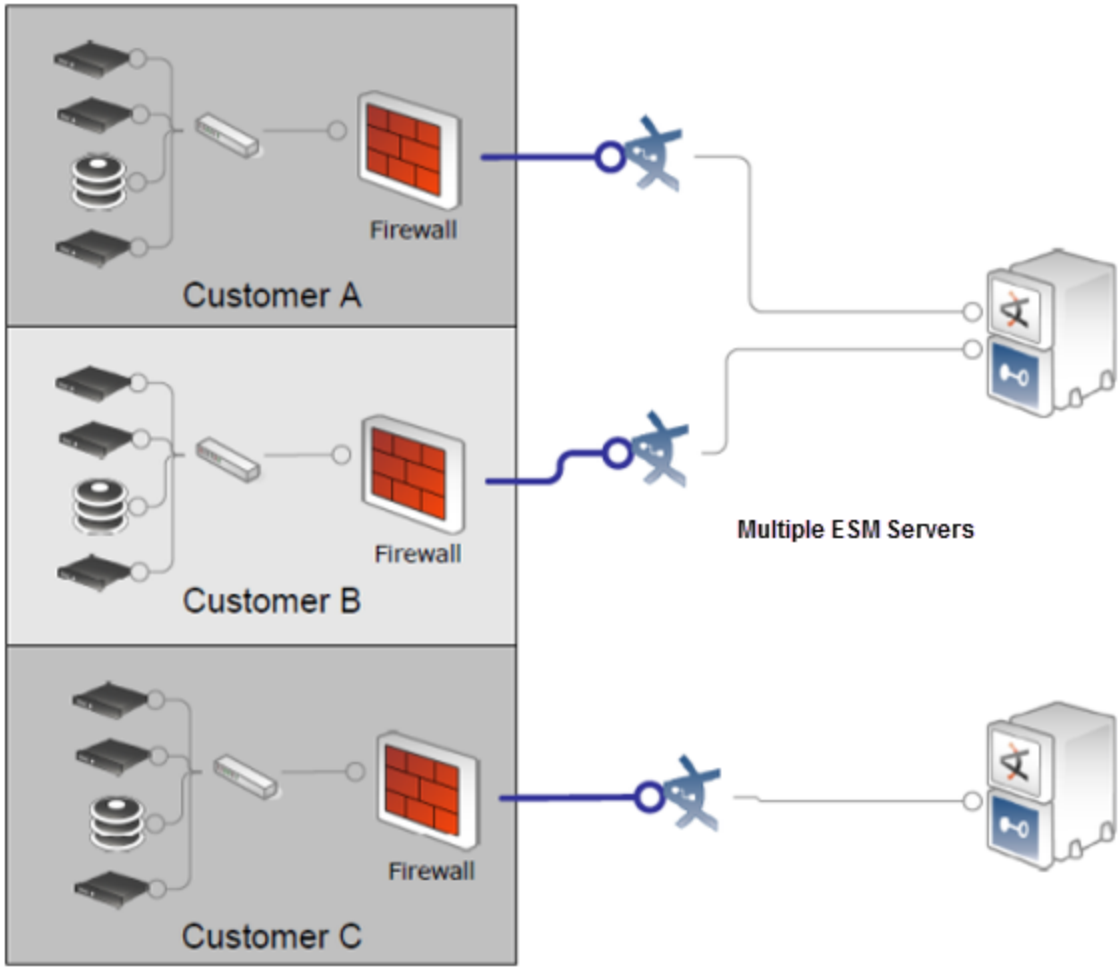
Multiple ESM Servers

In a multiple server 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 might be non-technical reasons for distributing across multiple Managers. For instance, the collection and processing might be broken up to match business units or regions.

In an MSSP environment, you can use multiple 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 volume of events.

You can run a series of performance tests to predetermine the threshold of each Manager. 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, you can 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

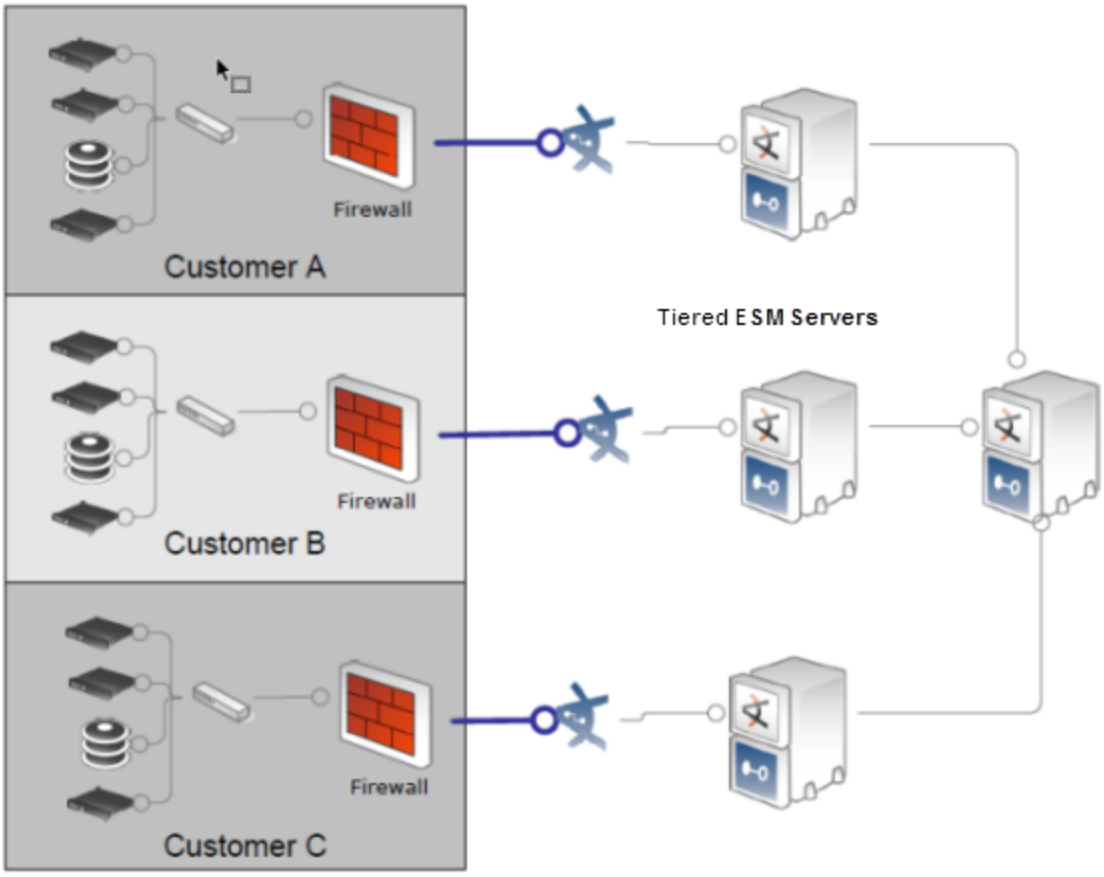
- There is no cross-correlation across all tenants or sharing of data between Managers.
- SOC workflow, including stages, annotations, and case management is done in separate Console instances.
- Configuration management is done at each Manager instance.

Tiered ESM Servers

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

In a tiered environment, there is more than one ArcSight Manager. In this case, you configure the lower-tiered Managers 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 only view the data at the first tier. The MSSP SOC typically only has access to the primary Manager.



Advantages

- Segregation of accessibility is simplified because tenants have access only to their dedicated machines.

- As each tenant's data is stored on a dedicated system, a high level of data separation is provided. Sensitive information can be obfuscated In events that are forwarded to the primary Manager.
- Selective cross-correlation between different tenants' events is possible.
- The MSSP SOC operators can monitor tenants' events from a single console.

Disadvantage

Managing multiple servers can be complex, but ESM's content management feature can help simplify some tasks. For more information, see Content Management and Creating or Editing Packages.

Understanding Options for 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 systems. In general, connectors can be located either at the individual tenant's site or at a central MSSP site.

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

For more information, see Granting or Removing Resource Permissions.

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 an ArcSight 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 premises, 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, 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).

Using the Network Model in an MSSP Environment

This topic assumes you are familiar with the fundamentals of network modeling in ArcSight or have read The Network Model. This topic reviews the network model topic and reiterates key rules in building assets within ArcSight, then covers three network and ArcSight scenarios that you might have to address when modeling your MSSP environment.

The networking modeling scenarios are as follows:

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

This topic includes the following subtopics:

Understanding Network Model Resources

ESM uses the following resources to model the network.

Assets represent individual nodes on the network, such as servers, routers, and laptops and have the following characteristics:

- Physical assets
- 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
- Inherit 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 and have the following characteristics:

- 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 have the following characteristics:

- 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 and have the following characteristics:

- Define the global logical network
- Contain one or more zones
- Configure connectors with networks
- Example: USA, Hong Kong, Europe

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. Customers have the following characteristics:

- 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.

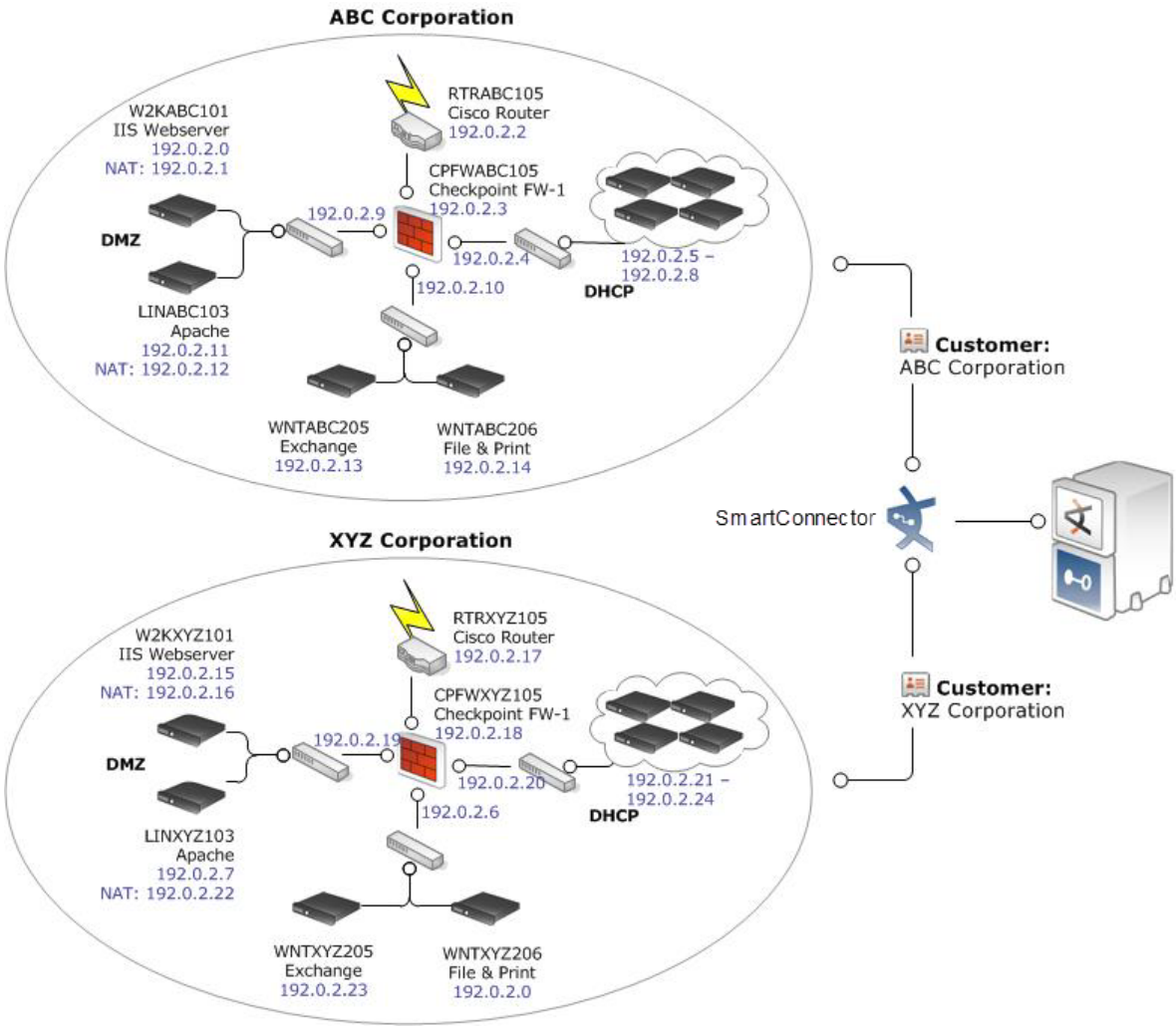
Understanding Customer Tagging

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 can be thought of as the owner of an event. Content developers can also use the `Customer` tag to develop customer-aware content.

Customer tagging is critical in MSSP environments because the `Customer` designation identifies the owner of events, ensuring that each customer (tenant) views only their events.

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 in Setting Customer Tags to Events.



Understanding the MSSP Network Model Challenge

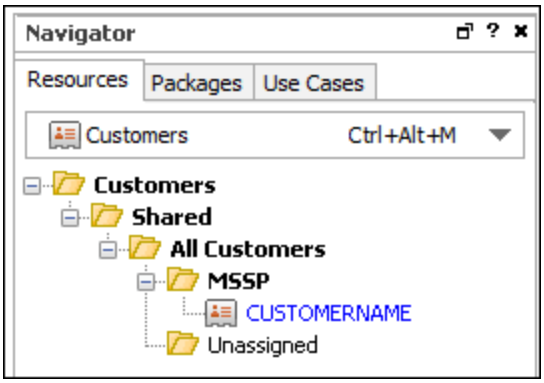
Since most organizations use private address spaces, addresses included in events from different customers can contain identical addresses but refer to different assets. For example, two tenants might use the private address space 192.0.2.x, and therefore both tenants might use the address 192.0.2.1 to refer to a local system.

Make sure you have the proper network information model, which includes zone information, and 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 the 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.

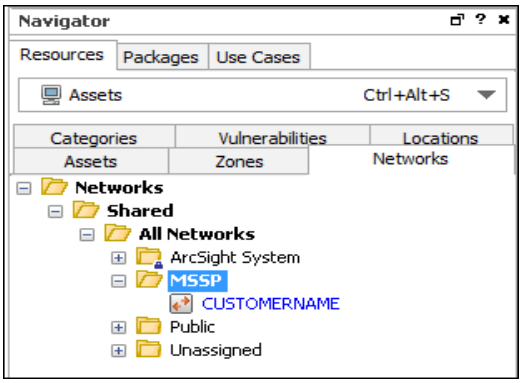
Setting Up the Network Model

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

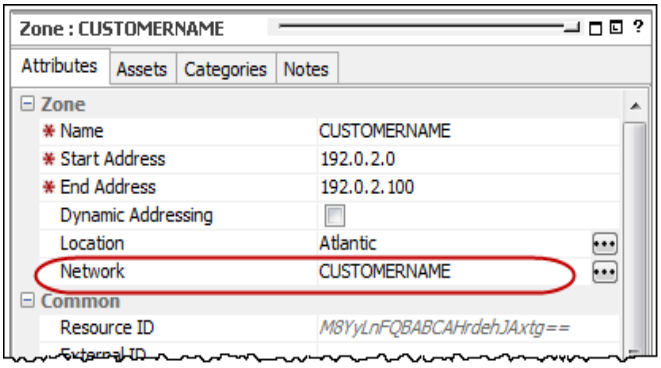
1. Log in to the ArcSight Console with administrator privileges.
2. In the Navigator, select the Resources tab.
3. Select the Customers resource, and then create customers.



4. On the Networks tab, create a Network resource for each customer. Use descriptive names to help you distinguish customer networks.



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

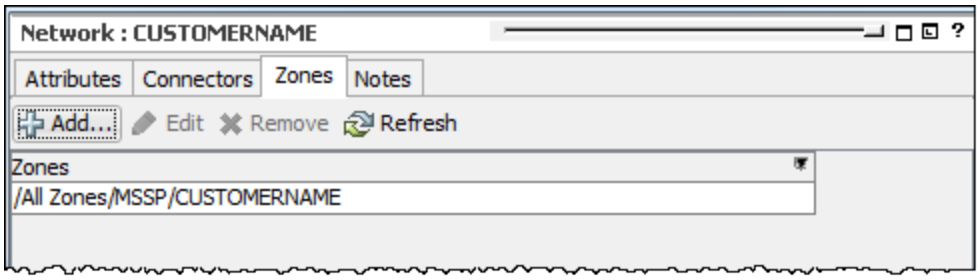


Note: If you save the zone without assigning a network, ESM automatically assigns the zone to `\All Networks\ArcSight System\Local`.

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

Connectors set events with customer tags. Tagging can be either static or dynamic. There are two deployment options, 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 plan to use MSSP Reports, a dedicated connector per customer is the required configuration. For more information, see Installing MSSP Reports.

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

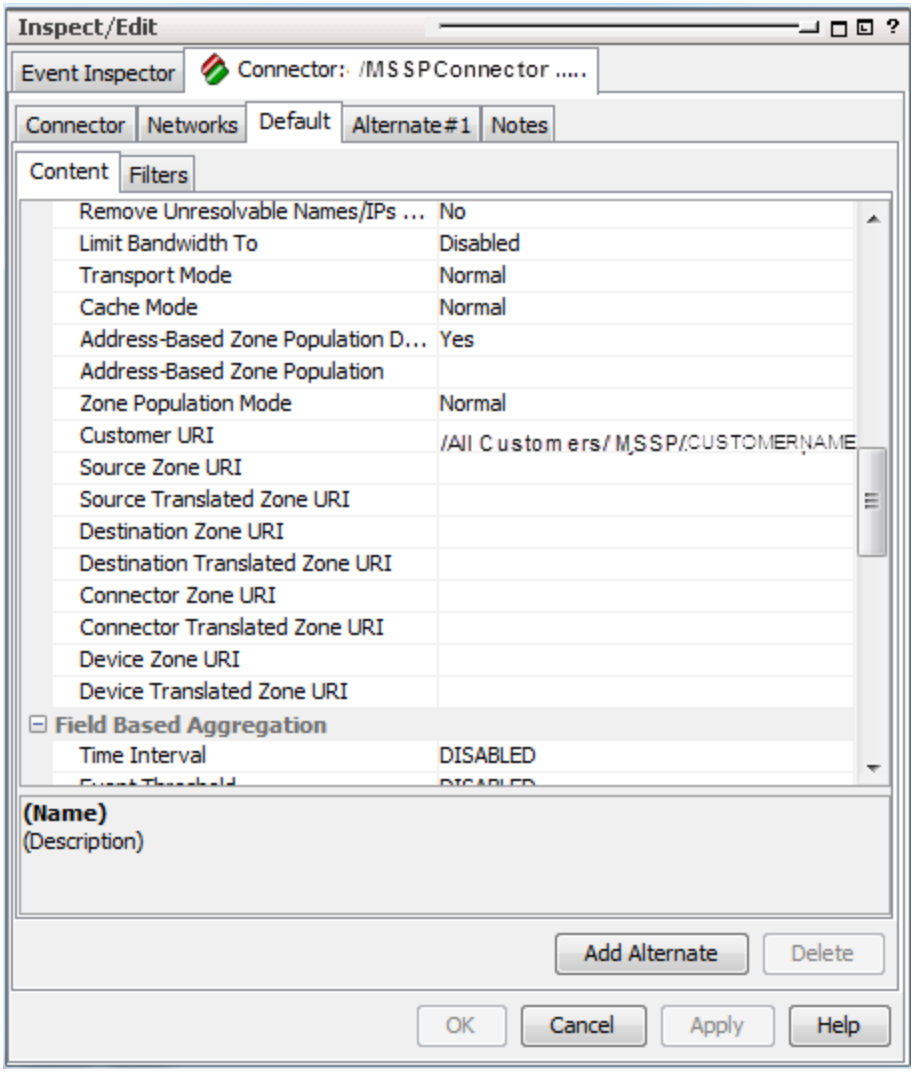
  Caution: While it is possible to have a shared connector serving customers with overlapping addresses, this setup is risky and can potentially send events to the wrong customer.

Using Static Customer Tags

Static tagging applies if a registered connector is dedicated to a single customer. Static tagging ensures that all events from the single connector are tagged with a specific customer.

1. In the Navigator, select Connectors.
2. Open the connector's editor.
3. Select Default, and then select the Content tab.
4. Under the Network section, set the Customer URI field to the customer resource. For example:

   `/All Customers/MSSP/CUSTOMERNAME`



Using Dynamic Customer Tags

Dynamic tagging applies if one registered connector is used for multiple customers with non-overlapping IP addresses. Dynamic tagging ensures that all events from the single connector are dynamically tagged so that event fields correctly identify which customer should see those events.

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.
  - Can be backed up.
- Map files:
  - Are external files.
  - Are placed in the connector installation directory.
  - Require manual updates.
  - While not easy to set up, 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 set up. 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. Micro Focus does not provide error checking or error messages for user-created expressions.

To set up the Customer URI with a Velocity template:

1. In the Navigator, select Connectors.
2. Right-click the connector and select Configure.
3. On the Default tab, select the Content subtab.
4. Locate the Customer URI setting and enter the Velocity template text. For example:

   ```
   #if($deviceHostName.endsWith("CUSTOMERNAME"))/All
   Customers/MSSP/CUSTOMERNAME#elseif($deviceHostName.endsWith
   ("CUSTOMERNAME2"))/All Customers/MSSP/CUSTOMERNAME2#end
   ```

   Note: Ignore the popup for customer resource selection.

5. Click the Transport Mode drop-down field, and then either select the existing value or press **Escape**. Verify that the value you entered in the Customer URI field persists.

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 a 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 a 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.

Managing Permissions in the MSSP Environment

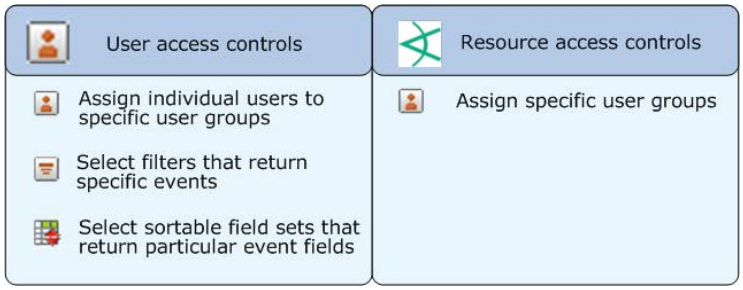
Correct setting of permissions to ESM resources, operations, and events ensures that customers are restricted to their own ESM content, and not any other customers' content.

The following topics provide information about setting permissions:

- Using Access Control Lists (ACLs) to Manage User Access to Resources
- Setting Permissions to Operations
- Using Enforced Filters to Set Permissions to Events

Using Access Control Lists (ACLs) to Manage User Access to Resources

ESM manages user access to resources through Access Control Lists (ACLs). You apply ACLs to user groups, which allows the users in that group to have read/write access to the resources that the ACL specifies.



You can further refine access to individual resources by specifying the user groups that can have read/write access to them.

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.

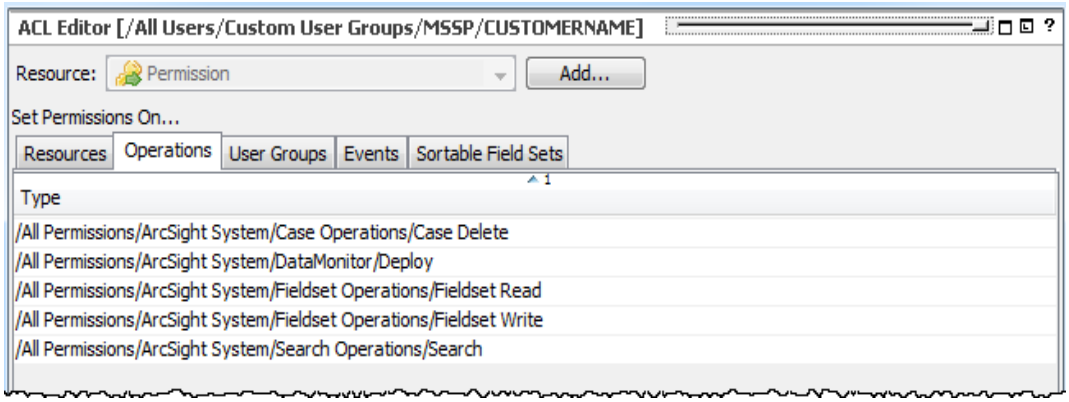
Note: ACLs in the MSSP environment are discussed further in Understanding the Provisioning Process.

For more information about ACLs, see Managing Permissions.

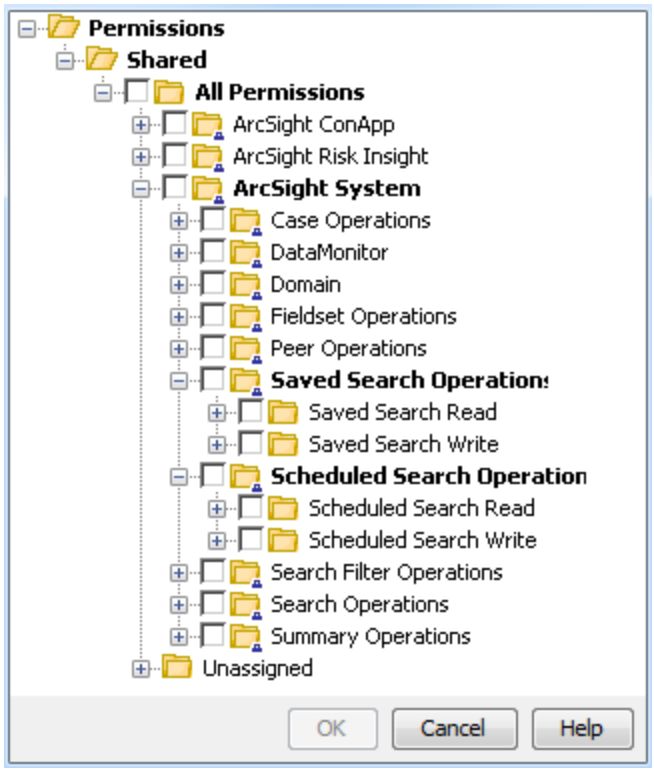
Setting Permissions to Operations

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

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. To view this list, from the ACL Editor's Operations tab, click Add.



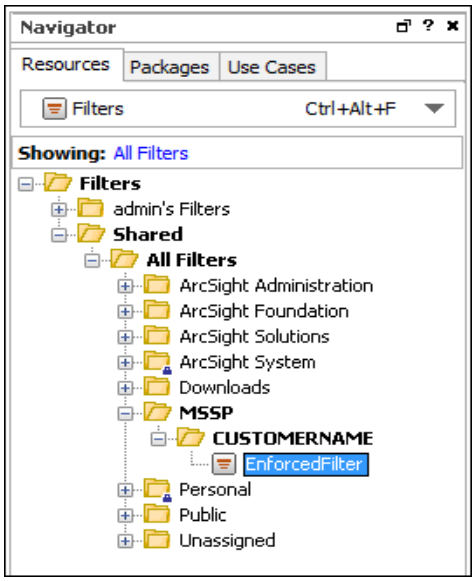
For more information about operations permissions, see Granting or Removing Operations Permissions.

Using Enforced Filters to Set Permissions to Events

Enforced filters dynamically limit the events viewed in active channels and reports. 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.

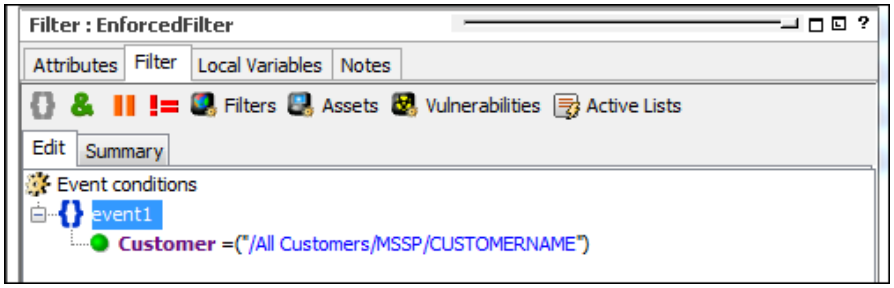
You add enforced filters to the ACL Editor's Events tab.

First, create a filter that matches a customer to the Customer resource:



Add the required filters to the ACL Editor's Events tab as enforced filters. 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:



Important notes about enforced filters:

- 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. 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.

Understanding the Provisioning Process

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

The provisioning process involves the following steps:

1. Create a customer tag `CUSTOMERNAME`.
2. Create user groups. Micro Focus recommends the following format:
   `/All Users/Custom User Groups/MSSP/CUSTOMERNAME`
3. Set up administrator users.
4. Set up enforced filters to set permissions to events.
5. Define a group for the user in each 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 Filters/MSSP/CUSTOMERNAME`
   `/All Locations/MSSP/CUSTOMERNAME`
   `/All Reports/MSSP/CUSTOMERNAME`
   `/All Rules/Real-time Rules/MSSP/CUSTOMERNAME`
   `/All Users/Custom User Groups/MSSP/CUSTOMERNAME` (see step 2 above)
   `/All Zones/MSSP/CUSTOMERNAME`
   `/All Networks/MSSP/CUSTOMERNAME`
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 applicable enforced filter.
7. Set permissions to operations.
8. Create a package under `/All Packages/MSSP/CUSTOMERNAME`, and include all of the resource groups from above in this package.

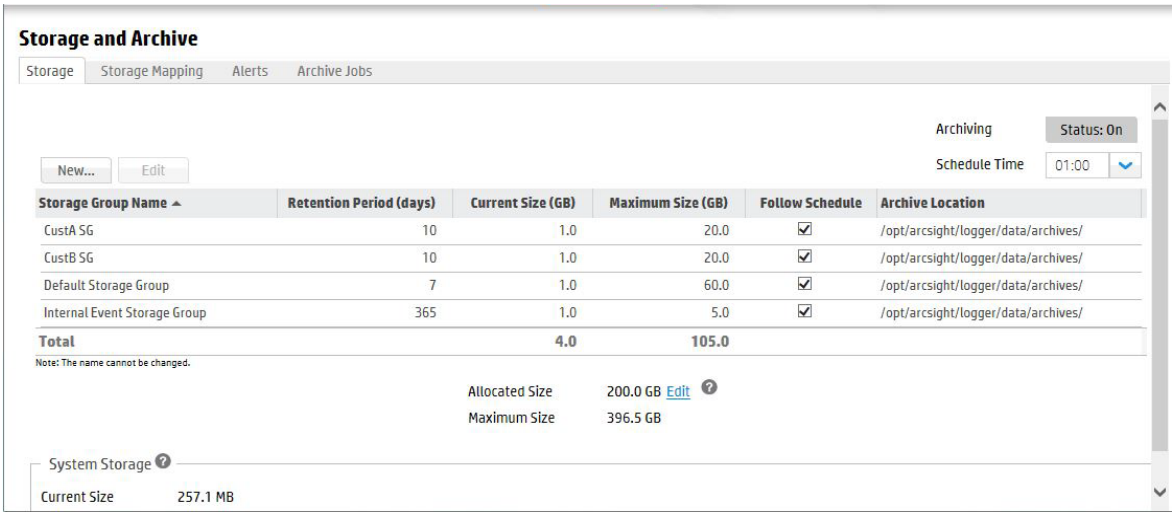
Using Storage Groups to Segregate Data

ESM provides a mechanism for you to segregate tenants' data by storing their events in a limited number of different storage groups. These storage groups 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.

Define storage groups in the ArcSight Command Center.

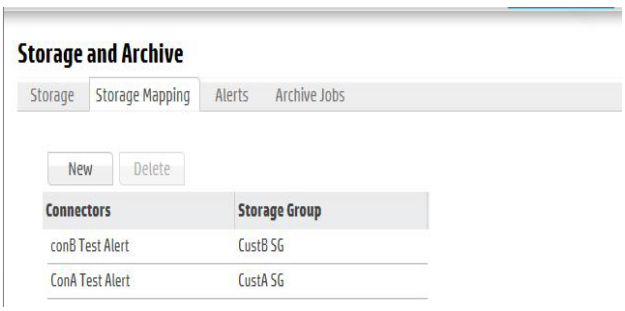
The following examples illustrate the process of defining a storage group per customer.

Step 1: Create a Storage Group per Customer



Step 2: Assign a Connector per Storage Group

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



Configuring ESM for the MSSP Environment

Configuring ESM for the MSSP environment requires setting up administrator users and configuring saved searches and search filters to prevent unintentional exposure of other tenants' events.

Setting Up Administrator Users

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. To prevent unauthorized access to other customers' data, do not share this information with the customer.
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.

Configuring Saved Searches and Search Filters

Saved searches and search filters that you create in the ArcSight Command Center conform to the enforced filters defined in the ACL Editor's Events tab for the customer. While there are no additional content-related tasks related to searches, you must perform configuration tasks.

To prevent unintentional exposure of other tenants' events in Command Center, configure the property settings described here.

Note: You must restart all services after you configure the property settings.

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.

After you edit the properties, restart all services:

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

Managing ESM Content

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

Configuring ESM resources correctly is critical to MSSP provisioning. Make sure that 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.

The following topics provide information about managing content:

- Understanding MSSP SOC and Customer Interaction Modes
- Configuring Content

Understanding 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 interaction modes:

- **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 that is operated by the MSSP. The customer might 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:

- **No customer access.** The customer does not use the ArcSight Console or the ArcSight Command Center. Interaction with the customer is carried out by means outside of the ArcSight solution, such as an external ticketing system or an MSSP portal that either integrates with ArcSight or is operated independently.
- **Provide reports to the customer.** For example, reports for compliance purposes. Reports are provided by email 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.

Configuring Content

The customer interaction modes require that the customer has access to some of, but not limited to, the following, resources:

- Events
- Cases
- Reports
- Data Monitors
- Dashboards
- Notifications
- Common Set of Rules
- Tenant-specific Rules

In turn, these resources might rely on the following event-based content:

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

Events

Since an MSSP system uses enforced filters, you must set the customer tag for events to ensure that reports and search results include only events belonging to the customer.

For base events, this is ensured at the connector level. For correlation events, the generating rule must set the customer tag.

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

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 that 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.

Note: You can also use a set of reports designed specifically for MSSP use.

Defining Reports

Reports derive their data through queries or trends. Queries run during report generation. As the method for running reports on a schedule 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 Trends.

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.
- 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 in 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.

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 Reports Templates/MSSP/CUSTOMERNAME`.

Data Monitors

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

Statistical 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 might be normal for one customer but not for another. Other DMs and rules can consume correlation events that statistical DMs generate.

As with ESM's other event monitoring resources, viewing events on data monitors requires permissions. These events are specified through enforced filters.

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

1. Log in as the tenant administrator user.
2. Create data monitors for the tenant. 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.

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. 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 email based alerts:

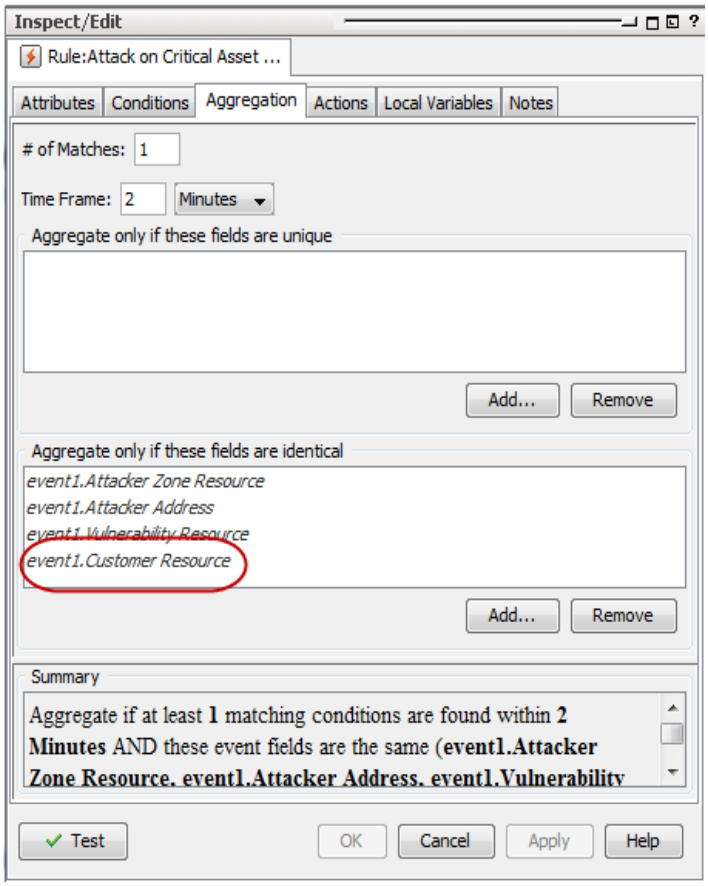
1. Prepare an active list containing customer names and associated email addresses to become recipients of notifications.
2. Use a variable in the rule to fetch the email address from the list based on the customer name.
3. Use the execute command rule action with the email address as the parameter to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

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.



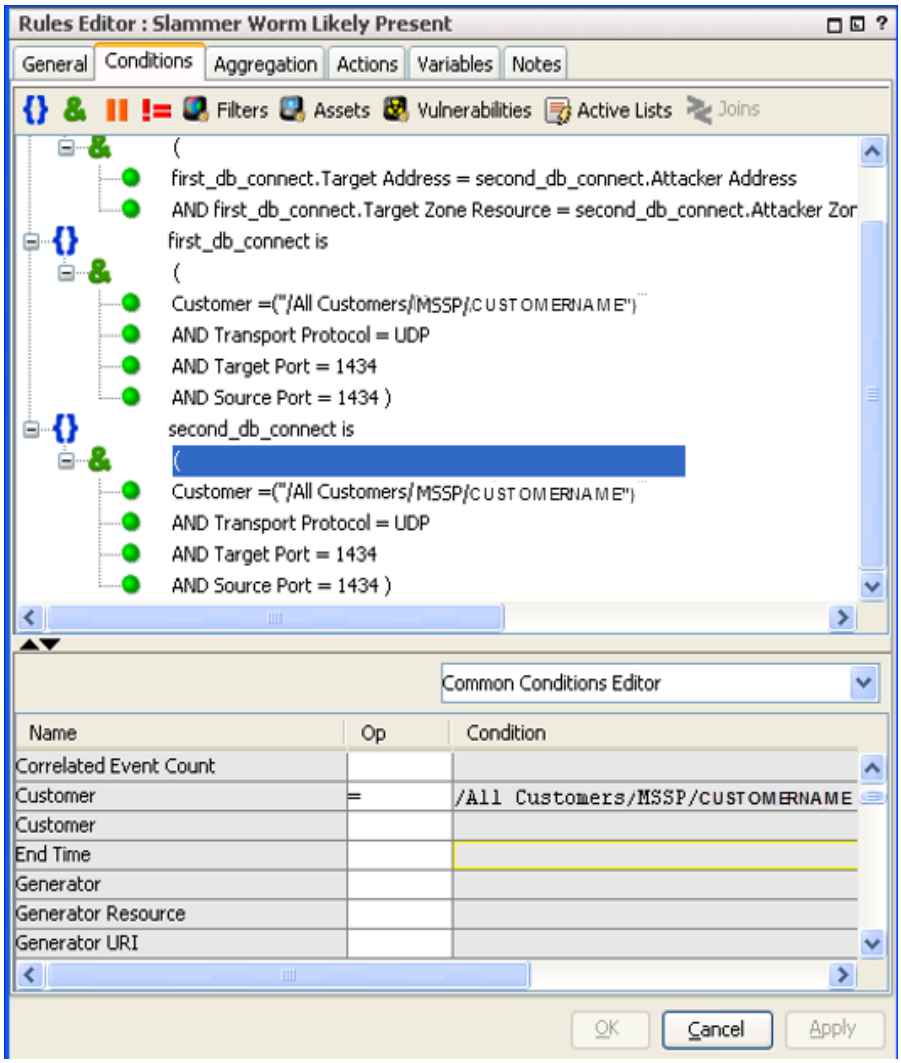
2. Set the correlation event customer tag to the customer value.

If events occur that trigger that rule, the correlation event generated by the triggered rule shows which event belongs to which customer.

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, define a set of rules where the condition for the rule refers to `Customer = "CUSTOMERNAME"`:

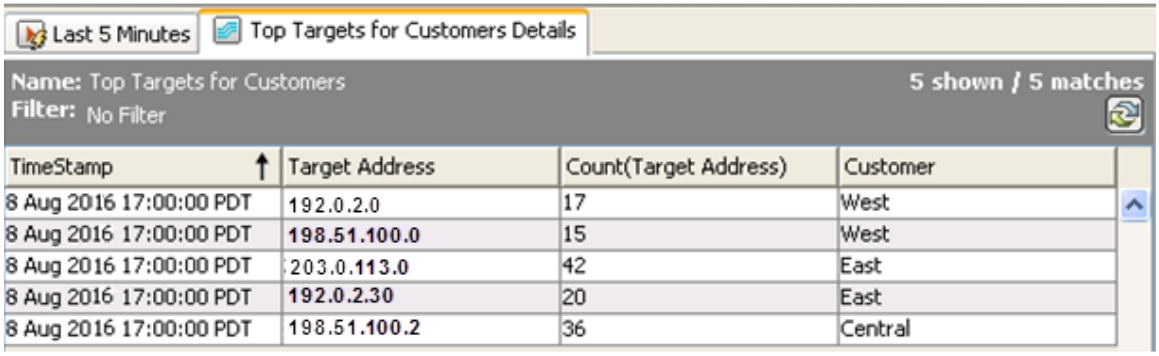


The generated correlation event for this rule will then include the aggregated customer tag in the Customer field.

Trends

To use a common trend for multiple customers:

- Include a Customer field in the trend schema that 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

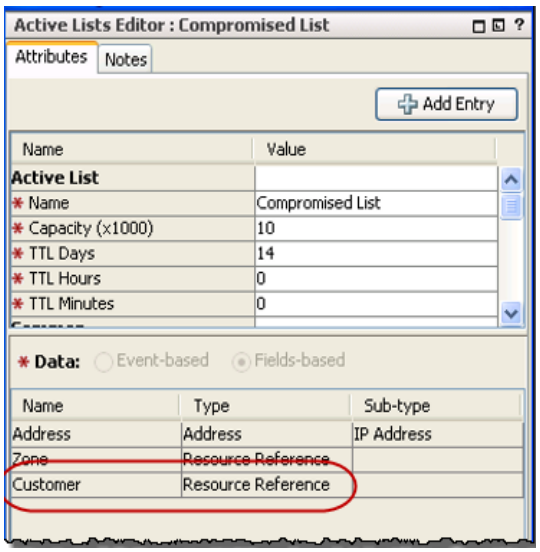
- In the trend query (the query used to fetch data from the trend for a report), use a Customer custom parameter to be used as a condition on the trend's Customer field. Set this custom parameter to the customer name when scheduling the reports.
- If you are using a separate trend per customer, log in as the customer administrator user to create each customer's trend.

Active Lists

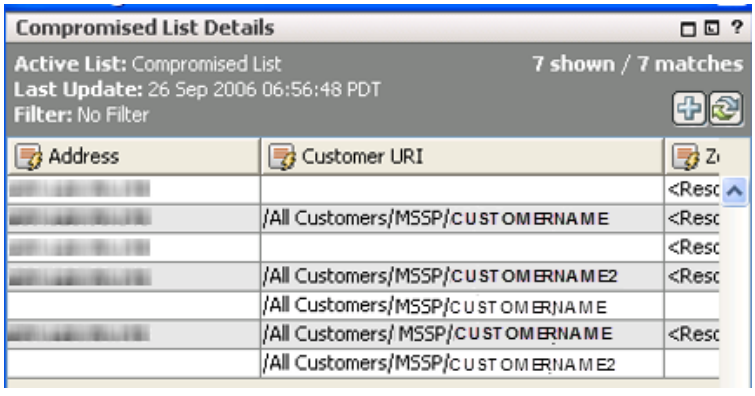
To create active lists common to all customers:

- 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 in the resulting list:



Installing MSSP Reports

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 Micro Focus 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.

For information about the included reports, installing them, and running them, see the Quick Start Guide to Reporting EPS Usage.

Troubleshooting the Deployment

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

Map file does not work

If your map file does not 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 do not contain valid entries.
2. If your `map.x.properties` does not contain 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 Understanding Customer Tagging.

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 a Velocity expression but is not evaluated properly, verify whether your Velocity expression has a syntax error.

Optimizing performance

- **Rules:** A poorly 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.

Adopting SOAR into the Multitenancy Environment

After you configure your ESM MSSP environment for multitenancy, if SOAR is integrated with ESM, you can adopt SOAR into your multitenancy solution for real-time detection and response capabilities. While ESM real-time analytics allows you to analyze events from multiple customers and detect threats, SOAR lets you manage customer cases and automated response activities such as case enrichments, attack mitigation, and notifications.

Note: When you adopt SOAR into your multitenancy solution, SOAR is only available to MSSP employees that have access to all tenants' data. End customers cannot directly access SOAR.

SOAR does not provide data segregation or tenant isolation. It provides tenant-based filtering capabilities so that you can differentiate the cases per tenant and perform response activities.

All tenant data is stored in the same datastore.

Adopting SOAR into your multitenancy environment involves the following activities:

	Task	See
❑	1. Integrate SOAR with ESM.	Integrating SOAR with ESM
❑	2. Edit the SOAR integration rule to segregate tenants' rules.	Editing the SOAR Integration Rule
❑	3. Define "Customer URI" as a scope item in SOAR.	Defining "Customer URI" as a Scope Item
❑	4. Add "Customer URI" as a visible alert field.	Adding "Customer URI" as a Visible Alert Field
❑	5. Add the customer name as a label.	Adding the Customer Name as a Label

Editing the SOAR Integration Rule

To segregate tenants' rules, the customer resource field for each standard rule that will be forwarded to SOAR must be aggregated. To accomplish this, you must use the ESM ArcSight Console to edit the SOAR Integration rule.

To edit the SOAR Integration rule:

1. In the Navigator, select the Resources tab, and then select Rules.
2. Under Rules > Shared > All Rules > Real-time Rules, double-click SOAR Integration Rule.
3. In the Inspect/Edit window, click the Actions tab.
4. Under On Every Event (Active), right-click Set Event Field Event Actions and select Edit.
5. In the name field, append the customer name to the rule name as a parameter. For example:

   ```
   ${customerName}: ${name}
   ```

   Note: The ${customerName} variable is derived from the correlation event Customer URI field. If a prior rule has not properly configured the Customer URI field, the value is empty.

Defining "Customer URI" as a Scope Item

Adopting SOAR into your multitenancy environment requires defining "Customer URI" as a scope item in the "Keyword" category and the "Related" role.

To define "Customer URI" as a scope item:

1. In SOAR, navigate to Respond > Configuration > Alert Source.
2. From the list of alert sources, select the ESM integration alert source and click Edit.
3. In the Alert Source Configuration Editor window, add the following to Configuration Content, and then click Save:

   ```
   baseevent.scope=/customer/uri:KEYWORD:RELATED
   ```

Adding "Customer URI" as a Visible Alert Field

After you define "Customer URI" as a scope item, you must add "Customer URI" as a visible alert field.

To add "Customer URI" as a visible alert field:

1. In SOAR, navigate to Configuration > Alert Source.
2. In the Alert Source Configuration Editor window, locate the ESM alert source, add the following to Visible Alert Fields, and then click Save:

   Field Name: `details.extension.customerURI`

   Visible Name: Customer URI

Adding the Customer Name as a Label

In order to differentiate cases, you must add the customer name as a label. First, you must create a label and then you must create classification playbooks based on the label.

To create a label:

1. In SOAR, navigate to Configuration > Case > Labels.
2. Create a label with the following values, and then click Save:

   Label Name: <customer name>

   Label Color: <assign a color to the label>

To create a classification playbook based on the label:

1. In SOAR, navigate to Playbooks > Classification.
2. Create a classification rule with the following values on the Conditions tab:

   Type: Alert source rule name matches regex

   Parameters: <javascript regex for the string in the rule name>

   For example: To match "Customer01," "customer01," "Customer 01," or "customer 01," the parameter value would be `(?s)(?i).*customer\s*01`.
3. On the Actions tab, specify the following values, and then click Save:

   Action: Add case label

   Parameters: <select the appropriate label>

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 Configuration Guide for ESM MSSP Multitenancy Environments (ESM 7.5)

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!