



HP ArcSight ESM

Software Version: 6.8c

IPv6 Standard Content Guide

November 12, 2014

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HP ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2014 Hewlett-Packard Development Company, L.P.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.hpenterprisesecurity.com/copyright>

Support

Contact Information

Phone	A list of phone numbers is available on the HP ArcSight Technical Support Page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hp.com
Protect 724 Community	https://protect724.hp.com

Contents

Chapter 1: IPv6 Overview	4
What is Standard Content?	4
Standard Content Packages	6
IPv6 Content	7
Chapter 2: Installation and Configuration	8
Installing the IPv6 Package	8
Configuring IPv6 Content	9
Chapter 3: IPv6 Use Case	10
IPv6 Resources	10
Send Documentation Feedback	19

Chapter 1: IPv6 Overview

This chapter discusses the following topics.

What is Standard Content?	4
Standard Content Packages	6
IPv6 Content	7

What is Standard Content?

Standard content is a series of coordinated resources (filters, rules, dashboards, reports, and so on) that address common security and management tasks. Standard content is designed to give you comprehensive correlation, monitoring, reporting, alerting, and case management out-of-the box with minimal configuration. The content provides a full spectrum of security, network, and configuration monitoring tasks, as well as a comprehensive set of tasks that monitor the health of the system.

Standard content is installed using a series of packages, some of which are installed automatically with the ArcSight Manager to provide essential system health and status operations. The remaining packages are presented as install-time options organized by category.

Standard content consists of the following:

- **ArcSight Core Security** content is installed automatically with the ArcSight Manager and consists of key resources for monitoring Microsoft Windows, firewall, IPS and IDS, NetFlow, and other essential security information.
- **ArcSight Administration** content contains several packages that provide statistics about the health and performance of ArcSight products.
 - ArcSight Administration is installed automatically with the ArcSight Manager and is essential for managing and tuning the performance of content and components.
 - ArcSight Admin DB CORR is installed automatically with the ArcSight Manager for the CORR-Engine (Correlation Optimized Retention and Retrieval) and provides information on the health of the CORR-Engine.

Note: The ArcSight Admin DB CORR content package is installed automatically when you perform a new ArcSight Manager installation. However package installation is different during upgrade. If you are upgrading your system from a previous version, check to see if the package is installed after upgrade. If the package is not installed, install it from the ArcSight Console.

- ArcSight Content Management is an optional package that shows information about content package synchronization with the ArcSight Content Management feature. The information

includes a history of content packages synchronized from a primary source to multiple destinations, and any common issues or errors encountered. You can install this package during ArcSight Manager installation or from the ArcSight Console any time after installation.

- ArcSight ESM HA Monitoring is an optional package that lets you monitor systems that use the ESM High Availability Module. You can install this package during ArcSight Manager installation or from the ArcSight Console any time after installation.
- ArcSight Search Filters is installed automatically with the ArcSight Manager for use in the ArcSight Command Center. You cannot edit or use these filters in the ArcSight Console. For information about the search filters, refer to the *ArcSight Command Center User's Guide*.

Note: The ArcSight Search Filters content package is installed automatically when you perform a new ArcSight Manager installation. However package installation is different during upgrade. If you are upgrading your system from a previous version, check to see if the package is installed after upgrade. If the package is not installed, install it from the ArcSight Console.

- **ArcSight System** content is installed automatically with the ArcSight Manager and consists of three packages: ArcSight Core, ArcSight Groups, and ArcSight Networks. ArcSight Core and ArcSight Groups contain resources required for basic security processing functions, such as threat escalation and priority calculations, as well as basic throughput channels required for out-of-the-box functionality. The ArcSight Networks package contains the zones that were in the ArcSight Core package in previous releases, in addition to local and global network resources.
- **ArcSight Foundation** content (such as Cisco Monitoring, Configuration Monitoring, Intrusion Monitoring, IPv6, NetFlow Monitoring, Network Monitoring, and Workflow) provide a coordinated system of resources with real-time monitoring capabilities for a specific area of focus, as well as after-the-fact analysis in the form of reports and trends. You can extend these foundations with additional resources specific to your needs or you can use them as a template for building your own resources and tasks. You can install a Foundation during installation or from the ArcSight Console any time after installation.
- **Shared Libraries** - ArcSight Administration and several of the ArcSight Foundations rely on a series of common resources that provide core functionality for common security scenarios. Dependencies between these resources and the packages they support are managed by the Package resource.
 - Anti Virus content is a set of filters, reports, and report queries used by ArcSight Foundations, such as Configuration Monitoring and Intrusion Monitoring.
 - Conditional Variable Filters content is a library of filters used by variables in standard content report queries, filters, and rule definitions. The Conditional Variable Filters are used by ArcSight Administration and certain ArcSight Foundations, such as Configuration Monitoring, Intrusion Monitoring, Network Monitoring, and Workflow.
 - Global Variables content is a set of variables used to create other resources and to provide event-based fields that cover common event information, asset, host, and user information, and

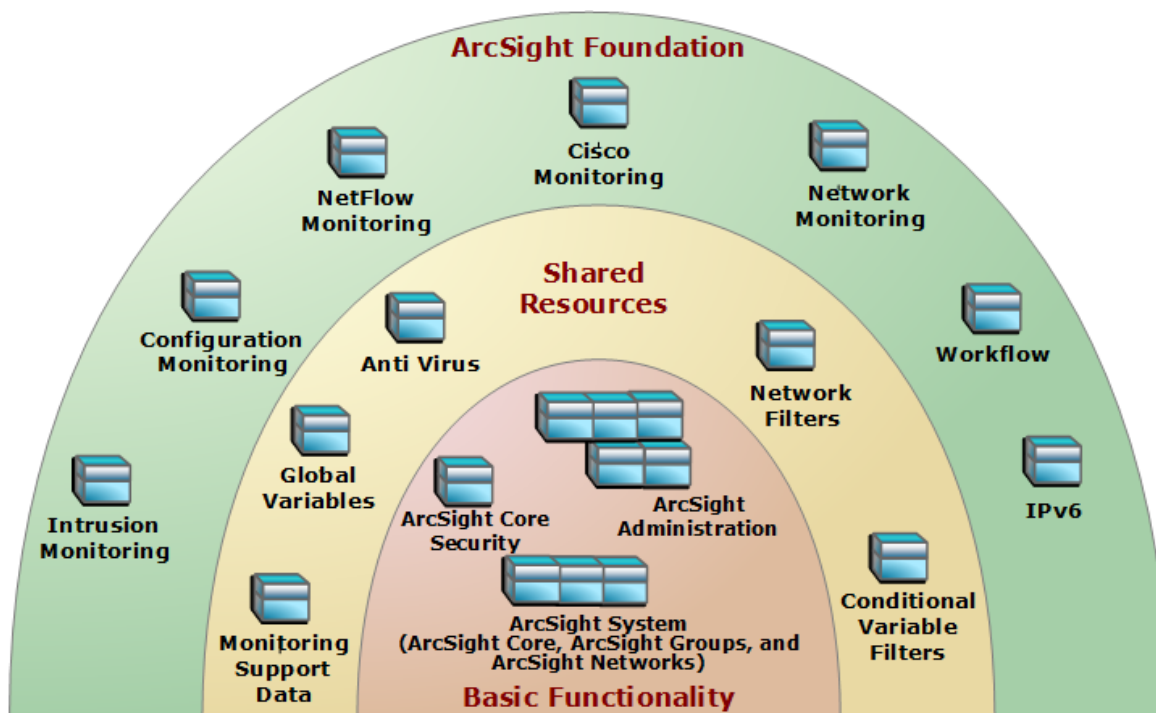
commonly used timestamp formats. The Global Variables are used by ArcSight Administration and certain ArcSight Foundations.

- Monitoring Support Data content is a set of active lists that store mapping information for HTTP return status code classes, Cisco firewall syslog message types, and encoded logon types.
- Network filters content is a set of filters required by ArcSight Administration and certain ArcSight Foundations, such as Intrusion Monitoring and Network Monitoring.

Caution: The resources in the ArcSight Core Security, ArcSight Administration, ArcSight DB CORR, Conditional Variable Filters, Global Variables, and Network Filters content packages are not locked even though they manage core functionality; HP recommends that you do not delete or modify these resources unless you are an advanced user who understands fully the resources and their dependencies.

Standard Content Packages

Standard content comes in packages (.arb files) that are either installed automatically or presented as install-time options. The following graphic outlines the packages.



The ArcSight Core Security, ArcSight Administration, and ArcSight System packages at the base provide content required for basic functionality. The common packages in the center contain shared resources that support multiple packages. The packages shown on top are ArcSight Foundations that address common network security and management scenarios.

Depending on the options you install, you will see the ArcSight Core Security, ArcSight Administration, and ArcSight System resources and some or all of the other package content.

Caution: When creating your own packages, you can explicitly include or exclude system resources in the package. Exercise caution if you delete packages that might have system resources. Make sure the system resources either belong to a locked group or are themselves locked. For more information about packages, refer to the *ArcSight Console User's Guide*.

IPv6 Content

The IPv6 content reports on data that comes from networks with IPv6 addresses.

This guide describes the IPv6 content. For information about ArcSight Core Security, ArcSight Administration, or ArcSight System content, refer to the *ArcSight Core Security*, *ArcSight Administration*, and *ArcSight System Standard Content Guide*. For information about an optional ArcSight Foundation, refer to the Standard Content Guide for that Foundation. ESM documentation is available on [Protect 724](https://protect724.hp.com) (<https://protect724.hp.com>).

Chapter 2: Installation and Configuration

This chapter discusses the following topics:

Installing the IPv6 Package	8
Configuring IPv6 Content	9

Installing the IPv6 Package

The IPv6 Foundation package is one of the standard content packages presented as install-time options. If you selected all the standard content packages to be *installed* at installation time, the packages and their resources are installed in the ArcSight Database and available in the Navigator panel resource tree. The package icons in the Navigator panel package view appear blue.

If you opted to exclude a Foundation package during ArcSight Manager installation, the package is *imported* into the Packages tab in the Navigator panel automatically, but is not available in the resource view. The package icon in the package view appears grey.

To install a package that is imported, but not installed:

1. On the Navigator panel Packages tab, navigate to the package you want to install.
2. Right-click the package and select **Install Package**.
3. In the Install Package dialog, click **OK**.
4. When the installation is complete, review the summary report and click **OK**.

The package resources are fully installed to the ArcSight Database, the resources are fully enabled and operational, and available in the Navigator panel resource tree.

To uninstall a package that is installed:

1. On the Navigator Panel Packages tab, navigate to the package you want to uninstall.
2. Right-click the package and select **Uninstall Package**.
3. In the Uninstall Package dialog, click **OK**.
4. The progress of the uninstall displays in the Progress tab of the Uninstalling Packages dialog. If a message displays indicating that there is a conflict, select an option in the Resolution Options area and click **OK**.
5. When uninstall is complete, review the summary and click **OK**.

The package is removed from the ArcSight Database and the Navigator panel resource tree, but remains available in the Navigator panel Packages tab, and can be re-installed at another time.

If you do not want the package to be available in any form, you can *delete* the package.

To delete a package and remove it from the ArcSight Console and the ArcSight Database:

1. On the Navigator Panel Packages tab, navigate to the package you want to delete.
2. Right-click the package and select **Delete Package**.
3. When prompted for confirmation, click **Delete**.

The package is removed from the Navigator panel Packages tab.

Configuring IPv6 Content

The IPv6 content is triggered by events from IPv6-enabled SmartConnectors. Contact your HP ArcSight sales representative for a list of IPv6-enabled SmartConnectors.

A network model keeps track of the network nodes participating in the event traffic. Modeling your network and categorizing critical assets using the standard asset categories is what activates some of the standard content and makes it effective. For information about populating the network model, refer to the ArcSight Console User's Guide. To learn more about the architecture of the ESM network modeling tools, refer to the *ESM 101 guide*.

The IPv6 content contains many reports. You can run reports on demand, automatically on a regular schedule, or both. By default, IPv6 reports are not scheduled to run automatically. Evaluate the reports that come with IPv6, and schedule the reports that are of interest to your organization and business objectives. For instructions about how to schedule reports, refer to the *ArcSight Console User's Guide*.

Chapter 3: IPv6 Use Case

The IPv6 content shows data that comes from networks with IPv6 addresses.

Standard content resources are grouped together in the ArcSight Console in use case resources. A use case resource provides a way to see a set of resources that help address a specific security issue or business requirement.

To view the resources associated with the IPv6 use case resource:

1. In the Navigator panel, select the **Use Cases** tab.
2. Open the **ArcSight Foundation/IPv6** group.
3. Right-click the IPv6 use case resource and select the **Open Use Case** option, or double-click the use case resource.

IPv6 Resources

The following table lists all the resources in the IPv6 use case.

Resources that Support the IPv6 Use Case

Resource	Description	Type	URI
Monitor Resources			
Successful Logins by Destination IPv6 Address	This report shows authentication successes from login attempts by destination IPv6 address. A chart shows the top destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Report	ArcSight Foundation/IPv6/
Top Alert IPv6 Destinations	This report shows the top IDS and IPS alert destinations per day.	Report	ArcSight Foundation/IPv6/
Top IDS Signature IPv6 Sources per Day	This report shows the Top IDS signature sources per day.	Report	ArcSight Foundation/IPv6/

Resources that Support the IPv6 Use Case, continued

Resource	Description	Type	URI
Attacker IPv6 Counts by ArcSight Priority	This report displays a table with the priority, attacker IPv6 address and the count of attack events where the category significance starts with Compromise or Hostile.	Report	ArcSight Foundation/IPv6/
Attacker Counts by IPv6 Device	This report displays a table with the device IPv6 address, attacker IPv6 address, and the count of attacker events where the category significance starts with Compromise or Hostile.	Report	ArcSight Foundation/IPv6/
Top IDS Signature IPv6 Destinations per Day	This report shows the top IDS signature destinations per day.	Report	ArcSight Foundation/IPv6/
Target Counts by IPv6 Attacker	This report displays the attacker address, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/IPv6/
Target Counts by IPv6 Device	This report displays the device address, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/IPv6/
Denied Outbound Connections by IPv6 Address	This report shows a summary of the denied outbound traffic by local address. A chart shows the top IPv6 addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Foundation/IPv6/
Target IPv6 Counts by ArcSight Priority	This report displays the priority, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/IPv6/
Top Alert IPv6 Sources	This report shows the top IDS and IPS alert sources per day. A chart shows the top IDS and IPS alert source IP addresses. A table shows the top alert source IP addresses, as well as the device vendor and product of the reporting device.	Report	ArcSight Foundation/IPv6/

Resources that Support the IPv6 Use Case, continued

Resource	Description	Type	URI
Successful Logins by Source IPv6 Address	This report shows authentication successes from login attempts by source IPv6 address. A chart shows the top source addresses with successful login attempts. A table shows the count of authentication successes by source-destination pair and by user.	Report	ArcSight Foundation/IPv6/
Top IPv6 Talkers	This report shows the Top talkers and a detailed list of the top talkers.	Report	ArcSight Foundation/IPv6/
Denied Inbound Connections by IPv6 Address	This report shows a summary of the denied inbound traffic by foreign address. A chart shows the top IPv6 addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Foundation/IPv6/
Top N Attacked IPv6 Targets	This report displays a 3D Stacking Bar Chart showing the Target Address and the sum of the Aggregated Event Count for events matching the Attack Events filter. It was deprecated.	Report	ArcSight Foundation/IPv6/
Alert Counts by IPv6 Device	This report shows the count of IDS and IPS alerts by device. A chart shows the top device IPv6 addresses with the highest counts. A table shows the list of all the devices, grouped by device vendor and product, then sorted by count.	Report	ArcSight Foundation/IPv6/
Top IPv6 Attackers	This report displays a chart of the attacker address, and the count of events where the category significance starts with Compromise or Hostile.	Report	ArcSight Foundation/IPv6/
Top N IPv6 Attacker Details	This report displays the priority, attacker address, and the count of attack events where the category significance starts with Compromise or Hostile. The query uses the sum of the aggregated event count instead of counting the EventID so that attackers are not split by the attack type.	Report	ArcSight Foundation/IPv6/

Resources that Support the IPv6 Use Case, continued

Resource	Description	Type	URI
Failed Logins by Destination IPv6 Address	This report shows authentication failures from login attempts by destination IPv6 address. A chart shows the top destination addresses with failed login attempts. A table shows the count of authentication failures by destination-source pair and by user.	Report	ArcSight Foundation/IPv6/
Failed Logins by Source IPv6 Address	This report shows authentication failures from login attempts by source IPv6 address. A chart shows the top source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Report	ArcSight Foundation/IPv6/
Attacker Counts By IPv6 Target	This report displays the attacker IPv6 address, the event name, and the count of attack events where the category significance starts with Compromise or Hostile, for the address specified in the parameters.	Report	ArcSight Foundation/IPv6/
Target IPv6 Counts by Event Name	This report displays the event name, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/IPv6/
Library Resources			
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Agent IPv6 Address	This variable is an alias for Device Custom IPv6 Address4.	Global Variable	ArcSight Foundation/Variables Library/IPv6
Target IPv6 Address	This field denotes the Target IPv6 address. The term target is dependent upon the originator field, i.e., Source or Destination, depending on the specific event. If the originator field is Destination, return Device Custom IPv6 Address2 (aliased as Destination IPv6 Address), or return Device Custom IPv6 Address1 (aliased as Source IPv6 Address)	Global Variable	ArcSight Foundation/Variables Library/IPv6

Resources that Support the IPv6 Use Case, continued

Resource	Description	Type	URI
Source IPv6 Address	This variable is an alias for Device Custom IPv6 Address1.	Global Variable	ArcSight Foundation/Variables Library/IPv6
Destination IPv6 Address	This variable is an alias for Device Custom IPv6 Address2.	Global Variable	ArcSight Foundation/Variables Library/IPv6
Attacker IPv6 Address	This field denotes the Attacker IPv6 address. The term attacker is dependent upon the originator field, i.e., Source or Destination, depending on the specific event. If the originator field is Source, return Device Custom IPv6 Address1 (aliased as Source IPv6 Address), or return Device Custom IPv6 Address2 (aliased as Destination IPv6 Address)	Global Variable	ArcSight Foundation/Variables Library/IPv6
Device IPv6 Address	This variable is an alias for Device Custom IPv6 Address3.	Global Variable	ArcSight Foundation/Variables Library/IPv6
Attack IPv6 Events	This filter selects events where the category significance starts with /Compromise or /Hostile.	Filter	ArcSight Foundation/IPv6/
External Source	This filter identifies events originating from outside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Inbound Events	This filter identifies events coming from the outside network targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
External Target	This filter identifies events targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Outbound Events	This filter identifies events originating from inside the company network, targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters

Resources that Support the IPv6 Use Case, continued

Resource	Description	Type	URI
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
IDS -IPS IPv6 Events	This filter passes Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) events.	Filter	ArcSight Foundation/IPv6/
Denied Inbound Connections by IPv6 Address	This query identifies the count of denied inbound connections by foreign address (address and hostname).	Query	ArcSight Foundation/IPv6/
Failed Logins by IPv6 Source-Destination Pair	This query returns authentication failure events from login attempts. The query returns the source address, source host name, destination address, destination host name, user name, user ID, count of failed logins, and device group.	Query	ArcSight Foundation/IPv6/
Denied Outbound Connections by IPv6 Address	This query identifies the count of denied outbound connections by local address (address and hostname).	Query	ArcSight Foundation/IPv6/
Failed Logins by Destination IPv6 Address (Chart)	This query returns authentication failure events from login attempts, including the count of failed login attempts by destination address.	Query	ArcSight Foundation/IPv6/
Target IPv6 Counts by Event Name	This query returns the event name, target address and the sum of the aggregated event count for events matching the Attack Events filter.	Query	ArcSight Foundation/IPv6/
Top 10 IPv6 Attackers	This query identifies the attacker address, and the count of events where the category significance starts with Compromise or Hostile. The query uses the sum of the aggregated event count instead of counting the EventID so that attackers are not split by the attack type.	Query	ArcSight Foundation/IPv6/

Resources that Support the IPv6 Use Case, continued

Resource	Description	Type	URI
Target Counts by IPv6 Attacker	This query returns the attacker address, target address and the sum of the aggregated event count for events matching the Attack Events filter.	Query	ArcSight Foundation/IPv6/
Target Counts by IPv6 Device	This query returns the device address, target address and the sum of the aggregated event count for events matching the Attack Events filter.	Query	ArcSight Foundation/IPv6/
Top 10 Attacked IPv6 Targets	This query selects the Target IPv6 Address and the sum of the Aggregated Event Count for events matching the Attack IPv6 Events filter.	Query	ArcSight Foundation/IPv6/
Attacker Counts by IPv6 Device	This query identifies the device address, attacker address, and the count of events where the category significance starts with Compromise or Hostile.	Query	ArcSight Foundation/IPv6/
Successful Logins by Source IPv6 Address (Chart)	This query returns authentication success events from login attempts.	Query	ArcSight Foundation/IPv6/
Alert Counts by IPv6 Device	This query returns the count of IDS and IPS alerts by device vendor, product, address and hostname.	Query	ArcSight Foundation/IPv6/
Top 10 IPv6 Talkers	This query returns the attacker address and the count of events in which the category significance starts with Compromise or Hostile. The query uses the sum of the aggregated event count instead of counting the EventID so that attackers are not split by the event name.	Query	ArcSight Foundation/IPv6/
Top IDS Signature IPv6 Sources per Day	This query over base IDS/Network events returns the attacker address, device vendor, device product, and the count of the events within the query timeframe.	Query	ArcSight Foundation/IPv6/

Resources that Support the IPv6 Use Case, continued

Resource	Description	Type	URI
Top IDS Signature IPv6 Destinations per Day	This query over base IDS/Network events returns the target address, device vendor, device product, and the count of the events within the query timeframe.	Query	ArcSight Foundation/IPv6/
Successful Logins by Destination IPv6 Address (Chart)	This query returns authentication success events from login attempts, including the count of failed login attempts by destination address.	Query	ArcSight Foundation/IPv6/
Top Alert IPv6 Sources	This query identifies the count of IDS and IPS alerts by source address, device vendor, and device product.	Query	ArcSight Foundation/IPv6/
Top 10 IPv6 Attacker Details	This query identifies the priority, attacker address, and the count of events where the category significance starts with Compromise or Hostile. The query uses the sum of the aggregated event count instead of counting the EventID so that attackers are not split by the attack type.	Query	ArcSight Foundation/IPv6/
Target IPv6 Counts by ArcSight Priority	This query returns the priority, target address and the sum of the aggregated event count for events matching the Attack Events filter.	Query	ArcSight Foundation/IPv6/
Attacker Counts By IPv6 Target	This query identifies the attacker IPv6 address, the event name, and the count of events where the category significance starts with Compromise or Hostile for the target information given in the parameters.	Query	ArcSight Foundation/IPv6/
Failed Logins by Source IPv6 Address (Chart)	This query returns authentication failure events from login attempts, including the count of failed login attempts by source address.	Query	ArcSight Foundation/IPv6/

Resources that Support the IPv6 Use Case, continued

Resource	Description	Type	URI
Attacker IPv6 Counts by ArcSight Priority	This query identifies the priority, attacker address, and the count of events where the category significance starts with Compromise or Hostile.	Query	ArcSight Foundation/IPv6/
Successful Logins by IPv6 Source-Destination Pair	This query returns authentication success events from login attempts.	Query	ArcSight Foundation/IPv6/
Top Alert IPv6 Destinations	This query returns the count of IDS and IPS alerts by destination address, device vendor, and device product.	Query	ArcSight Foundation/IPv6/
Top 10 IPv6 Targets	This query returns the target address and the sum of the aggregated event count for events matching the Attack Events filter used in the following reports: Top N Targets, Top N Targets (3D Pie Chart), Top N Targets (Bar Chart), Top N Targets (Inverted Bar Chart), Top N Targets (Pie Chart), Top N Targets (Table and Chart), and Top N Targets (Table).	Query	ArcSight Foundation/IPv6/
Simple Table Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/1 Table
Simple Chart Portrait	This template is designed to show one chart. The orientation is portrait.	Report Template	ArcSight System/1 Chart/Without Table
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	ArcSight System/1 Chart/With Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table

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 system, click the link above and an email window opens with the following information in the subject line:

Feedback on IPv6 Standard Content Guide (ESM 6.8c)

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 arc-doc@hp.com.

We appreciate your feedback!