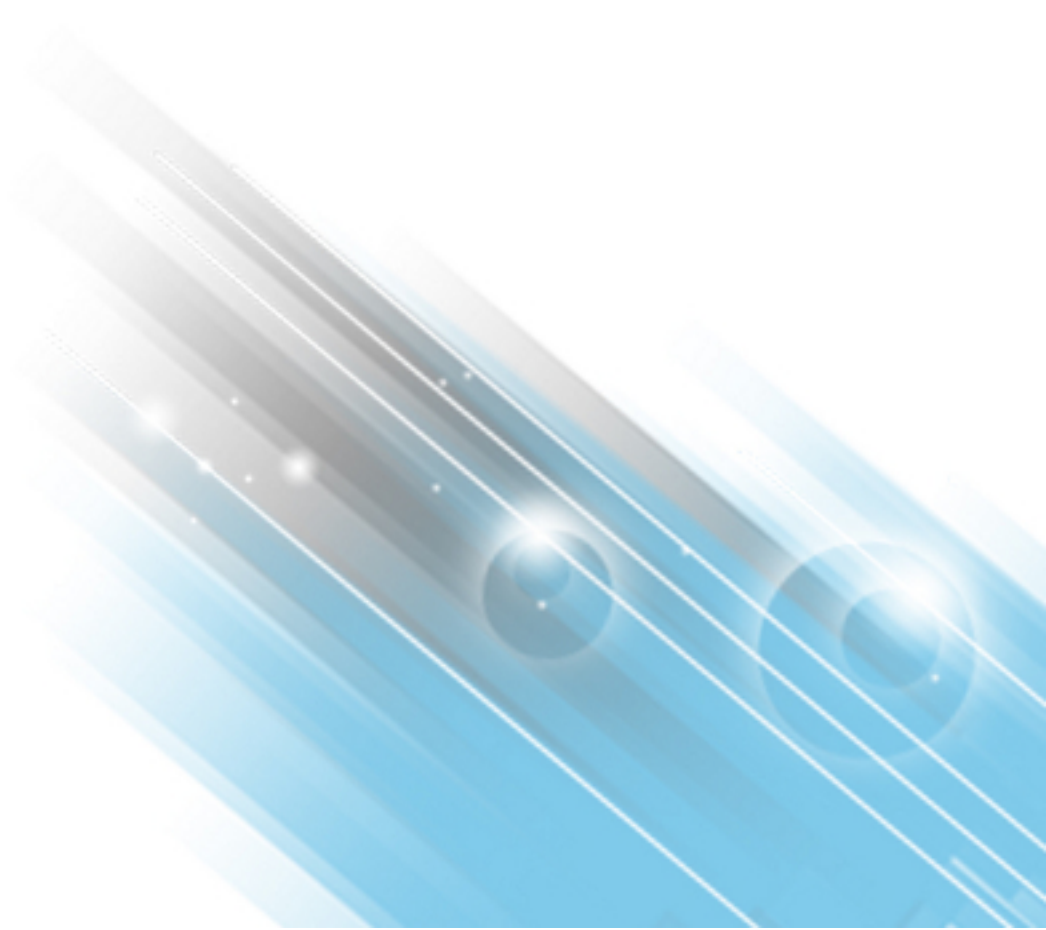




HP ArcSight ESM

Zone Updates Subscription Implementation Guide

February 16, 2016



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 2016 Hewlett-Packard Development Company, L.P.

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

<https://www.protect724.hpe.com/docs/DOC-13026>

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://www.protect724.hpe.com

Zone Update Subscription

The `zoneUpdate` command updates IPv4 address allocations and dark space information with updates that are provided in the periodic Zone Update Subscription Package, which is contained in the `Zone_Updates_<version>.zip` file. Use of this command is optional, and applies to the Manager and the ArcSight Console. You can use `zoneUpdate` after a successful Manager installation or upgrade. This command is available from the command line only, and has no GUI functionality.

Running `zoneUpdate` requires an ESM administrator login and password. While the process is running, do not use the same administrator account to access the ArcSight Console or ArcSight Command Center for other administrative tasks. Allow up to 50 minutes or longer for a first-time zone update, depending on the manager workload and the number of assets assigned to the global network. Subsequent incremental updates should not take as long. While `zoneUpdate` is running, other ESM administrators and users may access the Console or Command Center.

`zoneUpdate` performs these actions in the Global network:

- Inventories affected assets
- Removes old zones
- Installs and updates zones
- Auto-zones assets that appeared in the inventory of affected assets in the Global network

`zoneUpdate` updates zones in the Global network only. Local zones are not updated by this command. The behavior of `zoneUpdate` is the same for both dynamic and static zones.

Best Practices for Importing Packages

If you need to perform zone updates and/or operate under high loads, disable the `resource.move` property (which means to set it to `true`) and perform the package import. This can help prevent failure of import for large packages, in some cases. Before attempting a zone update, be sure to verify that the `resource.move` property is set to `true` in `server.properties`.

To set the `resource.move` property to `true`, add this statement in `server.properties`:

```
esm.manager.disable.resource.move=true
```

Refer to the ESM Administrator's Guide, "Editing Properties Files," for details on editing the `server.properties` file.

Recommendations

- HP recommends that assets are allocated to the local network only and that the Global network does not contain assets. Also, zones that have categories assigned to them, and then are removed and reinstalled as part of the zone update process lose the category assignments. HP also recommends you do not assign categories to the system zones.
- HP recommends that you perform a full system database table backup (`export_system_tables`) and export the current ArcSight Network package before using `zoneUpdate`, to ensure that you have a usable snapshot of your network model. If the zone update process is interrupted or a problem occurs and you must revert your data, be sure to use this backup to restore your ArcSight resources before attempting to run `zoneUpdate` again.
- HP recommends running `zoneUpdate` during non-peak system time. Running `zoneUpdate` can take up to 20 or 40 minutes, depending on Manager workload and the number of assets assigned to the Global network.

Running zoneUpdate

Note: Zone Groups belonging to Regional Internet Registries (RIR) that contain more than 1000 zones will place their corresponding zones in subgroups, each group containing up to 950 zones, to enable you to better manage those zones, and content related to them, from within the ArcSight Console.

1. Log in as user *arcsight*.
2. Verify that the Manager is running.
3. Extract the `Zone_Updates_<version>.zip` file into a directory. The directory can be of your choice. The zipped files extract into the folder `ArcSight_Networks_<version>`, which contains the files `ArcSight_Networks.arb` and `Zone_Removal_Tool.xml`. Do not change the name of this folder or the names of the extracted files.
4. Verify that the user *arcsight* has write permissions to the directory into which you extracted `Zone_Updates_<version>.zip`.
5. As user *arcsight*, run this command: `/opt/arcsight/manager/bin/arcsight zoneUpdate -m <Manager hostname or IP address> -u <user with administrative privileges> -f <folder where zip file was extracted>`

You are prompted for the user password.

Note: Be sure to enter the correct password. `zoneUpdate` uses the entered password several times, and temporarily locks you out if you use the wrong password. If this happens, you can reenable the user or wait for the user to be reenabled automatically.

Warning: Do not interrupt or kill `zoneUpdate` after the processing starts. Allow `zoneUpdate` to complete, and then make a determination of the condition of your zones and whether to install another version of the Zone Update Subscription package.

Recovery and Troubleshooting

Zone Updates Not Applied

If `zoneUpdate` runs with errors, and does not apply the zone updates from the Zone Update Subscription Package, follow these steps:

1. Restart the Manager.
2. Run `zoneUpdate` again.
3. If the above steps do not work, and you encounter the same errors as before, import the full system database table backup (`export_system_tables`) and the current ArcSight Network package that you exported before initially running `zoneUpdate`.
4. Run `zoneUpdate` again.

Package Exists Error When Applying the Zone Update Subscription Package

If you encounter these messages when running `zoneUpdate`:

```
Reading bundle 'Common Bundle Alias' Done. 0 min 0 sec 41 ms
Importing 1 packages
Importing package 1/1 '/All Packages/ArcSight System/ArcSight
Networks'
Parsing archive 'ArcSight Networks.xml'... Done. 0 min 1 sec 19 ms
Package Already Exists with Newer Content
```

```
Package '/All Packages/ArcSight System/ArcSight Networks' already
exists in the system with newer content
```

- ```
1: Leave newer package
2: Never override newer packages
3: Update package
4: Always update Packages
5: Abort
```
- 

Choose option 3, Update package.

# Asset Zoning

Assets that were zoned in the Global network before you run `zoneUpdate` will be zoned after the command completes.

# Asset Ranges

Asset ranges are not auto-zoned by `zoneUpdate`. Asset ranges will be unzoned by the running of the `zoneUpdate`; you must manually rezone asset ranges after you run `zoneUpdate` if you had asset ranges in the Global network.

For example, if you had an asset range in Zone A in a previous version of ESM, the asset range is unzoned after you run `zoneUpdate`. For this example, suppose Zone A was split into two zones, Zone A and Zone B, and after upgrade your asset range spans the last part of Zone A and first part of Zone B. In this case, the asset range becomes unzoned. To recover zoning, you must open each unzoned asset range resource and map it to the correct zone, or split it into two asset ranges that map to the new Zones A and B.

# zoneUpdate Syntax Example

```
/opt/arcsight/manager/bin/arcsight zoneUpdate -m <Manager hostname or IP address> -
u <user with administrative privileges> -f <folder where zip file was extracted>
```

For example, to update zones for Manager 192.0.2.0:

```
/opt/arcsight/manager/bin/arcsight zoneUpdate -m 192.0.2.0 -u admin2 -f
/opt/arcsight/manager
```

# zoneUpdate Parameters

This table lists `zoneUpdate` parameters:

|               |                                                                                                                                                          |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| -m <manager>  | The Manager hostname or IP address. Use of a hostname or an IP address depends on whether your Manager was configured using a hostname or an IP address. |
| -u <username> | The name of a user with administrative privileges.                                                                                                       |

|             |                                                                                                                                                                                                                                            |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -f <folder> | Folder name or the path to the folder that contains the unzipped Zone Update Subscription package. For example, /opt/arcsight/manager. Extract the file Zone_Updates_<version>.zip into this folder, and give the folder write permission. |
| -h          | Help                                                                                                                                                                                                                                       |

