Archer® Exchange

# Archer® Suite

Version 6.12

# Implementation Guide

February 2023

# Qualys Vulnerability Management

**Contact Information**
RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

**Trademarks**
RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.archerirm.com/company/trademarks. Other trademarks are trademarks of their respective owners.

**License Agreement**
This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

**Third-Party Licenses**
This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

**Note on Encryption Technologies**
This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

**Distribution**
Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. CUSTOMER IS SOLELY RESPONSIBLE FOR ENSURING THAT THE INSTALLATION OF THE APPLICATION IS PERFORMED IN A SECURE MANNER. RSA RECOMMENDS CUSTOMERS PERFORM A FULL SECURITY EVALUATION PRIOR TO IMPLEMENTATION.



May 2020

Revised: February 2023

# Table of Contents

# Release Notes

## What's New

The following table describes enhancements.

| Release Version | Published Date | Notes |
|---|---|---|
| **Archer 6.4 SP1** | August 2018 | Initial Release |
| **Archer 6.7** | May 2020 | Offering updated to leverage the Application Managed Output Writer for JavaScript Transporter and notes to update required Archer version 6.7 use cases. Added note regarding network connectivity issues when extracting large amounts of data. |
| **Archer 6.7** | December 2021 | Re-Signed JavaScript file. |
| **Archer 6.12** | February 2023 | RSA Archer 6.12 Qualys VM Knowledge Base Data Mapping update |

# Chapter 1: Overview

Qualys Vulnerability Management is a cloud-based service that provides immediate, global visibility into where your IT systems might be vulnerable to the latest Internet threats and how to protect them. It helps you to continuously identify threats and monitor unexpected changes in your network before they turn into breaches.

## Key Features and Benefits

The Qualys VM integration with the Archer IT & Security Vulnerabilities Program use case enables organizations to:

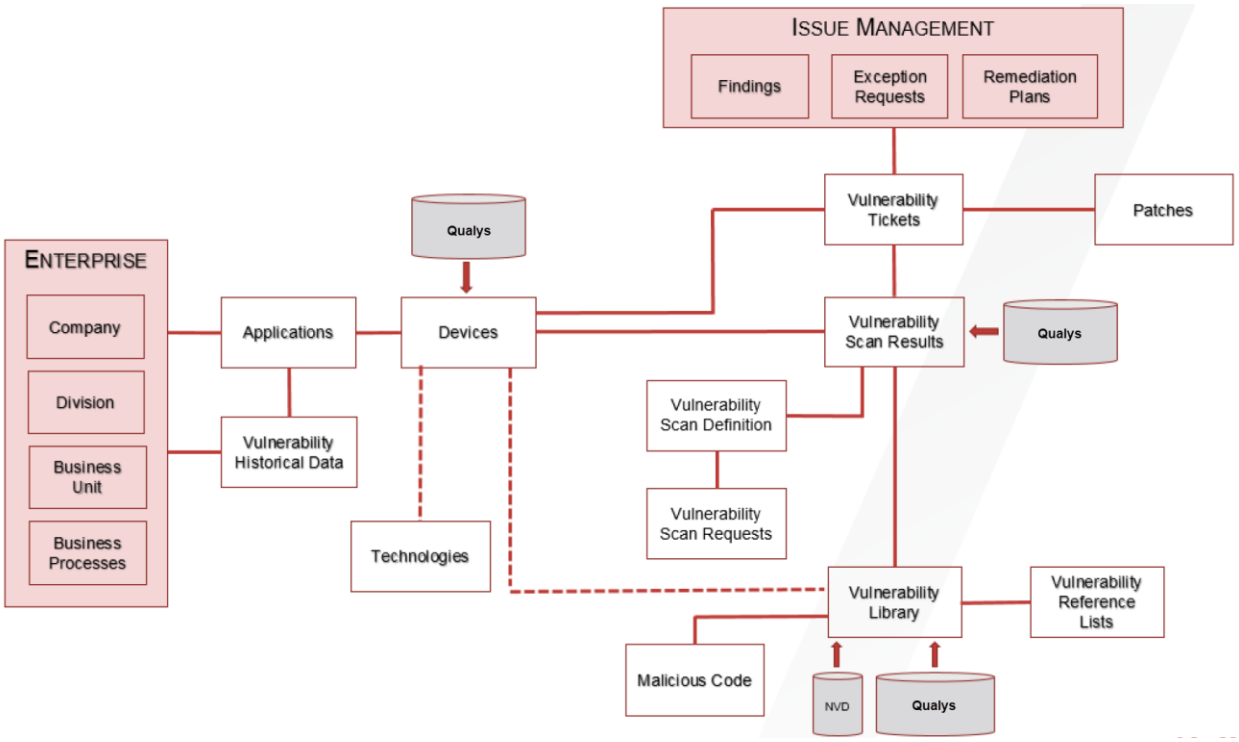
- Catalog network devices on a corporate network
- Discover network device vulnerabilities using scanning technology
- Supplement the Vulnerability Library with Qualys' knowledge base

**Important:** In the event your integration is attempting to extract large amounts data, the execution of the JavaScript code could take multiple hours. In order to avoid a timeout of the session token, the Archer Services Parameter must be extended. Currently the Archer Services account timeout parameter is set by default to 30 minutes. In the event the JavaScript code has not completed in the allotted timeframe, the data feed will fail.

## Requirements

| Components | Requirement |
|---|---|
| **Archer Solution** | IT Security Risk Management |
| **Archer Use Case** | IT & Security Vulnerabilities Program |
| **Archer Applications** | Devices, Vulnerability Library, and Vulnerability Scan Results |
| **Requires On-Demand License** | No |

## Integration Diagram



# Chapter 2: Installation and Configuration

This section provides instructions for configuring the Qualys VM data feeds in the Archer Platform. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

The Archer IT Security Vulnerability Program use case must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

**Important:** The Archer IT Security Vulnerability Program use case, Issues Management use case, and licensed applications from the Enterprise Catalog package must be installed and working prior to performing the integration. Perform the necessary tests to confirm that this is true prior to proceeding.

**Important:** The integration described in this guide is being provided as a reference implementation for evaluation and testing purposes. It may or may not meet the needs and use cases for your organization. If additional customizations or enhancements are needed, it is recommended that customers contact RSA Professional Services for assistance.

## System Requirements

The following components are required for installation and operation of the Qualys Vulnerability Management data feeds for the IT Security Vulnerability Program use case. The applications listed in the details section of the table serve as the target applications for the data feeds.

| Component | Details |
|---|---|
| Archer | Archer 6.12 or later |
| Prerequisite Applications<br><br>(Archer IT Security Vulnerabilities Program) | • Devices<br>• Vulnerability Library<br>• Vulnerability Scan Results |

# Data Feed Configuration

## Data Feeds

The following data feeds are provided with this integration:

| Data Feed | Description |
|---|---|
| Archer 6.12 Qualys VM Knowledge Base | The Archer 6.12 Qualys VM Knowledge Base feed is a JavaScript Transporter feed that utilizes API calls to extract all exploitable vulnerabilities from a Qualys vulnerability database. Qualys data is imported and leveraged in the Vulnerability Library application. |
| Archer 6.12 Qualys VM Hosts | The Archer 6.12 Qualys VM Hosts feed is a JavaScript Transporter feed that utilizes API calls to extract all the asset inventory discovered based on a client's scanner configuration and implementation. Qualys VM data is imported and leveraged in the Devices application.<br>For data ingestion, Archer offers configurable settings that allow individual clients to define how to uniquely identify devices in their organization. |
| Archer 6.12 Qualys VM Hosts Extracted From Detections | The Archer 6.12 Qualys VM Hosts Extracted From Detections feed is a JavaScript Transporter feed that utilizes API calls to extract all the asset inventory from the hosts vulnerability detection data. Qualys VM data is imported and leveraged in the Devices application.<br>For data ingestion, Archer offers configurable settings that allow individual clients to define how to uniquely identify devices in their organization. |
| Archer 6.12 Qualys VM Detections | The Archer 6.12 Qualys VM Detections feed is a JavaScript Transporter feed that utilizes API calls to extract a list of hosts with the hosts latest vulnerability data.<br>For data ingestion, Archer offers configurable settings that allow individual clients to define how to uniquely identify vulnerability detections in their organization.<br>For data ingestion, Archer offers configurable settings that allow individual clients to define how to uniquely identify devices in their organization. |

**Important:** You must install all package files before importing data feeds. Package files include the IT Security Vulnerabilities Program use case package, the Enterprise Catalog package, and the Issues Management prerequisite use case package. For more information, see the "Installing the Packages" section of the IT Security Vulnerabilities Program use case in the Archer Online Documentation.

Import and run the data feeds in the following order:

1. (Optional) NVD Data Feeds
   **Note:** For information on setting up the NVD data feeds, see the *NIST National Vulnerability Database (NVD) Data Feeds for Archer IT Security Vulnerability Program Implementation Guide* on the RSA Exchange on RSA Link.

2. Archer 6.12 Qualys VM Knowledge Base.dfx5
3. Archer 6.12 Qualys VM Hosts.dfx5
4. Archer 6.12 Qualys VM Hosts Extracted From Detections.dfx5
5. Archer 6.12 Qualys VM Detections.dfx5

**Note:** After setting up the data feeds, you can schedule the feeds to run when you want to. The Archer 6.12 Qualys VM feeds are designed in a way they can easily be decoupled and initiated on a more frequent schedule basis to fit your needs. For more information, see the Scheduling Data Feeds section.

## Configure the JavaScript Transporter Settings

Before you upload a JavaScript file, you must configure JavaScript Transporter settings in the Archer Control Panel.

1. On the General tab, go to the JavaScript Transporter section.
    1. Open the Archer Control Panel.
    2. Go to Instance Management and select All Instances.
    3. Select the instance.
    4. On the General tab, go to the JavaScript Transporter section.
2. Set the Max Memory Limit and the Script Timeout variable to align with the resources necessary to retrieve data. Most incremental feeds can probably be achieved with a Max Memory Limit of 3048 MB (3 GB) and a Script Timeout of 300 minutes (5 hours).
3. Require Signature is enabled by default on install and required for all Hosted clients.
    a. In the Signing Certificate Thumbprints section, add a thumbprint for each digitally signed JavaScript file.
        i. Double-click an empty cell in the Signing Certificate Thumbprints section.
        ii. Enter the digital thumbprint of the trusted certificate used to sign the JavaScript file.

        **Note:** For information on how to obtain digital thumbprints, see Obtaining Digital Thumbprints.

        **Important:** If you enable Require Signature and do not specify thumbprints, JavaScript files will not be accepted by the system.
4. On the toolbar, click Save.

### Digital Thumbprints

When running JavaScript data feeds, you can set the system to only allow digitally signed JavaScript files from trusted sources for security considerations.

For a certificate to be trusted, all the certificates in the chain including the Root CA Certificate and Intermediate CA certificates must be trusted on both the Web Server and Services Server machines.

## Archer Technologies LLC cert in the Trusted Root CA Store

Archer Technologies LLC certificate is not present on every machine's root by default.

1. On the JavaScript file, Right-click and select Properties.
    a. Click the Digital Signatures tab.
    b. From the Signature List window, select Archer Technologies LLC.
    c. Click the Details button.
    d. Click View Certificate.
    e. Click Install Certificate.
    f. Select Local Machine and click Next.
    g. Select Place all certificates in the following store and click Browse.
        i. Select Trusted Root Certification Authorities and click OK.
        ii. Click Next.
        iii. Click Finish.
2. Upon successful import, click OK.

## Obtaining a Certificate Thumbprint

1. On the Web Server and Services Server machines, open the Manage Computer Certificates program.
    a. Launch "certmgr" from the Start menu.
    b. Navigate to Certificates – Local Computer > Trusted Root Certification Authorities > Certificates.
2. Verify that the certificate is trusted.
    a. Double click the Archer Technologies LLC certificate.
    b. In the Certificate window, click the Certification Path tab.
    c. Ensure that the Certificate Status windows displays the following message: "This certificate is OK".

    **Note:** If the Certificate Status windows displays something different, follow the on-screen instructions.
3. Obtain the trusted certificate thumbprint.
    a. In the Certificate window, click the Details tab.
    b. Scroll to, and select, the Thumbprint field.
    c. The certificate's digital thumbprint appears in the window. Copy thumbprint.

**Note:** For information on adding digital thumbprints, see Step 4a of "Configure the JavaScript Transporter Settings" section of the document, regarding where thumbprint is relevant.

## Set Up the Archer 6.12 Qualys VM Knowledge Base Data Feed

We leverage the API (/api/2.0/fo/knowledge_base/vuln/?action=list) to obtain vulnerability data, such as the vulnerability description, threat and impact. The feed initiates the request to download the vulnerabilities from Qualys' Knowledge Base by targeting the Qualys platform where your account is located, along with the availability to pass additional API parameters.

**Important:** Before you upload a JavaScript file, configure JavaScript Transporter settings in the Archer Control Panel. For more information, see Configure the JavaScript Transporter Settings.

**Important:** With the exception of the optional parameters specified in this procedure, changes to the JavaScript Transporter configuration file can only be achieved in a hosted environment with a Professional Services engagement. For more information, contact your account representative.

**Important:** Retrieving all Knowledge Base content since the inception of the content cannot be achieved in a single data feed execution. Due to the amount of content requested in a single execution without the ability to truncate or paginate the data received from Qualys, clients are required to run multiple, manual executions of the Archer 6.12 Qualys VM Knowledge Base feed to achieve a base load of data. A combination of any of the following Qualys parameters could be leveraged to achieve the initial base load:

- last_modified_before / last_modified_after
- published_before / published_after
- id_min / id_max

**Important:** No truncation_limit is available for Knowledge Base data. Ultimately without the availability of a truncation_limit, we are unable to fully leverage our output writer and therefore not able to write portions of the data to file. We are storing the entirety of the data in memory which requires a temporary increase in the Max Memory Limit in the Archer Control Panel.

1. Go to the Manage Data Feeds page with the following steps:
   a. From the menu bar, click the  icon.
   b. Under Integration, click Data Feeds.
2. In the Manage Data Feeds section, click Import.
3. Locate and select the Archer 6.12 Qualys VM Knowledge Base.dfx5 file.
4. Click Open.
5. In the General Information section, in the Status field, select Active.
6. In the Additional Properties section, enable Optimize Calculations.
7. Click the Transport tab.
8. In the Transport Configuration section, complete the following:

a. Click Upload.

b. From the Upload JavaScript File dialog, click Add New.

c. Locate and select the Signed-QualysAPI_V1_0_8.js file, and click Open.

d. From the Upload JavaScript File dialog, click OK.

9. In the Custom Parameters section, enter key values.
   The following table describes the value to enter for each key in Custom Parameters.

| Key | Value | Description |
|---|---|---|
| dataSource | kb | |
| kbUrl | https://<Insert platform API Server>/api/2.0/fo/knowledge_base/vuln/?action=list&details=All&last_modified_after=<LastRunTime> | Note: For a complete list of supported parameters for this URL call and their explanations, see the Qualys API 2.0 Reference Guide (https://www.qualys.com/docs/qualys-api-vmpc-user-guide.pdf). For initial data loads, RSA recommends using parameters that chunk the data into consumable sizes to avoid memory constraint failures.<br><br>LastRunTime is a token captured in by Archer in the data feed execution.<br>Logic:<br>• Use LastRunTime token if valid date supplied, and if requested in the kbURL.<br>• If the LastRunTime token is not supplied but requested in the kbURL, default LastRunTime = 1970-01-10.<br>• A lastRunTimeOffset of -1 is added to the LastRunTime date in the form of days. |
| username | Requires valid value<br>Default = [empty] | |
| password | Requires valid value<br>Default = [empty] | |

**Important:** The keys and values are case-sensitive and cannot include extra spaces at the end of the strings.

**Note:** The listed values are in place by default. They can be configured to suit your environment.

10. The following additional parameters are valid options for the Custom Parameters section for the current JavaScript file.

| Key | Value | Description |
|---|---|---|
| requestsPerMin | Default = 60<br>[Configurable value] | A parameter to allow clients to govern the number of API requests made by Archer to the external integration.<br>Qualys Cloud Platform enforces limits on the API calls subscription users can make. The limits apply to the use of all APIs, except “session” API (session login/logout). |
| socketLimit | Default = 10<br>[Configurable value of 1-25] | Indicates the maximum number of open socket channels to an endpoint to be used for TCP connections. |
| maxRetry | Default = 1<br>[Configurable value of 0-2] | Indicates the amount of times a retry will occur where an "ECONNRESET" error is encountered. If a retry is unsuccessful and the maxRetry is exceeded, the data feed will fail. |
| proxy | Optional<br>Default = [empty] | |
| verifyCerts | Default = False<br>[Configurable value of True / False] | Validates the website address matches the address on the certificate, similar to browser level validation. |

11. For each key type, determine whether you want it to be Protected or Plain Text. Selecting Protected encrypts the key value for the specified key in the log.
12. Click the Source Definition tab.
    a. Click the Tokens sub-tab.
    b. Verify token values.
       The following table describes token values to verify.

| Token | Value |
|---|---|
| LastRunTime | (Populated by feed) |

**Note:** For more information about tokens, see "Data Feed Tokens" in the Archer Online Documentation.

13. Verify that key field values are not missing from the data feed setup window.
14. Click Save.

## Set Up the Archer 6.12 Qualys VM Hosts Data Feed

We leverage the API (/api/2.0/fo/asset/host/?action=list) to obtain a list of scanned hosts in the user's account. The feed initiates the request to download the hosts by targeting the Qualys platform where your account is located, along with the availability to pass additional API parameters.

**Important:** Before you upload a JavaScript file, configure JavaScript Transporter settings in the Archer Control Panel. For more information, see Configure the JavaScript Transporter Settings.

**Important:** With the exception of the optional parameters specified in this procedure, changes to the JavaScript Transporter configuration file can only be achieved in a hosted environment with a Professional Services engagement. For more information, contact your account representative.

**Important:** Archer implements with a unique key on DNS identification. However, we understand that environment configurations are unique across an organization's infrastructure, therefore the unique key to identify if a Device already exists inside Archer, is configurable to each client. And where clients have multiple scanners scanning the same set of devices or IP ranges, the unique key should be altered to a matching algorithm that identifies the device, regardless of the source.

1. Go to the Manage Data Feeds page with the following steps:
   a. From the menu bar, click the  icon.
   b. Under Integration, click Data Feeds.
2. In the Manage Data Feeds section, click Import.
3. Locate and select the Archer 6.12 Qualys VM Hosts.dfx5 file for the data feed.
4. Click Open.
5. In the General Information section, in the Status field, select Active.
6. In the Additional Properties section, enable Optimize Calculations.
7. Click the Transport tab.
8. In the Transport Configuration section, complete the following:

a. Click Upload.

b. From the Upload JavaScript File dialog, click Add New.

c. Locate and select the Signed-QualysAPI_V1_0_8.js file, and click Open.

d. From the Upload JavaScript File dialog, click OK.

9. In the Custom Parameters section, enter key values.
   The following table describes the value to enter for each key in Custom Parameters.

| Key | Value | Description |
|---|---|---|
| dataSource | hosts | |
| hostsUrl | https://<Insert platform API Server> /api/2.0/fo/asset/host/?action=list&details=All &show_tags=1&vm_scan_since=<LastRunTime> | Note: For a complete list of supported parameters for this URL call and their explanations, see the Qualys API 2.0 Reference Guide (https://www.qualys.com/docs/qualys-api-vmpc-user-guide.pdf).<br><br>LastRunTime is a token captured in by Archer in the data feed execution.<br>Logic:<br>• Use LastRunTime token if valid date supplied, and if requested in the hostsURL.<br>• If the LastRunTime token is not supplied but requested in the hostsURL, default LastRunTime = 1970-01-10, in specified batches.<br>• A lastRunTimeOffset of -1 is added to the LastRunTime date in the form of days. |
| username | Requires valid value<br><br>Default = [empty] | |
| password | Requires valid value<br><br>Default = [empty] | |

**Important:** The keys and values are case-sensitive, and cannot include extra spaces at the end of the strings.

**Note:** The listed values are in place by default. They can be configured to suit your environment.

10. (Optional) The following additional parameters are valid options for the Custom Parameters section for the current JavaScript file.

| Key | Value | Description |
|---|---|---|
| batchSize | Default = 500 (records at a time)<br>[Configurable] | Truncation_limit is a supported parameter to specify a maximum number of hosts records to process in a single call. JavaScript makes incremental calls to pull the next batch of data. If the requested list identifies more host records than the truncation limit, then the XML output includes the element and the URL for making another request for the next batch of host records. |
| requestsPerMin | Default = 60<br>[Configurable value] | A parameter to allow clients to govern the number of API requests made by Archer to the external integration.<br>Qualys Cloud Platform enforces limits on the API calls subscription users can make. The limits apply to the use of all APIs, except “session” API (session login/logout). |
| socketLimit | Default = 10<br>[Configurable value of 1-25] | Indicates the maximum number of open socket channels to an endpoint to be used for TCP connections. |
| maxRetry | Default = 1<br>[Configurable value of 0-2] | Indicates the amount of times a retry will occur where an "ECONNRESET" error is encountered. If a retry is unsuccessful and the maxRetry is exceeded, the data feed will fail. |
| proxy | Optional<br>Default = [empty] | |
| verifyCerts | Default = False<br>[Configurable value of True / False] | Validates the website address matches the address on the certificate, similar to browser level validation. |

11. For each key type, determine whether you want it to be Protected or Plain Text. Selecting Protected encrypts the key value for the specified key in the log.
12. Click the Source Definition tab.
    a. Click the Tokens sub-tab.
    b. Verify token values.
    The following table describes token values to verify.

| Token | Value |
|---|---|
| LastRunTime | (Populated by feed) |

    **Note:** For more information about tokens, see "Data Feed Tokens" in the Archer Online Documentation.
13. Verify that key field values are not missing from the data feed setup window.
14. Click Save.

## Set up the Archer 6.12 Qualys VM Hosts Extracted From Detections Data Feed

We leverage the API (/api/2.0/fo/asset/host/vm/detection/) to obtain a list of hosts with the hosts latest vulnerability data, based on the host based scan data available in the user's account. From this data, we specifically capture additional information regarding hosts identified as part of the vulnerability data extraction. The feed initiates the request to download the host detection data by targeting the Qualys platform where your account is located, along with the availability to pass additional API parameters.

**Important:** Before you upload a JavaScript file, configure JavaScript Transporter settings in the Archer Control Panel. For more information, see Configure the JavaScript Transporter Settings.

**Important:** With the exception of the optional parameters specified in this procedure, changes to the JavaScript Transporter configuration file can only be achieved in a hosted environment with a Professional Services engagement. For more information, contact your account representative.

**Important:** Archer implements with a unique key on DNS identification. However, we understand that environment configurations are unique across an organization's infrastructure, therefore the unique key to identify if a Device already exists inside Archer, is configurable to each client. And where clients have multiple scanners scanning the same set of devices or IP ranges, the unique key should be altered to a matching algorithm that identifies the device, regardless of the source.

1. Go to the Manage Data Feeds page with the following steps:
   a. From the menu bar, click the  icon.
   b. Under Integration, click Data Feeds.
2. In the Manage Data Feeds section, click Import.
3. Locate and select the Archer 6.12 Qualys VM Hosts Extracted From Detections.dfx5 file for the data feed.
4. Click Open.
5. In the General Information section, in the Status field, select Active.
6. In the Additional Properties section, enable Optimize Calculations.
7. Click the Transport tab.
8. In the Transport Configuration section, complete the following:
   a. Click Upload.
   b. From the Upload JavaScript File dialog, click Add New.
   c. Locate and select the Signed-QualysAPI_V1_0_8.js file, and click Open.
   d. From the Upload JavaScript File dialog, click OK.
9. In the Custom Parameters section, enter key values.
   The following table describes the value to enter for each key in Custom Parameters.

| Key | Value | Description |
|---|---|---|
| dataSource | hostDetections | |
| detectionUrl | https://<platform API server>/api/2.0/fo/asset/host/vm/detection/?action=list&status=Active,New,Fixed,Re-Opened&vm_scan_since=<LastRunTime> | Note: For a complete list of supported parameters for this URL call and their explanations, see the Qualys API 2.0 Reference Guide https://www.qualys.com/docs/qualys-api-vmpc-user-guide.pdf).<br><br>If the status parameter is not passed to the API, by default, the output only contains detections with New, Active, or Re-Opened.<br><br>LastRunTime is a token captured in by Archer in the data feed execution. Logic: |

| | | |
|---|---|---|
| | | • Use LastRunTime token if valid date supplied, and if requested in the detectionURL.<br>• If the LastRunTime token is not supplied but requested in the detectionURL, default LastRunTime = 1970-01-10, in specified batches.<br>• A lastRunTimeOffset of -1 is added to the LastRunTime date in the form of days. |
| username | Requires valid value<br>Default = [empty] | |
| password | Requires valid value<br>Default = [empty] | |

**Important:** The keys and values are case-sensitive, and cannot include extra spaces at the end of the strings.

**Note:** The listed values are in place by default. They can be configured to suit your environment.

10. (Optional) The following additional parameters are valid options for the Custom Parameters section for the current JavaScript file.

| Key | Value | Description |
|---|---|---|
| batchSize | Default = 500 (records at a time)<br>[Configurable] | Truncation_limit is a supported parameter to specify a maximum number of hosts records to process in a single call. JavaScript makes incremental calls to pull the next batch of data. If the requested list identifies more host records than the truncation limit, then the XML output includes the element and the URL for making another request for the next batch of host records. |
| requestsPerMin | Default = 60<br>[Configurable value] | A parameter to allow clients to govern the number of API requests made by Archer to the external integration.<br>Qualys Cloud Platform enforces limits on the API calls subscription users can make. The |

| | | |
|---|---|---|
| | | limits apply to the use of all APIs, except “session” API (session login/logout). |
| socketLimit | Default = 10<br>[Configurable value of 1-25] | Indicates the maximum number of open socket channels to an endpoint to be used for TCP connections. |
| maxRetry | Default = 1<br>[Configurable value of 0-2] | Indicates the amount of times a retry will occur where an "ECONNRESET" error is encountered. If a retry is unsuccessful and the maxRetry is exceeded, the data feed will fail. |
| proxy | Optional<br>Default = [empty] | |
| verifyCerts | Default = False<br>[Configurable value of True / False] | Validates the website address matches the address on the certificate, similar to browser level validation. |

11. For each key type, determine whether you want it to be Protected or Plain Text. Selecting Protected encrypts the key value for the specified key in the log.
12. Click the Source Definition tab.
    a. Click the Tokens sub-tab.
    b. Verify token values.
    The following table describes token values to verify.

| Token | Value |
|---|---|
| LastRunTime | (Populated by feed) |

    **Note:** For more information about tokens, see "Data Feed Tokens" in the Archer Online Documentation.
13. Verify that key field values are not missing from the data feed setup window.
14. Click Save.

## Set Up the Archer 6.12 Qualys VM Detections Data Feed

We leverage the API (/api/2.0/fo/asset/host/vm/detection/) which provides a list of hosts with each hosts latest vulnerability data, based on the host-based scan data available in the user’s account. Vulnerability detection data includes the latest complete vulnerability status for the hosts (New, Active, Fixed, Re-Opened) and the history information. The feed initiates the request to download the host detection data by targeting the Qualys platform where your account is located, along with the availability to pass additional API parameters.

**Important:** Before you upload a JavaScript file, configure JavaScript Transporter settings in the Archer Control Panel. For more information, see Configure the JavaScript Transporter Settings.

**Important:** With the exception of the optional parameters specified in this procedure, changes to the JavaScript Transporter configuration file can only be achieved in a hosted environment with a Professional Services engagement. For more information, contact your account representative.

**Important:** For detections, Archer implements with a unique key concept to associate the detection to a host and a vulnerability definition. However, we understand that environment configurations are unique across an organization's infrastructure, therefore the unique keys are configurable to each client, such as determining if a device already exists in your Archer environment. And where clients have multiple scanners scanning the same set of devices or IP ranges, the unique key should be altered to a matching algorithm that identifies the device, regardless of the source. Unique key default values are as follows:

| Identification of an object | Logic (configurable) |
|---|---|
| Detection | If DNS exists, concatenate DNS + QID + Port + Protocol.<br>If DNS does not exist, concatenate the Host ID + QID + Port + Protocol + First Found. |
| Device (Link Only) | If a Qualys Host ID exists, create a match from the detection to the device. Otherwise, use the DNS as the match on an active Device.<br>**Assumption:** Qualys Host ID is only captured on a device record after initial host ingestion. When defining the host infrastructure, we do not assume Qualys Host ID is a unique identifier by itself. |
| Vulnerability Library definition (Link Only) | If a QID exists, create a match from the detection to the vulnerability definition. |

1. Go to the Manage Data Feeds page with the following steps:
   a. From the menu bar, click the  icon.
   b. Under Integration, click Data Feeds.
2. In the Manage Data Feeds section, click Import.
3. Locate and select the Archer 6.12 Qualys VM Detections.dfx5 file for the data feed.
4. Click Open.
5. In the General Information section, in the Status field, select Active.
6. In the Additional Properties section, enable Optimize Calculations.
7. Click the Transport tab.

8. In the Transport Configuration section, complete the following:
   e. Click Upload.
   f. From the Upload JavaScript File dialog, click Add New.
   g. Locate and select the Signed-QualysAPI_V1_0_8.js file, and click Open.
   h. From the Upload JavaScript File dialog, click OK.
9. In the Custom Parameters section, enter key values.
   The following table describes the value to enter for each key in Custom Parameters.

| Key | Value | Description |
|---|---|---|
| dataSource | detections | |
| detectionUrl | https://<platform API server>/api/2.0/fo/asset/host/vm/detection/?action=list&status=Active,New,Fixed,Re-Opened&vm_scan_since=<LastRunTime> | Note: For a complete list of supported parameters for this URL call and their explanations, see the Qualys API 2.0 Reference Guide https://www.qualys.com/docs/qualys-api-vmpc-user-guide.pdf).<br><br>If the status parameter is not passed to the API, by default, the output only contains detections with New, Active, or Re-Opened.<br><br>LastRunTime is a token captured in by Archer in the data feed execution.<br>Logic:<br>• Use LastRunTime token if valid date supplied, and if requested in the detectionURL.<br>• If the LastRunTime token is not supplied but requested in the detectionURL, default LastRunTime = 1970-01-10, in specified batches.<br>• A lastRunTimeOffset of -1 is added to the LastRunTime date in the form of days. |
| username | Requires valid value<br><br>Default = [empty] | |

| | | |
|---|---|---|
| password | Requires valid value<br>Default = [empty] | |

**Important:** The keys and values are case-sensitive, and cannot include extra spaces at the end of the strings.

**Note:** The listed values are in place by default. They can be configured to suit your environment.

10. (Optional) The following additional parameters are valid options for the Custom Parameters section for the current JavaScript file.

| Key | Value | Description |
|---|---|---|
| batchSize | Default = 500 (records at a time)<br>[Configurable] | Truncation_limit is a supported parameter to specify a maximum number of hosts records to process in a single call. JavaScript makes incremental calls to pull the next batch of data. If the requested list identifies more host records than the truncation limit, then the XML output includes the element and the URL for making another request for the next batch of host records. |
| requestsPerMin | Default = 60<br>[Configurable value] | A parameter to allow clients to govern the number of API requests made by Archer to the external integration.<br>Qualys Cloud Platform enforces limits on the API calls subscription users can make. The limits apply to the use of all APIs, except “session” API (session login/logout). |
| socketLimit | Default = 10<br>[Configurable value of 1-25] | Indicates the maximum number of open socket channels to an endpoint to be used for TCP connections. |
| maxRetry | Default = 1<br>[Configurable value of 0-2] | Indicates the amount of times a retry will occur where an "ECONNRESET" error is encountered. If a retry is unsuccessful and the maxRetry is exceeded, the data feed will fail. |
| proxy | Optional<br>Default = [empty] | |

| | | |
|---|---|---|
| verifyCerts | Default = False<br>[Configurable value of True / False] | Validates the website address matches the address on the certificate, similar to browser level validation. |

11. For each key type, determine whether you want it to be Protected or Plain Text. Selecting Protected encrypts the key value for the specified key in the log.
12. Click the Source Definition tab.
    c. Click the Tokens sub-tab.
    d. Verify token values.
    The following table describes token values to verify.

| Token | Value |
|---|---|
| LastRunTime | (Populated by feed) |
| CrossReferencesMode | LinkOnly |
| RelatedReferencesMode | LinkOnly |

    **Note:** For more information about tokens, see "Data Feed Tokens" in the Archer Online Documentation.
13. Verify that key field values are not missing from the data feed setup window.
14. Click Save.

# Chapter 3: Using the Qualys Vulnerability Management Data Feeds

## Scheduling Data Feeds

**Important:** A data feed must be active and valid to successfully run.

As you schedule your data feed, the Data Feed Manager validates the information. If any information is invalid, an error message displays. You can save the data feed and correct the errors later, but the data feed does not process until you make corrections.

**Note:** All IT Security Vulnerabilities Program data feeds are set to run daily by default.

1. From the menu bar, click the icon.
2. Go to the Schedule tab of the data feed that you want to modify.

    a. From the menu bar, click the icon.

    b. Under Integration, click Data Feeds.

    c. Select the data feed.

    d. Click the Schedule tab.

3. Go to the Recurrences section and complete frequency, start and stop times, and time zone.
   The following table describes the fields in the Recurrences section.

| Field | Description |
|---|---|
| Frequency | Specifies the interval in which the data feed runs, for example, Minutely, Hourly, Daily, Weekly, Monthly, or Reference.<br>• Minutely. Runs the data feed by the interval set.<br>For example, if you specify 45 in the Every list, the data feed executes every 45 minutes.<br>• Hourly. Runs the data feed by the interval set, for example, every hour (1), every other hour (2) and so forth.<br>• Daily. Runs the data feed by the interval set, for example, every day (1), every other day (2) and, so forth.<br>• Weekly. Runs the data feed based on a specified day of the week, for example, every Monday of the first week (1), every other Monday (2), and so forth.<br>• Monthly. Runs the data feed based on a specified week of the month, for example, 1st, 2nd, 3rd, 4th, or Last.<br>• Recurrence. Runs a specified data feed as runs before the current one. This option indicates to the Data Feed Service that this data feed starts as soon as the referenced data feed completes successfully. For example, you can select to have a Threats data feed run immediately after your Assets data feed finishes. From the Reference Feed list, select after which existing data feed the current data feed starts.<br>A reference data feed will not run when immediately running a data feed. The Run Data Feed Now option only runs the current data feed. |
| Every | Specifies the interval of the frequency in which the data feed runs. |
| Start Time | Specifies the time the data feed starts running. |
| Start Date | Specifies the date on which the data feed schedule begins. |
| Time Zone | Specifies the time zone in of the server that runs the data feed. |

4. (Optional) To override the data feed schedule and immediately run your data feed, in the Run Data Feed Now section, click Start.
5. Click Save.

# Appendix A: Certification Environment

Date Tested: January 2020

| Product Name | Version Information | Operating System |
|---|---|---|
| Archer | 6.12 | Virtual Appliance |
| Qualys Vulnerability Management (VM) | NA | NA |