Nexpose

API 1.1 and 1.2 Guide

Product version: 6.0

Contents

Revision history

Revision date	Description
May 16, 2012	Created this guide, which consolidates two separate guides for API v1.1 and Extended API v1.2. As of this release date, the preceding separate guides are deprecated. Made formatting changes for improved readability.
August 8, 2012	Added information on vulnerability filtering.
April 17, 2013	Corrected formatting errors and typos.
May 24, 2013	Added the ManagePolicies element to the RoleCreate, RoleCreate RoleDetail RoleListing and RoleDelete APIs. The user ID element has been added to the RoleUpdateRequest example.
July 17, 2013	Added details to AdhocReportConfig API and corrected formatting errors.
November 13, 2013	Corrected formatting issues.
March 26, 2014	Added information about asset tagging support in site, asset group, report, and role APIs.
July 30, 2014	Updated document look and feel.
October 10, 2014	Made minor formatting changes.
November 12, 2014	Nexpose 5.11: Updated product version for guide.
November 19, 2014	Added note on proper use of *host* and *range* elements in SiteSave API and Site DTD.
February 4, 2015	Nexpose 5.12: Added information about new attributes to support expanded scan scheduling.
March 19, 2015	Provided examples for most API 1.1 calls. Replaced graphical XML samples with text-based samples.
April 8, 2015	Nexpose 5.13: Added information about scan scheduling enhancements.
May 27, 2015	Nexpose 5.14: Added information about scan blackouts. See *SiteDevicesScan* on page 44.
June 24, 2015	Nexpose 5.15: Updated product version.
July 29, 2015	Nexpose 5.16: Updated product version.
August 26, 2015	Nexpose 5.17: Updated product version.
October 8, 2015	Nexpose 6.0: Updated product version.

About this guide

This guide helps you to use the NexposeAPI to integrate the application's functionality with other tools in your environment or to automate some of the functionality.

This introductory section covers the application's architecture and functionality to help you understand the different operations that you can perform with the API. It also provides an overview of the API itself, addressing the following subjects:

- *Architecture and functionality* on page 14
- *Using the API* on page 21

Document conventions

Words in bold are names of hypertext links and controls.

Words in italics are document titles, chapter titles, and names of Web interface pages.

Steps of procedures are indented and are numbered.

Items in `Courier font` are commands, command examples, and directory paths.

Items in **`bold Courier font`** are commands you enter.

Variables in command examples are enclosed in box brackets.
Example: `[installer_file_name]`

Options in commands are separated by pipes. Example:

```
$ /etc/init.d/[daemon_name] start|stop|restart
```

Keyboard commands are bold and are enclosed in arrow brackets.Example:
Press and hold **<Ctrl + Delete>**

Note: NOTES contain information that enhances a description or a procedure and provides additional details that only apply in certain cases.

Tip: TIPS provide hints, best practices, or techniques for completing a task.

Warning: WARNINGS provide information about how to avoid potential data loss or damage or a loss of system integrity.

Throughout this document, Nexpose is referred to as *the application*.

Other documents and Help

Click the **Help** link on any page of the Security Console Web interface to find information quickly. You can download any of the following documents from the *Support* page in Help.

Administrator’s guide

The administrator’s guide helps you to ensure that Nexpose works effectively and consistently in support of your organization’s security objectives. It provides instruction for doing key administrative tasks:

- configuring host systems for maximum performance
- database tuning
- planning a deployment, including determining how to distribute Scan Engines
- capacity planning
- managing user accounts, roles, and permissions
- administering the Security Console and Scan Engines
- working with the database, backups, and restores
- using the command console
- maintenance and troubleshooting

User’s guide

The user’s guide helps you to gather and distribute information about your network assets and vulnerabilities using the application. It covers the following activities:

- logging onto the Security Console and familiarizing yourself with the interface
- managing dynamic discovery
- setting up sites and scans
- pairing Scan Engines with the Security Console
- running scans manually
- viewing asset and vulnerability data
- creating remediation tickets
- using preset and custom report templates
- using report formats
- reading and interpreting report data
- configuring scan templates
- configuring other settings that affect scans and report

For technical support

- Send an e-mail to support@rapid7.com (Enterprise and Express Editions only).
- Click the **Support** link on the Security Console Web interface.
- Go to community.rapid7.com.

Architecture and functionality

Understanding the Nexpose architecture will help you make to make the best use of the functions in the API.

Nexpose is a unified vulnerability solution that scans networks to identify the devices running on them and to test these devices for vulnerabilities and policy compliance. It analyzes the scan data and processes it for reports. You can use these reports to help you assess your network security at various levels of detail and remediate any vulnerabilities quickly.

Vulnerability checks identify security weaknesses in all layers of a network computing environment, including operating systems, databases, applications, and files. Checks can identify areas in your infrastructure that may be at risk for an attack and verify patch updates and security compliance measures.

Nexpose consists of two main components: Scan Engines and a Security Console. One or more Scan Engines (NSEs) search networks to discover devices and the processes running on them, such as operating systems, programs, and databases. The Scan Engines then test discovered assets for vulnerabilities, patches, and other security-related factors. A Security Console collects, analyzes, and stores the scan data, and it generates reports and vulnerability remediation procedures. Additionally, the console controls the Scan Engines and provides a Web-accessible user interface for managing all Nexpose functions.

An organization can deploy Scan Engines within its network or outside its firewall. It also can use Hosted Scanning Engines that are located in Rapid7 data centers.

The simplest configuration consists of a single Scan Engine and the Security Console on one host.

Sites

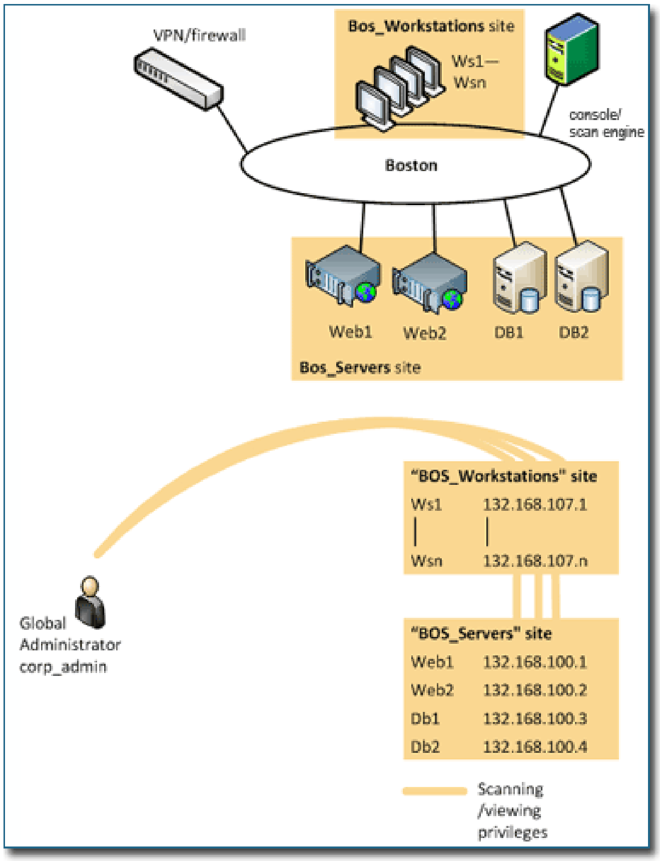
A site is a logical group of assets assembled for a scan by a specific, dedicated Scan Engine. The grouping principle may be something meaningful to you, such as a common geographic location or a range of IP addresses. Or, you may organize a site for a specific type of scan.

For example, a company sets up Nexpose in a Boston location. The Global Administrator, whose logon name is corp_admin wants to scan two sets of assets at different times and with different scanning parameters. So, he sets up two sites:

BOS_Servers includes Web and database servers.

BOS_Workstations includes the workstations.

The Global Administrator is in charge of scanning both sites.



The initial implementation with two sites

For more information about setting up sites an asset groups, see the user's guide, which you can download from the *Support* page of Help.

Distributed Scan Engines

Distributing multiple Scan Engines promotes fault tolerance and improves scanning performance while conserving bandwidth. It is a best practice to deploy at least one Scan Engine at each physical location, where it can scan assets locally. This frees up bandwidth for more remote connections. Also, installing Scan Engines locally, behind firewalls, removes the need for firewall rule exceptions.

Agentless operation

Nexpose scans exclusively over the network, using common Windows and UNIX network protocols to gain access to systems. It does not require agent software to be installed on the assets targeted for scanning. Agentless architecture lowers the total cost of ownership (TCO) and avoids potential security and stability issues associated with agents.

Asset groups

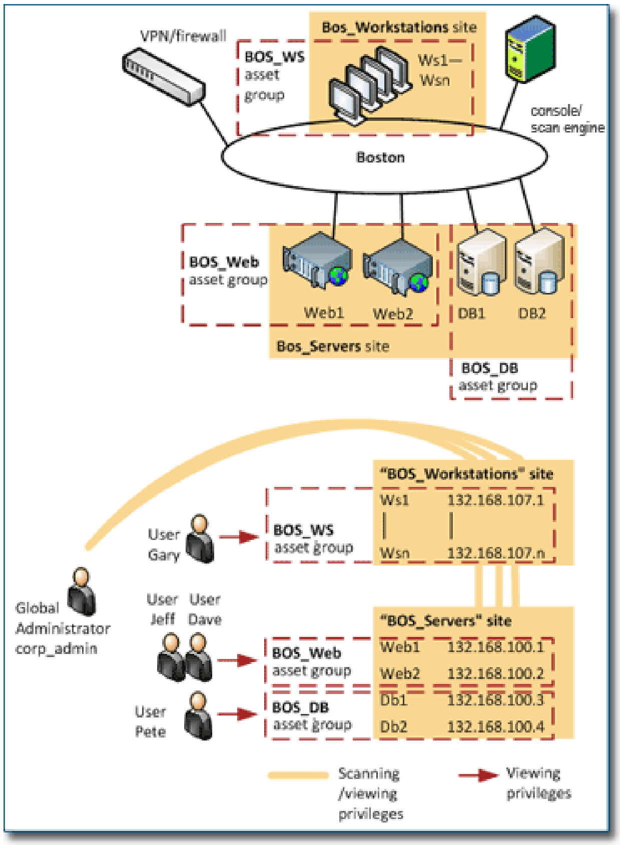
An asset group is a collection of assets, but unlike a site, it is not defined for scanning. An asset group typically is assigned to a nonadministrative user, who views scan reports about that group in order to perform any necessary remediation.

Using the example of the Boston company in the Sites section, the Global Administrator, who has control of the entire deployment, wants to delegate teams for remediating vulnerabilities on the Web servers, database servers, and workstations. So, he creates three asset groups.

BOS_Web includes the two Web servers. Two nonadministrative users, Jeff and Dave, who handle Web server maintenance and troubleshooting at the Boston location, have access to this group.

BOS_DB includes the two database servers. A nonadministrative user, Pete, who is a database manager, has access to this group.

BOS_WS includes all workstations. A nonadministrative user, Gary, who troubleshoots the workstations, has access to this group.



The implementation with three asset groups

For more information about setting up sites an asset groups, see the user's guide, which you can download from the *Support* page of Help.

Security Console

Each Scan Engine is controlled by a Security Console, which can be located anywhere on the network. The console communicates with the engines via encrypted SSL sessions over a defined Transmission Control Protocol (TCP) port. Engines talk only to the console, they do not talk to other engines.

In order to manage scans and view results, users log on to the Security Console interface using a Web browser over HTTPS (secure encrypted HTTP). The only software required for using the console is a Web browser.

User access control

The Security Console requires users to log on with Nexpose credentials. This authentication occurs over HTTPS, so it is entirely encrypted. The authentication database is stored in an encrypted format locally on the console server. Passwords are not stored or transmitted in plaintext.

Upon logging on, a user sees only information to which he or she has been granted access by a Global Administrator. A given user can have access to one or more entire sites, one or more assets within a site, or one or more asset groups. The Global Administrator can control access to sensitive security information by granting fine-grained, “need-to-know” user permissions.

Scanning

A scan includes one or more of the following phases:

Phase	What the Scan Engine does in this phase
Device discovery	Locates active devices on the network.
Service discovery	Determines the types of services running on devices found to be active on the network.
Access discovery	Scans active devices to determine configurations, including operating system, hardware, service and installed software.
Vulnerability assessment	Scans active devices for known vulnerabilities.

Device (asset) discovery

In device discovery, the first phase of a scan, the Scan Engine maps out the network and locates the active assets.

The Scan Engine can discover devices using ICMP ECHO requests, or by sending TCP packets to one or more ports in what is effectively a mini port scan. Systems responding to these packets are marked as active and will be included in subsequent scan phases.

You may wish to disable device discovery when scanning assets in a DMZ or any other area with strict protection, such as a firewall that drops blocked packets. When you disable device discovery, the application uses port scan results found in the discovery phase to determine which hosts are active. If any ports are found to be open on an asset, the application will mark that asset “alive.”

Service Discovery

In the service discovery phase the Scan Engine maps out the network services running on the active assets.

You can tune service discovery to enable or disable TCP and User Datagram Protocol (UDP) port scans. You can specify which ports to scan, including default port lists or all possible ports (1-65,535). Additionally, you can change the method of TCP port scanning to use full connections, half-open (SYN) scans, or other variations.

Once the application determines a port to be open, it performs a protocol handshake on that port to verify the type of service running on it. Doing so allows the application to determine if a service is running, even if it is not on the expected port. For example, an HTTP server may be running on port 1234, as opposed to the standard HTTP port 80.

Asset inventory

Once the application knows the network layout with active assets and services, it can perform an asset inventory to determine the configuration of many system components:

- operating system type and version (for example, Microsoft Windows XP SP2)
- system configuration
- hardware type (for example, Cisco 2621)
- service type and version (for example, Apache 2.0.54)
- service configuration
- installed software (for example, Mozilla Firefox 1.0.5)
- software configuration

Vulnerability assessment

In the vulnerability assessment phase, the application scans active devices for known vulnerabilities.

Vulnerability checks cover known vulnerabilities in a broad range of products. The Web spidering feature can discover vulnerabilities caused by Web application developers. The spider can search a Web site for common programming errors and backup copies of scripts that may divulge sensitive information.

You can specify certain vulnerabilities or vulnerability types for discovery. The application includes default scan templates with predefined vulnerability check settings. You also can custom-define your own vulnerability checks.

Reporting

You can create reports based on scan data in PDF, HTML, XML, and plain text formats. The application also can export data to most database systems or to structured file formats, such as XML, QualysXML, and CSV.

Configuring a report involves several steps:

- selecting a report template
- specifying sites, asset groups, or assets to include in the report
- selecting delivery options, such as e-mail to all authorized users
- scheduling when to generate the report

You can use built-in report templates, which include predefined settings for level of technical data, specific information for certain compliance audits, export format, and other features. See the user's guide for sample reports and export formats. You also can create custom report templates.

Report sections

Each report template consists of sections that include specific types of information. When you create a custom report, you can choose from a list of sections to generate information exactly according to your needs. Examples of report sections include *Discovered System Information*, *Discovered Vulnerabilities*, *Risk Assessment*, and *Remediation Plan*.

See the user's guide for a complete list of report sections, including descriptions and visual samples.

Management and diagnostic functions

You can use the logging and system reporting functions to monitor internal activity and troubleshoot problems. Additionally, you can configure the application to restart and to obtain required software updates when necessary.

Using the API

The API provides programming access to a subset of the full feature set that is available in the Security Console Web interface. Your range of API access depends on the user privileges assigned to your logon credentials.

You may access the API using encrypted Hypertext Transfer Protocol over a Secure Socket Layer connection. The API supports HTTP 1.0 and 1.1 syntax. For data exchange, you may use the Extensible Markup Language (XML) as defined by the W3C (http://www.w3.org/TR/REC-xml).

Working with two API versions

There are currently two versions of APIs: API v1.1 and Extended API v1.2. They are different in two major ways.

Each version provides a unique set of functions. However, many functions in each of the APIs support common categories of operation, such as vulnerability management and reporting. See the list of functions

Each version is validated with a different method. API v1.1 is validated with DTDs, and Extended API v1.2 is validated with XML schemas.

API v1.1 functions

The API 1.1 is available in Nexpose 4.0 or later and is broken down into the following functional categories:

- *Session Management* on page 30
- *Site management* on page 32
- *Scan management* on page 43
- *Device (asset) management* on page 64
- *Asset group management* on page 65
- *Vulnerability management* on page 70; additional vulnerability management is covered in the Extended API v1.2
- *Vulnerability exception management* on page 172
- *User management functions* on page 81
- *General management and diagnostic functions* on page 87

Note: The API does not support scan template creation.

The requests made to the API 1.1 are validated with DTDs documented in Section I of this guide.

Extended API v1.2 functions

The Extended API 1.2 provides extended functionality available in Nexpose 4.0 or later and. It is broken down into the following functional categories:

- *Asset group management* on page 65
- *Scan engine management* on page 132
- *Ticket management* on page 148
- *Vulnerability management* on page 164
- *Vulnerability exception management* on page 172
- *Multi-Tenant users* on page 188
- *Silo Profiles* on page 207
- *Silo Management* on page 232
- *Role Management* on page 261
- *Scan Engine Pool Management* on page 313

API 1.1 Session Management is required for all functions, including those for API 1.2.

The requests made to the API 1.2 are validated with the XML schemas provided in the package Extended_API_XMLSchemas_v1.2.zip. You can download all documentation and schemas from the *Support* page in Help.

Sending API requests

You access the API through a URL of the form:

```
https://<host>:<port>/api/api-version/xml
```

The client connecting to Nexpose must use HTTPS to engage the console. The client must then log on with valid credentials. Upon successful logon, Nexpose returns a session ID to the application. Use the session ID for subsequent requests rather than resubmitting the credentials. The following is a typical login sequence:

1. Open an HTTPS connection to the Web console, usually on port 3780.
2. Construct a LoginRequest XML request containing valid credentials.
3. Verify that the Content-type HTTP header is set to “text/xml”.
4. For API 1.1 operations, send the XML request to https://<host>:<port>/api/1.1/xml using HTTP POST Method.
   For API 1.2 operations, send the XML request to https://<host>:<port>/api/1.2/xml using HTTP POST Method.
5. Parse the returned LoginResponse.
6. If the success attribute is set to 1, extract the session-id attribute for use in subsequent requests.
7. If the success attribute is set to 0, extract the Failure information and report it.

The session-id is subject to timeout from inactivity regardless of how much work Nexpose is performing. You can specify the timeout period on the *Security Console Configuration* page of the Web interface. See the administrator's guide for details.

All subsequent requests must include the appropriate session-id in their respective request XML structure. This inclusion will allow the API program to perform actions on behalf of the credentials specified.

If the API request results in a failure, the response XML document will have the success attribute set to 0 and the Failure element will be returned. The format of the Failure element is as follows:

```
<!-- The failure description, consisting of one or more message and/or
exception -->
<!ELEMENT Failure ((message|Exception)*)>
<!-- the message describing the failure -->
<!ELEMENT message (#PCDATA)>
    <!-- the source of the message, such as the module that caused the
    error -->
    <!ATTLIST message source CDATA #IMPLIED>
    <!-- the source specific message code -->
    <!ATTLIST message code CDATA #IMPLIED>
<!-- the exception causing the failure -->
<!ELEMENT Exception (message, stacktrace?)>
    <!-- the name of the Exception class (for Java or C++ exceptions) -
    ->
    <!ATTLIST Exception name CDATA #IMPLIED>
<!ELEMENT stacktrace (#PCDATA)>
```

As the success and failure information is stored within the returned XML document, all requests processed by the API will return HTTP status code 200. Any other status code implies a problem on the Nexposeserver. Common causes of server errors include an older version of the application that do not have API support built-in, out of memory conditions, etc.

If you use a command that is not listed in the in administrator's guide, the application will return the XMLResponse.

For a sample implementation of some of the API functionality, see *Code samples* on page 323.

Sending an Extended API v1.2 request that includes a non-existent command or a request that in a failure, will cause a failure element to be returned. See *Error responses* on page 334 for more information.

As the success and failure information is stored within the returned XML document, all requests processed by the API will return HTTP status code 200. Any other status code implies a problem on the Nexpose server. Common causes of server errors include an older version of the application that has API support built-in, out of memory conditions, etc.

If you use a command that is not listed in the in administrator’s guide, the application will return the XMLResponse.

API requirements

You can interact with the API by writing an application that sends and receives XML messages to and from the Security Console. There are no restrictions on which language you use to write this program, except that the language needs libraries or routines to send POST requests over HTTPS. The API does not support requests over HTTP.

It is helpful if your client language has a library or routines to support XML processing, since all messages sent to and received from Nexpose are XML messages.

API applications

The API can be used for various applications, not limited to the following:

API data interface

Since the API responses are XML, it is straightforward to write scripts that extract relevant data from the responses, rather than exporting the data from the Web interface. The extracted data can then be processed according to the needs of your organization. The API simplifies the process of integrating data with other applications such as databases or third-party security tools.

API custom interfaces

Most users will only use a subset of functions on a regular basis. Since all major functionality is available through the API, you can write your own custom interface that exposes only necessary functions to the user—either a graphic user interface, or a text-only interface.

Control of scanning

The API is a convenient way to configure and run scans. You can run scans as needed without using the Web interface, and write scripts to run scans at scheduled intervals.

The structure of the API v1.1 section

This section is divided into categories of operations accessed by the API v1.1, such as session management or site management. For each category, all individual APIs that make up the API v1.1 are listed with descriptions and XML examples.

API 1.1 requests are validated with DTDs, which are listed at the end of this section.

Lists of individual APIs that make up API v1.1

Session management requests

Command	Description
Login	Log on to the Security Console and establish a session.
Logout	Log off from the Security Console, freeing the session and all related resources.

Site management requests

Command	Description
SiteListing	Provide a list of all sites the user is authorized to view or manage.
SiteConfig	Provide the configuration of the site, including its associated assets.
SiteSave	Save changes to a new or existing site.
SiteDelete	Delete the specified site and all associated scan data.
SiteScan	Scan the specified site.
SiteScanHistory	Provide a list of all previous scans of the site.
SiteDeviceListing	Provide a list of all of the assets in a site. If no site-id is specified, then this will return all of the assets for the Scan Engine, grouped by site-id.
SiteDevicesScan	Scan a specified subset of site assets.

Asset management requests

Command	Description
DeviceDelete	Delete the specified asset.

Asset group management requests

Command	Description
AssetGroupListing	Provide a list of all asset groups the user is authorized to view or manage.
AssetGroupConfig	Provide the configuration of the asset group, including its associated devices.
AssetGroupSave	Save changes to a new or existing asset group.
AssetGroupDelete	Delete the specified asset group and all associated scan data.

Scan requests

The API does not support scan template creation.

Command	Description
EngineListing	Provide a list of all scanning engines managed by the Security Console.
EngineActivity	Provide a list of current scan activities for a specific Scan Engine.
ScanActivity	Provide a list of current scan activities across all Scan Engines managed by the Security Console.
ScanPause	Pause a running scan.
ScanResume	Resume a running scan.
ScanStop	Stop a running scan.
ScanStatus	Check the current status of a scan.
ScanStatistics	Get scan statistics, including node and vulnerability breakdowns.

Vulnerability assessment requests

Command	Description
VulnerabiltyListing	Provide a list of vulnerabilities that can be checked
VulnerabilityDetails	Provide the full details of a vulnerability, including its description, cross-references, and solution.

Reporting requests

Command	Description
ReportTemplateListing	Provide a list of all report templates the user can access on the Security Console.
ReportTemplateConfig	Retrieve the configuration for a report template.
ReportTemplateSave	Save the configuration for a report template.
ReportListing	Provide a listing of all report definitions the user can access on the Security Console.
ReportHistory	Provide a history of all reports generated with the specified report definition.
ReportConfig	Retrieve the configuration for a report definition.
ReportSave	Save the configuration for a report definition.

Command	Description
ReportGenerate	Generate a new report using the specified report definition.
ReportDelete	Delete a previously generated report or report definition.
ReportAdhocGenerate	Generate a report once using a simple configuration, and send it back in a multipart mime response.

User management requests

Command	Description
UserListing	Provide a list of user accounts and information about those accounts.
UserAuthenticator	Provide a list of user authentication sources.
UserConfig	List information about a given user account.
UserSave	Create a new user account, or update the settings for an existing account.
UserDelete	Delete a user account.Note that you cannot delete a user account that is associated with reports or tickets.

General management and diagnostic requests

Command	Description
ConsoleCommand	Execute a Security Console command that is supplied as text via an API parameter. Commands are documented in the administrator's guide. If you use a command that is not listed the application will return the XMLResponse.
SystemInformation	Obtain system data, such as total RAM, free RAM, total disk space, free disk space, CPU speed, number of CPU cores, and other vital information.
StartUpdate	Induce the application to retrieve required updates and restart if necessary.
Restart	Induce the application to restart.
SendLog	Output diagnostic information into log files, zip the files, and encrypt the archive with a PGP public key that is provided as a parameter for the API call. Then, either e-mail this archive to an address that is specified as an API parameter, or upload the archive using HTTP or HTTPS to a URL that is specified as an API parameter.If you do not specify a key, the SendLogRequest uses a default key.

Session Management

Login

Log on to the Security Console and establish a session.

LoginRequest DTD

If no silo-id is specified, the user's silo will be set to the user's default silo, if it exists. If the silo-id is not specified, and no silos are defined for the user, then the login fails, unless the user is a super-user.

```
<!DOCTYPE LoginRequest [
<!ELEMENT LoginRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST LoginRequest sync-id CDATA #IMPLIED>
    <!-- the user id to login with -->
    <!ATTLIST LoginRequest user-id CDATA #REQUIRED>
    <!-- the password to login with -->
    <!ATTLIST LoginRequest password CDATA #REQUIRED>
    <!-- the silo to log into -->
    <!ATTLIST LoginRequest silo-id CDATA #IMPLIED>
]>
```

LoginRequest sample

```
<?xml version="1.0" encoding="UTF-8"?>
<LoginRequest user-id="nxadmin" password="nxadmin" />
```

LoginResponse

```
<!DOCTYPE LoginResponse [
<!ELEMENT LoginResponse (Failure?)>
    <!-- the session id to be used with all subsequent requests -->
    <!ATTLIST LoginResponse session-id CDATA #REQUIRED>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST LoginResponse success (0|1) #REQUIRED>
]>
```

LoginResponse sample

```
<LoginResponse success="1" session-
id="0DA2FE1D69917350BC15B43A60A2F217D77CF522"/>
```

Logout

Log off from the Security Console, freeing the session and all related resources.

LogoutRequest DTD

```
<!DOCTYPE LogoutRequest [
<!ELEMENT LogoutRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST LogoutRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST LogoutRequest session-id CDATA #REQUIRED>
]>
```

LogoutRequest sample

```
<?xml version="1.0" encoding="UTF-8"?>
<LogoutRequest session-id="${Login#Response#//LoginResponse[1]
/@session-id}" />
```

LogoutResponse DTD

```
<!DOCTYPE LogoutResponse [
<!ELEMENT LogoutResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST LogoutResponse success (0|1) #REQUIRED>
]>
```

LogoutResponse sample

```
<LogoutResponse success="1"/>
```

Site management

SiteListing

Provide a list of all sites the user is authorized to view or manage.

SiteListingRequest DTD

```
<!DOCTYPE SiteListingRequest [
<!ELEMENT SiteListingRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST SiteListingRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST SiteListingRequest session-id CDATA #REQUIRED>
]>
```

SiteListingRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<SiteListingRequest session-id="${Login#Response#//LoginResponse[1]
/@session-id}">
</SiteListingRequest>
```

SiteListingResponse DTD

```
<!DOCTYPE SiteListingResponse [
<!ELEMENT SiteListingResponse (Failure|SiteSummary*)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST SiteListingResponse success (0|1) #REQUIRED>
    <!-- See the SiteSummary DTD for more details -->
]>
```

SiteListingResponse example

```
<SiteListingResponse success="1"></SiteListingResponse>
```

SiteConfig

Provide the configuration of the site, including its associated assets.

SiteConfigRequest DTD

```
<!DOCTYPE SiteConfigRequest [
<!ELEMENT SiteConfigRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST SiteConfigRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST SiteConfigRequest session-id CDATA #REQUIRED>
    <!-- the ID of the site to retrieve the config for -->
    <!ATTLIST SiteConfigRequest site-id CDATA #REQUIRED>
]>
```

SiteConfigRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<SiteConfigRequest session-id="${Login#Response#//LoginResponse[1]
/@session-id}" site-id="${SiteSave#ResponseAsXml#//SiteSaveResponse[1]
/@site-id}">
</SiteConfigRequest>
```

SiteConfigResponse DTD

```
<!DOCTYPE SiteConfigResponse [
<!ELEMENT SiteConfigResponse (Failure|Site)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST SiteConfigResponse success (0|1) #REQUIRED>
    <!-- See the Site DTD for more details -->
]>
```

SiteConfigResponse sample

```
<SiteConfigResponse success="1">
<Site id="27" name="SOAPUI13006925d-7dac-428d-aaf1-4038a98838a1"
description="" riskfactor="1.0" isDynamic="0">
    <Description/>
    <Hosts>
            <host>server1.example.com</host>
            <host>server2.example.com</host>
            <host>server3.example.com</host>
            <host>server4.example.com</host>
            <host>server5.example.com</host>
    </Hosts>
    <Credentials></Credentials>
    <Alerting>
        <Alert name="test" enabled="1" maxAlerts="2">
            <scanFilter scanStart="1" scanStop="1" scanFailed="1"
            scanResumed="1" scanPaused="1"/>
            <vulnFilter severityThreshold="1" confirmed="1"
            unconfirmed="1" potential="1"/>
            <smtpAlert sender="user1@example.com"
            server="server6.example.com" limitText="0">
                    <recipient>user2@example.com</recipient>
            </smtpAlert>
        </Alert>
    </Alerting>
    <ScanConfig configID="28" name="Full audit" templateID="full-audit"
    engineID="3" configVersion="3">
        <Schedules></Schedules>
    </ScanConfig>
    </Site>
</SiteConfigResponse>
```

SiteSave

Save changes to a new or existing site.

SiteSaveRequest DTD

Note: Only enter DNS names in the *host* element. Do not enter an IP address in that element. Use the *range* element for IP address ranges. For a single IP address, use the *range* element where the *from* value is the IP address and the *to* value is empty.

```
<!DOCTYPE SiteSaveRequest [
<!ELEMENT SiteSaveRequest (Site)>
    <!-- user-defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST SiteSaveRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST SiteSaveRequest session-id CDATA #REQUIRED>
<!-- See the Site DTD for more details -->
]>
```

SiteSaveRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<SiteSaveRequest session-id="${Login#Response#//LoginResponse[1]
/@session-id}">
    <Site id="-1" name="SOAPUI1${Groovy Script-2#result}"
    description="" riskfactor="1.0" isDynamic="0">
        <Hosts>
            <host>server1.example.com</host>
            <host>server2.example.com</host>
            <host>server3.example.com</host>
            <host>server4.example.com</host>
            <host>server5.example.com</host>
        </Hosts>
        <Credentials></Credentials>
        <Alerting>
        <Alert enabled="1" name="test" maxAlerts="2"><scanFilter
        scanStart="1" scanStop="1" scanFailed="1" scanPaused="1"
        scanResumed="1"/><vulnFilter severityThreshold="1" confirmed="1"
        unconfirmed="1" potential="1"/><smtpAlert
        sender="user1.example.com" server="server6.example.com"
        limitText="0"><recipient>user1@example.com</recipient></smtpAle
        rt></Alert>
        </Alerting>
        <ScanConfig configID="1" name="Full audit" templateID="full-
        audit" engineID="${GetLocalScanEngine#result}"
        configVersion="3">
            <Schedules></Schedules>
            <ScanTriggers></ScanTriggers>
        </ScanConfig>
    </Site>
</SiteSaveRequest>
```

SiteSaveResponse DTD

```
<!DOCTYPE SiteSaveResponse [
<!ELEMENT SiteSaveResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST SiteSaveResponse success (0|1) #REQUIRED>
    <!-- the newly assigned site ID (unchanged for existing sites) -->
    <!ATTLIST SiteSaveResponse site-id CDATA #REQUIRED>
]>
```

SiteSaveResponse sample

```
<SiteSaveResponse success="1" site-id="27"/>
```

SiteDelete

Delete the specified site and all associated scan data.

If you have a scan in progress or a paused scan, you cannot delete the site in which that scan was initiated. If you send SiteDeleteRequest with a paused or in-progress scan, the application will return an error response. For more information, see *Error responses* on page 334.

It is a best practice to send SiteScanHistoryRequest first to determine if any scans are paused or running. See *SiteScanHistory* on page 39).

To stop a paused or running scan, send ScanStopRequest. See *ScanStop* on page 51).

When you are certain that no scans are running or paused, send SiteDeleteRequest.

SiteDeleteRequest DTD

```
<!DOCTYPE SiteDeleteRequest [
<!ELEMENT SiteDeleteRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST SiteDeleteRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST SiteDeleteRequest session-id CDATA #REQUIRED>
    <!-- the ID of the site to delete -->
    <!ATTLIST SiteDeleteRequest site-id CDATA #REQUIRED>
]>
```

SiteDeleteRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
```

```
    <SiteDeleteRequest session-id="${Login#Response#//LoginResponse[1]
    /@session-id}" site-id =
    "${SiteSave#ResponseAsXml#//SiteSaveResponse[1]/@site-id}">
</SiteDeleteRequest>
```

SiteDeleteResponse DTD

```
<!DOCTYPE SiteDeleteResponse [
<!ELEMENT SiteDeleteResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST SiteDeleteResponse success (0|1) #REQUIRED>
]>
```

SiteDeleteResponse sample

```
<SiteDeleteResponse success="1"/>
```

SiteDeviceListing

Provide a list of all of the assets in a site. If no site-id is specified, then this will return all of the assets for the Scan Engine, grouped by site-id.

SiteDeviceListingRequest DTD

```
<!DOCTYPE SiteDeviceListingRequest [
<!ELEMENT SiteDeviceListingRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST SiteDeviceListingRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST SiteDeviceListingRequest session-id CDATA #REQUIRED>
    <!-- the ID of the site to retrieve the device listing for -->
    <!ATTLIST SiteDeviceListingRequest site-id CDATA #IMPLIED>
]>
```

SiteDeviceListingRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
    <SiteDeviceListingRequest session-
    id="${Login#Response#//LoginResponse[1]/@session-id}" site-id =
    "${SiteSave#ResponseAsXml#//SiteSaveResponse[1]/@site-id}">
</SiteDeviceListingRequest>
```

SiteDeviceListingResponse DTD

```
<!DOCTYPE SiteDeviceListingResponse [
<!ELEMENT SiteDeviceListingResponse (Failure|SiteDevices*)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST SiteDeviceListingResponse success (0|1) #REQUIRED>
<!ELEMENT SiteDevices (device*)>
    <!-- See the device DTD for more details -->
    <!ATTLIST SiteDevices site-id CDATA #REQUIRED>
]>
```

SiteDeviceListingResponse sample

```
<SiteDeviceListingResponse success="1">
    <SiteDevices site-id="29"></SiteDevices>
</SiteDeviceListingResponse>
```

SiteScanHistory

Provide a list of all previous scans of the site.

SiteScanHistoryRequest DTD

```
<!DOCTYPE SiteScanHistoryRequest [
<!ELEMENT SiteScanHistoryRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST SiteScanHistoryRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST SiteScanHistoryRequest session-id CDATA #REQUIRED>
    <!-- the ID of the site to retrieve the scan history for -->
    <!ATTLIST SiteScanHistoryRequest site-id CDATA #REQUIRED>
]>
```

SiteScanHistoryRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
    <SiteScanHistoryRequest session-
    id="${Login#Response#//LoginResponse[1]/@session-id}" site-id =
    "${SiteSave#ResponseAsXml#//SiteSaveResponse[1]/@site-id}">
</SiteScanHistoryRequest>
```

SiteScanHistoryResponse DTD

```
<!DOCTYPE SiteScanHistoryResponse [
<!ELEMENT SiteScanHistoryResponse (Failure|ScanSummary*)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST SiteScanHistoryResponse success (0|1) #REQUIRED>
<!-- See the ScanSummary DTD for more details -->
]>
```

SiteScanHistoryResponse sample

```
<SiteScanHistoryResponse success="1">
    <ScanSummary scan-id="9" site-id="29" engine-id="3" name=""
    startTime="20150205T105847950" endTime="20150205T105958316"
    status="finished">
        <tasks pending="-1" active="-1" completed="-1"/>
        <nodes live="1" dead="0" filtered="0" unresolved="0" other="0"/>
        <vulnerabilities status="vuln-exploit" severity="1" count="2"/>
        <vulnerabilities status="vuln-exploit" severity="2" count="0"/>
        <vulnerabilities status="vuln-exploit" severity="3" count="0"/>
        <vulnerabilities status="vuln-exploit" severity="4" count="0"/>
        <vulnerabilities status="vuln-exploit" severity="5" count="1"/>
        <vulnerabilities status="vuln-exploit" severity="6" count="0"/>
        <vulnerabilities status="vuln-exploit" severity="7" count="0"/>
        <vulnerabilities status="vuln-exploit" severity="8" count="2"/>
        <vulnerabilities status="vuln-exploit" severity="9" count="0"/>
        <vulnerabilities status="vuln-exploit" severity="10" count="0"/>
        <vulnerabilities status="vuln-version" severity="1" count="2"/>
        <vulnerabilities status="vuln-version" severity="2" count="0"/>
        <vulnerabilities status="vuln-version" severity="3" count="0"/>
        <vulnerabilities status="vuln-version" severity="4" count="0"/>
        <vulnerabilities status="vuln-version" severity="5" count="0"/>
        <vulnerabilities status="vuln-version" severity="6" count="1"/>
        <vulnerabilities status="vuln-version" severity="7" count="1"/>
        <vulnerabilities status="vuln-version" severity="8" count="0"/>
        <vulnerabilities status="vuln-version" severity="9" count="0"/>
        <vulnerabilities status="vuln-version" severity="10" count="1"/>
        <vulnerabilities status="vuln-potential" severity="1"
        count="0"/>
        <vulnerabilities status="vuln-potential" severity="2"
        count="0"/>
        <vulnerabilities status="vuln-potential" severity="3"
        count="0"/>
        <vulnerabilities status="vuln-potential" severity="4"
        count="0"/>
        <vulnerabilities status="vuln-potential" severity="5"
        count="0"/>
        <vulnerabilities status="vuln-potential" severity="6"
        count="0"/>
        <vulnerabilities status="vuln-potential" severity="7"
        count="0"/>
        <vulnerabilities status="vuln-potential" severity="8"
        count="0"/>
        <vulnerabilities status="vuln-potential" severity="9"
        count="0"/>
        <vulnerabilities status="vuln-potential" severity="10"
        count="0"/>
        <vulnerabilities status="not-vuln-exploit" count="0"/>
        <vulnerabilities status="not-vuln-version" count="0"/>
        <vulnerabilities status="error" count="0"/>
        <vulnerabilities status="disabled" count="0"/>
        <vulnerabilities status="other" count="0"/>
    </ScanSummary>
</SiteScanHistoryResponse>
```

Scan management

This section includes management of Scan Engines.

SiteScan

Scan the specified site.

SiteScanRequest DTD

```
<!DOCTYPE SiteScanRequest [
<!ELEMENT SiteScanRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST SiteScanRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST SiteScanRequest session-id CDATA #REQUIRED>
    <!-- the ID of the site to scan -->
    <!ATTLIST SiteScanRequest site-id CDATA #REQUIRED>
]>
```

SiteScanRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<SiteScanRequest session-id="${Login#Response#//LoginResponse[1]
/@session-id}" site-id="${SiteSave#ResponseAsXml#//SiteSaveResponse[1]
/@site-id}">
</SiteScanRequest>
```

SiteScanResponse DTD

```
<!DOCTYPE SiteScanResponse [
<!ELEMENT SiteScanResponse (Failure|(Scan+))>
<!-- set to 1 upon success, 0 otherwise -->
<!ATTLIST SiteScanResponse success (0|1) #REQUIRED>
<!ELEMENT Scan EMPTY>
<!-- the scan ID, upon successful start -->
<!ATTLIST Scan scan-id CDATA #REQUIRED>
<!-- the engine the scan was dispatched to -->
<!ATTLIST Scan engine-id CDATA #REQUIRED>
]>
```

SiteScanResponse sample

```
<SiteScanResponse success="1">
    <Scan scan-id="9" engine-id="3"/>
</SiteScanResponse>
```

SiteDevicesScan

Scan a specified subset of site assets.

SiteDevicesScanRequest DTD

```
<!DOCTYPE SiteDevicesScanRequest [
<!ELEMENT SiteDevicesScanRequest (Devices?,Hosts?,Schedules?)>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST SiteDevicesScanRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST SiteDevicesScanRequest session-id CDATA #REQUIRED>
    <!-- the ID of the site whose devices are to be scanned -->
    <!ATTLIST SiteDevicesScanRequest site-id CDATA #REQUIRED>

<!ELEMENT Devices (device+)>
<!-- See the device DTD for more details -->

<!ELEMENT Hosts (range|hosts)+>
<!-- IPv4 address range of the form 10.0.0.1 -->
<!ELEMENT range EMPTY>
    <!ATTLIST range from CDATA #REQUIRED>
    <!ATTLIST range to CDATA #IMPLIED>
<!-- named host (usually DNS or Netbios name -->
<!ELEMENT host (#PCDATA)>
<!--This Schedules element is different from the element with the same
name in SiteConfigResponse. With this element, schedule a one-time scan
for the subset of assets. The scheduling functionality avoids conflicts
with existing schedules for start time and duration. Scans stop after
max duration is reached and adhere to blackouts. A Global Administrator
can force a scan to continue in a blackout period. The schedule is
removed from the database when the scan runs.-->
<!ELEMENT Schedules (AdHocSchedule*)>
    <!ATTLIST start CDATA #REQUIRED>
    <!ATTLIST template CDATA #IMPLIED>
    <!ATTLIST maxDuration CDATA #IMPLIED>

]>
```

SiteDevicesScanRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<SiteDevicesScanRequest session-
id="169CA1F157DE71E64F43A227B8692926FA029A60" site-id="1">
<Devices>
    <device id="1"/>
</Devices>
<Hosts>
    <range from="10.5.1.105"/>
</Hosts>
<Schedules>
    <AdHocSchedule start="20150311T164600000" template="full-audit-
    without-web-spider" maxDuration="1"/>
    <AdHocSchedule start="20150312T164600000" template="full-audit-
    without-web-spider" maxDuration="1"/>
</Schedules>
</SiteDevicesScanRequest>
```

SiteDevicesScanResponse DTD

```
<!DOCTYPE SiteDevicesScanResponse [

<!ELEMENT SiteDevicesScanResponse (Failure|(Scan+))>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST SiteDevicesScanResponse success (0|1) #REQUIRED>
<!ELEMENT Scan EMPTY>
    <!-- the scan ID, upon successful start -->
    <!ATTLIST Scan scan-id CDATA #REQUIRED>
    <!-- the engine the scan was dispatched to -->
    <!ATTLIST Scan engine-id CDATA #REQUIRED>
]>
```

SiteDevicesScanResponse sample

Without the AdHocSchedule element in the request:

```
<SiteDevicesScanResponse success="1"> <Scan scan-id="3" engine-id="3"/>
 </SiteDevicesScanResponse>
```

With the AdHocSchedule element in the request:

```
<SiteDevicesScanResponse success="1"/>
```

Error responses for SiteDevicesScan

If you are a Global Administrator or a user with SuperUser permissions, and your scan conflicts with a blackout period, you will see one of the following responses:

If you schedule the scan to start in a blackout period:

```
<SiteDevicesScanResponse success="0">
    <Failure>
        <message>The requested scan schedule cannot be saved at this
        time. Start time is in a blackout period, use force="true" to
        force this scan to run.</message>
    </Failure>
</SiteDevicesScanResponse>
```

If your scheduled duration runs into a blackout period:

```
<SiteDevicesScanResponse success="0">
    <Failure>
        <message>The requested scan schedule cannot be saved at this
        time. Scan duration running into a blackout period, use
        force="true" to force this scan to run.</message>
    </Failure>
</SiteDevicesScanResponse>
```

If you are not a Global Administrator or a user with SuperUser permissions, and your scan conflicts with a blackout period, you will see one of the following responses:

If you schedule the scan to start in a blackout period:

```
<SiteDevicesScanResponse success="0">
    <Failure>
        <message>Not authorized to schedule a scan due to start time in
        a blackout period.</message>
    </Failure>
</SiteDevicesScanResponse>
```

If your scheduled duration runs into a blackout period:

```
<SiteDevicesScanResponse success="0">
    <Failure>
        <message>Not authorized to schedule a scan due to scan duration
        running into a blackout period.</message>
    </Failure>
</SiteDevicesScanResponse>
```

ScanActivity

Provide a list of current scan activities across all Scan Engines managed by the Security Console.

ScanActivityRequest DTD

```
<!DOCTYPE ScanActivityRequest [
<!ELEMENT ScanActivityRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST ScanActivityRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST ScanActivityRequest session-id CDATA #REQUIRED>
]>
```

ScanActivityRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<ScanActivityRequest session-
id="1DF93E6D1880368DE78FFED7A86CE8344A77C1FB">
</ScanActivityRequest>
```

ScanActivityResponse DTD

```
<!DOCTYPE ScanActivityResponse [
<!ELEMENT ScanActivityResponse (Failure|ScanSummary*)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST ScanActivityResponse success (0|1) #REQUIRED>
<!-- See ScanSummary DTD for more details -->

]>
```

ScanActivityResponse sample

```
<ScanActivityResponse success="1">
<ScanSummary scan-id="2" site-id="1" engine-id="3" name=""
startTime="20150205T145923594" status="running">
    <tasks pending="0" active="0" completed="0"/>
    <nodes live="0" dead="0" filtered="0" unresolved="0" other="0"/>
    <vulnerabilities status="vuln-exploit" severity="1" count="0"/>
    <vulnerabilities status="vuln-exploit" severity="2" count="0"/>
    <vulnerabilities status="vuln-exploit" severity="3" count="0"/>
    <vulnerabilities status="vuln-exploit" severity="4" count="0"/>
```

ScanPause

Pause a running scan.

ScanPauseRequest DTD

```
<!DOCTYPE ScanPauseRequest [
<!ELEMENT ScanPauseRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST ScanPauseRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST ScanPauseRequest session-id CDATA #REQUIRED>
    <!-- the ID of the scan -->
    <!ATTLIST ScanPauseRequest scan-id CDATA #REQUIRED>
]>
```

ScanPauseRequest sample

```
<ScanPauseRequest session-id="${Login#Response#//LoginResponse[1]
/@session-id}" scan-id="${SiteScan#ResponseAsXml#//SiteScanResponse[1]
/Scan[1]/@scan-id}">
```

ScanPauseResponse DTD

```
<!DOCTYPE ScanPauseResponse [
<!ELEMENT ScanPauseResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST ScanPauseResponse success (0|1) #REQUIRED>
]>
```

ScanPauseResponse sample

```
<ScanPauseResponse success="1"/>
```

ScanResume

Resume a running scan.

ScanResumeRequest DTD

```
<!DOCTYPE ScanResumeRequest [
<!ELEMENT ScanResumeRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST ScanResumeRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST ScanResumeRequest session-id CDATA #REQUIRED>
    <!-- the ID of the scan -->
    <!ATTLIST ScanResumeRequest scan-id CDATA #REQUIRED>
]>
```

ScanResumeRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<ScanResumeRequest session-id="${Login#Response#//LoginResponse[1]
/@session-id}" scan-id="${SiteScan#ResponseAsXml#//SiteScanResponse[1]
/Scan[1]/@scan-id}">
</ScanResumeRequest>
```

ScanResumeResponse DTD

```
<!DOCTYPE ScanResumeResponse [
<!ELEMENT ScanResumeResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST ScanResumeResponse success (0|1) #REQUIRED>
]>
```

ScanResumeResponse sample

```
<ScanResumeResponse success="1"/>
```

ScanStop

Stop a running scan.

ScanStopRequest DTD

```
<!DOCTYPE ScanStopRequest [
<!ELEMENT ScanStopRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST ScanStopRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST ScanStopRequest session-id CDATA #REQUIRED>
    <!-- the ID of the scan -->
    <!ATTLIST ScanStopRequest scan-id CDATA #REQUIRED>
]>
```

ScanStopRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<ScanStopRequest session-id="${Login#Response#//LoginResponse[1]
/@session-id}" scan-id="${SiteScan#ResponseAsXml#//SiteScanResponse[1]
/Scan[1]/@scan-id}">
</ScanStopRequest>
```

ScanStopResponse DTD

```
<!DOCTYPE ScanStopResponse [
<!ELEMENT ScanStopResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST ScanStopResponse success (0|1) #REQUIRED>
]>
```

ScanStopResponse sample

```
<ScanStopResponse success="1"/>
```

ScanStatus

Check the current status of a scan.

ScanStatusRequest DTD

```
<!DOCTYPE ScanStatusRequest [
<!ELEMENT ScanStatusRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST ScanStatusRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST ScanStatusRequest session-id CDATA #REQUIRED>
    <!-- the ID of the scan -->
    <!ATTLIST ScanStatusRequest scan-id CDATA #REQUIRED>
]>
```

ScanStatusRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<ScanStatusRequest session-id="${Login#Response#//LoginResponse[1]
/@session-id}" scan-id="${SiteScan#ResponseAsXml#//SiteScanResponse[1]
/Scan[1]/@scan-id}">
</ScanStatusRequest>
```

ScanStatusResponse DTD

```
<!DOCTYPE ScanStatusResponse [
<!ELEMENT ScanStatusResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST ScanStatusResponse success (0|1) #REQUIRED>
    <!-- the ID of the scan -->
    <!ATTLIST ScanStatusResponse scan-id CDATA #REQUIRED>
    <!-- the ID of the Scan Engine -->
    <!ATTLIST ScanStatusResponse engine-id CDATA #REQUIRED>
    <!-- the current scan status -->
    <!ATTLIST ScanStatusResponse status
    (running|finished|stopped|error|
    dispatched|paused|aborted|unknown) #REQUIRED>
]>
```

ScanStatusResponse sample

```
<ScanStatusResponse success="1" scan-id="11" engine-id="3"
status="running"/>
```

ScanStatistics

Get scan statistics, including node and vulnerability breakdowns.

ScanStatisticsRequest DTD

```
<!DOCTYPE ScanStatisticsRequest [
<!ELEMENT ScanStatisticsRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST ScanStatisticsRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST ScanStatisticsRequest session-id CDATA #REQUIRED>
    <!-- the ID of the scan -->
    <!ATTLIST ScanStatisticsRequest scan-id CDATA #REQUIRED>
]>
```

ScanStatisticsRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<ScanStatisticsRequest session-
id="${Login#ResponseAsXml#//LoginResponse[1]/@session-id}" engine-id =
"${SiteScan-2#ResponseAsXml#//SiteScanResponse[1]/Scan[1]/@engine-id}"
scan-id="${SiteScan#ResponseAsXml#//SiteScanResponse[1]/Scan[1]/@scan-
id}">
</ScanStatisticsRequest>
```

ScanStatisticsResponse

```
<!DOCTYPE ScanStatisticsResponse [
<!ELEMENT ScanStatisticsResponse (Failure|ScanSummary)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST ScanStatisticsResponse success (0|1) #REQUIRED>
<!-- see the ScanSummary DTD for more details -->
]>
```

ScanStatisticsResponse sample

```
<ScanStatisticsResponse success="1">
    <ScanSummary scan-id="15" site-id="38" engine-id="3" name=""
    startTime="20150205T155838021" status="running">
        <tasks pending="-1" active="-1" completed="-1"/>
        <nodes live="0" dead="0" filtered="0" unresolved="0" other="0"/>
        <vulnerabilities status="vuln-exploit" severity="1" count="0"/>
        <vulnerabilities status="vuln-exploit" severity="2" count="0"/>
        <vulnerabilities status="vuln-exploit" severity="3" count="0"/>
        <vulnerabilities status="vuln-exploit" severity="4" count="0"/>
        <vulnerabilities status="vuln-exploit" severity="5" count="0"/>
        <vulnerabilities status="vuln-exploit" severity="6" count="0"/>
        <vulnerabilities status="vuln-exploit" severity="7" count="0"/>
        <vulnerabilities status="vuln-exploit" severity="8" count="0"/>
        <vulnerabilities status="vuln-exploit" severity="9" count="0"/>
        <vulnerabilities status="vuln-exploit" severity="10" count="0"/>
        <vulnerabilities status="vuln-version" severity="1" count="0"/>
        <vulnerabilities status="vuln-version" severity="2" count="0"/>
        <vulnerabilities status="vuln-version" severity="3" count="0"/>
        <vulnerabilities status="vuln-version" severity="4" count="0"/>
        <vulnerabilities status="vuln-version" severity="5" count="0"/>
        <vulnerabilities status="vuln-version" severity="6" count="0"/>
        <vulnerabilities status="vuln-version" severity="7" count="0"/>
        <vulnerabilities status="vuln-version" severity="8" count="0"/>
        <vulnerabilities status="vuln-version" severity="9" count="0"/>
        <vulnerabilities status="vuln-version" severity="10" count="0"/>
        <vulnerabilities status="vuln-potential" severity="1"
        count="0"/>
        <vulnerabilities status="vuln-potential" severity="2"
        count="0"/>
        <vulnerabilities status="vuln-potential" severity="3"
        count="0"/>
        <vulnerabilities status="vuln-potential" severity="4"
        count="0"/>
        <vulnerabilities status="vuln-potential" severity="5"
        count="0"/>
        <vulnerabilities status="vuln-potential" severity="6"
        count="0"/>
        <vulnerabilities status="vuln-potential" severity="7"
        count="0"/>
        <vulnerabilities status="vuln-potential" severity="8"
        count="0"/>
        <vulnerabilities status="vuln-potential" severity="9"
        count="0"/>
```

```
            <vulnerabilities status="vuln-potential" severity="10"
            count="0"/>
            <vulnerabilities status="not-vuln-exploit" count="0"/>
            <vulnerabilities status="not-vuln-version" count="0"/>
            <vulnerabilities status="error" count="0"/>
            <vulnerabilities status="disabled" count="0"/>
            <vulnerabilities status="other" count="0"/>
        </ScanSummary>
    </ScanStatisticsResponse>
```

EngineListing

Provide a list of all Scan Engines managed by the Security Console.

EngineListingRequest DTD

```
<!DOCTYPE EngineListingRequest [
<!ELEMENT EngineListingRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST EngineListingRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST EngineListingRequest session-id CDATA #REQUIRED>
]>
```

EngineListingRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<EngineListingRequest session-id="${Login#ResponseAsXml#//LoginResponse
[1]/@session-id}">
</EngineListingRequest>
```

EngineListingResponse DTD

```
<!DOCTYPE EngineListingResponse [
<!ELEMENT EngineListingResponse (Failure|EngineSummary*)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST EngineListingResponse success (0|1) #REQUIRED>

<!-- See the EngineSummary DTD for more details -->

]>
```

EngineListingResponse sample

```
<?xml version="1.0" encoding="utf-8"?>
<EngineListingRequest session-
id="B9C2EFC2AA13B34390B74D1DFA9FAF2B344F5F08">
</EngineListingRequest>
```

EngineActivity

Provide a list of current scan activities for a specific Scan Engine.

EngineActivityRequest DTD

```
<!DOCTYPE EngineActivityRequest [
<!ELEMENT EngineActivityRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST EngineActivityRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST EngineActivityRequest session-id CDATA #REQUIRED>
    <!-- the id of the engine to query -->
    <!ATTLIST EngineActivityRequest engine-id CDATA #REQUIRED>
]>
```

EngineActivityRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<EngineActivityRequest session-
id="${Login#ResponseAsXml#//LoginResponse[1]/@session-id}" engine-id =
"${SiteScan-2#ResponseAsXml#//SiteScanResponse[1]/Scan[1]/@engine-id}">
</EngineActivityRequest>
```

EngineActivityResponse DTD

```
<!DOCTYPE EngineActivityResponse [
<!ELEMENT EngineActivityResponse (Failure|ScanSummary*)>
<!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST EngineActivityResponse success (0|1) #REQUIRED>
    <!-- current status of the Scan Engine -->
    <!-- See the ScanSummary DTD for more details -->
]>
```

EngineActivityResponse sample

```
<EngineActivityResponse success="1">
<ScanSummary scan-id="43" site-id="10" engine-id="3" name=""
startTime="20150205T180644256" status="running">
    <tasks pending="0" active="0" completed="0"/>
    <nodes live="0" dead="0" filtered="0" unresolved="0" other="0"/>
    <vulnerabilities status="vuln-exploit" severity="1" count="0"/>
    <vulnerabilities status="vuln-exploit" severity="10" count="0"/>
    <vulnerabilities status="vuln-version" severity="1" count="0"/>
    <vulnerabilities status="vuln-version" severity="9" count="0"/>
    <vulnerabilities status="vuln-potential" severity="1" count="0"/>
    <vulnerabilities status="vuln-potential" severity="2" count="0"/>
    <vulnerabilities status="not-vuln-exploit" count="0"/>
    <vulnerabilities status="not-vuln-version" count="0"/>
    <vulnerabilities status="error" count="0"/>
    <vulnerabilities status="disabled" count="0"/>
    <vulnerabilities status="other" count="0"/>
</ScanSummary>
<ScanSummary scan-id="42" site-id="3" engine-id="3" name=""
startTime="20150205T180502678" status="running">
    <tasks pending="200" active="5" completed="812"/>
    <nodes live="6" dead="0" filtered="0" unresolved="0" other="0"/>
    <vulnerabilities status="vuln-exploit" severity="1" count="0"/>
    <vulnerabilities status="vuln-exploit" severity="2" count="0"/>
    <vulnerabilities status="vuln-version" severity="1" count="0"/>
    <vulnerabilities status="vuln-version" severity="2" count="0"/>
    <vulnerabilities status="vuln-potential" severity="1" count="0"/>
    <vulnerabilities status="vuln-potential" severity="2" count="0"/>
    <vulnerabilities status="vuln-potential" severity="3" count="0"/>
    <vulnerabilities status="vuln-potential" severity="4" count="0"/>
    <vulnerabilities status="not-vuln-exploit" count="0"/>
    <vulnerabilities status="not-vuln-version" count="0"/>
    <vulnerabilities status="error" count="0"/>
    <vulnerabilities status="disabled" count="0"/>
    <vulnerabilities status="other" count="0"/>
</ScanSummary>
</EngineActivityResponse>
```

General management and diagnostic functions

ConsoleCommand

Execute an arbitrary console command that is supplied as text via an API parameter. Console commands are documented in the administrator's guide and in Help. If you use a command that is not listed in the in administrator's guide, the application will return the XMLResponse.

ConsoleCommandRequest DTD

```
<!DOCTYPE ConsoleCommandRequest[
<!ELEMENT ConsoleCommandRequest (Command)>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST ConsoleCommandRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST ConsoleCommandRequest session-id CDATA #REQUIRED>
<!ELEMENT Command CDATA #REQUIRED>
]>
```

ConsoleCommandResponse DTD

```
<!DOCTYPE ConsoleCommandResponse[
<!ELEMENT ConsoleCommandResponse (Command,Output)>
    <!-- set to 1 upon success, 0 otherwise -->
        <!ATTLIST ConsoleCommandResponse success (0|1) #REQUIRED>
<!ELEMENT Command CDATA #REQUIRED>
<!ELEMENT Output CDATA #REQUIRED>
]>
```

Tip: Set a higher timeout value for a command that requires a substantial amount of time to execute and finish. Doing so ensures that the application has sufficient time to respond to the command.

SystemInformation

Obtain system data, such as total RAM, free RAM, total disk space, free disk space, CPU speed, number of CPU cores, and other vital information.

SystemInformationRequest DTD

```
<!DOCTYPE SystemInformationRequest[
<!ELEMENT SystemInformationRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST SystemInformationRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST SystemInformationRequest session-id CDATA #REQUIRED>
]>
```

SystemInformationRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<SystemInformationRequest session-id="${Login#Response#//LoginResponse
[1]/@session-id}">
</SystemInformationRequest>
```

SystemInformationResponse DTD

```
<!DOCTYPE SystemInformationResponse[
<!ELEMENT SystemInformationResponse (SystemInformationSummary)>
    <!ATTLIST SystemInformationResponse success (0|1) #REQUIRED>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ELEMENT SystemInformationSummary (Statistic*)>
        <!ELEMENT Statistic CDATA #IMPLIED>
            <!ATTLIST Statistic name (cpu-count|cpu-speed|disk-
            install|java-name|
            jre-version|last-update-date|last-update-id|disk-tmp|nsc-
            name|nsc-version|nse-version|os|ram-free|ram-total|up-
            time|db-product|db-version|java-heap-max|java-heap-
            committed|java-heap-free|java-heap-used|java-total-thread-
            count|java-started-thread-count|java-thread-peak-count|java-
            daemon-thread-count) #IMPLIED>
]>
```

SystemInformationResponse sample

```
<SystemInformationResponse success="1">
    <StatisticsInformationSummary>
        <Statistic name="cpu-count">2</Statistic>
        <Statistic name="cpu-speed">2660</Statistic>
        <Statistic name="disk-
        install">/opt/rapid7/nexpose=32901904</Statistic>
        <Statistic name="disk-tmp">../shared/temp=32901904</Statistic>
        <Statistic name="os">Ubuntu Linux 12.04</Statistic>
        <Statistic name="ram-free">170376</Statistic>
        <Statistic name="ram-total">8177868</Statistic>
        <Statistic name="up-time">45757264</Statistic>
        <Statistic name="db-product">postgresql</Statistic>
        <Statistic name="db-version">PostgreSQL 9.0.13 on x86_64-
        unknown-linux-gnu, compiled by GCC gcc (GCC) 4.1.2 20080704 (Red
        Hat 4.1.2-52), 64-bit</Statistic>
        <Statistic name="java-name">Java HotSpot(TM) 64-Bit Server
        VM</Statistic>
        <Statistic name="java-heap-max">6263537664</Statistic>
        <Statistic name="java-heap-committed">4829077504</Statistic>
        <Statistic name="java-heap-free">3694844920</Statistic>
        <Statistic name="java-heap-used">2568692744</Statistic>
        <Statistic name="jre-version">24.0-b56</Statistic>
        <Statistic name="nsc-name">CN=NeXpose Security Console,
        O=Rapid7</Statistic>
        <Statistic name="nsc-version">5.12.2</Statistic>
        <Statistic name="last-update-date">1423140440496</Statistic>
        <Statistic name="last-update-id">1028948869</Statistic>
        <Statistic name="java-daemon-thread-count">44</Statistic>
        <Statistic name="java-total-thread-count">67</Statistic>
        <Statistic name="java-thread-peak-count">118</Statistic>
        <Statistic name="java-started-thread-count">4950</Statistic>
    </StatisticsInformationSummary>
</SystemInformationResponse>
```

StartUpdate

Induce the application to retrieve required updates and restart if necessary.

StartUpdateRequest DTD

```
<!DOCTYPE StartUpdateRequest[
<!ELEMENT StartUpdateRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST StartUpdateRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST StartUpdateRequest session-id CDATA #REQUIRED>
]>
```

StartUpdateResponse DTD

Set a higher timeout value for a command that requires a substantial amount of time to execute and finish. Doing so ensures that the application has sufficient time to respond to the command.

```
<!DOCTYPE StartUpdateResponse[
<!ELEMENT StartUpdateResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST StartUpdateResponse success (0|1) #REQUIRED>
```

Restart

Restart the application.

RestartRequest DTD

```
<!DOCTYPE RestartRequest[
<!ELEMENT RestartRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST RestartRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST RestartRequest session-id CDATA #REQUIRED>
]>
```

RestartRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<ConsoleCommandRestart session-id="${Login#Response#//LoginResponse[1]
/@session-id}">
    <Command>restart</Command>
</ConsoleCommandRequest>
```

RestartResponse

There is no response to RestartRequest. When the application shuts down as part of the restart process, it terminates any active connections. Therefore, the application cannot issue a response when it restarts.

SendLog

Output diagnostic information into log files, zip the files, and encrypt the archive with a PGP public key that is provided as a parameter for the API call. Then, either e-mail this archive to an address that is specified as an API parameter, or upload the archive using HTTP or HTTPS to a URL that is specified as an API parameter.

If you do not specify a key, the SendLogRequest uses a default key.

SendLogRequest DTD

```
<!DOCTYPE SendLogRequest[
<!ELEMENT SendLogRequest (Transport)>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST SendLogRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST SendLogRequest session-id CDATA #REQUIRED>
    <!ATTLIST SendLogRequest keyid CDATA #IMPLIED>
<!ELEMENT Transport (Email|URL)>
    <!ATTLIST Transport protocol CDATA #REQUIRED (smtp|http|https)>
<!-- If protocol== "smtp" -->
    <!–- See the Email DTD for more details -->
<!-- If protocol == "http" || "https" -->
    <!ELEMENT URL CDATA #REQUIRED>
]>
```

SendLogResponse DTD

```
<!DOCTYPE SendLogResponse[
<!ELEMENT SendLogResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST SendLogResponse success (0|1) #REQUIRED>
]>
```

Device (asset) management

DeviceDelete

Delete the specified asset.

DeviceDeleteRequest DTD

```
<!DOCTYPE SiteDeleteRequest [
<!ELEMENT SiteDeleteRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST SiteDeleteRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST SiteDeleteRequest session-id CDATA #REQUIRED>
    <!-- the ID of the site to delete -->
    <!ATTLIST SiteDeleteRequest site-id CDATA #REQUIRED>
]>
```

DeviceDeleteRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
    <DeviceDeleteRequest session-id="${Login#Response#//LoginResponse
    [1]/@session-id}" device-id = "${SiteDeviceListing-
    SiteId#ResponseAsXml#//SiteDeviceListingResponse[1]/SiteDevices[1]
    /device[1]/@id}">
</DeviceDeleteRequest>
```

DeviceDeleteResponse DTD

```
<!DOCTYPE SiteDeleteResponse [
<!ELEMENT SiteDeleteResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST SiteDeleteResponse success (0|1) #REQUIRED>
]>
```

DeviceDeleteResponse sample

```
<DeviceDeleteResponse success="1"></DeviceDeleteResponse>
```

Asset group management

AssetGroupListing

Provide a list of all asset groups the user is authorized to view or manage.

AssetGroupListingRequest DTD

```
<!DOCTYPE AssetGroupListingRequest [
<!ELEMENT AssetGroupListingRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST AssetGroupListingRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST AssetGroupListingRequest session-id CDATA #REQUIRED>
]>
```

AssetGroupListingRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
    <AssetGroupListingRequest session-
    id="${Login#Response#//LoginResponse[1]/@session-id}">
</AssetGroupListingRequest>
```

AssetGroupListingResponse DTD

```
<!DOCTYPE AssetGroupListingResponse [
<!ELEMENT AssetGroupListingResponse (Failure|AssetGroupSummary*)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST AssetGroupListingResponse success (0|1) #REQUIRED>
<!-- See the AssetGroupSummary DTD for more details -->
]>
```

AssetGroupListingResponse sample

```
<AssetGroupListingResponse success="1">
    <AssetGroupSummary id="5" name="SoapUI1423162726606"
    description="SOAPUISAG" riskscore="4333.79443" dynamic="0"/>
</AssetGroupListingResponse>
```

AssetGroupConfig

Provide the configuration of the asset group, including its associated devices.

AssetGroupConfigRequest DTD

```
<!DOCTYPE AssetGroupConfigRequest [
<!ELEMENT AssetGroupConfigRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST AssetGroupConfigRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST AssetGroupConfigRequest session-id CDATA #REQUIRED>
    <!-- the ID of the group to retrieve the config for -->
    <!ATTLIST AssetGroupConfigRequest group-id CDATA #REQUIRED>
]>
```

AssetGroupConfigRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
    <AssetGroupConfigRequest session-
    id="${Login#Response#//LoginResponse[1]/@session-id}" group-
    id="${AssetGroupSave#ResponseAsXml#//AssetGroupSaveResponse[1]
    /@group-id}">
</AssetGroupConfigRequest>
```

AssetGroupConfigResponse

```
<!DOCTYPE AssetGroupConfigResponse [
<!ELEMENT AssetGroupConfigResponse (Failure|AssetGroup)>
<!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST AssetGroupConfigResponse success (0|1) #REQUIRED>
    <!-- See the AssetGroup DTD for more details -->
]>
```

AssetGroupConfigResponse sample

```
<AssetGroupConfigResponse success="1">
    <AssetGroup id="5" name="SoapUI1423162726606"
    description="SOAPUISAG" riskscore="4333.79443">
        <Devices>
            <device id="8" site-id="0" address="10.4.27.121"
            riskfactor="" riskscore="4333.7944"></device>
        </Devices>
    </AssetGroup>
</AssetGroupConfigResponse>
```

AssetGroupSave

Save changes to a new or existing static asset group.

AssetGroupSaveRequest API

```
<!DOCTYPE AssetGroupSaveRequest [
<!ELEMENT AssetGroupSaveRequest (AssetGroup, Failure?)>
```

```
    <!-- user-defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST AssetGroupSaveRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST AssetGroupSaveRequest session-id CDATA #REQUIRED>
    <!—- each asset group defines assets within it -->
    <!ELEMENT AssetGroup (Devices)>
    <!— set to -1 to create a new group, or a positive integer to
    update an existing group -->
    <!ATTLIST AssetGroup id CDATA #REQUIRED>
    <!ATTLIST AssetGroup name CDATA #REQUIRED>
    <!ATTLIST AssetGroup description CDATA #IMPLIED>
    <!—- container element for asset inclusions -->
    <!ELEMENT Devices (device+)>
    <!ELEMENT device EMPTY>
    <!-- the identifier of the asset to include in the group -->
    <!ATTLIST device id CDATA #REQUIRED>
]>
```

AssetGroupSaveRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<AssetGroupSaveRequest session-id="${Login#Response#//LoginResponse[1]
/@session-id}">
<AssetGroup id="-1" name="SoapUI${Groovy Script-3#result}"
description="SOAPUISAG">
<Users>
</Users>
<Devices>
<device id="${SiteDeviceListing-
SiteId#ResponseAsXml#//SiteDeviceListingResponse[1]/SiteDevices[1]
/device[1]/@id}"/></Devices>
<GroupPrivileges gid="-1" viewAssets="1" configureAssets="1">
</GroupPrivileges>
</AssetGroup>
</AssetGroupSaveRequest>
```

AssetGroupSaveResponse DTD

```
<!DOCTYPE AssetGroupSaveResponse [
<!ELEMENT AssetGroupSaveResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST AssetGroupSaveResponse success (0|1) #REQUIRED>
    <!-- the newly assigned group ID (unchanged for existing groups) --
    >
    <!ATTLIST AssetGroupSaveResponse group-id CDATA #REQUIRED>
]>
```

AssetGroupSaveResponse sample

```
<AssetGroupSaveResponse success="1" group-id="5"/>
```

AssetGroupDelete

Delete the specified asset group and all associated scan data.

AssetGroupDeleteRequest DTD

```
<!DOCTYPE AssetGroupDeleteRequest [
<!ELEMENT AssetGroupDeleteRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST AssetGroupDeleteRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST AssetGroupDeleteRequest session-id CDATA #REQUIRED>
    <!-- the ID of the group to delete -->
    <!ATTLIST AssetGroupDeleteRequest group-id CDATA #REQUIRED>
]>
```

AssetGroupDeleteRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
    <AssetGroupDeleteRequest session-
    id="${Login#Response#//LoginResponse[1]/@session-id}" group-id =
    "${AssetGroupSave#ResponseAsXml#//AssetGroupSaveResponse[1]/@group-
    id}">
</AssetGroupDeleteRequest>
```

AssetGroupDeleteResponse

```
<!DOCTYPE AssetGroupDeleteResponse [
<!ELEMENT AssetGroupDeleteResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST AssetGroupDeleteResponse success (0|1) #REQUIRED>
]>
```

AssetGroupDeleteResponse sample

```
<AssetGroupDeleteResponse success="1"></AssetGroupDeleteResponse>
```

Vulnerability management

VulnerabilityListing

Provide a list of vulnerabilities that can be checked.

VulnerabilityListingRequest

```
<!DOCTYPE VulnerabilityListingRequest [
<!ELEMENT VulnerabilityListingRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST VulnerabilityListingRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST VulnerabilityListingRequest session-id CDATA #REQUIRED>
]>
```

VulnerabilityListingResponse

```
<!DOCTYPE VulnerabilityListingResponse [
<!ELEMENT VulnerabilityListingResponse (Failure|VulnerabilitySummary*)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST VulnerabilityListingResponse success (0|1) #REQUIRED>
<!ELEMENT VulnerabilitySummary EMPTY>
    <!ATTLIST VulnerabilitySummary id CDATA #REQUIRED>
    <!ATTLIST VulnerabilitySummary title CDATA #REQUIRED>
    <!ATTLIST VulnerabilitySummary severity CDATA #REQUIRED>
    <!ATTLIST VulnerabilitySummary pciSeverity CDATA #REQUIRED>
    <!ATTLIST VulnerabilitySummary cvssScore CDATA #IMPLIED >
    <!ATTLIST VulnerabilitySummary cvssVector CDATA #IMPLIED >
    <!-- the published date and time is in ISO 8601 format,
    YYYYMMDDTHHMMSSsss, such as: 19981231T00000000 -->
    <!ATTLIST VulnerabilitySummary published CDATA #IMPLIED >
    <!-- the added date and time is in ISO 8601 format,
    YYYYMMDDTHHMMSSsss, such as: 19981231T00000000 -->
    <!ATTLIST VulnerabilitySummary added CDATA #REQUIRED>
    <!-- the modified date and time is in ISO 8601 format,
    YYYYMMDDTHHMMSSsss, such as: 19981231T00000000 -->
    <!ATTLIST VulnerabilitySummary modified CDATA #REQUIRED>
]>
```

VulnerabilityDetails

Provide the full details of a vulnerability, including its description, cross-references, and solution.

VulnerabilityDetailsRequest

```
<!DOCTYPE VulnerabilityDetailsRequest [
<!ELEMENT VulnerabilityDetailsRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST VulnerabilityDetailsRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST VulnerabilityDetailRequest session-id CDATA #REQUIRED>
    <!-- the id of the vulnerability to retrieve -->
    <!ATTLIST VulnerabilityDetailRequest vuln-id CDATA #REQUIRED>
]>
```

VulnerabilityDetailsResponse

```
<!DOCTYPE VulnerabilityDetailsResponse [
<!ELEMENT VulnerabilityDetailsResponse (Failure|Vulnerability)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST VulnerabilityDetailsResponse success (0|1) #REQUIRED>
<!ELEMENT Vulnerability (description, references, solution)>
    <!ATTLIST Vulnerability id CDATA #REQUIRED>
    <!ATTLIST Vulnerability title CDATA #REQUIRED>
    <!ATTLIST Vulnerability severity CDATA #REQUIRED>
    <!ATTLIST Vulnerability pciSeverity CDATA #REQUIRED>
    <!ATTLIST Vulnerability cvssScore CDATA #IMPLIED >
    <!ATTLIST Vulnerability cvssVector CDATA #IMPLIED >
    <!-- the published date and time is in ISO 8601 format,
    YYYYMMDDTHHMMSSsss, such as: 19981231T00000000 -->
    <!ATTLIST Vulnerability published CDATA #IMPLIED >
    <!-- the added date and time is in ISO 8601 format,
    YYYYMMDDTHHMMSSsss, such as: 19981231T00000000 -->
    <!ATTLIST Vulnerability added CDATA #REQUIRED>
    <!-- the modified date and time is in ISO 8601 format,
    YYYYMMDDTHHMMSSsss, such as: 19981231T00000000 -->
    <!ATTLIST Vulnerability modified CDATA #REQUIRED>
<!ELEMENT description (#PCDATA)>
<!ELEMENT references (reference*)>
<!ELEMENT reference (#PCDATA)>
    <!-- the source of the reference, such as cve, bid, mskb, etc -->
    <!ATTLIST reference source CDATA #REQUIRED>
<!ELEMENT solution (#PCDATA)>
]>
```

Reporting

ReportTemplateListing

Provide a list of all report templates the user can access on the Security Console.

ReportTemplateListing

```
<!DOCTYPE ReportTemplateListingRequest [
<!ELEMENT ReportTemplateListingRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST ReportTemplateListingRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST ReportTemplateListingRequest session-id CDATA #REQUIRED>
]>
```

ReportTemplateListingResponse

```
<!DOCTYPE ReportTemplateListingResponse [
<!ELEMENT ReportTemplateListingResponse
(Failure|ReportTemplateSummary*)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST ReportTemplateListingResponse success (0|1) #REQUIRED>
<!-- See the ReportTemplateSummary DTD for more details -->
]>
```

ReportTemplateConfig

Retrieve the configuration for a report template.

ReportTemplateConfigRequest

```
<!DOCTYPE ReportTemplateConfigRequest [
<!ELEMENT ReportTemplateConfigRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST ReportTemplateConfigRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST ReportTemplateConfigRequest session-id CDATA #REQUIRED>
    <!-- the ID of the report template to retrieve the config for -->
    <!ATTLIST ReportTemplateConfigRequest template-id CDATA #REQUIRED>
]>
```

ReportTemplateConfigResponse

```
<!DOCTYPE ReportTemplateConfigResponse [
<!ELEMENT ReportTemplateConfigResponse (Failure|ReportTemplate)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST ReportTemplateConfigResponse success (0|1) #REQUIRED>
<!-- See the ReportTemplate DTD for more details -->
]>
```

ReportTemplateSave

Save the configuration for a report template.

ReportTemplateSaveRequest

If the user attempts to save a report with a scope of “silo” without being logged into a silo, an error occurs.

```
<!DOCTYPE ReportTemplateSaveRequest [
<!ELEMENT ReportTemplateSaveRequest (ReportTemplate)>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST ReportTemplateSaveRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST ReportTemplateSaveRequest session-id CDATA #REQUIRED>
    <!-- the visibility (scope) of the report template -->
    <!ATTLIST ReportTemplateSaveRequest scope (global|silo) #IMPLIED>
<!-- See the ReportTemplate DTD for more details -->
]>
```

ReportTemplateSaveResponse

```
<!DOCTYPE ReportTemplateSaveResponse [
<!ELEMENT ReportTemplateSaveResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
```

```
        <!ATTLIST ReportTemplateSaveResponse success (0|1) #REQUIRED>
        <!-- the newly assigned report template ID (unchanged for existing
        report templates) -->
        <!ATTLIST ReportTemplateSaveResponse template-id CDATA #REQUIRED>
    ]>
```

ReportListing

Provide a listing of all report definitions the user can access on the Security Console.

ReportListingRequest

```
    <!DOCTYPE ReportListingRequest [
    <!ELEMENT ReportListingRequest EMPTY>
        <!-- user defined synchronization token id used to avoid duplicate
        requests -->
        <!ATTLIST ReportListingRequest sync-id CDATA #IMPLIED>
        <!-- the current session id -->
        <!ATTLIST ReportListingRequest session-id CDATA #REQUIRED>
    ]>
```

ReportListingResponse

```
    <!DOCTYPE ReportListingResponse [
    <!ELEMENT ReportListingResponse (Failure|ReportConfigSummary*)>
        <!-- set to 1 upon success, 0 otherwise -->
        <!ATTLIST ReportListingResponse success (0|1) #REQUIRED>
    <!-- See the ReportConfigSummary DTD for more details -->
    ]>
```

ReportHistory

Provide a history of all reports generated with the specified report definition.

ReportHistoryRequest

```
<!DOCTYPE ReportHistoryRequest [
<!ELEMENT ReportHistoryRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST ReportListingRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST ReportHistoryRequest session-id CDATA #REQUIRED>
    <!-- the report definition id -->
    <!ATTLIST ReportHistoryRequest reportcfg-id CDATA #REQUIRED>
]>
```

ReportHistoryResponse

```
<!DOCTYPE ReportHistoryResponse [
<!ELEMENT ReportHistoryResponse (Failure|ReportSummary*)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST ReportListingResponse success (0|1) #REQUIRED>
<!-- See the ReportSummary DTD for more details -->
]>
```

ReportConfig

Retrieve the configuration for a report definition.

ReportConfigRequest

```
<!DOCTYPE ReportConfigRequest [
<!ELEMENT ReportConfigRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST ReportConfigRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST ReportConfigRequest session-id CDATA #REQUIRED>
    <!-- the ID of the report to retrieve the config for -->
    <!ATTLIST ReportConfigRequest reportcfg-id CDATA #REQUIRED>
]>
```

ReportConfigResponse

```
<!DOCTYPE ReportConfigResponse [
<!ELEMENT ReportConfigResponse (Failure|ReportConfig)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST ReportConfigResponse success (0|1) #REQUIRED>
<!-- See the ReportConfig DTD for more details -->
]>
```

ReportSave

Save the configuration for a report definition.

ReportSaveRequest

```
<!DOCTYPE ReportSaveRequest [
<!ELEMENT ReportSaveRequest (ReportConfig)>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST ReportSaveRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST ReportSaveRequest session-id CDATA #REQUIRED>
    <!-- Should the report be generated now? This is checked only if
    the report is NOT
    scheduled or scan based. -->
    <!ATTLIST ReportSaveRequest generate-now (0|1) "1">
<!-- See the ReportConfig DTD for more details -->
]>
```

ReportSaveResponse

```
<!DOCTYPE ReportSaveResponse [
<!ELEMENT ReportSaveResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST ReportSaveResponse success (0|1) #REQUIRED>
    <!-- the newly assigned report config ID (unchanged for existing
    reports) -->
    <!ATTLIST ReportSaveResponse reportcfg-id CDATA #REQUIRED>
]>
```

ReportGenerate

Generate a new report using the specified report definition.

ReportGenerateRequest

```
<!DOCTYPE ReportGenerateRequest [
<!ELEMENT ReportGenerateRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST ReportGenerateRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST ReportGenerateRequest session-id CDATA #REQUIRED>
    <!ATTLIST ReportGenerateRequest report-id CDATA #REQUIRED>
]>
```

ReportGenerateResponse

```
<!DOCTYPE ReportGenerateResponse [
<!ELEMENT ReportGenerateResponse (Failure|ReportSummary)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST ReportGenerateResponse success (0|1) #REQUIRED>
<!-- See the ReportSummary DTD for more details -->
]>
```

ReportDelete

Delete a previously generated report or report definition.

ReportDeleteRequest

```
<!DOCTYPE ReportDeleteRequest [
<!ELEMENT ReportDeleteRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST ReportDeleteRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST ReportDeleteRequest session-id CDATA #REQUIRED>
    <!-- the report definition id to remove the definition and all
    reports generated with the definition -->
    <!ATTLIST ReportDeleteRequest reportcfg-id CDATA #IMPLIED>
    <!-- the id of the generated report to remove -->
    <!ATTLIST ReportDeleteRequest report-id CDATA #IMPLIED>
]>
```

ReportDeleteResponse

```
<!DOCTYPE ReportDeleteResponse [
<!ELEMENT ReportDeleteResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST ReportDeleteResponse success (0|1) #REQUIRED>
]>
```

ReportAdhocGenerate

Generate a report once using a simple configuration, and send it back in a multi-part mime response.

ReportAdhocGenerateRequest

```
<!DOCTYPE ReportAdhocGenerateRequest [
<!ELEMENT ReportAdhocGenerateRequest (AdhocReportConfig)>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST ReportAdhocGenerateRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST ReportAdhocGenerateRequest session-id CDATA #REQUIRED>
<!-- With the site, device, and group filters you determine which
assets to include in the report. With the vuln-severity and vuln-status
filters you control which vulnerabilities to include in the report. -->
<!ELEMENT AdhocReportConfig (Filters, Baseline?) >
    <!-- the id of the report template used -->
    <!ATTLIST AdhocReportConfig template-id CDATA #REQUIRED>
    <!ATTLIST AdhocReportConfig format (pdf|html|rtf|xml|text|csv|raw-
    xml|raw-xml-v2|
    ns-xml|qualys-xml) #REQUIRED>
<!-- The configuration must include at least one of device (asset),
site, group (asset group) or scan filter to define the scope of report.
The vuln-status filter can be used only with raw report formats: csv or
raw_xml. If the vuln-status filter is not included in the
configuration, all the vulnerability test results (including
invulnerable instances) are exported by default in csv and raw_xml
reports. -->
<!ELEMENT Filters (filter+)>
<!ELEMENT filter EMPTY>
    <!ATTLIST filter type (site|group|device|scan|vuln-severity|vuln-
    categories|vuln-status|
    cyberscope-component|cyberscope-bureau|cyberscope-enclave|tag)
    #REQUIRED>
<!-- the ID of a specific site, group, device or scan.
For scan, this can also be "last" for the most recently run scan
For vuln-status, the ID can have one of the following values:
1) vulnerable-exploited (The check was positive. An exploit verified
the vulnerability.)
2) vulnerable-version (The check was positive. The version of the
scanned service or software is associated with known vulnerabilities.)
3) potential (The check for a potential vulnerability was positive.)
These values are supported for CSV and XML formats.
-->
<!-- For vuln-categories, the required format is include/exclude:
[category_from_approved_list]
Examples:
include:Adobe,Microsoft
exclude:Windows,Oracle -->
    <!ATTLIST filter id CDATA #REQUIRED>
<!ELEMENT Baseline EMPTY>
```

```
<!-- the date to use as the baseline scan in ISO 8601 format,
YYYYMMDDTHHMMSSss, such as:
19981231T00000000. Additionally, "first" can be used for the first run
scan, or "previous" for the most recently run scan prior to the current
scan. Note that the Baseline compareTo attribute is optional unless you
are creating a Baseline Comparison report, Executive Overview report,
or a cus- tom report that incorporates the Baseline Comparison section,
in which case the attribute is required.-->
    <!ATTLIST Baseline compareTo CDATA #IMPLIED>
]>
```

ReportAdhocGenerateResponse

Response to ReportAdhocGenerateRequest is a Multipart Mime message where the first part is 'response_xml' which contains the following xml element:

```
<!DOCTYPE ReportAdhocGenerateResponse [
<!ELEMENT ReportAdhocGenerateResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST ReportAdhocGenerateResponse success (0|1) #REQUIRED>
]>
```

The rest of the parts of the multipart mime contain the actual report files depending upon how many files are there. All these files are encoded using the base64 format.

User management functions

Only Global Administrators can use these functions.

UserListing

Provide a list of user accounts and information about those accounts.

UserListingRequest DTD

```
<!DOCTYPE UserListingRequest [
    <!ELEMENT UserListingRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST UserListingRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST UserListingRequest session-id CDATA #REQUIRED>
]>
```

UserListingRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<UserListingRequest session-id="${Login#Response#//LoginResponse[1]
/@session-id}" />
```

UserListingResponse DTD

```
<!DOCTYPE UserListingResponse [
<!ELEMENT UserListingResponse (Failure|UserSummary*)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST UserListingResponse success (0|1) #REQUIRED>
]>
```

UserListingResponse sample

```
<UserListingResponse success="1">
    <UserSummary id="1" authSource="Builtin Administrators"
    authModule="XML" userName="nxadmin" fullName="nxadmin" email=""
    administrator="1" disabled="0" locked="0" siteCount="2"
    groupCount="0"/>
    <UserSummary id="7" authSource="Builtin Users"
    authModule="DataStore" userName="SoapUIfc02724b-d420-4cca-9e8d-
    d29ba7213291" fullName="boonuser" email="user@example.com"
    administrator="0" disabled="0" locked="0" siteCount="0"
    groupCount="0"/>
    <UserSummary id="13" authSource="Builtin Users"
    authModule="DataStore" userName="SoapUI2b0c9fad-ed39-4046-bb59-
    b9d99b3073a1" fullName="boonuser" email="user@example.com"
    administrator="0" disabled="0" locked="0" siteCount="0"
    groupCount="0"/>
</UserListingResponse>
```

UserAuthenticatorListing

Provide a list of user authentication sources.

UserAuthenticatorListingRequest DTD

```
<!DOCTYPE UserAuthenticatorListingRequest [
<!ELEMENT UserAuthenticatorListingRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST UserAuthenticatorListingRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST UserAuthenticatorListingRequest session-id CDATA
    #REQUIRED>
]>
```

UserAuthenticatorListingRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
    <UserAuthenticatorListingRequest session-
    id="${Login#Response#//LoginResponse[1]/@session-id}" />
```

UserAuthenticatorListingResponse DTD

```
<!DOCTYPE UserAuthenticatorListingResponse [
<!ELEMENT UserAuthenticatorListingResponse
(Failure|AuthenticatorSummary*)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST UserAuthenticatorListingResponse success (0|1) #REQUIRED>
]>
```

UserAuthenticatorListingResponse sample

```
<UserAuthenticatorListingResponse success="1">
    <AuthenticatorSummary id="1" authSource="Builtin Administrators"
    authModule="XML"/>
    <AuthenticatorSummary id="2" authSource="Builtin Users"
    authModule="DataStore"/>
</UserAuthenticatorListingResponse>
```

UserConfig

List information about a given user account.

DTD

```
<!DOCTYPE UserConfigRequest [
<!ELEMENT UserConfigRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST UserConfigRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST UserConfigRequest session-id CDATA #REQUIRED>
    <!-- the id of the user to retrieve the config for -->
    <!ATTLIST UserConfigRequest id CDATA #REQUIRED>
]>
```

UserConfigRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<UserConfigRequest session-id="${Login#Response#//LoginResponse[1]
/@session-id}" id = "1" />
```

UserConfigResponse DTD

```
<!DOCTYPE UserConfigResponse [
<!ELEMENT UserConfigResponse (Failure|UserConfig)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST UserConfigResponse success (0|1) #REQUIRED>
<!-- See the UserConfig DTD for more details. Note: a user's password
will never be included in the response -->
]>
```

UserConfigResponse sample

```
<UserConfigResponse success="1">
    <UserConfig id="14" role-name="user" authsrcid="2"
    name="testb2739f90-5438-4e64-be4c-28c257e1c792"
    fullname="SOAPUIUserb2739f90-5438-4e64-be4c-28c257e1c792"
    email="user@example.com" enabled="1"/>
</UserConfigResponse>
```

UserSave

Create a new user account, or update the settings for an existing account. Note that specifying a UserConfig with an id of -1 indicates a create request.UserSaveRequest

It is not possible to create user accounts with custom roles, but it is possible to query these accounts with UserListing or UserConfig.

You cannot change the user name after you create an account. Therefore, the user name that you specify in the update request must be the current user name.

UserSaveRequest DTD

```
<!DOCTYPE UserSaveRequest [
<!ELEMENT UserSaveRequest UserConfig>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST UserSaveRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST UserSaveRequest session-id CDATA #REQUIRED>
<!-- See the UserConfig DTD for more details -->
]>
```

UserSaveRequest sample

```
<UserSaveRequest session-id="${Login#Response#//LoginResponse[1]
/@session-id}">
<UserConfig id="-1" role-name="user" authsrcid="2" name="test${Groovy
Script#result}" fullname="SOAPUIUser${Groovy Script#result}" password =
"password" email="user@example.com" enabled="1">
</UserConfig>
</UserSaveRequest>
```

UserSaveResponse

```
<!DOCTYPE UserSaveResponse [
<!ELEMENT UserSaveResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST UserSaveResponse success (0|1) #REQUIRED>
    <!-- the id of the user created or updated -->
    <!ATTLIST UserSaveResponse user-id CDATA #REQUIRED>
]>
```

UserSaveResponse sample

```
<UserSaveResponse success="1" id="14"></UserSaveResponse>
```

UserDelete

Delete a user account. Note that you cannot delete a user account that is associated with reports or tickets.

UserDeleteRequest DTD

```
<!DOCTYPE UserDeleteRequest [
<!ELEMENT UserDeleteRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST UserDeleteRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST UserDeleteRequest session-id CDATA #REQUIRED>
    <!-- the ID of the user to delete -->
    <!ATTLIST UserDeleteRequest id CDATA #REQUIRED>
]>
```

UserDeleteRequest sample

```
<UserDeleteRequest session-id="${Login#Response#//LoginResponse[1]
/@session-id}" id="${UserSave#ResponseAsXml#//UserSaveResponse[1]/@id}"
>
</UserDeleteRequest>
```

UserDeleteResponse DTD

Note: You cannot delete your own user account.

```
<!DOCTYPE UserDeleteResponse [
<!ELEMENT UserDeleteResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST UserDeleteResponse success (0|1) #REQUIRED>
]>
```

UserDeleteResponse sample

```
<UserDeleteResponse success="1"></UserDeleteResponse>
```

General management and diagnostic functions

ConsoleCommand

Execute an arbitrary console command that is supplied as text via an API parameter. Console commands are documented in the administrator's guide and in Help. If you use a command that is not listed in the in administrator's guide, the application will return the XMLResponse.

ConsoleCommandRequest DTD

```
<!DOCTYPE ConsoleCommandRequest[
<!ELEMENT ConsoleCommandRequest (Command)>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST ConsoleCommandRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST ConsoleCommandRequest session-id CDATA #REQUIRED>
<!ELEMENT Command CDATA #REQUIRED>
]>
```

ConsoleCommandResponse DTD

```
<!DOCTYPE ConsoleCommandResponse[
<!ELEMENT ConsoleCommandResponse (Command,Output)>
    <!-- set to 1 upon success, 0 otherwise -->
        <!ATTLIST ConsoleCommandResponse success (0|1) #REQUIRED>
<!ELEMENT Command CDATA #REQUIRED>
<!ELEMENT Output CDATA #REQUIRED>
]>
```

Tip: Set a higher timeout value for a command that requires a substantial amount of time to execute and finish. Doing so ensures that the application has sufficient time to respond to the command.

SystemInformation

Obtain system data, such as total RAM, free RAM, total disk space, free disk space, CPU speed, number of CPU cores, and other vital information.

SystemInformationRequest DTD

```
<!DOCTYPE SystemInformationRequest[
<!ELEMENT SystemInformationRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST SystemInformationRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST SystemInformationRequest session-id CDATA #REQUIRED>
]>
```

SystemInformationRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<SystemInformationRequest session-id="${Login#Response#//LoginResponse
[1]/@session-id}">
</SystemInformationRequest>
```

SystemInformationResponse DTD

```
<!DOCTYPE SystemInformationResponse[
<!ELEMENT SystemInformationResponse (SystemInformationSummary)>
    <!ATTLIST SystemInformationResponse success (0|1) #REQUIRED>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ELEMENT SystemInformationSummary (Statistic*)>
        <!ELEMENT Statistic CDATA #IMPLIED>
            <!ATTLIST Statistic name (cpu-count|cpu-speed|disk-
            install|java-name|
            jre-version|last-update-date|last-update-id|disk-tmp|nsc-
            name|nsc-version|nse-version|os|ram-free|ram-total|up-
            time|db-product|db-version|java-heap-max|java-heap-
            committed|java-heap-free|java-heap-used|java-total-thread-
            count|java-started-thread-count|java-thread-peak-count|java-
            daemon-thread-count) #IMPLIED>
]>
```

SystemInformationResponse sample

```
<SystemInformationResponse success="1">
    <StatisticsInformationSummary>
        <Statistic name="cpu-count">2</Statistic>
        <Statistic name="cpu-speed">2660</Statistic>
        <Statistic name="disk-
        install">/opt/rapid7/nexpose=32901904</Statistic>
        <Statistic name="disk-tmp">../shared/temp=32901904</Statistic>
        <Statistic name="os">Ubuntu Linux 12.04</Statistic>
        <Statistic name="ram-free">170376</Statistic>
        <Statistic name="ram-total">8177868</Statistic>
        <Statistic name="up-time">45757264</Statistic>
        <Statistic name="db-product">postgresql</Statistic>
        <Statistic name="db-version">PostgreSQL 9.0.13 on x86_64-
        unknown-linux-gnu, compiled by GCC gcc (GCC) 4.1.2 20080704 (Red
        Hat 4.1.2-52), 64-bit</Statistic>
        <Statistic name="java-name">Java HotSpot(TM) 64-Bit Server
        VM</Statistic>
        <Statistic name="java-heap-max">6263537664</Statistic>
        <Statistic name="java-heap-committed">4829077504</Statistic>
        <Statistic name="java-heap-free">3694844920</Statistic>
        <Statistic name="java-heap-used">2568692744</Statistic>
        <Statistic name="jre-version">24.0-b56</Statistic>
        <Statistic name="nsc-name">CN=NeXpose Security Console,
        O=Rapid7</Statistic>
        <Statistic name="nsc-version">5.12.2</Statistic>
        <Statistic name="last-update-date">1423140440496</Statistic>
        <Statistic name="last-update-id">1028948869</Statistic>
        <Statistic name="java-daemon-thread-count">44</Statistic>
        <Statistic name="java-total-thread-count">67</Statistic>
        <Statistic name="java-thread-peak-count">118</Statistic>
        <Statistic name="java-started-thread-count">4950</Statistic>
    </StatisticsInformationSummary>
</SystemInformationResponse>
```

StartUpdate

Induce the application to retrieve required updates and restart if necessary.

StartUpdateRequest DTD

```
<!DOCTYPE StartUpdateRequest[
<!ELEMENT StartUpdateRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST StartUpdateRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST StartUpdateRequest session-id CDATA #REQUIRED>
]>
```

StartUpdateResponse DTD

Set a higher timeout value for a command that requires a substantial amount of time to execute and finish. Doing so ensures that the application has sufficient time to respond to the command.

```
<!DOCTYPE StartUpdateResponse[
<!ELEMENT StartUpdateResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST StartUpdateResponse success (0|1) #REQUIRED>
```

Restart

Restart the application.

RestartRequest DTD

```
<!DOCTYPE RestartRequest[
<!ELEMENT RestartRequest EMPTY>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST RestartRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST RestartRequest session-id CDATA #REQUIRED>
]>
```

RestartRequest sample

```
<?xml version="1.0" encoding="utf-8"?>
<ConsoleCommandRestart session-id="${Login#Response#//LoginResponse[1]
/@session-id}">
    <Command>restart</Command>
</ConsoleCommandRequest>
```

RestartResponse

There is no response to RestartRequest. When the application shuts down as part of the restart process, it terminates any active connections. Therefore, the application cannot issue a response when it restarts.

SendLog

Output diagnostic information into log files, zip the files, and encrypt the archive with a PGP public key that is provided as a parameter for the API call. Then, either e-mail this archive to an address that is specified as an API parameter, or upload the archive using HTTP or HTTPS to a URL that is specified as an API parameter.

If you do not specify a key, the SendLogRequest uses a default key.

SendLogRequest DTD

```
<!DOCTYPE SendLogRequest[
<!ELEMENT SendLogRequest (Transport)>
    <!-- user defined synchronization token id used to avoid duplicate
    requests -->
    <!ATTLIST SendLogRequest sync-id CDATA #IMPLIED>
    <!-- the current session id -->
    <!ATTLIST SendLogRequest session-id CDATA #REQUIRED>
    <!ATTLIST SendLogRequest keyid CDATA #IMPLIED>
<!ELEMENT Transport (Email|URL)>
    <!ATTLIST Transport protocol CDATA #REQUIRED (smtp|http|https)>
<!-- If protocol== "smtp" -->
    <!—- See the Email DTD for more details -->
<!-- If protocol == "http" || "https" -->
    <!ELEMENT URL CDATA #REQUIRED>
]>
```

SendLogResponse DTD

```
<!DOCTYPE SendLogResponse[
<!ELEMENT SendLogResponse (Failure?)>
    <!-- set to 1 upon success, 0 otherwise -->
    <!ATTLIST SendLogResponse success (0|1) #REQUIRED>
]>
```

DTD listings

This section includes DTDs for validating the API calls listed throughout this document.

Device DTD

```
<!DOCTYPE device [
<!ELEMENT device (description?)>
    <!-- the ID of the device -->
    <!ATTLIST device id CDATA #REQUIRED>
    <!-- the ID of the site the device belongs to -->
    <!ATTLIST device site-id CDATA #IMPLIED>
    <!-- the primary address or hostname of the device -->
    <!ATTLIST device address CDATA #IMPLIED>
    <!-- the current riskfactor (weighting) for the device -->
    <!ATTLIST device riskfactor CDATA "1.0">
    <!-- the current risk score of the device -->
    <!ATTLIST device riskscore CDATA #IMPLIED>
]>
```

SiteSummary DTD

```
<!DOCTYPE SiteSummary [
<!ELEMENT SiteSummary EMPTY>
    <!ATTLIST SiteSummary id CDATA #REQUIRED>
    <!ATTLIST SiteSummary name CDATA #REQUIRED>
    <!ATTLIST SiteSummary description CDATA #IMPLIED>
    <!ATTLIST SiteSummary riskfactor CDATA "1.0">
    <!-- The riskscore stored in the application is a computed value
    equal to riskscore * riskfactor. The risk scores are only computed
    after the site is scanned. This presents a problem when the site
    administrator changes the site riskfactor. To account for changing
    the riskfactor take the existing computed riskscore divide by the
    old riskfactor and multiply by the new riskfactor.-->
    <!ATTLIST SiteSummary riskscore CDATA "0.0">
]>
```

Site DTD

This DTD continues on the following three pages.

Note: Only enter DNS names in the *host* element. Do not enter an IP address in that element. Use the *range* element for IP address ranges. For a single IP address, use the *range* element where the *from* value is the IP address and the *to* value is empty.

```
<!DOCTYPE Site [
<!ELEMENT Site (Hosts, Credentials, Alerting, ScanConfig, Tags)>
    <!—Use id="-1" to create a new Site -->
    <!ATTLIST Site id CDATA #REQUIRED>
    <!ATTLIST Site name CDATA #REQUIRED>
    <!ATTLIST Site description CDATA #IMPLIED>
    <!ATTLIST Site riskfactor CDATA "1.0">
<!ELEMENT Hosts ((range|host)+)>
<!-- IPv4 address range of the form 10.0.0.1 -->
<!ELEMENT range EMPTY>
    <!ATTLIST range from CDATA #REQUIRED>
    <!ATTLIST range to CDATA #IMPLIED>
<!-- named host (usually DNS or Netbios name -->
<!ELEMENT host (#PCDATA)>
<!ELEMENT Credentials (adminCredentials*)>
<!ELEMENT adminCredentials (#PCDATA|Headers|HTMLForms|PEMKey)>
    <!-- cifs Concurrent Versioning System (CVS) -->
    <!-- ftp File Transfer Protocol (FTP) -->
    <!-- http HyperText Transfer Protocol (HTTP) -->
    <!-- htmlform Web form authentication -->
    <!-- httpheaders HTTP session authentication -->
    <!-- as400 IBM AS/400 -->
    <!-- notes Lotus Notes/Domino -->
    <!-- tds Microsoft SQL Server -->
    <!-- sybase Sybase SQL Server -->
    <!-- cifs Microsoft Windows/Samba (SMB/CIFS) -->
    <!-- oracle Oracle -->
    <!-- mysql MySQL Server -->
    <!-- db2 IBM DB2 Server -->
    <!-- postgresql PostgreSQL Server -->
    <!-- pop Post Office Protocol (POP) -->
    <!-- remote execution Remote Execution -->
    <!-- snmp Simple Network Management Protocol -->
    <!-- ssh Secure Shell (SSH) -->
    <!-- ssh-key Secure Shell (SSH) Public Key -->
    <!-- telnet TELNET -->
<!ATTLIST adminCredentials service CDATA #REQUIRED
(cvs|ftp|http|as400|notes|htmlform|httpheaders|tds|sybase|cifs|oracle|m
ysql|db2|pop|postgresql|
remote execution|snmp|ssh|ssh-key|telnet)>
<!ATTLIST adminCredentials host CDATA #IMPLIED>
    <!ATTLIST adminCredentials port CDATA #IMPLIED>
<!-- the userid, password and realm attributes should ONLY be used
```

```
if a security blob cannot be generated and the data is being
transmitted/stored using external encryption (eg, HTTPS)
SiteSaveRequest doesn't handle the security blob right now
So username/password attributes should be used in that case-->
<!ATTLIST adminCredentials USERID CDATA #IMPLIED>
<!ATTLIST adminCredentials PASSWORD CDATA #IMPLIED>
<!-- when using snmp assign the community name to the password
attribute -->
<!ATTLIST adminCredentials realm CDATA #IMPLIED>
<!-- when using httpheaders, this represents the set of headers to pass
with the
authentication request -->
<!ELEMENT Headers (Header+)>
<!-- A regular expression used to match against the response to
identify authentication
failures. -->
    <!ATTLIST Headers soft403 CDATA #IMPLIED>
<!-- the base URL of the application for which the form authentication
applies. -->
    <!ATTLIST Headers webapproot CDATA #IMPLIED>
<!ELEMENT Header (#PCDATA)>
    <!ATTLIST Header name CDATA #REQUIRED>
    <!ATTLIST Header value CDATA #IMPLIED>
    <!-- when using htmlform, this represents the login form
    information -->
<!ELEMENT HTMLForms (HTMLForm+)>
    <!-- the URL of the login page containing the login form -->
    <!ATTLIST HTMLForms parentpage CDATA #IMPLIED>
    <!-- A regular expression used to match against the response to
    identify
    authentication failures. -->
    <!ATTLIST HTMLForms soft403 CDATA #IMPLIED>
    <!-- the base URL of the application for which the form
    authentication applies. -->
    <!ATTLIST HTMLForms webapproot CDATA #IMPLIED>
<!ELEMENT HTMLForm (Field*)>
    <!-- the name of the form being submitted -->
    <!ATTLIST HTMLForm name CDATA #IMPLIED>
    <!-- the HTTP action (URL) through which to submit the login form -
    ->
    <!ATTLIST HTMLForm action CDATA #REQUIRED>
    <!-- the HTTP request method with which to submit the form -->
    <!ATTLIST HTMLForm method CDATA #IMPLIED>
    <!-- the HTTP encoding type with which to submit the form -->
    <!ATTLIST HTMLForm enctype CDATA #IMPLIED>
<!ELEMENT Field (#PCDATA)>
    <!-- the name of the HTML field (form parameter) -->
    <!ATTLIST Field name CDATA #IMPLIED>
    <!-- the value of the HTML field (form parameter) -->
    <!ATTLIST Field value CDATA #IMPLIED>
    <!-- the type of the HTML field (form parameter) -->
    <!ATTLIST Field type CDATA #IMPLIED>
    <!-- is the HTML field (form parameter) dynamically generated? If
    so, the login
    page is requested and the value of the field is extracted from the
    response. -->
    <!ATTLIST Field dynamic CDATA #IMPLIED>
    <!-- if the HTML field (form parameter) is a radio button, checkbox
    or select field,
    this flag determines if the field should be checked (selected) -->
    <!ATTLIST Field checked CDATA #IMPLIED>
    <!-- when using ssh-key, this represents the PEM-format keypair
    information -->
<!ELEMENT PEMKey (#PCDATA)>
<!ELEMENT Alerting (Alert*)>
<!ELEMENT Alert (scanFilter?, vulnFilter?,
(smtpAlert|snmpAlert|syslogAlert))>
    <!ATTLIST Alert name CDATA #REQUIRED>
    <!ATTLIST Alert enabled (0|1) "0">
    <!ATTLIST Alert maxAlerts CDATA>
<!ELEMENT scanFilter (#PCDATA)>
    <!ATTLIST scanFilter scanStart (0|1) "0">
    <!ATTLIST scanFilter scanStop (0|1) "0">
    <!ATTLIST scanFilter scanFailed (0|1) "0">
    <!ATTLIST scanFilter scanPaused (0|1) "0">
    <!ATTLIST scanFilter scanResumed (0|1) "0">
<!ELEMENT vulnFilter EMPTY>
    <!-- severityThreshold defaults to 1. Currently the application
    only supports values of 1 (Any Severity), 4 (Severe and Critical)
    and 8 (Only Critical). >
    <!ATTLIST vulnFilter severityThreshold (1|2|3|4|5|6|7|8|9|10)
    #REQUIRED>
    <!ATTLIST vulnFilter confirmed (0|1) "1">
    <!ATTLIST vulnFilter unconfirmed (0|1) "1">
<!ELEMENT smtpAlert (recipient+)>
    <!ATTLIST smtpAlert sender CDATA #IMPLIED>
    <!ATTLIST smtpAlert server CDATA #IMPLIED>
    <!ATTLIST smtpAlert port CDATA "25">
    <!ATTLIST smtpAlert limitText (0|1) "0">
<!ELEMENT recipient (#PCDATA)>
<!ELEMENT snmpAlert EMPTY>
    <!ATTLIST snmpAlert community CDATA>
    <!ATTLIST snmpAlert server CDATA #REQUIRED>
    <!ATTLIST snmpAlert port CDATA "162">
```

```
<!ELEMENT syslogAlert EMPTY>
<!ATTLIST syslogAlert server CDATA #REQUIRED>
<!ATTLIST syslogAlert port CDATA "514">
<!ELEMENT Users (user+)>
<!ELEMENT user EMPTY>
    <!-- the ID of a non-admin user who has access to this site -->
    <!ATTLIST user id CDATA #REQUIRED>
    <!-- See the ScanConfig DTD for more details -->
<!ELEMENT Tags (Tag+) >
<!ELEMENT Tag (param+) >
    <!-- Use id="-1" to create a new tag -->
    <!ATTLIST Tag id CDATA #REQUIRED>
    <!-- the name of the tag. -->
    <!ATTLIST Tag name CDATA #REQUIRED>
    <!-- the type of the tag. -->
    <!ATTLIST Tag type CDATA #REQUIRED
    (general|location|owner|criticality)>
<! ELEMENT Param>
    <!ATTLIST Param name CDATA #REQUIRED(source|color)>
    <!ATTLIST Param value CDATA #REQUIRED>
```

AssetGroupSummary DTD

```
<!DOCTYPE AssetGroupSummary [
<!ELEMENT AssetGroupSummary EMPTY>
    <!ATTLIST AssetGroupSummary id CDATA #REQUIRED>
    <!ATTLIST AssetGroupSummary name CDATA #REQUIRED>
    <!ATTLIST AssetGroupSummary description CDATA #IMPLIED>
    <!ATTLIST AssetGroupSummary riskscore CDATA #IMPLIED>
]>
```

AssetGroup DTD

```
<!DOCTYPE AssetGroup [
<!ELEMENT AssetGroup (Devices)>
    <!-- Use id="-1" to create a new Asset Group -->
    <!ATTLIST AssetGroup id CDATA #REQUIRED>
    <!ATTLIST AssetGroup name CDATA #REQUIRED>
    <!ATTLIST AssetGroup description CDATA #IMPLIED>
    <!ATTLIST AssetGroup riskscore CDATA #IMPLIED>
<!ELEMENT Devices (device+)>
    <!-- See the device DTD for more details -->
<!ELEMENT Users (user+)>
<!ELEMENT user EMPTY>
    <!-- the ID of a non-admin user who has access to this site -->
    <!ATTLIST user id CDATA #REQUIRED>
<!ELEMENT Tags (Tag+) >
<!ELEMENT Tag (param+) >
    <!-- Use id="-1" to create a new tag -->
    <!ATTLIST Tag id CDATA #REQUIRED>
    <!-- the name of the tag. -->
    <!ATTLIST Tag name CDATA #REQUIRED>
    <!-- the type of the tag. -->
    <!ATTLIST Tag type CDATA #REQUIRED
    (general|location|owner|criticality)>
<! ELEMENT Param>
    <!ATTLIST Param name CDATA #REQUIRED(source|color)>
    <!ATTLIST Param value CDATA #REQUIRED>
]>
```

EngineSummary DTD

Prior to the release dated October 15, 2008, EngineSummaryResponse always returned “unknown” for EngineStatus values. As of October 15, 2008, the EngineSummaryResponse may return a value other than “unknown.”

```
<!DOCTYPE EngineSummary [
<!ELEMENT EngineSummary EMPTY>
    <!ATTLIST EngineSummary id CDATA #REQUIRED>
    <!ATTLIST EngineSummary name CDATA #REQUIRED>
    <!ATTLIST EngineSummary address CDATA #REQUIRED>
    <!ATTLIST EngineSummary port CDATA #REQUIRED>
    <!-- current status of the Scan Engine -->
    <!ATTLIST EngineSummary status (Active|Pnding-auth|Incompatible|
    Not-responding|Unknown) #REQUIRED>
    <!-- the visibility (scope) of the Scan Engine -->
    <!ATTLIST ReportTemplateSummary scope (global|silo) #IMPLIED>
]>
```

ScanConfig DTD

```
<!DOCTYPE ScanConfig [

<!--This Schedules element is different from the element with the same
name in SiteDevicesScanRequest-->
<!ELEMENT ScanConfig (Schedules?)>
    <!ATTLIST ScanConfig configID CDATA>
    <!ATTLIST ScanConfig name CDATA>
    <!-- Specify the scan template to use when starting a scan job -->
    <!ATTLIST ScanConfig templateID CDATA #REQUIRED>
    <!-- the Scan Engine to use. Omit to use the default engine -->
    <!ATTLIST ScanConfig engineID CDATA #IMPLIED>
    <!ATTLIST ScanConfig configVersion (3) "3">

<!ELEMENT Schedules (Schedule*)>
<!-- To use multiple scan schedules in a site, include a Schedule
element for each desired schedule. Make sure not to schedule
overlapping scans with the same scan template. This will cause an
error. You can overlap scans with different templates.-->
<!ELEMENT Schedule EMPTY>
    <!ATTLIST Schedule enabled (0|1) "0">
    <!ATTLIST Schedule type (daily|hourly|monthly-date|monthly-
    day|weekly) #IMPLIED>
    <!ATTLIST Schedule interval CDATA>
    <!-- the earliest date to run the scan on in the following format,
    YYYYMMDDTHHMMSSsss, such as: 19981231T00000000 -->
    <!ATTLIST Schedule start CDATA #REQUIRED>
    <!-- the amount of time, in minutes, to allow execution before
    stopping -->
    <!ATTLIST Schedule maxDuration CDATA #IMPLIED>
    <!-- the date after which the schedule is disabled in the following
    format,
    YYYYMMDDTHHMMSSsss, such as: 19981231T00000000 -->
    <!ATTLIST Schedule notValidAfter CDATA #IMPLIED>
    <!-- Apply a specific scan template to a schedule. If you do not
    specify a template for a given schedule, the schedule will use the
    template specified for the site. -->
    <!ATTLIST Schedule template CDATA #IMPLIED>
    <!-- Set a schedule to be in effect as of the next applicable day
    or date as indicated in the following attributes. This makes it
    unnecessary to indicate a specific start date for a schedule. -->
    <!ATTLIST Schedule is-extended (false|true) #IMPLIED>
    <!-- The hour of the day that the schedule starts. If you do not
    specify an hour, the schedule will start at the top of the next
   hour. This attribute is only valid if the is-extended attribute is
   set to true. -->
    <!ATTLIST Schedule hour
    (1|2|3|4|5|6|7|8|9|10|11|12|13|14|15|16|17|18|19|20|21|22|23)
    #IMPLIED -->
    <!-- The minute of the hour that the schedule starts. If you do not
    specify a minute, the schedule will start at the top of the hour.
    This attribute is only valid if the is-extended attribute is set to
    true. -->
    <!ATTLIST Schedule minute
    (0|1|2|3|4|5|6|7|8|9|10|11|12|13|14|15|16|17|18|19|20|
    21|22|23|24|25|26|27|28|29|30|31|32|33|34|35|36|37|38|39|40|
    41|42|43|44|45|46|47|48|49|50|51|52|53|54|55|56|57|58|59) #IMPLIED>
    <!-- The date of the month that the schedule starts. Only valid if
    used with monthly-date and if the is-extended attribute is set to
    true. Required for monthly-date. If you do not include the date in
    the current or specified month, the request will return an error. -
    ->
    <!ATTLIST Schedule date
    (1|2|3|4|5|6|7|8|9|10|11|12|13|14|15|16|17|18|19|20|
    21|22|23|24|25|26|27|28|29|30|31|last) #IMPLIED>
    <!-- The day of the week that the schedule starts. Only valid if
    used with monthly-day or weekly and if the is-extended attribute is
    set to true. Required for monthly-day and weekly. -->
    <!ATTLIST Schedule day
    (monday|mon|tuesday|tue|wednesday|wed|thursday|thur
    friday|fri|saturday|sat|sunday|sun) #IMPLIED>
    <!-- The ordinal date of the month, such as third Saturday, that
    the schedule starts. Only valid if used with monthly-day and if the
    is-extended attribute is set to true. Required for monthly-day. -->
    <!ATTLIST Schedule occurrence (1|2|3|4|last) #IMPLIED>
    <!-- The month that the schedule starts. Only valid if used with
    monthly-date or monthly-day and if the is-extended attribute is set
    to true. -->
    <!ATTLIST Schedule start-month
    (january|jan|february|feb|march|mar|april|apr|may|june|jun|july|
    jul|august|aug|september|sep|october|oct|november|nov|december|
    dec) #IMPLIED>
]>
```

Examples of a scan schedules

The following schedule runs at 1:35 a.m. on the second Wednesday of every month, starting on the following April. If the scan exceeds the maximum duration of 60 minutes, it restarts from the beginning.

```
<Schedule enabled='1' is-extended='true' type='monthly-day' start_
month='April' occurrence='2' day='wednesday' hour='1' minute='35'
interval='10' maxDuration='60' repeaterType='restart' />
```

The following schedule runs weekly on Mondays, starting at 8 p.m.

```
<Schedule is-extended="true" interval="1" type="weekly" day="monday"
hour="20" interval='10' maxDuration='60' repeaterType='restart'/>
```

The following schedule starts at 8 p.m. on the 18th day of the current month.

```
<Schedule is-extended="true" interval="1" type="monthly-date" date="18"
hour="20"/>
```

ScanSummary DTD

```
<!DOCTYPE ScanSummary [
<!ELEMENT ScanSummary (message?, tasks?, nodes?, vulnerabilities*)>
    <!ATTLIST ScanSummary scan-id CDATA #REQUIRED>
    <!-- the site that was scanned -->
    <!ATTLIST ScanSummary site-id CDATA #REQUIRED>
    <!-- the engine the scan was dispatched to -->
    <!ATTLIST ScanSummary engine-id CDATA #REQUIRED>
    <!ATTLIST ScanSummary name CDATA #REQUIRED>
    <!-- the scan start date and time in ISO 8601 format,
    YYYYMMDDTHHMMSSsss, such as: 19981231T00000000 -->
    <!ATTLIST ScanSummary startTime CDATA #REQUIRED>
    <!-- the scan completion date and time in ISO 8601 format,
    YYYYMMDDTHHMMSSsss, such as: 19981231T00000000 -->
    <!ATTLIST ScanSummary endTime CDATA #IMPLIED>
    <!ATTLIST ScanSummary status (running|finished|stopped|error|
    dispatched|paused|aborted|unknown) #REQUIRED>
<!ELEMENT message (#PCDATA)>
<!ELEMENT tasks EMPTY>
    <!ATTLIST tasks pending CDATA #REQUIRED>
    <!ATTLIST tasks active CDATA #REQUIRED>
    <!ATTLIST tasks completed CDATA #REQUIRED>
<!ELEMENT nodes EMPTY>
    <!ATTLIST nodes live CDATA #REQUIRED>
    <!ATTLIST nodes dead CDATA #REQUIRED>
    <!ATTLIST nodes filtered CDATA #REQUIRED>
    <!ATTLIST nodes unresolved CDATA #REQUIRED>
    <!ATTLIST nodes other CDATA #REQUIRED>
<!ELEMENT vulnerabilities EMPTY>
    <!ATTLIST vulnerabilities status (vuln-exploit|vuln-version|
    vuln-potential| not-vuln-exploit| not-vuln-version|
    error|disabled|other)
    #REQUIRED>
    <!-- vulnerability severity (1-10, only provided with vuln-exploit
    and vuln-version status) -->
    <!ATTLIST vulnerabilities severity CDATA #IMPLIED>
    <!-- the number of vulnerabilities with the specified status and
    severity -->
    <!ATTLIST vulnerabilities count CDATA #REQUIRED>
]>
```

ReportTemplateSummary DTD

```
<!DOCTYPE ReportTemplateSummary [
<!ELEMENT ReportTemplateSummary (description?)>
    <!-- the id of the report template -->
    <!ATTLIST ReportTemplateSummary id CDATA #REQUIRED>
    <!-- the name of the report template -->
    <!ATTLIST ReportTemplateSummary name CDATA #REQUIRED>
    <!-- the visibility (scope) of the report template -->
    <!ATTLIST ReportTemplateSummary scope (global|silo) #IMPLIED>
    <!-- With a data template, you can export comma-separated value
    (CSV) files with vulnerability- based data. With a document
    template, you can create PDF, RTF, HTML, or XML reports with asset-
    based information. -->
    <!ATTLIST ReportTemplateSummary type (data|document) #REQUIRED>
    <!-- whether the report template is built-in, and therefore cannot
    be modified (0=false,
    1=true) -->
    <!ATTLIST ReportTemplateSummary builtin (0|1) #REQUIRED
<!ELEMENT description (#PCDATA)>
]>
```

ReportTemplate DTD

```
<!DOCTYPE ReportTemplate [
<!ELEMENT ReportTemplate (description?,ReportSections?,Settings)>
<!-- the id of the report template -->
    <!ATTLIST ReportTemplate id CDATA #REQUIRED>
    <!-- the name of the report template -->
    <!ATTLIST ReportTemplate name CDATA #REQUIRED>
    <!-- the visibility (scope) of the report template -->
    <!ATTLIST ReportTemplate scope (global|silo) #IMPLIED>
    <!-- With a data template, you can export comma-separated value
    (CSV) files with vulnerability- based data. With a document
    template, you can create PDF, RTF, HTML, or XML reports with asset-
    based information. When you retrieve a report template, the type
    will always be visible even though type is implied. When
    ReportTemplate
    is sent as a request, and the type attribute is not provided, the
    type attribute defaults to doc- ument, allowing for backward
    compatibility with existing API
    clients. -->
    <!ATTLIST ReportTemplateSummary type (data|document) #IMPLIED>
    <!-- the report template is built-in, and cannot be modified
    (0=false, 1=true) -->
    <!ATTLIST ReportTemplate builtin (0|1) #REQUIRED
<!ELEMENT description (#PCDATA)>
<!ELEMENT ReportSections (ReportSection+,property*)>
<!ELEMENT property (#PCDATA)>
    <!-- the name of the property -->
    <!ATTLIST property name CDATA #REQUIRED>
<!ELEMENT ReportSection (property*)>
    <!ATTLIST ReportSection name CDATA #REQUIRED>
    <!-- section specific content to include -->
<!ELEMENT property (#PCDATA)>
<!-- the name of the property -->
    <!ATTLIST property name CDATA #REQUIRED>
<!ELEMENT Settings(showDeviceNames)>
<!ELEMENT showDeviceNames EMPTY>
    <!ATTLIST showDeviceNames enabled (0|1) "0">
]>
```

ReportConfigSummary DTD

```
<!DOCTYPE ReportConfigSummary [
<!ELEMENT ReportConfigSummary EMPTY>
    <!-- the id of the report template -->
    <!ATTLIST ReportConfigSummary template-id CDATA #REQUIRED>
    <!-- the report definition (config) id -->
    <!ATTLIST ReportConfigSummary cfg-id CDATA #REQUIRED>
    <!-- the current status of the report -->
    <!ATTLIST ReportConfigSummary status
    (Started|Generated|Failed|Aborted|Unknown) #REQUIRED>
    <!-- the date and time the report was generated, in ISO 8601
    format, YYYYMMDDTHHMMSSsss, such as: 19981231T00000000 -->
    <!ATTLIST ReportConfigSummary generated-on CDATA #REQUIRED>
    <!-- the URL to use to access the report (not set for database
    exports) -->
    <!ATTLIST ReportConfigSummary report-URI CDATA #IMPLIED>
    <!ATTLIST ReportConfigSummary scope (global|silo) #IMPLIED>
]>
```

ReportConfig DTD

```
<!DOCTYPE ReportConfig [
<!ELEMENT ReportConfig (description?, Filters, Users, Baseline?,
Generate, Delivery, DBExport?)>
    <!-- the id of the report definition (config) -->
    <!ATTLIST ReportConfig id CDATA #REQUIRED>
    <!-- the unique name assigned to the report definition -->
    <!ATTLIST ReportConfig name CDATA #REQUIRED>
    <!-- With the site, device, and group filters you determine which
    assets to include in the report. With the vuln-severity and vuln-
    status filters you control which vulnerabilities to include in the
    report. -->
<!ELEMENT AdhocReportConfig (Filters, Baseline?) >
    <!-- the id of the report template used -->
    <!ATTLIST ReportConfig template-id CDATA #REQUIRED>
    <!ATTLIST ReportConfig format (pdf|html|rtf|xml|text|
    csv|db|raw-xml|raw-xml-v2|ns-xml|qualys-xml) #REQUIRED>
    <!ATTLIST ReportConfig owner CDATA #REQUIRED>
    <!ATTLIST ReportConfig timezone CDATA #REQUIRED>
<!ELEMENT description (#PCDATA)>
    <!-- The configuration must include at least one of device (asset),
    site, group (asset group) or scan filter to define the scope of
    report. The vuln-status filter can be used only with raw report
    formats: csv or raw_xml. If the vuln-status filter is not included
    in the configuration, all the vulnerability test results (including
    invulnerable instances) are exported by default in csv and raw_xml
    reports. -->
<!ELEMENT Filters (filter+)>
<!ELEMENT filter EMPTY> <!ATTLIST filter type
(site|group|device|scan|vuln-categories|
vuln-severity|vuln-status|cyberscope-component|cyberscope-
bureau|cyberscope-enclave|tag)
#REQUIRED>
    <!-- the ID of a specific site, group, device or scan.
    For scan, this can also be "last" for the most recently run scan.
    For vuln-status, the ID can have one of the following values:
    1) vulnerable-exploited (The check was positive. An exploit
    verified the vulnerability.)
    2) vulnerable-version (The check was positive. The version of the
    scanned service or software is associated with known
    vulnerabilities.)
    3) potential (The check for a potential vulnerability was
    positive.) These values are supported for CSV and XML formats.
    -->
    <!ATTLIST filter id CDATA #REQUIRED>
    <!-- For vuln-categories, the required format is include/exclude:
    [category_from_approved_list]
    Examples:
    include:Adobe,Microsoft
    exclude:Windows,Oracle -->
<!ELEMENT Users (user+)>
<!ELEMENT user EMPTY>
    <!-- the ID of a non-admin user who has access to this site -->
    <!ATTLIST user id CDATA #REQUIRED>
    <!ELEMENT Baseline EMPTY>
    <!-- the date to use as the baseline scan in ISO 8601 format,
    YYYYMMDDTHHMMSSsss, such as:
    19981231T00000000. Additionally,"first" can be used for the first
    run scan, or "previous" for the most recently run scan prior to the
    current scan. The Baseline compareTo attribute is optional unless
    you are creating a Baseline Comparison, Executive Overview, or
    custom report that incorpo- rates the Baseline Comparison section,
    in which case the attribute is required.-->
    <!ATTLIST Baseline compareTo CDATA #IMPLIED>
<!ELEMENT Generate (Schedule?)>
    <!-- will the report be generated after a scan completes (1), or is
    it ad-hoc/scheduled (0) -->
    <!ATTLIST Generate after-scan (0|1) "0">
    <!ATTLIST Generate schedule CDATA #IMPLIED>
<!ELEMENT Schedule EMPTY>
    <!ATTLIST Schedule enabled (0|1) "1">
    <!ATTLIST Schedule type (daily|hourly|monthly-date|monthly-
    day|weekly) #REQUIRED>
    <!ATTLIST Schedule interval CDATA #REQUIRED>
    <!-- the earliest date to generate the report on in ISO 8601
    format, YYYYMMDDTHHMMSSsss, such as: 19981231T00000000 -->
    <!ATTLIST Schedule start CDATA #REQUIRED>
    <!-- the date after which the schedule is disabled in ISO 8601
    format, YYYYMMDDTHHMMSSsss, such as: 19981231T00000000 -->
    <!ATTLIST Schedule notValidAfter CDATA #IMPLIED>
<!ELEMENT Delivery (Storage, Email?)>
<!–- See the Email DTD for more details -->
<!ELEMENT Storage (location?)>
    <!-- whether to store report on server -->
    <!ATTLIST Storage storeOnServer (0|1) "1">
<!-- Directory location to store report in (for non-default storage) --
>
<!ELEMENT location (#PCDATA)>
<!ELEMENT DBExport (credentials?, param*)>
    <!-- the db type to export to -->
    <!ATTLIST DBExport type CDATA #REQUIRED>
    <!ATTLIST DBExport type CDATA #REQUIRED>
<!ELEMENT credentials (#PCDATA)>
    <!-- the userid, password and realm attributes should ONLY be used
    if a security blob cannot be generated and the data is being
    transmitted/stored using external encryption (eg, HTTPS) -->
    <!ATTLIST credentials USERID CDATA #IMPLIED>
    <!ATTLIST credentials PASSWORD CDATA #IMPLIED>
    <!-- DB specific, usually the database name -->
    <!ATTLIST credentials realm CDATA #IMPLIED>
<!ELEMENT param (#PCDATA)>
    <!-- the name of the parameter -->
    <!ATTLIST param name CDATA #REQUIRED>
]>
```

Email DTD

The sendAs and sendToAclAs attributes are optional, but one of them is required for sending reports via e-mail. The sendAs attribute is required for sending e-mails to users who are not on the report access list. The sendToAcl attribute is required for sending e-mails to report access list members.

E-mails and attachments are sent via the Internet in cleartext and are not encrypted. If you do not set a valid value for either attribute, the application will save the report but not send it via e-mail. If you set a valid value for the sendAs attribute but not for the sendToAclAs attribute, the application will send the report via e-mail to non-access-list members only. If you set a valid value for the sendToAclAs attribute, the application will send the report via e-mail to access-list members only. If you set a valid value for both attributes, the application will send reports via e-mail to access-list members and non-members.

```
<!DOCTYPE Email [
<!ELEMENT Email (Recipients?, SmtpRelayServer?, Sender?)
    <!-- send as file attachment or zipped file to individuals who are
    not members of the report access list -->
    <!ATTLIST Email sendAs (file|zip) #OPTIONAL>
    <!-- send to all the authorized users of sites, groups and devices
    -->
    <!ATTLIST Email toAllAuthorized (0|1) "0">
    <!-- send to users on the report access listd file or the url-->
    <!ATTLIST Email sendToAclAs (file|zip|url) #OPTIONAL>
<!ELEMENT Recipients (Recipient*)>
<!ELEMENT Recipient (#PCDATA)>
<!ELEMENT SmtpRelayServer (#PCDATA)>
<!ELEMENT Sender (#PCDATA)>
]>
```

ReportSummary DTD

```
<!DOCTYPE ReportSummary [
<!ELEMENT ReportSummary EMPTY>
    <!-- the id of the generated report -->
    <!ATTLIST ReportSummary id CDATA #IMPLIED>
    <!-- the report definition (config) id -->
    <!ATTLIST ReportSummary cfg-id CDATA #REQUIRED>
    <!-- the current status of the report -->
    <!ATTLIST ReportSummary status
    (Started|Generated|Failed|Aborted|Unknown) #REQUIRED>
    <!-- the date and time the report was generated, in ISO 8601
    format, YYYYMMDDTHHMMSSsss, such as: 19981231T00000000 -->
    <!ATTLIST ReportSummary generated-on CDATA #IMPLIED>
    <!-- the URL to use to access the report (not set for database
    exports) -->
    <!ATTLIST ReportSummary report-URI CDATA #IMPLIED>
]>
```

UserConfig DTD

The current version of the API does not support creating user accounts with custom roles. You can only create user accounts with preset roles.

If values for allSites and allGroups are false or not specified, you can specify sites and groups using nested site and group elements.

You cannot change the user name after you create an account.

```
<!DOCTYPE UserConfig [
<!ELEMENT UserConfig (UserSite|UserGroup)*>
    <!-- the id of the user, set to -1 to create a new user -->
    <!ATTLIST UserConfig id CDATA #REQUIRED>
    <!-- the role of the user -->
    <!ATTLIST UserConfig role-name (global-admin|security-manager|site-
    admin|
    system-admin|user|custom) #REQUIRED>
    <!-- the id of the autentication source for the user -->
    <!ATTLIST UserConfig authsrcid CDATA #REQUIRED>
    <!-- the login name of the user -->
    <!ATTLIST UserConfig name CDATA #REQUIRED>
    <!-- the full name of the user -->
    <!ATTLIST UserConfig fullname CDATA #REQUIRED>
    <!-- the email address of the user -->
    <!ATTLIST UserConfig email CDATA #IMPLIED>
    <!-- new password -->
    <!ATTLIST UserConfig password CDATA #IMPLIED>
    <!-- 1 to enable this user, 0 to disable -->
    <!ATTLIST UserConfig enabled (0|1) #IMPLIED>
    <!-- true if the user has access to all sites, false otherwise -->
    <!ATTLIST UserConfig allSites (true|false) #IMPLIED>
    <!-- true if the user has access to all groups, false otherwise -->
    <!ATTLIST UserConfig allGroups (true|false) #IMPLIED>
<!-- See the UserSite DTD for more details -->
<!-- See the UserGroup DTD for more details -->
]>
```

User Site DTD

```
<!DOCTYPE Site [
    <!-- the id of the site the user is associated with -->
    <!ATTLIST Site id CDATA #REQUIRED>
]>
```

User Group DTD

```
<!DOCTYPE Group [
    <!-- the id of the group the user is associated with -->
    <!ATTLIST Group id CDATA #REQUIRED>
]>
```

UserSummary DTD

```
<!DOCTYPE UserSummary [
    <!-- the id of the user -->
    <!ATTLIST UserSummary id CDATA #REQUIRED>
    <!-- the source used to authenticate this user -->
    <!ATTLIST UserSummary authSource CDATA #REQUIRED>
    <!-- the module used to authenticated this user -->
    <!ATTLIST UserSummary authModule CDATA #REQUIRED>
    <!-- the login name of the user -->
    <!ATTLIST UserSummary userName CDATA #REQUIRED>
    <!-- the actual name of the user -->
    <!ATTLIST UserSummary fullname CDATA #REQUIRED>
    <!-- the email address of the user (may be empty) -->
    <!ATTLIST UserSummary email CDATA #REQUIRED>
    <!-- true if this user is an administrator, false otherwise -->
    <!ATTLIST UserSummary administrator (1|0) #REQUIRED>
    <!-- true if this user is disabled, false otherwise -->
    <!ATTLIST UserSummary disabled (1|0) #REQUIRED>
    <!-- true if this user is locked, false otherwise -->
    <!ATTLIST UserSummary locked (1|0) #REQUIRED>
    <!-- the number of sites this user is allowed to access -->
    <!ATTLIST UserSummary siteCount CDATA #REQUIRED>
    <!-- the number of groups this user belongs to -->
    <!ATTLIST UserSummary groupCount CDATA #REQUIRED>
]>
```

AuthenticatorSummary DTD

```
<!DOCTYPE AuthenticatorSummary [
<!ELEMENT AuthenticatorSummary EMPTY>
    <!-- the id of the authenticator -->
    <!ATTLIST AuthenticatorSummary id CDATA #REQUIRED>
    <!-- true if this authenticator authenticates using an external
    source,
    false otherwise -->
    <!ATTLIST AuthenticatorSummary external (0|1) #REQUIRED>
    <!-- the name of the authenticator source -->
    <!ATTLIST AuthenticatorSummary authSource CDATA #REQUIRED>
    <!-- the name of the authenticator module -->
    <!ATTLIST AuthenticatorSummary authModule CDATA #REQUIRED>
]>
```

XMLResponse DTD

This DTD provides the structure for the API response to a call for a non-existent API function.

```
<!DOCTYPE XMLResponse [

<!-- This element makes sure that valid XML is returned when an error
occurs. -->
<!ELEMENT XMLResponse (Failure)>
    <!-- This attribute will always return 0 since it represents some
    kind of failure in the request or the response. -->
    <!ATTLIST XMLResponse success "0">
]>
```

Failure DTD

```
<!DOCTYPE Failure [
<!-- The failure description, consisting of one or more message and/or
exception -->
<!ELEMENT Failure ((message|Exception)*)>
<!-- the message describing the failure -->
<!ELEMENT message (#PCDATA)>
    <!-- the source of the message, such as the module that caused the
    error -->
    <!ATTLIST message source CDATA #IMPLIED>
    <!-- the source specific message code -->
    <!ATTLIST message code CDATA #IMPLIED>
<!-- the exception causing the failure -->
<!ELEMENT Exception (message, stacktrace?)>
    <!-- the name of the Exception class (for Java or C++ exceptions) -
    ->
    <!ATTLIST Exception name CDATA #IMPLIED>
<!ELEMENT stacktrace (#PCDATA)>
]>
```

Using the Extended API v1.2 section

This section is divided into categories of operations accessed by the Extended API v1.2, such as vulnerabilty exception management or Scan Engine pool management. For each category, all individual APIs that make up the Extended API v1.2 are listed with the following information.

- a description of the API's function
- descriptions of all attributes of the user-generated API request
- descriptions of all elements of the API request and any attributes for those elements
- an XML example of the request
- descriptions of all attributes of the system-generated response to the API request
- descriptions of all elements of the response and any attributes for those elements
- an XML example of the response

Using breadcrumb headings

The headings for all nested elements, sub-elements, and attributes are presented in a breadcrumb style, so that you will know which request, response, or parent element each item refers to. The particular item in the breadcrumb path that is being addressed appears in bold type.

For example, EngineActivityResponse has an element named ScanSummary. The heading for ScanSummary appears as follows:

EngineActivityResponse > ScanSummary

ScanSummary has a sub-element named NodeSummary. The heading for NodeSummary appears as follows:

EngineActivityResponse > ScanSummary > NodeSummary

Validation with schemas

The requests made to the Extended API 1.2 are validated with the XML schemas provided in the Extended_API_XMLSchemas_v1.2.zip archive. You can download all documentation and schemas from the *Support* page in Help. Click the Support link on any page of the Security Console Web interface.

Lists of individual APIs that make up Extended API v1.2

Session management

Command	Description
Login	Start a session.
Logout	Allows you to obtain a session identifier that you can use in subsequent requests.

Asset discovery connection management

Command	Description
DiscoveryConnectionConnect	Initiate a connection to either a vCenter server or directly to standalone ESX(i) hosts.
DiscoveryConnectionCreate	Create a connection for dynamic discovery of virtual assets.
DiscoveryConnectionListingRequest	Obtain a list of available dynamic discovery connections.
DiscoveryConnectionUpdate	Edit an existing connection for dynamic discovery of virtual assets.
DiscoveryConnectionDelete	Remove a connection from the list of available dynamic discovery connections.

Scan Engine management

Command	Description
EngineSave	Configure a new scan engine, or update settings for an existing scan engine.
EngineListing	Provide a list of available scan engines and information about them.
EngineConfig	List detailed configuration information about a specific scan engine.
EngineActivity	Provide status of a given scan engine and its current scans, including the number, count, and severity of vulnerabilities discovered.
EngineDelete	Remove a scan engine from the list of available engines.

Ticketing

Command	Description
TicketCreate	Creates a new ticket, and assigns a name, priority, vulnerabilities, and other attributes to the ticket.
TicketListing	Returns a list of tickets based on filter criteria.
TicketDetails	Returns detailed information about an individual ticket.
TicketDelete	Deletes a ticket.

Multi-Tenant Users

Command	Description
MultiTenantUserCreate	Creates a new multi-tenant user. This API will fail if a user already exists by the same name, regardless of the silo associations for that user. When choosing user names, a globally unique naming convention should be followed, such as e-mail addresses, username@silo, or other such conventions. A multi-tenant user is a user in a silo-aware environment. This is not necessarily a user who has access to multiple silos. These APIs are only accessible to global administrators with "super-user" privileges.
MultiTenantUserListing	Returns a summary listing of users.
MultiTenantUserUpdate	Updates multi-tenant users.
MultiTenantUserConfig	Retrieves user details for a specified multi-tenant user.
MultiTenantUserDelete	Deletes a specified multi-tenant user.

Silo profiles

Command	Description
SiloProfileCreate	Creates a new silo profile.
SiloProfileListing	Returns a summary listing of silo profiles.
SiloProfileUpdate	Updates silo profiles.
SiloProfileConfig	Encapsulates information about the silo profile.
SiloProfileDelete	Deletes a specified silo profile.

Silo management

Command	Description
SiloCreate	Creates a new silo.
SiloListing	Provides a list of all silos and information about them.
SiloConfig	Modifies the configuration of an existing silo.
SiloUpdate	Modifies the configuration of an existing silo.
SiloDelete	Deletes an existing silo.

Role management

Command	Description
RoleCreate	Creates a new role that can be applied to any user.
RoleListing	Returns a summary list of all roles.
RoleDetails	Returns a detailed description of a single role.
RoleUpdate	Updates a specific role with new information.
RoleDelete	Deletes a specified role

Scan Engine Pool management

Command	Description
EnginePoolCreate	Creates a new engine pool and associates engines with the pool.
EnginePoolListing	Returns a summary list of all engine pools.
EnginePoolDetails	Returns a detailed description of a single engine pool.
EnginePoolUpdate	Updates a specific engine pool with new information.
EnginePoolDelete	Deletes a specified engine pool.

Vulnerability management

Command	Description
VulnerabilityListing	Provides a list of vulnerabilities checked during scans. A vulnerability is considered "credentialed" when all of its checks require credentials or if the check depends on previous authentication during a scan.

Command	Description
VulnerabilityDetails	Provides details of vulnerabilities. A vulnerability is considered "credentialed" when all of its checks require credentials or if the check depends on previous authentication during a scan.

Vulnerability exception management

Command	Description
PendingVulnExceptionCount	Provides a list of vulnerability exceptions marked "Under Review."
VulnerabilityExceptionListing	Lists all vulnerability exceptions for your organization or specific asset in your organization.
VulnerabilityExceptionCreate	Users can create vulnerability exceptions that apply to all instances of a vulnerability on all assets.
VulnerabilityExceptionResubmit	Allows a user with appropriate permissions to resubmit an vulnerability exception request with a new comment and reason after an exception has been rejected.
VulnerabilityExceptionRecall	Allows a user with “Submit” permissions to recall a vulnerability exception. Recall is used by a submitter to undo an exception request that has not been approved yet.
VulnerabilityExceptionApprove	Allows users with appropriate permissions to approve a vulnerability exception request, update comments and expiration dates on vulnerability exceptions that are “Under Review.”
VulnerabilityExceptionReject	Allows users with appropriate permissions to reject a vulnerability exception request and update comments for the vulnerability exception request.
VulnerabilityExceptionDelete	Allows users with appropriate permissions to delete a vulnerability exception request. Vulnerability exceptions can be deleted at any time regardless of status.
VulnerabilityExceptionUpdateComment	llows users who can submit exceptions and review exceptions to update comments on vulnerability exceptions in the work flow process.

Command	Description
VulnerabilityExceptionUpdateExpirationDate	Allows users with “Reviewer” permission to update the expiration date for an existing exception that has been approved.

Session management

This section covers all requests and responses related to API session management.

Login

Allows you to obtain a session identifier that you can use in subsequent requests.

LoginRequest attributes

Name	Description	Datatype	Range
user-id	The unique identifier of the user (required)	xs:string	any sequence of characters allowed in XML; of any length
password	The user's password (required)	xs:string	any sequence of characters allowed in XML; of any length
silo-id	a string that uniquely identifies the silo (optional)	xs:string	any sequence of characters allowed in XML; of any length

LoginRequest example

```
<?xml version="1.0" encoding="UTF-8"?>
<LoginRequest user-id="user1" password="12345"/>
```

LoginResponse attribute

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length

LoginResponse example

```
<?xml version="1.0" encoding="UTF-8"?>
<LoginResponse session-id="82C2395A9AA5B4E6F354A3706A2CDC1E307F1459"/>
```

Logout

Ends a session. To prevent unnecessary consumption of system resources, it is a best practice to call Logout once for each called instance of Login.

LogoutRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

LogoutRequest example

```
<?xml version="1.0" encoding="UTF-8"?>
<LogoutRequest session-id="82C2395A9AA5B4E6F354A3706A2CDC1E307F1459"/>
```

LogoutResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

LogoutResponse example

```
<?xml version="1.0" encoding="UTF-8"?>
<LogoutResponse/>
```

Asset discovery connection management

This section covers all requests and responses related to managing asset discovery.

DiscoveryConnectionCreate

In order to perform dynamic asset discovery, the application can connect to either a vCenter server or directly to standalone ESX(i) hosts.

Direct connections to the following vCenter versions are supported for dynamic asset discovery:

- vCenter 4.1
- vCenter 4.1, Update 1
- vCenter 5.0

Direct connections to the following ESX(i) versions are supported for vAsset discovery:

- ESX 4.1
- ESX 4.1, Update 1
- ESXi 4.1
- ESXi 4.1, Update 1
- ESXi 5.0

The preceding list of supported ESX(i) versions is for direct connections to standalone hosts. To determine if the application supports a connection to an ESX(i) host that is managed by vCenter, consult VMware's interoperability matrix at http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php.

For more information and best practices about setting up discovery connections, see the administrator's guide, which you can download from the Support page in Help.

DiscoveryConnectionCreateRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

DiscoveryConnectionCreateRequest element

DiscoveryConnectionCreateRequest has one element:

- DiscoveryConnection
- DiscoveryConnectionCreateRequest > DiscoveryConnection attributes

Name	Description	Data type	Range
name	the fully qualified domain name of the target vCenter server or standalone ESX(i) host (required)	xs:string	any sequence of characters allowed in XML; of any length
address	the IP address of the target vCenter server or standalone ESX(i) host (required)	xs:string	any sequence of characters allowed in XML; of any length
user-name	a user name for an account on the target vCenter server or standalone ESX(i) host; to be used for logging on to the target and initiating discovery connections (required)	xs:string	any sequence of characters allowed in XML; of any length
password	a password for an account on the target vCenter server or standalone ESX(i) host; to be used for logging on to the target and initiating discovery connections (required)	xs:string	any sequence of characters allowed in XML; of any length
protocol	the protocol used for connecting to the target (required)	protocol	“http:” or “https:”
port	the port used for connecting to the target (required)	xs:positiveInteger	1 to 65535

DiscoveryConnectionCreateRequest example

```
<DiscoveryConnectionCreateRequest session-id="sessionID" sync-
id="1234">
    <DiscoveryConnection
    name="testConnection"
    address="vcenter1.example.com"
    port="443"
    user-name="user1"
    protocol='HTTPS'
    password="abcdefg"/>
</DiscoveryConnectionCreateRequest>
```

DiscoveryConnectionCreateResponse attributes

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length
id	a unique ID for the discovery connection (required)	xs:positiveInteger	any mathematical integer greater than 0

DiscoveryConnectionCreateResponse example

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<DiscoveryConnectionCreateResponse id="7" sync-id="1234"/>
```

DiscoveryConnectionUpdate

This call changes attributes for an existing connection to a target vCenter server or a standalone ESX(i) host.

DiscoveryConnectionUpdateRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

DiscoveryConnectionUpdateRequest element

DiscoveryConnectionUpdateRequest has one element:

- DiscoveryConnection

DiscoveryConnectionUpdateRequest > DiscoveryConnection attributes

Name	Description	Datatype	Range
id	a unique ID for the discovery connection (required)	xs:positiveInteger	any mathematical integer greater than 0
name	the fully qualified domain name of the target vCenter server or standalone ESX(i) host (required)	xs:string	any sequence of characters allowed in XML; of any length
address	the IP address of the target vCenter server or standalone ESX(i) host (required)	xs:string	any sequence of characters allowed in XML; of any length
user-name	a user name for an account on the target vCenter server or standalone ESX(i) host; to be used for logging on to the target and initiating discovery connections (required)	xs:string	any sequence of characters allowed in XML; of any length
password	a password for an account on the target vCenter server or standalone ESX(i) host; to be used for logging on to the target and initiating discovery connections (required)	xs:string	any sequence of characters allowed in XML; of any length
protocol	the protocol used for connecting to the target (required)	protocol	“http:” or “https:”
port	the port used for connecting to the target (required)	xs:positiveInteger	1 to 65535

DiscoveryConnectionUpdateRequest example

```
<DiscoveryConnectionUpdateRequest session-id="sessionID" sync-
id="1234">
    <DiscoveryConnection id="7"
    name="Connection112"
    address="vcenter001.example.com"
    port="443"
    protocol="HTTPS"
    user-name="user1"
    password="abcdefg"/>
</DiscoveryConnectionUpdateRequest>
```

DiscoveryConnectionUpdateResponse attributes

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length
id	a unique ID for the discovery connection (required)	xs:positiveInteger	any mathematical integer greater than 0

DiscoveryConnectionUpdateResponse example

```
?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<DiscoveryConnectionUpdateResponse sync-id="1234"/>
```

DiscoveryConnectionListing

This call returns information about all available connections for dynamic discovery of assets, including whether or not connections are active. This is important because dynamic discovery of assets is only possible with active connections.

DiscoveryConnectionListingRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

DiscoveryConnectionListingRequest example

```
<DiscoveryConnectionListingRequest session-id="sessionID" sync-
id="1234"/>
```

DiscoveryConnectionListingResponse attributes

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length
id	a unique ID for the discovery connection (required)	xs:positiveInteger	any mathematical integer greater than 0

DiscoveryConnectionListingResponse element

DiscoveryConnectionListingResponse has one element:

- DiscoveryConnectionSummary

DiscoveryConnectionListingResponse > DiscoveryConnectionSummary attributes

Name	Description	Datatype	Range
id	a unique ID for the discovery connection (required)	xs:positiveInteger	any mathematical integer greater than 0
user-name	a user name for an account on the target vCenter server or standalone ESX(i) host; to be used for logging on to the target and initiating discovery connections (required)	xs:string	any sequence of characters allowed in XML; of any length
name	the fully qualified domain name of the target vCenter server or standalone ESX(i) host (required)	xs:string	any sequence of characters allowed in XML; of any length
address	the IP address of the target vCenter server or standalone ESX(i) host (required)	xs:string	any sequence of characters allowed in XML; of any length

Name	Description	Datatype	Range
protocol	the protocol used for connecting to the target (required)	protocol	“http:” or “https:”
port	the port used for connecting to the target (required)	xs:positiveInteger	1 to 65535
connection-status	whether or not the connection is active; dynamic discovery is only possible with active connections (required)	xs:string	any sequence of characters allowed in XML; of any length

DiscoveryConnectionListingResponse example

```
<DiscoveryConnectionListingResponse sync-id="1234">
    <DiscoveryConnectionSummary id="7" connection-status="Connected"
    user-name="user1" proto- col="HTTPS" port="443"
    address="vcenter1.example.com" name="testConnection"/>
    <DiscoveryConnectionSummary id="6" connection-status="Connected"
    user-name="root" proto- col="HTTPS" port="443"
    address="vcenter2.example.com"
    name="test"/>
</DiscoveryConnectionListingResponse>
```

DiscoveryConnectionDelete

This call deletes an existing connection to a target used for dynamic discovery of assets.

DiscoveryConnectionDeleteRequest attributes

Name	Description	Datatype	Range
id	the id of the discovery connection to be deleted (required)	xs:positiveInteger	any mathematical integer greater than 0
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

DiscoveryConnectionDeleteRequest example

```
<DiscoveryConnectionDeleteRequest session-id="sessionID" sync-id="1234"
id="7"/>
```

DiscoveryConnectionDeleteResponse attributes

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length
id	a unique ID for the discovery connection (required)	xs:positiveInteger	any mathematical integer greater than 0

DiscoveryConnectionDeleteResponse example

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<DiscoveryConnectionDeleteResponse sync-id="1234"/>
```

DiscoveryConnectionConnect

This call initiates a connection to a target used for dynamic discovery of assets. As long as a connection is active, dynamic discovery is continuous.

DiscoveryConnectionConnectRequest attributes

Name	Description	Datatype	Range
id	the id of the discovery connection to be initiated (required)	xs:positiveInteger	any mathematical integer greater than 0
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

DiscoveryConnectionConnectRequest example

```
<DiscoveryConnectionConnectRequest session-id="sessionID" sync-
id="1234" id="6"/>
```

DiscoveryConnectionConnectResponse attributes

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length
id	a unique ID for the discovery connection (required)	xs:positiveInteger	any mathematical integer greater than 0

DiscoveryConnectionConnectResponse example

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<DiscoveryConnectionConnectResponse sync-id="1234"/>
```

Scan engine management

This section covers all requests and responses related to managing Scan Engines.

EngineActivity

Provides the status of a given scan engine and its current scans, including the number, count, and severity of vulnerabilities discovered.

EngineActivityRequest attributes

Name	Description	Datatype	Range
engine-id	a unique numeric identifier for the scan engine, assigned by the console in the order of creation (required)	xs:positiveInteger	any mathematical integer greater than 0
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

EngineActivityRequest example

```
<?xml version="1.0" encoding="UTF-8"?>
<EngineActivityRequest engine-id="2"
session-id="C26C1361F5F8911952EA8C9BD3BE2F6C035A0663"/>
```

EngineActivityResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

EngineActivityResponse element

EngineActivityResponse has the following element:

- ScanSummary

EngineActivityResponse > ScanSummary

A set of status information about a scan.

EngineActivityResponse > ScanSummary attributes

Name	Description	Datatype	Range
endTime	the date and time at which a scan ends (optional)	xs:dateTime	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters
engine-id	a unique numeric identifier for the scan engine, assigned by the security console (required)	xs:positiveInteger	any mathematical integer greater than 0
scan-id	a unique numeric identifier for a scan, assigned by the security console (required)	xs:positiveInteger	any mathematical integer greater than 0
site-id	a unique numeric identifier for a site, assigned by the security console (required)	xs:positiveInteger	any mathematical integer greater than 0
startTime	the date and time at which a scan starts (optional)	xs:dateTime	CCYY-MMDDthh:mm:ssZ
status	the status of a scan (required)	xs:string	"running" "finished" "stopped" "error" "dispatched" "paused" "aborted" "unknown"

EngineActivityResponse > ScanSummary content

Name	Description	Datatype	Range
message	a message generated by a scan engine regarding how it finished or if it finished (optional)	xs:string	any sequence of characters allowed in XML; of any length

EngineActivityResponse > ScanSummary sub-elements

The ScanSummary element contains the following sub-elements:

- NodeSummary
- VulnerabilitySummary
- TaskSummary
- Message

EngineActivityResponse > ScanSummary > NodeSummary

A current count of targets that the application has attempted to scan categorized by status.

EngineActivityResponse > ScanSummary > NodeSummary attributes

Name	Description	Datatype	Range
dead	the count of dead nodes (scan targets) (required)	xs:nonNegativeInteger	any integer equal to, or greater than 0
filtered	the count of filtered nodes (required)	xs:nonNegativeInteger	any integer equal to, or greater than 0
live	the count of live nodes (required)	xs:nonNegativeInteger	any integer equal to, or greater than 0
other	the count of nodes regarded as "other" (required)	xs:nonNegativeInteger	any integer equal to, or greater than 0
unresolved	the count of unresolved nodes (required)	xs:nonNegativeInteger	any integer equal to, or greater than 0

EngineActivityResponse > ScanSummary > VulnerabilitySummary

A summary of information about the count of discovered vulnerabilities grouped by status and severity.

EngineActivityResponse > ScanSummary > VulnerabilitySummary attributes

Name	Description	Datatype	Range
count	count of vulnerabilities found (required)	xs:nonNegativeInteger	any integer equal to, or greater than 0
severity	severity of each found vulnerability (optional)	xs:nonNegativeInteger	any integer equal to, or greater than 0
status	type of each vulnerability (required)	xs:string	"vuln-exploit" "vuln-version" "vuln-potential" "not-vuln-exploit" "not-vuln-version" "error" "disabled" "other"

EngineActivityResponse > ScanSummary > TaskSummary

The count of scan tasks that have been scanned, are currently being scanned, and have scans pending. The grouping is by scan status.

EngineActivityResponse > ScanSummary > TaskSummary attributes

Name	Description	Datatype	Range
active	count of in-progress tasks (required)	xs:nonNegativeInteger	any integer equal to, or greater than 0
completed	count of finished tasks (required)	xs:nonNegativeInteger	any integer equal to, or greater than 0
pending	count of tasks scheduled to start in the future (required)	xs:nonNegativeInteger	any integer equal to, or greater than 0

EngineActivityResponse example

```
<?xml version="1.0" encoding="UTF-8"?>
<EngineActivityResponse sync-id="2">
<ScanSummary engine-id="2" scan-id="4" site-id="1" startTime="2009-12-
17T11:45:19.031-08:00" status="running">
    <Message/>
    <NodeSummary dead="0" filtered="0" live="7" other="0"
    unresolved="0"/>
    <TaskSummary active="8" completed="72" pending="3"/>
    ...
    <VulnerabilitySummary count="0" severity="6" status="vuln-
    exploit"/>
    <VulnerabilitySummary count="1" severity="7" status="vuln-
    exploit"/>
    <VulnerabilitySummary count="0" severity="8" status="vuln-
    exploit"/>
    <VulnerabilitySummary count="0" severity="9" status="vuln-
    exploit"/>
    ...
    <VulnerabilitySummary count="0" severity="6" status="vuln-
    version"/>
    <VulnerabilitySummary count="0" severity="7" status="vuln-
    version"/>
    <VulnerabilitySummary count="0" severity="8" status="other"/>
    <VulnerabilitySummary count="0" severity="9" status="vuln-
    version"/>
    <VulnerabilitySummary count="0" severity="10" status="disabled"/>
    <VulnerabilitySummary count="0" severity="1" status="vuln-
    potential"/>
    ...
    <VulnerabilitySummary count="0" severity="9" status="vuln-
    potential"/>
    <VulnerabilitySummary count="0" severity="10" status="other"/>
    <VulnerabilitySummary count="64" severity="0" status="not-vuln-
    exploit"/>
    <VulnerabilitySummary count="0" severity="0" status="not-vuln-
    version"/>
    <VulnerabilitySummary count="0" severity="0" status="error"/>
    <VulnerabilitySummary count="0" severity="0" status="disabled"/>
    <VulnerabilitySummary count="0" severity="0" status="other"/>
</ScanSummary>
</EngineActivityResponse>
```

EngineConfig

Lists detailed configuration information about a specific scan engine.

EngineConfigRequest attributes

Name	Description	Datatype	Range
engine-id	a unique numeric identifier for the scan engine, assigned by the console in the order of creation (required)	xs:positiveInteger	any mathematical integer greater than 0
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

EngineConfigRequest example

```
<?xml version="1.0" encoding="UTF-8"?>
<EngineConfigRequest engine-id="3"
session-id="C26C1361F5F8911952EA8C9BD3BE2F6C035A0663"/>
```

EngineConfigResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

EngineConfigResponse element

- EngineConfig

EngineConfigResponse > EngineConfig

Lists detailed configuration information about a specific scan engine.

EngineConfigResponse > EngineConfig attributes

Name	Description	Datatype	Range
priority	the relative priority of a scan engine assigned by a user during the configuration of that engine (optional)	xs:string	“very-low” “low” “normal” “high” “very high”
address	the IP address or DNS name of a scan engine (required)	xs:string	any sequence of characters allowed in XML; of any length
id	a unique numeric identifier for the scan engine, assigned by the security console (required)	xs:int	any mathematical integer
name	a name assigned to the scan engine by the security console (required)	xs:string	any sequence of characters allowed in XML; of any length
port	the number of the port on which the engine listens for requests from the security console (required)	xs:positiveInteger	1 to 65535
scope	a parameter that specifies whether the engine has a global or silo-specific scope (required)	xs:string	any sequence of characters allowed in XML; of any length

EngineConfigResponse > EngineConfig element

EngineConfig contains the following sub-element:

- Site

Site

Information about a site to which a scan engine is assigned.

EngineConfigResponse > EngineConfig > Site attributes

Name	Description	Datatype	Range
id	a unique numeric identifier for the scan engine, assigned by the security console (required)	xs:positiveInteger	any mathematical integer greater than 0
name	a name assigned to the site during site configuration (optional)	xs:string	any sequence of characters allowed in XML; of any length

EngineConfigResponse example

```
<?xml version="1.0" encoding="UTF-8"?>
<EngineConfigResponse>
   <EngineConfig address="127.0.0.1" id="2" name="Local scan engine"
   port="40814" pri- ority="very-high" scope=”global”>
      <Site id="1" name="Sales Dept."/>
   </EngineConfig>
</EngineConfigResponse>
```

EngineDelete

Removes a scan engine from the list of available engines.

EngineDeleteRequest attributes

Name	Description	Datatype	Range
engine-id	a unique numeric identifier for the scan engine, assigned by the console in the order of creation (required)	xs:positiveInteger	any mathematical integer greater than 0
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

Name	Description	Datatype	Range
scope	a parameter that specifies whether the engine has a global or silo-specific scope (required)	xs:string	"global""silo" (default value)

EngineDeleteRequest example

```
<?xml version="1.0" encoding="UTF-8"?>
<EngineDeleteRequest engine-id="3" scope="global"
session-id="C26C1361F5F8911952EA8C9BD3BE2F6C035A0663"/>
```

EngineDeleteResponse attribute

Name	Description	Datatype	Range
sync-id	a parameter that identifies an instance of a request (optional)	xs:string	any sequence of characters allowed in XML; of any length

EngineDeleteResponse example

```
<?xml version="1.0" encoding="UTF-8"?>
<EngineDeleteResponse/>
```

EngineListing

Provides a list of available scan engines and information about them.

EngineListingRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; maximum length is 40 characters
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

EngineListingRequest example

```
<?xml version="1.0" encoding="UTF-8"?>
<EngineListingRequest session-
id="C26C1361F5F8911952EA8C9BD3BE2F6C035A0663"/>
```

EngineListingResponse attribute

Name	Description	Datatype	Range
sync-id	a parameter that identifies an instance of a request (optional)	xs:string	any sequence of characters allowed in XML; of any length

EngineListingResponse element

- EngineSummary

EngineListingResponse > EngineSummary

A set of status information about a scan engine.

EngineListingResponse > EngineSummary attributes

Name	Description	Datatype	Range
status	the current operating status of the engine (required)	xs:string	“active” “pending-authorization” “incompatible” “not-responding” “unknown”
address	the IP address or DNS name of a scan engine (required)	xs:string	any sequence of characters allowed in XML; of any length
id	a unique numeric identifier for the scan engine, assigned by the security console (required)	xs:int	any mathematical integer
name	a name assigned to the scan engine by the security console (required)	xs:string	any sequence of characters allowed in XML; of any length
port	the number of the port on which the engine listens for requests from the security console (required)	xs:positiveInteger	1 to 65535

Name	Description	Datatype	Range
scope	a parameter that specifies whether the engine has a global or silo-specific scope (required)	xs:string	“global” “silo” (default value)

EngineListingResponse example

```
<?xml version="1.0" encoding="UTF-8"?>
<EngineListingResponse>
    <EngineSummary address="location.example.com" id="1"
    name="Distributed Scan Engine" port="40814" scope="global"
    status="unknown"/>
    <EngineSummary address="127.0.0.1" id="2" name="Local scan engine"
    port="40814" scope="global" status="active"/>
</EngineListingResponse>
```

EngineSave

Configures a new scan engine, or updates settings for an existing scan engine.

EngineSaveRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

EngineSaveRequest element

- EngineConfig

EngineSaveRequest > EngineConfig

Lists and specifies detailed configuration information about a specific scan engine.

EngineSaveRequest > EngineConfig > EngineConfig attributes

Name	Description	Datatype	Range
priority	the relative priority of a scan engine assigned by a user during the configuration of that engine (optional)	xs:string	"very-low" "low" "normal" "high" "very high"
address	the IP address or DNS name of a scan engine (required)	xs:string	any sequence of characters allowed in XML; of any length
id	a unique numeric identifier for the scan engine, assigned by the security console (required)	xs:int	in EngineSaveRequest, it must be set to -1
name	a name assigned to the scan engine by the security console (required)	xs:string	any sequence of characters allowed in XML; of any length
port	the number of the port on which the engine listens for requests from the security console (required)	xs:positiveInteger	1 to 65535
scope	a parameter that specifies whether the engine has a global or silo-specific scope (required)	xs:string	“global” “silo”

EngineSaveRequest > EngineConfig element

EngineConfig contains the following sub-element:

- Site

EngineSaveRequest > EngineConfig > Site

Information about a site to which a scan engine is assigned.

EngineSaveRequest > EngineConfig > Site attributes

Name	Description	Datatype	Range
id	a unique numeric identifier for the scan engine, assigned by the security console (required)	xs:positiveInteger	any mathematical integer greater than 0
name	a name assigned to the site a user during site configuration (optional)	xs:string	any sequence of characters allowed in XML; of any length

EngineSaveRequest example

```
<?xml version="1.0" encoding="UTF-8"?>
<EngineSaveRequest session-
id="C869588064DD3EEAE0B6A5AD1CAFB2D88CF23948" >
    <EngineConfig address="10.2.8.99" id="-1" name="New engine"
    port="40814" scope="global"/>
</EngineSaveRequest>
```

EngineSaveResponse attribute

Name	Description	Datatype	Range
id	a unique numeric identifier for the scan engine, assigned by the console in the order of creation (required)	xs:positiveInteger	any mathematical integer greater than 0

EngineSaveResponse element

- EngineConfig

EngineSaveResponse > EngineConfig

Lists detailed configuration information about a specific scan engine.

EngineSaveResponse > EngineConfig attributes

Name	Description	Datatype	Range
priority	the relative priority of a scan engine assigned by a user during the configuration of that engine (optional)	xs:string	"very-low" "low" "normal" "high" "very high"
address	the IP address or DNS name of a scan engine (required)	xs:string	any sequence of characters allowed in XML; of any length
id	a unique numeric identifier for the scan engine, assigned by the security console (required)	xs:int	any mathematical integer
name	a name assigned to the scan engine by the security console (required)	xs:string	any sequence of characters allowed in XML; of any length
port	the number of the port on which the engine listens for requests from the security console (required)	xs:positiveInteger	1 to 65535
scope	a parameter that specifies whether the engine has a global or silo-specific scope (required)	xs:string	“global” “silo”

EngineSaveResponse > EngineConfig element

EngineConfig contains the following sub-element:

- Site

EngineSaveResponse > EngineConfig > Site

Information about a site to which a scan engine is assigned.

EngineSaveResponse > EngineConfig > Site attributes

Name	Description	Datatype	Range
id	a unique numeric identifier for the scan engine, assigned by the security console (required)	xs:positiveInteger	any mathematical integer greater than 0
name	a name assigned to the site a user during site configuration (optional)	xs:string	any sequence of characters allowed in XML; of any length

EngineSaveResponse example

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<EngineSaveResponse sync-id="coyofXPZobUZ1302588254054">
    <EngineConfig priority="normal" scope="global" port="3780"
    name="wGCqk1302588254336" id="6" address="10.96.0.130">
    <Site name="random 66760" id="6"/>
    </EngineConfig>
</EngineSaveResponse>
```

Ticket management

This section covers all requests and responses related to managing tickets.

TicketCreate

Creates a new ticket, and assigns a name, priority, vulnerabilities, and other attributes to the ticket.

TicketCreateRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; maximum length is 40 characters
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

TicketCreateRequest element

TicketCreateRequest contains the following element:

- TicketCreate

TicketCreateRequest > TicketCreate

Specifies all details about the ticket.

TicketCreateRequest > TicketCreate attributes

Name	Description	Datatype	Range
name	ticket name (required)	xs:string	any sequence of characters allowed in XML
device-id	the asset for which the ticket is being created. The asset must exist (required)	xs:positiveInteger	any integer greater than zero

Name	Description	Datatype	Range
assigned-to	the login name of the person to whom the ticket is assigned. The user must have view asset privilege on the asset specified in the device-id attribute (required)	xs:string	any sequence of characters allowed in XML; of any length
priority	the relative priority of the ticket, assigned by the creator of the ticket (required)	xs:string	“low” “moderate” “normal” “high” “critical”

TicketCreateRequest > TicketCreate elements

TicketCreate contains the following sub-elements:

- Comments
- Vulnerabilities

TicketCreateRequest > TicketCreate > Comments

An optional list of comments associated with the ticket. Comments contains the following sub-element:

- Comment

TicketCreateRequest > TicketCreate > Comments > Comment

An annotation associated with a particular ticket.

TicketCreateRequest > TicketCreate > Comments > Comment content

Name	Description	Datatype	Range
comment	a comment about the ticket. (optional)	xs:string	any sequence of characters allowed in XML; of any length

TicketCreateRequest > TicketCreate > Comments > Vulnerabilities

The list of vulnerabilities addressed by the ticket.

TicketCreateRequest > TicketCreate > Comments > Vulnerabilities sub-element

The Vulnerabilities element contains the following sub-element:

- Vulnerability

TicketCreateRequest > TicketCreate > Comments > Vulnerabilities > Vulnerability

A vulnerability addressed by the ticket. At least one Vulnerability element must exist.

TicketCreateRequest > TicketCreate > Comments > Vulnerabilities > Vulnerability attribute

Name	Description	Datatype	Range
id	the vulnerability name (required)	xs:string	any sequence of characters allowed in XML; of any length

TicketCreateRequest example

```
<?xml version="1.0" encoding="UTF-8"?>
<TicketCreateRequest session-
id="C869588064DD3EEAE0B6A5AD1CAFB2D88CF23948" sync-id="A2B2D7">
<TicketCreate name="ticket1" priority="normal" device-id="3" assigned-
to="jsmith">
    <Vulnerabilities>
        <Vulnerability id="cisco-ntp-bof"/>
        <Vulnerability id="http-cisco-0002"/>
    </Vulnerabilities>
    <Comments>
        <Comment>Please fix ASAP</Comment>
    </Comments>
</TicketCreate>
</TicketCreateRequest>
```

TicketCreateResponse attributes

Name	Description	Datatype	Range
id	the id of the newly-created ticket. This number is used to refer to the ticket when making further requests (required)	xs:long	an mathematical long integer
sync-id	a user-specified identifier that can be used to ensure that a ticket request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

TicketCreateResponse example

```
<?xml version="1.0" encoding="UTF-8"?>
<TicketCreateResponse session-
id="C869588064DD3EEAE0B6A5AD1CAFB2D88CF23948" sync-id="A2B2D7"
id="21"/>
```

TicketListing

Returns a list of tickets based on filter criteria.

TicketListingRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	A user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

TicketListingRequest element

TicketListingRequest contains zero or more of the following element:

- Filter

TicketListingRequest > Filter

If no filters are specified, all tickets will be returned. Otherwise, tickets that match the filter criteria will be returned in a TicketListingResponse. Multiple filter criteria can be specified by using multiple Filter elements.

When multiple Filter elements are specified, filters of the same type are treated as though they were combined via an OR operator, while filters of different types are treated as though they were combined via an AND operator.

TicketListingRequest > Filter attributes

Name	Description	Datatype	Range
type	specifies the type of filter (required)	xs:string	“O” (Open) “A” (Assigned) “M” (Modified) “X” (Fixed) “P” (Partial) “R” (Rejected Fix) “Z” (Prioritized) “F” (Not Reproducible) “I” (Not Issue) “C” (Closed) “U” (Unknown)
value	specifies the filter criteria (required)	xs:string	any sequence of characters allowed in XML; of any length

TicketListingRequest > Filter types

The following values can be used as filter types for TicketListingRequest.

Name	Description	Datatype	Range
name	Filters by ticket name.	Full text match	name
state	Filters by ticket state.	“O” (Open) “A” (Assigned) “M” (Modified) “X” (Fixed) “P” (Partial) “R” (Rejected Fix) “Z” (Prioritized) “F” (Not Reproducible) “I” (Not Issue) “C” (Closed) “U” (Unknown)	state
id	Filters by ticket id.	Numeric match	id
author	Filters by ticket author.	Full text match	author
priority	Filters by the most recent ticket priority.	“low” “moderate” “normal” “high” “critical”	priority
created-before	Filters by creation date (non-inclusive), expressed in milliseconds or a valid value for xs:dateTime	See http://www.w3.org/TR/REC-xml.	created-before

Name	Description	Datatype	Range
created-on-or-before	Filters by creation date (non-inclusive), expressed in milliseconds or a valid value for xs:dateTime	See http://www.w3.org/TR/REC-xml.	created-on-or-before
created-after	Filters by creation date (non-inclusive), expressed in milliseconds or a valid value for xs:dateTime	See http://www.w3.org/TR/REC-xml.	created-after
created-on-or-after	Filters by creation date (non-inclusive), expressed in milliseconds or a valid value for xs:dateTime	See http://www.w3.org/TR/REC-xml.	created-on-or-after
device-id	Filters by asset identifier	Numeric match	device-id
assigned	Filters by login name of the user to whom the ticket was assigned	Full text match	assigned

TicketListingRequest example 1

In the following example, tickets that have the name “ticket1” OR “ticket2” AND are assigned to “jsmith”, AND have a priority of “moderate” are being requested.

```
<?xml version="1.0" encoding="UTF-8"?>
<TicketListingRequest session-
id="C869588064DD3EEAE0B6A5AD1CAFB2D88CF23948" sync-id="A2B2D7">
    <Filter type="name" value="ticket1"/>
    <Filter type="name" value="ticket2"/>
    <Filter type="assigned" value="jsmith"/>
    <Filter type="priority" value="moderate"/>
</TicketListingRequest>
```

TicketListingRequest example 2

In the following example, tickets that are created before AND after the specified dates, AND assigned to “jsmith” OR “mjones”, AND are associated with device 10 are being requested.

```
<TicketListingRequest session-
id="C869588064DD3EEAE0B6A5AD1CAFB2D88CF23948" sync-id="A2B2D7">
    <Filter type="created-before" value="2010-01-01T00:00:00"/>
    <Filter type="created-after" value="2009-11-26T03:20:00-05:00"/>
    <Filter type="assigned" value="jsmith"/>
    <Filter type="assigned" value="mjones"/>
    <Filter type="device-id" value="10"/>
</TicketListingRequest>
```

TicketListingResponse attribute

Name	Description	Datatype	Range
sync-id	a parameter that identifies an instance of a request (optional)	xs:string	any sequence of characters allowed in XML; of any length

TicketListingResponse element

TicketListingResponse contains zero or more of the following element:

- TicketSummary

TicketListingResponse > TicketSummary

A description of a ticket that satisfies the filter criteria specified in the TicketListingRequest. Multiple TicketSummary elements appear if more than one ticket satisfies the filter criteria. If no tickets satisfy the filter criteria, then no TicketSummary elements are returned.

TicketListingResponse > TicketSummary attributes

Name	Description	Datatype	Range
id	the id number of the ticket (required)	xs:positiveInteger	any integer greater than zero
name	ticket name (255 character limit) (required)	xs:string	any sequence of characters allowed in XML
device-id	the asset the ticket is created for (required)	xs:positiveInteger	any integer greater than zero

Name	Description	Datatype	Range
assigned-to	the login name of person to whom the ticket is assigned. The user must have view asset privilege on the asset specified in the device-id attribute. (required)	xs:string	any sequence of characters allowed in XML; of any length
priority	the relative priority of the ticket, assigned by the creator of the ticket (required)	xs:enumeration	“low” “moderate” “normal” “high” “critical”
author	the login name of the person who created the ticket (required)	xs:string	any sequence of characters allowed in XML; of any length
createdOn	date and time of ticket creation (required)	xs:dateTime	any valid value for xs:dateTime
state	the current status of the ticket (required)	xs:string	"O" (Open) "A" (Assigned) "M" (Modified) "X" (Fixed) "P" (Partial) "R" (Rejected Fix) "Z" (Prioritized) "F" (Not Reproducible) "I" (Not Issue) "C" (Closed) "U" (Unknown)

TicketListingResponse example

```
<?xml version="1.0" encoding="UTF-8"?>
    <TicketListingResponse sync-id="A2B2D7">
    <TicketSummary id="4" name="ticketName" priority="normal" assigned-
    to="dhall" state="TICKET_CLOSED" author="rjames" created-on="2010-
    01-27T12:00:00-08:00"/>
    <TicketSummary id="5" name="ticketName2" priority="normal"
    assigned-to="mjones" state="TICKET_OPENED" author="jsmith" created-
    on="2010-01-27T12:15:00-08:00"/>
</TicketListingResponse>
```

TicketDetails

Returns detailed information about an individual ticket.

TicketDetailsRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	A user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

TicketDetailsRequest element

TicketDetailsRequest contains one or more of the following element:

- Ticket

TicketDetailsRequest > Ticket

The ticket being requested.

TicketDetailsRequest > Ticket attribute

Name	Description	Datatype	Range
id	the id number of the ticket (required)	xs:positiveInteger	any integer greater than zero

TicketDetailsRequest example

```
<?xml version="1.0" encoding="UTF-8"?>
<TicketDetailsRequest session-
id="C869588064DD3EEAE0B6A5AD1CAFB2D88CF23948" sync-id="A2B2D7">
    <Ticket id="4"/>
</TicketDetailsRequest>
```

TicketDetailsResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that can be used to ensure that a ticket request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

TicketDetailsResponse element

TicketDetailsResponse contains one or more of the following element:

- TicketInfo

TicketDetailsResponse > TicketInfo

Specific information about the requested ticket.

TicketDetailsResponse > TicketInfo attributes

Name	Description	Datatype	Range
id	the id number of the ticket (required)	xs:positiveInteger	any integer greater than zero
name	ticket name (255 character limit) (required)	xs:string	any sequence of characters allowed in XML; up to 255 characters
device-id	the asset for which the ticket is being created. The asset must exist. (required)	xs:long	any mathematical long integer
assigned-to	the name of person to whom the ticket is assigned. The user must have view asset privilege on the asset specified in the device-id attribute. (required)	xs:string	any sequence of characters allowed in XML; of any length

Name	Description	Datatype	Range
priority	the relative priority of the ticket, assigned by the creator of the ticket (required)	xs:string	“low” “moderate” “normal” “high” “critical”
author	the login name of the person who created the ticket (required)	xs:string	any sequence of characters allowed in XML; of any length
created-on	date and time of ticket creation (required)	xs:dateTime	any valid value for xs:dateTime
state	the current state of the ticket (required)	xs:string	"O" (Open) "A" (Assigned) "M" (Modified) "X" (Fixed) "P" (Partial) "R" (Rejected Fix) "Z" (Prioritized) "F" (Not Reproducible) "I" (Not Issue) "C" (Closed) "U" (Unknown)

TicketDetailsResponse > TicketInfo elements

TicketInfo contains the following element:

- Vulnerabilities
- TicketHistory

TicketDetailsResponse > TicketInfo > Vulnerabilities

The list of vulnerabilities covered by the ticket.

TicketDetailsResponse > TicketInfo > Vulnerabilities sub-element

The Vulnerabilities element contains the following sub-element:

- Vulnerability

TicketDetailsResponse > TicketInfo > Vulnerabilities > Vulnerability

A vulnerability covered by the ticket. At least one Vulnerability element must exist.

TicketDetailsResponse > TicketInfo > Vulnerabilities > Vulnerability attribute

Name	Description	Datatype	Range
id	a string corresponding to the vulnerability name (required)	xs:string	any sequence of characters allowed in XML; of any length

TicketDetailsResponse > TicketInfo > Vulnerabilities > TicketHistory

A list of entries detailing changes in the ticket.

TicketDetailsResponse > TicketInfo > Vulnerabilities > TicketHistory element

TicketHistory has one or more of the following element:

- Entry

TicketDetailsResponse > TicketInfo > Vulnerabilities > TicketHistory > Entry

Gives details about a specific change in the ticket.

TicketDetailsResponse > TicketInfo > Vulnerabilities > TicketHistory > Entry attributes

Name	Description	Datatype	Range
author	the login name of the person who created the ticket (required)	xs:string	any sequence of characters allowed in XML; of any length
created-on	date and time of ticket creation (required)	xs:dateTime	any valid value for xs:dateTime

TicketDetailsResponse > TicketInfo > Vulnerabilities > TicketHistory > Entry sub-elements

Entry contains the following sub-elements:

- Event
- Comment

TicketDetailsResponse > TicketInfo > Vulnerabilities > TicketHistory > Entry > Event

An event in the history of the ticket.

TicketDetailsResponse > TicketInfo > Vulnerabilities > TicketHistory > Entry > Event attribute

Name	Description	Datatype	Range
state	the status of the ticket at the time the event was recorded (required)	xs:string	any sequence of characters allowed in XML; of any length

TicketDetailsResponse > TicketInfo > Vulnerabilities > TicketHistory > Entry > Event content

Name	Description	Datatype	Range
event	description of ticket event (optional)	xs:string	any sequence of characters allowed in XML; of any length

TicketDetailsResponse > TicketInfo > Vulnerabilities > TicketHistory > Entry > Event > Comment

A comment that is associated with the ticket.

TicketDetailsResponse > TicketInfo > Vulnerabilities > TicketHistory > Entry > Event > Comment content

Name	Description	Datatype	Range
comment	comment on the ticket entry (optional)	xs:string	any sequence of characters allowed in XML; of any length

TicketDetailResponse example

```
<?xml version="1.0" encoding="UTF-8"?>
<TicketDetailsResponse sync-id="A2B2D7">
    <TicketInfo id="4" name="ticket1" state="O" priority="normal"
    assigned-to="jsmith" device-id="2" author="mjones" created-
    on="2009-11-26T03:20:00">
        <Vulnerabilities>
            <Vulnerability id="dns-kaminsky-bug"/>
            <Vulnerability id="cisco-ntp-bof"/>
            <Vulnerability id="http-cisco-0002"/>>
        </Vulnerabilities>
        <TicketHistory>
            <Entry author="tester" created-on="2010-01-27T12:15:00">
                    <Comment>Assigned to rjames.</Comment>
                    <Event state="O">Created Ticket</Event>
            </Entry>
        </TicketHistory>
</TicketInfo>
</TicketDetailsResponse>
```

TicketDelete

Deletes a ticket.

TicketDeleteRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	A user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

TicketDeleteRequest element

TicketDeleteRequest contains the following sub-element:

- Ticket

TicketDeleteRequest > Ticket

An individual ticket.

TicketDeleteRequest > Ticket attribute

Name	Description	Datatype	Range
id	the id number of the ticket to be deleted (required)	xs: positiveInteger	an integer greater than 0

TicketDeleteRequest example

```
<?xml version="1.0" encoding="UTF-8"?>
<TicketDeleteRequest session-
id="C869588064DD3EEAE0B6A5AD1CAFB2D88CF23948" sync-id="A2B2D7">
    <Ticket id="33"/>
</TicketDeleteRequest>
```

TicketDeleteResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that can be used to ensure that a ticket request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

TicketDeleteResponse example

```
<?xml version="1.0" encoding="UTF-8"?>
<TicketDeleteResponse sync-id="A2B2D7">
</TicketDeleteResponse>
```

Vulnerability management

This section covers APIs related to vulnerability management.

VulnerabilityListing

Provides a list of vulnerabilities checked.

A vulnerability is considered “credentialed” when all of its checks require credentials or if the check depends on previous authentication during a scan.

VulnerabilityListingRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	A user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

VulnerabilityListingRequest example

```
<?xml version="1.0" encoding="UTF-8"?>
<VulnerabilityListingRequest session-
id="A655DBEDD9BC14577226FCB54EC53055FE3BC6E7" sync- id="A2B2D7"/>
```

VulnerabilityListingResponse attribute

Name	Description	Datatype	Range
sync-id	a parameter that identifies an instance of a request (optional)	xs:string	any sequence of characters allowed in XML; of any length

VulnerabilityListingResponse element

- VulnerabilityListingResponse contains the following sub-element:
- VulnerabilitySummary

VulnerabilityListingResponse > VulnerabilitySummary

A summary description of the vulnerability.

VulnerabilityListingResponse > VulnerabilitySummary attributes

Name	Description	Datatype	Range
id	the unique identifier of a vulnerability (required)	xs:string	any sequence of characters allowed in XML; of any length
title	the title of the vulnerability (required)	xs:string	any sequence of characters allowed in XML; of any length
safe	used to indicate whether all checks for the vulnerability are safe; unsafe checks may cause denial of service or otherwise disrupt system performance (required)	xs:boolean	"1" or "true" = safe "0" or "false" = unsafe
added	used to indicate when this vulnerability was first included in the application (required)	xs:date	valid date in the form YYYY-MM-DD
modified	used to note the last date the vulnerability was modified (required)	xs:date	valid date in the form YYYY-MM-DD
severity	how critical the vulnerability is on a scale of 1 to 10 (required)	xs:int	any mathematical integer between 1 and 10
pciSeverity	PCI severity value for the vulnerability on a scale of 1 to 5 (required)	xs:int	any mathematical integer between 1 and 5
published	the date when the information about the vulnerability was first released (optional)	xs:date	valid date in the form YYYY-MM-DD
cvss:vector	indicates how the vulnerability is exploited according to PCI standards (optional)	xs:string	any sequence of characters allowed in XML; of any length
cvss:score	the computation of the Common Vulnerability Scoring System indicating compliance with PCI standards on a scale from 0 to 10.0 (optional)	xs:int	any mathematical integer between 0 and 10

VulnerabilityListingResponse example

```
<VulnerabilityListingResponse sync-id="A2B2D7">
    <VulnerabilitySummary id="http-coldfusionmx-path-leak"
    title="Macromedia Coldfusion MX Server Path Leakage Vulnerability"
    severity="3" safe="true" pciSeverity="2" cvssScore="5.0"
    cvssVector="(AV:N/AC:L/Au:N/C:P/I:N/A:N)"
    added="20041101T000000000" modified="20090317T000000000"/>
    <VulnerabilitySummary id="http-savant-cgitest-bof" title="Savant
    CGITEST.EXE Buffer Overflow" severity="10" safe="false"
    pciSeverity="5" cvssScore="9.3" cvssVector="
    (AV:N/AC:M/Au:N/C:C/I:C/A:C)" added="20041101T000000000"
    modified="20090317T000000000"/>
</VulnerabilityListingResponse>
```

VulnerabilityDetails

Provides details of vulnerabilities.

A vulnerability is considered “credentialed” when all of its checks require credentials or if the check depends on previous authentication during a scan.

VulnerabilityDetailsRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	A user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length
vuln-id	a unique identifier of a vulnerability in the application’s vulnerability database (required)	xs:string	any sequence of characters allowed in XML; of any length

VulnerabilityDetailsRequest example

```
<?xml version="1.0" encoding="UTF-8"?>
<VulnerabilityDetailsRequest session-
id="DB079E8C082501A05DA950E4586E7745A776A68A" vuln-id="http-helix-
double-request-bof"/>
```

VulnerabilityDetailsResponse attributes

Name	Description	Datatype	Range
id	the unique identifier of a vulnerability (required)	xs:string	any sequence of characters allowed in XML; of any length
title	the title of the vulnerability (required)	xs:string	any sequence of characters allowed in XML; of any length
safe	used to indicate whether all checks for the vulnerability are safe; unsafe checks may cause denial of service or otherwise disrupt system performance (required)	xs:boolean	"1" or "true" = safe "0" or "false" = unsafe
added	used to indicate when this vulnerability was first included in the application (required)	xs:date	valid date in the form YYYY-MM-DD
modified	used to note the last date the vulnerability was modified (required)	xs:date	valid date in the form YYYY-MM-DD
severity	how critical the vulnerability is on a scale of 1 to 10 (required)	xs:int	any mathematical integer between 1 and 10
pciSeverity	PCI severity value for the vulnerability on a scale of 1 to 5 (required)	xs:int	any mathematical integer between 1 and 5
published	the date when the information about the vulnerability was first released (optional)	xs:date	valid date in the form YYYY-MM-DD
cvss:vector	indicates how the vulnerability is exploited according to PCI standards (optional)	xs:string	any sequence of characters allowed in XML; of any length
cvss:score	the computation of the Common Vulnerability Scoring System indicating compliance with PCI standards on a scale from 0 to 10.0 (optional)	xs:int	any mathematical integer between 0 and 10

VulnerabilityDetailsResponse element

VulnerabilityDetailsResponse contains the following element:

- Vulnerability

VulnerabilityDetailsResponse > Vulnerability sub-elements

Vulnerability contains the following sub-elements:

- description
- references
- solution

VulnerabilityDetailsResponse > Vulnerability attributes

Name	Description	Datatype	Range
id	the unique identifier of a vulnerability (required)	xs:string	any sequence of characters allowed in XML; of any length
title	the title of the vulnerability (required)	xs:string	any sequence of characters allowed in XML; of any length
safe	used to indicate whether all checks for the vulnerability are safe; unsafe checks may cause denial of service or otherwise disrupt system performance (required)	xs:boolean	"1" or "true" = safe "0" or "false" = unsafe
added	used to indicate when this vulnerability was first included in the application (required)	xs:date	valid date in the form YYYY-MM-DD
modified	used to note the last date the vulnerability was modified (required)	xs:date	valid date in the form YYYY-MM-DD
severity	how critical the vulnerability is on a scale of 1 to 10 (required)	xs:int	any mathematical integer between 1 and 10

Name	Description	Datatype	Range
pciSeverity	PCI severity value for the vulnerability on a scale of 1 to 5 (required)	xs:int	any mathematical integer between 1 and 5
published	the date when the information about the vulnerability was first released (optional)	xs:date	valid date in the form YYYY-MM-DD
cvss:vector	indicates how the vulnerability is exploited according to PCI standards (optional)	xs:string	any sequence of characters allowed in XML; of any length
cvss:score	the computation of the Common Vulnerability Scoring System indicating compliance with PCI standards on a scale from 0 to 10.0 (optional)	xs:int	any mathematical integer between 0 and 10

VulnerabilityDetailsResponse example

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<VulnerabilityDetailsResponse>
    <Vulnerability title="RealNetworks Helix Universal Server Double
    Request Buffer
    Overflow" severity="10" safe="false" published="20021219T000000000"
    pciSeverity="5" modified="20110104T000000000" id="http-helix-dou-
    ble-request-bof"
    cvssVector="(AV:N/AC:L/Au:N/C:P/I:P/A:P)" cvssScore="7.5"
    added="1099247400000">
        <description>
            <body>
                    <p>Certain versions of RealNetworks Helix Universal
                    Server are susceptible to a remotely exploit- able
                    buffer overflow condition when parsing two abnormally
                    long, successive GET requests. On Win- dows
                    platforms, this yields SYSTEM privilege; impact is
                    unknown for UNIX platforms.</p>
            </body>
        </description>
        <references>
            <reference
            source="BID">http://www.securityfocus.com/bid/6454</referenc
            e>
            <reference
            source="BID">http://www.securityfocus.com/bid/6456</referenc
            e>
            <reference
            source="BID">http://www.securityfocus.com/bid/6458</referenc
            e>
            <reference source="CERT-
            VN">http://www.kb.cert.org/vuls/id/974689</reference>
            </references>
        <solution>
            <body>
                    <p>Fix RealNetworks Helix Universal Server Double
                    Request Buffer Overflow</p>
                    <p>Download and apply the patch from: <a href=
                    "http://www.service.real.com/help/faq/security/
                    bufferoverrun12192002.html">
                    http://www.service.real.com/help/faq/security/buffer
                    overrun12192002.html</a>
                    </p>
```

```
                   <p/>
                   <p>Install the patch at: <a
                   href="http://www.service.real.com/help/faq/security/
                   bufferoverrun12192002.html">
                   http://www.service.real.com/help/faq/security/buffer
                   overrun12192002.html</a></p>
           </body>
        </solution>
    </Vulnerability>
</VulnerabilityDetailsResponse>
```

Vulnerability exception management

This section covers all requests and responses related to managing vulnerability exceptions.

PendingVulnExceptionCount

Provides a list of vulnerability exceptions marked “Under Review.”

PendingVulnExceptionCountRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

PendingVulnExceptionCountRequest example

```
<PendingVulnExceptionsCountRequest session-
id="ACE5A792020058C1F86C9952E9A5855BC295D8C3"/>
```

PendingVulnExceptionCountResponse element

PendingVulnExceptionCountResponse contains the following Sub-element:

- SiloVulnDetails

PendingVulnExceptionCountResponse > SiloVulnDetails attributes

Name	Description	Datatype	Range
silo-id	a string that uniquely identifies the silo (required)*	xs:string	any sequence of characters allowed in XML; of any length
oldestExceptionCreationDate	the oldest creation date from the list of Pending Vuln Exceptions in the silo-id (required)*	xs:string	valid date in the form DD-MM-YYYY

Name	Description	Datatype	Range
pendingVulnExceptionsCount	the count of Pending Vuln Exceptions for the silo-id (required)*	xs:int	any mathematical integer

PendingVulnExceptionCountResponse examples

Provides a list of vulnerability exceptions marked “Under Review” for all silos in which the user can approve vulnerability exceptions. Approving an exception is dependent upon the user having access to all sites applicable to the exception as well as having rights to approve exceptions.

The following are three basic examples of possible responses to the PendingVulnExceptionCountRequest.

Example 1

An API request is made using a session id of a user who has access to two silos demo_silo_1 and demo_silo_2 with the required “Approve Vulnerability” privilege.

```
<PendingVulnExceptionsCountResponse>
<SiloVulnDetails pendingVulnExceptionsCount="1"
oldestExceptionCreationDate="03-04-2011" siloId="demo_silo_1"/>
<SiloVulnDetails pendingVulnExceptionsCount="2"
oldestExceptionCreationDate="03-02-2011" siloId="demo_silo_2"/>
</PendingVulnExceptionsCountResponse>
```

Example 2

An API request is made using a session id of a user who has access to two silos demo_silo_1 and demo_silo_2 but the two silos do not have any pending exceptions that are marked Under Review.

```
<PendingVulnExceptionsCountResponse>
<SiloVulnDetails pendingVulnExceptionsCount="0"
oldestExceptionCreationDate="N/A" siloId="demo_silo_1"/>
<SiloVulnDetails pendingVulnExceptionsCount="0"
oldestExceptionCreationDate="N/A" siloId="demo_silo_2"/>
</PendingVulnExceptionsCountResponse>
```

Example 3

An API request is made using a session id of a user who has access to two silos demo_silo_1 and demo_silo_2 but does not have the appropriate rights assigned to “Approve Vulnerability.”

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Failure error-code="-1">
<Message>Error encountered, unable to fulfill request.</Message>
<Exception>
<Message>The requested user does not have permission to view
vulnerability exception data for any of the silos</Message>
<Stacktrace> ... trace log ... </Stacktrace>
```

VulnerabilityExceptionListing

Lists all vulnerability exceptions for your organization or specific asset in your organization.

VulnerabilityExceptionListingRequest element

VulnerabilityExceptionListingRequest contains the following element:

- VulnerabilityExceptionListingRequest

VulnerabilityExceptionListingRequest attributes

Name	Description	Datatype	Range
status	the state of a vulnerability exception in the work flow process (optional)	xs:string	must be "Under Review," "Approved," or "Rejected."
time-duration	a parameter that specifies a time interval (optional)	xs:duration	valid interval in the following format: PnYnMnDTnHnMnS.

VulnerabilityExceptionListingRequest example

```
<VulnerabilityExceptionListingRequest sync-id="1" session-id="1234"
status="Approved" time-duration="P5Y2M10D" />
```

VulnerabilityExceptionListingReponse element

VulnerabilityExceptionListingResponse contains the following element:

- VulnerabilityException

VulnerabilityExceptionListingReponse > VulnerabilityException attributes

The information required for an exception depends on the scope. In addition to attributes listed as required in the following table, certain attributes are necessary for certain exception scopes, even though they are listed as optional. See the notes following the table for more information.

Name	Description	Datatype	Range
vuln-id	a unique identifier of a vulnerability in the application’s vulnerability database (required)	xs:string	any sequence of characters allowed in XML; of any length
exception-id	a unique number assigned to the exception (required)	xs:positiveInteger	any mathematical integer greater than 0
submitter	the name of submitter of the exception (required)	xs:string	any sequence of characters allowed in XML; of any length
reviewer	the name of the reviewer of the exception (optional)	xs:string	any sequence of characters allowed in XML; of any length
status	the state of the exception in the work flow process (required)	listStatusType	must be set to "Under Review," "Approved," or "Rejected"
reason	the reason for exception status (required)	reasonType	must be set to either "False Positive", "Compensating Control," "Acceptable Use," "Acceptable Risk," or "Other"

Name	Description	Datatype	Range
scope	scope of the exception (required)	listScopeType	must be set to either: "All Instances," "All Instances on a Specific Asset," or "Specific Instance of Specific Asset"
device-id	a unique number assigned to an asset (optional)	xs:positiveInteger	any mathematical integer greater than 0
port-no	a unique number assigned to a port on an asset (optional)	xs:positiveInteger	a positive integer greater than 0 and less than 65536
expiration-date	the date an exception will expire, causing the vulnerability to be included in reports risk scores (optional)	xs:string	any sequence of characters allowed in XML; of any length
vuln-key	a string representing the specific vulnerable component in a discovered instance of the vulnerability referenced by the vuln-id attribute, such as a program, file or user account (optional)	xs:string	any sequence of characters allowed in XML; of any length

VulnerabilityExceptionListingReponse > VulnerabilityException sub-elements

VulnerabilityException contains the following sub-elements:

- submitter-comment
- reviewer-comment

Scope-related requirements for VulnerabilityException attributes

In addition to attributes listed as required in the preceding table, certain attributes are necessary for certain exception scopes, even though they are listed as optional.

- An exception for all instances of a vulnerability on all assets only requires the vuln-id attribute. The device-id, vuln-key and port-no attributes are ignored for this scope type.
- An exception for all instances on a specific asset requires the vuln-id and device-id attributes. The vuln-key and port-no attributes are ignored for this scope type.
- An exception for a specific instance of a vulnerability on a specific asset requires the vuln-id, device-id. Additionally, the port-no and/or the key attribute must be specified.

VulnerabilityExceptionListingResponse example

```
<VulnerabilityExceptionListingResponse>

<VulnerabilityException scope="All Instances" reason="Other" status="Under
Review" submitter="v4test" exception-id="7" vuln-id="dcerpc-ms-netapi-
netpathcanonicalize-dos">

<submitter-comment>submitter comment</submitter-comment>

</VulnerabilityException>

<VulnerabilityException device-id="1" scope="All Instances on a Specific
Asset" reason="Other" status="Under Review" submitter="v4test" exception-
id="8" vuln-id="dcerpc-ms-netapi-netpathcanonicalize-dos">

<submitter-comment>submitter comment</submitter-comment>

</VulnerabilityException>

<VulnerabilityException vuln-key="123" port-no="445" device-id="1"
scope="Specific Instance of Specific Asset" reason="Other" status="Under
Review" submitter="v4test" exception-id="9" vuln-id="dcerpc-ms-netapi-
netpathcanonicalize-dos">

<submitter-comment>submitter comment</submitter-comment>

</VulnerabilityException>

</VulnerabilityExceptionListingResponse>
```

VulnerabilityExceptionCreate

Users can create vulnerability exceptions that apply to all instances of a vulnerability on all assets.

Users must have “Manage Sites” and “Submit Vulnerability Exceptions” permissions to create vulnerability exceptions.

VulnerabilityExceptionCreateRequest element

VulnerabilityExceptionCreateRequest contains the following required element:

- comment

VulnerabilityExceptionCreateRequest attributes

Name	Description	Datatype	Range
vuln-id	a unique identifier of a vulnerability in the application’s vulnerability database (required)	xs:string	any sequence of characters allowed in XML; of any length
reason	the reason for exception status (required)	reasonType	must be set to either "False Positive", "Compensating Control," "Acceptable Use," "Acceptable Risk," or "Other"
scope	list of scope type; user can specify if a vulnerability is excepted by port or by asset (required)	listScopeType	must be set to either: "All Instances," "All Instances on a Specific Asset," or "Specific Instance of Specific Asset"

VulnerabilityExceptionCreateRequest examples

If scope is “All instances”

```
<VulnerabilityExceptionCreateRequest
session-id="16A80F42BE4D0525FDDA217C16257E08773FB1CD" vuln-id="dcerpc-
ms-netapi-netpathcanonical- ize-dos" reason="Other" scope="All
Instances">
    <comment>submitter comment</comment>
</VulnerabilityExceptionCreateRequest>
```

If scope is “All instances on a Specific Asset”

```
<VulnerabilityExceptionCreateRequest session-
id="16A80F42BE4D0525FDDA217C16257E08773FB1CD" vuln- id="dcerpc-ms-
netapi-netpathcanonicalize-dos" reason="Other" device-id="1" scope="All
Instances on a Specific Asset">
    <comment>submitter comment</comment>
</VulnerabilityExceptionCreateRequest>
```

If scope is “Specific instance of Specific Asset”

```
<VulnerabilityExceptionCreateRequest session-
id="1ACC917DE40A340B17537543E11147D65C53EE42" vuln- id="dcerpc-ms-
netapi-netpathcanonicalize-dos" reason="Other" scope="Specific Instance
of Specific Asset"
device-id="1" port-no="445" vuln-key="123">
    <comment>submitter comment</comment>
</VulnerabilityExceptionCreateRequest>
```

VulnerabilityExceptionCreateResponse attribute

Name	Description	Datatype	Range
exception-id	a unique number assigned to the exception (required)	xs:positiveInteger	any mathematical integer greater than 0

VulnerabilityExceptionCreateResponse example

```
<VulnerabilityExceptionCreateResponse sync-id="optional" exception-
id="135"/>
```

VulnerabilityExceptionResubmit

Allows a user with appropriate permissions to resubmit an vulnerability exception request with a new comment and reason after an exception has been rejected.

You can only resubmit a request that has a “Rejected” status; if an exception is “Approved” or “Under Review” you will receive an error message stating that the exception request cannot be resubmitted.

You must have “Manage Sites” and “Submit Vulnerability Exceptions” permissions to resubmit a vulnerability exception that is applicable to all instances of a vulnerability on all assets in the scope.

To submit an exception to applicable vulnerabilities on a specific asset, on one instance or all instances, you must have "Submit Vulnerability Exceptions" permission.

VulnerabilityExceptionResubmitRequest attributes

Name	Description	Datatype	Range
exception-id	A unique number assigned to the exception (required)	xs:positiveInteger	any mathematical integer greater than 0

Name	Description	Datatype	Range
reason	the reason for exception status (optional)	reasonType	must be set to either "False Positive", "Compensating Control," "Acceptable Use," "Acceptable Risk," or "Other"

VulnerabilityExceptionResubmitRequest sub-element

VulnerabilityExceptionResubmitRequest contains the following sub-element:

- comment

VulnerabilityExceptionResubmitRequest > Comment attribute

Name	Description	Datatype	Range
comment	user's remarks that explain why an exception is being resubmitted (required)	commentType	any sequence of characters allowed in XML; of any length

VulnerabilityExceptionResubmitRequest example

```
<VulnerabilityExceptionReSubmitRequest sync-id="12" session-
id="E732466B48A9FE3F87D3FA69BDBFE89D7A21287D" exception-id="1"
reason="other" >
    <comment>Re-submitter comment</comment>
</VulnerabilityExceptionReSubmitRequest>
```

VulnerabilityExceptionResubmitResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

VulnerabilityExceptionResubmitResponse example

```
<VulnerabilityExceptionReSubmitResponse sync-id="optional"/>
```

VulnerabilityExceptionRecall

Allows a user with “Submit” permissions to recall a vulnerability exception. Recall is used by a submitter to undo an exception request that has not been approved yet.

You can only recall a vulnerability exception that has “Under Review” status.
To recall an exception that applies to all instances on all assets you must have “Manage Sites” permission.

VulnerabilityExceptionRecallRequest attribute

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length
exception-id	a unique number assigned to the exception (required)	xs:positiveInteger	any mathematical integer greater than 0

VulnerabiltyExceptionRecallRequest example

```
<VulnerabilityExceptionRecallRequest session-id="1234" sync-id="1"
exception-id="123" />
```

VulnerabilityExceptionRecallResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

VulnerabilityExceptionRecallResponse example

```
<VulnerabilityExceptionRecallResponse sync-id="optional" />
```

VulnerabilityExceptionApprove

Allows users with appropriate permissions to approve a vulnerability exception request, update comments and expiration dates on vulnerability exceptions that are “Under Review.”

To approve a vulnerability exception that has a scope of “All instances on all devices” you must have “Manage Sites” and “Approve Vulnerability Exceptions” permissions.

To approve a vulnerability exception that applies to a specific instance of a vulnerability on an asset or to all instances of a vulnerability on a specific asset you must have "Approve Vulnerability Exceptions" permissions.

VulnerabilityExceptionApproveRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length
exception-id	a unique number assigned to the exception (required)	xs:positiveInteger	any mathematical integer greater than 0

VulnerabilityExceptionApproveRequest element

VulnerabilityExceptionApproveRequest contains the following sub-element:

- comment

VulnerabilityExceptionApproveRequest > Comment attribute

Name	Description	Datatype	Range
comment	user remarks to explain why an exception is being resubmitted (if the provided reason for the exception request to be approved is “other”, the comment attribute is required; otherwise it is optional)	commentType	any sequence of characters allowed in XML; of any length

VulnerabilityExceptionApproveRequest example

```
<VulnerabilityExceptionApproveRequest session-id="1234" sync-id="1"
exception-id="123" expiration-date="2011-03-02">
    <comment>optional comment</comment>
</ VulnerabilityExceptionApproveRequest >
```

VulnerabilityExceptionApproveResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

VulnerabilityExceptionApproveResponse example

```
<VulnerabilityExceptionApproveResponse synch-id=" optional"/>
```

VulnerabilityExceptionReject

Allows users with appropriate permissions to reject a vulnerability exception request and update comments for the vulnerability exception request.

To reject a vulnerability exception that has a scope of “All instances on all devices” you must have “Manage Sites” and “Approve Vulnerability Exceptions” permissions. To reject a vulnerability exception that applies to a specific instance of a vulnerability on an asset or to all instances of a vulnerability on a specific asset you must have “Approve Vulnerability Exceptions” permissions.The expiration date cannot be changed for a vulnerability request that has been rejected.

VulnerabilityExceptionRejectRequest attribute

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length
exception-id	a unique number assigned to the exception (required)	xs:positiveInteger	any mathematical integer greater than 0

VulnerabilityExceptionRejectRequest element

VulnerabilityExceptionRejectRequest contains the following sub-element:

- comment

VulnerabiltyExceptionRejectRequest example

```
<VulnerabilityExceptionRejectRequest session-id="1234" sync-id="1"
exception-id="123">
    <comment>optional comment</comment>
</ VulnerabilityExceptionRejectRequest>
```

VulnerabilityExceptionRejectResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

VulnerabilityExceptionRejectResponse example

```
<VulnerabilityExceptionRejectResponse synch-id=" optional"/>
```

VulnerabilityExceptionDelete

Allows users with appropriate permissions to delete a vulnerability exception request.

Vulnerability exceptions can be deleted at any time regardless of status. To delete and exception on all instances of all assets you must have “Manage Sites” permission.

VulnerabilityExceptionDeleteRequest attribute

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length
exception-id	a unique number assigned to the exception (required)	xs:positiveInteger	any mathematical integer greater than 0

VulnerabilityExceptionDeleteRequest example

```
<VulnerabilityExceptionDeleteRequest session-id="1234" sync-id="1"
exception-id="123" /
```

VulnerabilityExceptionDeleteResponse attribute

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

VulnerabilityExceptionDeleteResponse example

```
<VulnerabilityExceptionDeleteResponse sync-id="optional" />
```

VulnerabilityExceptionUpdateComment

Allows users who can submit exceptions and review exceptions to update comments on vulnerability exceptions in the work flow process.

Comments can be updated for all exception states except for “Delete.” To update a Submitter comment you must have “Submitter” permission. To update a Reviewer comment you must have “Reviewer” permission.

VulnerabilityExceptionUpdateCommentRequest attribute

Name	Description	Datatype	Range
exception-id	A unique number assigned to the exception (required)	xs:positiveInteger	any mathematical integer greater than 0

VulnerabilityExceptionUpdateCommentRequest elements

VulnerabilityExceptionUpdateCommentRequest contains the following elements:

- reviewer-comment
- submitter-comment

VulnerabilityExceptionUpdateCommentRequest example

```
<VulnerabilityExceptionUpdateCommentRequest exception-id="45">
    <reviewer-comment>This exception was incorrectly tagged as a false-
    positive, but it should be a compensating control.</reviewer-
    comment> </VulnerabilityExceptionUp- dateCommentRequest>
```

VulnerabilityExceptionUpdateCommentResponse attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

VulnerabilityExceptionUpdateCommentResponse example

```
<VulnerabilityExceptionUpdateCommentResponse/>
```

VulnerabilityExceptionUpdateExpirationDate

Allows users with “Reviewer” permission to update the expiration date for an existing exception that has been approved.

You cannot change or update the state, scope, reason, or comments on an approved vulnerability exception.

VulnerabilityExceptionUpdateExpirationDateRequest attributes

Name	Description	Datatype	Range
exception-id	A unique number assigned to the exception (required)	xs:positiveInteger	any mathematical integer greater than 0
expiration-date	the date an exception will expire and display in reports again (required)	xs:date	valid date in the form YYYY-MM-DD

VulnerabilityExceptionUpdateExpirationDateRequest example

```
<?xml version="1.0" encoding="UTF-8"?>
<VulnerabilityExceptionUpdateExpirationDateRequest exception-id="56"
expiration- date="2012-09-03"/> {code}
```

VulnerabilityExceptionUpdateExpirationDateResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

VulnerabilityExceptionUpdateExpirationDateResponse example

```
<?xml version="1.0" encoding="UTF-8"?>
<VulnerabilityExceptionUpdateExpirationDateResponse/>
```

Multi-Tenant users

MultiTenantUserCreate

Creates a new multi-tenant user. This API will fail if a user already exists by the same name, regardless of the silo associations for that user. When choosing user names, a globally unique naming convention should be followed, such as e-mail addresses, username@silo, or other such conventions.

A multi-tenant user is a user in a silo-aware environment. This is not necessarily a user who has access to multiple silos.

These APIs are only accessible to global administrators with “super-user” privileges.

MultiTenantUserCreateRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

MultiTenantUserCreateRequest element

- MultiTenantUserConfig

- MultiTenantUserConfig

Encapsulates a user's information that is used across all the silos to which they have access.

MultiTenantUserCreateRequest > MultiTenantUserConfig attributes

Name	Description	Datatype	Range
authsrcid	The ID of the user's authentication source. (required)	xs:positiveInteger	any mathematical integer greater than 0
user-name	The login name of the user. (required)	xs:string	any sequence of characters allowed in XML; of any length

Name	Description	Datatype	Range
full-name	The full name of the user. (required)	xs:string	any sequence of characters allowed in XML; of any length
email	The e-mail address of the user. (optional)	xs:string	A valid e-mail, according to RFC822
password	The password to be set for the user. Only used for built-in authentication. (required)	xs:string	any sequence of characters allowed in XML; of any length
enabled	Enable or disable the user account. (required)	xs:boolean	“1” or “true” = enabled “0” or “false” = disabled
superuser	Account is a superuser, with access to multi-tenant and system APIs. (required)	xs:boolean	“1” or “true” = super-user “0” or “false” = unprivileged

MultiTenantUserCreateRequest > MultiTenantUserConfig element

MultiTenantUserConfig contains the following sub-element:

- SiloAccesses

MultiTenantUserCreateRequest > MultiTenantUserConfig > SiloAccesses

A list of elements that define a user's access permissions.

MultiTenantUserCreateRequest > MultiTenantUserConfig > SiloAccesses elements

SiloAccesses contains the following sub-element:

- SiloAccess

MultiTenantUserCreateRequest > MultiTenantUserConfig > SiloAccesses > SiloAccess

SiloAccess defines the access a user has to a specific silo, including their role and the objects they have access to.

MultiTenantUserCreateRequest > MultiTenantUserConfig > SiloAccesses > SiloAccess attributes

Name	Description	Datatype	Range
all-groups	defines whether the user has access to all groups within the silo. (required)	xs:boolean	“1” or “true” = access to all groups “0” or “false” = does not have access to all groups
all-sites	defines whether the user has access to all sites within the silo. (required)	xs:boolean	“1” or “true” = access to all sites “0” or “false” = does not have access to all sites
default-silo	sets this silo as the default silo. When the user logs onto the system, this is the silo they will be taken to if a silo is not specified; only one SiloAccess within the UserConfig can be marked as the default-silo, otherwise an error is returned (required)	xs:boolean	“1” or “true” = this is the default silo “0” or “false”= this is not the default silo
role-name	the name of the role to which a user is assigned. (required)	xs:string	built-in role names are: ’global-admin security-manager site-admin system-admin user customother possible strings include any user-defined role names

Name	Description	Datatype	Range
silo-id	a string that uniquely identifies the silo (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 50 characters

MultiTenantUserCreateRequest > MultiTenantUserConfig > SiloAccesses > SiloAccess sub-elements

The element SiloAccess has the following Sub-elements:

- AllowedGroups
- AllowedSites

MultiTenantUserCreateRequest > MultiTenantUserConfig > SiloAccesses > SiloAccess > AllowedGroups

A list of groups to which the user has access. If all-groups is set to true, no AllowedGroups can be specified.

MultiTenantUserCreateRequest > MultiTenantUserConfig > SiloAccesses > SiloAccess > AllowedGroups sub-element

The AllowedGroups element contains zero or more of the following sub-element:

- AllowedGroup

MultiTenantUserCreateRequest > MultiTenantUserConfig > SiloAccesses > SiloAccess > AllowedGroups > AllowedGroup

A group to which a user has access.

MultiTenantUserCreateRequest > MultiTenantUserConfig > SiloAccesses > SiloAccess > AllowedGroups > AllowedGroup > attribute

Name	Description	Datatype	Range
id	The group ID. (required)	xs:positiveInteger	any integer greater than 0

MultiTenantUserCreateRequest > MultiTenantUserConfig > SiloAccesses > SiloAccess > AllowedGroups > AllowedSites

A list of sites to which the user has access. If all-sites is set to true, no AllowedSites can be specified.

MultiTenantUserCreateRequest > MultiTenantUserConfig > SiloAccesses > SiloAccess > AllowedGroups > AllowedSites attribute

Name	Description	Datatype	Range
id	The group ID. (required)	xs:positiveInteger	any integer greater than 0

MultiTenantUserCreateRequest example

The following request creates a super-user account with privileges for two silos, each with a different role and site permissions.

```
<MultiTenantUserCreateRequest session-
id="C8F0CA79D9CE6049E2A9B78F8CAEFB235BF6219C">
    <MultiTenantUserConfig full-name="John Doe" user-name="jdoe"
    authsrcid="1"
    email="jdoe@company.com" password="abc123" superuser="false"
    enabled="true">
        <SiloAccesses>
            <SiloAccess all-groups="true" all-sites="false" role-
            name="user"
            silo-id="pci-silo-001" default-silo="true">
                    <AllowedSites>
                        <AllowedSite id="1"/>
                        <AllowedSite id="7"/>
                    </AllowedSites>
            </SiloAccess>
            <SiloAccess all-groups="false" all-sites="true" role-
            name="site-admin" silo-id="pci- silo-002" default-
            silo="false">
            </SiloAccess>
        </SiloAccesses>
    </MultiTenantUserConfig>
</MultiTenantUserCreateRequest>
```

MultiTenantCreateResponse attributes

Name	Description	Datatype	Range
sync-id	A user-specified identifier that can be used to ensure that a ticket request is not duplicated.(optional)	xs:string	any sequence of characters allowed in XML; of any length
user-id	ID of the newly created user. (required)	xs:positive integer	any integer greater than zero

MultiTenantUserCreateResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<MultiTenantUserCreateResponse user-id="4567"/>
```

MultiTenantUserListing

Returns a summary listing of users.

MultiTenantUserListingRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

MultiTenantUserListingRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<MultiTenantUserListingRequest session-
id="7E53108F40A617611B2A7D3C78CAB793464B5E62"/>
```

MultiTenantUserListingResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

MultiTenantUserListingResponse element

MultiTenantUserListing has the following element:

- MultiTenantUserSummaries

MultiTenantUserListingResponse > MultiTenantUserSummaries

A list of multi-tenant user summaries.

MultiTenantUserListingResponse > MultiTenantUserSummaries element

MultiTenantUserSummaries contains zero or more of the following element:

- MultiTenantUserSummary

MultiTenantUserListingResponse > MultiTenantUserSummaries > MultiTenantUserSummary

The multi-tenant user summary encapsulates summary information about the user across all the silos to which they have access.

MultiTenantUserListingResponse > MultiTenantUserSummaries > MultiTenantUserSummary attributes

Name	Description	Datatype	Range
id	The user ID. (required)	xs:positiveInteger	any integer greater than 0
user-name	The login name of the user. (required)	xs:string	any sequence of characters allowed in XML; of any length
full-name	The full name of the user. (required)	xs:string	any sequence of characters allowed in XML; of any length
email	The e-mail address of the user. (optional)	xs:string	any sequence of characters allowed in XML; of any length
enabled	Enable or disable the user account. (required)	xs:boolean	“1” or “true” = enabled “0” or “false” = disabled

Name	Description	Datatype	Range
superuser	Account is a superuser, with access to multi-tenant and system APIs. Only a global administrator can be upgraded to a super-user. (required)	xs:boolean	“1” or “true” = super-user “0” or “false” = unprivileged
auth-module	The authentication module used to authenticate the user. (required)	xs:string	any sequence of characters allowed in XML; of any length
auth-source	The authentication source used to authenticate the user. (required)	xs:string	any sequence of characters allowed in XML; of any length
locked	Whether the account is locked. (required)	xs:boolean	“1” or “true” = locked “0” or “false” = unlocked
silo-count	Number of silos to which the user has access. (required)	xs:positiveInteger	any integer greater than 0

MultiTenantUserListingResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<MultiTenantUserListingResponse>
    <MultiTenantUserSummaries>
        <MultiTenantUserSummary id="4567" full-name="John Doe" user-
        name="jdoe" email="jdoe@com- pany.com" superuser="false"
        enabled="true" auth-module="Datastore" auth-source="Builtin
        Users" silo-count="1" locked="false"/>
    </MultiTenantUserSummaries>
</MultiTenantUserListingResponse>
```

MultiTenantUserUpdate

Updates multi-tenant users.

MultiTenantUserUpdateRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

MultiTenantUserUpdateRequest element

MultiTenantUserUpdateRequest has the following element:

- MultiTenantUserConfig

MultiTenantUserUpdateRequest > MultiTenantUserConfig

Encapsulates information about the user across all the silos to which they have access.

MultiTenantUserUpdateRequest > MultiTenantUserConfig attributes

Name	Description	Datatype	Range
authsrcid	The ID of the user's authentication source. (required)	xs:positiveInteger	any mathematical integer greater than 0
user-name	The login name of the user. (required)	xs:string	any sequence of characters allowed in XML; of any length
full-name	The full name of the user. (required)	xs:string	any sequence of characters allowed in XML; of any length
email	The e-mail address of the user. (optional)	xs:string	A valid e-mail, according to RFC822
password	The password to be set for the user. Only used for built-in authentication. (required)	xs:string	any sequence of characters allowed in XML; of any length
enabled	Enable or disable the user account. (required)	xs:boolean	“1” or “true” = enabled “0” or “false” = disabled
superuser	Account is a super-user, with access to multi-tenant and system APIs. (required)	xs:boolean	“1” or “true” = super-user “0” or “false” = unprivileged

MultiTenantUserUpdateRequest > MultiTenantUserConfig element

The MultiTenantUserConfig element contains the following sub-element:

- SiloAccesses

MultiTenantUserUpdateRequest > MultiTenantUserConfig > SiloAccesses

A list of elements that define a user's access permissions.

MultiTenantUserUpdateRequest > MultiTenantUserConfig > SiloAccesses element

SiloAccesses contains the following sub-element:

- SiloAccess

MultiTenantUserUpdateRequest > MultiTenantUserConfig > SiloAccesses > SiloAccess

SiloAccess defines the access a user has to a specific silo, including their role and the objects they have access to.

MultiTenantUserUpdateRequest > MultiTenantUserConfig > SiloAccesses > SiloAccess attributes

Name	Description	Datatype	Range
all-groups	Defines whether the user has access to all groups within the silo. (required)	xs:boolean	"1" or "true" = access to all groups "0" or "false" = does not have access to all groups
all-sites	Defines whether the user has access to all sites within the silo. (required)	xs:boolean	"1" or "true" = access to all sites "0" or "false" = does not have access to all sites

Name	Description	Datatype	Range
default-silo	Sets this silo as the default silo. When the user logs onto the system, this is the silo they will be taken to if a silo is not specified. Only one SiloAccess within the UserConfig can be marked as the default-silo, otherwise an error is returned. (required)	xs:boolean	"1" or "true" = this is the default silo "0" or "false"= this is not the default silo
role-name	The name of the role to which a user is assigned. (required)	xs:string	built-in role names are: 'global-admin security-manager site-admin system-admin user custom other possible strings include any user-defined role names
silo-id	a string that uniquely identifies the silo (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 50 characters

MultiTenantUserUpdateRequest > MultiTenantUserConfig >SiloAccesses > SiloAccess sub-elements

The element SiloAccess has the following sub-elements:

- AllowedGroups
- AllowedSites

MultiTenantUserUpdateRequest > MultiTenantUserConfig > SiloAccesses > SiloAccess > AllowedGroups

A list of groups to which the user has access. If all-groups is set to true, no AllowedGroups can be specified.

MultiTenantUserUpdateRequest > MultiTenantUserConfig > SiloAccesses > SiloAccess > AllowedGroups sub-element

The AllowedGroups element contains zero or more of the following sub-element:

- AllowedGroup

MultiTenantUserUpdateRequest > MultiTenantUserConfig > SiloAccesses > SiloAccess > AllowedGroups > AllowedGroup

A group to which a user has access.

MultiTenantUserUpdateRequest > MultiTenantUserConfig > SiloAccesses > SiloAccess > AllowedGroups > AllowedGroup > attribute

Name	Description	Datatype	Range
id	The group ID. (required)	xs:positiveInteger	any integer greater than 0

MultiTenantUserUpdateRequest > MultiTenantUserConfig > SiloAccesses > SiloAccess > AllowedGroups > AllowedSites

A list of sites to which the user has access. If all-sites is set to true, no AllowedSites can be specified.

MultiTenantUserUpdateRequest > MultiTenantUserConfig > SiloAccesses > SiloAccess > AllowedGroups > AllowedSites attribute

Name	Description	Datatype	Range
id	The group ID. (required)	xs:positiveInteger	any integer greater than 0

MultiTenantUserUpdateRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<MultiTenantUserUpdateRequest session-
id="261E42019979542806A6667D59871183F2410E6D">
    <MultiTenantUserConfig id="4567" full-name="John Doe" user-
    name="jdoe" authsrcid="1" email="jdoe@company.com"
    password="abc123" superuser="false" enabled="true">
        <SiloAccesses>
```

```
                <SiloAccess all-groups="true" all-sites="true" role-
                name="site-admin" silo-id="pci-silo-002" default-
                silo="true"/>
            </SiloAccesses>
        </MultiTenantUserConfig>
    </MultiTenantUserUpdateRequest>
```

MultiTenantUserUpdateResponse attributes

Name	Description	Datatype	Range
sync-id	A user-specified identifier that can be used to ensure that a ticket request is not duplicated.(optional)	xs:string	any sequence of characters allowed in XML; of any length
user-id	ID of the updated user. (required)	xs:positive integer	any integer greater than zero

MultiTenantUserUpdateResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<MultiTenantUserUpdateResponse user-id="4567"/>
```

MultiTenantUserConfig

Retrieves user details for a specified multi-tenant user.

MultiTenantUserConfigRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length
user-id	The ID of the requested profile. (required)	xs:positiveInteger	any integer greater than 0

MultiTenantUserConfigRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<MultiTenantUserConfigRequest session-
id="894BB1D9FB797E89F5951F05BED5AAC1FD6EAF9E" user- id="4567"/>
```

MultiTenantUserConfigResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that can be used to ensure that a ticket request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

MultiTenantUserConfigResponse element

MultiTenantUserConfig has the following element:

- MultiTenantUserConfig

- MultiTenantUserConfig

Encapsulates information about the user across all the silos to which they have access.

MultiTenantUserConfigResponse > MultiTenantUserConfig attributes

Name	Description	Datatype	Range
authsrcid	The ID of the user's authentication source. (required)	xs:positiveInteger	any mathematical integer greater than 0
user-name	The login name of the user. (required)	xs:string	any sequence of characters allowed in XML; of any length
full-name	The full name of the user. (required)	xs:string	any sequence of characters allowed in XML; of any length
email	The e-mail address of the user. (optional)	xs:string	A valid e-mail, according to RFC822
password	The password to be set for the user. Only used for built-in authentication. (required)	xs:string	any sequence of characters allowed in XML; of any length
enabled	Enable or disable the user account. (required)	xs:boolean	“1” or “true” = enabled “0” or “false” = disabled

Name	Description	Datatype	Range
superuser	Account is a super-user, with access to multi-tenant and system APIs. (required)	xs:boolean	“1” or “true” = super-user “0” or “false” = unprivileged

MultiTenantUserConfigResponse > MultiTenantUserConfig element

The MultiTenantUserConfig element contains the following sub-element:

- SiloAccesses

MultiTenantUserConfigResponse > MultiTenantUserConfig > SiloAccesses

A list of elements that define a user's access permissions.

MultiTenantUserConfigResponse > MultiTenantUserConfig > SiloAccesses element

SiloAccesses contains the following sub-element:

- SiloAccess

MultiTenantUserConfigResponse > MultiTenantUserConfig > SiloAccesses > SiloAccess

SiloAccess defines the access a user has to a specific silo, including their role and the objects they have access to.

MultiTenantUserConfigResponse > MultiTenantUserConfig > SiloAccesses > SiloAccess attributes

Name	Description	Datatype	Range
all-groups	Defines whether the user has access to all groups within the silo. (required)	xs:boolean	"1" or "true" = access to all groups "0" or "false" = does not have access to all groups

Name	Description	Datatype	Range
all-sites	Defines whether the user has access to all sites within the silo. (required)	xs:boolean	"1" or "true" = access to all sites "0" or "false" = does not have access to all sites
default-silo	Sets this silo as the default silo. When the user logs onto the system, this is the silo they will be taken to if a silo is not specified. Only one SiloAccess within the UserConfig can be marked as the default-silo, otherwise an error is returned. (required)	xs:boolean	"1" or "true" = this is the default silo "0" or "false"= this is not the default silo
role-name	The name of the role to which a user is assigned. (required)	xs:string	built-in role names are: 'global-admin security-manager site-admin system-admin user custom other possible strings include any user-defined role names
silo-id	a string that uniquely identifies the silo (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 50 characters

MultiTenantUserConfigResponse > MultiTenantUserConfig >SiloAccesses > SiloAccess sub-elements

The element SiloAccess has the following sub-elements:

- AllowedGroups
- AllowedSites

MultiTenantUserConfigResponse > MultiTenantUserConfig > SiloAccesses > SiloAccess > AllowedGroups

A list of groups to which the user has access. If all-groups is set to true, no AllowedGroups can be specified.

MultiTenantUserConfigResponse > MultiTenantUserConfig > SiloAccesses > SiloAccess > AllowedGroups sub-element

The AllowedGroups element contains zero or more of the following sub-element:

- AllowedGroup

MultiTenantUserConfigResponse > MultiTenantUserConfig > SiloAccesses > SiloAccess > AllowedGroups > AllowedGroup

A group to which a user has access.

MultiTenantUserConfigResponse > MultiTenantUserConfig > SiloAccesses > SiloAccess > AllowedGroups > AllowedGroup > attribute

Name	Description	Datatype	Range
id	The group ID. (required)	xs:positiveInteger	any integer greater than 0

MultiTenantUserConfigResponse > MultiTenantUserConfig > SiloAccesses > SiloAccess > AllowedGroups > AllowedSites

A list of sites to which the user has access. If all-sites is set to true, no AllowedSites can be specified.

MultiTenantUserConfigResponse > MultiTenantUserConfig > SiloAccesses > SiloAccess > AllowedGroups > AllowedSites attribute

Name	Description	Datatype	Range
id	The group ID. (required)	xs:positiveInteger	any integer greater than 0

MultiTenantUserConfigResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<MultiTenantUserConfigResponse>
    <MultiTenantUserConfig id="4567" full-name="John Doe" user-
    name="jdoe" authsrcid="1" email="jdoe@company.com"
    superuser="false" enabled="true">
        <SiloAccesses>
            <SiloAccess all-groups="true" all-sites="true" role-
            name="site-admin" silo-id="pci-silo-002" default-
            silo="true"/>
        </SiloAccesses>
    </MultiTenantUserConfig>
</MultiTenantUserConfigResponse>
```

MultiTenantUserDelete

Deletes a specified multi-tenant user.

MultiTenantUserDeleteRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length
user-id	The ID of the user to be deleted.*	xs:int	any integer
user-name	The logon name of the user to be delete.*	xs:int	any integer

* Only user-id or user-name should be specified, but one of these attributes is required.

MultiTenantUserDeleteRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<MultiTenantUserDeleteRequest session-
id="814923161274ADEEDD625B8EBC5DB0E17BF00388" user- id="4567"/>
```

MultiTenantUserDeleteResponse attribute

Name	Description	Datatype	Range
sync-id	A user-specified identifier that can be used to ensure that a ticket request is not duplicated. (optional)	xs:string	any sequence of characters allowed in XML; of any length

MultiTenantUserDeleteResponse element

An empty MultiTenantUserDeleteResponse element is returned if the deletion is successful.

MultiTenantUserDeleteResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<MultiTenantUserDeleteResponse/>
```

Silo Profiles

SiloProfileCreate

Creates a new silo profile.

SiloProfileCreateRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileCreateRequest element

SiloProfileCreateRequest contains the following element:

- SiloProfileConfig

SiloProfileCreateRequest > SiloProfileConfig

Encapsulates information about the silo profile.

SiloProfileCreateRequest > SiloProfileConfig attributes

Name	Description	Datatype	Range
id	Unique silo profile identifier. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters
name	Display name of the silo profile. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters

Name	Description	Datatype	Range
description	Description of the silo profile. (optional)	xs:string	a sequence of characters (letters, numerals, hyphens, underscores, and @ symbol--the first character cannot be a hyphen); maximum length is 1024 characters
all-licensed-modules	All licensed modules are granted to silos with this profile. (required)	xs:boolean	"1" or "true" = enable all licensed modules "0" or "false" = enable specific modules
all-global-engines	All global engines are available to silos with this profile. (required)	xs:boolean	"1" or "true" = enable all engines; "0" or "false" = enable specific engines
all-global-report-templates	All global report templates are available to silos with this profile. (required)	xs:boolean	"1" or "true" = enable all report templates; "0" or "false" = enable specific report templates
all-global-scan-templates	All global scan templates are available to silos with this profile. (required)	xs:boolean	"1" or "true" = enable all scan templates; "0" or "false" = enable specific scan templates

SiloProfileCreateRequest > SiloProfileConfig elements

The SiloProfileConfig element can contain the following sub-elements:

- GlobalReportTemplates
- GlobalScanEngines
- GlobalScanTemplates
- LicensedModules
- RestrictedReportFormats
- RestrictedReportSections

SiloProfileCreateRequest > SiloProfileConfig > GlobalReportTemplates

The GlobalReportTemplates element is used if the all-global-report-templates attribute of SiloProfileConfig is set to false. It contains a list of global report templates available to silos with this profile.

SiloProfileCreateRequest > SiloProfileConfig > GlobalReportTemplates element

The GlobalReportTemplates element contains zero or more of the following sub-element:

- GlobalReportTemplate

SiloProfileCreateRequest > SiloProfileConfig > GlobalReportTemplates > GlobalReportTemplate

A global report template available to the silo with this profile.

SiloProfileCreateRequest > SiloProfileConfig > GlobalReportTemplates > GlobalReportTemplate attribute

Name	Description	Datatype	Range
name	the name of a global report template (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileCreateRequest > SiloProfileConfig > GlobalScanEngines

The GlobalScanEngines element is used if the all-global-engines attribute of SiloProfileConfig is set to false. It contains a list of global scan engines available to silos with this profile.

SiloProfileCreateRequest > SiloProfileConfig > GlobalScanEngines element

The GlobalScanEngines element contains zero or more of the following sub-element:

- GlobalScanEngine

SiloProfileCreateRequest > SiloProfileConfig > GlobalScanEngines > GlobalScanEngine

A global scan engine available to the silo with this profile.

SiloProfileCreateRequest > SiloProfileConfig > GlobalScanEngines > GlobalScanEngine attribute

Name	Description	Datatype	Range
name	the name of a global scan engine (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileCreateRequest > SiloProfileConfig > GlobalScanTemplates

The GlobalScanTemplates element is used if the all-global-scan-templates attribute of SiloProfileConfig is set to false. It contains a list of global scan templates available to silos with this profile.

SiloProfileCreateRequest > SiloProfileConfig > GlobalScanTemplates element

The GlobalScanTemplates element contains zero or more of the following sub-element:

- GlobalScanTemplate

SiloProfileCreateRequest > SiloProfileConfig > GlobalScanTemplates > GlobalScanTemplate

A global scan template available to the silo with this profile.

SiloProfileCreateRequest > SiloProfileConfig > GlobalScanTemplates > GlobalScanTemplate attribute

Name	Description	Datatype	Range
name	the name of a global scan template (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileCreateRequest > SiloProfileConfig > LicensedModules

The LicensedModules element is used if the all-licensed-modules attribute of SiloProfileConfig is set to false. It contains a list of licensed modules granted to silos with this profile.

SiloProfileCreateRequest > SiloProfileConfig > LicensedModules element

The LicensedModules element contains zero or more of the following sub-element:

- LicensedModule

SiloProfileCreateRequest > SiloProfileConfig > LicensedModules > LicensedModule

A licensed module granted to the silo with this profile.

SiloProfileCreateRequest > SiloProfileConfig > LicensedModules > LicensedModule attribute

Name	Description	Datatype	Range
name	the name of a licensed module (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileCreateRequest > SiloProfileConfig > RestrictedReportFormats

Defines report formats that cannot be used in the creation of report templates and report generation.

SiloProfileCreateRequest > SiloProfileConfig > RestrictedReportFormats element

The RestrictedReportFormats element can contain the following sub-element:

- RestrictedReportFormat

SiloProfileCreateRequest > SiloProfileConfig > RestrictedReportFormats > RestrictedReportFormat

Defines report formats that cannot be used in the creation of report templates and report generation.

SiloProfileCreateRequest > SiloProfileConfig > RestrictedReportFormats > RestrictedReportFormat attribute

Name	Description	Datatype	Range
name	the name of the report format that is being restricted (required)	xs:reportFormatType	The following values are acceptable: “csv” “db” “html” “ns-xml” “pdf” “qualys-xml” “raw-xml” “raw-xml-v2” “rtf” “scap-xml” “text”

SiloProfileCreateRequest > SiloProfileConfig > RestrictedReportSections

Defines report sections that only specifically permitted users can see and use in the creation of report templates and report generation.

SiloProfileCreateRequest > SiloProfileConfig > RestrictedReportSections element

The RestrictedReportSections element can contain the following sub-element:

- RestrictedReportSection

SiloProfileCreateRequest > SiloProfileConfig > RestrictedReportSections > RestrictedReportSection attribute

Name	Description	Datatype	Range
name	the name of the report section that is being restricted (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters

SiloProfileCreateRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<SiloProfileCreateRequest session-
id="E782149DD1498AF7144BEBEEF25686C308932554" sync-id="SILO-PROFILE-
CREATE-0009-009">
    <SiloProfileConfig all-global-report-templates="1" all-global-
    engines="1" all-global-scan-templates="1" all-licensed-modules="1"
    description="my description" id="myprofile-10" name="My SiloProfile
    10">
        <RestrictedReportSections>
            <RestrictedReportSection name="BaselineComparison"/>
            <RestrictedReportSection name="ScanSettings"/>
            <RestrictedReportSection name="SystemOverview"/>
        </RestrictedReportSections>
    </SiloProfileConfig>
</SiloProfileCreateRequest>
```

SiloProfileCreateResponse attributes

Name	Description	Datatype	Range
sync-id	A user-specified identifier that can be used to ensure that a ticket request is not duplicated. (optional)	xs:string	any sequence of characters allowed in XML; of any length
silo-profile-id	ID of the newly created silo profile. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters

SiloProfileCreateResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<SiloProfileCreateResponse silo-profile-id="global-profile"/>
```

SiloProfileListing

Returns a summary listing of silo profiles.

SiloProfileListingRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileListingRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<SiloProfileListingRequest session-
id="A7F2B8625847250122C2313C9A8C1800F971A27D"/>
```

SiloProfileListingResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that can be used to ensure that a ticket request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileListingResponse element

SiloProfileListingResponse contains the following sub-element:

- SiloProfileSummaries

SiloProfileListingResponse > SiloProfileSummaries

A list of silo profile summaries.

SiloProfileListingResponse > SiloProfileSummaries element

SiloProfileSummaries contains zero or more of the following element:

- SiloProfileSummary

SiloProfileListingResponse > SiloProfileSummaries > SiloProfileSummary

The silo profile summary encapsulates information about the silo profiles.

SiloProfileListingResponse > SiloProfileSummaries > SiloProfileSummary attributes

Name	Description	Datatype	Range
id	Unique silo profile identifier. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters
name	Display name of the silo profile. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters
description	Description of the silo profile. (optional)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 2048 characters
global-report-template-count	The number of report templates available to the silo. (required)	xs:positiveInteger	any mathematical integer greater than 0
global-scan-engine-count	The number scan engines that are available to the silo. (required)	xs:positiveInteger	any mathematical integer greater than 0
global-scan-template-count	The number of scan templates available to the silo. (required)	xs:positiveInteger	any mathematical integer greater than 0
licensed-module-count	The number of licensed modules available to the silo. (required)	xs:positiveInteger	any mathematical integer greater than 0

Name	Description	Datatype	Range
restricted-report-section-count	The number of report sections restricted in the silo. (required)	xs:positiveInteger	any mathematical integer greater than 0
all-licensed-modules	All licensed modules are granted to silos with this profile. (required)	xs:boolean	"1" or "true" = enable all licensed modules; "0" or "false" = enable specific modules
all-global-engines	All global engines are available to silos with this profile. (required)	xs:boolean	"1" or "true" = enable all engines; "0" or "false" = enable specific engines
all-global-report-templates	All global report templates are available to silos with this profile. (required)	xs:boolean	"1" or "true" = enable all report templates; "0" or "false" = enable specific report templates
all-global-scan-templates	All global scan templates are available to silos with this profile. (required)	xs:boolean	"1" or "true" = enable all scan templates; "0" or "false" = enable specific scan templates

SiloProfileListingResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<SiloProfileListingResponse sync-id="SILO-PROFILE-LISTING-0002-002">
    <SiloProfileSummaries>
        <SiloProfileSummary restricted-report-section-count="0"
        licensed-module-count="7" global- scan-template-count="15"
        global-scan-engine-count="2" global-report-template-count="13"
        id="default" name="Default Silo Profile" description="Default
        Silo Profile" all-licensed-mod- ules="true" all-global-scan-
        templates="true" all-global-engines="true" all-global-report-
        tem- plates="true"/>
        <SiloProfileSummary restricted-report-section-count="2"
        licensed-module-count="7" global- scan-template-count="2"
        global-scan-engine-count="2" global-report-template-count="2"
        id="mypro- file-1" name="My SiloProfile 1" description="my
        description" all-licensed-modules="true" all- global-scan-
        templates="false" all-global-engines="false" all-global-report-
        templates="false"/>
    </SiloProfileSummaries>
</SiloProfileListingResponse>
```

SiloProfileUpdate

Updates silo profiles.

SiloProfileUpdateRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileUpdateRequest element

The SiloProfileUpdateRequest element contains the following sub-element:

- SiloProfileConfig

SiloProfileUpdateRequest > SiloProfileConfig

Encapsulates information about the silo profile.

SiloProfileUpdateRequest > SiloProfileConfig attributes

Name	Description	Datatype	Range
id	Unique silo profile identifier. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters
name	Display name of the silo profile. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters
description	Description of the silo profile. (optional)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 1024 characters
all-licensed-modules	All licensed modules are granted to silos with this profile. (required)	xs:boolean	"1" or "true" = enable all licensed modules"0" or "false" = enable specific modules
all-global-engines	All global engines are available to silos with this profile. (required)	xs:boolean	"1" or "true" = enable all engines "0" or "false" = enable specific engines
all-global-report-templates	All global report templates are available to silos with this profile. (required)	xs:boolean	"1" or "true" = enable all report templates "0" or "false" = enable specific report templates

Name	Description	Datatype	Range
all-global-scan-templates	All global scan templates are available to silos with this profile. (required)	xs:boolean	"1" or "true" = enable all scan templates "0" or "false" = enable specific scan templates

SiloProfileUpdateRequest > SiloProfileConfig

Encapsulates information about the silo profile.

SiloProfileUpdateRequest > SiloProfileConfig elements

The SiloProfileConfig element can contain the following sub-elements:

- GlobalReportTemplates
- GlobalScanEngines
- GlobalScanTemplates
- LicensedModules
- RestrictedReportFormats
- RestrictedReportSections

SiloProfileUpdateRequest > SiloProfileConfig > GlobalReportTemplates

The GlobalReportTemplates element is used if the all-global-report-templates attribute of SiloProfileConfig is set to false. It contains a list of global report templates available to silos with this profile.

SiloProfileUpdateRequest > SiloProfileConfig > GlobalReportTemplates element

The GlobalReportTemplates element contains zero or more of the following sub-element:

- GlobalReportTemplate

SiloProfileUpdateRequest > SiloProfileConfig > GlobalReportTemplates > GlobalReportTemplate

A global report template available to the silo with this profile.

SiloProfileUpdateRequest > SiloProfileConfig > GlobalReportTemplates > GlobalReportTemplate attribute

Name	Description	Datatype	Range
name	the name of a global report template (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileUpdateRequest > SiloProfileConfig > GlobalScanEngines

The GlobalScanEngines element is used if the all-global-engines attribute of SiloProfileConfig is set to false. It contains a list of global scan engines available to silos with this profile.

SiloProfileUpdateRequest > SiloProfileConfig > GlobalScanEngines element

The GlobalScanEngines element contains zero or more of the following sub-element:

- GlobalScanEngine

SiloProfileUpdateRequest > SiloProfileConfig > GlobalScanEngines > GlobalScanEngine

A global scan engine available to the silo with this profile.

SiloProfileUpdateRequest > SiloProfileConfig > GlobalScanEngines > GlobalScanEngine attribute

Name	Description	Datatype	Range
name	the name of a global scan engine (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileUpdateRequest > SiloProfileConfig > GlobalScanTemplates

The GlobalScanTemplates element is used if the all-global-scan-templates attribute of SiloProfileConfig is set to false. It contains a list of global scan templates available to silos with this profile.

SiloProfileUpdateRequest > SiloProfileConfig > GlobalScanTemplates element

The GlobalScanTemplates element contains zero or more of the following sub-element:

- GlobalScanTemplate

SiloProfileUpdateRequest > SiloProfileConfig > GlobalScanTemplates > GlobalScanTemplate

A global scan template available to the silo with this profile.

SiloProfileUpdateRequest > SiloProfileConfig > GlobalScanTemplates > GlobalScanTemplate attribute

Name	Description	Datatype	Range
name	the name of a global scan template (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileUpdateRequest > SiloProfileConfig > LicensedModules

The LicensedModules element is used if the all-licensed-modules attribute of SiloProfileConfig is set to false. It contains a list of licensed modules granted to silos with this profile.

SiloProfileUpdateRequest > SiloProfileConfig > LicensedModules element

The LicensedModules element contains zero or more of the following sub-element:

- LicensedModule

SiloProfileUpdateRequest > SiloProfileConfig > LicensedModules > LicensedModule

A licensed module granted to the silo with this profile.

SiloProfileUpdateRequest > SiloProfileConfig > LicensedModules > LicensedModule attribute

Name	Description	Datatype	Range
name	the name of a licensed module (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileUpdateRequest > SiloProfileConfig > RestrictedReportFormats

Defines report formats that cannot be used in the creation of report templates and report generation.

SiloProfileUpdateRequest > SiloProfileConfig > RestrictedReportFormats element

The RestrictedReportFormats element can contain the following sub-element:

- RestrictedReportFormat

SiloProfileUpdateRequest > SiloProfileConfig > RestrictedReportFormats > RestrictedReportFormat

Defines report formats that cannot be used in the creation of report templates and report generation.

SiloProfileUpdateRequest > SiloProfileConfig > RestrictedReportFormats > RestrictedReportFormat attribute

Name	Description	Datatype	Range
name	the name of the report format that is being restricted (required)	xs:reportFormatType	The following values are acceptable: “csv” “db” “html” “ns-xml” “pdf” “qualys-xml” “raw-xml” “raw-xml-v2” “rtf” “scap-xml” “text”

SiloProfileUpdateRequest > SiloProfileConfig > RestrictedReportSections

Defines report sections that only specifically permitted users can see and use in the creation of report templates and report generation.

SiloProfileUpdateRequest > SiloProfileConfig > RestrictedReportSections element

The RestrictedReportSections element can contain the following sub-element:

- RestrictedReportSection

SiloProfileUpdateRequest > SiloProfileConfig > RestrictedReportSections > RestrictedReportSection attribute

Name	Description	Datatype	Range
name	the name of the report section that is being restricted (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters

SiloProfileUpdateRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<SiloProfileUpdateRequest session-
id="36FABBDFEEBFAAFFE89178640381D35D95889D72">
    <SiloProfileConfig id="global-profile" name="Global profile"
    description="A profile with access to all templates and modules"
    all-licensed-modules="true" all-global-engines="false" all-global-
    report-templates="true" all-global-scan-templates="true">
        <GlobalScanEngines>
            <GlobalScanEngine name="pen-test-engine-103"/>
        </GlobalScanEngines>
        <RestrictedReportSections>
            <RestrictedReportSection name="BaselineComparison"/>
        </RestrictedReportSections>
    </SiloProfileConfig>
</SiloProfileUpdateRequest>
```

SiloProfileUpdateResponse attributes

Name	Description	Datatype	Range
sync-id	a user-specified identifier that can be used to ensure that a ticket request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length
silo-profile-id	ID of the updated silo profile. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters

SiloProfileUpdateResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<SiloProfileUpdateResponse silo-profile-id="global-profile"/>
```

SiloProfileConfig

Encapsulates information about the silo profile.

SiloProfileConfigRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length
silo-profile-id	the ID of the silo profile being requested (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters

SiloProfileConfigRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<SiloProfileConfigRequest session-
id="781A27A1942F957B5E282A307D39695E6D3EFBB4" silo-profile- id="pci-
profile"/>
```

SiloProfileConfigResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileConfigResponse element

SiloProfileConfigResponse contains the following element:

- SiloProfileConfig

SiloProfileConfigResponse > SiloProfileConfig attributes

Name	Description	Datatype	Range
id	Unique silo profile identifier. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters
name	Display name of the silo profile. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters
description	Description of the silo profile. (optional)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 2048 characters
all-licensed-modules	All licensed modules are granted to silos with this profile. (required)	xs:boolean	"1" or "true" = enable all licensed modules; "0" or "false" = enable specific modules
all-global-engines	All global engines are available to silos with this profile. (required)	xs:boolean	"1" or "true" = enable all engines; "0" or "false" = enable specific engines
all-global-report-templates	All global report templates are available to silos with this profile. (required)	xs:boolean	"1" or "true" = enable all report templates; "0" or "false" = enable specific report templates
all-global-scan-templates	All global scan templates are available to silos with this profile. (required)	xs:boolean	"1" or "true" = enable all scan templates"0" or "false" = enable specific scan templates

SiloProfileConfigResponse > SiloProfileConfig elements

The SiloProfileConfig element can contain the following sub-elements:

- GlobalReportTemplates
- GlobalScanEngines
- GlobalScanTemplates
- LicensedModules
- RestrictedReportFormats
- RestrictedReportSections

SiloProfileConfigResponse > SiloProfileConfig > GlobalReportTemplates

The GlobalReportTemplates element is used if the all-global-report-templates attribute of SiloProfileConfig is set to false. It contains a list of global report templates available to silos with this profile.

SiloProfileConfigResponse > SiloProfileConfig > GlobalReportTemplates element

The GlobalReportTemplates element contains zero or more of the following sub-element:

- GlobalReportTemplate

SiloProfileConfigResponse > SiloProfileConfig > GlobalReportTemplates > GlobalReportTemplate

A global report template available to the silo with this profile.

SiloProfileConfigResponse > SiloProfileConfig > GlobalReportTemplates > GlobalReportTemplate attribute

Name	Description	Datatype	Range
name	the name of a global report template (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileConfigResponse > SiloProfileConfig > GlobalScanEngines

The GlobalScanEngines element is used if the all-global-engines attribute of SiloProfileConfig is set to false. It contains a list of global scan engines available to silos with this profile.

SiloProfileConfigResponse > SiloProfileConfig > GlobalScanEngines element

The GlobalScanEngines element contains zero or more of the following sub-element:

- GlobalScanEngine

SiloProfileConfigResponse > SiloProfileConfig > GlobalScanEngines > GlobalScanEngine

A global scan engine available to the silo with this profile.

SiloProfileConfigResponse > SiloProfileConfig > GlobalScanEngines > GlobalScanEngine attribute

Name	Description	Datatype	Range
name	the name of a global scan engine (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileConfigResponse > SiloProfileConfig > GlobalScanTemplates

The GlobalScanTemplates element is used if the all-global-scan-templates attribute of SiloProfileConfig is set to false. It contains a list of global scan templates available to silos with this profile.

SiloProfileConfigResponse > SiloProfileConfig > GlobalScanTemplates element

The GlobalScanTemplates element contains zero or more of the following sub-element:

- GlobalScanTemplate

SiloProfileConfigResponse > SiloProfileConfig > GlobalScanTemplates > GlobalScanTemplate

A global scan template available to the silo with this profile.

SiloProfileConfigResponse > SiloProfileConfig > GlobalScanTemplates > GlobalScanTemplate attribute

Name	Description	Datatype	Range
name	the name of a global scan template (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileConfigResponse > SiloProfileConfig > LicensedModules

The LicensedModules element is used if the all-licensed-modules attribute of SiloProfileConfig is set to false. It contains a list of licensed modules granted to silos with this profile.

SiloProfileConfigResponse > SiloProfileConfig > LicensedModules element

The LicensedModules element contains zero or more of the following sub-element:

- LicensedModule

SiloProfileConfigResponse > SiloProfileConfig > LicensedModules > LicensedModule

A licensed module granted to the silo with this profile.

SiloProfileConfigResponse > SiloProfileConfig > LicensedModules > LicensedModule attribute

Name	Description	Datatype	Range
name	the name of a licensed module (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileConfigResponse > SiloProfileConfig > RestrictedReportFormats

Defines report formats that cannot be used in the creation of report templates and report generation.

SiloProfileConfigResponse > SiloProfileConfig > RestrictedReportFormats element

The RestrictedReportFormats element can contain the following sub-element:

- RestrictedReportFormat

SiloProfileConfigResponse > SiloProfileConfig > RestrictedReportFormats > RestrictedReportFormat

Defines report formats that cannot be used in the creation of report templates and report generation.

SiloProfileConfigResponse > SiloProfileConfig > RestrictedReportFormats > RestrictedReportFormat attribute

Name	Description	Datatype	Range
name	the name of the report format that is being restricted (required)	xs:reportFormatType	The following values are acceptable: “csv” “db” “html” “ns-xml” “pdf” “qualys-xml” “raw-xml” “raw-xml-v2” “rtf” “scap-xml” “text”

SiloProfileConfigResponse > SiloProfileConfig > RestrictedReportSections

Defines report sections that only specifically permitted users can see and use in the creation of report templates and report generation.

SiloProfileConfigResponse > SiloProfileConfig > RestrictedReportSections element

The RestrictedReportSections element can contain the following sub-element:

- RestrictedReportSection

SiloProfileConfigResponse > SiloProfileConfig > RestrictedReportSections > RestrictedReportSection attribute

Name	Description	Datatype	Range
name	the name of the report section that is being restricted (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters

SiloProfileConfigResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<SiloProfileConfigResponse sync-id="SILO-PROFILE-CREATE-0002-002">
    <SiloProfileConfig id="myprofile-10" name="My SiloProfile 10"
    description="my description" all-licensed-modules="true" all-
    global-scan-templates="true" all-global-engines="true" all-global-
    report- templates="true">
        <GlobalReportTemplates/>
        <GlobalScanEngines/>
        <GlobalScanTemplates/>
        <LicensedModules/>
        <RestrictedReportSections>
            <RestrictedReportSection name="BaselineComparison"/>
        </RestrictedReportSections>
    </SiloProfileConfig>
</SiloProfileConfigResponse>
```

SiloProfileDelete

Deletes a specified silo profile.

SiloProfileDeleteRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

Name	Description	Datatype	Range
silo-profile-id	The ID of the silo profile to be deleted. (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileDeleteRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<SiloProfileDeleteRequest session-
id="CACE8566CB7E36C71CAE35E0CE3D429A4D4F6202" silo-profile- id="pci-
profile"/>
```

SiloProfileDeleteResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloProfileDeleteResponse element

An empty SiloProfileDeleteResponse element is returned if the deletion is successful.

SiloProfileDeleteResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<SiloProfileDeleteResponse/>
```

Silo Management

This section covers all requests and responses related to managing silos.

SiloCreate

Creates a new silo.

SiloCreateRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloCreateRequest element

SiloCreateRequest contains the following element:

- SiloConfig

SiloCreateRequest > SiloConfig

Contains the complete configuration settings for a silo.

SiloCreateRequest > SiloConfig attributes

Name	Description	Datatype	Range
id	a string that uniquely identifies the silo. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 50 characters

Name	Description	Datatype	Range
name	The name of the silo as it will be displayed. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters
silo-profile-id	The ID of the silo profile associated with this silo. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters
description	The full description of the silo. (optional)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 2048 characters
max-assets	The maximum number of assets that can be scanned. (required)	xs:nonNegativeInteger	any integer greater than or equal to 0
max-hosted-assets	The maximum number of assets that can be scanned with hosted scan engines. (required)	xs:nonNegativeInteger	any integer greater than or equal to 0
max-users	The maximum number of users that can be associated with this silo. (required)	xs:nonNegativeInteger	any integer greater than or equal to 0

SiloCreateRequest > SiloConfig sub-elements

The SiloConfig element contains the following sub-elements:

- Merchant
- Organization

SiloCreateRequest > SiloConfig > Merchant (optional)

A company that performs credit card transactions.

SiloCreateRequest > SiloConfig > Merchant attributes

These attributes are pieces of information that must be submitted by a merchant in the Payment Card Industry (PCI) Data Security Standard (DSS) Attestation of Onsite Assessments–Merchants. Choose all industries that apply. You also can specify other industries as needed. See OtherIndustries (on page "SiloCreateRequest > SiloConfig > OtherIndustries" on page 236).

Name	Description	Datatype	Range
acquirer-relationship	whether the merchant has a relationship with more than one companies that provides credit card processing (required)	xs:boolean	“1” or “true” “0” or “false”
agent-relationship	whether the merchant has a relationship with a agents such as a gateway, a Web hosting company, or a loyalty program (required)	xs:boolean	“1” or “true” “0” or “false”
payment-application	the software application used for processing credit card transactions (required)	xs:string	any sequence of characters allowed in XML; of any length
payment-version	the version of the software application used for processing credit card transactions (required)	xs:string	any sequence of characters allowed in XML; of any length
ecommerce	e-commerce industry (required)	xs:boolean	“1” or “true” “0” or “false”
grocery	grocery industry (required)	xs:boolean	“1” or “true” “0” or “false”
mail-order	mail-order or telephone-order industry (required)	xs:boolean	“1” or “true” “0” or “false”
petroleum	petroleum industry (required)	xs:boolean	“1” or “true” ; “0” or “false”
retail	retail industry (required)	xs:boolean	“1” or “true” ; “0” or “false”

Name	Description	Datatype	Range
telecommunication	telecommunication industry (required)	xs:boolean	“1” or “true” ; “0” or “false”
travel	travel industry (required)	xs:boolean	“1” or “true” ; “0” or “false”
url	the merchant's Web site URL (required)	xs:string	any sequence of characters allowed in XML; of any length
company	the name of the merchant's company (required)	xs:string	any sequence of characters allowed in XML; of any length
email-address	the e-mail address of an entity representing the merchant (optional)	xs:string	any sequence of characters allowed in XML; of any length
first-name	the first name of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
last-name	the last name of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
phone-number	the phone number of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
title	the title of an entity representing the merchant (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloCreateRequest > SiloConfig > Merchant sub-elements

The Merchant element contains the following sub-elements:

- DBAs
- OtherIndustries
- QSA
- Address

SiloCreateRequest > SiloConfig > Merchant > Address

The merchant's street address.

SiloCreateRequest > SiloConfig > Merchant > Address attributes

Name	Description	Datatype	Range
city	the merchant's city (required)	xs:string	any sequence of characters allowed in XML; of any length
country	the merchant’s country (required)	xs:string	any sequence of characters allowed in XML; of any length
line 1	the first line of the merchant’s street address (required)	xs:string	any sequence of characters allowed in XML; of any length
line 2	the second line of the merchant’s street address (optional)	xs:string	any sequence of characters allowed in XML; of any length
state	the merchant’s state (required)	xs:string	any sequence of characters allowed in XML; of any length
zip	the merchant’s zip code (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloCreateRequest > SiloConfig > Merchant > DBAs

A pluralized element that holds multiple DBA elements.

SiloCreateRequest > SiloConfig > Merchant > DBAs sub-element

DBAs contains the following sub-element:

- DBA

SiloCreateRequest > SiloConfig > Merchant > DBAs > DBA

An acronym for “Doing business as.” It is an alternate name under which the merchant operates.

SiloCreateRequest > SiloConfig > Merchant > DBAs > DBA attribute

Name	Description	Datatype	Range
name	the alternate name for the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloCreateRequest > SiloConfig > OtherIndustries

Industries that do not fit into the Merchant industry categories listed in the PCI-DSS Attestation of Onsite Assessments–Merchants. See Merchant (optional) (on page "SiloCreateRequest >

SiloConfig > Merchant (optional)" on page 233).

SiloCreateRequest > SiloConfig > OtherIndustries sub-element

OtherIndustries has the following sub-element:

- Industry

SiloCreateRequest > SiloConfig > OtherIndustries > Industry

An industry not listed in the Payment Card Industry (PCI) Data Security Standard (DSS) Attestation of Onsite Assessments–Merchants.

Name	Description	Datatype	Range
name	the name of the industry (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloCreateRequest > SiloConfig > QSA (optional)

The qualified security assessor.

SiloCreateRequest > SiloConfig > QSA attributes

Name	Description	Datatype	Range
url	the merchant's Web site URL (required)	xs:string	any sequence of characters allowed in XML; of any length
company	the name of the merchant's company (required)	xs:string	any sequence of characters allowed in XML; of any length
email-address	the e-mail address of an entity representing the merchant (optional)	xs:string	any sequence of characters allowed in XML; of any length
first-name	the first name of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
last-name	the first name of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
phone-number	the phone number of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length

Name	Description	Datatype	Range
title	the title of an entity representing the merchant (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloCreateRequest > SiloConfig > QSA sub-element

QSA contains the following sub-element:

- Address

SiloCreateRequest > SiloConfig > QSA > Address

The merchant's street address.

SiloCreateRequest > SiloConfig > Organization

The contact information of a silo tenant.

SiloCreateRequest > SiloConfig > Organization attributes

Name	Description	Datatype	Range
url	the tenant's Web site URL (required)	xs:string	any sequence of characters allowed in XML; of any length
company	the name of the tenant's company (required)	xs:string	any sequence of characters allowed in XML; of any length
email-address	the e-mail address of an entity representing the tenant (optional)	xs:string	any sequence of characters allowed in XML; of any length
first-name	the first name of an entity representing the tenant (required)	xs:string	any sequence of characters allowed in XML; of any length
last-name	the last name of an entity representing the tenant (required)	xs:string	any sequence of characters allowed in XML; of any length
phone-number	the phone number of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
title	the title of an entity representing the merchant (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloCreateRequest example

```
<SiloCreateRequest sync-id="SILO-CREATE-0003-003" session-
id="F9CD2D8AA3208284F101A411549EA5CB6897FBF4">
    <SiloConfig description="test silo" name="test silo" id="silo-3"
    silo-profile-id="myprofile-1" max-assets="1000" max-users="25" max-
    hosted-assets="0">
        <Merchant company="testcompany" email-address="test@test.com"
        first-name="test" last-name="testing" phone-number="12345"
        title="t" url="www.test.com" acquirer-relationship="true" agent-
        relationship="true" ecommerce="true" grocery="true" mail-
        order="true" payment-application="application" payment-
        version="version" petroleum="true" retail="true"
        telecommunication="true" travel="true">
        <Address city="Bangalore" country="India" line1="Hosur"
        line2="ITPL"
        state="karnataka" zip="560000"/>
            <DBAs>
                    <DBA name="TestDBA"/>
            </DBAs>
            <OtherIndustries>
                    <Industry name="TestIndustry"/>
            </OtherIndustries>
            <QSA company="testcmp" email-address="testemail@qsa.com"
            first-name="first" last- name="last" phone-
            number="1234567890" title="test" url="www.qsa.com">
                    <Address city="Bangalore" country="India"
                    line1="KTPO" line2="Whitefield" state="karnataka"
                    zip="560001"/>
            </QSA>
        </Merchant>
        <Organization company="testorg" email-address="test@org.com"
        first-name="t" last- name="lastname" phone-number="1234567890"
        title="test" url="www.example.com">
            <Address city="Bangalore" country="India"
            line1="mahadevapura" line2="ITPL" state="karnataka"
            zip="560002"/>
        </Organization>
    </SiloConfig>
</SiloCreateRequest>
```

SiloCreateResponse attributes

Name	Description	Datatype	Range
id	a string that uniquely identifies the silo (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 50 characters
sync-id	A user-specified identifier that can be used to ensure that a request is not duplicated. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters

SiloCreateResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<SiloCreateResponse id="pci-silo-001"/>
```

SiloListing

Provides a list of all silos and information about them.

SiloListingRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloListingRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<SiloListingRequest session-
id="A7F2B8625847250122C2313C9A8C1800F971A27D"/>
```

SiloListingResponse attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a response is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloListingResponse element

SiloListingResponse contains the following element:

- SiloSummaries

SiloListingResponse > SiloSummaries

Provides list of silo summaries.

SiloListingResponse > SiloSummaries sub-element

SiloSummaries contains the following sub-element:

- SiloSummary

SiloListingResponse > SiloSummaries > SiloSummary

Provides summary information about silos.

SiloListingResponse > SiloSummaries > SiloSummary attributes

Name	Description	Datatype	Range
description	a description of the silo (optional)	xs:string	any sequence of characters allowed in XML; of any length
name	the name of the silo (required)	xs:string	any sequence of characters allowed in XML; of any length
id	a unique identifier for the silo (required)	xs:string	any sequence of characters allowed in XML; of any length
silo-profile-id	a unique identifier for the silo profile on which the silo is based (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloListingResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<SiloListingResponse sync-id="SILO-LISTING-0002-002">
    <SiloSummaries>
        <SiloSummary id="accoutingsilo" name="Accounting department"
        description="Silo for accounting department" silo-profile-
        id="Departmental silos">
    </SiloSummaries>
</SiloListingResponse>
```

SiloConfig

Contains the complete configuration settings for a silo.

SiloConfigRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length
id	a string that uniquely identifies the silo (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 50 characters
name	A user-specified name for the silo. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters

SiloConfigRequest elements

SiloConfigRequest has no elements.

SiloConfigRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<SiloConfigRequest session-
id="2E4B328600D5885981CC866CCE23CB94998E283C" silo-id=""/>
```

SiloConfigResponse attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
id	An identifier for the silo. (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloConfigResponse element

SiloConfigResponse contains the following element:

- SiloConfig

SiloConfigResponse > SiloConfig

Contains the complete configuration settings for a silo.

SiloConfigResponse > SiloConfig attributes

Name	Description	Datatype	Range
id	a string that uniquely identifies the silo (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 50 characters
name	The name of the silo as it will be displayed. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters
silo-profile-id	The ID of the silo profile associated with this silo. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters
description	The full description of the silo. (optional)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 2048 characters

Name	Description	Datatype	Range
max-assets	The maximum number of assets that can be scanned. (required)	xs:nonNegativeInteger	any integer greater than or equal to 0
max-hosted-assets	The maximum number of assets that can be scanned with hosted scan engines. (required)	xs:nonNegativeInteger	any integer greater than or equal to 0
max-users	The maximum number of users that can be associated with this silo. (required)	xs:nonNegativeInteger	any integer greater than or equal to 0

SiloConfigResponse > SiloConfig sub-elements

The SiloConfig element contains the following sub-elements:

- Merchant
- Organization

SiloConfigResponse > SiloConfig > Merchant (optional)

A company that performs credit card transactions.

SiloConfigResponse > SiloConfig > Merchant attributes

These attributes are pieces of information that must be submitted by a merchant in the Payment Card Industry (PCI) Data Security Standard (DSS) Attestation of Onsite Assessments– Merchants. Choose all industries that apply. You also can specify other industries as needed. See *SiloConfigResponse > SiloConfig > OtherIndustries* on page 247.

Name	Description	Datatype	Range
acquirer-relationship	whether the merchant has a relationship with more than one companies that provides credit card processing (required)	xs:boolean	“1” or “true” “0” or “false”

Name	Description	Datatype	Range
agent-relationship	whether the merchant has a relationship with a agents such as a gateway, a Web hosting company, or a loyalty program (required)	xs:boolean	“1” or “true” “0” or “false”
payment-application	the software application used for processing credit card transactions (required)	xs:string	any sequence of characters allowed in XML; of any length
payment-version	the version of the software application used for processing credit card transactions (required)	xs:string	any sequence of characters allowed in XML; of any length
ecommerce	e-commerce industry (required)	xs:boolean	“1” or “true” “0” or “false”
grocery	grocery industry (required)	xs:boolean	“1” or “true” “0” or “false”
mail-order	mail-order or telephone-order industry (required)	xs:boolean	“1” or “true” “0” or “false”
petroleum	petroleum industry (required)	xs:boolean	“1” or “true” ; “0” or “false”
retail	retail industry (required)	xs:boolean	“1” or “true” ; “0” or “false”
telecommunication	telecommunication industry (required)	xs:boolean	“1” or “true” ; “0” or “false”
travel	travel industry (required)	xs:boolean	“1” or “true” ; “0” or “false”
url	the merchant's Web site URL (required)	xs:string	any sequence of characters allowed in XML; of any length
company	the name of the merchant's company (required)	xs:string	any sequence of characters allowed in XML; of any length
email-address	the e-mail address of an entity representing the merchant (optional)	xs:string	any sequence of characters allowed in XML; of any length

Name	Description	Datatype	Range
first-name	the first name of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
last-name	the last name of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
phone-number	the phone number of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
title	the title of an entity representing the merchant (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloConfigResponse > SiloConfig > Merchant sub-elements

The Merchant element contains the following sub-elements:

- DBAs
- OtherIndustries
- QSA
- Address

SiloConfigResponse > SiloConfig > Merchant > Address

The merchant's street address.

SiloConfigResponse > SiloConfig > Merchant > Address attributes

Name	Description	Datatype	Range
city	the merchant's city (required)	xs:string	any sequence of characters allowed in XML; of any length
country	the merchant’s country (required)	xs:string	any sequence of characters allowed in XML; of any length
line 1	the first line of the merchant’s street address (required)	xs:string	any sequence of characters allowed in XML; of any length

Name	Description	Datatype	Range
line 2	the second line of the merchant’s street address (optional)	xs:string	any sequence of characters allowed in XML; of any length
state	the merchant’s state (required)	xs:string	any sequence of characters allowed in XML; of any length
zip	the merchant’s zip code (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloConfigResponse > SiloConfig > Merchant > DBAs

A pluralized element that holds multiple DBA elements.

SiloConfigResponse > SiloConfig > Merchant > DBAs sub-element

DBAs contains the following sub-element:

- DBA

SiloConfigResponse > SiloConfig > Merchant > DBAs > DBA

An acronym for “Doing business as.” It is an alternate name under which the merchant operates.

SiloConfigResponse > SiloConfig > Merchant > DBAs > DBA attribute

Name	Description	Datatype	Range
name	the alternate name for the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloConfigResponse > SiloConfig > OtherIndustries

Industries that do not fit into the Merchant industry categories listed in the PCI-DSS Attestation of Onsite Assessments–Merchants. See *SiloConfigResponse > SiloConfig > Merchant (optional)* on page 244.

SiloConfigResponse > SiloConfig > OtherIndustries sub-element

OtherIndustries has the following sub-element:

- Industry

SiloConfigResponse > SiloConfig > OtherIndustries > Industry

An industry not listed in the Payment Card Industry (PCI) Data Security Standard (DSS) Attestation of Onsite Assessments–Merchants.

Name	Description	Datatype	Range
name	the name of the industry (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloConfigResponse > SiloConfig > QSA (optional)

The qualified security assessor.

SiloConfigResponse > SiloConfig > QSA attributes

Name	Description	Datatype	Range
url	the merchant's Web site URL (required)	xs:string	any sequence of characters allowed in XML; of any length
company	the name of the merchant's company (required)	xs:string	any sequence of characters allowed in XML; of any length
email-address	the e-mail address of an entity representing the merchant (optional)	xs:string	any sequence of characters allowed in XML; of any length
first-name	the first name of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
last-name	the first name of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
phone-number	the phone number of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
title	the title of an entity representing the merchant (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloConfigResponse > SiloConfig > QSA sub-element

QSA contains the following sub-element:

- Address

SiloConfigResponse > SiloConfig > QSA > Address

The merchant's street address.

SiloConfigResponse > SiloConfig > Organization

The contact information of a silo tenant.

SiloConfigResponse >SiloConfig >Organizationattributes

Name	Description	Datatype	Range
url	the tenant’s Web site URL (required)	xs:string	any sequence of characters allowed in XML; of any length
company	the name of the tenant’s company (required)	xs:string	any sequence of characters allowed in XML; of any length
email-address	the e-mail address of an entity representing the tenant (optional)	xs:string	any sequence of characters allowed in XML; of any length
first-name	the first name of an entity representing the tenant (required)	xs:string	any sequence of characters allowed in XML; of any length
last-name	the last name of an entity representing the tenant (required)	xs:string	any sequence of characters allowed in XML; of any length
phone-number	the phone number of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
title	the title of an entity representing the merchant (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloConfigResponse example

```
<SiloConfigResponse sync-id="SILO-CONFIG-0003-003">
    <SiloConfig max-users="25" max-hosted-assets="0" max-assets="100"
    silo-profile-id="myprofile-1" id="silo-3" name="test silo 333"
    description="test silo 3333">
        <Merchant travel="true" telecommunication="true" retail="true"
        petroleum="true" payment-version="version" payment-
        application="application" mail-order="true" grocery="true"
        ecommerce="true" agent-relationship="true" acquirer-
        relationship="true" url="www.test.com" title="t" phone-
```

```
      number="12345" last-name="testing" first-name="test" email-
      address="test@test.com" company="testcompany">
           <Address zip="560000" state="karnataka" line2="ITPL"
           line1="Hosur"
           country="India" city="Bangalore"/>
           <DBAs>
                   <DBA name="TestDBA"/>
           </DBAs>
           <OtherIndustries>
                   <Industry name="TestIndustry"/>
           </OtherIndustries>
           <QSA url="www.qsa.com" title="test" phone-
           number="1234567890" last-name="last" first-name="first"
           email-address="testemail@qsa.com" company="testcmp">
                   <Address zip="560001" state="karnataka"
                   line2="Whitefield" line1="KTPO" coun- try="India"
                   city="Bangalore"/>
           </QSA>
       </Merchant>
       <Organization url="www.org.com" title="test" phone-
       number="1234567890" last-name="last- name" first-name="t" email-
       address="test@org.com" company="testorg">
           <Address zip="560002" state="karnataka" line2="ITPL"
           line1="mahadevapura" coun- try="India" city="Bangalore"/>
       </Organization>
    </SiloConfig>
</SiloConfigResponse>
```

SiloUpdate

Modifies the configuration of an existing silo.

SiloUpdateRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloUpdateRequest element

SiloConfigResponse contains the following element:

- SiloConfig

SiloUpdateRequest > SiloConfig

Contains the complete configuration settings for a silo.

SiloUpdateRequest > SiloConfig attributes

Name	Description	Datatype	Range
id	a string that uniquely identifies the silo (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 50 characters
name	The name of the silo as it will be displayed. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters
silo-profile-id	The ID of the silo profile associated with this silo. (required)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters
description	The full description of the silo. (optional)	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 2048 characters
max-assets	The maximum number of assets that can be scanned. (required)	xs:nonNegativeInteger	any integer greater than or equal to 0

Name	Description	Datatype	Range
max-hosted-assets	The maximum number of assets that can be scanned with hosted scan engines. (required)	xs:nonNegativeInteger	any integer greater than or equal to 0
max-users	The maximum number of users that can be associated with this silo. (required)	xs:nonNegativeInteger	any integer greater than or equal to 0

SiloUpdateRequest > SiloConfig > Merchant (optional)

A company that performs credit card transactions.

SiloUpdateRequest > SiloConfig > Merchant attributes

These attributes are pieces of information that must be submitted by a merchant in the Payment Card Industry (PCI) Data Security Standard (DSS) Attestation of Onsite Assessments–Merchants. Choose all industries that apply. You also can specify other industries as needed. See *SiloUpdateRequest > SiloConfig > OtherIndustries* on page 255.

Name	Description	Datatype	Range
acquirer-relationship	whether the merchant has a relationship with more than one companies that provides credit card processing (required)	xs:boolean	“1” or “true” “0” or “false”
agent-relationship	whether the merchant has a relationship with a agents such as a gateway, a Web hosting company, or a loyalty program (required)	xs:boolean	“1” or “true” “0” or “false”
payment-application	the software application used for processing credit card transactions (required)	xs:string	any sequence of characters allowed in XML; of any length

Name	Description	Datatype	Range
payment-version	the version of the software application used for processing credit card transactions (required)	xs:string	any sequence of characters allowed in XML; of any length
ecommerce	e-commerce industry (required)	xs:boolean	“1” or “true” “0” or “false”
grocery	grocery industry (required)	xs:boolean	“1” or “true” “0” or “false”
mail-order	mail-order or telephone-order industry (required)	xs:boolean	“1” or “true” “0” or “false”
petroleum	petroleum industry (required)	xs:boolean	“1” or “true” ; “0” or “false”
retail	retail industry (required)	xs:boolean	“1” or “true” ; “0” or “false”
telecommunication	telecommunication industry (required)	xs:boolean	“1” or “true” ; “0” or “false”
travel	travel industry (required)	xs:boolean	“1” or “true” ; “0” or “false”
url	the merchant's Web site URL (required)	xs:string	any sequence of characters allowed in XML; of any length
company	the name of the merchant's company (required)	xs:string	any sequence of characters allowed in XML; of any length
email-address	the e-mail address of an entity representing the merchant (optional)	xs:string	any sequence of characters allowed in XML; of any length
first-name	the first name of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
last-name	the last name of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
phone-number	the phone number of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
title	the title of an entity representing the merchant (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloUpdateRequest > SiloConfig > Merchant sub-elements

The Merchant element contains the following sub-elements:

- DBAs
- OtherIndustries
- QSA
- Address

SiloUpdateRequest > SiloConfig > Merchant > Address

The merchant's street address.

SiloUpdateRequest > SiloConfig > Merchant > Address attributes

Name	Description	Datatype	Range
city	the merchant's city (required)	xs:string	any sequence of characters allowed in XML; of any length
country	the merchant’s country (required)	xs:string	any sequence of characters allowed in XML; of any length
line 1	the first line of the merchant’s street address (required)	xs:string	any sequence of characters allowed in XML; of any length
line 2	the second line of the merchant’s street address (optional)	xs:string	any sequence of characters allowed in XML; of any length
state	the merchant’s state (required)	xs:string	any sequence of characters allowed in XML; of any length
zip	the merchant’s zip code (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloUpdateRequest > SiloConfig > Merchant > DBAs

A pluralized element that holds multiple DBA elements.

SiloUpdateRequest > SiloConfig > Merchant > DBAs sub-element

DBAs contains the following sub-element:

- DBA

SiloUpdateRequest > SiloConfig > Merchant > DBAs > DBA

An acronym for “Doing business as.” It is an alternate name under which the merchant operates.

SiloUpdateRequest > SiloConfig > Merchant > DBAs > DBA attribute

Name	Description	Datatype	Range
name	the alternate name for the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloUpdateRequest > SiloConfig > OtherIndustries

Industries that do not fit into the Merchant industry categories listed in the PCI-DSS Attestation of Onsite Assessments–Merchants. See *SiloUpdateRequest > SiloConfig > Merchant (optional)* on page 252.

SiloUpdateRequest > SiloConfig > OtherIndustries sub-element

OtherIndustries has the following sub-element:

- Industry

SiloUpdateRequest > SiloConfig > OtherIndustries > Industry

An industry not listed in the Payment Card Industry (PCI) Data Security Standard (DSS) Attestation of Onsite Assessments–Merchants.

Name	Description	Datatype	Range
name	the name of the industry (required)	xs:string	any sequence of characters allowed in XML; of any length

SiloUpdateRequest > SiloConfig > QSA (optional)

The qualified security assessor.

SiloUpdateRequest > SiloConfig > QSA attributes

Name	Description	Datatype	Range
url	the merchant's Web site URL (required)	xs:string	any sequence of characters allowed in XML; of any length

Name	Description	Datatype	Range
company	the name of the merchant's company (required)	xs:string	any sequence of characters allowed in XML; of any length
email-address	the e-mail address of an entity representing the merchant (optional)	xs:string	any sequence of characters allowed in XML; of any length
first-name	the first name of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
last-name	the first name of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
phone-number	the phone number of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
title	the title of an entity representing the merchant (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloUpdateRequest > SiloConfig > QSA sub-element

QSA contains the following sub-element:

- Address

SiloUpdateRequest > SiloConfig > QSA > Address

The merchant's street address.

SiloUpdateRequest > SiloConfig > Organization

The contact information of a silo tenant.

SiloUpdateRequest > SiloConfig > Organization attributes

Name	Description	Datatype	Range
url	the tenant’s Web site URL (required)	xs:string	any sequence of characters allowed in XML; of any length
company	the name of the tenant’s company (required)	xs:string	any sequence of characters allowed in XML; of any length

Name	Description	Datatype	Range
email-address	the e-mail address of an entity representing the tenant (optional)	xs:string	any sequence of characters allowed in XML; of any length
first-name	the first name of an entity representing the tenant (required)	xs:string	any sequence of characters allowed in XML; of any length
last-name	the last name of an entity representing the tenant (required)	xs:string	any sequence of characters allowed in XML; of any length
phone-number	the phone number of an entity representing the merchant (required)	xs:string	any sequence of characters allowed in XML; of any length
title	the title of an entity representing the merchant (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloUpdateRequest example

```
<SiloUpdateRequest sync-id="SILO-CREATE-0003-003" session-
id="F9CD2D8AA3208284F101A411549EA5CB6897FBF4">
    <SiloConfig description="test silo 3333" name="test silo 333"
    id="silo-3"
    silo-profile-id="myprofile-1" max-assets="100" max-users="25" max-
    hosted-assets="0">
        <Merchant company="testcompany" email-address="test@test.com"
        first-name="test" last-name="testing" phone-number="12345"
        title="t" url="www.test.com" acquirer-relationship="true" agent-
        relationship="true" ecommerce="true" grocery="true" mail-
        order="true" payment-application="application" payment-
        version="version" petroleum="true" retail="true"
        telecommunication="true" travel="true">
            <Address city="Bangalore" country="India" line1="Hosur"
            line2="ITPL" state="karnataka" zip="560000"/>
            <DBAs>
                    <DBA name="TestDBA"/>
            </DBAs>
            <OtherIndustries>
                    <Industry name="TestIndustry"/>
            </OtherIndustries>
            <QSA company="testcmp" email-address="testemail@qsa.com"
            first-name="first" last- name="last" phone-
            number="1234567890" title="test" url="www.qsa.com">
```

```
                <Address city="Bangalore" country="India"
                line1="KTPO" line2="Whitefield" state="karnataka"
                zip="560001"/>
            </QSA>
        </Merchant>
        <Organization company="testorg" email-address="test@org.com"
        first-name="t" last- name="lastname" phone-number="1234567890"
        title="test" url="www.org.com">
            <Address city="Bangalore" country="India"
            line1="mahadevapura" line2="ITPL" state="karnataka"
            zip="560002"/>
        </Organization>
    </SiloConfig>
</SiloUpdateRequest>
```

SiloUpdateResponse attributes

Name	Description	Datatype	Range
id	a string that uniquely identifies the silo (required)	xs:string	any sequence of characters allowed in XML; maximum length is 50 characters
sync-id	A user-specified identifier that can be used to ensure that a request is not duplicated. (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloUpdateResponse elements

SiloUpdateRequest has no elements.

SiloUpdateResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<SiloUpdateResponse id="pci-silo-001"/>
```

SiloDelete

Deletes an existing silo.

SiloDeleteRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length
silo-name	A user-specified name for the silo.*	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 64 characters
silo-id	a string that uniquely identifies the silo*	xs:string	a sequence of characters (letters, numerals, hyphens, and underscores--the first character cannot be a hyphen); maximum length is 50 characters

SiloDeleteRequest elements

SiloDeleteRequest has no elements.

SiloDeleteRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<SiloDeleteRequest session-
id="9C46275CC41DE1BFB856B8BD6AEF43F0BCA0D448" silo-id="pci-silo-001"/>
```

SiloDeleteResponse attribute

Name	Description	Datatype	Range
sync-id	A user-specified identifier that can be used to ensure that a request is not duplicated. (optional)	xs:string	any sequence of characters allowed in XML; of any length

SiloDeleteResponse elements

SiloDeleteResponse has no elements.

SiloDeleteResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<SiloDeleteResponse/>
```

Role Management

This section contains all requests and responses related to managing roles.

RoleCreate

Creates a new role that can be applied to any user.

RoleCreateRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

RoleCreateRequest element

A RoleCreateRequest element contains one or more of the following element:

- Role

RoleCreateRequest > Role

A detailed description of an individual role.

RoleCreateRequest > Role attributes

Name	Description	Datatype	Range
name	The short name of the role. (required)	xs:string	any sequence of characters allowed in XML; maximum length is 64 characters
full-name	The full name of the role. (required)	xs:string	any sequence of characters allowed in XML; maximum length is 256 characters
enabled	Whether or not the role is enabled. (required)	xs:boolean	“1” or “true” = enabled

Name	Description	Datatype	Range
scope	Specifies if the role has global or silo scope. (optional)	xs:string	“global”“silo”Defaults to “silo” if not specified.

RoleCreateRequest > Role elements

The Role element contains one of each of the following sub-elements:

- Description
- AssetGroupPrivileges
- GlobalPrivileges
- SitePrivileges

RoleCreateRequest > Role > Description

The Description element contains a string that describes the role.

RoleCreateRequest > Role > AssetGroupPrivileges

The AssetGroupPrivileges element encapsulates the privileges that the role has with respect to asset groups. The AssetGroupPrivileges element contains the following sub-elements:

- ConfigureAssets
- ViewAssetData

RoleCreateRequest > Role > AssetGroupPrivileges > ConfigureAssets

The user has the ability to add or remove assets in accessible asset groups; does not include the ability to delete underlying asset definitions or discovered asset data.

RoleCreateRequest > Role > AssetGroupPrivileges > ConfigureAssets attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > AssetGroupPrivileges > ViewAssetData

The user has the ability to view discovered information about all assets in accessible asset groups, including IP addresses, installed software, and vulnerabilities.

RoleCreateRequest > Role > AssetGroupPrivileges > ViewAssetData attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges

The GlobalPrivileges element encapsulates the global privileges that the role has within a silo. The GlobalPrivileges element contains the following sub-elements:

- CreateReports
- ConfigureGlobalSettings
- ManageSites
- ManageAssetGroups
- ManageDynamicAssetGroups
- ManageScanTemplates
- ManageReportTemplates
- GenerateRestrictedReports
- ManageScanEngines
- SubmitVulnExceptions
- ApproveVulnExceptions
- DeleteVulnExceptions
- CreateTickets
- CloseTickets
- TicketAssignee
- AddUsersToSite
- AddUsersToGroup
- AddUsersToReport
- ManageTags

RoleCreateRequest > Role > GlobalPrivileges > CreateReports

The user has the ability to create reports for accessible sites.

RoleCreateRequest > Role > GlobalPrivileges > CreateReports attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > ConfigureGlobalSettings

The user has the ability to change global settings, such as selection of a risk scoring model used for discovered vulnerabilities and exclusion of assets from all scans.

RoleCreateRequest > Role > GlobalPrivileges > ConfigureGlobalSettings attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > ManageSites

The user has the ability to create and change settings for sites including running scans and deleting sites and assets.

RoleCreateRequest > Role > GlobalPrivileges > ManageSites attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > ManageAssetGroups

The user has the ability to create and change settings for static asset groups, including deleting groups.

RoleCreateRequest > Role > GlobalPrivileges > ManageAssetGroups attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege“0” or “false” = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > ManageDynamicAssetGroups

The user has the ability to create and change settings for dynamic asset groups, including deleting groups.

A role with ManageDynamicAssetGroups should include ManageAssetGroups, ViewAssetData, ConfigureAssets, and access to all sites.

RoleCreateRequest > Role > GlobalPrivileges > ManageDynamicAssetGroups attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege“0” or “false” = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > ManagePolicies

The user has the ability to create, edit, and change policies.

RoleCreateRequest > Role > GlobalPrivileges > ManagePolicies attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > ManageScanTemplates

The user has the ability to create, edit, and delete scan templates.

In previous releases, only Global Administrators had this permission.

The user cannot configure the scan template for a *particular site* unless the site permission ConfigureScanTemplates is set to *true*. See *RoleCreateRequest > Role > SitePrivileges* on page 272).

RoleCreateRequest > Role > GlobalPrivileges > ManageScanTemplates attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > ManageReportTemplates

The user has the ability to create, edit, and delete report templates.

RoleCreateRequest > Role > GlobalPrivileges > ManageReportTemplates attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > GenerateRestrictedReports

The user has the ability to use certain report sections when creating reports and to generate reports with restricted sections.

RoleCreateRequest > Role > GlobalPrivileges > GenerateRestrictedReports attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > ManageScanEngines

The user has the ability to create, edit, and delete scan engines.

The user cannot configure the scan engine for a particular site unless the site permission ConfigureEngines is set to true. See *RoleCreateRequest > Role > SitePrivileges* on page 272).

RoleCreateRequest > Role > GlobalPrivileges > ManageScanEngines attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > SubmitVulnExceptions

For accessible scan data, the user has the ability to submit vulnerability exceptions for approval. Upon approval the vulnerabilities are excluded from reports.

RoleCreateRequest > Role > GlobalPrivileges > SubmitVulnExceptions attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > ApproveVulnExceptions

For accessible scan data, the user has the ability to approve vulnerability exceptions, which would cause the vulnerabilities to be excluded from reports.

RoleCreateRequest > Role > GlobalPrivileges > ApproveVulnExceptions attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > DeleteVulnExceptions

For accessible scan data, the user has the ability to remove vulnerabilties from the list of vulnerability exceptions, which would cause the vulnerabilities to be included in reports.

RoleCreateRequest > Role > GlobalPrivileges > DeleteVulnExceptions attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > CreateTickets

The user has the ability to create job tickets for vulnerability remediation.

RoleCreateRequest > Role > GlobalPrivileges > CreateTickets attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > CloseTickets

The user has the ability to close job tickets for vulnerability remediation.

RoleCreateRequest > Role > GlobalPrivileges > CloseTickets attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > TicketAssignee

The user has the ability to be assigned job tickets for vulnerability remediation. With this permission the user also can be added to access lists to view reports.

RoleCreateRequest > Role > GlobalPrivileges > TicketAssignee attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > AddUsersToSite

The user has the ability to add other users to accessible sites.

RoleCreateRequest > Role > GlobalPrivileges > AddUsersToSite attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > AddUsersToGroup

The user has the ability to add other users to accessible asset groups.

RoleCreateRequest > Role > GlobalPrivileges > AddUsersToGroup attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > AddUsersToReport

A report owner has the ability to create a report access list and share instances of a report with other individuals via e-mail or a distributed URL.

RoleCreateRequest > Role > GlobalPrivileges > AddUsersToReport attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleCreateRequest > Role > GlobalPrivileges > ManageTags

The user can create and edit tags and delete tags except for built-in criticality tags. The user implicitly has access to all sites.

RoleCreateRequest > Role > GlobalPrivileges > ManageTags attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleCreateRequest > Role > SitePrivileges

The SitePrivileges element encapsulates the privileges that the role has with respect to sites. The SitePrivileges element contains the following sub-elements:

- ConfigureAlerts
- ConfigureCredentials
- ConfigureEngines
- ConfigureScanTemplates
- ConfigureScheduleScans
- ConfigureSiteSettings
- ConfigureTargets
- ManualScans
- PurgeData
- ViewAssetData

RoleCreateRequest > Role > SitePrivileges > ConfigureAlerts

The user has the ability to set up alerts that notify users about specific scan-related events for accessible sites.

RoleCreateRequest > Role > SitePrivileges > ConfigureAlerts attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > SitePrivileges > ConfigureCredentials

The user has the ability to enter and modify logon credentials for deeper scanning capability on password-protected assets for accessible sites.

RoleCreateRequest > Role > SitePrivileges > ConfigureCredentials attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > SitePrivileges > ConfigureEngines

The user has the ability to assign a scan engine to each accessible site.

RoleCreateRequest > Role > SitePrivileges > ConfigureEngines attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > SitePrivileges > ConfigureScanTemplates

The user has the ability to assign a scan template to each accessible site.

RoleCreateRequest > Role > Site Privileges > ConfigureScanTemplates attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > Site Privileges > ConfigureScheduleScans

The user has the ability to create schedules to automatically scan accessible sites.

RoleCreateRequest > Role > Site Privileges > ConfigureScheduleScans attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > Site Privileges > ConfigureSiteSettings

The user has the ability to enter a site description and risk factor in the configuration for each accessible site.

RoleCreateRequest > Role > Site Privileges > ConfigureSiteSettings attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > Site Privileges > ConfigureTargets

The user has the ability to specify IP addresses, address ranges, and host names to scan in accessible sites.

RoleCreateRequest > Role > Site Privileges > ConfigureTargets attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > Site Privileges > ManualScans

The user has the ability to manually start one-off scans of accessible sites; does not include the ability to configure scan settings.

RoleCreateRequest > Role > Site Privileges > ManualScans attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > Site Privileges > PurgeData

The user has the ability to manually purge asset data from a site.

RoleCreateRequest > Role > Site Privileges > PurgeData attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest > Role > Site Privileges > ViewAssetData

The user has the ability to view discovered information about all assets in accessible asset groups, including IP addresses, installed software, and vulnerabilities.

RoleCreateRequest > Role > Site Privileges > ViewAssetData attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleCreateRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<RoleCreateRequest session-id="${Login#ResponseAsXml#//LoginResponse[1]
/@session-id}">
<Role name="reporting" full-name="Reporting Role" enabled="1"
scope="global" >
```

```
    <Description>Can run scans and reports.</Description>
    <GlobalPrivileges>
        <CreateReports enabled="true"/>
        <ManageTags enabled="true"/>
        <ConfigureGlobalSettings enabled="false"/>
        <ManageSites enabled="false"/>
        <ManageAssetGroups enabled="false"/>
        <ManageDynamicAssetGroups enabled="false"/>
        <ManagePolicies enabled="false"/>
        <ManageScanTemplates enabled="false"/>
        <ManageReportTemplates enabled="true"/>
        <GenerateRestrictedReports enabled="true"/>
        <ManageScanEngines enabled="false"/>
        <SubmitVulnExceptions enabled="false"/>
        <ApproveVulnExceptions enabled="false"/>
        <DeleteVulnExceptions enabled="true"/>
        <CreateTickets enabled="false"/>
        <CloseTickets enabled="false"/>
        <TicketAssignee enabled="false"/>
        <AddUsersToSite enabled="false"/>
        <AddUsersToGroup enabled="false"/>
        <AddUsersToReport enabled="false"/>
    </GlobalPrivileges>
    <SitePrivileges>
        <ViewAssetData enabled="true"/>
        <ConfigureSiteSettings enabled="true"/>
        <ConfigureTargets enabled="true"/>
        <ConfigureEngines enabled="true"/>
        <ConfigureScanTemplates enabled="false"/>
        <ConfigureAlerts enabled="false"/>
        <ConfigureCredentials enabled="false"/>
        <ConfigureScheduleScans enabled="false"/>
        <ManualScans enabled="false"/>
        <PurgeData enabled="false"/>
    </SitePrivileges>
    <AssetGroupPrivileges>
        <ViewAssetData enabled="true"/>
        <ConfigureAssets enabled="true"/>
    </AssetGroupPrivileges>
</Role>
</RoleCreateRequest>
```

RoleCreateResponse attributes

Name	Description	Datatype	Range
sync-id	a user-specified identifier that can be used to ensure that a user request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length
id	ID of the newly-created role. (required)	xs:positive integer	any integer greater than zero

RoleCreateResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<RoleCreateResponse id="3">
</RoleCreateResponse>
```

RoleListing

Returns a summary list of all roles.

RoleListingRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

RoleListingRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<RoleListingRequest session-
id="7E53108F40A617611B2A7D3C78CAB793464B5E62"/>
```

RoleListingResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

RoleListingResponse element

The RoleListingResponse element contains zero or more of the following element:

- RoleSummary

RoleListingResponse > RoleSummary

The role summary encapsulates information about a role.

RoleListingResponse > RoleSummary attributes

Name	Description	Datatype	Range
id	The unique identifier of the role. (required)	xs:positiveInteger	any mathematical integer greater than 0
full-name	The full name of the role. (required)	xs:string	any sequence of characters allowed in XML; of any length
description	A description of the role. (optional)	xs:string	any sequence of characters allowed in XML; of any length
enabled	Whether or not the role is enabled. (required)	xs:boolean	“1” or “true” = enabled
scope	Specifies if the role has global or silo scope. (optional)	xs:string	“global” “silo” Defaults to “silo” if not specified.

RoleListingResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<RoleListingResponse>
    <RoleSummary name="reporting" full-name="Reporting Role" id="3"
    enabled="true" scope="global"/>
    <RoleSummary name="global-admin" full-name="Global Administrator"
    id="4" enabled="false" scope="global"/>
</RoleListingReponse>
```

RoleDetails

Returns a detailed description of a single role.

RoleDetails attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

RoleDetailsRequest element

A RoleDetailsRequest element contains one of the following element:

- Role

RoleDetailsRequest > Role

Specifies an individual role.

RoleDetailsRequest > Role attributes

Name	Description	Datatype	Range
name	The short name of the role. (required)	xs:string	any sequence of characters allowed in XML; of any length
scope	Specifies if the role has global or silo scope. (optional)	xs:string	“global” “silo” Defaults to “silo” if not specified.

RoleDetailsRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<RoleDetailsRequest session-
id="7E53108F40A617611B2A7D3C78CAB793464B5E62">
    <Role name="reporting" scope="global"/>
</RoleDetailsRequest>
```

RoleDetailsResponse attribute

Name	Description	Datatype	Range
sync-id	A user-specified identifier that can be used to ensure that a user request is not duplicated.(optional)	xs:string	any sequence of characters allowed in XML; of any length

RoleDetailsResponse element

The RoleDetailsResponse element contains one of the following element:

- Role

RoleDetailsResponse > Role

A detailed description of an individual role.

RoleDetailsResponse > Role attributes

Name	Description	Datatype	Range
id	The unique identifier of the role. (required)	xs:positiveInteger	any mathematical integer greater than 0
full-name	The full name of the role. (required)	xs:string	any sequence of characters allowed in XML; of any length
description	A description of the role. (optional)	xs:string	any sequence of characters allowed in XML; of any length
enabled	Whether or not the role is enabled. (required)	xs:boolean	“1” or “true” = enabled
scope	Specifies if the role has global or silo scope. (optional)	xs:string	“global” “silo” Defaults to “silo” if not specified.

RoleDetailsResponse > Role elements

The Role element contains one of each of the following sub-elements:

- Description
- AssetGroupPrivileges
- GlobalPrivileges
- SitePrivileges

RoleDetailsResponse > Role > Description

The Description element contains a string that describes the role.

RoleDetailsResponse > Role > AssetGroupPrivileges

The AssetGroupPrivileges element encapsulates the privileges that the role has with respect to asset groups. The AssetGroupPrivileges element contains the following sub-elements:

- ConfigureAssets
- ViewAssetData

RoleDetailsResponse > Role > AssetGroupPrivileges > ConfigureAssets

The user has the ability to add or remove assets in accessible asset groups; does not include the ability to delete underlying asset definitions or discovered asset data.

RoleDetailsResponse > Role > AssetGroupPrivileges > ConfigureAssets attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (**required**)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > AssetGroupPrivileges > ViewAssetData

The user has the ability to view discovered information about all assets in accessible asset groups, including IP addresses, installed software, and vulnerabilities.

RoleDetailsResponse > Role > AssetGroupPrivileges > ViewAssetData attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges

The GlobalPrivileges element encapsulates the global privileges that the role has within a silo. The GlobalPrivileges element contains the following sub-elements:

- CreateReports
- ConfigureGlobalSettings
- ManageSites
- ManageAssetGroups
- ManageDynamicAssetGroups
- ManageScanTemplates
- ManageReportTemplates
- GenerateRestrictedReports
- ManageScanEngines
- SubmitVulnExceptions
- ApproveVulnExceptions
- DeleteVulnExceptions
- CreateTickets
- CloseTickets
- TicketAssignee
- AddUsersToSite
- AddUsersToGroup
- AddUsersToReport
- ManageTags

RoleDetailsResponse > Role > GlobalPrivileges > CreateReports

The user has the ability to create reports for accessible sites.

RoleDetailsResponse > Role > GlobalPrivileges > CreateReports attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > ConfigureGlobalSettings

The user has the ability to change global settings, such as selection of a risk scoring model used for discovered vulnerabilities and exclusion of assets from all scans.

RoleDetailsResponse > Role > GlobalPrivileges > ConfigureGlobalSettings attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > ManageSites

The user has the ability to create and change settings for sites including running scans and deleting sites and assets.

RoleDetailsResponse > Role > GlobalPrivileges > ManageSites attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > ManageAssetGroups

The user has the ability to create and change settings for static asset groups, including deleting groups.

RoleDetailsResponse > Role > GlobalPrivileges > ManageAssetGroups attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > ManageDynamicAssetGroups

The user has the ability to create and change settings for dynamic asset groups, including deleting groups.

A role with ManageDynamicAssetGroups should include ManageAssetGroups, ViewAssetData, ConfigureAssets, and access to all sites.

RoleDetailsResponse > Role > GlobalPrivileges > ManageDynamicAssetGroups attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > ManagePolicies

The user has the ability to create, edit, and change settings for policies.

RoleDetailsResponse > Role > GlobalPrivileges > ManagePolicies attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > ManageScanTemplates

The user has the ability to create, edit, and delete scan templates.

In previous releases, only Global Administrators had this permission.

The user cannot configure the scan template for a particular site unless the site permission ConfigureScanTemplates is set to *true*. See *RoleDetailsResponse > Role > SitePrivileges* on page 290.

RoleDetailsResponse > Role > GlobalPrivileges > ManageScanTemplates attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > ManageReportTemplates

The user has the ability to create, edit, and delete report templates.

RoleDetailsResponse > Role > GlobalPrivileges > ManageReportTemplates attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > GenerateRestrictedReports

The user has the ability to use certain report sections when creating reports and to generate reports with restricted sections.

RoleDetailsResponse > Role > GlobalPrivileges > GenerateRestrictedReports attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > ManageScanEngines

The user has the ability to create, edit, and delete scan engines.

The user cannot configure the scan engine for a particular site unless the site permission ConfigureEngines is set to true. See *RoleDetailsResponse > Role > SitePrivileges* on page 290.

RoleDetailsResponse > Role > GlobalPrivileges > ManageScanEngines attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > SubmitVulnExceptions

For accessible scan data, the user has the ability to submit vulnerability exceptions for approval. Upon approval the vulnerabilities are excluded from reports.

RoleDetailsResponse > Role > GlobalPrivileges > SubmitVulnExceptions attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > ApproveVulnExceptions

For accessible scan data, the user has the ability to approve vulnerability exceptions, which would cause the vulnerabilities to be excluded from reports.

RoleDetailsResponse > Role > GlobalPrivileges > ApproveVulnExceptions attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > DeleteVulnExceptions

For accessible scan data, the user has the ability to remove vulnerabilties from the list of vulnerability exceptions, which would cause the vulnerabilities to be included in reports.

RoleDetailsResponse > Role > GlobalPrivileges > DeleteVulnExceptions attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > CreateTickets

The user has the ability to create job tickets for vulnerability remediation.

RoleDetailsResponse > Role > GlobalPrivileges > CreateTickets attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > CloseTickets

The user has the ability to close job tickets for vulnerability remediation.

RoleDetailsResponse > Role > GlobalPrivileges > CloseTickets attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > TicketAssignee

The user has the ability to be assigned job tickets for vulnerability remediation.

RoleDetailsResponse > Role > GlobalPrivileges > TicketAssignee attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > AddUsersToSite

The user has the ability to add other users to accessible sites.

RoleDetailsResponse > Role > GlobalPrivileges > AddUsersToSite attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > AddUsersToGroup

The user has the ability to add other users to accessible asset groups.

RoleDetailsResponse > Role > GlobalPrivileges > AddUsersToGroup attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > AddUsersToReport

A report owner has the ability to create a report access list and share instances of a report with other individuals via e-mail or a distributed URL.

RoleDetailsResponse > Role > GlobalPrivileges > AddUsersToReport attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > GlobalPrivileges > ManageTags

The user can create and edit tags and delete tags except for built-in criticality tags. The user implicitly has access to all sites.

RoleDetailsResponse > Role > GlobalPrivileges > ManageTags attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > SitePrivileges

The SitePrivileges element encapsulates the privileges that the role has with respect to sites. The SitePrivileges element contains the following sub-elements:

- ConfigureAlerts
- ConfigureCredentials
- ConfigureEngines
- ConfigureScanTemplates
- ConfigureScheduleScans
- ConfigureSiteSettings
- ConfigureTargets
- ManualScans
- PurgeData
- ViewAssetData

RoleDetailsResponse > Role > SitePrivileges > ConfigureAlerts

The user has the ability to set up alerts that notify users about specific scan-related events for accessible sites.

RoleDetailsResponse > Role > SitePrivileges > ConfigureAlerts attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > SitePrivileges > ConfigureCredentials

The user has the ability to enter and modify logon credentials for deeper scanning capability on password-protected assets for accessible sites.

RoleDetailsResponse > Role > SitePrivileges > ConfigureCredentials attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > SitePrivileges > ConfigureEngines

The user has the ability to assign a scan engine to each accessible site.

RoleDetailsResponse > Role > SitePrivileges > ConfigureEngines attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > SitePrivileges > ConfigureScanTemplates

The user has the ability to assign a scan template to each accessible site.

RoleDetailsResponse > Role > Site Privileges > ConfigureScanTemplates attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > Site Privileges > ConfigureScheduleScans

The user has the ability to create schedules to automatically scan accessible sites.

RoleDetailsResponse > Role > Site Privileges > ConfigureScheduleScans attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > Site Privileges > ConfigureSiteSettings

The user has the ability to enter a site description and risk factor in the configuration for each accessible site.

RoleDetailsResponse > Role > Site Privileges > ConfigureSiteSettings attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > Site Privileges > ConfigureTargets

The user has the ability to specify IP addresses, address ranges, and host names to scan in accessible sites.

RoleDetailsResponse > Role > Site Privileges > ConfigureTargets attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > Site Privileges > ManualScans

The user has the ability to manually start one-off scans of accessible sites; does not include the ability to configure scan settings.

RoleDetailsResponse > Role > Site Privileges > ManualScans attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > Site Privileges > PurgeData

The user has the ability to manually purge asset data from a site.

RoleDetailsResponse > Role > Site Privileges > PurgeData attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse > Role > Site Privileges > ViewAssetData

The user has the ability to view discovered information about all assets in accessible asset groups, including IP addresses, installed software, and vulnerabilities.

RoleDetailsResponse > Role > Site Privileges > ViewAssetData attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleDetailsResponse example

```
<RoleDetailsResponse>
    <Role id="10" enabled="true" full-name="Reporting Role"
    name="reporting" scope="global">
        <AssetGroupPrivileges>
            <ConfigureAssets enabled="true"/>
            <ViewAssetData enabled="true"/>
        </AssetGroupPrivileges>
        <Description>Can run scans and reports.</Description>
        <GlobalPrivileges>
            <AddUsersToGroup enabled="false"/>
            <AddUsersToReport enabled="false"/>
            <AddUsersToSite enabled="false"/>
            <ApproveVulnExceptions enabled="false"/>
            <CloseTickets enabled="false"/>
            <ConfigureGlobalSettings enabled="false"/>
            <CreateReports enabled="true"/>
            <CreateTickets enabled="false"/>
            <DeleteVulnExceptions enabled="true"/>
            <GenerateRestrictedReports enabled="true"/>
            <ManageAssetGroups enabled="false"/>
            <ManageDynamicAssetGroups enabled="false"/>
            <ManagePolicies enabled="false"/>
            <ManageReportTemplates enabled="true"/>
            <ManageScanEngines enabled="false"/>
            <ManageScanTemplates enabled="false"/>
            <ManageSites enabled="false"/>
            <ManageTags enabled="true"/>
            <SubmitVulnExceptions enabled="false"/>
            <TicketAssignee enabled="false"/>
        </GlobalPrivileges>
        <SitePrivileges>
            <ConfigureAlerts enabled="false"/>
            <ConfigureCredentials enabled="false"/>
            <ConfigureEngines enabled="true"/>
            <ConfigureScanTemplates enabled="false"/>
            <ConfigureScheduleScans enabled="false"/>
            <ConfigureSiteSettings enabled="true"/>
            <ConfigureTargets enabled="true"/>
            <ManualScans enabled="false"/>
            <PurgeData enabled="false"/>
            <ViewAssetData enabled="true"/>
        </SitePrivileges>
    </Role>
    </RoleDetailsResponse>
```

RoleUpdate

Updates a specific role with new information. A RoleUpdate is similar to a RoleCreate, except that a RoleUpdate replaces any previously existing information with the new information specified in the RoleUpdateRequest.

RoleUpdateRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

RoleUpdateRequest element

A RoleUpdateRequest element contains one or more of the following element:

- Role

RoleUpdateRequest > Role

A detailed description of an individual role.

RoleUpdateRequest > Role attributes

Name	Description	Datatype	Range
id	The unique identifier of the role. (required)	xs:positiveInteger	any mathematical integer greater than 0
name	The short name of the role. (required)	xs:string	any sequence of characters allowed in XML; maximum length is 64 characters
full-name	The full name of the role. (required)	xs:string	any sequence of characters allowed in XML; maximum length is 256 characters
enabled	Whether or not the role is enabled. (required)	xs:boolean	“1” or “true” = enabled

Name	Description	Datatype	Range
scope	Specifies if the role has global or silo scope. (optional)	xs:string	“global” “silo” Defaults to “silo” if not specified.

The id attribute specifies the role to be updated. If a role with the specified id attribute exists, any other attributes or elements will have their information replaced with the corresponding information in the RoleUpdateRequest. Only the id attribute remains unchanged.

RoleUpdateRequest > Role elements

The Role element contains one of each of the following sub-elements:

- Description
- AssetGroupPrivileges
- GlobalPrivileges
- SitePrivileges

RoleUpdateRequest > Role > Description

The Description element contains a string that describes the role.

RoleUpdateRequest > Role > AssetGroupPrivileges

The AssetGroupPrivileges element encapsulates the privileges that the role has with respect to asset groups. The AssetGroupPrivileges element contains the following sub-elements:

- ConfigureAssets
- ViewAssetData

RoleUpdateRequest > Role > AssetGroupPrivileges > ConfigureAssets

The user has the ability to add or remove assets in accessible asset groups; does not include the ability to delete underlying asset definitions or discovered asset data.

RoleUpdateRequest > Role > AssetGroupPrivileges > ConfigureAssets attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > AssetGroupPrivileges > ViewAssetData

The user has the ability to view discovered information about all assets in accessible asset groups, including IP addresses, installed software, and vulnerabilities.

RoleUpdateRequest > Role > AssetGroupPrivileges > ViewAssetData attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges

The GlobalPrivileges element encapsulates the global privileges that the role has within a silo. The GlobalPrivileges element contains the following sub-elements:

- CreateReports
- ConfigureGlobalSettings
- ManageSites
- ManageAssetGroups
- ManageDynamicAssetGroups
- ManageScanTemplates
- ManageReportTemplates
- GenerateRestrictedReports
- ManageScanEngines
- SubmitVulnExceptions
- ApproveVulnExceptions
- DeleteVulnExceptions
- CreateTickets
- CloseTickets
- TicketAssignee
- AddUsersToSite
- AddUsersToGroup
- AddUsersToReport
- ManageTags

RoleUpdateRequest > Role > GlobalPrivileges > CreateReports

The user has the ability to create reports for accessible sites.

RoleUpdateRequest > Role > GlobalPrivileges > CreateReports attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges > ConfigureGlobalSettings

The user has the ability to change global settings, such as selection of a risk scoring model used for discovered vulnerabilities and exclusion of assets from all scans.

RoleUpdateRequest > Role > GlobalPrivileges > ConfigureGlobalSettings attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges > ManageSites

The user has the ability to create and change settings for sites including running scans and deleting sites and assets.

RoleUpdateRequest > Role > GlobalPrivileges > ManageSites attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges > ManageAssetGroups

The user has the ability to create and change settings for static asset groups, including deleting groups.

RoleUpdateRequest > Role > GlobalPrivileges > ManageAssetGroups attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges > ManageDynamicAssetGroups

The user has the ability to create and change settings for dynamic asset groups, including deleting groups.

A role with ManageDynamicAssetGroups should include ManageAssetGroups, ViewAssetData, ConfigureAssets, and access to all sites.

RoleUpdateRequest > Role > GlobalPrivileges > ManageDynamicAssetGroups attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges > ManageScanTemplates

The user has the ability to create, edit, and delete scan templates.

In previous releases, only Global Administrators had this permission.

The user cannot configure the scan template for a particular site unless the site permission ConfigureScanTemplates is set to *true*. See *RoleUpdateRequest > Role > SitePrivileges* on page 305).

RoleUpdateRequest > Role > GlobalPrivileges > ManageScanTemplates attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges > ManageReportTemplates

The user has the ability to create, edit, and delete report templates.

RoleUpdateRequest > Role > GlobalPrivileges > ManageReportTemplates attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges > GenerateRestrictedReports

The user has the ability to use certain report sections when creating reports and to generate reports with restricted sections.

RoleUpdateRequest > Role > GlobalPrivileges > GenerateRestrictedReports attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges > ManageScanEngines

The user has the ability to create, edit, and delete scan engines.

The user cannot configure the scan engine for a particular site unless the site permission ConfigureEngines is set to true. See *RoleUpdateRequest > Role > SitePrivileges* on page 305).

RoleUpdateRequest > Role > GlobalPrivileges > ManageScanEngines attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges > SubmitVulnExceptions

For accessible scan data, the user has the ability to submit vulnerability exceptions for approval. Upon approval the vulnerabilities are excluded from reports.

RoleUpdateRequest > Role > GlobalPrivileges > SubmitVulnExceptions attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges > ApproveVulnExceptions

For accessible scan data, the user has the ability to approve vulnerability exceptions, which would cause the vulnerabilities to be excluded from reports.

RoleUpdateRequest > Role > GlobalPrivileges > ApproveVulnExceptions attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (**required**)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges > DeleteVulnExceptions

For accessible scan data, the user has the ability to remove vulnerabilties from the list of vulnerability exceptions, which would cause the vulnerabilities to be included in reports.

RoleUpdateRequest > Role > GlobalPrivileges > DeleteVulnExceptions attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges > CreateTickets

The user has the ability to create job tickets for vulnerability remediation.

RoleUpdateRequest > Role > GlobalPrivileges > CreateTickets attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges > CloseTickets

The user has the ability to close job tickets for vulnerability remediation.

RoleUpdateRequest > Role > GlobalPrivileges > CloseTickets attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges > TicketAssignee

The user has the ability to be assigned job tickets for vulnerability remediation.

RoleUpdateRequest > Role > GlobalPrivileges > TicketAssignee attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (**required**)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges > AddUsersToSite

The user has the ability to add other users to accessible sites.

RoleUpdateRequest > Role > GlobalPrivileges > AddUsersToSite attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges > AddUsersToGroup

The user has the ability to add other users to accessible asset groups.

RoleUpdateRequest > Role > GlobalPrivileges > AddUsersToGroup attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges > AddUsersToReport

A report owner has the ability to create a report access list and share instances of a report with other individuals via e-mail or a distributed URL.

RoleUpdateRequest > Role > GlobalPrivileges > AddUsersToReport attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > GlobalPrivileges > ManageTags

The user can create and edit tags and delete tags except for built-in criticality tags. The user implicitly has access to all sites.

RoleUpdateRequest > Role > GlobalPrivileges > ManageTags attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > SitePrivileges

The SitePrivileges element encapsulates the privileges that the role has with respect to sites. The SitePrivileges element contains the following sub-elements:

- ConfigureAlerts
- ConfigureCredentials
- ConfigureEngines
- ConfigureScanTemplates
- ConfigureScheduleScans
- ConfigureSiteSettings
- ConfigureTargets
- ManualScans
- PurgeData
- ViewAssetData

RoleUpdateRequest > Role > SitePrivileges > ConfigureAlerts

The user has the ability to set up alerts that notify users about specific scan-related events for accessible sites.

RoleUpdateRequest > Role > SitePrivileges > ConfigureAlerts attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleUpdateRequest > Role > SitePrivileges > ConfigureCredentials

The user has the ability to enter and modify logon credentials for deeper scanning capability on password-protected assets for accessible sites.

RoleUpdateRequest > Role > SitePrivileges > ConfigureCredentials attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleUpdateRequest > Role > SitePrivileges > ConfigureEngines

The user has the ability to assign a scan engine to each accessible site.

RoleUpdateRequest > Role > SitePrivileges > ConfigureEngines attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	"1" or "true" = role has this privilege "0" or "false" = role does not have this privilege

RoleUpdateRequest > Role > SitePrivileges > ConfigureScanTemplates

The user has the ability to assign a scan template to each accessible site.

RoleUpdateRequest > Role > Site Privileges > ConfigureScanTemplates attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > Site Privileges > ConfigureScheduleScans

The user has the ability to create schedules to automatically scan accessible sites.

RoleUpdateRequest > Role > Site Privileges > ConfigureScheduleScans attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > Site Privileges > ConfigureSiteSettings

The user has the ability to enter a site description and risk factor in the configuration for each accessible site.

RoleUpdateRequest > Role > Site Privileges > ConfigureSiteSettings attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > Site Privileges > ConfigureTargets

The user has the ability to specify IP addresses, address ranges, and host names to scan in accessible sites.

RoleUpdateRequest > Role > Site Privileges > ConfigureTargets attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > Site Privileges > ManualScans

The user has the ability to manually start one-off scans of accessible sites; does not include the ability to configure scan settings.

RoleUpdateRequest > Role > Site Privileges > ManualScans attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > Site Privileges > PurgeData

The user has the ability to manually purge asset data from a site.

RoleUpdateRequest > Role > Site Privileges > PurgeData attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest > Role > Site Privileges > ViewAssetData

The user has the ability to view discovered information about all assets in accessible asset groups, including IP addresses, installed software, and vulnerabilities.

RoleUpdateRequest > Role > Site Privileges > ViewAssetData attribute

Name	Description	Datatype	Range
enabled	Indicates if the role has this privilege. (required)	xs:boolean	“1” or “true” = role has this privilege “0” or “false” = role does not have this privilege

RoleUpdateRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<RoleUpdateRequest session-
id="36FABBDFEEBFAAFFE89178640381D35D95889D72">
    <Role name="reporting" full-name="Reporting Role" enabled="1"
    scope="global" id="4">
        <Description>Can run scans and reports.</Description>
        <GlobalPrivileges>
            <CreateReports enabled="true"/>
            <ConfigureGlobalSettings enabled="false"/>
            <ManageSites enabled="false"/>
            <ManageAssetGroups enabled="false"/>
            <ManageDynamicAssetGroups enabled="false"/>
            <ManageScanTemplates enabled="false"/>
            <ManageReportTemplates enabled="true"/>
            <GenerateRestrictedReports enabled="true"/>
            <ManageScanEngines enabled="false"/>
            <SubmitVulnExceptions enabled="false"/>
            <ApproveVulnExceptions enabled="false"/>
            <CreateTickets enabled="false"/>
            <CloseTickets enabled="false"/>
            <TicketAssignee enabled="false"/>
            <AddUsersToSite enabled="false"/>
            <AddUsersToGroup enabled="false"/>
            <AddUsersToReport enabled="false"/>
            <ManageTags enabled="false"/>
        </GlobalPrivileges>
        <SitePrivileges>
            <ViewAssetData enabled="true"/>
            <ConfigureSiteSettings enabled="true"/>
            <ConfigureTargets enabled="true"/>
            <ConfigureEngines enabled="true"/>
            <ConfigureScanTemplates enabled="false"/>
            <ConfigureAlerts enabled="false"/>
            <ConfigureCredentials enabled="false"/>
            <ConfigureScheduleScans enabled="false"/>
            <ManualScans enabled="false"/>
            <PurgeData enabled="false"/>
        </SitePrivileges>
        <AssetGroupPrivileges>
            <ViewAssetData enabled="true"/>
            <ConfigureAssets enabled="true"/>
        </AssetGroupPrivileges>
    </Role>
</RoleCreateRequest>
```

RoleUpdateResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that can be used to ensure that a user request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

RoleUpdateResponse elements

An empty RoleUpdateResponse element is returned after a successful update.

RoleUpdateResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<RoleUpdateResponse>
</RoleUpdateResponse>
```

RoleDelete

Deletes a specified role.

RoleDeleteRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

RoleDeleteRequest element

A RoleDeleteRequest contains one or more of the following element:

- Role

RoleDeleteRequest Role

Specifies an individual role.

RoleDeleteRequest Role attributes

Name	Description	Datatype	Range
name	The short name of the role. (required)	xs:string	any sequence of characters allowed in XML; of any length
scope	Specifies if the role has global or silo scope. (optional)	xs:string	“global” “silo” Defaults to “silo” if not specified.

RoleDeleteRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<RoleDeleteRequest session-
id="36FABBDFEEBFAAFFE89178640381D35D95889D72">
    <Role name="reporting" scope="global"/>
</RoleDeleteRequest>
```

RoleDeleteResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

RoleDeleteResponse elements

An empty RoleDeleteResponse element is returned if the deletion is successful.

RoleDeleteResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<RoleDeleteResponse>
</RoleDeleteResponse>
```

Scan Engine Pool Management

This section contains all requests and responses related to managing scan engine pools.

EnginePoolCreate

Creates a new engine pool, and adds scan engines to the pool.

EnginePoolCreateRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication (required)	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

EnginePoolCreateRequest element

An EnginePoolCreateRequest element contains exactly one of the following element:

- EnginePool

EnginePoolCreateRequest > EnginePool

An engine pool is a group of scan engines that can be operated as though it were a single scan engine.

EnginePoolCreateRequest > EnginePool attributes

Name	Description	Datatype	Range
name	The name of the engine pool. **(required)**	xs:string	any sequence of characters allowed in XML; of any length
scope	Specifies if the engine pool has global or silo scope. **(optional)**	xs:string	“global” “silo” Defaults to “silo” if not specified.

EnginePoolCreateRequest > EnginePool element

The EnginePool element contains zero or more of the following sub-element:

- Engine

EnginePoolCreateRequest > EnginePool > Engine

An individual scan engine that is a member of an engine pool.

EnginePoolCreateRequest > EnginePool > Engine attribute

Name	Description	Datatype	Range
name	The name of the engine. **(required)**	xs:string	any sequence of characters allowed in XML; of any length

EnginePoolCreateRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<EnginePoolCreateRequest session-
id="36FABBDFEEBFAAFFE89178640381D35D95889D72" sync-id="sync">
    <EnginePool name="poolA" scope="global">
        <Engine name="engine3"/>
        <Engine name="engine4"/>
    </EnginePool>
</EnginePoolCreateRequest>
```

EnginePoolCreateResponse attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication **(required)**	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated **(optional)**	xs:string	any sequence of characters allowed in XML; of any length

EnginePoolCreateResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<EnginePoolCreateResponse id="4"/>
```

EnginePoolListing

Returns a summary list of all engine pools.

EnginePoolListingRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication **(required)**	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated **(optional)**	xs:string	any sequence of characters allowed in XML; of any length

EnginePoolListingRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<EnginePoolListingRequest session-
id="36FABBDFEEBFAAFFE89178640381D35D95889D72">
</EnginePoolListingRequest>
```

EnginePoolListingResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated (optional)	xs:string	any sequence of characters allowed in XML; of any length

EnginePoolListingResponse element

An EnginePoolListingResponse element contains zero or more of the following element:

- EnginePoolSummary

EnginePoolListingResponse > EnginePoolSummary

Encapsulates information about an engine pool.

EnginePoolListingResponse > EnginePoolSummary attributes

Name	Description	Datatype	Range
id	The unique identifier of the engine pool. **(required)**	xs:positiveInteger	any mathematical integer greater than 0
name	The name of the engine pool. **(required)**	xs:string	any sequence of characters allowed in XML; of any length
scope	Specifies if the engine pool has global or silo scope. **(optional)**	xs:string	“global” “silo” Defaults to “silo” if not specified.

EnginePoolListingResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<EnginePoolListingResponse>
    <EnginePoolSummary id="1" name="poolA" scope="global"/>
    <EnginePoolSummary id="3" name="poolB" scope="global"/>
</EnginePoolListingResponse>
```

EnginePoolDetails

Returns detailed information about a single engine pool.

EnginePoolDetailsRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication **(required)**	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated **(optional)**	xs:string	any sequence of characters allowed in XML; of any length

EnginePoolDetailsRequest element

An EnginePoolDetailsRequest element contains a single instance of the following element:

- EnginePool

EnginePoolDetailsRequestEnginePool

An engine pool is a group of scan engines that can be operated as though it were a single scan engine.

EnginePoolDetailsRequest EnginePool attribute

Name	Description	Datatype	Range
name	The name of the engine pool. **(required)**	xs:string	any sequence of characters allowed in XML; of any length

EnginePoolDetailsRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<EnginePoolDetailsRequest>
    <EnginePool name="enginePool5"/>
</EnginePoolDetailsRequest>
```

EnginePoolDetailsResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated **(optional)**	xs:string	any sequence of characters allowed in XML; of any length

EnginePoolDetailsResponse element

The EnginePoolDetailsResponse element contains one of the following element:

- EnginePool

EnginePoolDetailsResponse > EnginePool

An engine pool is a group of scan engines that can be operated as though it were a single scan engine.

EnginePoolDetailsResponse > EnginePool attributes

Name	Description	Datatype	Range
name	The name of the engine pool. **(required)**	xs:string	any sequence of characters allowed in XML; of any length

Name	Description	Datatype	Range
scope	Specifies if the engine pool has global or silo scope. **(optional)**	xs:string	“global” “silo” Defaults to “silo” if not specified.

EnginePoolDetailsResponse > EnginePool element

The EnginePool element contains zero or more of the following sub-element:

- EngineSummary

A set of status information about a scan engine.

EnginePoolDetailsResponse > EnginePool > EngineSummary attributes

Name	Description	Datatype	Range
address	the IP address of a scan engine **(required)**	xs:string	any sequence of characters allowed in XML; of any length
id	a unique numeric identifier for the scan engine, assigned by the security console in the order of creation **(required)**	xs:positiveInteger	any sequence of characters allowed in XML; of any length
name	a name assigned to the scan engine by the security console **(required)**	xs:string	any sequence of characters allowed in XML; of any length
port	the number of the port on which the engine listens for requests from the security console **(required)**	xs:positiveInteger	any mathematical integer greater than 0
scope	a parameter that specifies whether the engine has a global or silo-specific scope **(required)**	xs:string	“global” “silo”
status	the current operating status of the engine **(required)**	xs:string	“active” “pending-authorization” “incompatible” “not-responding” “unknown”

EnginePoolDetailsResponse example

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<EnginePoolDetailsResponse>
    <EnginePool id="5" name="pool5" scope="global">
        <EngineSummary status="active" scope="global" id="23"
        name="engineA" address="127.0.0.1" port="40814"/>
        <EngineSummary status="active" scope="global" id="55"
        name="engineB" address="10.2.0.1" port="40814"/>
    </EnginePool>
</EnginePoolDetailsResponse>
```

EnginePoolUpdate

Updates a specific role with new information. An EnginePoolUpdate is similar to an EnginePoolCreate, except that an EnginePoolUpdate replaces any previously existing information with the new information specified in the EnginePoolUpdateRequest.

EnginePoolUpdateRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication **(required)**	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated **(optional)**	xs:string	any sequence of characters allowed in XML; of any length

EnginePoolUpdateRequest element

The EnginePoolUpdateRequest element contains one instance of the following element:

- EnginePool

EnginePoolUpdateRequest > EnginePool

An engine pool is a group of scan engines that can be operated as though it were a single scan engine.

EnginePoolUpdateRequest > EnginePool attributes

Name	Description	Datatype	Range
id	The unique identifier of the engine pool. **(required)**	xs:positiveInteger	any mathematical integer greater than 0
name	The name of the engine pool. **(required)**	xs:string	any sequence of characters allowed in XML; of any length

Name	Description	Datatype	Range
scope	Specifies if the engine pool has global or silo scope. **(optional)**	xs:string	“global” “silo” Defaults to “silo” if not specified.

The id attribute specifies the engine pool to be updated. If an engine pool with the specified id attribute exists, any other attributes or elements will have their information replaced with the corresponding information in the EnginePoolUpdateRequest. Only the id attribute remains unchanged.

EnginePoolUpdateRequest > EnginePool element

The EnginePool element contains zero or more of the following sub-element:

- Engine

EnginePoolUpdateRequest > EnginePool> Engine

An individual scan engine that is a member of an engine pool.

EnginePoolUpdateRequest > EnginePool> Engine attribute

Name	Description	Datatype	Range
name	The name of the engine. **(required)**	xs:string	any sequence of characters allowed in XML; of any length

EnginePoolUpdateRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<EnginePoolUpdateRequest session-
id="36FABBDFEEBFAAFFE89178640381D35D95889D72">
    <EnginePool id="4" name="poolAtoB" scope="global">
        <Engine name="engine4"/>
    </EnginePool>
</EnginePoolUpdateRequest>
```

EnginePoolUpdateResponse attributes

Name	Description	Datatype	Range
id	ID of the newly-modified engine pool.**(required)**	xs:positive integer	any integer greater than zero

Name	Description	Datatype	Range
sync-id	a user-specified identifier that can be used to ensure that a user request is not duplicated **(optional)**	xs:string	any sequence of characters allowed in XML; of any length

EnginePoolUpdateResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<EnginePoolUpdateResponse id="4"/>
```

EnginePoolDelete

Deletes an engine pool.

EnginePoolDeleteRequest attributes

Name	Description	Datatype	Range
session-id	a token that identifies a session after authentication **(required)**	xs:string	any sequence of characters allowed in XML; of any length
sync-id	a user-specified identifier that ensures that a request is not duplicated **(optional)**	xs:string	any sequence of characters allowed in XML; of any length

EnginePoolDeleteRequest element

The EnginePoolDeleteRequest element contains one instance of the following element:

- EnginePool

EnginePoolDeleteRequest > EnginePool

An engine pool is a group of scan engines that can be operated as though it were a single scan engine.

EnginePoolDeleteRequest > EnginePool attributes

Name	Description	Datatype	Range
name	The name of the engine pool. **(required)**	xs:string	any sequence of characters allowed in XML; of any length

Name	Description	Datatype	Range
scope	Specifies if the engine pool has global or silo scope. **(optional)**	xs:string	“global” “silo” Defaults to “silo” if not specified.

EnginePoolDeleteRequest example

```
<?xml version="1.0" encoding="utf-8"?>
<EnginePoolDeleteRequest session-
id="36FABBDFEEBFAAFFE89178640381D35D95889D72">
    <EnginePool name="enginePool5" scope="global"/>
</EnginePoolDeleteRequest>
```

EnginePoolDeleteResponse attribute

Name	Description	Datatype	Range
sync-id	a user-specified identifier that ensures that a request is not duplicated **(optional)**	xs:string	any sequence of characters allowed in XML; of any length

EnginePoolDeleteResponse elements

An empty EnginePoolDeleteResponse element is returned if the deletion is successful.

EnginePoolDeleteResponse example

```
<?xml version="1.0" encoding="utf-8"?>
<EnginePoolDeleteResponse />
```

Code samples

This section contains sample code for a simple implementation of an API client. It is not a complete implementation, but the code samples demonstrate how an API client interacts with the application.

The sample code is written in Ruby, but has been written such that you will not need Ruby expertise to understand how the code works. The code is not meant to illustrate the “best” way of implementing an API client. It is a generic implementation that can be adapted to suit your organization's language choice and coding standards.

A more complete API implementation is available at www.metasploit.com/redmine/projects/framework/repository/entry/lib/rapid7/nexpose.rb

Fundamental API sequence

The fundamental sequence for interacting with the API is the following:

1. Open an HTTPS connection to the Web console, usually on port 3780.
2. Verify that the Content-type HTTP header is set to “text/xml”.
3. Construct a LoginRequest XML request containing valid credentials.
4. Send the XML request via the HTTPS connection to https://ncs:3780/api/1.1/xml using HTTP POST Method, where “ncs” is the host name of the security console.
5. Parse the returned LoginResponse.
6. If the success attribute is set to 1, extract the session-id attribute for use in subsequent requests. If the success attribute is set to 0, extract the Failure information and report it.
7. Construct an XML request containing the session ID.
8. Send the XML request via the HTTPS connection to https://ncs:3780/api/1.1/xml if the API command is a version 1.1 command, or to https://ncs:3780/api/1.2/xml if the API command is a version 1.2 command, using the HTTP POST Method, where “ncs” is the hostname of the security console.
9. Parse the returned XML response.
10. If the success attribute is set to 1, extract the requisite information for the XML response. If the success attribute is set to 0, extract the Failure information and report it.
11. Repeat steps 7-10 for the API calls you wish to make. When you have finished, go to Step 13.
12. Construct a LogoutRequest XML request containing the session ID.
13. Send the XML request via the HTTPS connection to https://ncs:3780/api/1.1/xml using the HTTP POST Method, where “ncs” is the hostname of the security console. If the success attribute is set to 1, the session has ended. If the success attribute is set to 0, extract the Failure information and report it.

Preliminaries: HTTPS connection initialization example

The sample API client implementation is structured as a single class, called APIClient, that makes the HTTPS connection to the Security Console and sends XML requests via HTTP POST. The API commands are methods of the APIClient class. In this example, we concentrate on the HTTPS connection initialization. The API command methods are stubs; their content will be documented and explained in subsequent sections.

```
# The three 'require' lines load the libraries that the APIClient
# needs to make an HTTPS connection with the
Security Console,
# and also the standard Ruby XML parser. The libraries that you use
# could be different depending on your environment and requirements.
require 'net/https'
require 'net/http' require 'rexml/document'
class APIClient
# The initialize method creates the APIClient object and the HTTPS
# connection to the specified host and port. The '@' symbol
# in front of the variable names makes the variable visible to all the
# methods in the class.
#
# Since the application uses a self-signed certificate, this client
uses
# @client.verify_mode = OpenSSL::SSL::VERIFY_NONE which configures the
# SSL connection to forego checking that the host name of the server
# matches the SSL certificate, even though the encryption itself is
# functional. This leaves this particular implementation of the
# APIClient vulnerable to a potential Man-in-the-Middle attack.
# However, configuring SSL host verification is beyond the scope
# of this document.
    def initialize(host, port = 3780)
        @client = Net::HTTP.new(host, port)
        @client.use_ssl = true
        @client.verify_mode = OpenSSL::SSL::VERIFY_NONE
        # The URIs for the API. We only use 1.1 APIs in this
        # implementation, but changing the URI is straightforward.
        @uri11 = "/api/1.1/xml"
        @uri12 = "/api/1.2/xml"
        # The HTTP message header must have the content type
        # configured to "text/xml"
        @ext_header = {"Content-type" => "text/xml"}
    end
# This helper method takes messages created by the API client,
# POSTs the messages to the API URI, and parses the response with
# the REXML XML parser. The parsed response is assigned to the
# @response variable, which is visible to all the methods in the
# class.
    def post(body)
        @response = REXML::Document.new(@client.post
(@uri11, body, @ext_header).body).rootend
#The methods below implement the API commands.
    def login
        ...
    end
    def logout
        ...
    end
    def usercreate
        ...
    end
    def sitecreate
```

```
            ...
        end
        def sitelisting
            ...
        end
        def scansite
            ...
        end
        def vulndetail
            ...
        end
        def report
            ...
        end
    end
    #Creates the API client
    client = APIClient.new("hostname.com", 3780)
```

Login implementation

The Login command is essential to the operation of a API client. The client must send a LoginRequest, along with valid credentials, to the API in order to receive a valid session id. The session id must be included with every subsequent interaction with the API.

```
    def login(username, password)
        # Create the LoginRequest XML message with the provided username
        # and password.
        body = "<LoginRequest user-id=\"#{username}\" password=\"#
        {password}\"></LoginRequest>"
        # Sends a POST request containing the XML message created in the
        # previous line, and creates a response. post(body)
        # The application returns an XML response. If the response has a
        success
        # attribute of 1, then the session id is extracted and assigned
        # to the @sessionid variable. Otherwise, the login has failed,
        # and the reason is output as a Failure XML message. if
        @response.attributes["success"].to_i == 1
            @sessionid = @response.attributes["session-id"]
            puts "Login successful: #{@sessionid}"
        else
            puts @response end
    end
```

User creation implementation

This method builds and posts a UserSaveRequest to create a new user. This implementation specifically creates users and activates them, so some of the UserSaveRequest attributes are given defaults.

```
def usercreate(login, password, name, email, role="user")
    # An id of -1 creates a user. id = "-1"
    authsrc = "2"
    enabled = "1" allgroups = "true" allsites = "true"
    # Build the UserSaveRequest XML message with the session ID
    # and attributes.
    body = "<UserSaveRequest session-id=\"#{@sessionid}\">"
    body << "<UserConfig id=\"#{id}\" authsrcid=\"#{authsrc}\" name=\"#
    {login}\" " body << "password=\"#{password}\" fullname=\"#{name}\"
    email=\"#{email}\" "
    body << "role-name=\"#{role}\" enabled=\"#{enabled}\" allGroups=\"#
    {allgroups}\" all- Sites=\"#{allsites}\">"
    body << "</UserConfig>"
    body << "</UserSaveRequest>"
    # Send the request and receive the response. post(body)
    # Process response and return message depending on
    # success or failure.
    if @response.attributes["success"].to_i == 1 puts "Creation of user
    #{login} successful."
    else
    puts @response
    end
end
# Use the method with the API client. Create a user named
# John Smith with the login "newguy", the password "secret",
# the e-mail address jsmith@company.com, and assign the "user"
# role.
client.usercreate("newguy", "secret", "John Smith",
"jsmith@company.com", role="user")
```

Site creation implementation

This method builds and posts a SiteSaveRequest to create a new site. This implementation specifically creates sites, so some of the SiteSaveRequest attributes are given defaults.

```
def sitecreate(host, name, description='', template="full-audit")
    # An id of -1 creates a new site. id = "-1"
    # Build the SiteSaveRequest XML message with the session ID
    # and attributes.
    body = "<SiteSaveRequest session-id=\"#{@sessionid}\">"
    body << "<Site id=\"#{id}\" name=\"#{name}\" description=\"#
    {description}\">" body << "<Hosts><host>#{host}</host></Hosts>"
    body << "<Credentials></Credentials>"
    body << "<Alerting></Alerting>"
    body << "<ScanConfig configID=\"#{id}\" name=\"Special Example\"
    templateID=\"#
    {template}\"></ScanConfig>" body << "</Site>"
    body << "</SiteSaveRequest>"
    # Send the request and receive the response. post(body)
    # Process response and return message depending on
    # success or failure.
    if @response.attributes["success"].to_i == 1 puts "Creation of site
    #{name} successful."
    else
        puts @response
    end
end
# Use the method with the API client -- create a site with
# IP address 10.0.0.1 called "Primary Site", and assign the "full-
# audit" scan template to the site.
client.sitecreate("10.0.0.1", "Primary Site", "The primary site.",
"full-audit")
```

Site listing implementation

This method builds and posts a ScanListingRequest. It then extracts a subset of the available information from the ScanListingResponse and produces formatted output.

```
def sitelisting
    # Build the SiteListingRequest with the session ID. Note
    # that the SiteListingRequest has no attributes or elements.
    body = "<SiteListingRequest session-id=\"#{@sessionid}
    \"></SiteListingRequest>"
    # Send the request and receive the response. post(body)
    # Process response and return message depending on
    # success or failure. If successful, extract data
    # from the response.
    if @response.attributes["success"].to_i == 1
        # Loop through each of the SiteSummary elements in the
        # in the response.
        @response.elements.each('SiteSummary') do |s|
            puts "Site ID: #{s.attributes['id']}" puts "Name: #
            {s.attributes['name']}"
            puts "Description: #{s.attributes['description']}"
            # This is a score calculated from two attributes.
            puts "Risk Factor + Risk Score: #{s.attributes
            ['riskfactor'].to_i + s.attributes['risks- core'].to_i}"
            puts
        end
    else
puts @response end
end
# Use the method with the API client
client.sitelisting
```

Site scan implementation

This method builds and posts a SiteScanRequest.

```
def scansite(id)
    # Build the SiteScanRequest with the session ID and the site ID.
    body = "<SiteScanRequest session-id=\"#{@sessionid}\" site-id=\"#
    {id}\">
</SiteScanRequest>"
    # Send the request and receive the response. post(body)
    # Process response and return message depending on success
    # or failure.
    if @response.attributes["success"].to_i == 1 puts "Scan started."
else
    puts @response end
end
# Use the method with the API client -- scan the site that
# has site ID 12
client.scansite(12)
```

Vulnerability details implementation

This method builds and posts a VulnerabilityDetailsRequest. It then extracts a subset of the available information from the VulnerabilityDetailsResponse and produces formatted output.

```
def vulndetail(vulnid)
    # Build the VulnerabilityDetailsRequest with the session ID and the
    vuln ID. body = "<VulnerabilityDetailsRequest session-id=\"#
    {@sessionid}\" vuln-id=\"#
{vulnid}\">"
    body << "</VulnerabilityDetailsRequest>"
    # Send the request and receive the response. post(body)
    # Process response and return message depending on success
    # or failure. If successful, extract data from the response.
    if @response.attributes["success"].to_i == 1
        puts "Title: #{@response.elements["Vulnerability"].attributes
        ["title"]}"
        puts "Description: #{@response.elements
        ["Vulnerability/description"].text}"
        puts "PCI Severity: #{@response.elements
        ["Vulnerability"].attributes
["pciSeverity"]}"
    puts "Severity: #{@response.elements["Vulnerability"].attributes
    ["severity"]}"
    end
end
# Use the method with the API client -- request details of the
# vulnerability called "apache-buffer-overflow" client.vulndetail
("apache-buffer-overflow")
```

Ad hoc report generation implementation

The ReportAdhocGeneration API command is unusual. While the responses returned by the other commands are in XML format, a successful response to a ReportAdhocGenerationRequest is composed of two components: an XML message and a base64-encoded file, all wrapped in a multi-part MIME-encoded message.

```
--AxB9sl3299asdjvbA
Content-Type: application/xml; charset=UTF-8; name=response_xml

<ReportAdhocGenerateResponse success="1"/>
--AxB9sl3299asdjvbA
Content-Type: text/xml; name=report.xml
Content-Transfer-Encoding: base64

PE5leHBvc2VSZXBvcnQgdmVyc2lvbj0iMS4wIj4NCjxzY2Fucz4NCjxzY2FuIGlkPSI2IiB
uYW1l
PSJBbm90aGVyIExvY2FsIEhvc3QiIHN0YXJ0VGltZT0iMjAxMDA3MzBUMTIxNTU3MDQ2IiB
lbmRU
aW1lPSIyMDEwMDczMFQxMjIxMDcyOTYiIHN0YXR1cz0iZmluaXNoZWQiLz4NCjwvc2NhbnM
+PG5v
... lines deleted ...
PC9OZXhwb3NlUmVwb3J0Pg==DQo=
--AxB9sl3299asdjvbA--
```

For this reason, the ReportAdhocGenerationResponse must be split into its components. After being separated, the XML message is parsed, and the base64-encoded file is decoded.

```
def report(templateid, format, siteid, filename="report")
    # Build the ReportAdhocGenerateRequest, including the session
    # ID, the report template ID, the ID of the site for which
    # the report is being run, and a filename for the generated
    # report.
    body = "<ReportAdhocGenerateRequest session-id=\"#{@sessionid}\">"
    body << "<AdhocReportConfig template-id=\"#{templateid}\"
    format=\"#{format}\">" body << "<Filters><filter type=\"site\"
    id=\"#{siteid}\"></filter></Filters>" body <<
    "</AdhocReportConfig>"
    body << "</ReportAdhocGenerateRequest>"
    # POST the ReportAdhocGenerateRequest message with
    # "Content-type: text/xml" header
    @response = @client.post(@uri11, body, @ext_header).body
    # Parse the XML portion of the response. xmlresponse =
    REXML::Document.new(@response).root
    # If the ReportAdhocGenerateRequest was successful,
    # split the entire response into parts using the MIME
    # message boundary string as the delineator. The application
    # uses the string "--AxB9s13299asdjvbA" as the boundary
    # string. One of the sections contains a content
    # header and the base64-encoded report. The report is
    # split from the header, decoded, and written to a file.
    if xmlresponse.attributes["success"].to_i == 1
        filename = filename + "." + format
        f = File.new(filename, "w")
        f.write
@response.split(/--AxB9sl3299asdjvbA/)[2].split(/base64/
).last.unpack('m')[0]
        f.close
        puts "Report generation request successful."
    else
        puts @response
    end
end
# Use the method with the API client -- produce a report on
# the site with ID 12 using the "audit-report" template
# in raw XML format. Write the report to a file called
# "myreport.raw-xml".
client.report("audit-report", "raw-xml", 12, "myreport")
```

Logout implementation

This method ends the client session and logs out the user.

```
def logout
    # Build the LogoutRequest XML message, including the session ID.
    body = "<LogoutRequest session-id=\"#{@sessionid}
    \"></LogoutRequest>"
    # Send the request and receive the response post(body)
    # Process response and return message depending on success
    # or failure.
    if @response.attributes["success"].to_i == 1
        puts "Logout of #{@sessionid} successful"
    else
        puts @response end
    end
```

Error responses

Examining error messages that the API generates can be helpful in understanding why requests fail.

Error messages include stack traces, which can be lengthy. For the examples in this chapter, large portions of stack traces will be represented by ellipses (...).

Example:

```
<stacktrace>org.xml.sax.SAXParseException: XML document structures must
start and end within the same entity.
    ...
Error parsing XML at line 1, column 54
</stacktrace>
```

This chapter includes descriptions of general types of error responses.

Examples will include valid requests, intentionally invalid requests, and responses for these requests.

Error attributes

Name	Description	Datatype	Range
sync-id	A user-specified identifier that can be used to ensure that a ticket request is not duplicated.	xs:string	any sequence of characters allowed in XML; of any length
error-code	A numeric identifier for an error type	xs:int	any signed integer small enough to be represented as a four-byte, two's complement number

Error content

Name	Description	Datatype	Range
message	a message generated by a scan engine regarding a scan-related event	text	any combination of characters

Error element

- Exception

Error > Exception

A detailed reason why the system threw an exception.

Error > Exception content

Name	Description	Datatype	Range
message	A message generated by a scan engine regarding a scan-related event.	text	any combination of characters
Stacktrace	Report of the active stack frames at a certain point in time during the execution the API.	text	any combination of characters

Error responses for malformed XML

API requests that include invalid XML structures will generate one type of error message. Examples of malformed XML include misplaced or omitted characters such as closing tags or quotation marks.

Malformed XML error responses will include the `<Failure>` or `<XML response>` tags. See the DTDs for these tags for more information in *DTD listings* on page 92.

This is a malformed XML request:

```
<LoginRequest user-id="a" password="......">
```

The request is missing a closing `</LoginRequest>` tag.

This is the error response for the preceding request:

```
<LoginResponse success="0">
<Failure>
<Exception>
<message>XML document structures must start and end within the same
entity.</message>
<stacktrace>org.xml.sax.SAXParseException: XML document structures must
start and end within the same entity.
```

```
    ...
Error parsing XML at line 1, column 54
</stacktrace>
</Exception>
</Failure>
</LoginResponse>
```

This is another example of a request with XML structure that is not well formed.

```
<?xml version="1.0" encoding="UTF-8"?>
<Failure>
    <Message>The format of the request is invalid. Error located at
    line 1, col 11
</Message>
<Exception>
<Message>XML document structures must start and end within the same
entity.
</Message>
        <Stacktrace>
            org.xml.sax.SAXParseException: XML document structures must
            start and end within the same entity.&#13;
            ...
        Error parsing XML at line 1, column 11&#13;
        </Stacktrace>
    </Exception>
</Failure>
```

Error responses for requests for non-existent API functions

Requests for non-existent API functions will generate one type of error message.

These requests often include misspelled functions, such as in the following example:

```
<LorginRequest user-id="a" password="......"/>
```

"`Login`" is misspelled as "`Lorgin`".

This is the error response for the preceding request:

```
<XMLResponse success="0">
<Failure>
<Exception>
<message>Failed initializing handler for LorginRequest</message>
<stacktrace>org.xml.sax.SAXException: Failed initializing handler for
LorginRequest
    ...
</stacktrace>
</Exception>
</Failure>
</XMLResponse>
```

Error responses common to all valid requests

Any valid API request will generate an error response if you send it while the application is still starting.

Any valid API request except for LoginRequest will generate an error response under the following circumstances:

- Your session is invalid because it expired over time, it was manually closed, or the session ID is invalid.
- You do not enter a `session-id` attribute value.
- You do not include the `session-id` attribute.

Following is an example of an error response. The string `[api]` represents the API call that was made with a bad session ID.

```
<[api]Response success="0">
<Failure>
<Exception>
<message>Session not found</message>
<stacktrace>com.rapid7.net.http.HTTPException: Session not found
    ...
</stacktrace>
</Exception>
</Failure>
</[api]Response>
```

Required attribute missing

A required attribute is not in the request.

```
<?xml version="1.0" encoding="UTF-8"?>
<Failure>
    <Message>The format of the request is invalid. Error located at
    line 1, col 89
</Message>
    <Exception>
        <Message>cvc-complex-type.4: Attribute 'session-id' must appear
        on element 'EngineActivityRequest'.</Message>
        <Stacktrace>
            org.xml.sax.SAXParseException: cvc-complex-type.4: Attribute
            'session-id' must appear on element
            'EngineActivityRequest'.&#13;
            ...
            Error parsing XML at line 1, column 89&#13;
        </Stacktrace>
    </Exception>
</Failure>
```

Required element missing

A required element is not in the request.

```
<?xml version="1.0" encoding="UTF-8"?>
<Failure>
    <Message>The format of the request is invalid. Error located at
    line 1, col 113</Message>
    <Exception>
        <Message>cvc-complex-type.2.4.b: The content of element
        'EngineSaveRequest' is not complete. One of '{EngineConfig}' is
        expected.</Message>
        <Stacktrace>
            org.xml.sax.SAXParseException: cvc-complex-type.2.4.b: The
            content of element 'EngineSaveRequest' is not complete. One
            of '{EngineConfig}' is expected.&#13;
            ...
            Error parsing XML at line 1, column 113&#13;
        </Stacktrace>
    </Exception>
</Failure>
```

Unknown request

The application could not find an API end point to invoke, most likely due to misspelling of the root element name.

```
<?xml version="1.0" encoding="UTF-8"?>
<Failure>
    <Message>The format of the request is invalid. Error located at
    line 1, col 24</Message>
    <Exception>
        <Message>cvc-elt.1: Cannot find the declaration of element
        'BadEndpoint'.</Message>
        <Stacktrace>
            org.xml.sax.SAXParseException: cvc-elt.1: Cannot find the
            declaration of element 'EndpointDoesnotExist'.&#13;
            ...
            Error parsing XML at line 1, column 24&#13;
        </Stacktrace>
    </Exception>
</Failure>
```

Unexpected attribute

An additional, superfluous attribute exists in any element where it is not expected.

```
<?xml version="1.0" encoding="UTF-8"?>
<Failure>
    <Message>The format of the request is invalid. Error located at
    line 1, col 155
</Message>
    <Exception>
        <Message>cvc-complex-type.3.2.2: Attribute 'extra' is not
        allowed to appear in element 'EngineActivityRequest'.</Message>
        <Stacktrace>
            org.xml.sax.SAXParseException: cvc-complex-type.3.2.2:
            Attribute 'extra' is not allowed to appear in element
            'EngineActivityRequest'.&#13;
            ...
        Error parsing XML at line 1, column 155&#13;
        </Stacktrace>
    </Exception>
</Failure>
```

Invalid value

One of the values entered in the request is outside the acceptable range.

```
<?xml version="1.0" encoding="UTF-8"?>
<Failure>
    <Message>The format of the request is invalid. Error located at
    line 1, col 144</Message>
    <Exception>
        <Message>cvc-minInclusive-valid: Value '-5' is not facet-valid
        with respect to minInclusive '1' for type
        'positiveInteger'.</Message>
        <Stacktrace>
            org.xml.sax.SAXParseException: cvc-minInclusive-valid: Value
            '-5' is not facet-valid with respect to minInclusive '1' for
            type 'positiveInteger'.&#13;
            ...
        Error parsing XML at line 1, column 144&#13;
        </Stacktrace>
    </Exception>
</Failure>
```

Scan engine unreachable

A socket timeout occurred on the engine referenced in the save request.

```
<Failure>
    <Message>Error encountered, unable to fulfill request.</Message>
    <Exception>
        <Message/>
        <Stacktrace>
            java.net.SocketTimeoutException&#13;
            ...
            at com.rapid7.thread.ThreadedCallRunner.run
            (ThreadedCallRunner.java:44)&#13;
        </Stacktrace>
    </Exception>
</Failure>
```