ivanti

Data Center Discovery

SCAN ENGINE USER GUIDE

Contents

Introduction

This user guide for the Ivanti Data Center Discovery scan engine provides all the information needed to operate the scan engine through its user interface ("dashboard"). This document uses a series of use cases to identify potential configuration options that may be required to manage your project. Read this guide to learn about:

- How the scan engine works
- Using the dashboard to set up a scan
- Use cases for scanning basic to complex estates
- How to analyze the scan data
- General administration

The documentation set for the Data Center Discovery scan engine contains the following guides:

Guide	Description
Prerequisites Guide	Defines system requirements for the installation.
Installation Guide	Guides you through installing the Data Center Discovery Scan Engine.
Deployment Guide	Provides deployment scenarios and constraints.
User Guide	Helps users control and configure the Scan Engine.
Security Guide	Outlines security considerations.

About the Data Center Discovery scan engine

The Data Center Discovery scan engine is a discovery and inventory tool used to gather relevant data in an estate. It's designed to retrieve this information in a secure form.

It's both **agentless** and **secure** and is designed to have a small deployment footprint within your estate.

Agentless integration describes a process whereby the scan engine does not require the installation of additional software on the target servers from which the scan engine will gather data.

Additional attributes of the product are:

- It's quickly installed (less than 5 minutes assuming prerequisites have been met), allowing you to move on to the scan configuration stage.
- It's centrally managed. Multiple scanning servers can be controlled from a single dashboard.

Secure identifies that the scan-engine software was designed with the protection of the process and data-retrieval operations in mind.

The credentials you enter into the product do not have to be shared with Ivanti. A customer-specific private key can be generated to isolate knowledge of the encrypted data within the deployment. This is encrypted using the RSA-2048 algorithm.

The scan engine focuses on the inventory of complex enterprise server technologies from Oracle, Microsoft, IBM, VMWare, and others to deliver the visualization of physical, virtual, and cloud-based hardware and software assets. It's designed for use in all sizes of network estates, with a multi-

threaded architecture and an innovative database design enabling scalability to support 100,000+ devices.

The scan engine is deployed entirely within the client network; it retains all data centrally and securely. Security is enhanced through intelligent credential management and seamless integration with user access control products, proxies, and administration gateways. For more on security, refer to the **Scan Engine Security Guide**.

Installation instructions

The installation instructions for the scan engine software are available in the **Scan Engine Installation Guide.**

Accessing the configuration user interface – "dashboard"

The scan-engine interface is web based, so it's typically remotely accessible from any device over a browser interface to the installation device. To access the dashboard after installation, type the following URL in your Internet Explorer browser:

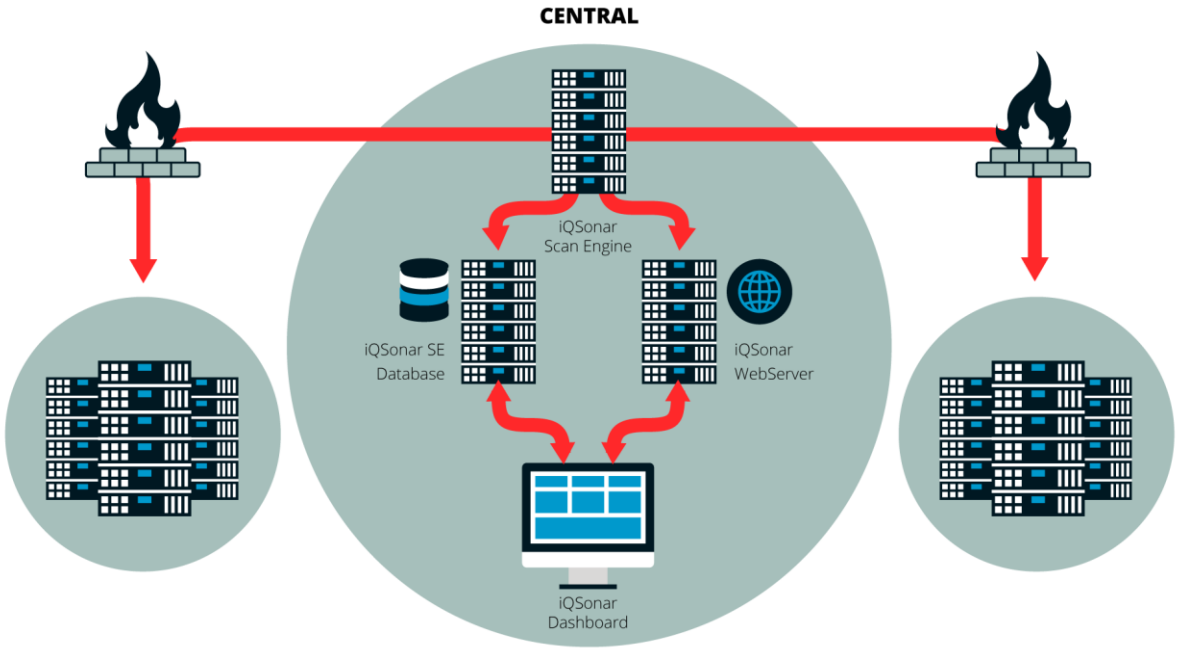
http://{hostmachine}/{uipath}

The **hostmachine** is the hostname (or IP address of the host) upon which the scan engine UI installation is made. If this is the local device, then the "localhost" value may be used here. The **uipath** element is specified as part of the Data Center Discovery scan engine UI. The default value for the installer is "Data Center Discovery".

An example for access to the UI on a local device installation is: **http://localhost/Ivanti**

How the Data Center Discovery scan engine works

The scan engine is composed of scan-engine software, a database, and controlling dashboard. The web-based dashboard is used by the scan administrator to identify scan targets within the estate, provide credentials that will allow access to the targets, and configure projects that identify the scope of the scanning operations.



About the scan process

The Data Center Discovery scan engine searches your estate for target devices. The possible target device ranges are identified as part of the configuration of the scan engine. They can be a set of IP ranges (essentially any access point for devices). These IP ranges are probed and active devices are identified. The primary discovery methods used to discover devices on an estate are **Ping** and **Port Scan**.

Once a device is discovered, a test is executed. This test is called device uniqueness. If the device passes the uniqueness test, it's retained for additional scanning.

The unique device is then scanned for applications. The applications must pass the uniqueness test in order to be scanned further.

The unique devices and/or application-scanned information is stored in the scan database.

Supported platforms

The platforms supported for the features outlined in this document are:

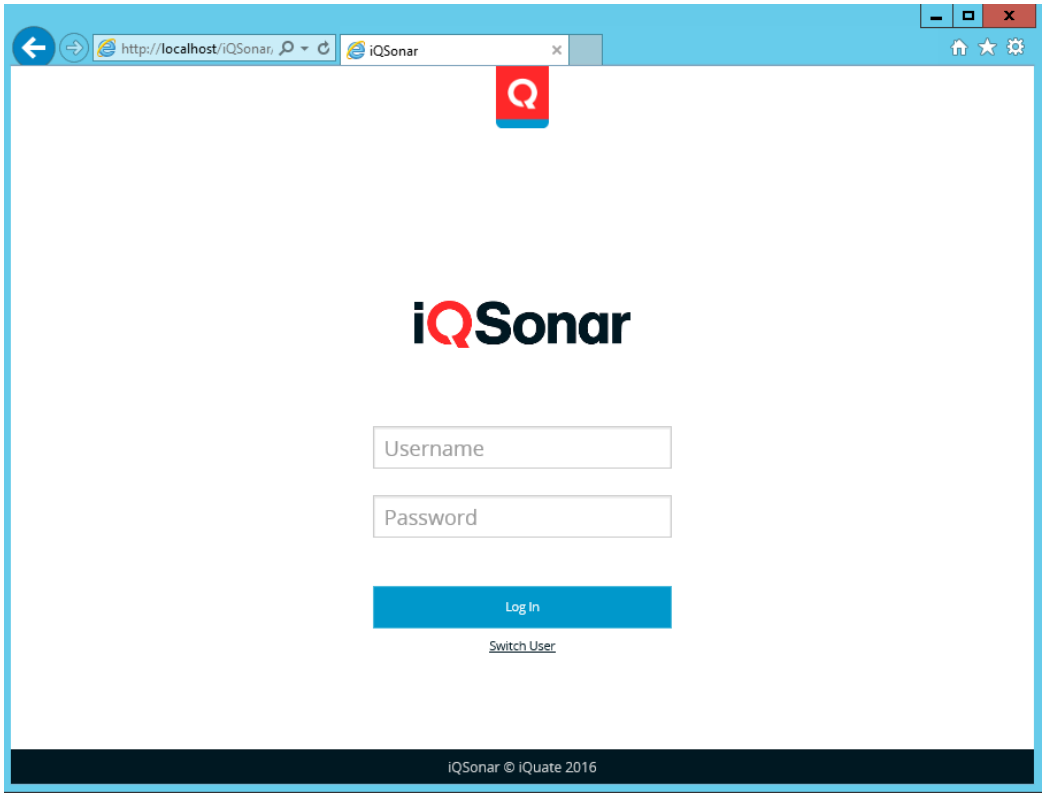
- Windows Server
- Windows Desktop
- Linux
- HP-UX
- Solaris
- AIX
- Network
- Routers/switches
- Printers
- Storage devices

Initial login

Following the installation, a single login exists for the dashboard. Access to the dashboard is provided with the defaults of:

- **Username:** Admin
- **Password:** password

You need to protect access to the web interface by the creating additional user logins and appropriate password values, and by modifying the default **Admin** password.



Once a correct set of credentials is provided, the standard user interface for the dashboard is presented. It's composed of the top-level scanning component items that you use to configure the scan operations for an estate. The work load of scanning an estate may be broken into sub-components using multiple scan engines (services). In such a case, the configuration and scanning information shares a central scan-engine database.

User interface

The scan engine includes an administrative UI, called the dashboard, which allows configuration and control from a web browser.

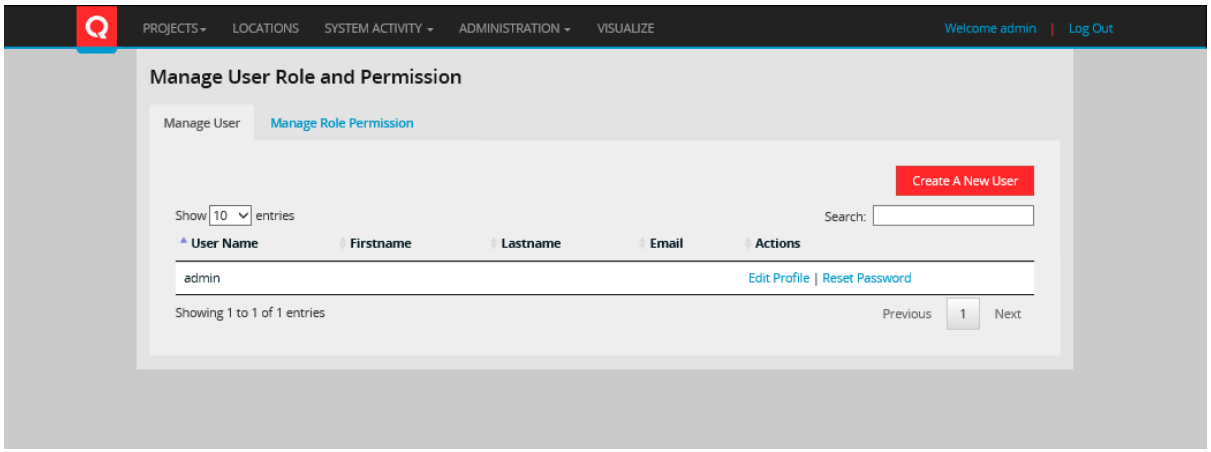
This is a view of the scan engine dashboard immediately after login. The UI contains the following sections as shown in the screenshot above:

- **Projects:** Breaks down the scan operation by functional requirements.
- **Locations:** Breaks down the scan operations by localities.
- **System activity:** Shows system activity across the scan estate.
- **Administration:** Controls the general operations of the scan.
- **Visualize:** Shows a visual representation of the scan estate and results.

> **Note:** Since the scan engine has not been activated, an optional **Activation** banner is displayed. Click this banner to move to the activation section of the UI immediately.

Change Admin password

As a general security procedure, it's advisable to change the default Admin user password.



To change the password

1. From the **Administration** drop-down menu, select the **User Settings** tab.

2. Under the Manage User tab, click the **Reset Password** link.
3. Provide a new password.
4. Click the **Reset** button.

Active Directory and application users

Login: Admin

The scan-engine UI supports the creation of users that you can assign to project-specific roles. Users can be either local to the scan-engine UI application, or they can be pre-existing Active Directory (A/D) Users. The rest of this document provides example use-cases with local users. However, any local-user identity can be replaced with an A/D registered user.

> **Note:** To use Active Directory authentication, select the **Enable Active Directory for User Accounts** option during the IIS Configuration step of the installation process. If this option is not selected, enabling Active Directory authentication for the scan-engine application in IIS will allow the use of Active Directory accounts.

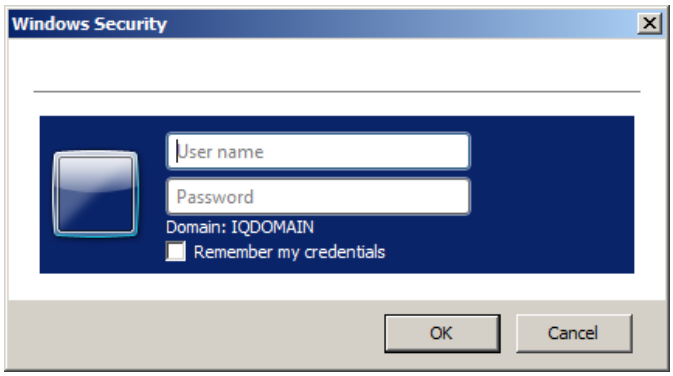
The following steps show how a user called **demouser** (from a domain called **demodomain**) logged into the application. This Active Directory user is associated with the administration role for the scan engine (i.e., this A/D user has the same permissions as the built-in admin user). Refer to the image above for reference.

1. Select the **Administration** icon or click the **Administration** drop-down menu in the dashboard. The administrator role already exists and does not require any specific handling.
2. Select the **User Settings** tab.
3. Select the **Manage User** tab.
4. Click the **Create A New User** button.
5. Click the **AD user** checkbox; this is an Active Directory user.
6. Insert the domain name into the Domain Name field (e.g., demodomain).
7. Insert the domain user into the Username field (e.g., demouser).
8. Insert a value as the Firstname field (optional).
9. Insert a value as the Lastname field (optional).
10. Provide an email address for the receipt of e-mails (optional).
11. Note a password is not required, as this is an A/D user.
12. Select the **Administrator** role for the user.
13. Click the **Create** button.

The new user is available for login.

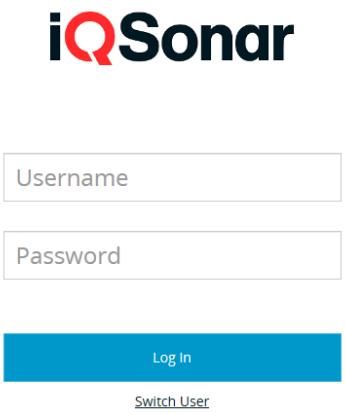
Active Directory login

If the current domain login doesn't match a Data Center Discovery scan engine-registered active domain user account, a Windows Challenge login window will display.



Provide the domain login information for the A/D user and click the **OK** button.

> **Note:** The above Windows challenge is used **exclusively** for Active Directory user login. The UI standard login challenge below is used **exclusively** for application-based user logins. If you're presented with the standard login window and want to log in with a domain user, then click the **Switch User** link at the bottom of the banner.



How to start

There are several important steps you must follow to ensure device and application discovery and that the information required is retrieved from the scan:

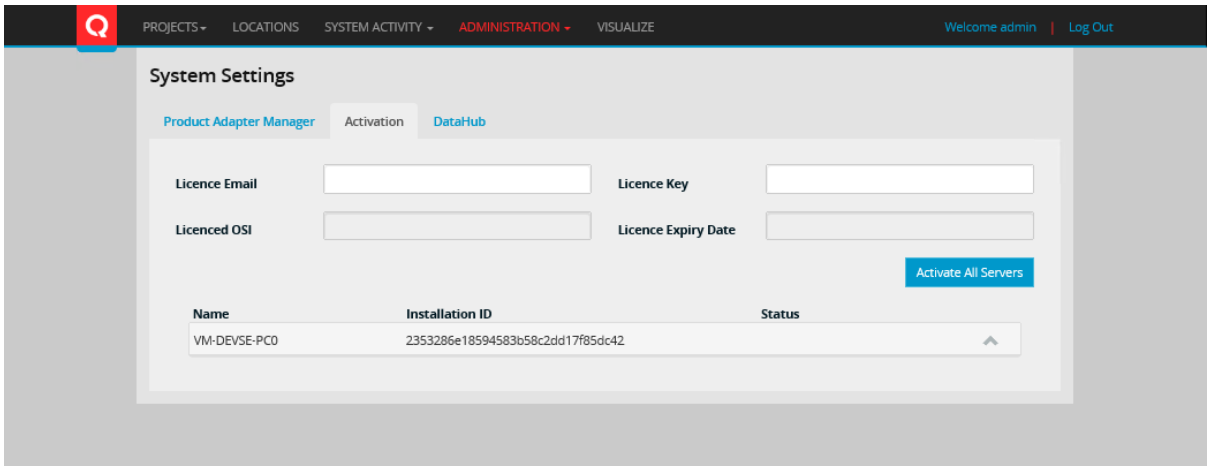
- Set up a scan from the dashboard
- Initiate scanning discovery and scanning services
- View the scan data and log files

System settings – activation

The scanning service requires an activation license. If you haven't previously set up the licensing for this scan engine, then you need to do this *before* starting the scan by accessing the **Administration > System Settings** tab.

This license is provided by Ivanti support or through an online activation website.

Automatic activation requires an assigned email address and an assigned license key. Clicking the **Activate All Servers** button will initiate the registration of the scan engine. Projects can now be allowed to execute.



Setting up the scan

There are several important steps involved in setting up the scan from the scan-engine dashboard. The two most important steps are inputting the **targets** (which are the IP ranges to scan) and the **operating system** and **application** credentials that will be used to gain access to the target devices.

There are six sets of instructions that you need to follow:

1. Scan Windows
2. Input targets
3. Set up connections
4. Enable product adapters
5. Input operating system credentials
6. Input application credentials

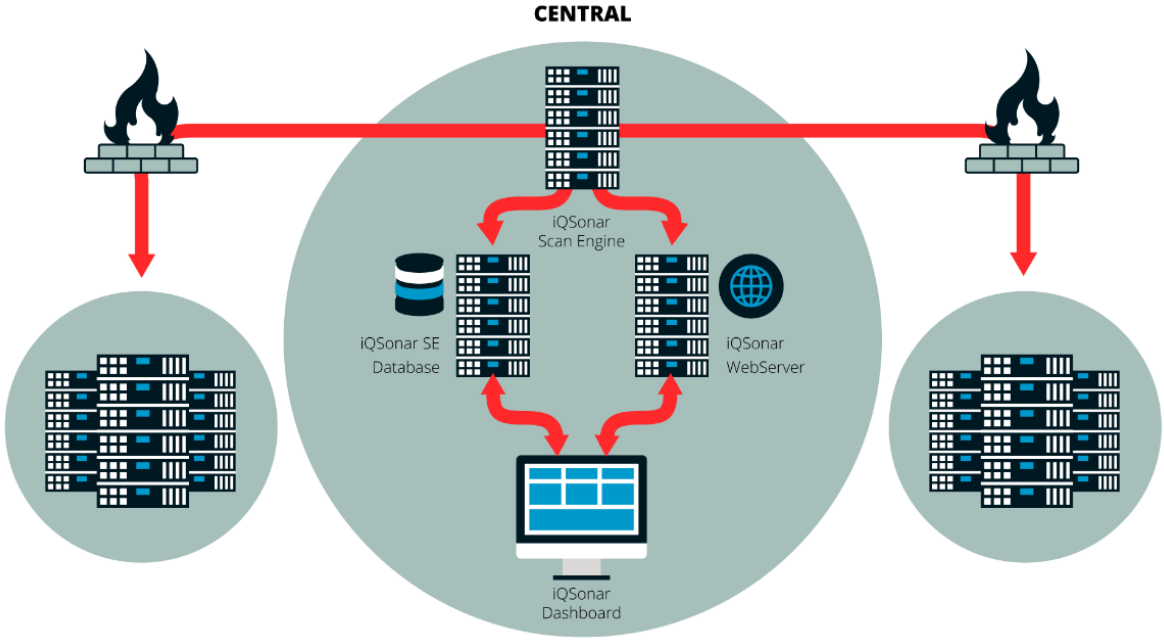
The rest of the document is composed of a number of use cases. These are complete configuration examples that walk you through the configuration of the scan-engine UI. These use cases should act as a basis for deciding on the details of an actual on-site configuration.

The use cases provided here are:

- **Use Case 1: Basic estate (or POC).** A basic estate is composed of a single location or a single non-disjoint network. Responsibility for the network resides with a single person or group. The scan results do not have to be segmented into different overall projects (e.g., Oracle project results, SQL Server project results, etc.)
- **Use Case 2: Multi-departmental estate.** A multi-departmental estate is composed of multiple locations and/or a disjoint network infrastructure. Responsibility for the network resides with a single person or group, with the complexity that locations are typically geographically disjointed and are also split into production and test sub-areas. The scan results may be segmented into different overall projects (e.g., Oracle project results, SQL Server project results, etc.) depending on the customer use case.
- **Use Case 3: Complex estate.** A complex estate is composed of multiple locations and/or a disjoint network infrastructure. Responsibility for the network resides with a central person, but responsibility also resides with a local infrastructure control person or group. Local control covers test and production sub-areas. The scan results may be segmented into different overall projects (e.g., Oracle project results, SQL Server project results, etc.). Additionally, to spread the CPU load and network load of the scanning operations, additional scan engines have to be deployed.

Use case 1 – Basic estate

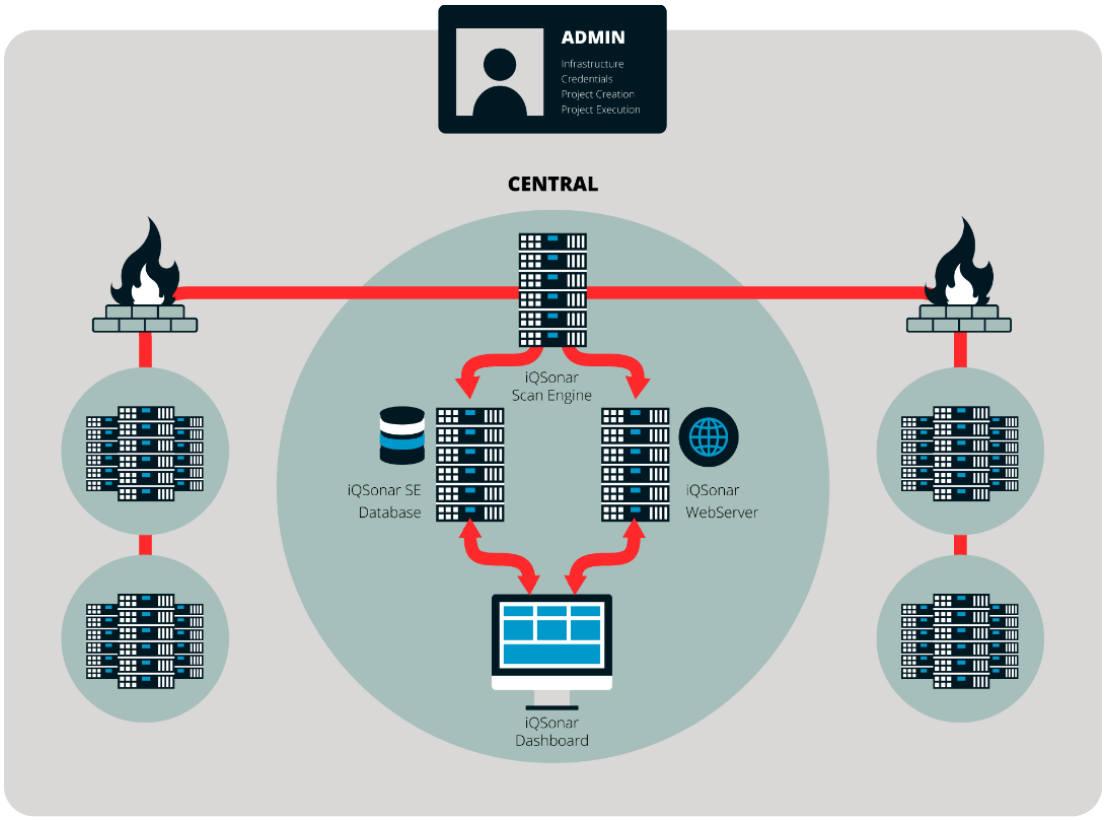
For a basic estate, the network infrastructure is composed of a relatively open network with no major restrictions in terms of firewalls, network latency, or bandwidth.



Basic estate - Responsibility ownership

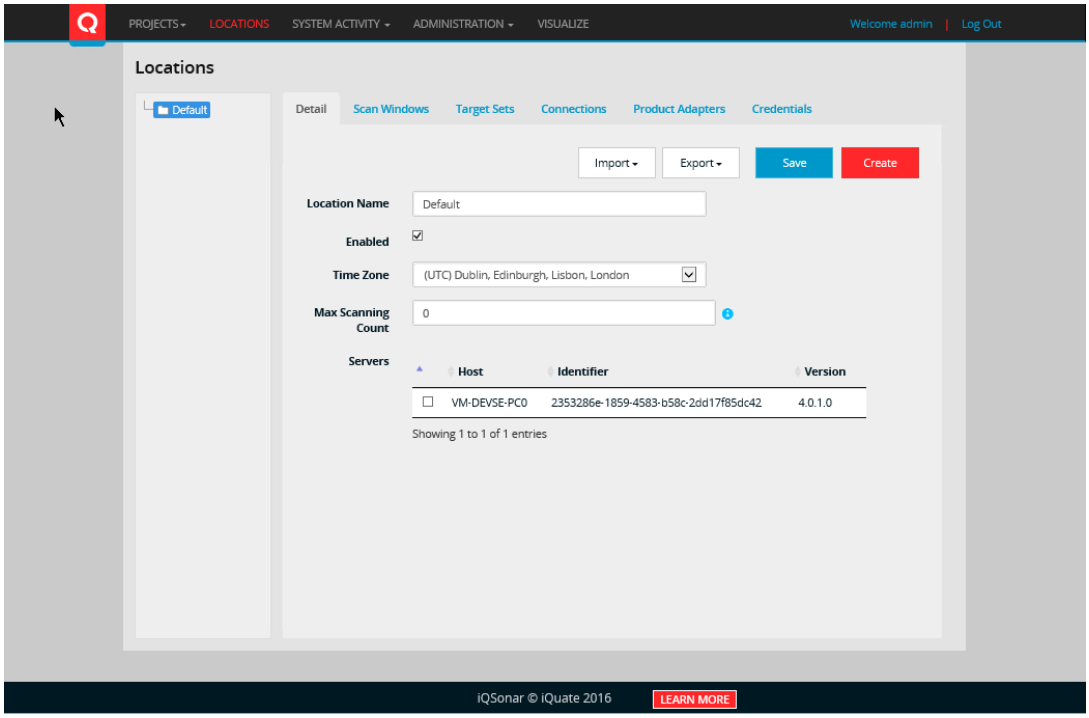
The advantage of a basic estate or POC (Proof of Concept) is that little configuration or control is required during the running of the scan operation; in addition, responsibility for the network configuration is (typically) restricted to a single person.

This sole responsibility will reside in an identity called “Admin” who identifies the target infrastructure, the credential to be used during the scan operation, and the projects that are to be run within the estate.



Basic estate - Locations

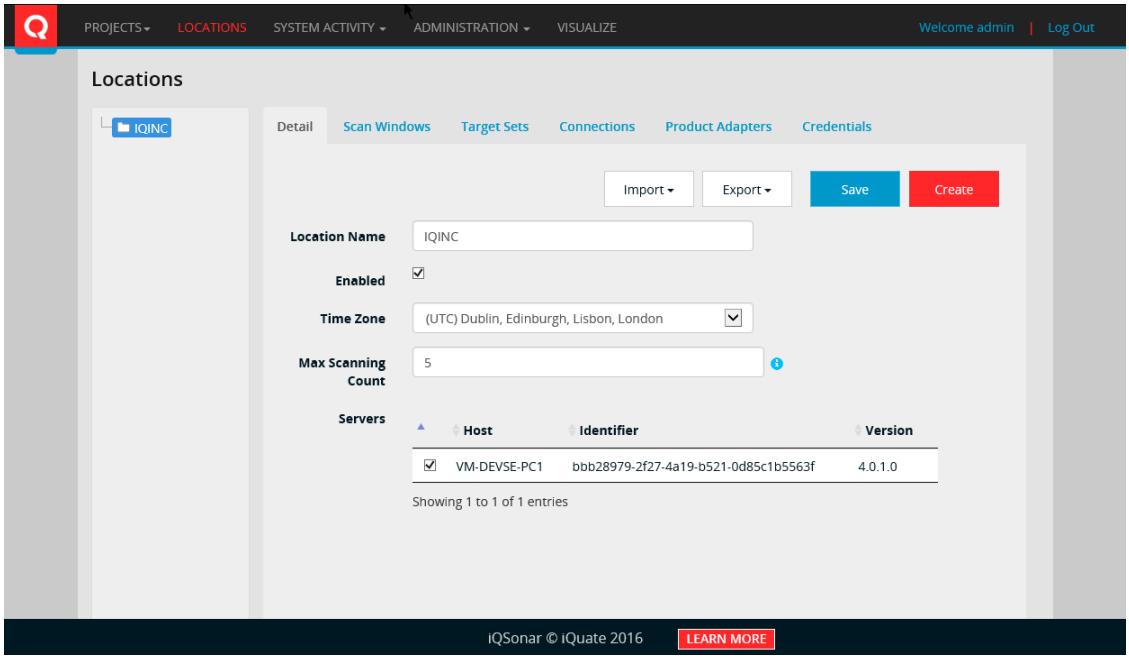
A default location is provided with the standard install. This default location can be used to encompass all of the proposed estate. Follow the instructions below:



1. Select the **Locations** icon or click the **Locations** drop-down menu in the dashboard. This displays the current available locations. By default, a single location called “Default” is

available as a top-level item. This is the top-level grouping and cannot be deleted (but can be renamed). It's recommended that you rename it to a customer/project-appropriate value.

2. Enter the details of your new default location in the Location Name field.
3. Ensure that **Enabled** is selected.
4. Enter the Time Zone of this locality.
5. Enter the Max Scanning Count of **5** (how many concurrent jobs that can be run for targets in this location).
6. Select the scan engines associated with this locality.
7. Click the **Save** button to save your details.



This single location is sufficient for a small project – a basic estate; however, larger projects may need more granular control over which/how elements of the estate are to be scanned.

Basic estate - Scan Windows

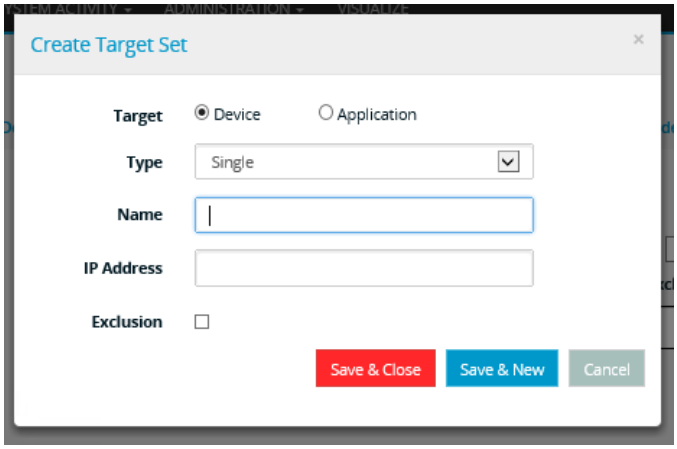
Scan Windows provides a means to limit the period when active scanning of an estate is carried out. For mission-critical enterprises, the possibility of additional network traffic or CPU is viewed as a risk. For this reason, you can specify specific time periods for scanning.

For a basic estate or POC, it's assumed that no restrictions will be applied. The Scan Windows settings can be ignored for this basic estate operation.

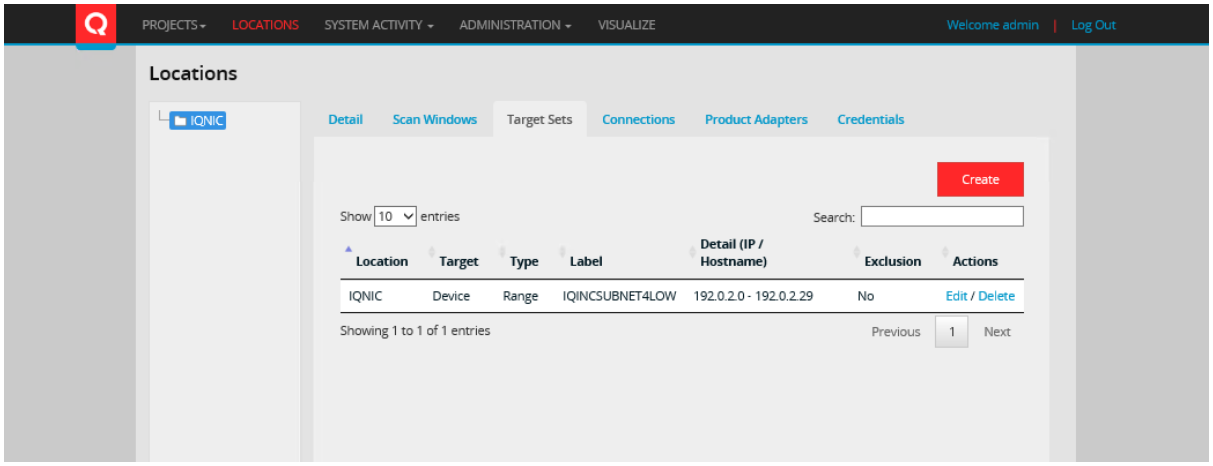
Basic estate - Targets

Targets are used to identify the scope of the scan operations. Scan operations can be targeted against a single IP address, a range of IP addresses, or a complete subnet. The location needs to have

an associated IP range to scan. The following procedure identifies an example range of IP addresses and associates this range with a name of **SUBNET4LOW.**



1. Select the top-level location.
2. Select the **Targets** tab.
3. Click the **Create** button to add a new target.
4. In the Create Target Set dialog, set the IP Range Type to **Range**.
5. Set the Name to be **SUBNET4LOW**.
6. Set the Start IP to be **192.0.2.0** - this is an example value.
7. Set the End IP to be **192.0.2.29** - this is an example value.
8. Clear the **Exclusion** option.
9. Click the **OK** button.
10. Check that the new range is now associated with the location.



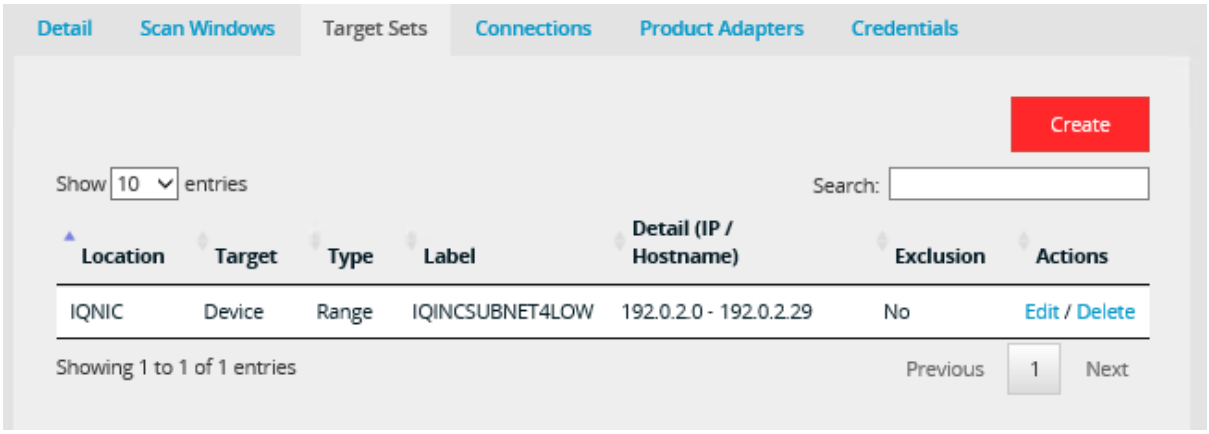
Basic estate - Direct application scanning

If you want to scan an application directly, for instance, where the device is inaccessible or where you're certain of the existence of an application, the option is available to perform a direct application scan.

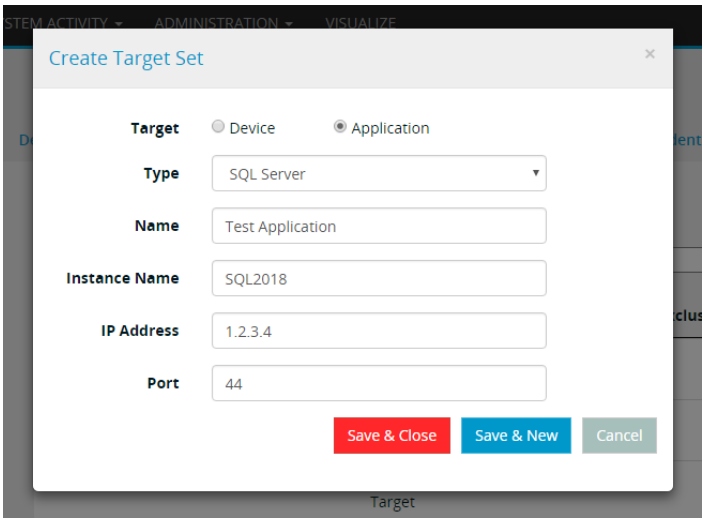
To do a direct application scan, you must identify the application type in question and provide the necessary connection details to connect to the application. This is done by creating an application target.

To create an application target

1. Select the **Target Sets** tab on the location in question.



2. Click the **Create** button to display the Create Target Set dialog.



3. Select **Application**, and then select the specific application type which is to be scanned.
4. Issues to be considered for specific application types:
   - Instance Name is not required for vCenter type.
   - The default port will be used if none is specified.
   - Port needs to be specified for vCenter.
5. Click **Save & Close**.

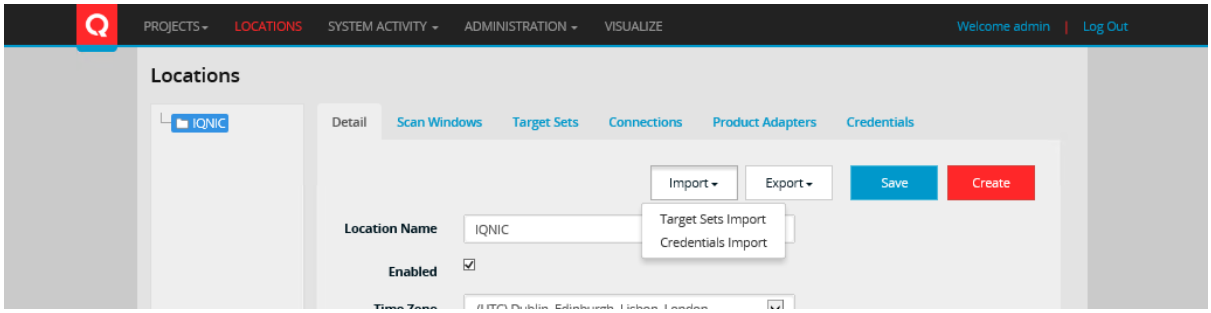
The new application target will appear in the Targets list for the location. You can edit or delete the target in the same way as other targets.

> **Note:** If the application target is created in a location that doesn't have the required settings enabled for the target to be scanned successfully (e.g., required connection is not enabled), the

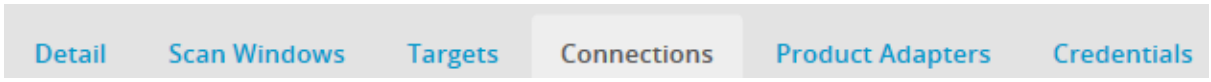
> target will still be created, but a warning message will appear, notifying you of the settings that need to be enabled to successfully scan the target.

Basic estate - Bulk-load of targets

The ability to bulk load targets is provided under the **Locations > Details** tab. The Import and Export menus provide the ability to import targets. Follow the instructions and file formats provided (a template is provided).



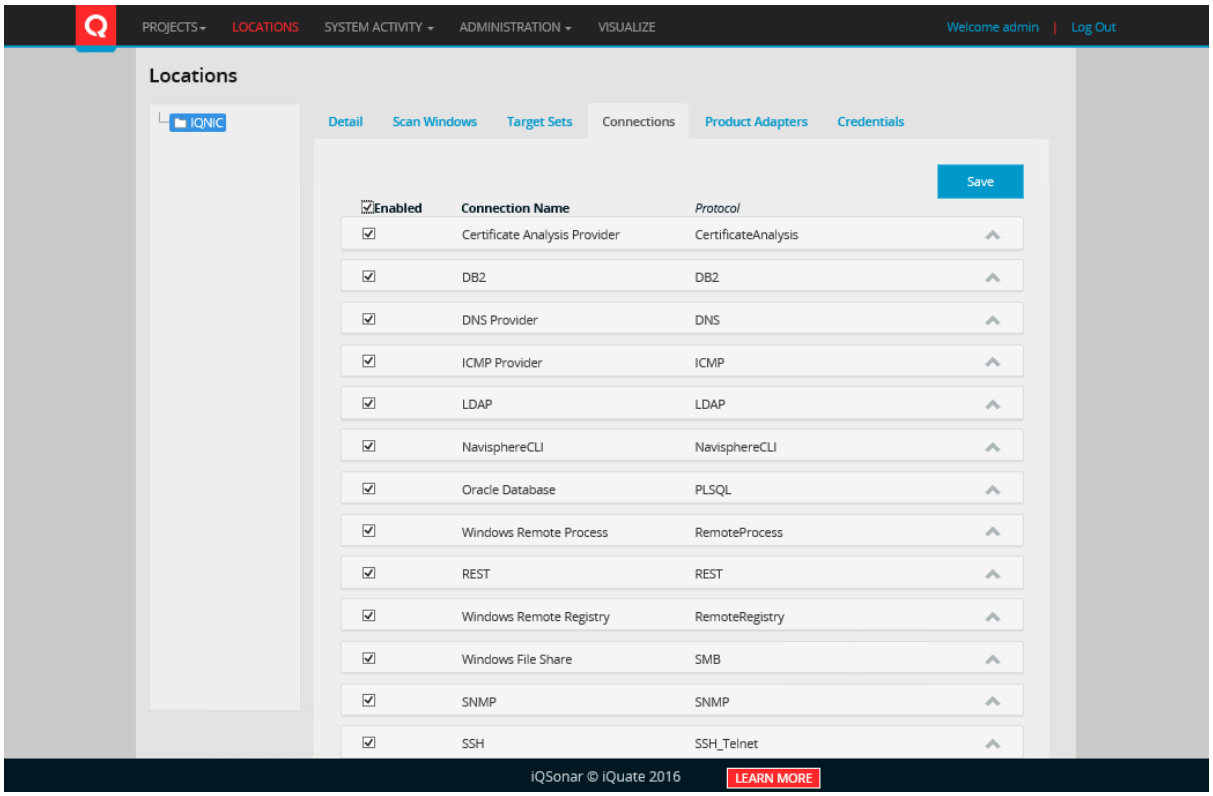
Basic estate - Connections



Connections are the means by which information retrieval is achieved by the scan engine. Each connection type is associated with one or more configuration items (such as connection time, command time out, etc.)

A connection type is a logical communication path to a target device or application. Underlying this logical connection is one or more physical protocols that are established between the scan engine and the target device. These connections are used to execute commands that retrieve data.

1. Click the top-level **Enabled** check box.
2. Click the **Save** button.
3. Click the items icon on any row to show associated configuration items.



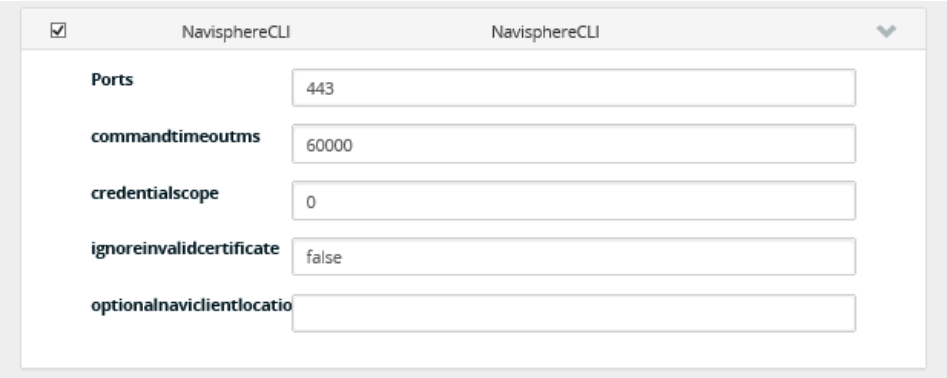
Basic estate - NavisphereCLI connection

The connection type **NavisphereCLI** is used by the storage product adapter to retrieve storage information from EMC-based storage devices. This product adapter is still in BETA release and subject to change.

The connection is based on the installation of the NavisphereCLI software as specified in the **Scan Engine Prerequisites Guide**. This connection uses a third-party API to connect to and retrieve storage usage/configuration information from the remote storage device.

There are specific elements of the configuration that you need to address here to allow the retrieval of the storage device information.

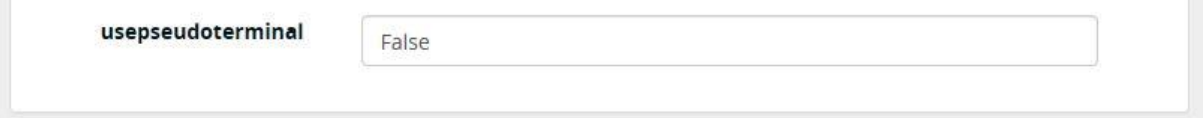
Click the **NavisphereCLI** expand button to expand the options. The settings provided here must match those that were specified during the installation of the NavisphereCLI package.



- **Port**: The secure port used to establish the SSL connection to the remote storage device. This only needs to be modified if another port is being used.
- **Command Time Out**: This time out value does not need to be modified.
- **Credential Scope**: Credentials for NavisphereCLI software can be created globally or locally for storage. If global credentials are to be used, then set the credentialscope value to **0**; if local credentials are used, then set this value to **1**.
- **Ignore Invalid Certificate:** The security associated with the NavisphereCLI client can be installed with either **medium** or **high** security settings. SSL interaction requires the exchange of certificate information and a high security setting will enforce that certificate validation must pass. This option downgrades this requirement to the medium level and allows certificate checking to be ignored.
- **Optional NaviClient Location:** The location of the NavisphereCLI software is typically located through the use of the Windows registry. If a non-standard installation of the NavisphereCLI software was carried out, the location of the software installation directory can be specified using this option.

Basic estate - SSH connection

- **Command Prefix Code:** The connection type **SSH** can be used in with the command prefix SUDO to escalate your permissions to cover additional commands contained within the sudoers file. SH is used by default; to specify a custom command prefix, set **usecommandprefix** to **True**.
- **Use Command Without Path:** By default, the scan engine executes commands on the target by defining the full path to it. In the case of a restricted shell (HMC, for example), slashes are not permitted. This results in the commands failing if the full path is defined. By setting this option to **True**, the command will execute without using the full path.
- **Use Pseudo Terminal:** A sudoers file with the configuration requiretty will fail to execute commands when a terminal isn't provided. Setting usepseudoterminal with a value of **True** will prevent this failure.



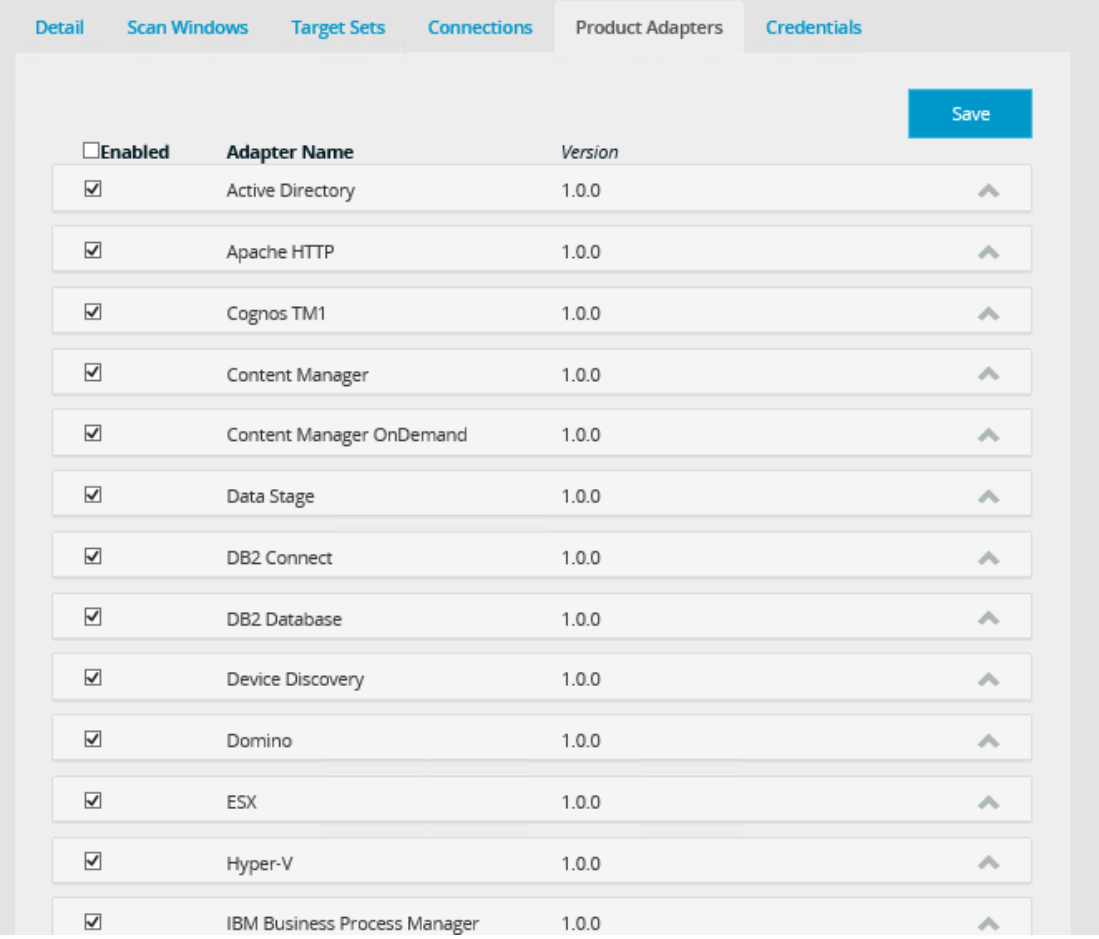
Basic estate - SSHProxy connection

- **RequestFailedPermittedRetries:** When using the SSHProxy connection, it's possible for the proxy server to deny the connection and attempt a shell. In this situation, an exception will be thrown with the message "The request has failed." This option allows you to configure the number of attempts the scan engine will re-attempt the connection before the connection is abandoned for the given target. It supports Integer values.

Basic estate - Product adapters

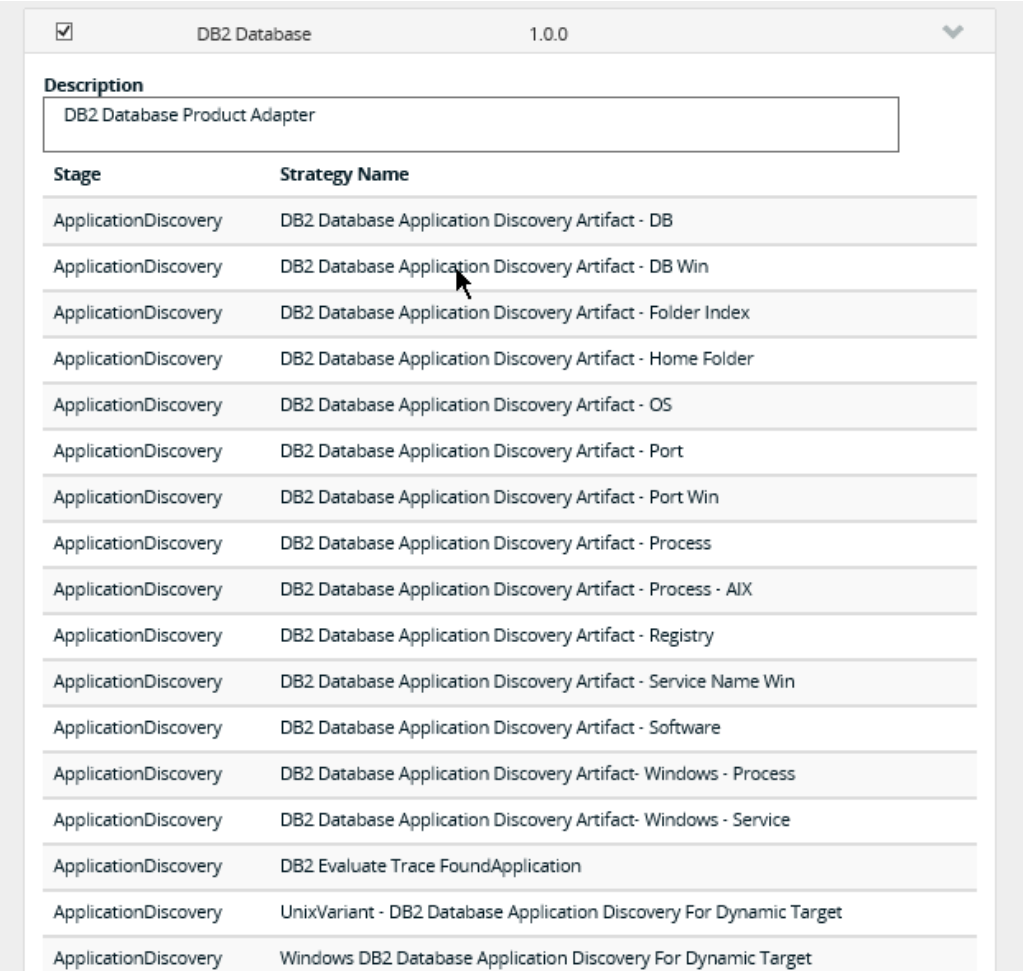
The **Product Adapter** functionality means that additional protocols, commands, and "transformation of scanned data" can be added to the core platform. This product development can be driven by customer requirements or emerging technology.

The Product Adapter dialog below identifies the currently enabled product adapters:



The expand button enables you to further expand elements of the product adapter, exposing the individual strategies that you can then enable or disable. Any enabling or disabling of a product adapter can be achieved clicking the **Save** button.

Clicking the expand button again collapses the expanded product adapter.



DB2 Database 1.0.0

Description

DB2 Database Product Adapter

Stage	Strategy Name
ApplicationDiscovery	DB2 Database Application Discovery Artifact - DB
ApplicationDiscovery	DB2 Database Application Discovery Artifact - DB Win
ApplicationDiscovery	DB2 Database Application Discovery Artifact - Folder Index
ApplicationDiscovery	DB2 Database Application Discovery Artifact - Home Folder
ApplicationDiscovery	DB2 Database Application Discovery Artifact - OS
ApplicationDiscovery	DB2 Database Application Discovery Artifact - Port
ApplicationDiscovery	DB2 Database Application Discovery Artifact - Port Win
ApplicationDiscovery	DB2 Database Application Discovery Artifact - Process
ApplicationDiscovery	DB2 Database Application Discovery Artifact - Process - AIX
ApplicationDiscovery	DB2 Database Application Discovery Artifact - Registry
ApplicationDiscovery	DB2 Database Application Discovery Artifact - Service Name Win
ApplicationDiscovery	DB2 Database Application Discovery Artifact - Software
ApplicationDiscovery	DB2 Database Application Discovery Artifact- Windows - Process
ApplicationDiscovery	DB2 Database Application Discovery Artifact- Windows - Service
ApplicationDiscovery	DB2 Evaluate Trace FoundApplication
ApplicationDiscovery	UnixVariant - DB2 Database Application Discovery For Dynamic Target
ApplicationDiscovery	Windows DB2 Database Application Discovery For Dynamic Target

To disable individual strategies, access the scan engine's configuration file:

1. Navigate to the bin folder in the install directory. (Typically C:\Program Files\iQuate\iQSonar ScanEngine 4.0)
2. Open the iQuate.iQSonar.ScanEngine.exe.config file.
3. Locate the line beginning **<add key="DisabledStrategies**".
4. Modify the value property to contain a list of strategies to be disabled. The value must be a comma-separated list with each entry taking the form: <ProductAdapterName>:<StrategyName>.

   For example, to disable the DB2 Evaluate Trace Found Application Strategy in the DB2 Database product adapter, the value DB2 Database:DB2 Evaluate Trace Found Application Strategy should be added to the DisabledStrategies list.

Basic estate - System credentials

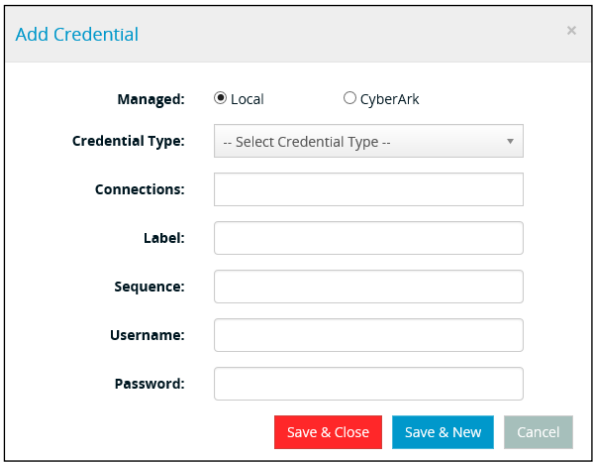
System Credentials are the credentials used to provide access to an operating system (such as Windows or *Nix) or an operating system component (such WMI or Remote Registry).

You can manage credentials locally in the underlying scan-engine database or retrieve them from a configured **CyberArk** installation. The default setting when creating a credential is **Local** – this indicates the credential is managed by the scan engine. To create a **CyberArk** credential, select the **CyberArk** option from the **Managed** radio buttons. Also configure the following additional fields:

- **Safe:** The safe within the **CyberArk** vault where the **Credential** is stored. This field is optional; however, it should be noted that where no value is provided, the **CyberArk** integration component will return the first matching credential.
- **Folder**: The folder within the **Safe** where the **Credential** resides. This field is optional; however, it should be noted that where no value is provided, the **CyberArk** integration component will return the first matching credential.
- **Account name**: The name of the credential.

These types of credentials are equivalent to a real user trying to access a remote system from the scan engine device.

1. Select the top-level location.
2. Select the **Credentials** tab.
3. Click the **Create** button to add a credential.
4. The default Managed setting is **Local** – this indicates that the credential is managed by the scan engine.



5. Set the Credential Type to **UNIX Linux**.
6. Set the Name to be **UnixScan**.
7. Set the connection types to **SSH**, **SSHProxy**, and **Telnet**.
8. Type the label for this credential (e.g., UnixScanUser).
9. Provide an ordering value for this credential. This is a relative value (i.e., sequence one (1) credentials will be used before sequence two (2) credentials, and so on).
10. Type the UnixScanUser username value; this user will be used to remotely access the target devices. This can be a user specially created for the scanning process or an existing login.
11. Type the UnixScanUser user password value; this value will be encrypted for later use and will not be stored in cleartext.
12. Click the **Save & Close** button.
13. Check that the new credential is now associated with the location.

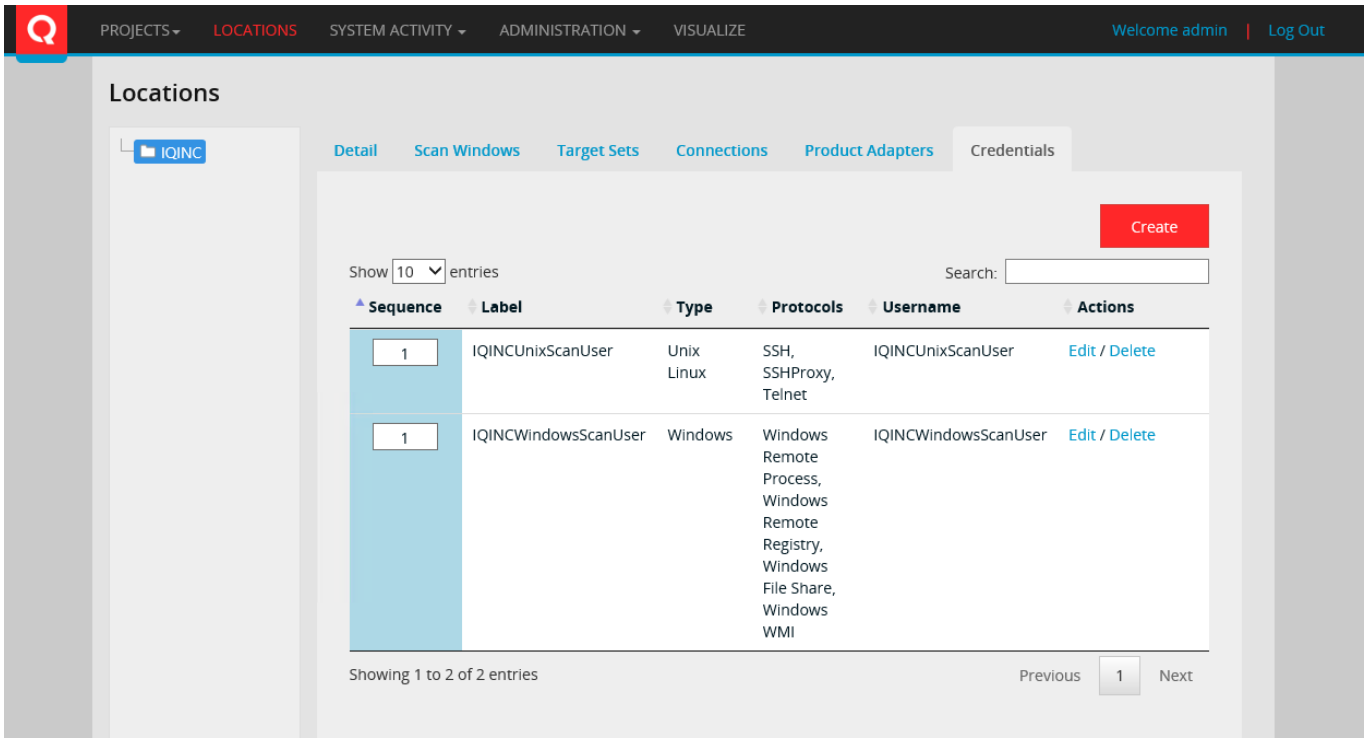
UNIX Linux has an additional field labelled **Child Credential,** which can be filled with an SSH Proxy credential and is optional.

In the case that a SSH Proxy credential is assigned to a UNIX Linux credential, the password field of the UNIX Linux credential becomes optional. When there is no child credential attached to a UNIX Linux credential, the password field becomes required again.

An SSH Proxy credential cannot be deleted if it's assigned to an existing UNIX Linux credential.

Repeat the process to add a **Windows** account credential:

1. Select the **Credentials** tab.
2. Click the **Create** button to add a credential.
3. View the Create a Credential dialog that is opened.
4. Set the Credential Type to **Windows**.
5. Set the Label to be **WindowsScanUser**.
6. Provide an ordering value for this credential. This is a relative value (i.e., sequence one (1) credentials will be used before sequence two (2) credentials, and so on).
7. Set the connection type to **Windows WMI**, **Windows Remote Process**, **Windows File Share**, and **Windows Remote Registry**.
8. Type the WindowsScanUser username value; this user will be used to remotely access the target devices. This can be a user specially created for the scanning process or an existing login (remember to include a domain if this is a domain account). For example, DEMODOMAIN\demouser; a local windows account should use '.' as a domain value (e.g., '.\demouser).
9. Type the WindowsScanUser user password value; this value will be encrypted for later use and will not be stored in cleartext.
10. Click the **Save & Close** button.
11. Check that the new credential is now associated with the location.



Basic estate - Application credentials

Application Credentials are credentials that are used to provide access to an application such as Oracle, SQL Server, DB2, or vSphere.

> **Note:** The ability to scan these applications is dependent on the availability of third-party client libraries. These third-party libraries must be either automatically or manually installed (see the **Scan Engine Prerequisites Guide** for further discussion).

These types of credentials are equivalent to a real user trying to access a remote application from the scanning server.

> **Note:** The number of lockout attempts set in the Connections option will control how many times the credential will be attempted.
>
> Note that if the credential has an invalid password, a large number of configured lockout attempts may cause that user to be blocked.
>
> Make sure of your environmental authentication settings before modifying the option.
>
> Non-instance-based connections (i.e., Device Connections or vCenter), will be attempted up to the number of lockout attempts set in the Connections option.
>
> If the configured number of attempts fail, this credential will go into cooldown.

Follow this process to create a set of credentials that will be used as part of the scanning process:

Oracle scan credential

1. Select the **Credentials** tab.
2. Click the **Create** button to add a credential.
3. View the Create a Credential dialog that is opened.
4. Set the Credential Type to **Oracle Database**.
5. See the Connection Type set to **Oracle Database**.
6. Set the Label to **OracleScanUser**.
7. Provide a sequence value for this credential. This is a relative value (i.e., sequence one (1) credentials will be used before sequence two (2) credentials, and so on).
8. Type the OracleScanUser username value; this user will be used to remotely access the target Oracle application. This can be a user specially created for the scanning process or an existing user (e.g., IQOuser).
9. Type the OracleScanUser user password value; this value will be encrypted for later use and will not be stored in cleartext.
10. Click the **Save & Close** button.
11. Check that the new credential is now associated with the location.

SQL scan credential

1. Select the **Credentials** tab.
2. Click the **Create** button to add a credential.
3. View the Create a Credential dialog that is opened.
4. Set the Credential Type to **MS SQL Server**.
5. See the Connection Type set to **MS SQL server**.

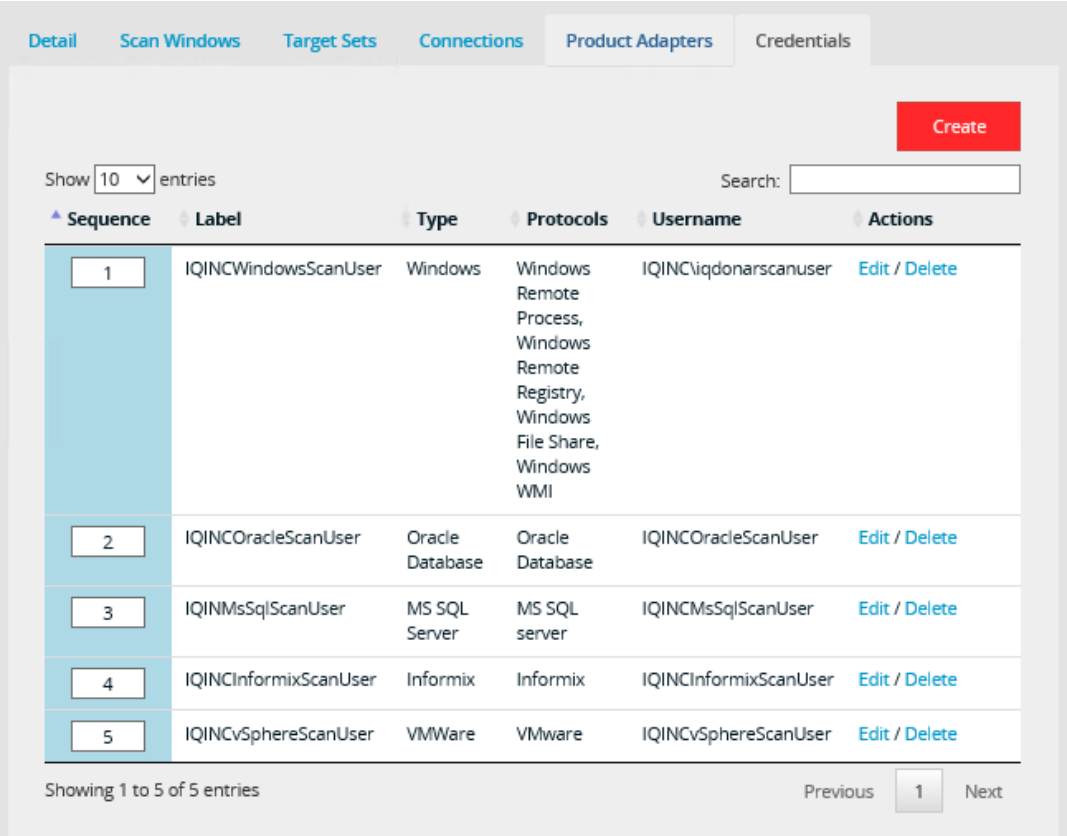
6. Set the Label to **MsSqlScanUser**
7. Provide a sequence value for this credential. This is a relative value (i.e., sequence one (1) credentials will be used before sequence two (2) credentials, and so on).
8. Type the MsSqlScanUser username value; this user will be used to remotely access the target Oracle application. This can be a user specially created for the scanning process or an existing user (e.g., IQSuser).
9. Type the MsSqlScanUser user password value; this value will be encrypted for later use and will not be stored in cleartext.
10. Click the **Save & Close** button.
11. Check that the new credential is now associated with the location.

Informix scan credential

1. Select the **Credentials** tab.
2. Click the **Create** button to add a credential.
3. View the Create a Credential dialog that is opened.
4. Set the Credential Type to **Informix**.
5. Set the Connection Type set to **Informix**.
6. Set the Label to **InformixScanUser**.
7. Provide a sequence value for this credential. This is a relative value (i.e., sequence one (1) credentials will be used before sequence two (2) credentials, and so on).
8. Type the InformixScanUser username value; this user will be used to remotely access the target Oracle application. This can be a user specially created for the scanning process or an existing user (e.g., IQSuser).
9. Type the InformixScanUser user password value; this value will be encrypted for later use and will not be stored in cleartext.
10. Click the **Save & Close** button.
11. Check that the new credential is now associated with the location.

vSphere scan credential

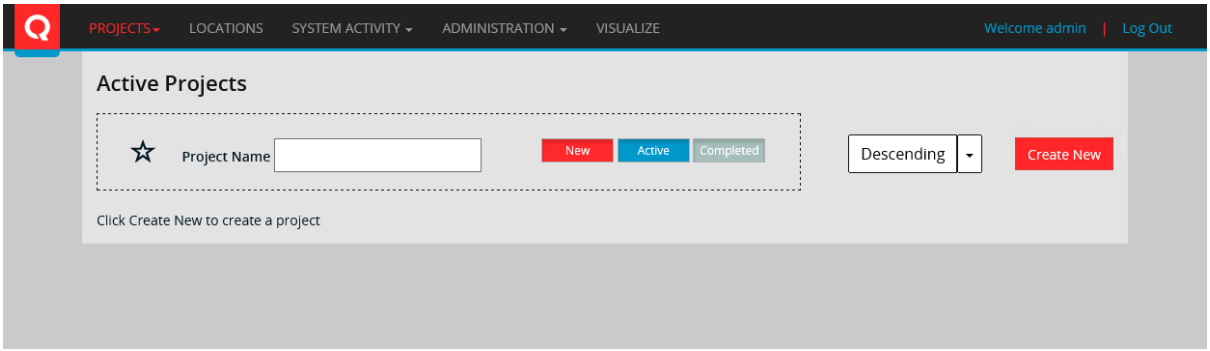
1. Select the **Credentials** tab.
2. Click the **Create** button to add a credential.
3. View the Create a Credential dialog that is opened.
4. See the Credential Type to **VMware**.
5. Set the Connection Type set to **VMware**.
6. Set the Label to **vSphereScanUser**.
7. Provide a sequence value for this credential. This is a relative value (i.e., sequence one (1) credentials will be used before sequence two (2) credentials, and so on).
8. Type the vSphereScanUser username value; this user will be used to remotely access the target Oracle application. This can be a user specially created for the scanning process or an existing user (e.g., IQSuser).
9. Type the vSphereScanUser user password value; this value will be encrypted for later use and will not be stored in cleartext.
10. Click the **Save & Close** button.
11. Check that the new credential is now associated with the location.



Basic estate - Project

A default location is provided with the standard installation. You can use this default location to encompass all of the proposed estate. Follow the instructions below:

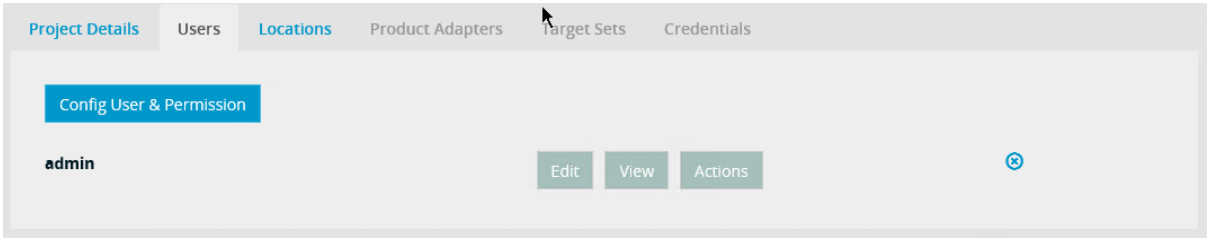
1. Select the **Projects** icon or click the **Projects** drop-down menu in the dashboard. This displays the current available projects. By default, no projects are defined.
2. Select the **Active Projects** menu.



3. Click the **Create New** button to add a project.
4. View the Create Project dialog that is opened.
5. Set the Name to **BasicEstate**.
6. Set the Description to **How to scan a basic Estate**.
7. Set the Start Time to the current time.
8. Click the **Next** button.

Users tab

1. Click the **Config User & Permission** button.
2. Select the admin user to be included in this project. A user that is associated with a project is used in combination with user permissions to govern the actions that can be carried out by the user. The admin user has full permissions to access all aspects of a project.
3. Click the **Next** button.



Locations tab

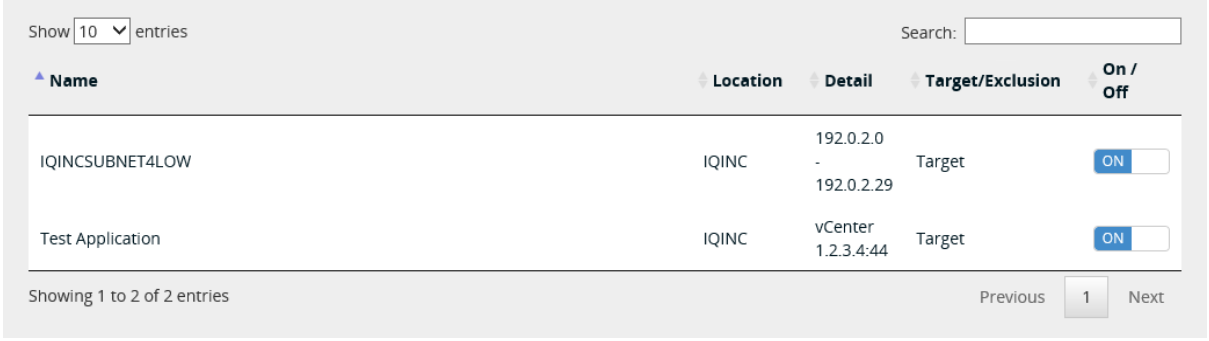
1. Select the only location available.
2. Click the **Next** button.

Product Adapters tab

1. Leave all the product adapters enabled.
2. Click the **Next** button.

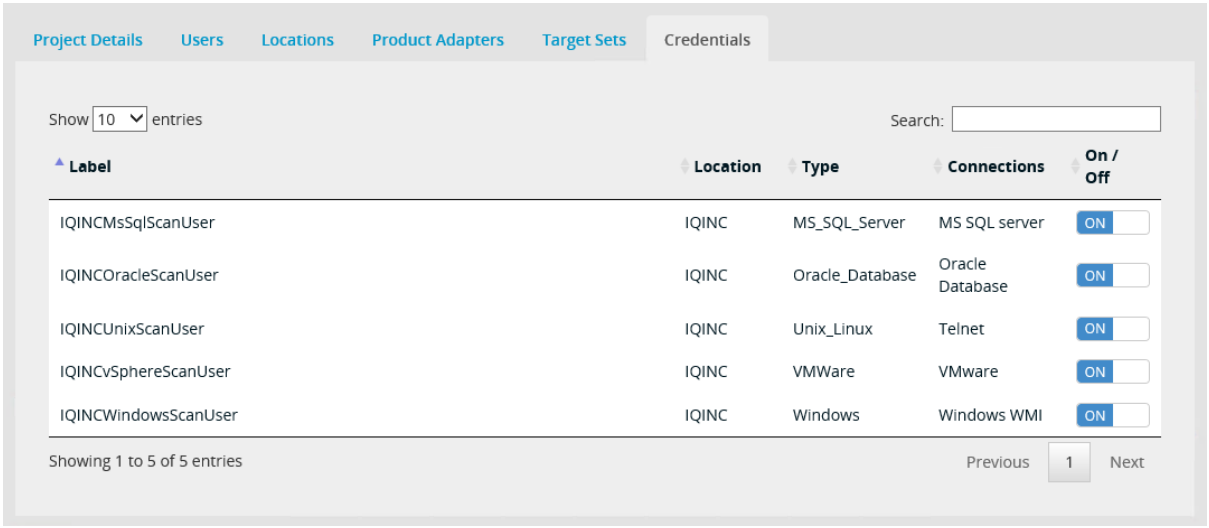
IP Ranges tab

1. Ensure that the SUBNET4LOW IP Range is set to **On**.
2. Click the **Next** button.

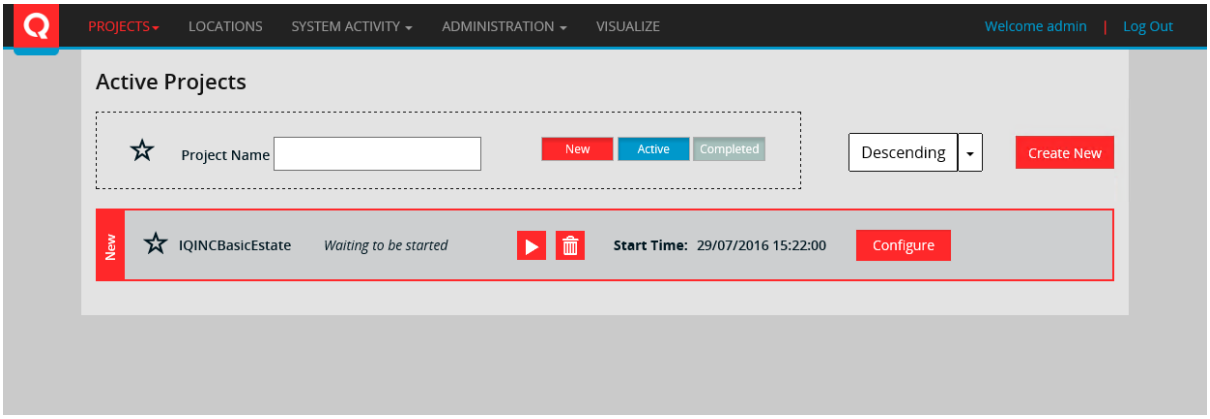


Credentials tab

1. Ensure that all credentials are set to **On**.



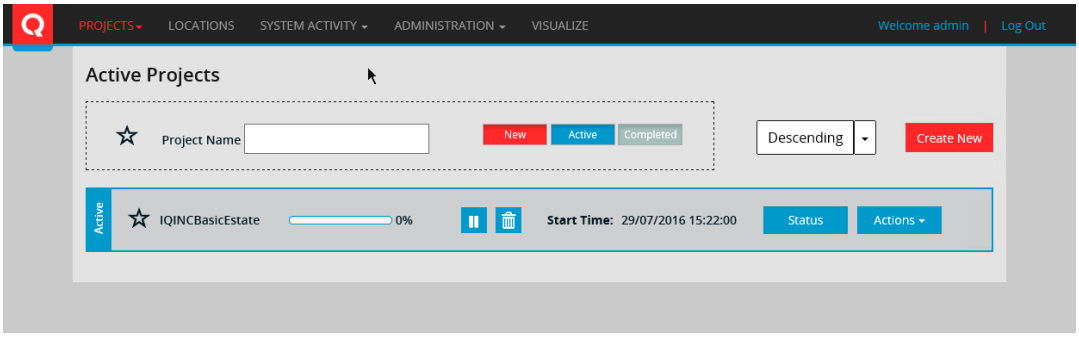
2. Click the **Create** button.
3. Ensure that the new project is present in the Projects list.



Basic estate - Start scan

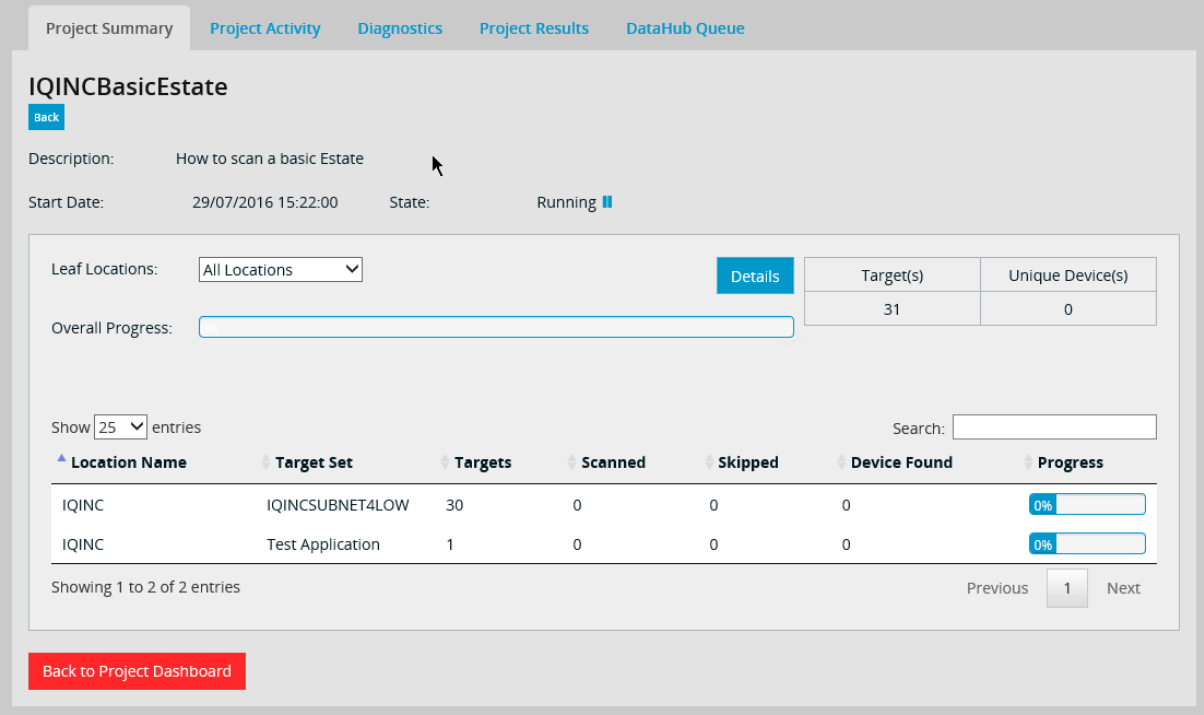
The final step of this process is to initiate a project scan. Projects are initiated from the Active Project tab.

1. Select the **Projects** icon or click the **Projects** drop-down menu.
2. Select the **Active Projects** tab.
3. Identify the **BasicEstate** project.
4. Click the **Run** button to initiate the scan operation.
5. Watch the progress bar to identify ongoing scan operations. Let the project run to completion.



Basic estate - Status

Additional information about the status of the scanning process is available by clicking the **Status** button.

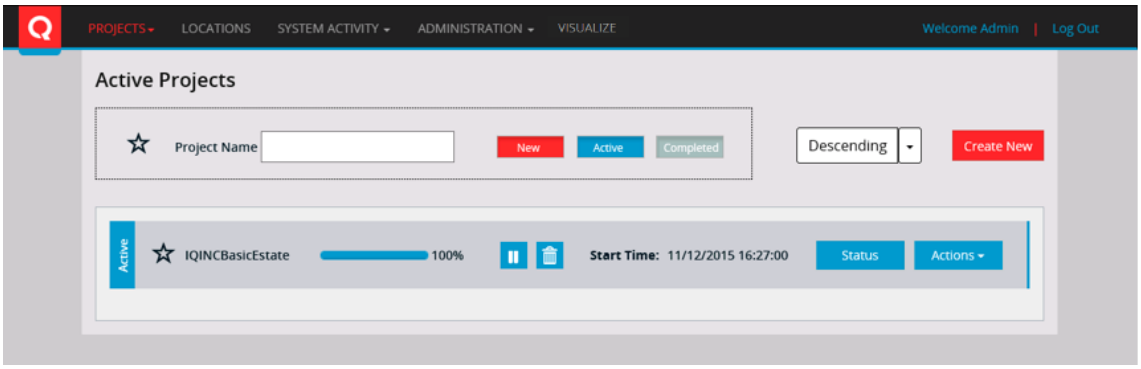


Refer to the **Project scan analysis** section for details about how to examine and diagnose the scanning operations.

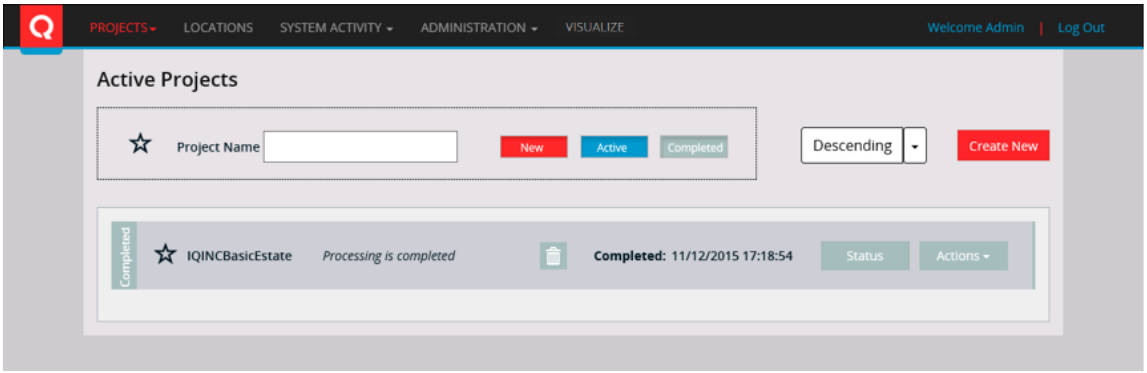
Basic estate - Mark scan as complete

The decision to mark a project complete is one not taken by the scanning software. It's a decision determined by the administrator that needs to take into account the scan coverage of the identified estate (including the discovery of any unexpected devices/applications), any requirement to add additional scan targets, successful access to all target devices (credential coverage), and the need for rescan operations. It's typically not the case that 100% coverage on the UI is the only criterion for marking a project complete.

1. Select the **Projects** icon or click the **Projects** drop-down menu.
2. Select the **Active Projects** tab.
3. Identify the **BasicEstate** project.
4. Let the project run until it is 100% complete.



5. Click the **Status** button to identify that all elements have been sufficiently collected.
6. Click the **Actions** drop-down menu and select **Complete**.
7. Identify that the project is now in the completed state and that the project color has changed.



Additional information about the status of the scanning process is available by clicking the **Status** button.

Basic estate - Mark scan as archived

Once the scan project is no longer required, it can be archived.

1. Click the **Actions** drop-down menu and select **Archive**.
2. Archive the project once the scan is no longer required.

Archived projects are available under the **Projects > Archived Projects** tab.

Use case 2 - Multi-departmental estate

A **multi-departmental estate** is composed of multiple locations and/or a disjoint network infrastructure. Responsibility for the network/infrastructure resides with a single user or single group, with the additional complexity that locations are typically geographically disjointed and are also split into production and test sub-areas. Projects to execute scans are assigned as a local responsibility. However, responsibility for the infrastructure remains with the global admin group.

The scan results may be segmented into different overall projects (e.g. Oracle project results, SQL Server project results, etc.) depending on the customer use case.

Multi-departmental estate – Personnel expectations

Given the extended complexity of this coverage, it's expected that a single administrator and scan owner will not be sufficient.

Summary

The ability to segment into different overall projects (e.g. Oracle project results, SQL Server project results, etc.) is required for this use case. It's assumed that the following areas of concern must be supported:

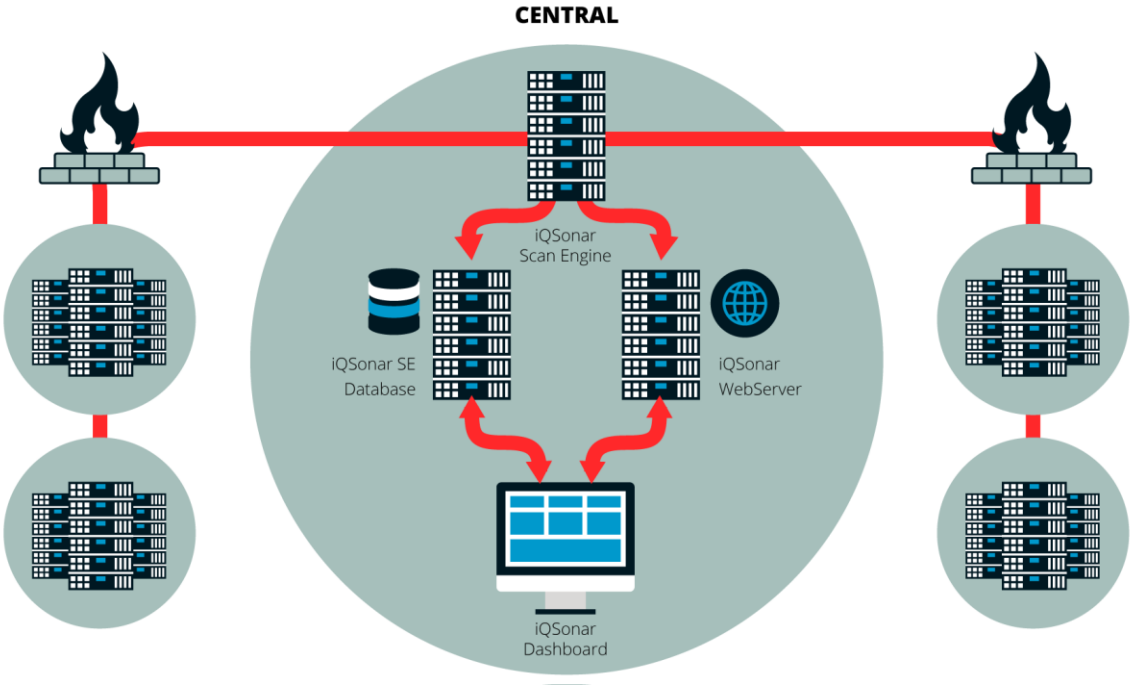
- **Global Infrastructure**: Identification and control of infrastructure globally. This "user" is responsible for the description of the infrastructure to be scanned, which includes IP address ranges, IP address range exclusions, Scan Windows and Connection types to be used.
- **Global Project Manager:** This "user" is responsible for global identification and control of project(s).
- **EMEA Manager:** This "user" is responsible for tracking and executing EMEA projects.
- **Americas Manager**: This "user" is responsible for tracking and executing an Americas project.

To support the project as described, the following items are required:

- **2 projects:** Americas Project, EMEA Project
- **4 users:** Admin, Project.Manager, America.User, EMEA.User
- **3 roles:** Administrator, Project Manager, Project Viewer
- **1 scan engine**

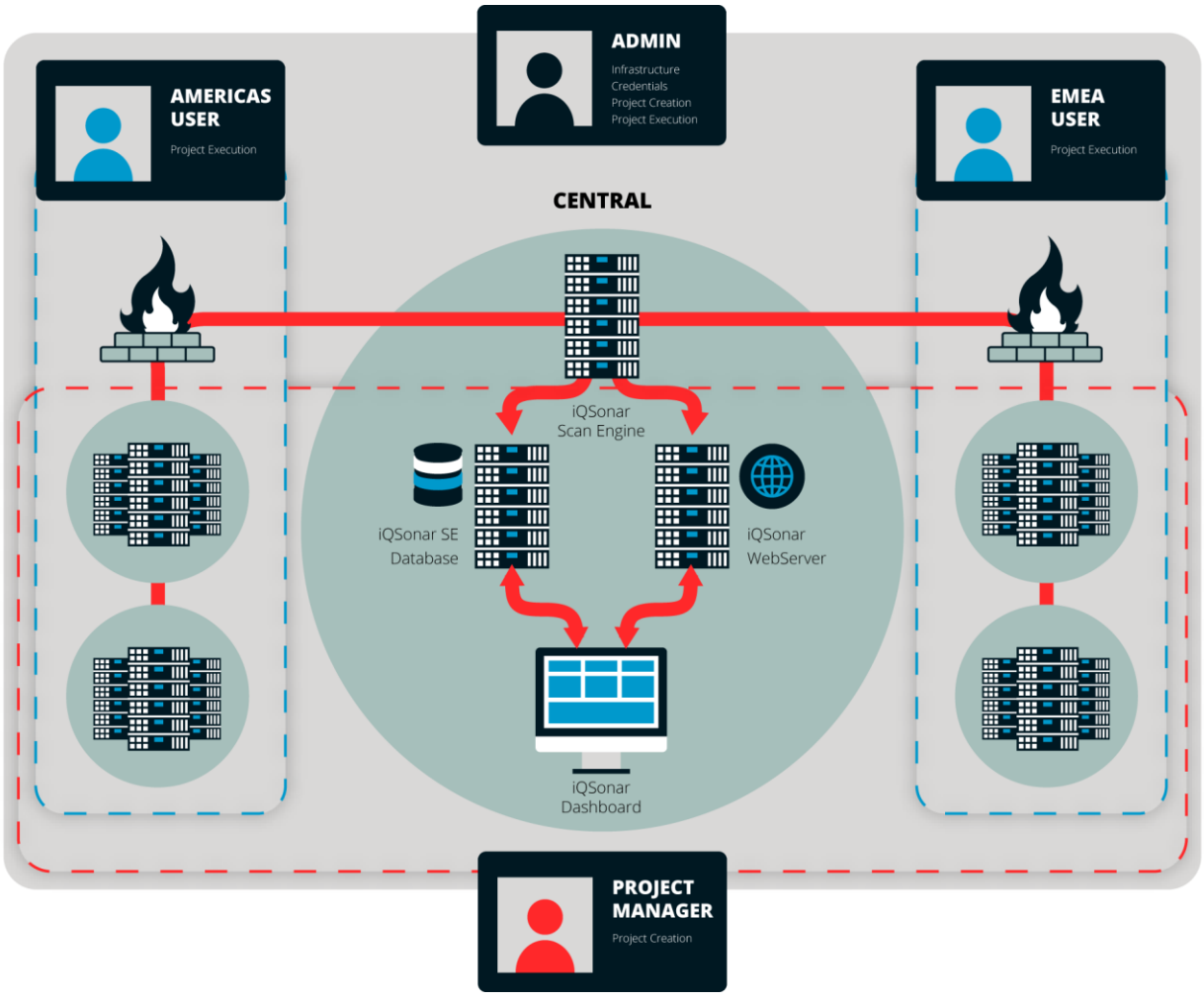
Multi-departmental estate – Network infrastructure

This network is composed of a relatively open network with no major restrictions in terms of firewalls, network latency, or bandwidth. The network structure is geographically dispersed into the Americas and EMEA. Each of these locations has a production and test set of devices.



Multi-departmental estate – Responsibility & ownership

The areas of responsibility for the four users are identified in the diagram below.

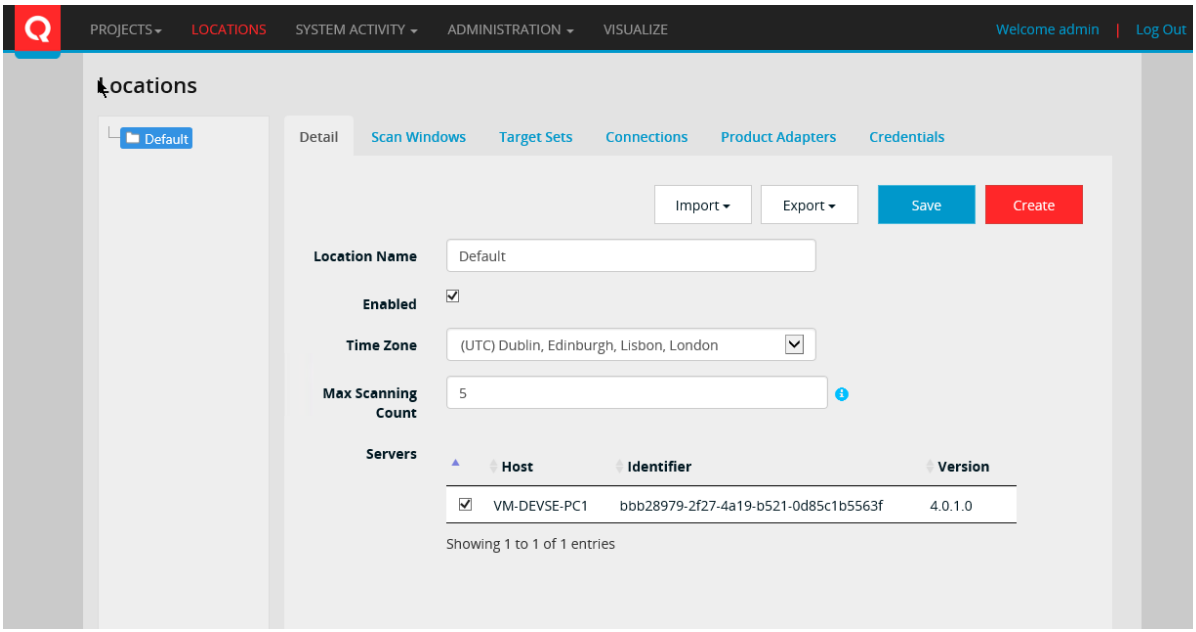


Multi-departmental estate – Top-level location

Login: Admin

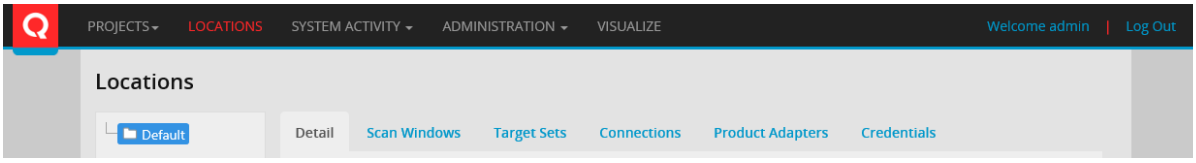
A default location is provided with the standard install. This default location can be used to encompass all of the proposed estate. Follow the instructions below:

Select the **Locations** icon or **Locations** drop-down menu in the dashboard. This displays the current available locations. By default, a single location called **default** is available as a root item (if it hasn't been modified in a previous session). This is the top-level grouping and cannot be deleted.



However, it is recommended that you rename it to a customer/project appropriate value.

1. Enter the details of a new default location.
2. Enter the Time Zone of this locality.
3. Ensure that **Enabled** is selected.
4. Enter the Max Scanning Count of **5** (how many concurrent jobs that can be run for targets in this location).
5. Select the scan engine's association with this locality.
6. Save your details by clicking the **Save** button.



This single location will **not** be sufficient for a multi-department project. You'll need more granular control over the elements of the estate that need to be scanned.

Multi-departmental estate – Country-level location

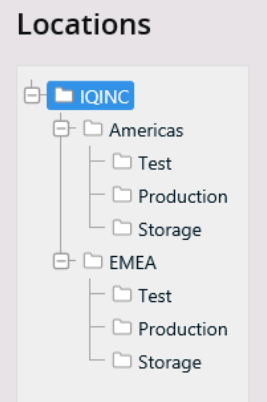
Login: Admin

The medium-size company is split into two regional (scan) locations. Each region can be allowed to run its own scan projects (e.g., an Oracle audit may be done on a regional level at different times). Each location is also sub-divided into production and test devices and storage infrastructure as described below:

- Americas
  - Test
  - Production
  - Storage
- EMEA
  - Test
  - Production
  - Storage

You need to add these new locations:

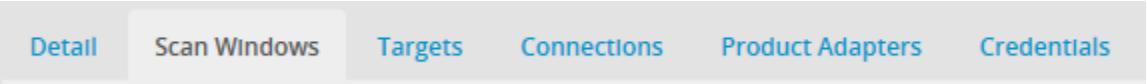
1. Select the **Locations** icon or **Locations** drop-down menu in the dashboard.
2. Select the top-level location.
3. Click the **Create** button to add a sub-location to the root location.



4. Provide the new Location Name **Americas**.
5. Select a suitable Time Zone for the location.
6. Click the **Create** button.
7. Select the top-level Location.
8. Repeat steps 3-6 and create a location called **EMEA** under the root location.
9. Select the **Americas** Location.
10. Repeat steps 3-6 and create three different locations called **Production, Test,** and **Storage** under Americas.
11. Select the **EMEA** Location.
12. Repeat steps 3-6 and create three different locations called **Production, Test,** and **Storage** under EMEA.

Multi-departmental estate – Scan Windows

Login: Admin



Scan Windows provides a means to limit the period when active scanning of an estate is carried out. It's assumed that the Scan Windows isn't required for the multi-departmental estate. This is a feature that would be required for a complex estate.

Multi-departmental estate – Targets

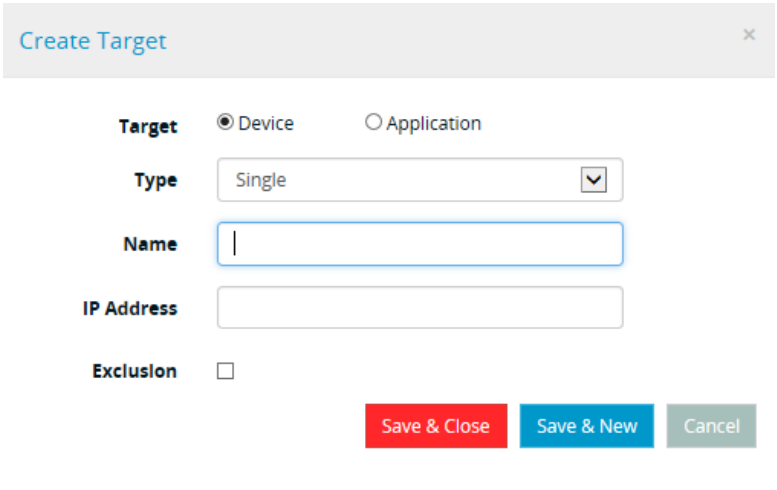
Login: Admin

It's assumed that the EMEA and Americas production and test locations have all been assigned ranges within a single subnet (this is not entirely realistic but is provided as a simple example for demonstration purposes).

Targets are used to identify the scope of scan operations. Scan operations can be targeted against a single IP address, a range of IP addresses, or a complete subnet. The location needs to have associated IP addresses to scan.

Americas-test location

1. Select the top-level location.
2. Select the **Americas** location.
3. Select the **Test** Location.
4. Select the **Targets** tab.
5. Click the **Create** button to add a new target.
6. View the **Create Target** dialog.



7. Set the Type to **Range.**
8. Set the Name to be **USTEST.**
9. Set the Start IP to 192.0.2.0.

10. Set the End IP to 192.0.2.29.
11. Clear the **Exclusion** option.
12. Click the **OK** button.
13. Check that the new range is now associated with the location.

EMEA-test location

1. Select the top-level location.
2. Select the **EMEA** location.
3. Select the **Test** Location.
4. Select the **Targets** tab.
5. Click the **Create** button to add a new target.
6. Set the Type to **Range.**
7. Set the Name to be **EMEATEST.**
8. Set the Start IP to be 192.0.2.30.
9. Set the End IP to be 192.0.2.49.
10. Clear the **Exclusion** option.
11. Click the **OK** button.

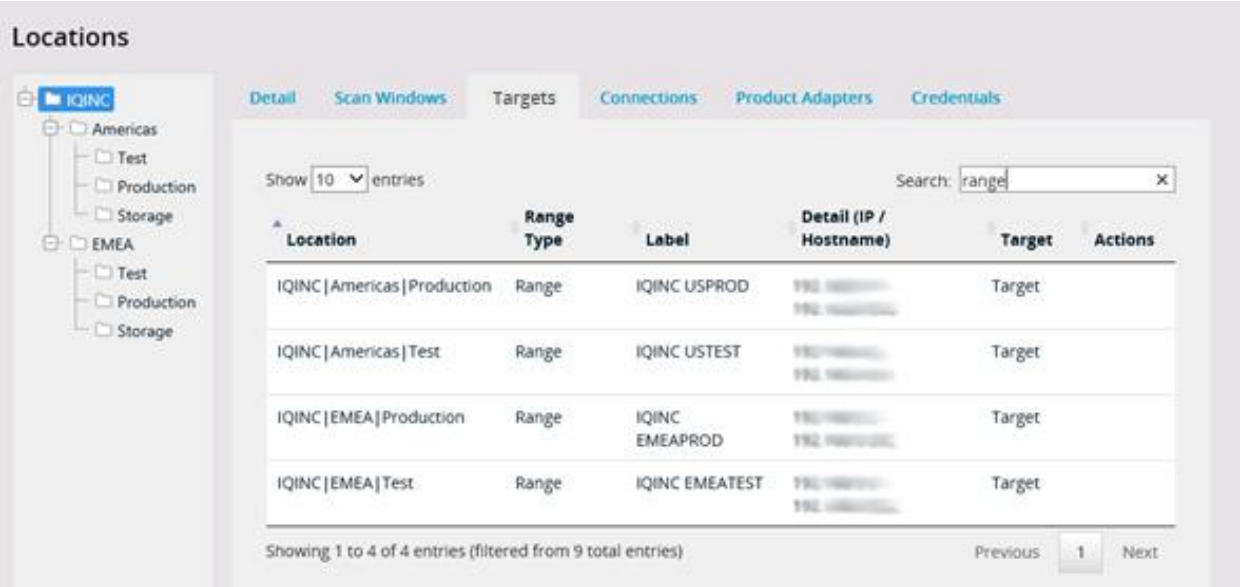
Americas-production location

1. Select the top-level location.
2. Select the **Americas** location.
3. Select the **Production** location.
4. Select the **IP Ranges** tab.
5. Click the **Create** button to add a new target.
6. Set the Type to **Range.**
7. Set the Name to be **USPROD.**
8. Set the Start IP to 192.0.2.50.
9. Set the End IP to 192.0.2.79.
10. Clear the **Exclusion** option.
11. Click the **OK** button.

EMEA-production location

1. Select the top-level location.
2. Select the **EMEA** location.
3. Select the **Production** location.
4. Select the **Targets** tab.
5. Click the **Create** button to add a new target.
6. Set the IP Range Type to **Range.**
7. Set the Name to be **EMEAPROD.**
8. Set the Start IP to 192.0.2.80.
9. Set the End IP to 192.0.2.109.
10. Clear the **Exclusion** option.
11. Click the **OK** button.

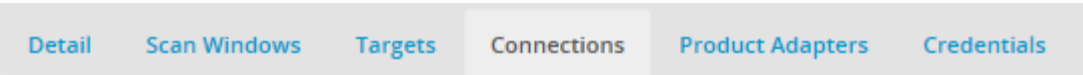
> **Note:** Click in the various locations and identify the targets that are associated with the location. The top-level location will show the accumulation of all targets that have been specified.



> **Note: No Location** covers the additional IP addresses 192.0.2.110-192.0.2.254. This means that they're not considered to be targets for the scan operation. These values cover the storage targets but have not been assigned.

Multi-departmental estate – Connections

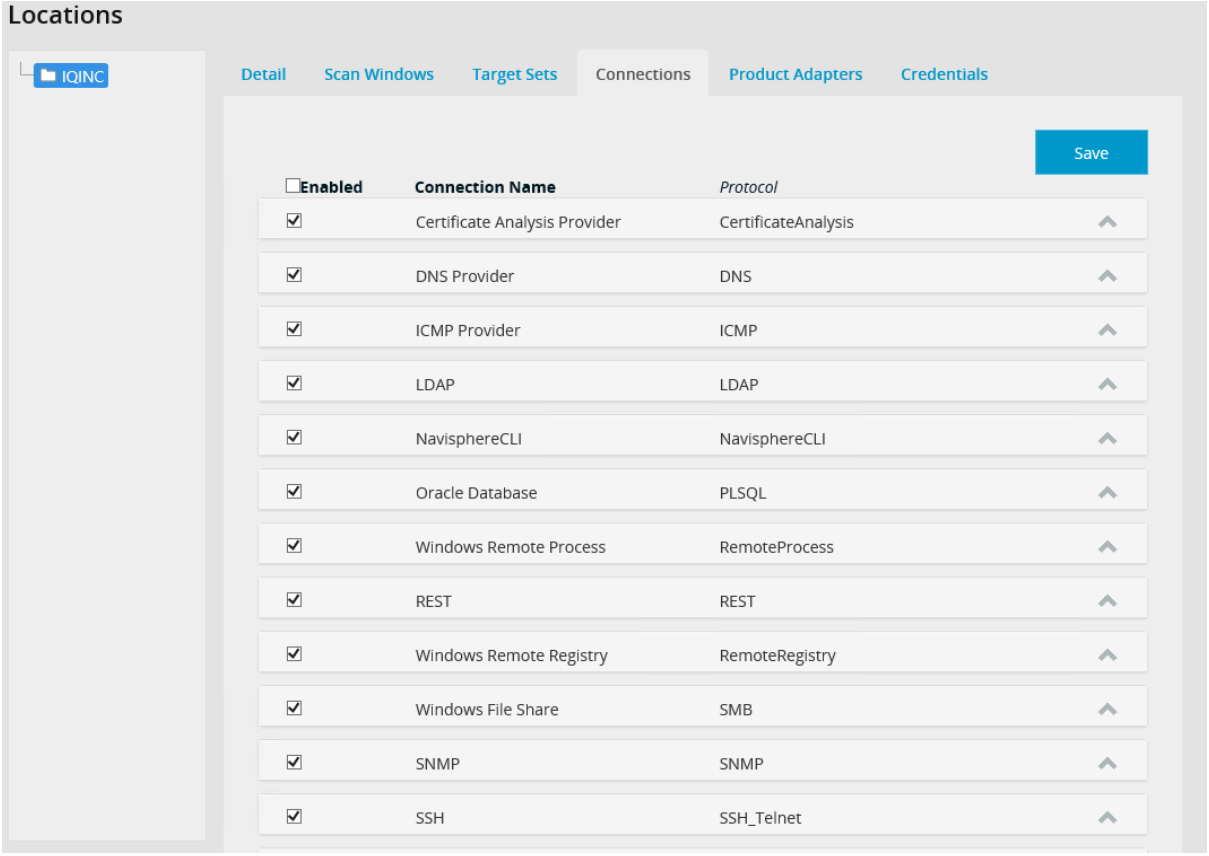
Login: Admin



Connections are the means by which information retrieval is achieved by the scan engine. Each connection type is associated with one or more configuration items (such as connection time, command time out, etc.)

A connection type is a logical communication path to a target device or application. Underlying this connection is one or more physical protocols established between the scan engine and the target device that are used to execute commands that retrieve data.

1. Enable all connection types.
2. Click the **Update** button.
3. Click the **Items** icon on any row to show associated configuration items.

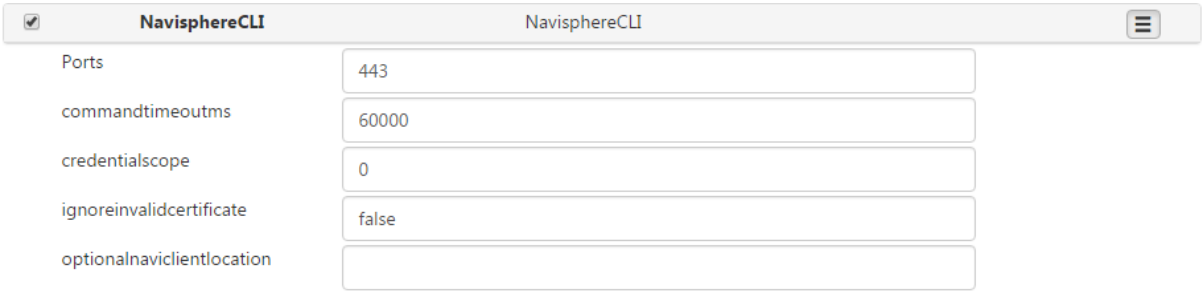


Multi-departmental estate – NavisphereCLI connection

The connection type **NavisphereCLI** is used by the storage product adapter to retrieve storage information from EMC-based devices. This product adapter is still in BETA release and subject to change.

The connection is based on the installation of the NavisphereCLI software as specified in the **Scan Engine Prerequisites Guide**. This connection uses the third-party API to connect to and retrieve information from the remote storage device. There are specific elements of the configuration that you need to address here to allow the retrieval of this information.

Click the NavisphereCLI expand button to expand the options. The settings provided here must match those that were specified during the installation of the NavisphereCLI package.



Port: This is a secure port used to establish the SSL connection to the remote storage device. You only need to modify this if another port is being used.

Command Time Out: This time out value does not need to be modified.

Credential Scope: Credentials for NavisphereCLI software can be created globally or locally for storage. If global credentials are to be used, then set the credential scope value to **0**; if local credentials are used then set this value to **1.**

Ignore Invalid Certificate: The security associated with the NavisphereCLI client can be installed with either medium or high security settings. SSL interaction requires the exchange of certificate information and a high security setting will ensure that certificate validation must pass. This option downgrades this requirement to the medium level and allows certificate checking to be ignored.

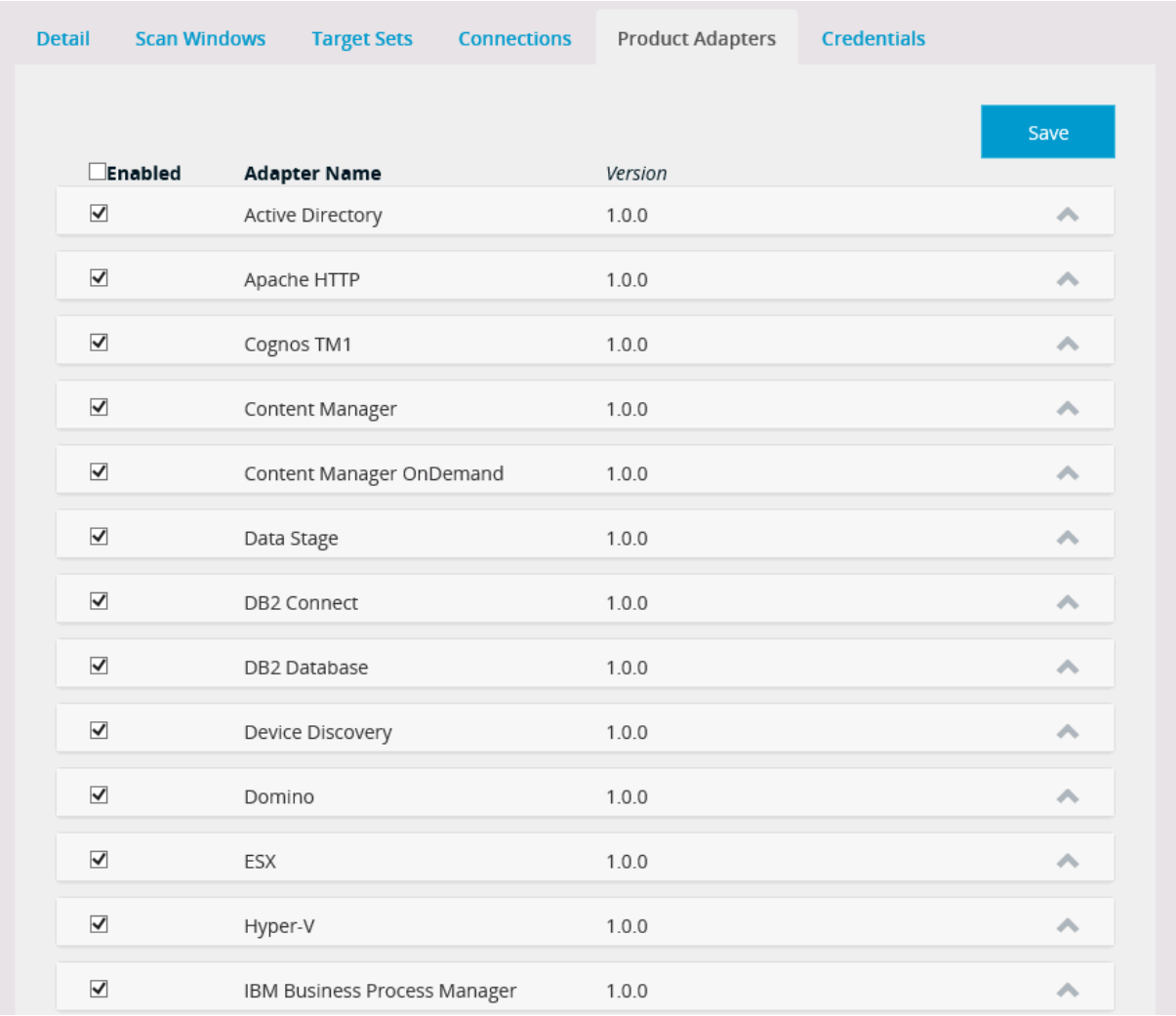
Optional NaviClient Location: The location of the NavisphereCLI software is typically located through the use of the Windows registry. If a non-standard installation of the NavisphereCLI software was carried out, you can specify the location of the software installation directory using this option.

Multi-departmental estate – Product adapters

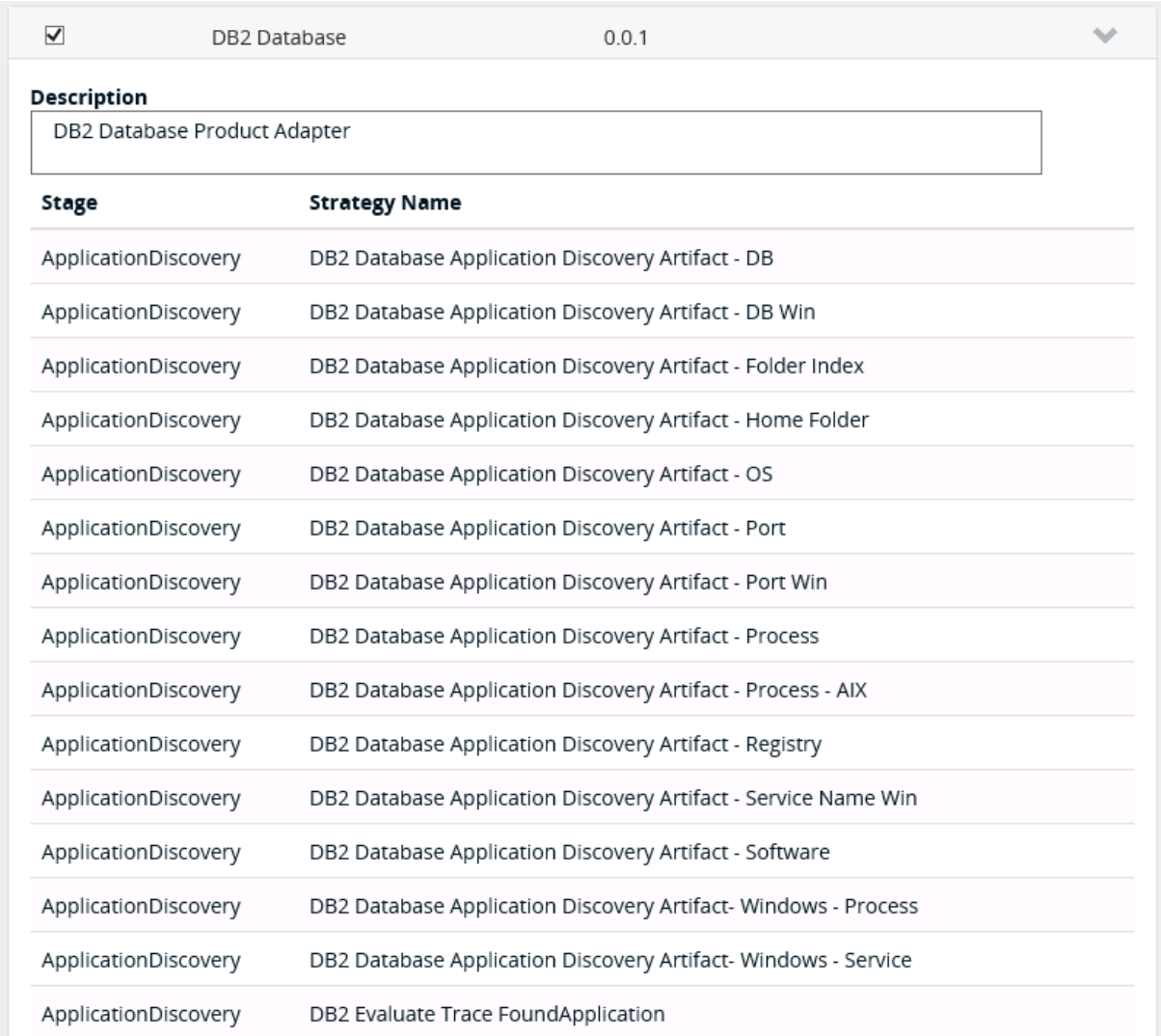
Login: Admin

The scan engine was built to cover a wide range of discovery and is not exclusively tailored to any specific product. It was built to allow enterprise customers to gather the data they need from the multitude of devices and applications on their network.

The scan engine Product Adapter functionality means that additional protocols, commands, and “transformation of scanned data” can easily be added to the scan engine’s core platform, which offers excellent security, credential management, data lineage, change history, user interfaces, and export APIs. The Product Adapter dialog below identifies the currently enabled product adapters:



The expand button enables you to further expand elements of the product adapter, exposing the individual strategies that you can then enable or disable. Clicking the expand button again collapses the expanded product adapter. Save any changes using the **Update** button.



To disable individual strategies, access the scan engine's configuration file:

1. Navigate to the bin folder in the install directory. (Typically C:\Program Files\iQuate\iQSonar ScanEngine 4.0).
2. Open the iQuate.iQSonar.ScanEngine.exe.config file.
3. Locate the line beginning **<add key="DisabledStrategies".**
4. Modify the value property to contain a list of strategies to be disabled. The value must be a comma-separated list with each entry taking the form <ProductAdapterName>:<StrategyName>. For example, to disable the DB2 Evaluate Trace Found Application Strategy in the DB2 Database product adapter, the value DB2 Database:DB2 Evaluate Trace Found Application Strategy should be added to the DisabledStrategies list.

Multi-departmental estate – System credentials

Login: Admin

System credentials are used to provide access to an operating system (such as Windows or *NIX) or an operating system component (such DNS, WMI, DNS, Remote Registry).

These types of credentials are equivalent to a real user trying to access a remote system from the scan-engine device.

Because the credentials are closely tied to the infrastructure, it's assumed that they're handled by the administration role that also handles the targets and location information.

For the purposes of scanning, it's possible that an administrator will create an estate-wide set of credentials to be used exclusively for scanning operations. Alternatively, existing credentials can be used. A final alternative is to provide a mixture of these two approaches.

The second approach will be used for the multi-departmental estate with company-wide OS credentials provided at the top-level location and specific credentials provided at lower levels.

Multi-departmental estate – Global system credential

System credentials are used to provide access to an operating system (such as Windows or *NIX) or an operating system component (such DNS, WMI, DNS, Remote Registry).

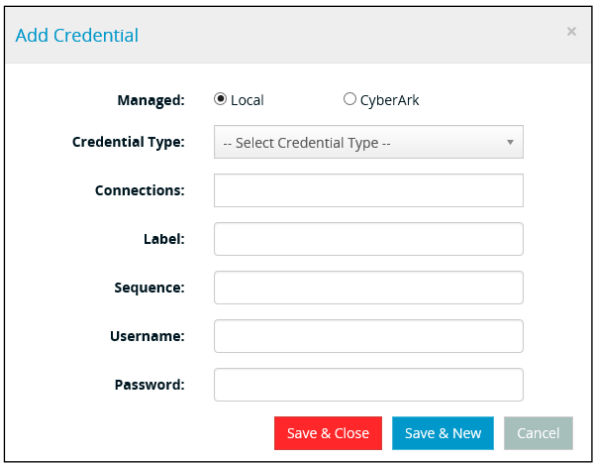
You can manage credentials locally in the underlying Data Center Discovery scan engine database or retrieve them from a configured CyberArk installation. The default setting when creating a credential is **Local** – this indicates the credential is managed by the scan engine. To create a CyberArk credential, select the **CyberArk** option from the **Managed** radio buttons.

Also configure the following additional fields:

- **Safe:** The safe within the **CyberArk** vault where the **Credential** is stored. This field is optional; however, it should be noted that where no value is provided, the **CyberArk** integration component will return the first matching credential.
- **Folder**: The folder within the **Safe** where the **Credential** resides. This field is optional; however, it should be noted that where no value is provided, the **CyberArk** integration component will return the first matching credential.
- **Account name**: The name of the credential.

These types of credentials are equivalent to a real user trying to access a remote system from the scan engine device.

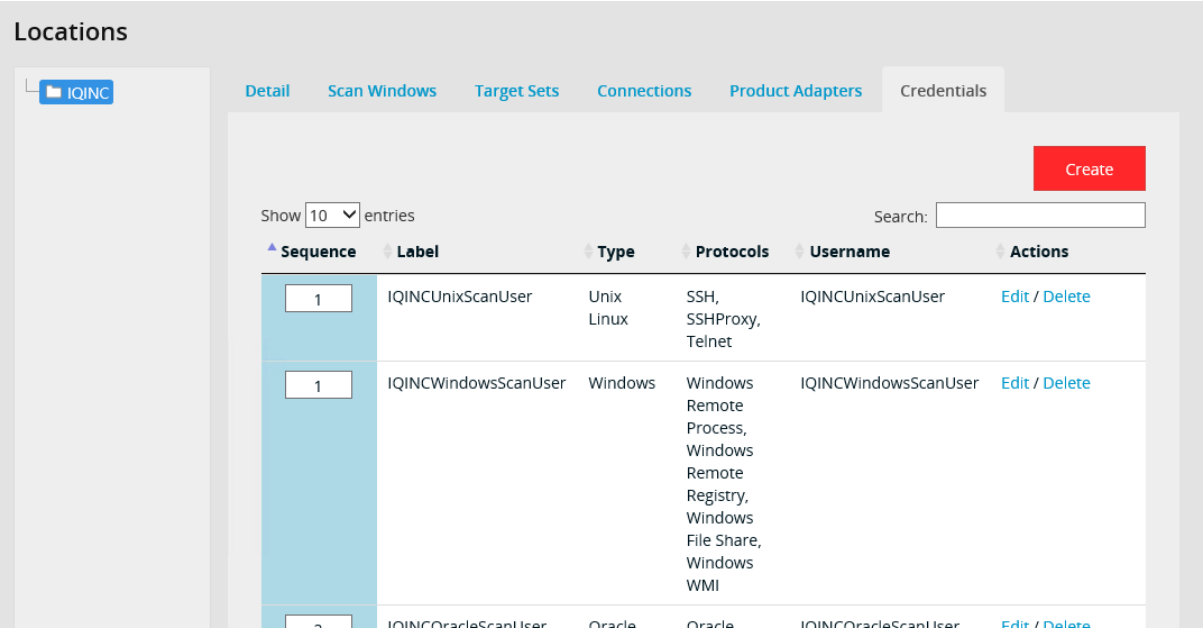
14. Select the top-level location.
15. Select the **Credentials** tab.
16. Click the **Create** button to add a credential.
17. The default Managed setting is **Local** – this indicates that the credential is managed by the scan engine.



18. Set the Credential Type to **UNIX Linux**.
19. Set the Name to be **UnixScan**.
20. Set the connection types to **SSH**, **SSHProxy**, and **Telnet**.
21. Type the label for this credential (e.g., UnixScanUser).
22. Provide an ordering value for this credential. This is a relative value (i.e., sequence one (1) credentials will be used before sequence two (2) credentials, and so on).
23. Type the UnixScanUser username value; this user will be used to remotely access the target devices. This can be a user specially created for the scanning process or an existing login.
24. Type the UnixScanUser user password value; this value will be encrypted for later use and will not be stored in cleartext.
25. Click the **Save & Close** button.
26. Check that the new credential is now associated with the location.

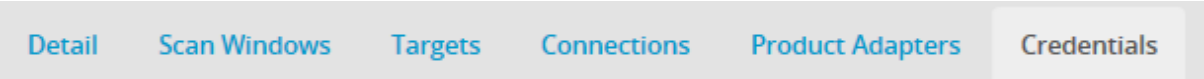
Repeat the process to add a **Windows** account credential:

1. Select the **Credentials** tab.
2. Click the **Create** button to add a credential.
3. View the Create a Credential dialog that is opened.
4. Set the Credential Type to **Windows**.
5. Set the Label to be **WindowsScanUser**.
6. Provide an ordering value for this credential. This is a relative value (i.e., sequence one (1) credentials will be used before sequence two (2) credentials, and so on).
7. Set the connection type to **Windows WMI**, **Windows Remote Process**, **Windows File Share**, and **Windows Remote Registry**.
8. Type the WindowsScanUser username value; this user will be used to remotely access the target devices. This can be a user specially created for the scanning process or an existing login (remember to include a domain if this is a domain account). For example, DEMODOMAIN\demouser; a local windows account should use '.' as a domain value (e.g., '.\demouser).
9. Type the WindowsScanUser user password value; this value will be encrypted for later use and will not be stored in cleartext.
10. Click the **Save & Close** button.
11. Check that the new credential is now associated with the location.



Multi-departmental estate – Application credentials

Login: Admin



Application credentials are used to provide access to an application such as Oracle, SQL Server, DB2, or vSphere. It's assumed that EMEA and Americas use application-specific credentials that are not shared.

These types of credentials are equivalent to a real user trying to access a remote application from the scanning server. Follow this section to set up four application accounts for each location (Americas and EMEA):

- Oracle Admin
- SQL Server Admin
- vSphere Admin
- Informix Admin

Multi-departmental estate – Americas application credentials

Login: Admin

This sequence establishes application credentials for the Americas location. Application credentials are used to provide access to an application such as Oracle, SQL Server, Informix, or vSphere.

> **Note:** The ability to scan these applications is dependent on the availability of third-party client libraries. These third-party libraries must be either automatically or manually installed (see the **Scan Engine Prerequisites Guide** for further discussion).

These types of credentials are equivalent to a real user trying to access a remote application from the scan engine device.

In this section, set up four application accounts:

- Oracle Admin
- SQL Server Admin
- Informix Admin
- vSphere Admin

Americas Oracle scan credential

1. Select the **Americas** location.
2. Select the **Credentials** tab.
3. Click the **Create** button to add a credential.
4. View the Create a Credential dialog that is opened.
5. Set the Credential Type to **Oracle Database**.
6. See the Connection type set to **Oracle Database**.
7. Set the Label to be **USOracleScanUser**.
8. Provide a sequence value for this credential. This is a relative value (i.e., sequence one (1) credentials will be used before sequence two (2) credentials, and so on).
9. Type USOracleScanUser username value; this user will be used to remotely access the target Oracle application. This can be a user that has been specially created for the scanning process or an existing user e.g. IQOuser.
10. Type the USOracleScanUser user password value; this value will be encrypted for later use and will not be stored in cleartext.
11. Click the **Save & Close** button.
12. Check that the new credential is now associated with the location.

Americas SQL scan credential

1. Select the **Americas** location.
2. Select the **Credentials** tab.
3. Click the **Create** button to add a credential.
4. View the Create a Credential dialog that is opened.
5. Set the Credential Type to **MS SQL Server.**
6. See the Connection type set to **MS SQL server**.
7. Set the Label to be **USMsSqlScanUser**.
8. Provide a sequence value for this credential. This is a relative value (i.e., sequence one (1) credentials will be used before sequence two (2) credentials, and so on).
9. Type USMsSqlScanUser username value; this user will be used to remotely access the target Oracle application. This can be a user that has been specially created for the scanning process or an existing user e.g. IQSuser.
10. Type the USMsSqlScanUser user password value; this value will be encrypted for later use and will not be stored in cleartext.
11. Click the **Save & Close** button.
12. Check that the new credential is now associated with the location.

Americas Informix scan credential

1. Select the **Americas** location.
2. Select the **Credentials** tab.
3. Click the **Create** button to add a credential.
4. View the Create a Credential dialog that is opened.
5. Set the Credential Type to **Informix**.
6. Set the Connection type set to **Informix**.

7. Set the Label to be **USInformixScanUser**.
8. Provide a sequence value for this credential. This is a relative value (i.e., sequence one (1) credentials will be used before sequence two (2) credentials, and so on).
9. Type USInformixScanUser username value; this user will be used to remotely access the target Oracle application. This can be a user that has been specially created for the scanning process or an existing user e.g. IQSuser.
10. Type the USInformixScanUser user password value; this value will be encrypted for later use and will not be stored in cleartext.
11. Click the **Save & Close** button.
12. Check that the new credential is now associated with the location.

Americas vSphere scan credential

1. Select the **Americas** location.
2. Select the **Credentials** tab.
3. Click the **Create** button to add a credential.
4. View the Create a Credential dialog that is opened.
5. See the Credential Type to **VMware**.
6. Set the Connection type set to **VMware**.
7. Set the Label to be **USvSphereScanUser**.
8. Provide a sequence value for this credential. This is a relative value (i.e., sequence one (1) credentials will be used before sequence two (2) credentials, and so on).
9. Type USvSphereScanUser username value; this user will be used to remotely access the target Oracle application. This can be a user that has been specially created for the scanning process or an existing user e.g. IQSuser.
10. Type the USvSphereScanUser user password value; this value will be encrypted for later use and will not be stored in cleartext.
11. Click the **Save & Close** button.
12. Check that the new credential is now associated with the location.

Multi-departmental estate – EMEA application credentials

This sequence establishes application credentials for the EMEA location.

Application credentials are used to provide access to an application such as Oracle, SQL Server, DB2, or vSphere.

> **Note:** The ability to scan these applications is dependent on the availability of third-party client libraries. These third-party libraries must be either automatically or manually installed (see the **Scan Engine Prerequisites Guide** for further discussion).

These types of credentials are equivalent to a real user trying to access a remote application from the scan-engine device.

In this section, set up four application accounts:

- Oracle Admin
- SQL Server Admin
- Informix Admin
- vSphere Admin

EMEA Oracle scan credential

1. Select the **EMEA** location.
2. Select the **Credentials** tab.
3. Click the **Create** button to add a credential.
4. View the Create a Credential dialog that is opened.
5. Set the Credential Type to **scan credential**.
6. See the Connection type set to **scan credential**.
7. Set the Label to be **EMEAOracleScanUser**.
8. Provide a sequence value for this credential. This is a relative value (i.e., sequence one (1) credentials will be used before sequence two (2) credentials, and so on).
9. Type EMEAOracleScanUser username value; this user will be used to remotely access the target Oracle application. This can be a user that has been specially created for the scanning process or an existing user e.g. IQOuser.
10. Type the EMEAOracleScanUser user password value; this value will be encrypted for later use and will not be stored in cleartext .
11. Click the **Save & Close** button.
12. Check that the new credential is now associated with the location.

EMEA SQL scan credential

1. Select the **EMEA** location.
2. Select the **Credentials** tab.
3. Click the **Create** button to add a credential.
4. View the Create a Credential dialog that is opened.
5. Set the Credential Type to **MS SQL Server**.
6. See the Connection type set to **MS SQL server**.
7. Set the Label to be **EMEAMsSqlScanUser**.
8. Provide a sequence value for this credential. This is a relative value (i.e., sequence one (1) credentials will be used before sequence two (2) credentials, and so on).
9. Type EMEAMsSqlScanUser username value; this user will be used to remotely access the target Oracle application. This can be a user that has been specially created for the scanning process or an existing user e.g. IQSuser.
10. Type the EMEAMsSqlScanUser user password value; this value will be encrypted for later use and will not be stored in cleartext.
11. Click the **Save & Close** button.
12. Check that the new credential is now associated with the location.

EMEA Informix scan credential

1. Select the **EMEA** location.
2. Select the **Credentials** tab.
3. Click the **Create** button to add a credential.
4. View the Create a Credential dialog that is opened.
5. Set the Credential Type to **Informix**.
6. Set the Connection type set to **Informix**.
7. Set the Label to be **EMEAInformixScanUser**.
8. Provide a sequence value for this credential. This is a relative value (i.e., sequence one (1) credentials will be used before sequence two (2) credentials, and so on).
9. Type EMEAInformixScanUser username value; this user will be used to remotely access the target Oracle application. This can be a user that has been specially created for the scanning process or an existing user e.g. IQIuser.

10. Type the EMEAInformixScanUser user password value; this value will be encrypted for later use and will not be stored in cleartext.
11. Click the **Save & Close** button.
12. Check that the new credential is now associated with the location.

EMEA vSphere scan credential

1. Select the **EMEA** location.
2. Select the **Credentials** tab.
3. Click the **Create** button to add a credential.
4. View the Create a Credential dialog that is opened.
5. See the Credential Type to **VMware**.
6. Set the Connection type set to **VMware**.
7. Set the Label to be **EMEAvSphereScanUser**.
8. Provide a sequence value for this credential. This is a relative value (i.e., sequence one (1) credentials will be used before sequence two (2) credentials, and so on).
9. Type EMEAvSphereScanUser username value; this user will be used to remotely access the target Oracle application. This can be a user that has been specially created for the scanning process or an existing user e.g. IQSuser.
10. Type the EMEAvSphereScanUser user password value; this value will be encrypted for later use and will not be stored in cleartext.
11. Click the **Save & Close** button.
12. Check that the new credential is now associated with the location.

Multi-departmental estate – User roles

Login: Admin

The control of access to projects is now not centralized around a single individual or group; you need to create specific roles and login users to support the distribution of control.

To support the project as described, the following user-related items are required:

- **3 roles:** Administrator, Project Manager, Project Viewer
- **4 users:** Admin, Project.Manager, America.User, EMEA.User

Create roles

Login: Admin

The new roles that need to be added are Project Manager and Project Viewer. The Administrator role already exists by default and doesn't require any specific handling.

Project_Manager role

1. Select the **Administration** icon or click the **Administration** drop-down menu.
2. Select the **User Settings > Manage Role Permission** tab.
3. Click the **Add New** button.
4. Insert **Project_Manager** into the role name.
5. Insert a short description for this role, such as Project Creation and Modification.
6. Select the **Project Dashboard** permission.
7. Select the **Project Admin** permission.
8. Click the **Create** button.

Project_Viewer role

1. Select the **User Settings > Manage Role Permission** tab.
2. Click the **Add New** button.
3. Insert **Project_Viewer** into the role name.
4. Insert a short description for this role, such as Project Viewing Only.
5. Select the **Project Dashboard** permission.
6. Click the **Create** button.

Create users

Login: Admin

You need to add these new users:

- Project.Manager
- America.User
- EMEA.user

The Administrator already exists and does not require any specific handling.

Project.Manager user

1. Select the **Administration** icon or click the **Administration** drop-down menu.
2. Select the **User Settings > Manage User** tab.
3. Click the **Create A New User** button.
4. Clear the **AD user** checkbox; this is not an Active Directory user.
5. Insert **Project.Manager** into the Username field.
6. Insert **Project** in the Firstname field.
7. Insert **Manager** in the Lastname field.
8. Provide an email address for the receipt of emails.
9. Insert a password and confirm the password value.
10. Select the **Project_Manager** permission for this user.
11. Click the **Create** button.

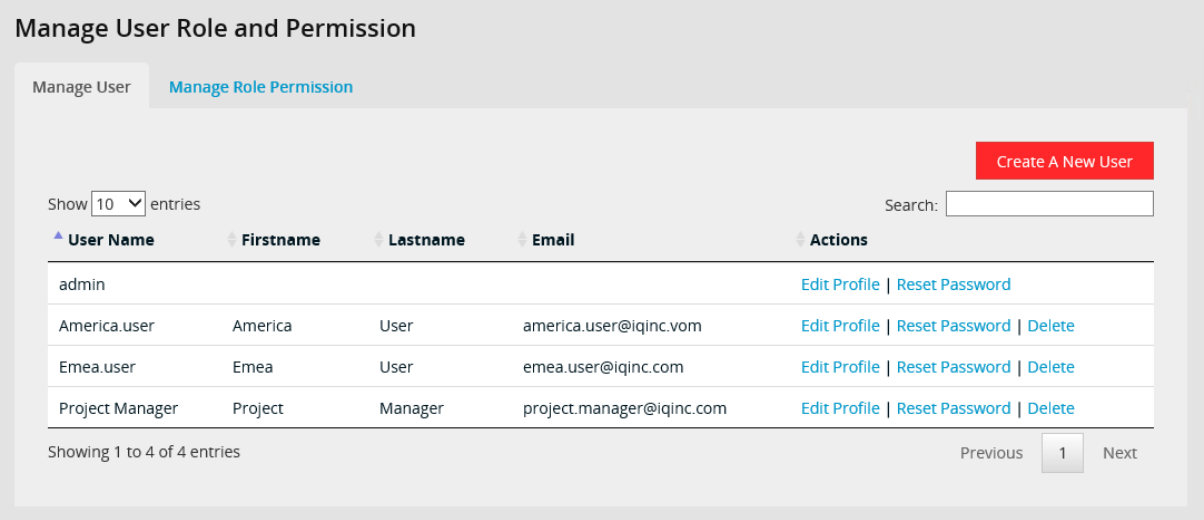
America.user user

1. Select the **User Settings > Manage User** tab.
2. Click the **Create A New User** button.
3. Clear the **AD user** checkbox; this is not an Active Directory user.
4. Insert **America.user** into the Username field.
5. Insert **America** in the Firstname field.
6. Insert **America** in the Lastname field.
7. Provide an email address for the receipt of emails.
8. Insert a password and confirm the password value.
9. Select the **Project_Viewer** role for this user.
10. Click the **Create** button.

EMEA.user user

1. Select the **User Settings > Manage User** tab.
2. Click the **Create A New User** button.
3. Clear the **AD user** checkbox; this is not an Active Directory user.

4. Insert **EMEA.user** into the Username field.
5. Insert **EMEA** in the Firstname field.
6. Insert **EMEA** in the Lastname field.
7. Provide an email address for the receipt of emails.
8. Insert a password and confirm the password value.
9. Select the **Project_Viewer** role for this user.
10. Click the **Create** button.



Multi-Departmental Estate – Project EMEA

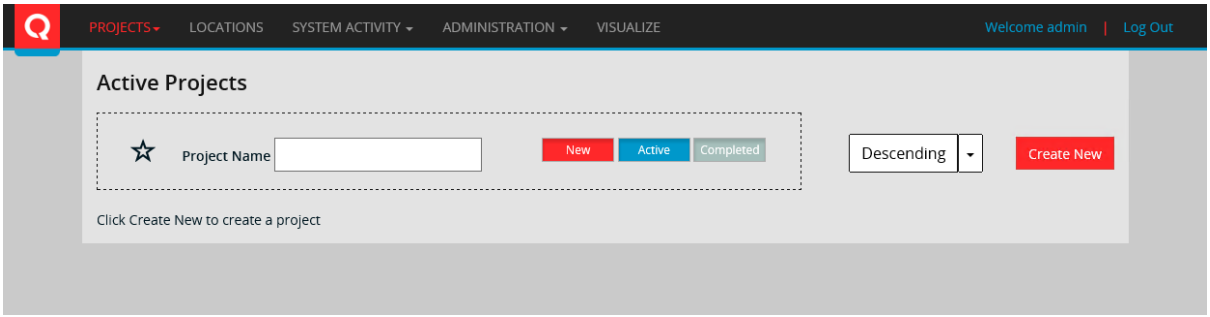
Login: Project.Manager

The project manager is responsible for the definition of all projects, including the EMEA scan project. The administrator is responsible for the definition of the infrastructure used by the project (for example, locations and credentials that will be defined for use).

> **Note:** The Projects icon and drop-down menu are the only options available to the Project.Manager user.

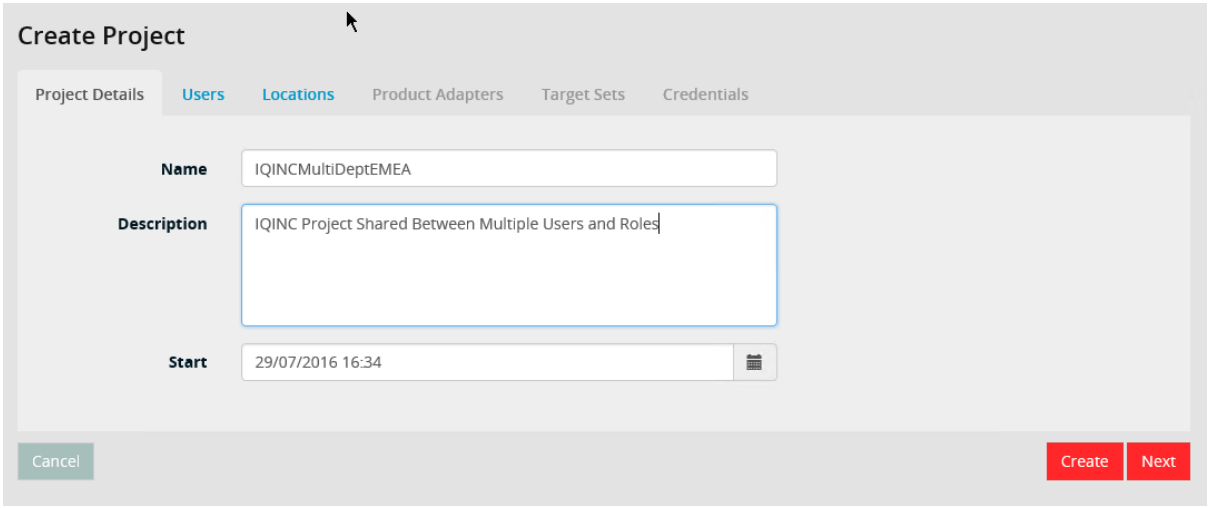
Follow the instructions below:

1. Click the **Projects** icon or **Projects** drop-down menu. This displays the currently available projects. By default, no projects are defined.



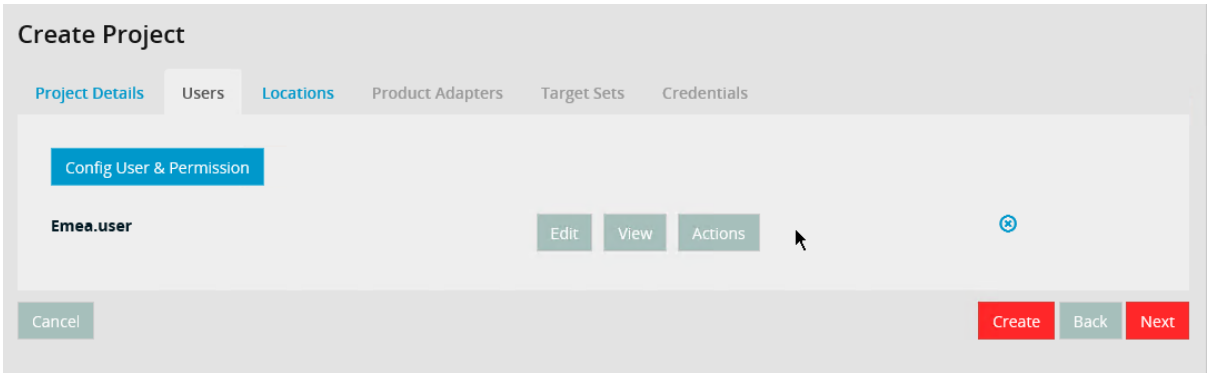
2. Select the **Active Projects** tab.
3. Click the **Create New** button to add a project.

4. View the Create Project dialog that is opened.
5. Set the Name to **MultiDeptEMEA**.
6. Set the Description to **Project Shared Between Multiple Users and Roles**.
7. Set the Start time to the current time.
8. Click the **Next** button.



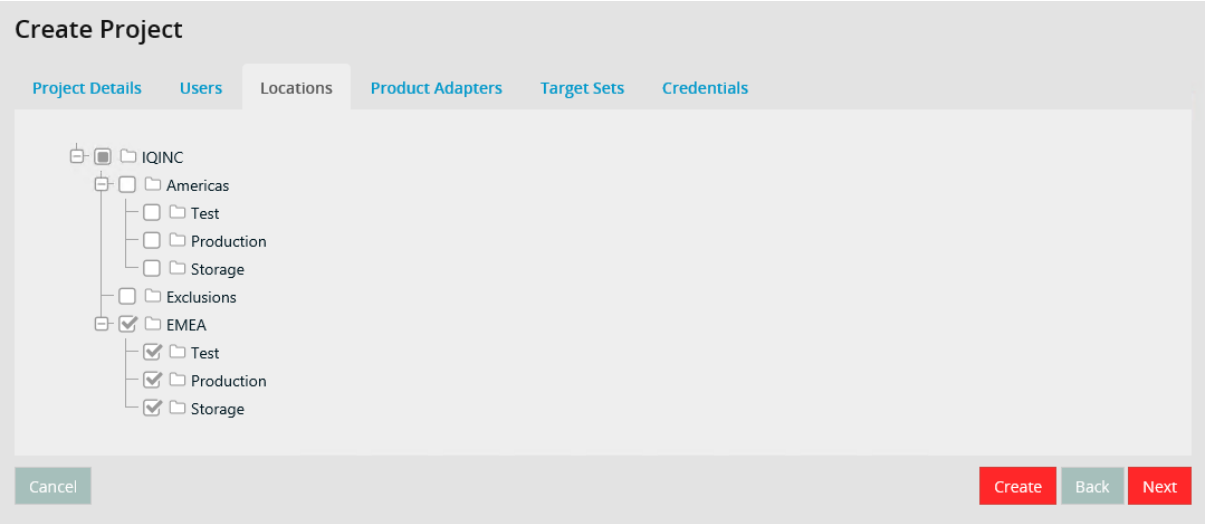
Users tab

1. Click the **Config User & Permission** button.
2. Select the **EMEA.user** to be included with this project.
3. Click the **Next** button.



Locations tab

4. Select the EMEA location.
5. Click the **Next** button.

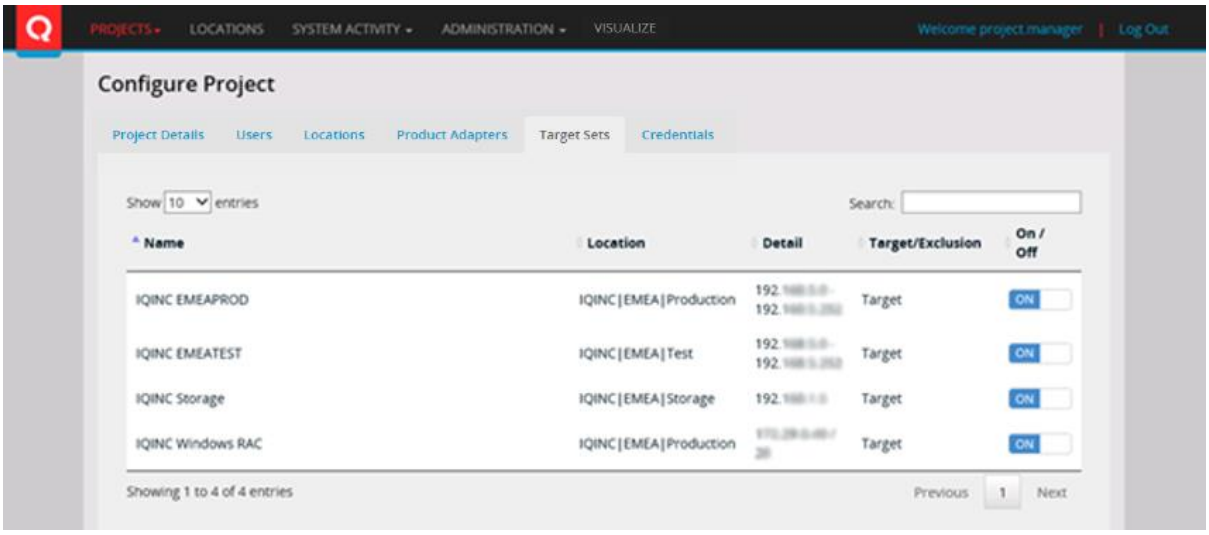


Product Adapters tab

1. Leave all the Product Adapters enabled.
2. Click the **Next** button.

IP Ranges tab

1. Ensure that the targets associated with the EMEA location are enabled.
2. Note that only targets that have been associated with the EMEA location are listed. The association of locations to targets has been provided by the admin user.



3. Click the **Next** button.

Credentials tab

1. Ensure that all credentials are set to **On**.
2. Click the **Next** button.

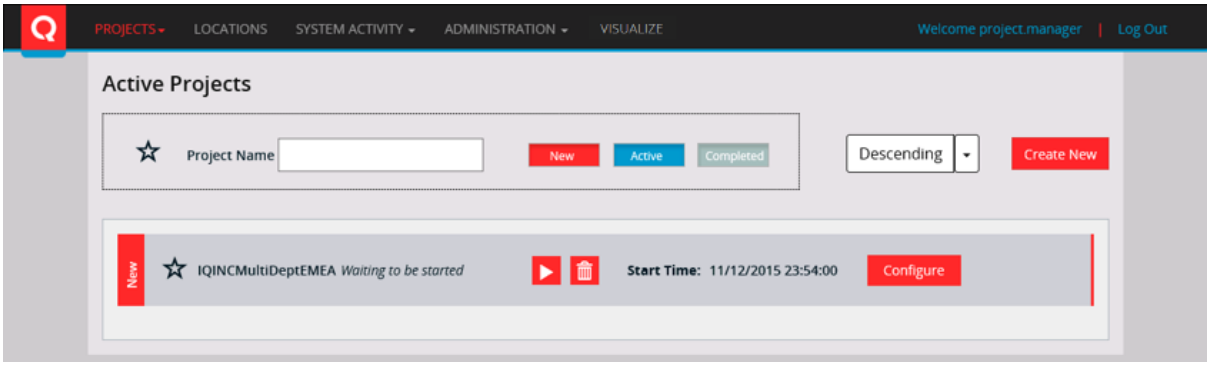
Multi-departmental estate – Project Americas

Login: Project.Manager

Follow the instructions below:

> **Note:** The Projects icon and drop-down menu are the only options available to the Project.Manager user.

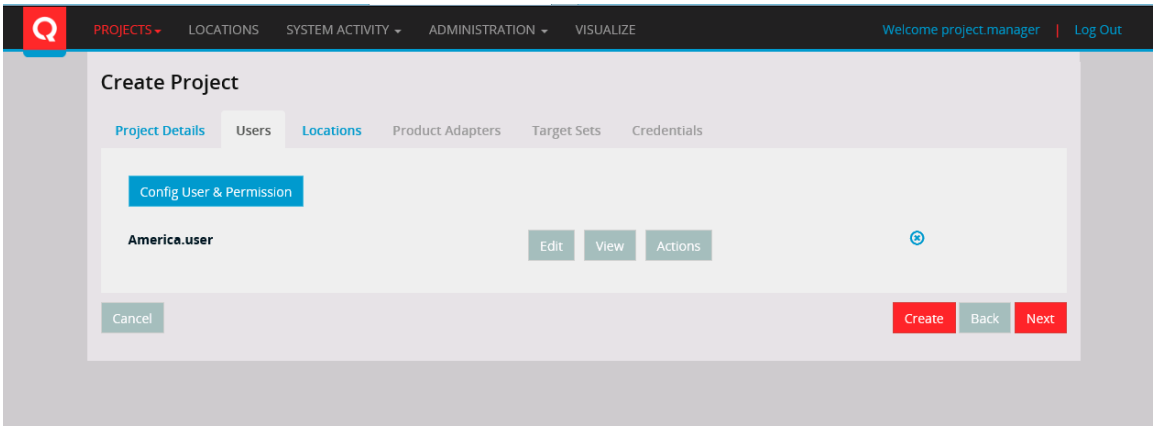
1. Click the **Projects** icon or **Projects** drop-down menu.



2. Select the **Active Projects**.
3. Note that the previously created EMEA project is available.
4. Click the **Create New** button to add a project.
5. View the Create Project dialog that is opened.
6. Set the Name to **MultiDeptAmericas**.
7. Set the Description to **Amercias Project Shared Between Multiple Users and Roles**.
8. Set the Start Time to the current time.
9. Click the **Next** button.

Users tab

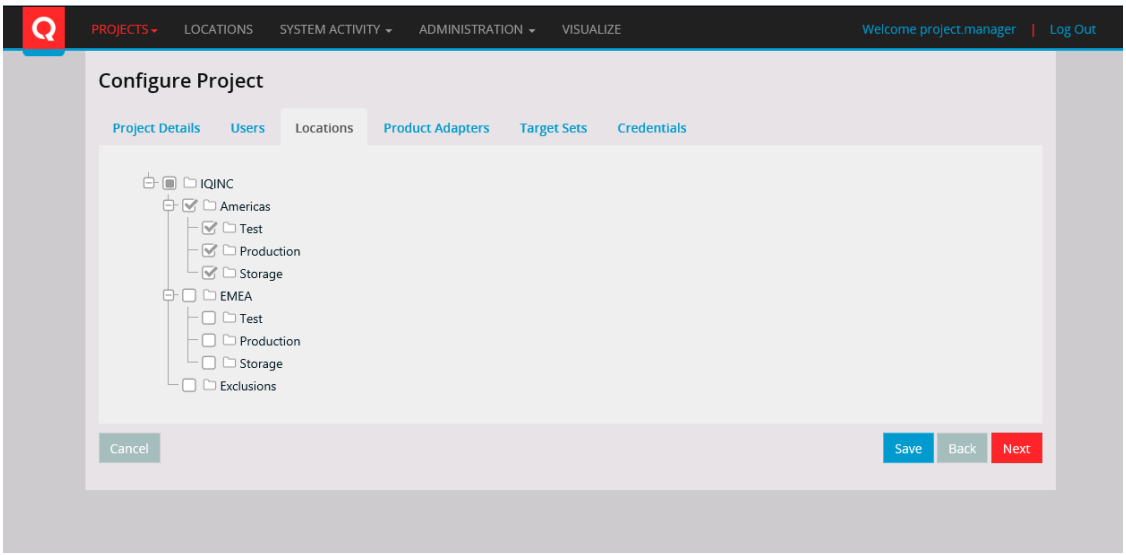
1. Click on the **Config User & Permission** button.
2. Select the **America.user** user to be included with this project.



3. Click the **Next** button.

Locations tab

1. Select the **Americas** location.



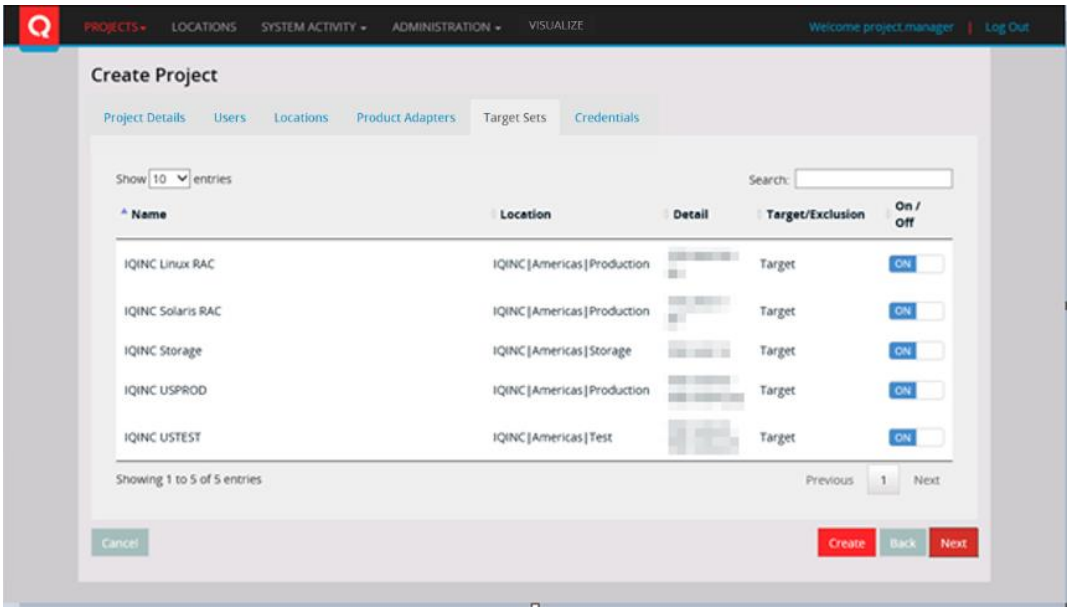
2. Note that all the sub-areas are also selected.
3. Click the **Next** button.

Product Adapters tab

1. Leave all the Product Adapters enabled.
2. Click the **Next** button.

IP Ranges tab

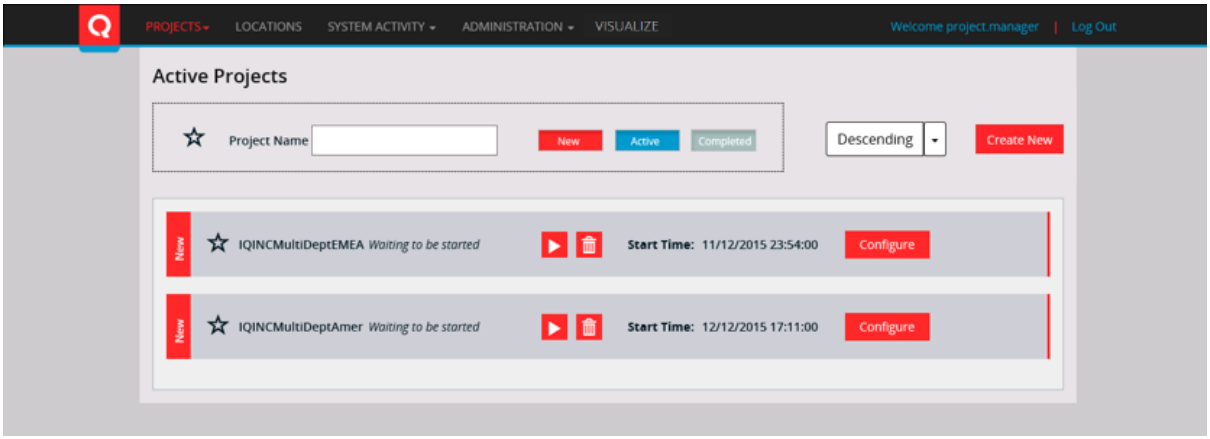
1. Ensure that the targets associated with the Americas are enabled.
2. Note that only targets that have been associated with the Americas location are listed. The association of locations with targets was provided by the admin user when describing the infrastructure.



3. Click the **Next** button.

Credentials tab

1. Ensure that all credentials are set to **On**.
2. Click the **Next** button.
3. Click the **Create** button.
4. Ensure that the new project is present in the Projects list.



Multi-departmental estate – Operations

This section shows how the operation scans are configured and started.

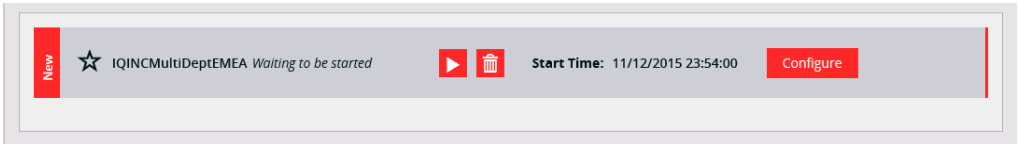
Multi-departmental estate – Start EMEA scan

Login: EMEA.user

The final step of this process is to initiate a project scan. If the licensing for this scan engine has not been previously setup, you'll need to do this before starting the scan. This is done under the **Administration > System Settings** tab. See the **System Settings - Activation** section of this document for more information.

Once all the configuration information has been identified (infrastructure by the Admin User and projects by the Project.Manager), the EMEA.user is then responsible for the day-to-day running of the EMEA project. Projects are initiated from the **Active Project** tab.

1. Click the **Projects** icon or **Projects** drop-down menu.
2. Select the **Active Projects** tab.
3. Identify the **MultiDeptEMEA** project.



4. Click the **Run** button.
5. Watch the progress bar to identify ongoing scan operations. Let the project run until it is 100% complete.

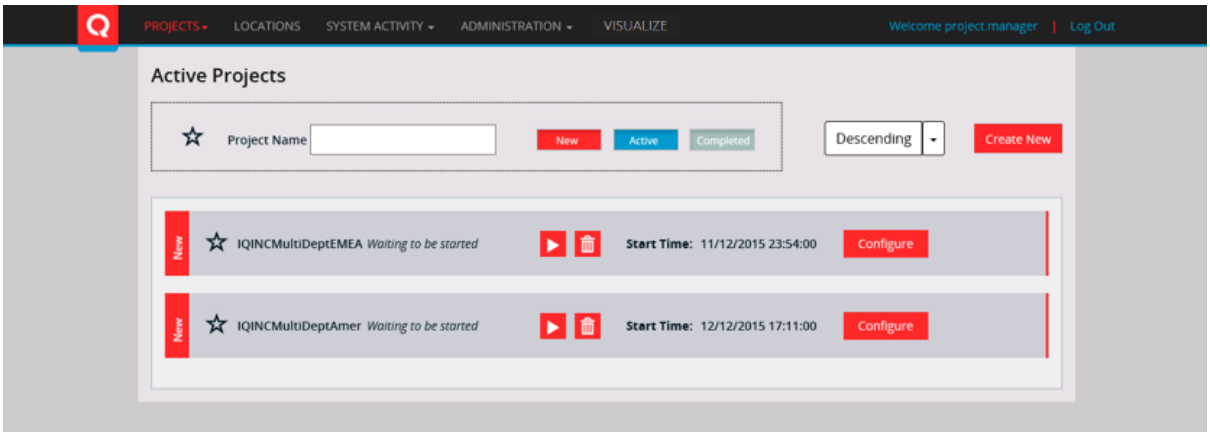
Multi-departmental estate – Start Americas scan

Login: America.user

The final step of this process is to initiate a project scan. You need to have previously set up the licensing for this scan engine before starting the scan. This is done under the **Administration > System Settings** tab. See the **System Settings - Activation** section of this document for more information.

Once the configuration information has been identified (infrastructure by the Admin User and projects by the Project.Manager), the America.user is then responsible for the day-to-day running of the Americas project. Projects are initiated from the **Active Project** tab.

1. Click the **Projects** icon or **Projects** drop-down menu.
2. Select the **Active Projects** tab.
3. Identify the **MultiDeptAmericas** project.



4. Click the **Run** button.
5. Watch progress bar to identify ongoing scan operations. Let the project run until it is 100% complete.

Multi-departmental estate – Status Americas scan

Login: America.user

Additional information about the status of the scanning process is available by click the **Status** button.

The examination and diagnosis of the scanning operations is discussed in a later chapter.

Multi-departmental estate – Status EMEA scan

Login: EMEA.user

Additional information about the status of the scanning process is available by clicking the **Status** button.

The examination and diagnosis of the scanning operations is discussed in a later chapter.

Multi-departmental estate – Americas mark scan as complete

The decision to mark a project as "complete" is one not taken by the scanning software. It's a decision made by the administrator that needs to take into account the scan coverage of the identified estate (including the discovery of any unexpected devices/applications), any requirement to add additional scan targets, successful access to all target devices (credential coverage), and the need for rescan operations. It's (typically) not the case that 100% coverage on the UI is the only criterion for marking a project complete.

Login: America.user

1. Click the **Projects** icon or **Projects** drop-down menu.
2. Select the **Active Projects** tab.
3. Identify the **MultiDeptAmericas** project.
4. Let the project run until it is 100% complete.
5. Use the Status button to identify that all elements have been sufficiently collected.
6. Click the **Actions** drop-down menu and select **Complete**.
7. Identify that the project is now in the Completed state and that the project colour has changed.

Additional information about the status of the scanning process is available by clicking on the **Status** button. The examination and diagnosis of the scanning operations is discussed in a later section.

Multi-departmental estate – EMEA mark scan as complete

The decision to mark a project as "complete" is one not taken by the scanning software. It's a decision made by the administrator that needs to take into account the scan coverage of the identified estate (including the discovery of any unexpected devices/applications), any requirement to add additional scan targets, successful access to all target devices (credential coverage), and the need for rescan operations. It's (typically) not the case that 100% coverage on the UI is the only criterion for marking a project complete.

Login: EMEA.user

1. Click the **Projects** icon or **Projects** drop-down menu.
2. Select the **Active Projects** tab.
3. Identify the **MultiDeptEMEA** project.
4. Let the project run until it is 100% complete.
5. Click the **Status** button to identify that all elements have been sufficiently collected.
6. Click the **Actions** drop-down menu and select **Complete**.
7. Identify that the project is now in the completed state and that the project color has changed.

Additional information about the status of the scanning process is available by clicking the **Status** button. The examination and diagnosis of the scanning operations is discussed in a later section.

Use case 3 – Complex estate

A **complex estate** is composed of multiple locations and/or disjoint network infrastructures. Responsibility for the network/infrastructure resides with a single person or single group with the complexity that locations are typically geographically disjointed and are also split into production and test sub-areas. Projects to execute scans are assigned as local responsibility. However, responsibility for the infrastructure remains with the global admin group.

The scan results may be segmented into different overall projects (e.g. Oracle project results, SQL Server project results, etc.) depending on the customer use case.

Additional aspects to a complex estate (which are distinct from the multi-department estate) are:

- A requirement for load balancing of scanning operations, that is, more than one scanning engine is required to carry the CPU load. The results of the scanning operation are written back to a shared scan-engine database.
- Scan Windows that identify when scanning operations are permitted within the estate.

Complex estate – Personnel expectations

Given the extended complexity of this coverage, it's expected that a single administrator and scan owner will not be sufficient.

Complex estate summary

The ability to segment into different overall projects (e.g. Oracle project results, SQL Server project results, etc.) is required for this customer use case. It's assumed that the following areas of concern must be supported:

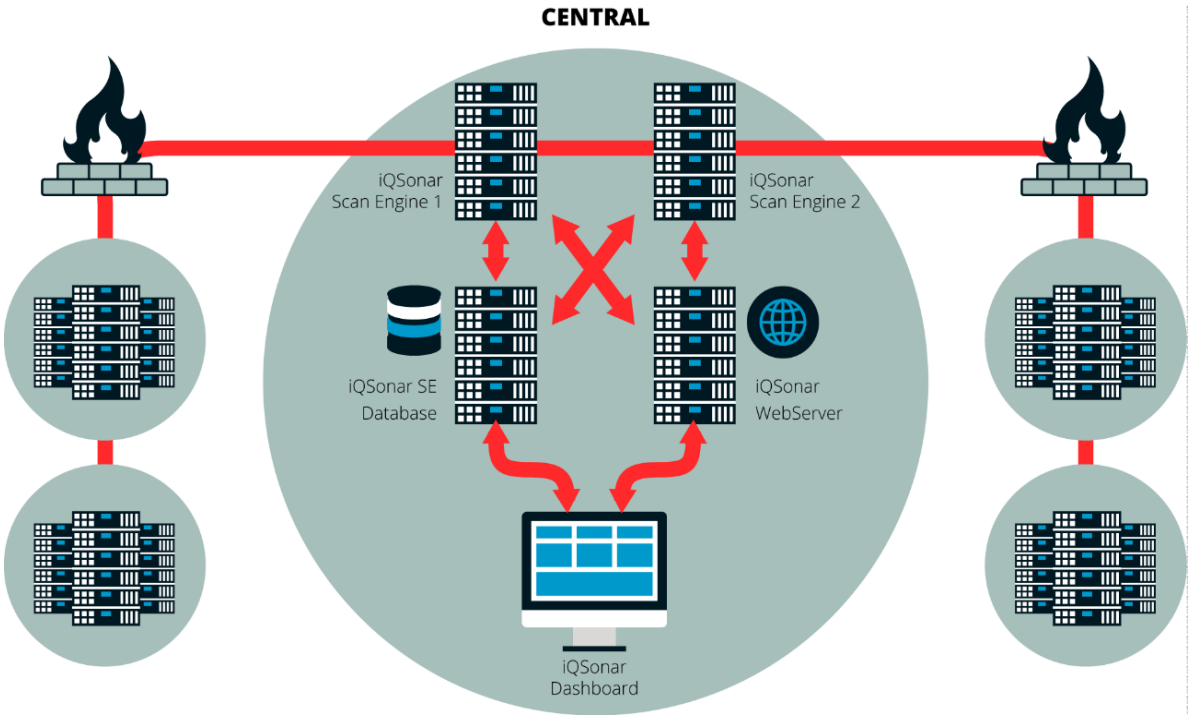
- **Global Infrastructure**: Identification and control of infrastructure globally. This "user" is responsible for the description of the infrastructure to be scanned, which includes IP address ranges, IP address range exclusions, Scan Windows and Connection types to be used.
- **Global Project Manager**: This "user" is responsible for global identification and control of project(s).
- **EMEA Manager**: This "user" is responsible for tracking and executing a EMEA project.
- **Americas Manager**: This "user" is responsible for tracking and executing an Americas project.

To support the project as described, the following items are required:

1. **2 projects:** Americas project, EMEA project
2. **4 users:** Admin, Project.Manager, America.User, EMEA.User
3. **3 roles:** Administrator, Project Manager, Project Viewer
4. **2 scan engines:** Follow the **Scan Engine Installation Guide** to install multiple scan engines.

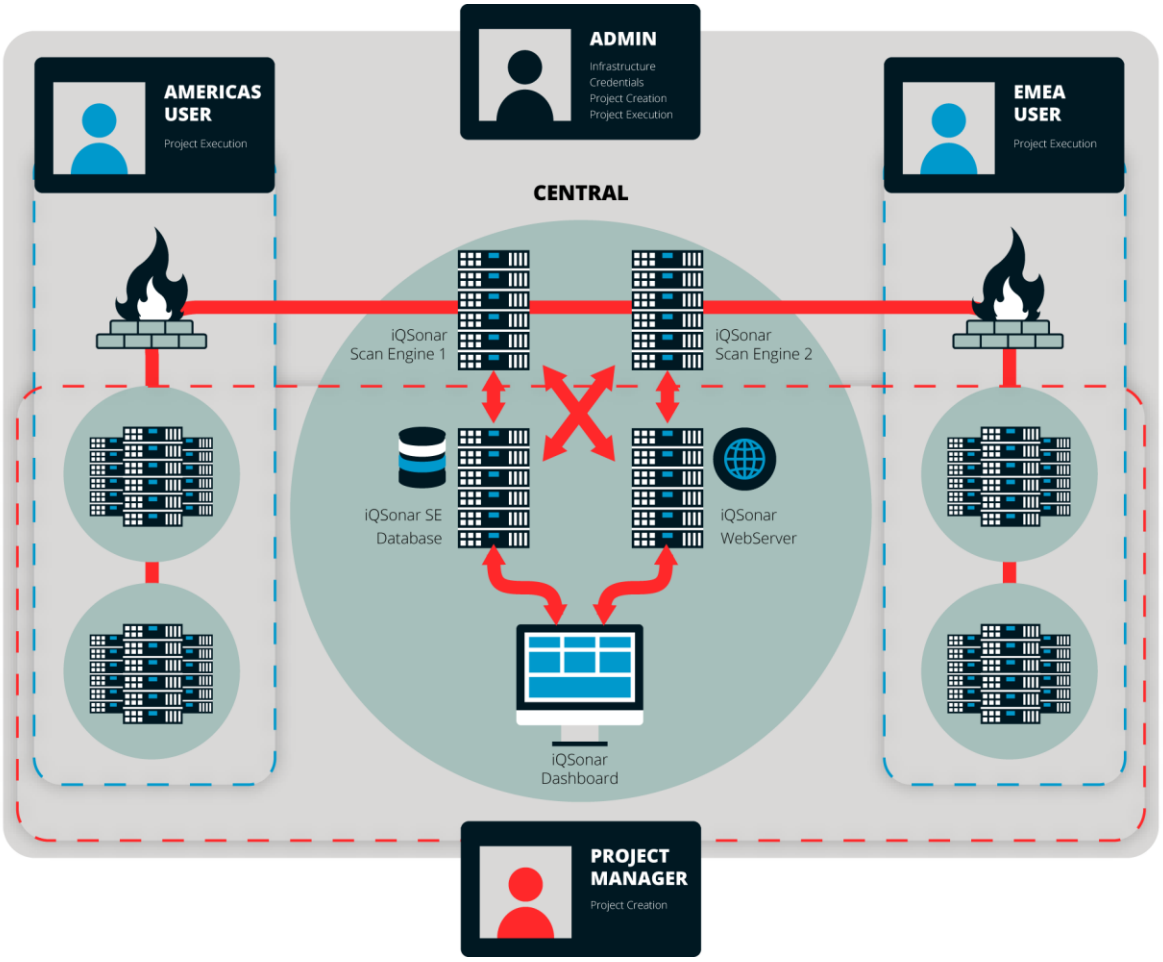
Complex estate – Network infrastructure

This network is composed of a relatively open network with no major restrictions in terms of firewalls, network latency, or bandwidth. The network structure is geographically dispersed into Americas and EMEA. Each of these locations has a production, test, and storage device.



Complex estate – Responsibility & ownership

The dashed line identifies the areas of responsibility for four users within the scan engine.



Installation of primary and secondary scan engine

It's possible to associate multiple scan engines with a single scan configuration. This allows separate scan engine resources to be assigned to subsections of an estate configuration.

The registration of a secondary scanning server is achieved by installing the scan-engine software on a new device (see the **Scan Engine Installation Guide**), on a new scanning server, and specifying the name of the scan-engine database provided during the first installation.

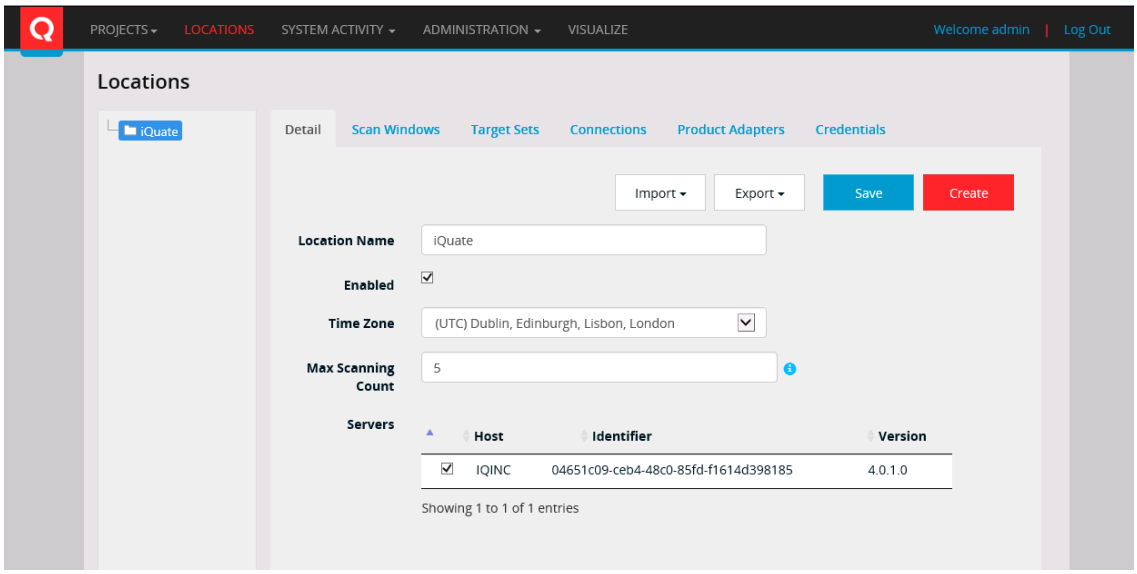
The installation of the second scanning server using the shared database ensures that the configuration information for the estate is known to both.

Complex estate – Top-level location

Login: Admin

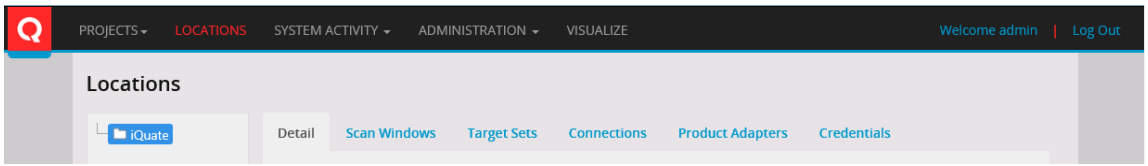
A default location is provided with the standard install. This default location can be used to encompass all of the proposed estate. Follow the instructions below:

Select the **Locations** icon or **Locations** drop-down menu in the dashboard. This displays the current available locations. By default, a single location called **default** is available as a root item (if it hasn't been modified in a previous session). This is the top-level grouping and cannot be deleted.



However, it can be renamed and it's recommended that you rename it to a customer/project-appropriate value.

1. Enter the details of your new default location (e.g. , Ivanti).
2. Ensure that **Enabled** is selected.
3. Enter the Time Zone of this locality. Enter the Max Scanning Count of **5.** (The number of concurrent jobs that can be run for targets in this location. A locality could be associated with targets accessible over a slow data connection, and for this reason large numbers of concurrent jobs is not advisable.)
4. Select the scan engines associated with this locality.
5. Click the **Save** button to save your details.



This single location is **not** sufficient for a medium project, because you need to have a more granular control over the elements of the estate that need to be scanned.

Complex estate – Country-level location

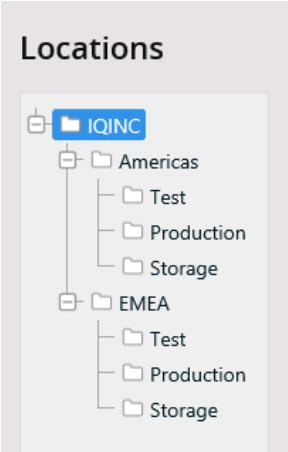
Login: Admin

The complex company is split into two regional (scan) locations. Each region could be allowed to run its own scan projects (e.g., an Oracle audit may be done on a regional level at different times). Each location is also sub-divided into production, test, and storage device infrastructure as described below:

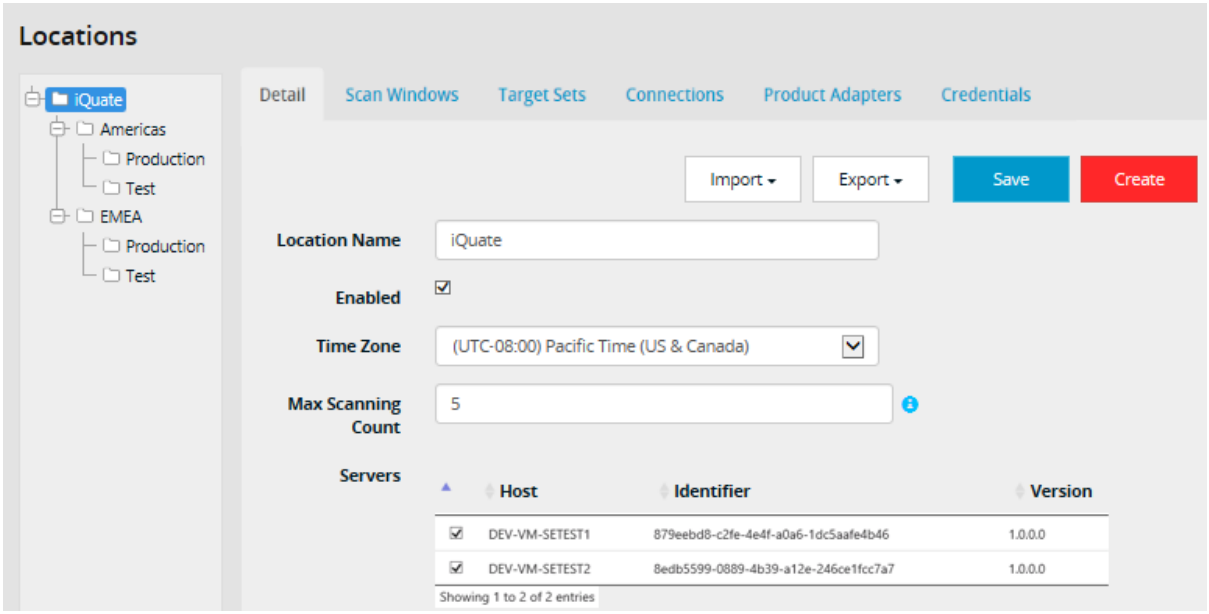
- Americas
  - Test
  - Production
  - Storage
- EMEA
  - Test
  - Production
  - Storage

These new locations need to be added:

1. Select the **Locations** icon or **Locations** drop-down menu in the dashboard.
2. Set up the complex estate with the following localities. See the **Multi-departmental estate – Country-level locations** section.



3. Click the **Ivanti Location**.
4. Enable both Scan engines for the default Ivanti location.



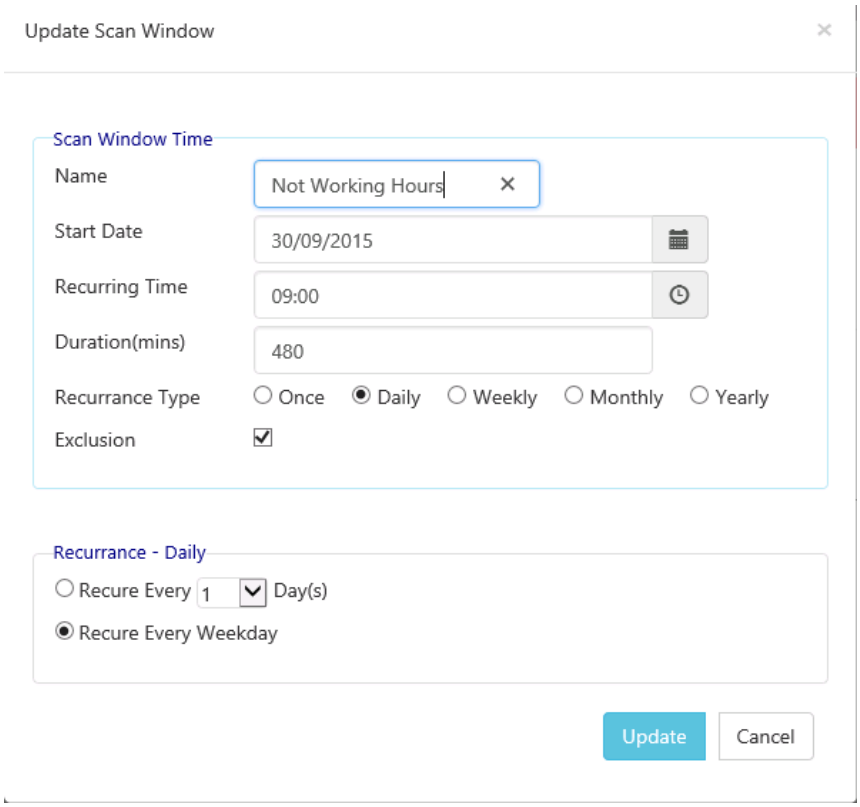
5. Click the **Americas** Location.
6. Enable the first scan engines for the Americas location.
7. Disable the second scan engines for the Americas location.
8. Click the **EMEA** Location.
9. Enable the second scan engines for the EMEA location.
10. Disable the first scan engines for the EMEA location.

The result of this configuration is that projects that make use of locations will abide by the association of a scan engine to each of the locations. If additional areas are added under the Ivanti location, these will have both scan engines available to projects.

The rest of the items in the complex estate configuration are similar to the configuration of a medium-sized company. For that reason, references to the medium-sized company configuration are provided below at the end of this section.

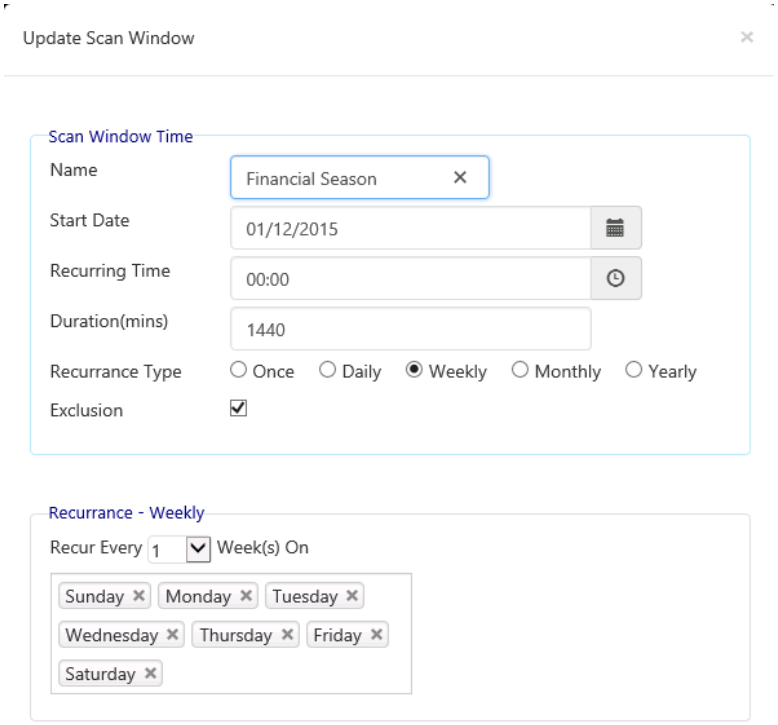
Complex estate – Scan Windows

Scan Windows provides a means to limit the period when active scanning of an estate is carried out. For mission-critical enterprises, the possibility of additional network traffic or CPU is viewed as a risk. For this reason, specific time periods may be specified for scanning. For a complex estate, it's assumed that two restrictions will be applied. Scanning cannot occur during working hours (9-5) weekdays. Secondly, the weeks from Thanksgiving to January are also excluded for Financial Season.



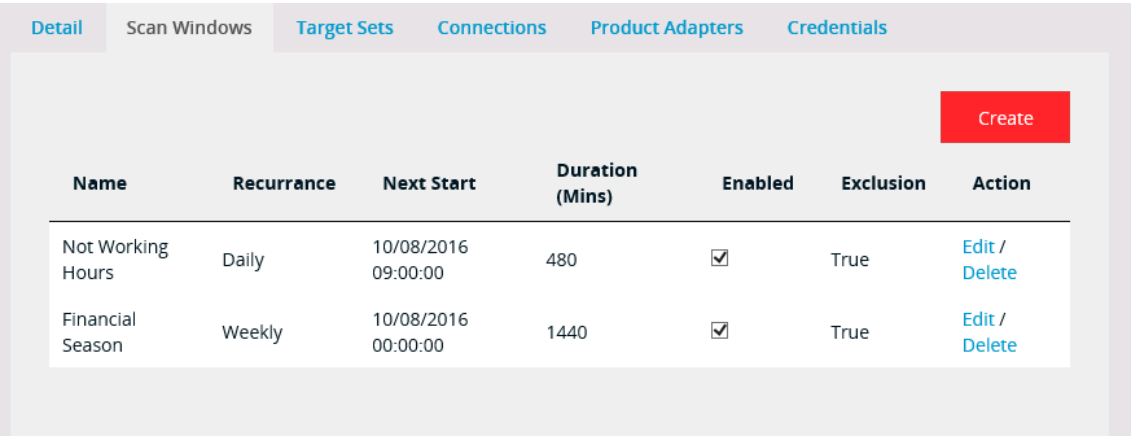
1. Click the **Create** button.
2. Type **Not Working Hours** in the Name box.
3. Select **9.00am** in The Recurring Time box.
4. Type **480** (mins) in the Duration box.
5. Click the **Daily** radio button.
6. Click the **Exclusion** box.
7. Click the **Recur Every Weekday** radio button.
8. Click the **Create** button to save the scan window.

Secondly, the weeks from Thanksgiving to January are also excluded for Financial Season.



1. Click the **Create** button.
2. Type **Financial Season** in the Name box.
3. Select **00.00am** in The Recurring Time box.
4. Type **1440** (mins) in the Duration box.
5. Click the **Weekly** radio button.
6. Click the **Exclusion** box.
7. Click the **Recur Every 1 week** radio button.
8. Select every day of the week.
9. Click the **Create** button to save the scan window.

The Scan Windows exclusions will be displayed.



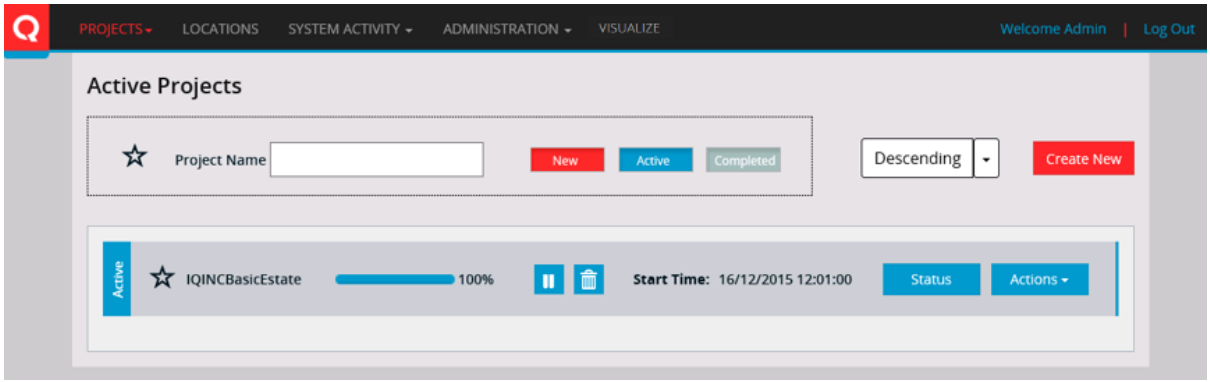
Complex estate - Configurations

The configuration of the complex estate from this point on is similar to the multi-departmental estate. For this reason, references are provided to the previous section to continue the configuration.

Complex estate section	Equivalent multi-departmental estate section
Complex estate – Targets	See Multi-departmental estate – Targets
Complex estate - Connections	See Multi-departmental estate – Connections
Complex estate – Product Adapters	See Multi-departmental estate – Product Adapters
Complex estate – System Credentials	See Multi-departmental estate – System Credentials
Complex estate – Global System Credentials	See Multi-departmental estate – Global System Credentials
Complex estate – Application Credentials	See Multi-departmental estate – Application Credentials
Complex estate – Americas Application Credentials	See Multi-departmental estate – Americas Application Credentials
Complex estate – EMEA Application Credentials	See Multi-departmental estate – EMEA Application Credentials
Complex estate – Users & Roles	See Multi-departmental estate – Users and Roles
Complex estate – Create Users	See Multi-departmental estate – Create Users
Complex estate – Create Roles	See Multi-departmental estate – Create Roles
Complex estate – Project EMEA	See Multi-departmental estate – Project EMEA
Complex estate – Project Americas	See Multi-departmental estate – Project Americas
Complex estate – Start EMEA Scan	See Multi-departmental estate – Start EMEA Scan
Complex estate – Start Americas Scan	See Multi-departmental estate – Start Americas Scan
Complex estate – Status EMEA Scan	See Multi-departmental estate – Status EMEA Scan
Complex estate – Status Americas Scan	See Multi-departmental estate – Status Americas Scan
Complex estate – Americas Mark Scan as Complete	See Multi-departmental estate - Americas Mark Scan as Complete
Complex estate – EMEA Mark Scan as Complete	See Multi-departmental estate - EMEA Mark Scan as Complete

Project scan analysis

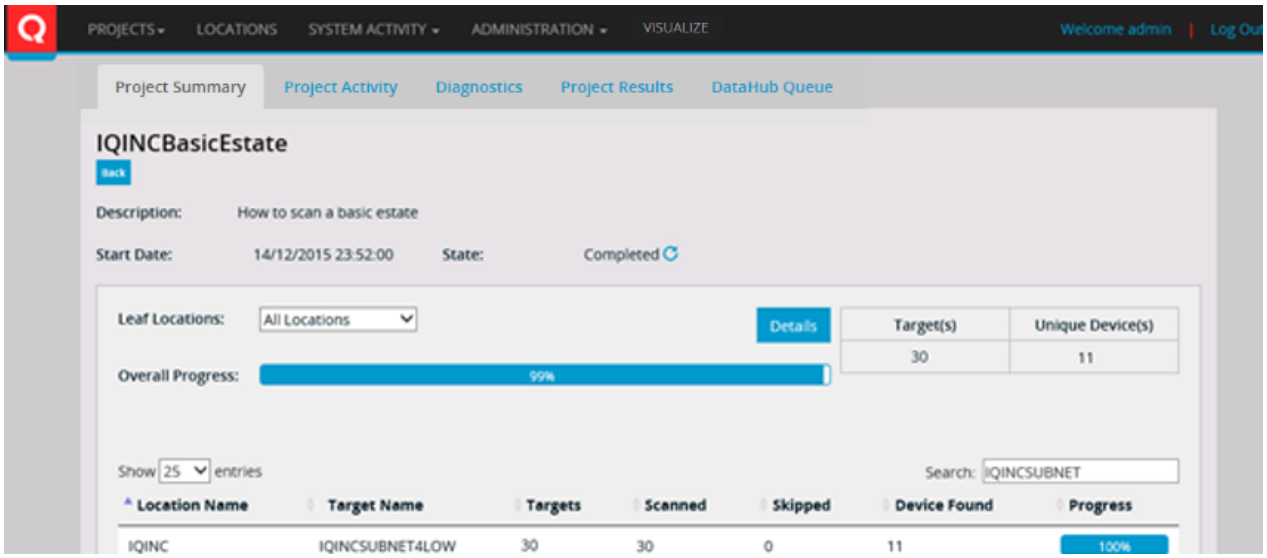
You can analyze the scanning operation from the UI interface. The analysis is carried out on a project by project basis. Under **Active Projects**, identify the project of interest.



Click the **Status** button to open the top-level Project Summary window.

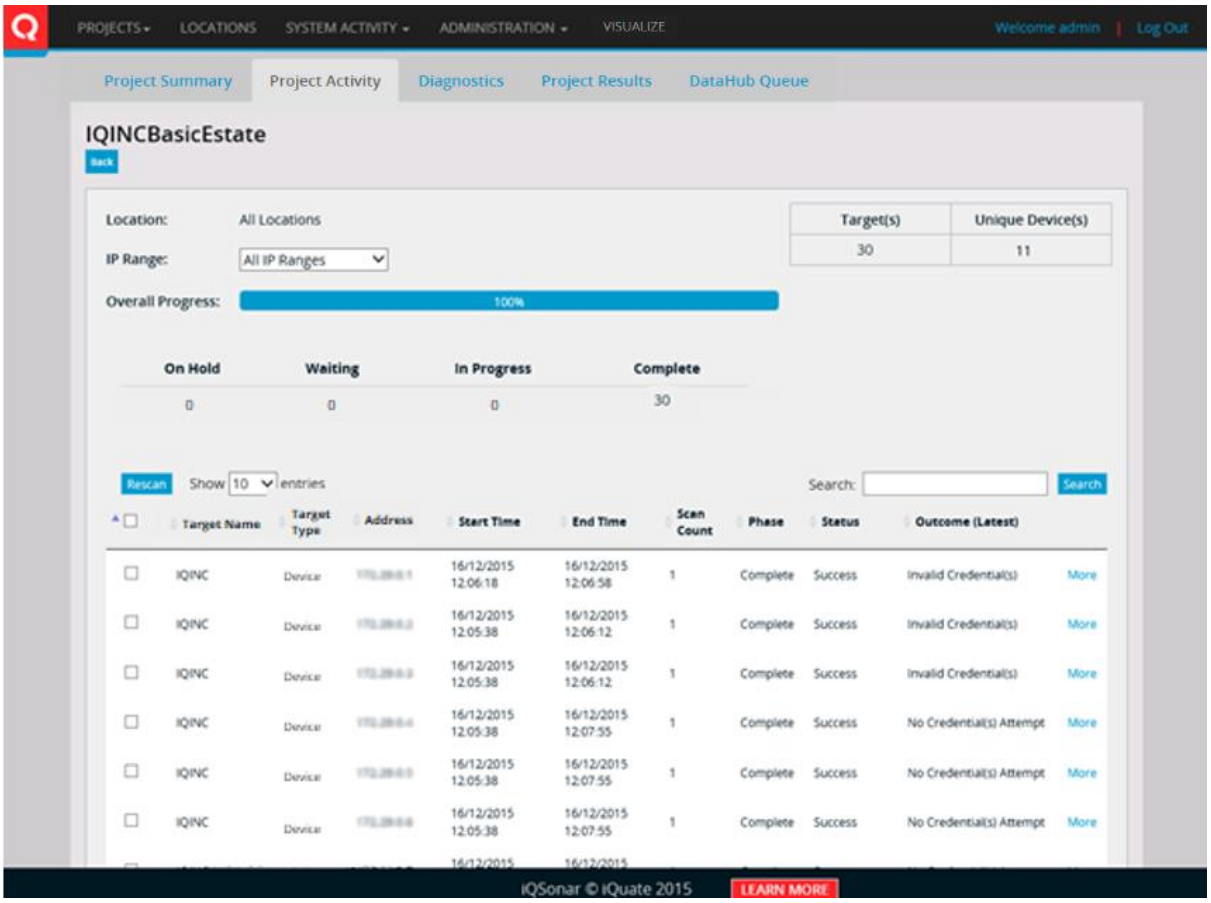
Project summary

This window identifies the total number of targets, number of unique devices identified, the overall progress of the project scan, and a breakdown for all locations in the project with a scan progress for each of the locations.



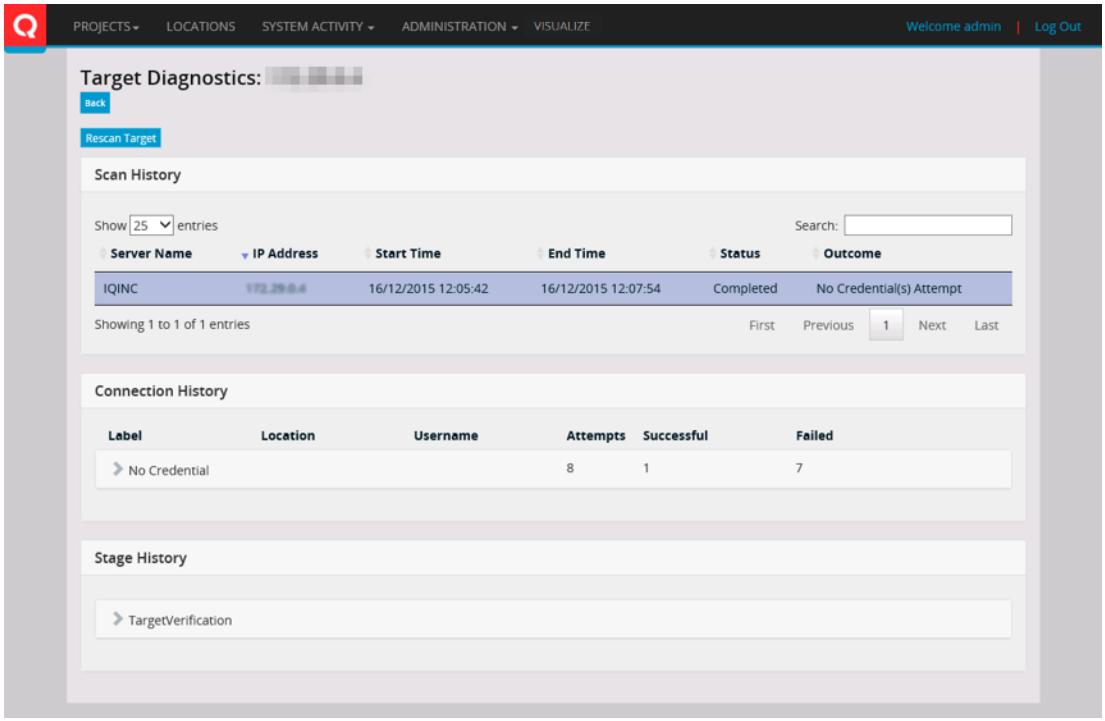
Project activity

If you need to examine a specific device, select the **Project Activity** tab. This tab provides a breakdown of the scan operations associated with each target device linked with the project. Each target is associated with a unique IP address, the number of times that the device has been scanned, the current scan status, and last scan operation outcome (e.g., failed credential, valid credentials, etc.)



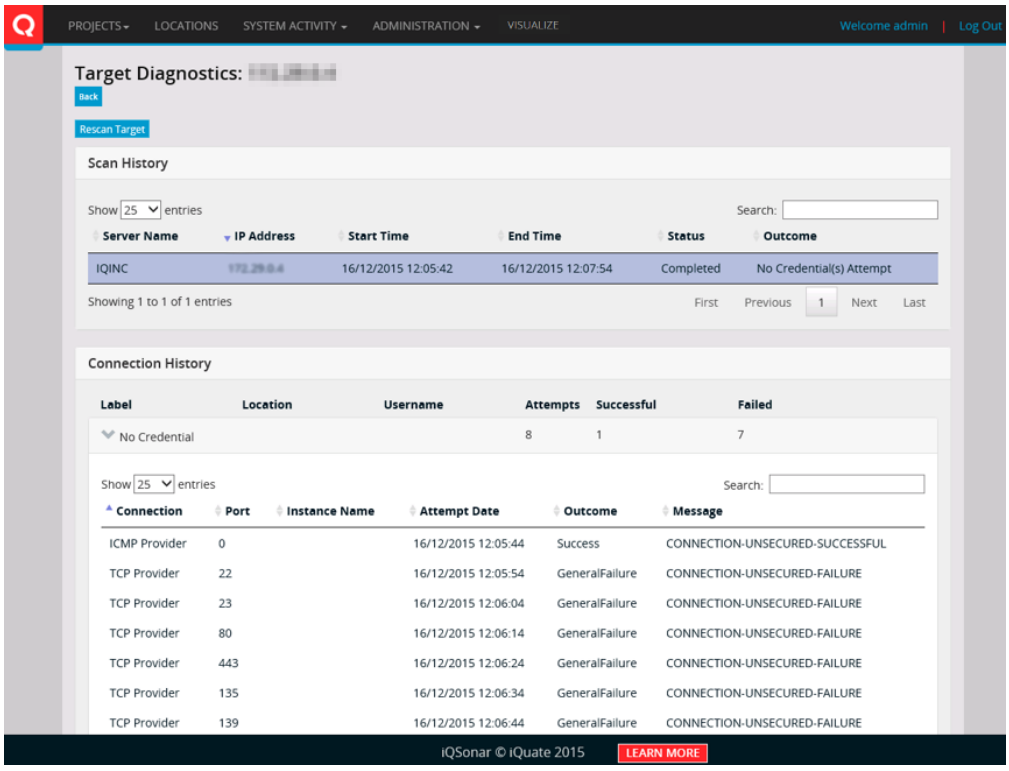
Additional detail is available for each target by clicking the **More…** button.

Project activity – No credential(s) attempt

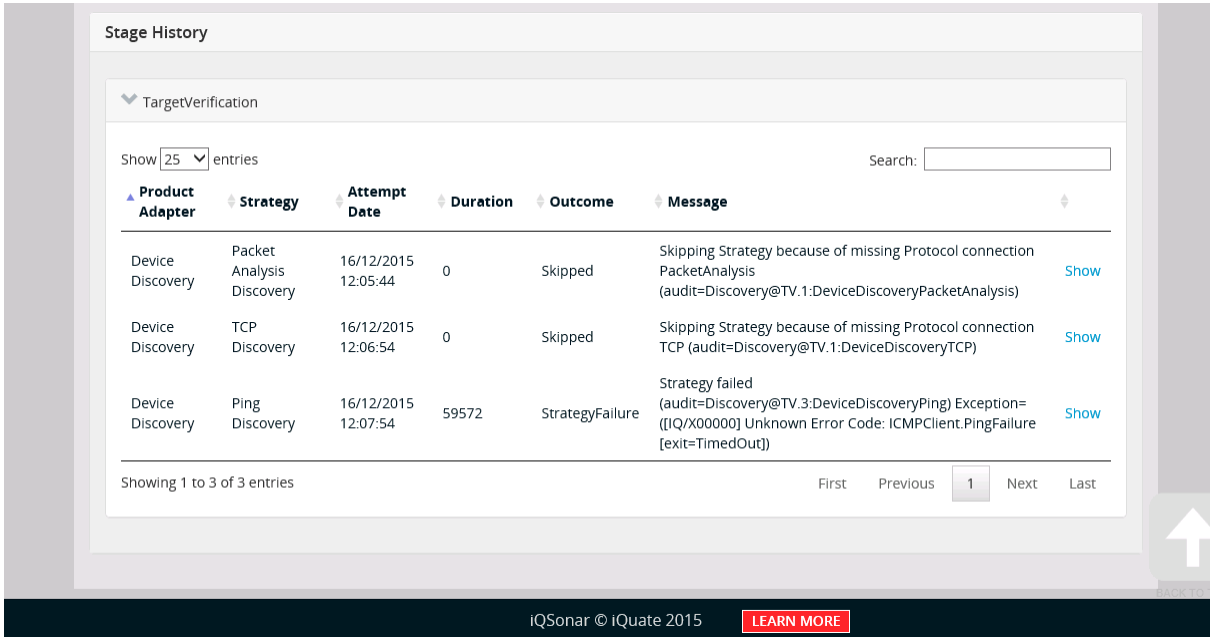


For a credential failure, the diagnostics are split into the connection history and stage history.

The **connection history** establishes that a target connected using protocols available within the project. The connection history identifies that there is a section where connections were attempted (without any credentials being used). Eight attempts were made to various ports on the target; One was successful over the ICMP Provider, which is the remote target ping operation.



The **stage history** only has a **TargetVerification** stage. This identifies attempts that were made to identify if a target exists on the IP address selected. Click the Banner line **(>)** to expand the elements that were attempted during the target verification stage.



Three strategies were available to check if this target could be discovered:

- The first strategy attempted to perform packet analysis of network traffic to identify that the target is active, but the necessary protocol connection to support this was not available to the scan engine.
- The lack of a TCP connection to the target meant that the second strategy was **skipped**.
- The third strategy attempted to ping the target IP address but returned a **strategyFailure** (i.e., a response wasn't received within the time limit).

Additional information for each strategy is available by clicking the **Show** button associated with the strategy.

Project activity – Valid credential

For a credential success, the diagnostics are split into additional stages that identify the additional operations carried out on the device. The connection history still identifies the establishment of a connection to the target using protocols available within the project as with the failure case. Each successful credential usage is identified.

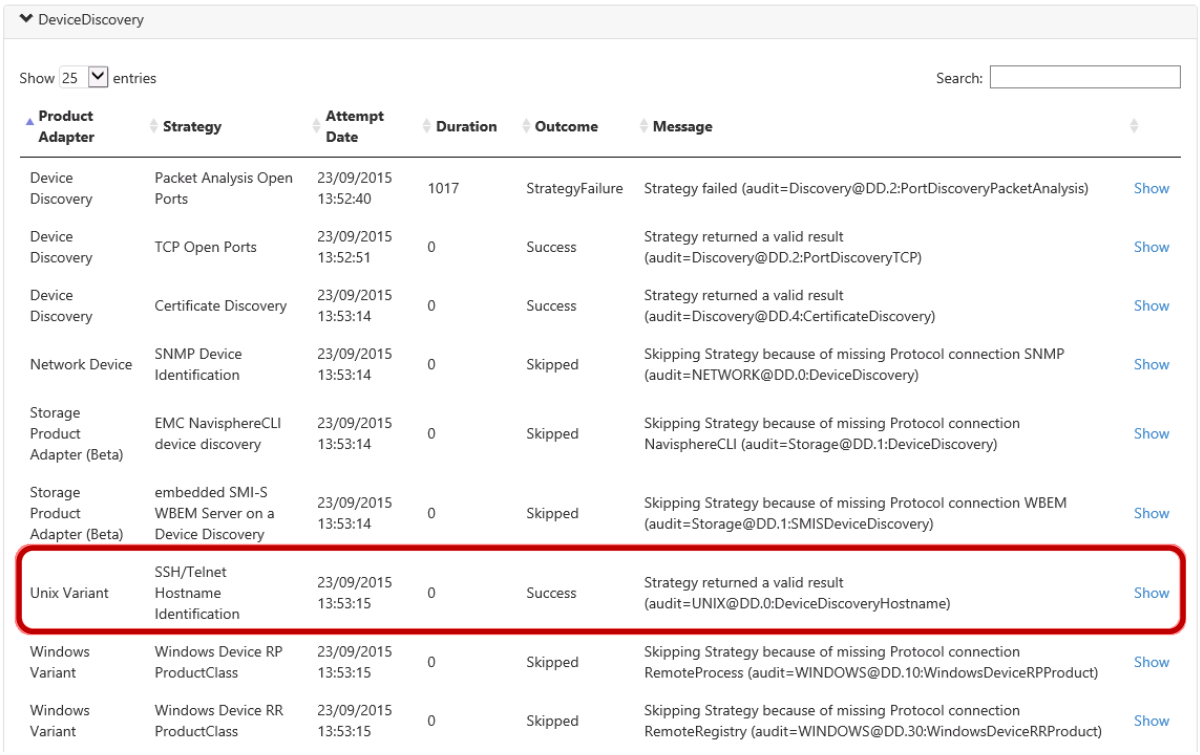
The stage history now has a series of additional stages that have been attempted based on the availability of valid credentials for a target. This summarizes the strategies that were run on the target. Click any Banner line **(>)** to expand the elements that were attempted during the stage.

Target verification

The **target verification** identifies the two successful strategies that were used to identify the presence of a target.

Device discovery

The **device discovery** stage identifies the outcomes of the strategies that retrieve initial information related to a target (e.g., the hostname of the target).



DeviceDiscovery

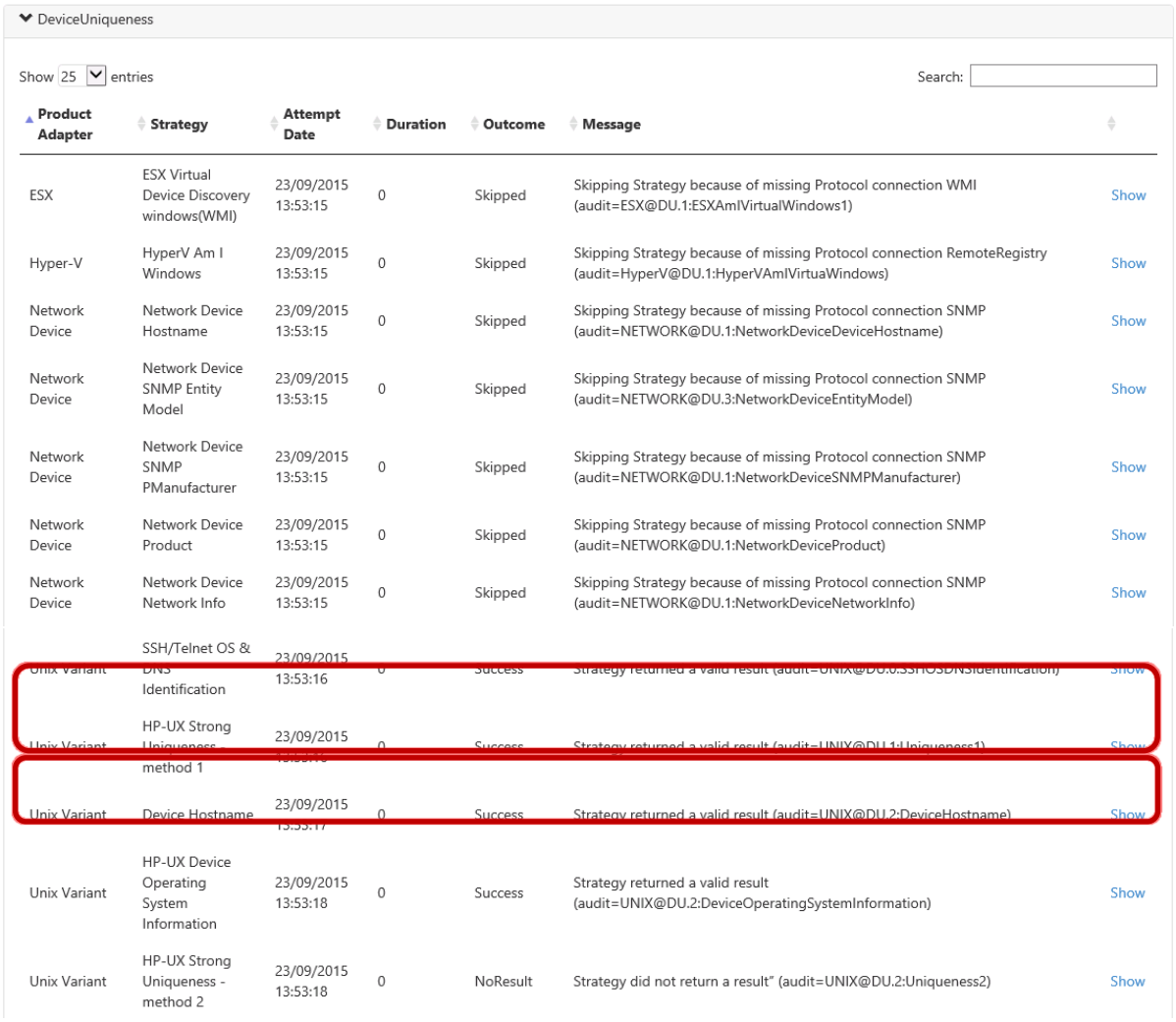
Show 25 entries Search:

Product Adapter	Strategy	Attempt Date	Duration	Outcome	Message	
Device Discovery	Packet Analysis Open Ports	23/09/2015 13:52:40	1017	StrategyFailure	Strategy failed (audit=Discovery@DD.2:PortDiscoveryPacketAnalysis)	Show
Device Discovery	TCP Open Ports	23/09/2015 13:52:51	0	Success	Strategy returned a valid result (audit=Discovery@DD.2:PortDiscoveryTCP)	Show
Device Discovery	Certificate Discovery	23/09/2015 13:53:14	0	Success	Strategy returned a valid result (audit=Discovery@DD.4:CertificateDiscovery)	Show
Network Device	SNMP Device Identification	23/09/2015 13:53:14	0	Skipped	Skipping Strategy because of missing Protocol connection SNMP (audit=NETWORK@DD.0:DeviceDiscovery)	Show
Storage Product Adapter (Beta)	EMC NavisphereCLI device discovery	23/09/2015 13:53:14	0	Skipped	Skipping Strategy because of missing Protocol connection NavisphereCLI (audit=Storage@DD.1:DeviceDiscovery)	Show
Storage Product Adapter (Beta)	embedded SMI-S WBEM Server on a Device Discovery	23/09/2015 13:53:14	0	Skipped	Skipping Strategy because of missing Protocol connection WBEM (audit=Storage@DD.1:SMISDeviceDiscovery)	Show
Unix Variant	SSH/Telnet Hostname Identification	23/09/2015 13:53:15	0	Success	Strategy returned a valid result (audit=UNIX@DD.0:DeviceDiscoveryHostname)	Show
Windows Variant	Windows Device RP ProductClass	23/09/2015 13:53:15	0	Skipped	Skipping Strategy because of missing Protocol connection RemoteProcess (audit=WINDOWS@DD.10:WindowsDeviceRPProduct)	Show
Windows Variant	Windows Device RR ProductClass	23/09/2015 13:53:15	0	Skipped	Skipping Strategy because of missing Protocol connection RemoteRegistry (audit=WINDOWS@DD.30:WindowsDeviceRRProduct)	Show

The example above identifies that the UNIX Variant product adapter successfully retrieved device discovery information over the SSH Telnet strategy. Clicking the **Show** button identifies the command that was executed.

Device uniqueness

The **device uniqueness** stage ensures that duplicates of a target are not generated by ensuring that each target is uniquely identified using attributes associated with the target.



DeviceUniqueness

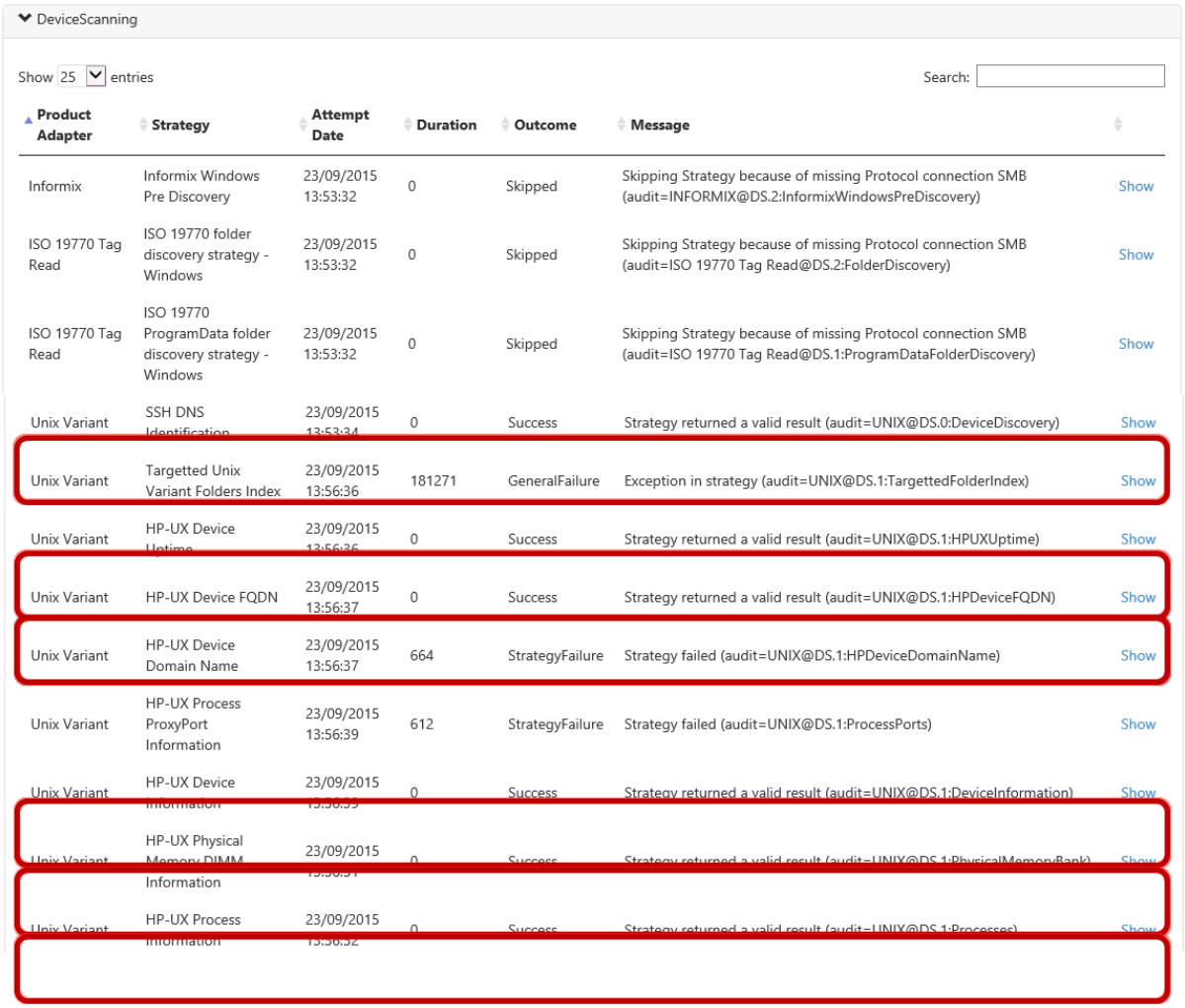
Show 25 entries Search:

Product Adapter	Strategy	Attempt Date	Duration	Outcome	Message	
ESX	ESX Virtual Device Discovery windows(WMI)	23/09/2015 13:53:15	0	Skipped	Skipping Strategy because of missing Protocol connection WMI (audit=ESX@DU.1:ESXAmIVirtualWindows1)	Show
Hyper-V	HyperV Am I Windows	23/09/2015 13:53:15	0	Skipped	Skipping Strategy because of missing Protocol connection RemoteRegistry (audit=HyperV@DU.1:HyperVAmIVirtuaWindows)	Show
Network Device	Network Device Hostname	23/09/2015 13:53:15	0	Skipped	Skipping Strategy because of missing Protocol connection SNMP (audit=NETWORK@DU.1:NetworkDeviceDeviceHostname)	Show
Network Device	Network Device SNMP Entity Model	23/09/2015 13:53:15	0	Skipped	Skipping Strategy because of missing Protocol connection SNMP (audit=NETWORK@DU.3:NetworkDeviceEntityModel)	Show
Network Device	Network Device SNMP PManufacturer	23/09/2015 13:53:15	0	Skipped	Skipping Strategy because of missing Protocol connection SNMP (audit=NETWORK@DU.1:NetworkDeviceSNMPManufacturer)	Show
Network Device	Network Device Product	23/09/2015 13:53:15	0	Skipped	Skipping Strategy because of missing Protocol connection SNMP (audit=NETWORK@DU.1:NetworkDeviceProduct)	Show
Network Device	Network Device Network Info	23/09/2015 13:53:15	0	Skipped	Skipping Strategy because of missing Protocol connection SNMP (audit=NETWORK@DU.1:NetworkDeviceNetworkInfo)	Show
Unix Variant	SSH/Telnet OS & DNS Identification	23/09/2015 13:53:16	0	Success	Strategy returned a valid result (audit=UNIX@DU.0:SSHOSDNSIdentification)	Show
Unix Variant	HP-UX Strong Uniqueness - method 1	23/09/2015 13:53:16	0	Success	Strategy returned a valid result (audit=UNIX@DU.1:Uniqueness1)	Show
Unix Variant	Device Hostname	23/09/2015 13:53:17	0	Success	Strategy returned a valid result (audit=UNIX@DU.2:DeviceHostname)	Show
Unix Variant	HP-UX Device Operating System Information	23/09/2015 13:53:18	0	Success	Strategy returned a valid result (audit=UNIX@DU.2:DeviceOperatingSystemInformation)	Show
Unix Variant	HP-UX Strong Uniqueness - method 2	23/09/2015 13:53:18	0	NoResult	Strategy did not return a result" (audit=UNIX@DU.2:Uniqueness2)	Show

The example above identifies that the UNIX Variant product adapter successfully retrieved device uniqueness information over the SSH Telnet strategy. Clicking the **Show** button identifies the command(s) that were executed.

Device scanning

The **device scanning** stage retrieves information about the target device (DNS name, FQDN, domain-name, list of folders, system uptime, memory, process information, etc.).



DeviceScanning

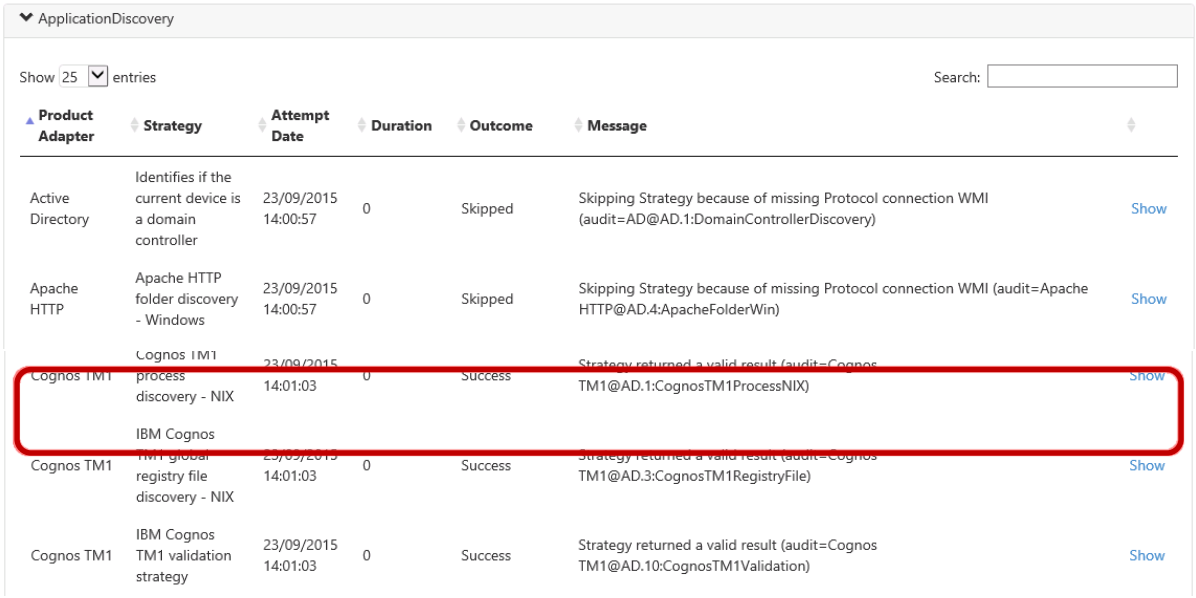
Show 25 entries Search:

Product Adapter	Strategy	Attempt Date	Duration	Outcome	Message	
Informix	Informix Windows Pre Discovery	23/09/2015 13:53:32	0	Skipped	Skipping Strategy because of missing Protocol connection SMB (audit=INFORMIX@DS.2:InformixWindowsPreDiscovery)	Show
ISO 19770 Tag Read	ISO 19770 folder discovery strategy - Windows	23/09/2015 13:53:32	0	Skipped	Skipping Strategy because of missing Protocol connection SMB (audit=ISO 19770 Tag Read@DS.2:FolderDiscovery)	Show
ISO 19770 Tag Read	ISO 19770 ProgramData folder discovery strategy - Windows	23/09/2015 13:53:32	0	Skipped	Skipping Strategy because of missing Protocol connection SMB (audit=ISO 19770 Tag Read@DS.1:ProgramDataFolderDiscovery)	Show
Unix Variant	SSH DNS Identification	23/09/2015 13:53:34	0	Success	Strategy returned a valid result (audit=UNIX@DS.0:DeviceDiscovery)	Show
Unix Variant	Targetted Unix Variant Folders Index	23/09/2015 13:56:36	181271	GeneralFailure	Exception in strategy (audit=UNIX@DS.1:TargettedFolderIndex)	Show
Unix Variant	HP-UX Device Uptime	23/09/2015 13:56:36	0	Success	Strategy returned a valid result (audit=UNIX@DS.1:HPUXUptime)	Show
Unix Variant	HP-UX Device FQDN	23/09/2015 13:56:37	0	Success	Strategy returned a valid result (audit=UNIX@DS.1:HPDeviceFQDN)	Show
Unix Variant	HP-UX Device Domain Name	23/09/2015 13:56:37	664	StrategyFailure	Strategy failed (audit=UNIX@DS.1:HPDeviceDomainName)	Show
Unix Variant	HP-UX Process ProxyPort Information	23/09/2015 13:56:39	612	StrategyFailure	Strategy failed (audit=UNIX@DS.1:ProcessPorts)	Show
Unix Variant	HP-UX Device Information	23/09/2015 13:56:39	0	Success	Strategy returned a valid result (audit=UNIX@DS.1:DeviceInformation)	Show
Unix Variant	HP-UX Physical Memory DIMM Information	23/09/2015 13:56:51	0	Success	Strategy returned a valid result (audit=UNIX@DS.1:PhysicalMemoryBank)	Show
Unix Variant	HP-UX Process Information	23/09/2015 13:56:52	0	Success	Strategy returned a valid result (audit=UNIX@DS.1:Processes)	Show

The example above identifies that the UNIX Variant product adapter successfully retrieved device artifacts over the SSH Telnet strategy. Clicking the **Show** button identifies the command(s) that were executed.

Application discovery

The **application discovery** stage identifies the outcome of the strategies that retrieve initial application information related to a target (e.g. the presence of an application on a target device).



ApplicationDiscovery

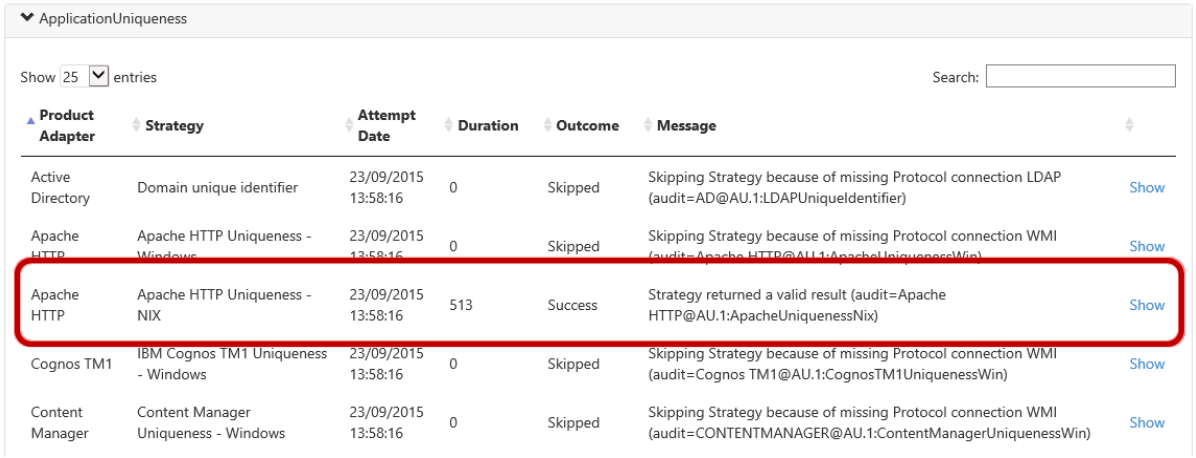
Show 25 entries Search:

Product Adapter	Strategy	Attempt Date	Duration	Outcome	Message	
Active Directory	Identifies if the current device is a domain controller	23/09/2015 14:00:57	0	Skipped	Skipping Strategy because of missing Protocol connection WMI (audit=AD@AD.1:DomainControllerDiscovery)	Show
Apache HTTP	Apache HTTP folder discovery - Windows	23/09/2015 14:00:57	0	Skipped	Skipping Strategy because of missing Protocol connection WMI (audit=Apache HTTP@AD.4:ApacheFolderWin)	Show
Cognos TM1	Cognos TM1 process discovery - NIX	23/09/2015 14:01:03	0	Success	Strategy returned a valid result (audit=Cognos TM1@AD.1:CognosTM1ProcessNIX)	Show
Cognos TM1	IBM Cognos TM1 global registry file discovery - NIX	23/09/2015 14:01:03	0	Success	Strategy returned a valid result (audit=Cognos TM1@AD.3:CognosTM1RegistryFile)	Show
Cognos TM1	IBM Cognos TM1 validation strategy	23/09/2015 14:01:03	0	Success	Strategy returned a valid result (audit=Cognos TM1@AD.10:CognosTM1Validation)	Show

The example above identifies that the Cognos TM1 product adapter successful identified application information. Clicking the **Show** button identifies the command that was executed to perform the application discovery.

Application uniqueness

The **application uniqueness** stage ensures that duplicates of an application on a target are not generated by ensuring that each application is uniquely identified using attributes associated with the application.



ApplicationUniqueness

Show 25 entries Search:

Product Adapter	Strategy	Attempt Date	Duration	Outcome	Message	
Active Directory	Domain unique identifier	23/09/2015 13:58:16	0	Skipped	Skipping Strategy because of missing Protocol connection LDAP (audit=AD@AU.1:LDAPUniqueIdentifier)	Show
Apache HTTP	Apache HTTP Uniqueness - Windows	23/09/2015 13:58:16	0	Skipped	Skipping Strategy because of missing Protocol connection WMI (audit=Apache HTTP@AU.1:ApacheUniquenessWin)	Show
Apache HTTP	Apache HTTP Uniqueness - NIX	23/09/2015 13:58:16	513	Success	Strategy returned a valid result (audit=Apache HTTP@AU.1:ApacheUniquenessNix)	Show
Cognos TM1	IBM Cognos TM1 Uniqueness - Windows	23/09/2015 13:58:16	0	Skipped	Skipping Strategy because of missing Protocol connection WMI (audit=Cognos TM1@AU.1:CognosTM1UniquenessWin)	Show
Content Manager	Content Manager Uniqueness - Windows	23/09/2015 13:58:16	0	Skipped	Skipping Strategy because of missing Protocol connection WMI (audit=CONTENTMANAGER@AU.1:ContentManagerUniquenessWin)	Show

The example above identifies that the UNIX Variant product adapter successfully retrieved application uniqueness information using the Apache HTTP Uniqueness (UNIX) strategy.

Log files

The UI is the normal method for the examination of scanning operations. A (text) log file can prove useful to remotely diagnose a scan engine problem. The log files provide a detailed list of what is happening while the scan is running. Any errors that have occurred can be found there.

The log files are broken down into two types:

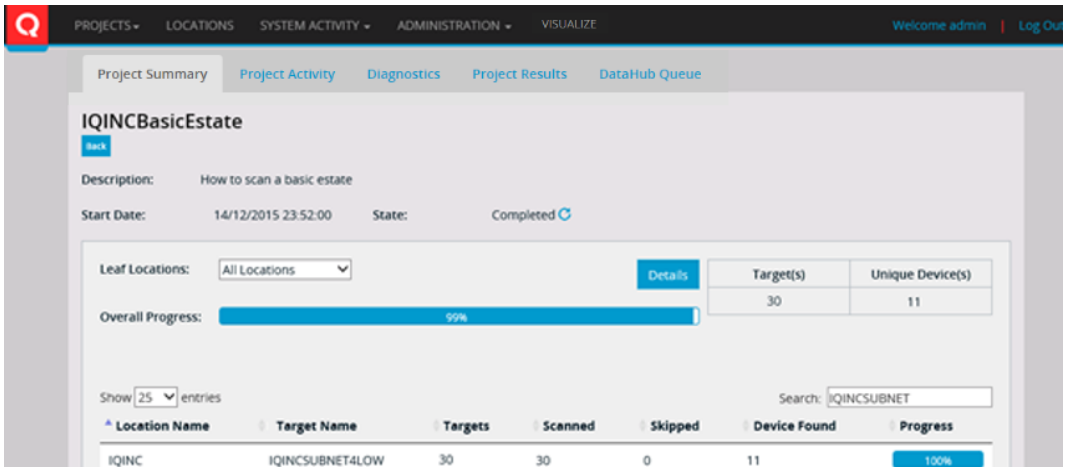
- Scan Service Logging
  - Filename: Service.log
  - Additional Overflow File Name: Service.log.N (Where is N is a number between 1 and 10).
  - The logs associated with the overall scan operation. When a file gets too large, a new file is created and the original file is renamed to service.log.N
- Individual Target Specific Logging
  - Filename: Target-W.X.Y.Z.log (Where W.X.Y.Z is an IP address of the target).
  - The logs associated with the operations applied to an individual target.

To access these log files, go to this location:

Local Disk (C:) > **\ProgramData\iQuate\iQSonar ScanEngine 4.0\Logs**

Projects status – Project summary

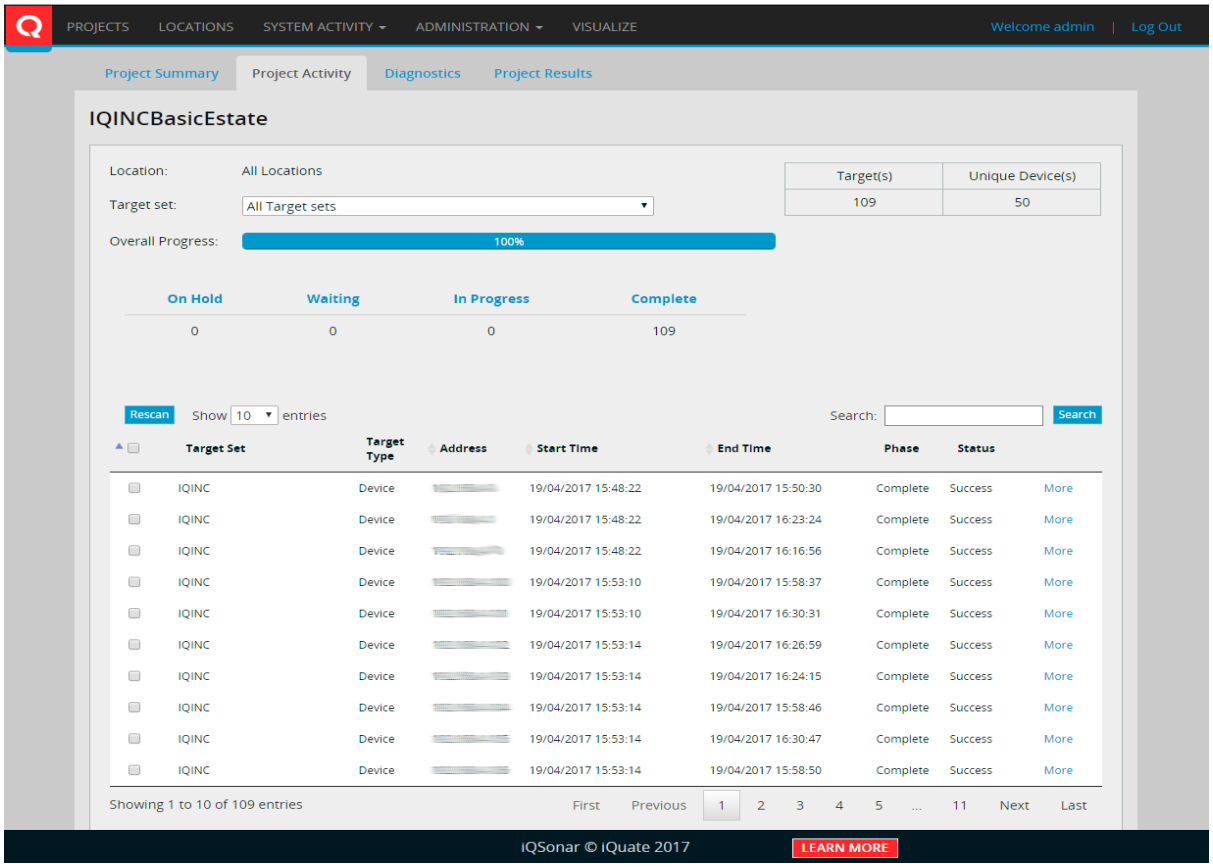
The **Project > Active Projects > Status > Project Summary** tab identifies the overall statistics of the scan project.



Projects status – Project activity

The **Project > Active Projects > Status > Project Activity** tab identifies the operations that are carried out on each IP address in the available ranges specified in the project. The overall status of the scan process is provided in the Outcome column.

Click the **Learn More** button for additional information on the scan of the device.



Projects status – Project results

The **Project > Active Projects > Status > Project Results** tab provides a breakdown of the scan results associated with each target device linked with the project. The difference between the Project Activity and Project Results dialogs is that project activity relates to all IP addresses identified within a target range; the project results only deal with items that have information associated with the IP address.

The results of the scan are broken down into four categories:

- **Found Device:** A device that was identified as a potential target for scanning.
- **Device:** A confirmed device that has been promoted to the status of a full device; this device exists and will be subject to an examination for installed applications.
- **Found Application:** The application that was identified as a potential target for scanning.
- **Application**: A confirmed application that has been promoted to the status of a full application; this application exists and is subject to an examination for installed applications.

Each category is available as a separate tab for further examination, and each provides additional action buttons:

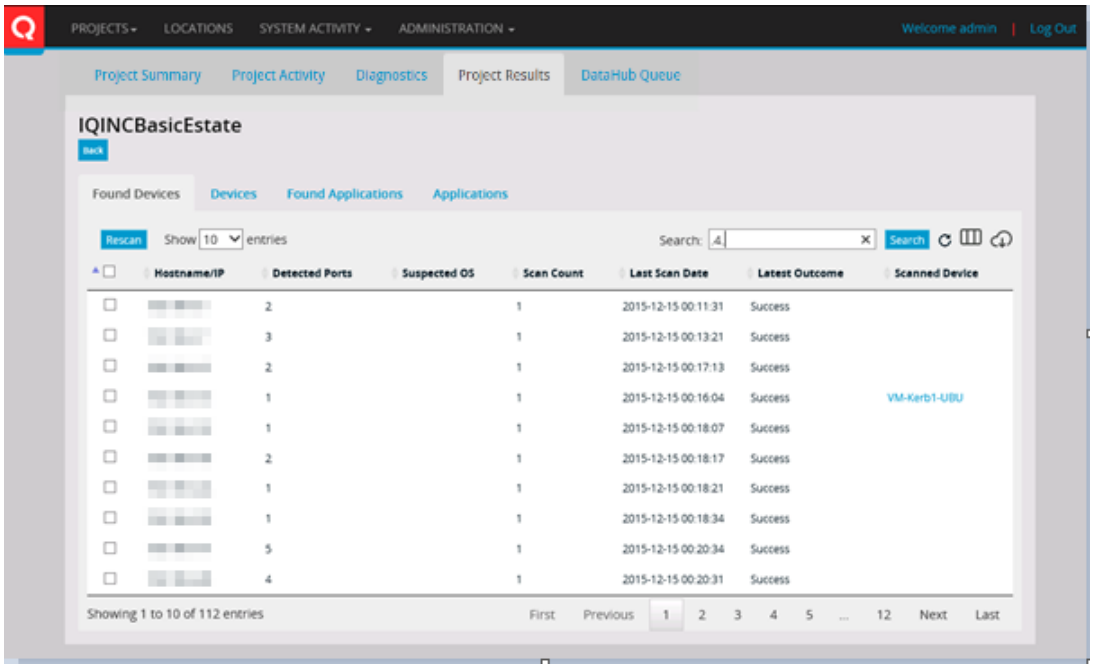
Button	Action
Search	Filter the results on a specific string value.
	Refresh the results window to get a more up-to-date list.

	(Column select) Enable or disable specific columns within the results tables.
	(Download) Save the results as a CSV file.

Found devices

This is a device that was identified as a potential target for scanning (i.e., this is more than just an IP address that forms a range of IP addresses). It's believed to exist as a real device but it is not confirmed that this device represents a device that is distinct from all other devices (uniqueness).

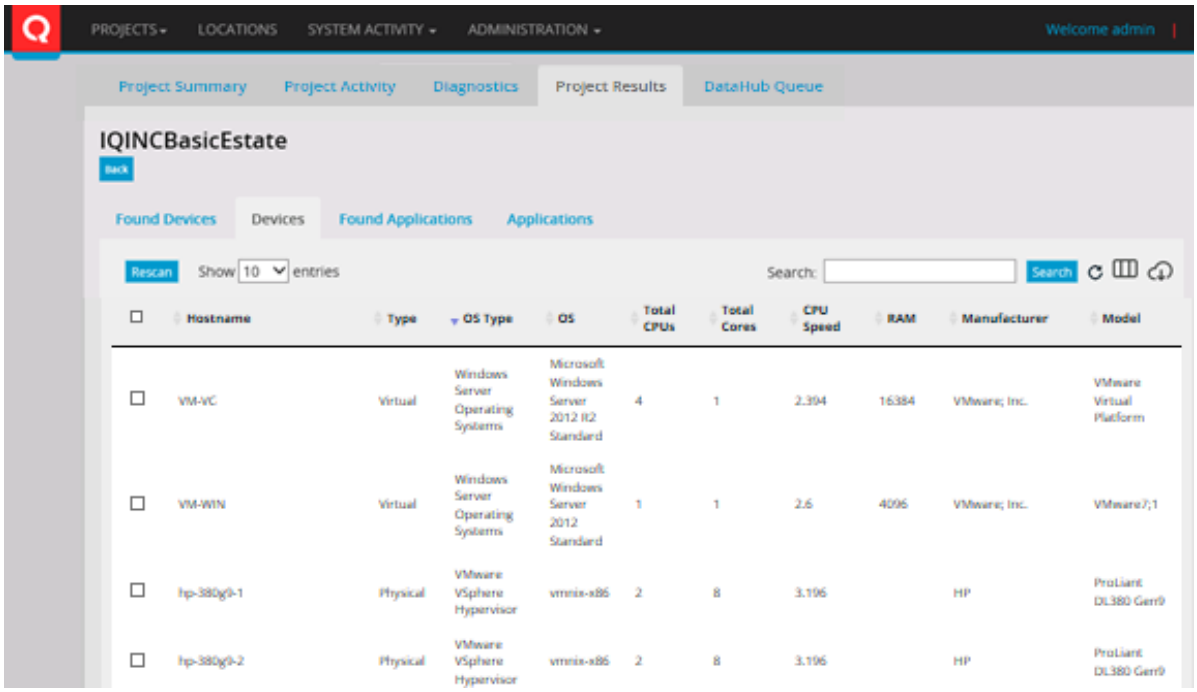
The basic information that has been identified for the device is displayed: The hostname/IP address, number of open ports on the device, suspected operating system, the number of times the device has been scanned, last scan date, last outcome of a scan operation, and finally if the device has been fully scanned (i.e., is a full device). A link to the fully scanned information is provided, which identifies the case when a found device has been promoted to device status.



Devices

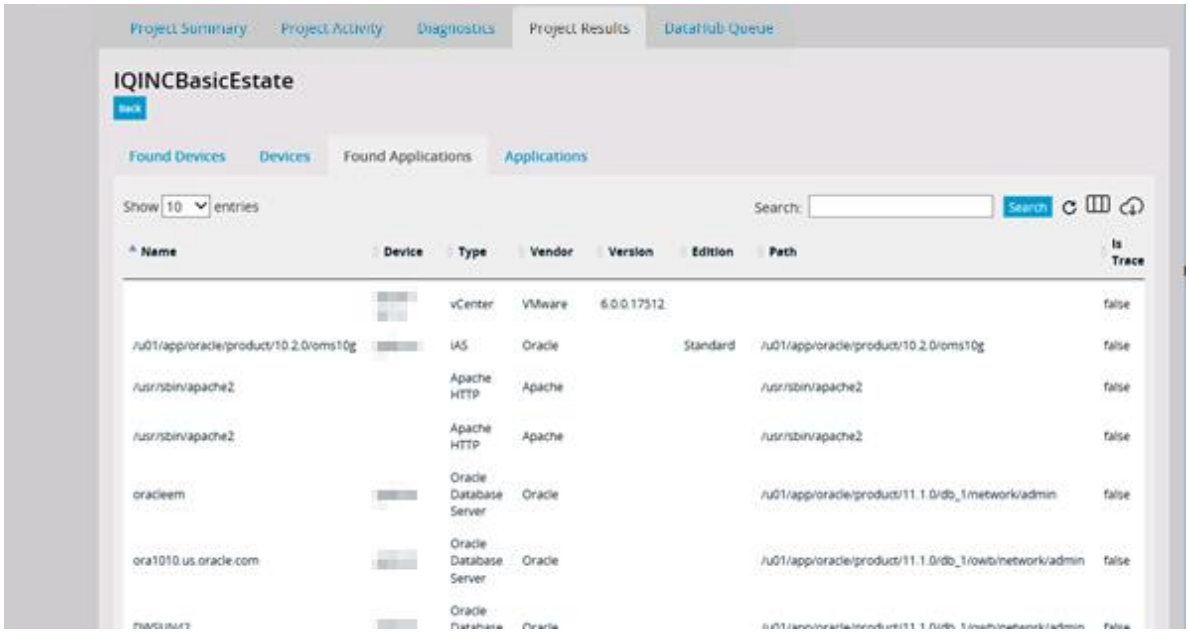
This is a successfully scanned device. This device is known to exist and will be subject to an examination for installed applications. This tab identifies the top-level hardware components of the device:

- Physical or virtual flag
- Operating system
- CPU count
- CPU speed
- RAM
- Manufacturer



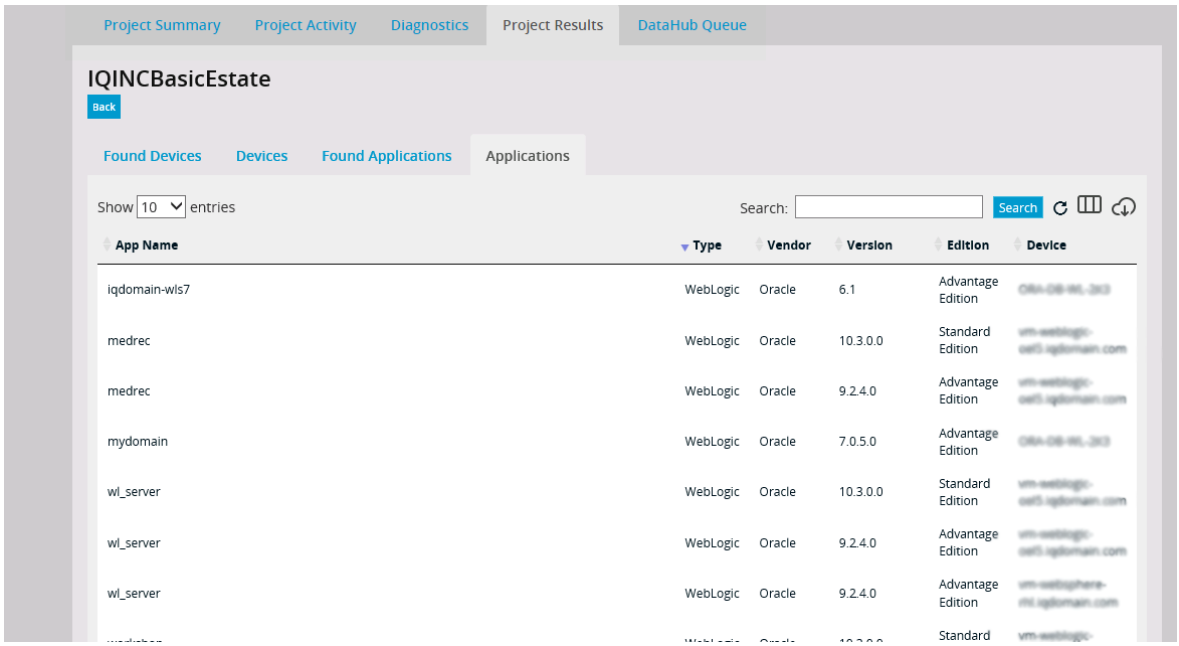
Found applications

This is an application that was identified as a potential target for scanning. It's believed to exist as a real application but it is not confirmed that this application represents an application that is distinct from all other applications (uniqueness).



Applications

This is a successfully scanned application that represents an application distinct from all other applications (based on uniqueness).

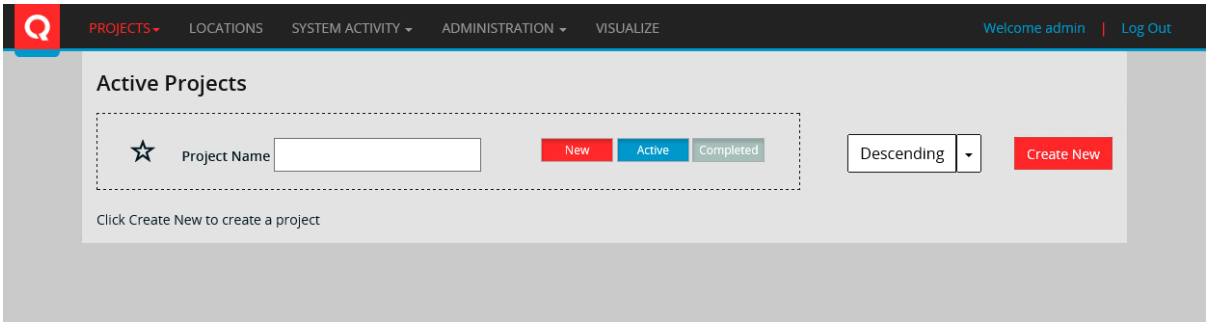


Project status – Diagnostics

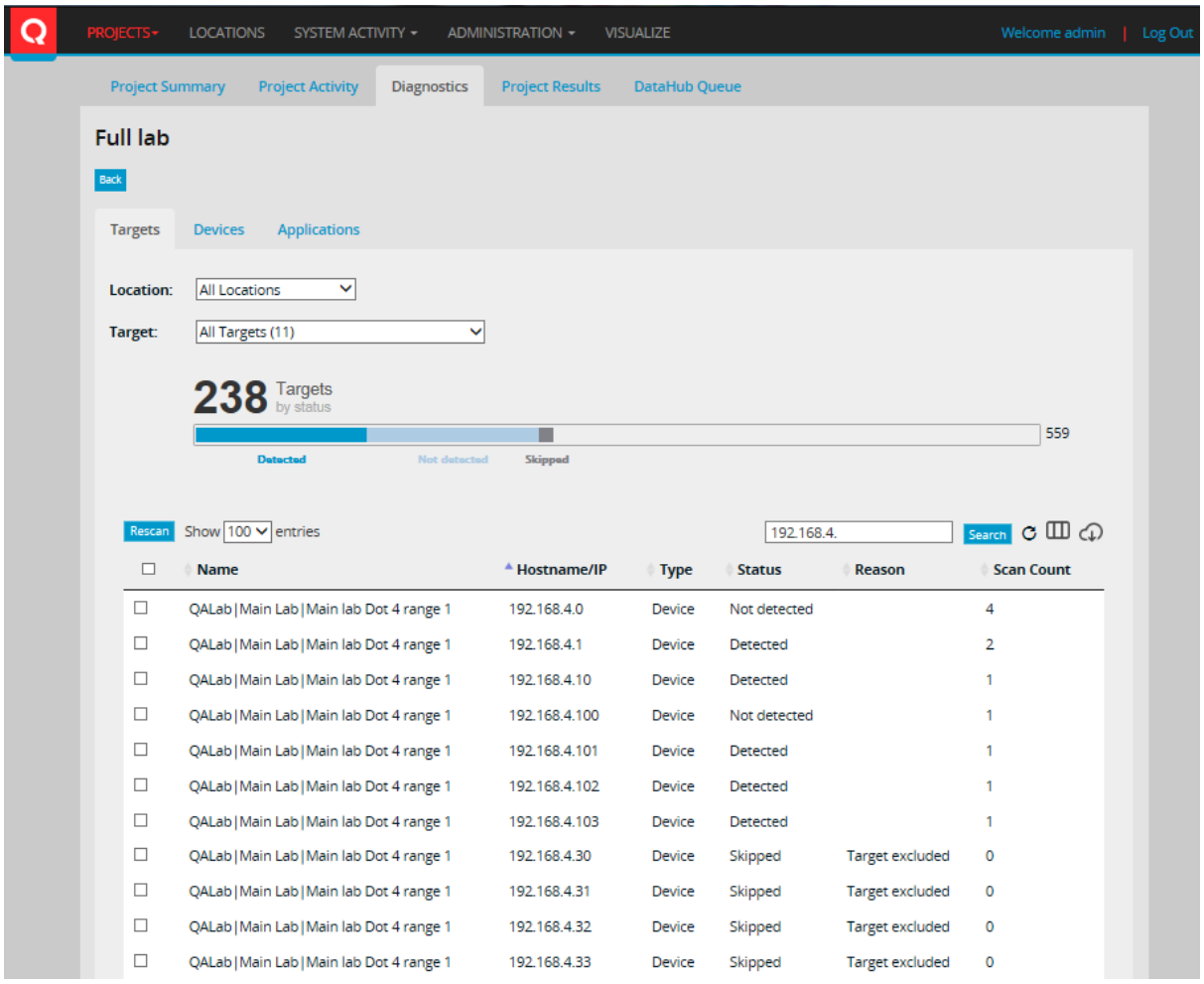
If you want to see a page that summarizes the results of target scans, do so on the Diagnostics page.

To diagnose a project

1. Click the **Projects** drop-down menu at the top of any page, and select **Active Projects**.
2. On the resulting Projects page, choose the project you want to diagnose, and click its **Status** button.



3. Click the **Diagnostics** tab near the top of the page.



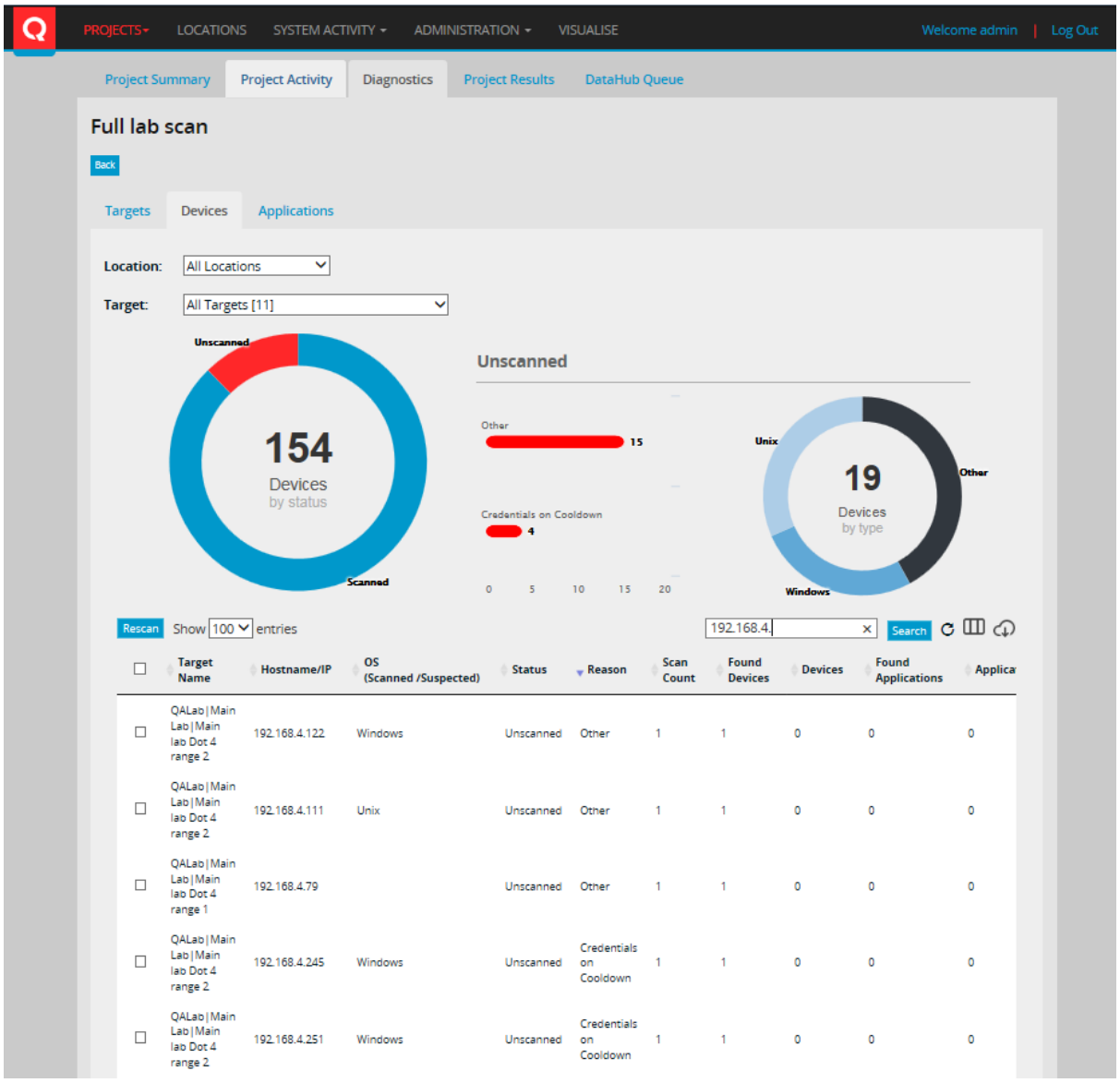
Note the three tabs: **Targets, Devices** and **Applications**. All three tabs have a Location field and a Target field to enable you to filter the available data. Updating either of these fields refreshes the data below them (charts and data table). The Location field displays the same list of Leaf Locations as is seen in the drop-down on the Project Summary page. None of these tabs will display any rows before scanning has commenced.

The **Targets tab** summarizes the targets that were attempted to be scanned and identifies whether they were detected or not detected during the scan. It's populated (currently) from the history.v_DiagnosticsTargetList DB view. The items on this tab that are detected are then covered in more detail on the Devices tab (i.e., whether or not they were scanned). The bar chart on the Targets tab is populated from the history.v_DiagnosticsTargetsChart DB view.

If a target is rescanned, it's removed from the chart and the data table when it's submitted for rescanning, and only reappears on both on completion of the second scan.

If a target is excluded, then the **Diagnostics Targets** tab will show a status of **Skipped** and a Reason of **Target excluded**. If the target is then included, the Status and Reason fields will not update on the Diagnostics Targets tab until the target is rescanned.

The **Devices tab** summarizes the results of device target scans:



The charts give you an overview of the scan results and can be used to drill down further into particular categories by clicking the various elements.

Chart 1 (the pie chart on the left) is the Status chart, which tells you how many scanned and unscanned results there are. The table below can be filtered by clicking on a slice.

The Unscanned section on the right shows further details for the unscanned devices:

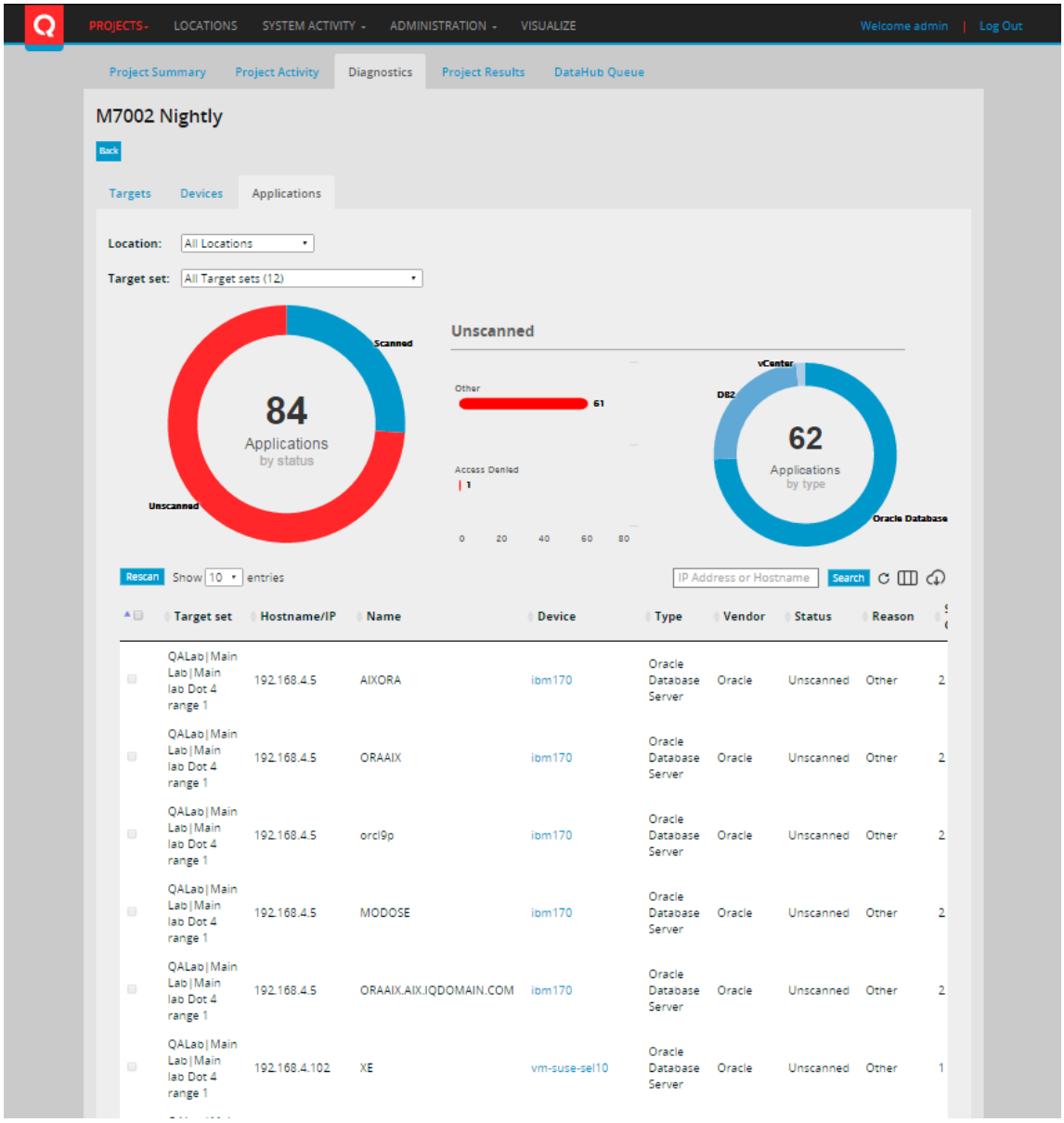
- Chart 2 (the bar chart) is the Reasons chart and gives the reasons for unsuccessful scans. You can click on each reason bar in this chart to filter the results based on this reason. The two pie charts will change to show only these devices, and the table below will be filtered also.
- Chart 3 (the pie chart on the right) is the Type chart and gives the suspected OS of the unscanned devices. You can click on this chart to filter the results, filtering the other two charts and the table below.

The table at the bottom of the page summarizes the scan results for each individual target. This table lists all the targets that a scan has been attempted on and summarizes how the scan went.

Things to note are:

- The Status column tells you whether the target has been scanned or is unscanned. If a target hasn't been detected, then this information will be displayed on the Targets tab.
- The OS (Scanned/Suspected) column shows you either the suspected OS if the target is unscanned, or the scanned OS if it has been scanned.
- The Reason column gives the reason a target was not scanned
- Scan Count gives the number of times a target has been scanned.
- There are also columns that show how many Found Devices, Devices, Found Applications, and Applications have been found as part of the scan.
- The More link will take you to the Device details page in the case of scanned rows, or the Found Device details page in the case of unscanned rows.

The **Applications tab** gives the same type of summary for applications.



Differences from the Devices tab to note are:

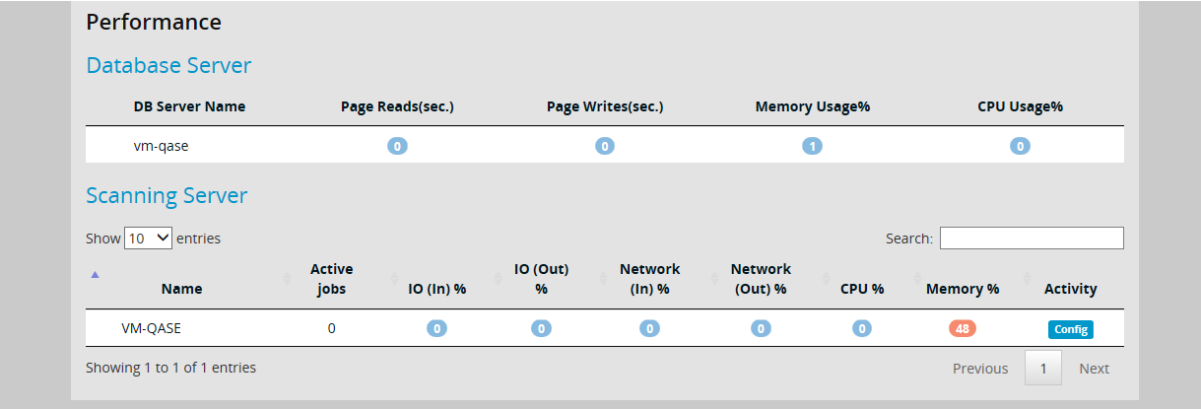
- The suspected OS chart instead shows the different applications.
- If the application was scanned as part of a device scan, the Device column shows a link to the Device details page of the device the application was found on.

System activity

The **System Activity** section of the dashboard provides a means to assess the current running activity of the scan engine and its associated components.

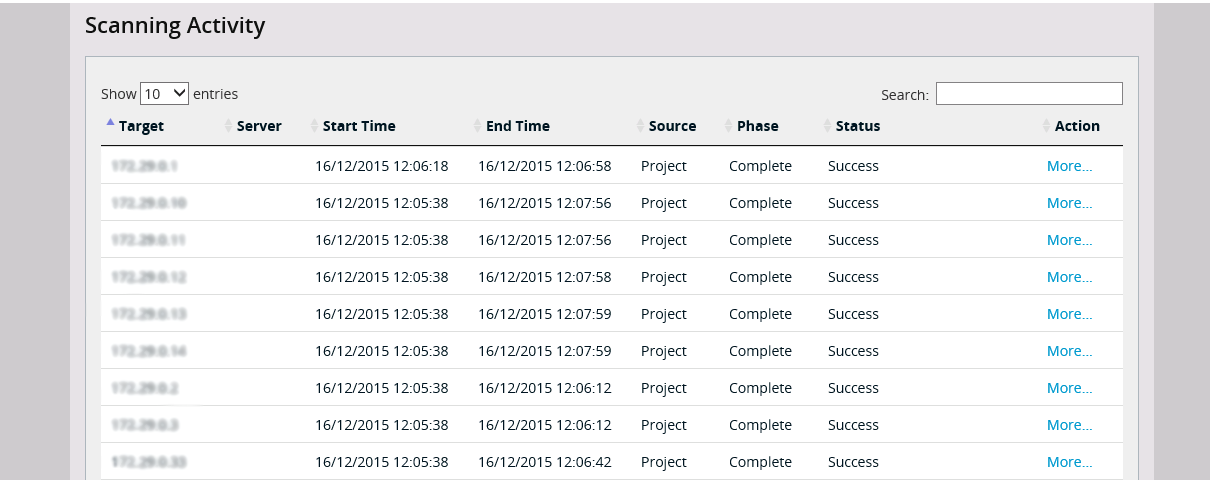
System performance

The **System Performance** tab provides general statistics on the scan engines under the control of the dashboard. Since the dashboard is composed of a backend database that stores scan data and one or more scan engines, the system performance is broken into these two sections. Statistics are provided on current I/O rates, memory usage, CPU, etc.



Scanning activity

The **Scanning Activity** tab provides in-depth feedback on the scanning operations run against each of the targets identified in the scanning ranges (not just the active devices in the ranges). Each row of the table identifies a single target.

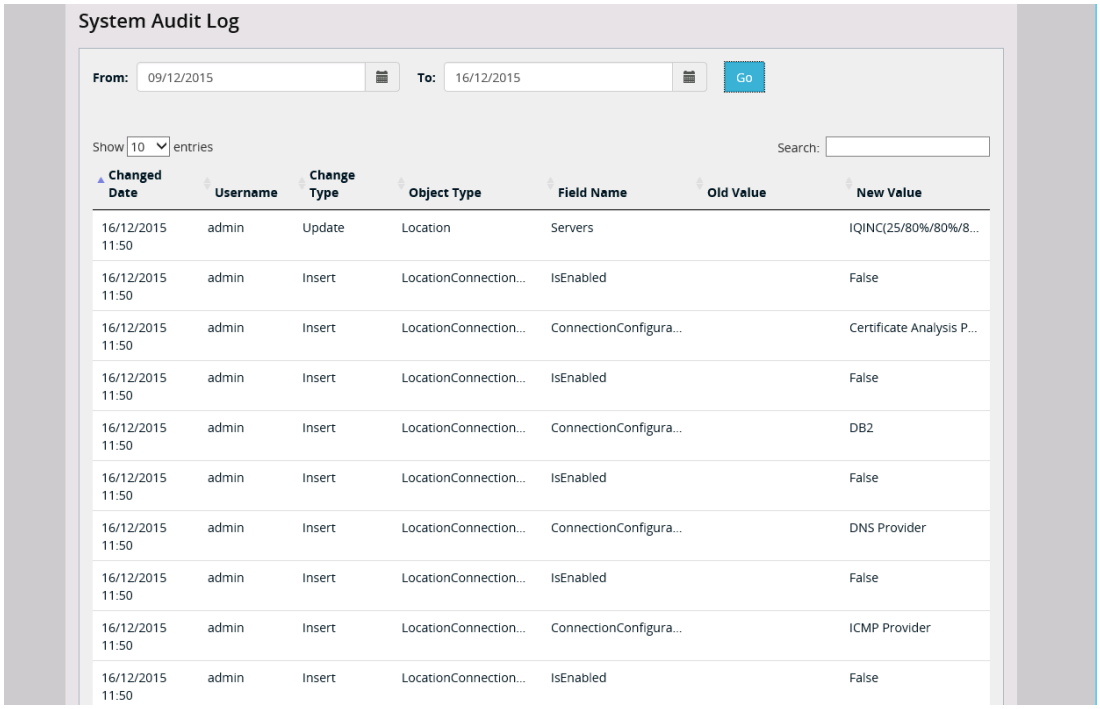


The search field allows a list of targets to be restricted. This search field is “freeform,” that is, a value of **0.1** will identify targets such as 192.2.0.1, 192.3.0.10, 192.4.0.11, etc.

> **Note:** Additional information on any target row can be identified by clicking the **More…** button.

System audit log

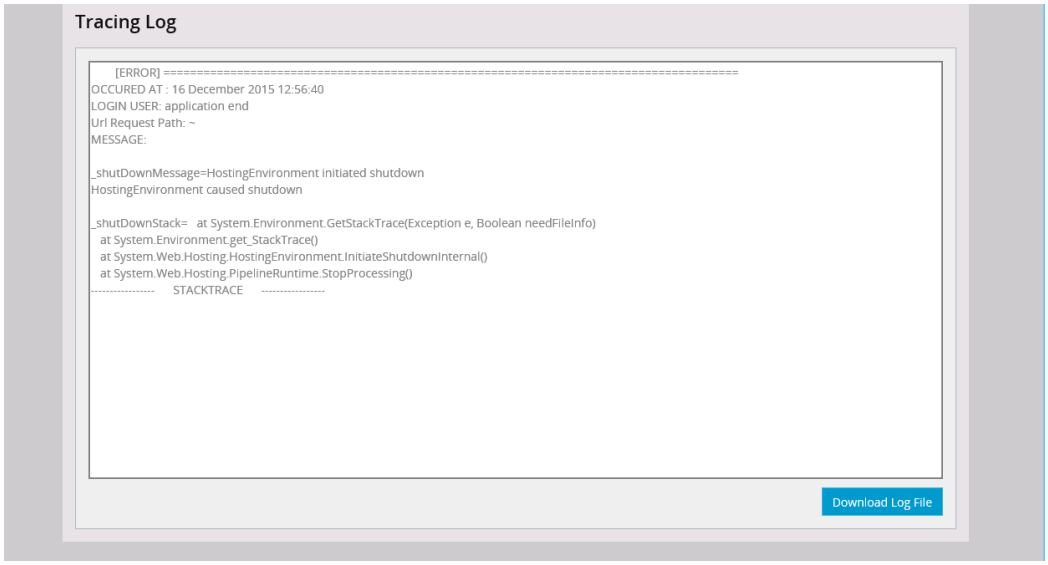
The system audit log enables you to track all major modifications made to the scan-engine configuration. The audit log tracks the modifications down to the individual configuration attributes within the configuration setup. A search option enables you to retrieve modifications in specific area(s). Click the Go button to retrieve the audit log entries for the time period specified.



Tracing log

The tracing log is provided for dashboard diagnostics. If errors occur within the dashboard, information identified within this tab will be requested by Ivanti support to aid in further analysis.

You can download the log to the local device using the **Download Log File** button.



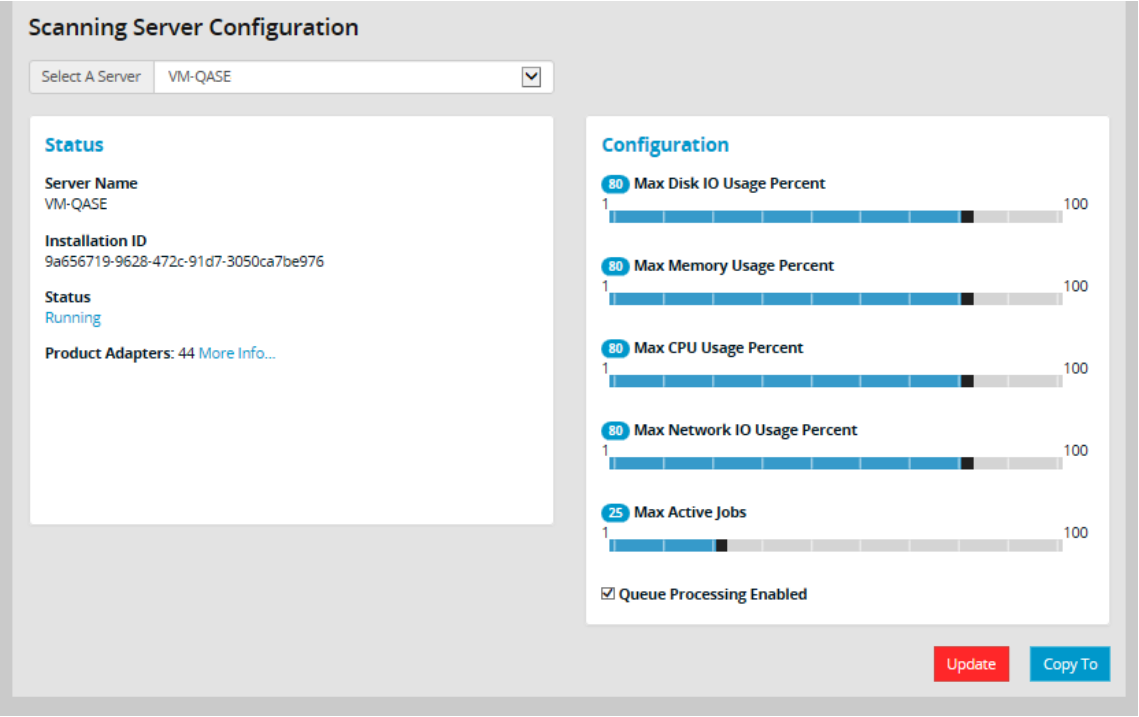
Administration

Administration of the scan engine enables you to establish global settings for the scanning process.

Scanning servers

A single dashboard can support multiple servers. To access a scanning server's configuration details, select a server from the drop-down list.

You can configure these items, which are intended to provide a form of system "throttling" to ensure that system resources are not overloaded on the scan-engine server.



- **Max Disk IO Usage Percent**: Identifies the percentage of the available disk I/O to be used by the scan engine before throttling is applied.
- **Max Memory Usage Percent**: Establishes the percentage of the available memory to be used by the scan engine before throttling is applied.
- **Max CPU Usage Percent**: Establishes the percentage of the available CPU to be used by the scan engine before throttling is applied.
- **Max Network IO Usage Percent**: Establishes the percentage of the available network I/O to be used by the scan engine before throttling is applied.
- **Max Active Jobs**: The maximum number of scanning jobs that will be held as active within the scan engine. If the current number of jobs is higher than this value, then no additional jobs will be requested.
- **Queue Processing Enabled**: If this option is disabled, the scan engine will not request any jobs (scanning operations will be suspended).

The disk I/O, memory, CPU, and network I/O usage of the scanning server is constantly monitored. If, at any point, the average value over 5 minutes for one or more of these metrics exceeds the configured limit, the scanning server will stop serving additional jobs.

Job serving will resume when average values (over 5 minutes) for all metrics fall below the configured levels. Although serving of new jobs will be paused, existing jobs will run to completion and will continue to consume resources. In some cases, depending on the complexity and breadth of the jobs in progress, the level of resource usage may be sustained and in some cases may increase.

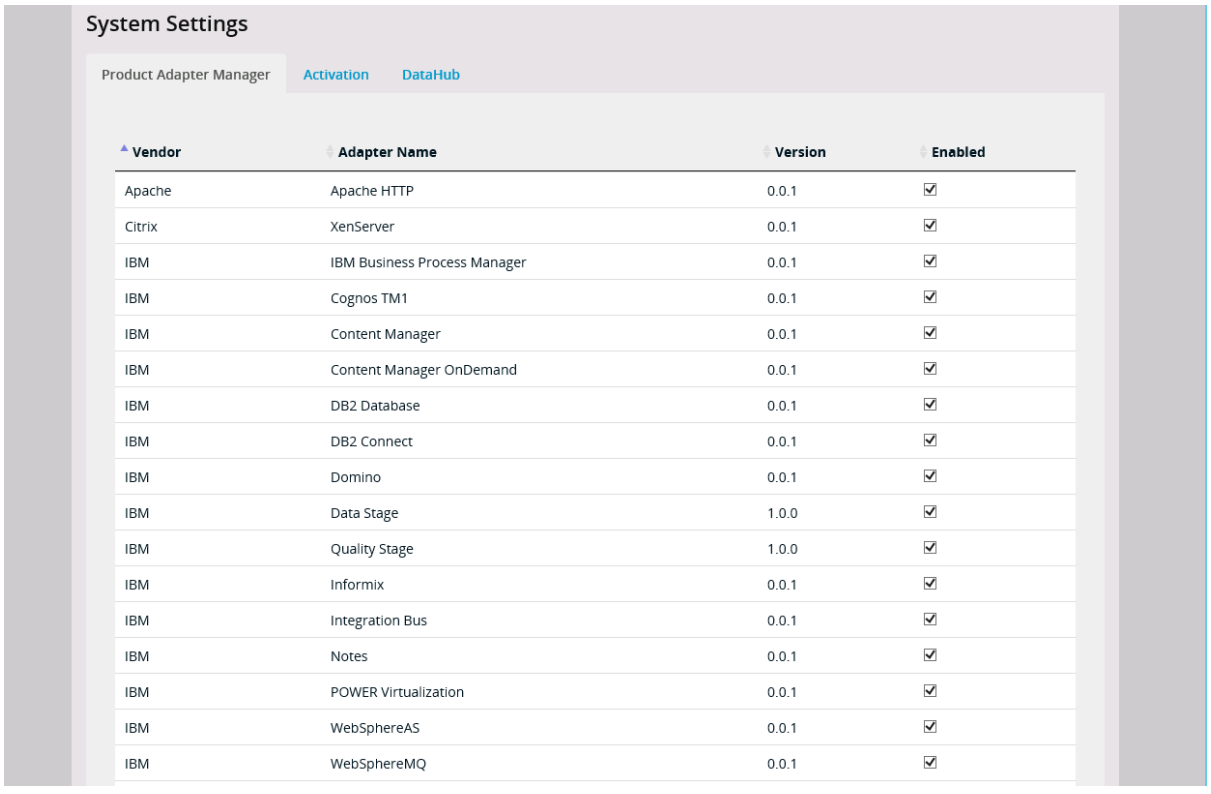
System settings

System settings cover all aspects of the scanning process. All scan engines associated with this dashboard are governed by these settings (i.e., the settings have global implications).

System settings – Product adapter manager

This tab provides the ability to enable and disable product adapters across an entire scan estate. This global setting affects all locations and projects that attempt to use a specific product adapter.

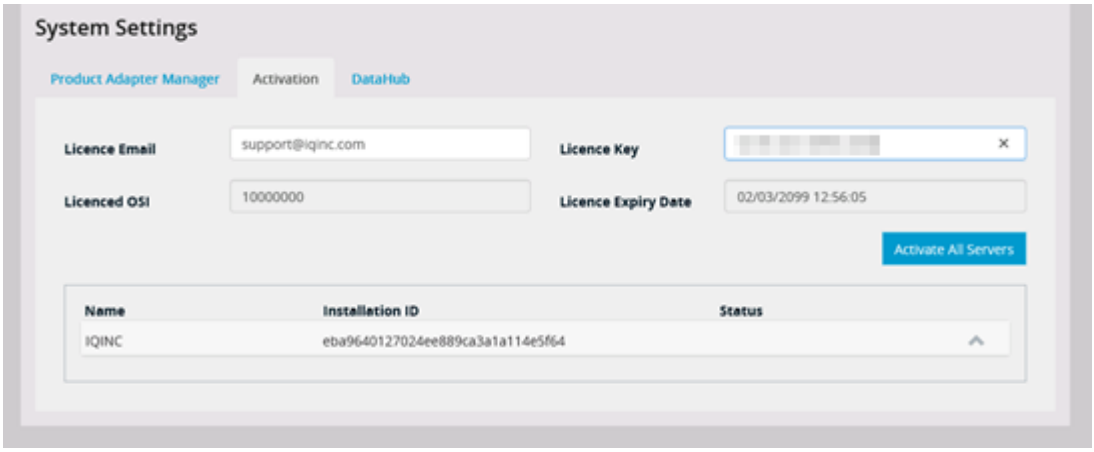
A product adapter can be disabled for a number of reasons. The primary reason would be that a specific product is not present in an estate; attempting to locate the product wastes scanning resources.



Vendor	Adapter Name	Version	Enabled
Apache	Apache HTTP	0.0.1	☑
Citrix	XenServer	0.0.1	☑
IBM	IBM Business Process Manager	0.0.1	☑
IBM	Cognos TM1	0.0.1	☑
IBM	Content Manager	0.0.1	☑
IBM	Content Manager OnDemand	0.0.1	☑
IBM	DB2 Database	0.0.1	☑
IBM	DB2 Connect	0.0.1	☑
IBM	Domino	0.0.1	☑
IBM	Data Stage	1.0.0	☑
IBM	Quality Stage	1.0.0	☑
IBM	Informix	0.0.1	☑
IBM	Integration Bus	0.0.1	☑
IBM	Notes	0.0.1	☑
IBM	POWER Virtualization	0.0.1	☑
IBM	WebSphereAS	0.0.1	☑
IBM	WebSphereMQ	0.0.1	☑

System settings – Activation

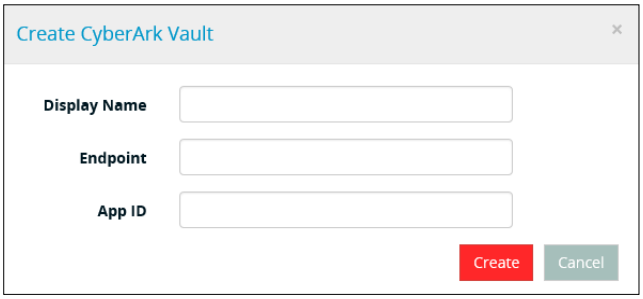
Accessing the scanning service requires an activation license. This license is provided by Ivanti support or through an online activation website.



Provide the license email and license key values and click the **Activate All Servers** button. Projects can now be allowed to execute.

System settings – CyberArk

You can configure the scan engine to retrieve credential passwords and (optionally) usernames from CyberArk. This screen allows the registration of one or more CyberArk vaults.



The display name is a label used in the Credentials screen to distinguish between multiple vault setups.

The endpoint is the URL of the Cyberark Application Identity Manager Central Credential Manager Web Service. This is typically **http://<Address>/AIMWebService/V1.1/AIM.asmx**

The App ID is the name of the application account set up for the scan engine to use.

See the **Scan Engine Prerequisites Guide** for CyberArk prerequisite details.

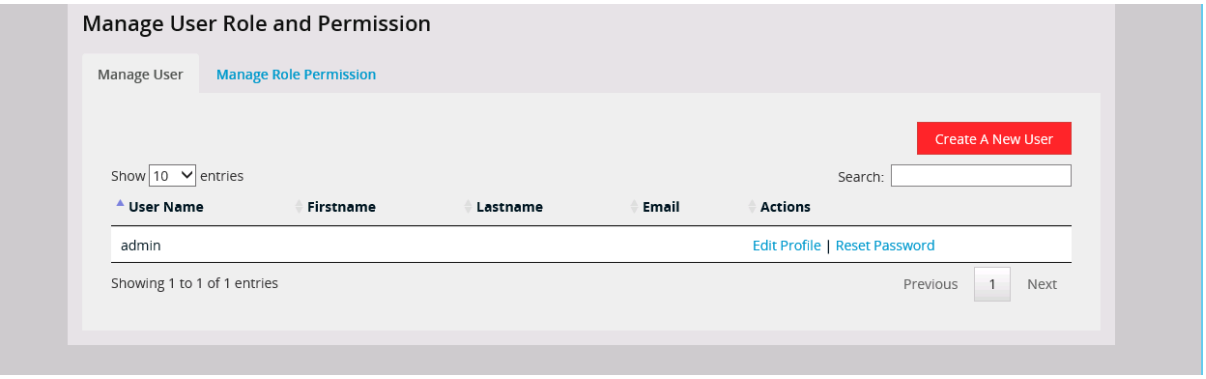
User settings

The User Settings options enable you to create, delete, and edit existing and new user identities. The scan engine supports the use of locally managed or Active Directory user accounts. In addition, you can assign roles to users that apply a scope limiting the operations allowed.

User settings – Manage user (local)

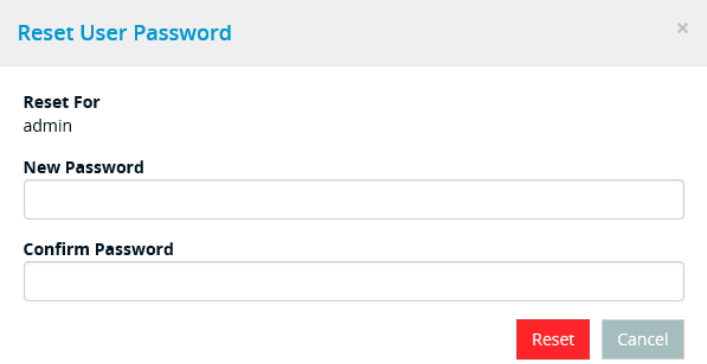
This tab provides the ability to create and modify users associated with the dashboard. By default, an installation provides a single user called **admin** with a password of **password**.

For additional security, it's recommended that you reset the default password for the admin user.



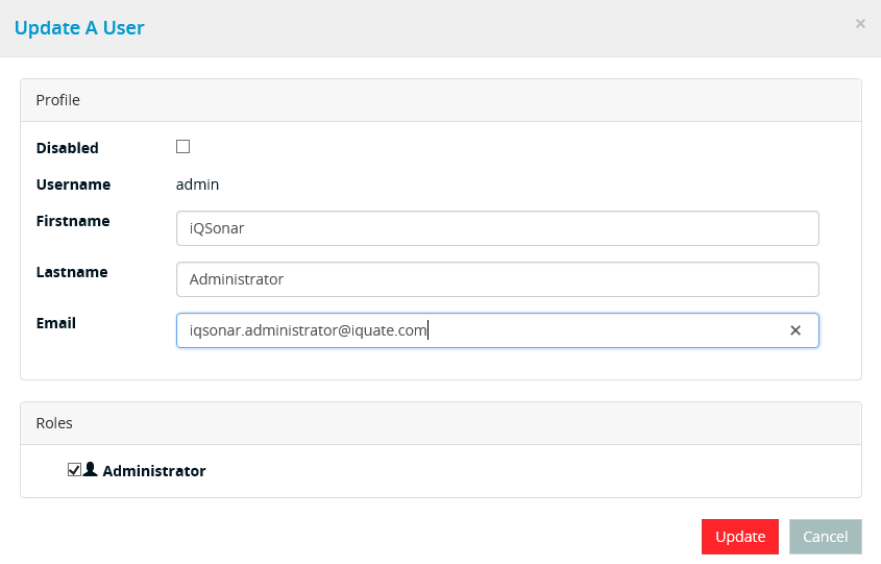
To change the password

1. Click the **Reset Password** button.
2. Provide the new password.
3. Click the **Update** button.



To edit the profile

1. Select the admin user.
2. Click the **Edit Profile** option.
3. Provide a First Name for the administrator.
4. Provide a Last Name for the administrator.
5. Provide an email address for the administrator.
6. Click **Update** to save new information.

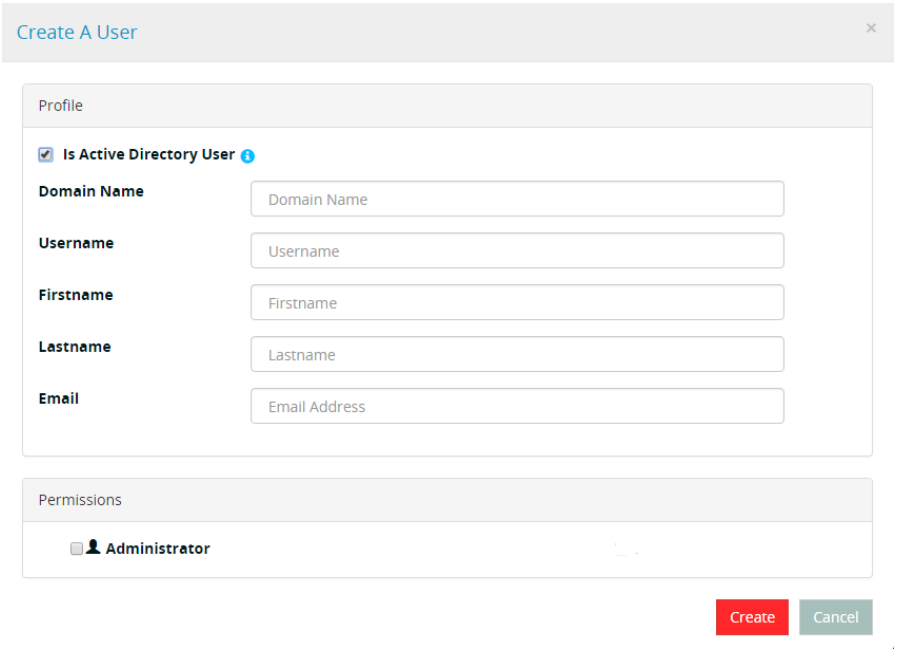


User settings – Manage user (Active Directory)

The scan engine also supports the use of Windows accounts to access the dashboard. Unless it was explicitly enabled during installation, Active Directory authentication is disabled by default. To use Active Directory accounts where this option was *not* selected at installation, it's necessary to configure IIS to allow Windows Authentication.

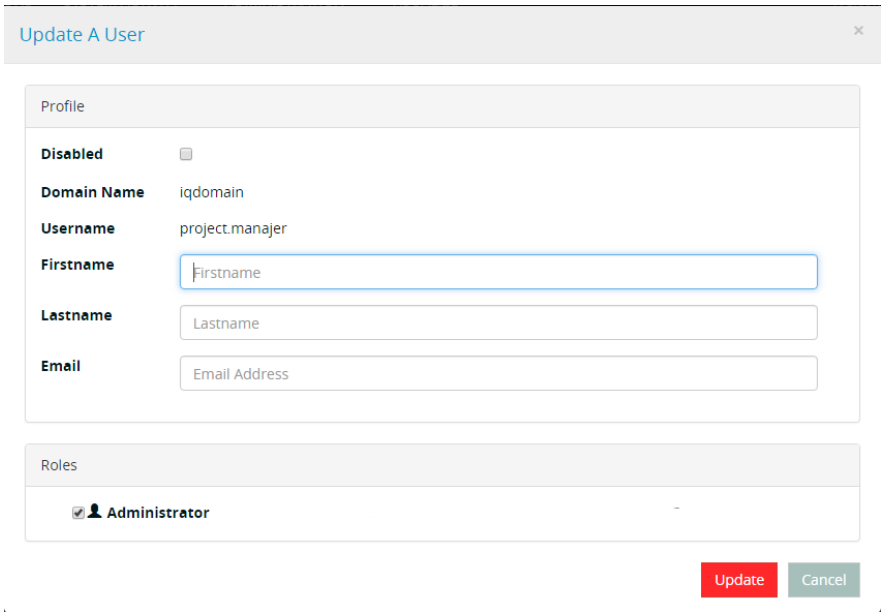
To create a user

1. Select the **Is Active Directory User** option.
2. Provide the Domain Name.
3. Provide the User Name.
4. Provide the First Name (optional).
5. Provide the Last Name (optional).
6. Provide the Email (optional).
7. Select the Permissions.



To edit the profile

1. Select the AD user that needs to be modified.
2. Click the **Edit Profile** option.
3. Made the corresponding changes.
4. Click **Update** to save new information.

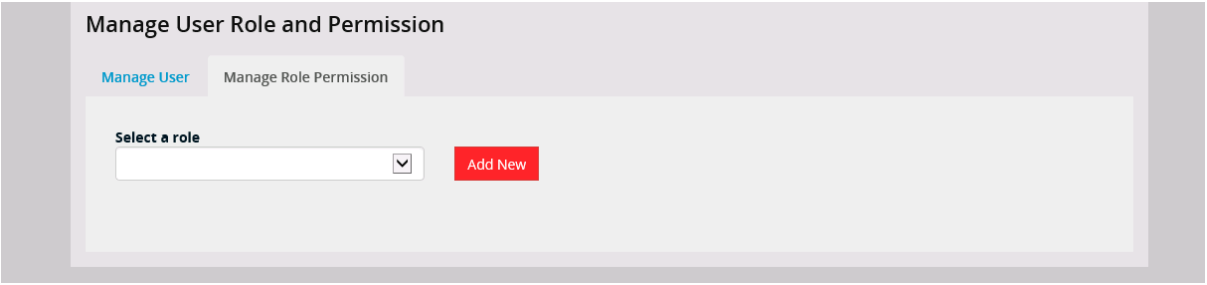


User settings – Manage role permission

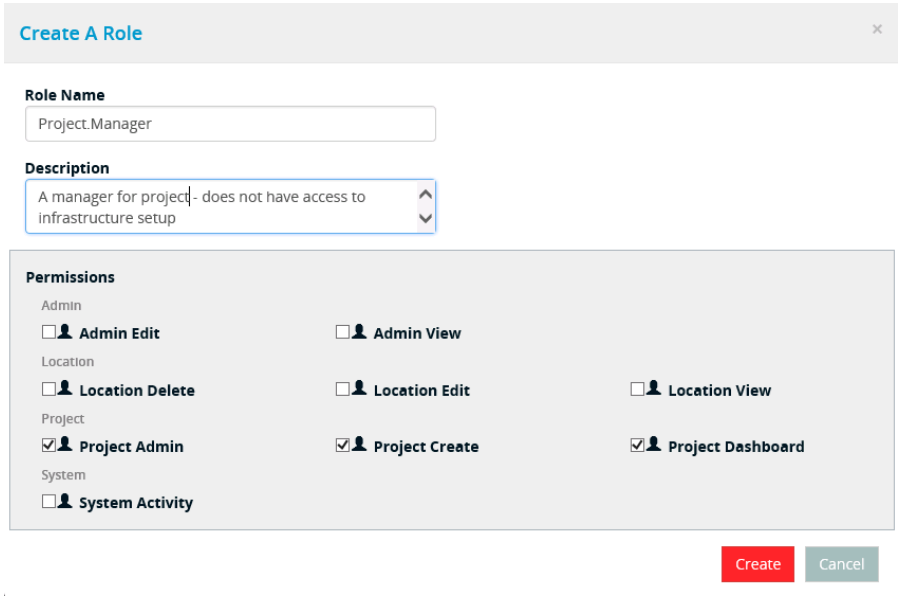
Roles allow for subsets of the functionality (provided by the dashboard) to be enabled or disabled on a per-user basis. This process also ties in with the creation of users described in the previous section. You can define a role that limits the dashboard functionality. Users can then be assigned this role and thereby acquire specific privileges.

To create a role with permissions

1. Click **Add New** button to create a new role.



2. Provide a role name, such as Project.Manager.
3. Provide a description of the role.
4. Select permissions for the role, such as Project Administrator permissions.
5. Click **Create** to save the role.
6. Assign a role to a user under the **Manage User** Tab. This is covered in the use-cases examples provided in this document.


Create A Role
Role Name
Project.Manager
Description
A manager for project - does not have access to infrastructure setup
Permissions
Admin
Admin Edit
Admin View
Location
Location Delete
Location Edit
Location View
Project
Project Admin
Project Create
Project Dashboard
System
System Activity
Create
Cancel

Appendix A: Key terms, emails, and links

Term	Description
CSV	Comma-separated values
IIS	Internet Information Services
Ivanti support	https://www.ivanti.com/support/ivanti-support
Microsoft support for KB932370	http://support.microsoft.com/kb/932370
NETSTAT	A command on the command prompt to access ports.
Oracle Licensing Management Services (LMS)	Oracle LMS is an organization that promotes the management, governance, and awareness of the proper use and distribution for Oracle systems through expert services. *as defined by Oracle
Oracle Rac	Real Application Cluster
Partitioning (Hard)	Hard partitioning physically segments a server and separates it into distinct smaller systems, typically with its own CPUs, operating system, separate boot area, memory, input/output subsystem, and network resources. *as defined by Oracle
Partitioning (Soft)	Soft partitioning segments the operating system using OS resource managers. The operating system limits the number of CPUs where an Oracle database is running by creating areas where CPU resources are allocated to applications within the same operating system. *as defined by Oracle
PS Command	A command on UNIX boxes to display active processes.
Remote Registry	Allows Windows authenticated users to remotely modify registry settings on a device.
SID	Security identifier
WMI	Windows Management Instrumentation