



# Data Center Discovery v4.6.1.269

---

SCAN ENGINE USER GUIDE

---

## Contents

Introduction .....	6
About the Data Center Discovery scan engine.....	7
Installation instructions .....	8
Accessing the configuration user interface – “dashboard” .....	8
How the Data Center Discovery scan engine works .....	8
Initial login.....	10
User interface.....	10
Change Admin password .....	11
Active Directory and application users.....	11
Active Directory login .....	12
How to start .....	13
System settings – activation.....	13
Setting up the scan .....	13
Use case 1 – Basic estate .....	15
Basic estate - Responsibility & ownership.....	15
Basic estate - Locations .....	16
Basic estate - Scan Windows .....	17
Basic estate - Target Sets.....	17
Basic estate - Direct application scanning.....	18
Basic estate - Bulk-load of targets.....	19
Basic estate – Connections.....	20
Basic estate - NavisphereCLI connection.....	20
Basic estate - SSH connection.....	21
Basic estate - SSHProxy connection.....	21
Basic estate - Product adapters.....	22
Basic estate - System credentials .....	23
Basic estate - Application credentials .....	25
Basic estate - Project .....	27
Users tab.....	28
Locations tab.....	28
Product Adapters tab.....	28
Target Sets tab .....	28
Credentials tab.....	29

Basic estate - Start scan .....	29
Basic estate - Status.....	30
Basic estate - Mark scan as complete.....	30
Basic estate - Mark scan as archived .....	31
Use case 2 - Multi-departmental estate .....	32
Multi-departmental estate – Personnel expectations .....	32
Summary.....	32
Multi-departmental estate – Network infrastructure.....	32
Multi-departmental estate – Responsibility & ownership .....	33
Multi-departmental estate – Top-level location .....	34
Multi-departmental estate – Country-level location .....	34
Multi-departmental estate – Scan Windows .....	35
Multi-departmental estate – Targets .....	35
Multi-departmental estate – Connections.....	38
Multi-departmental estate – NavisphereCLI connection .....	38
Multi-departmental estate – Product adapters.....	39
Multi-departmental estate – System credentials .....	40
Multi-departmental estate – Global system credential .....	41
Multi-departmental estate – Application credentials.....	42
Multi-departmental estate – Americas application credentials.....	43
Multi-departmental estate – EMEA application credentials .....	45
Multi-departmental estate – User roles.....	47
Create roles.....	47
Create users.....	47
Multi-Departmental Estate – Project EMEA.....	49
Users tab.....	49
Locations tab.....	50
Product Adapters tab.....	50
Target Sets tab .....	50
Credentials tab.....	51
Multi-departmental estate – Project Americas.....	51
Users tab.....	52
Locations tab.....	52
Product Adapters tab.....	52
Target Sets tab .....	52
Credentials tab.....	53

Multi-departmental estate – Operations .....	53
Multi-departmental estate – Start EMEA scan.....	53
Multi-departmental estate – Start Americas scan.....	54
Multi-departmental estate – Status Americas scan .....	54
Multi-departmental estate – Status EMEA scan.....	55
Multi-departmental estate – Americas mark scan as complete .....	55
Multi-departmental estate – EMEA mark scan as complete.....	55
Use case 3 – Complex estate .....	57
Complex estate – Personnel expectations .....	57
Summary.....	57
Complex estate – Network infrastructure.....	57
Complex estate – Responsibility & ownership.....	58
Installation of primary and secondary scan engine .....	59
Complex estate – Top-level location .....	59
Complex estate – Country-level location .....	60
Complex estate – Scan Windows .....	61
Complex estate - Configurations .....	63
Project scan analysis .....	65
Project summary .....	65
Project diagnostics target – No credential(s) attempt .....	66
Project diagnostics target – Valid credential.....	67
Log files.....	72
Projects status – Project summary.....	72
Projects status – Project results .....	72
Found devices .....	73
Devices.....	73
Found applications.....	74
Applications .....	75
Project reports .....	75
Project status – Diagnostics .....	75
System activity .....	79
System performance .....	79
Scanning activity.....	79
System audit log .....	79
Tracing log .....	80
Administration .....	81

Scanning servers.....	81
System settings.....	82
System settings – Product adapter manager.....	82
System settings – Activation.....	82
System settings – CyberArk .....	83
User settings.....	83
User settings – Manage user (local) .....	83
User settings – Manage user (Active Directory) .....	85
User settings – Manage role permission .....	86
Configuration settings .....	87
Configuration settings - Job serving .....	87
Configuration settings - Scanning.....	87
Appendix A: Key terms, emails, and links .....	88

**Copyright notice**

This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as “Ivanti”), and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit [www.ivanti.com](http://www.ivanti.com).

Copyright © 2018, Ivanti. All rights reserved.

Ivanti and its logos are registered trademarks or trademarks of Ivanti, Inc. and its affiliates in the United States and/or other countries. Other brands and names may be claimed as the property of others.

Protected by patents, see <http://www.ivanti.com/patents>

Rev 03/18

## Introduction

This user guide provides all the information you need to operate the Ivanti Data Center Discovery scan engine through its dashboard UI. 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 retrieve relevant data from an estate in a secure manner.

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 *Data Center Discovery—Scan Engine Security Guide*.

## Installation instructions

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

## Accessing the configuration user interface – “dashboard”

The scan engine interface is web based, so it’s 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:

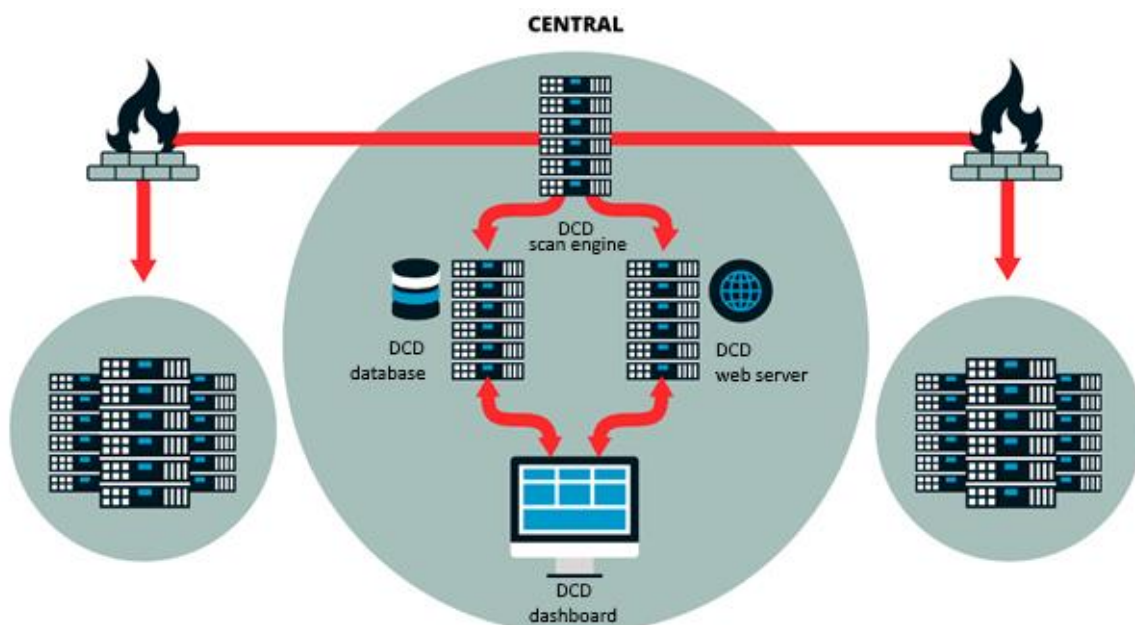
**`http://{hostname}/{uipath}`**

The **hostname** 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 page exists for the dashboard. Access to the dashboard is provided with the defaults of:

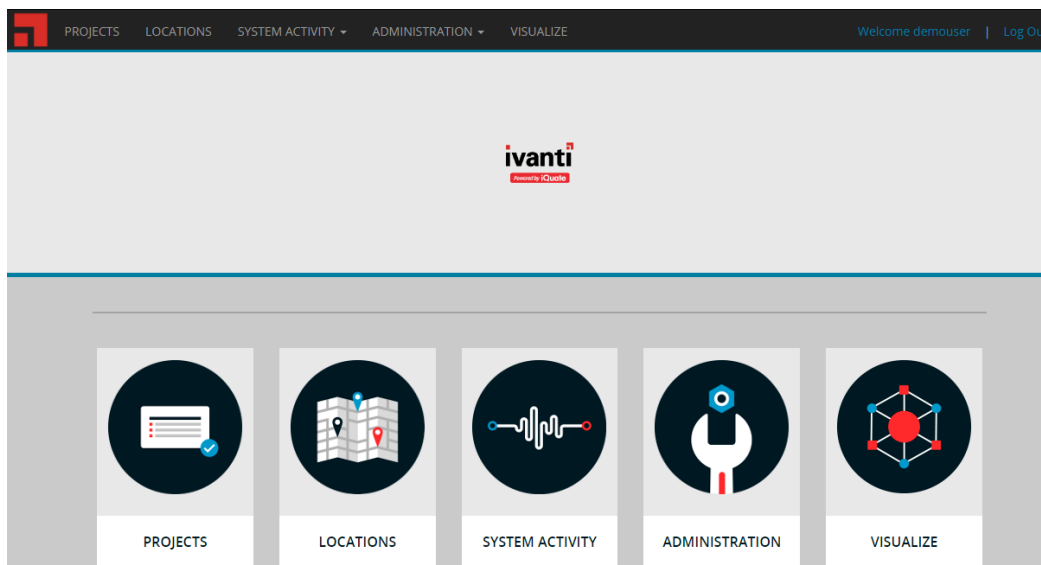
- **Username:** Admin
- **Password:** password

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 displays. 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.



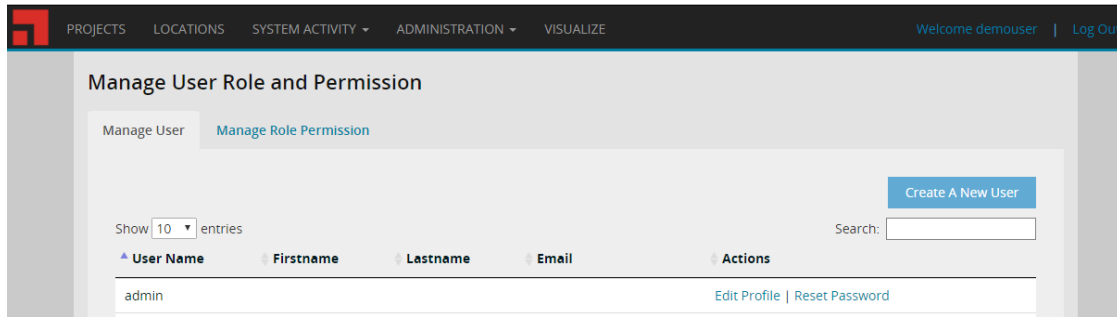
This is a view of the scan engine dashboard immediately after login. The UI contains the following sections as shown in the image above:

- **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 devices and applications with relationship connections.

**Note:** If the scan engine hasn't been activated, an optional **Activation** banner displays. Click this banner to move immediately to the activation section of the UI.

## Change Admin password

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



### To change the password

1. Open **Administration > User Settings**.
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.

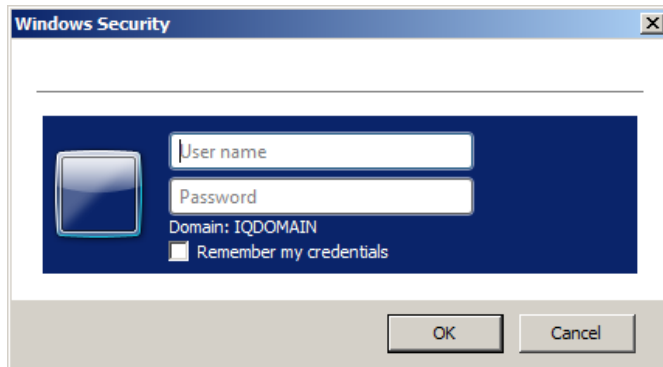
**Note:** To use Active Directory authentication, select the **Enable Active Directory for User Accounts** option during the IIS Configuration step of the installation process. If this option is not selected, enabling Active Directory authentication for the scan engine application in IIS will allow the 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. Click the **Administration > User Settings** menu in the dashboard. The administrator role already exists and does not require any specific handling.
2. Select the **Manage User** tab.
3. Click the **Create A New User** button.
4. Click the **AD user** checkbox; this is an Active Directory user.
5. Insert the domain name into the Domain Name field (e.g., demodomain).
6. Insert the domain user into the Username field (e.g., demouser).
7. Insert a value as the Firstname field (optional).
8. Insert a value as the Lastname field (optional).
9. Provide an email address for the receipt of e-mails (optional).
10. Note a password is not required, as this is an A/D user.
11. Select the **Administrator** role for the user.
12. Click the **Create** button. The new user will now be 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 login page.

## 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 initiates the registration of the scan engine. Projects can now be allowed to execute.

The screenshot shows the 'System Settings' page with the 'Activation' tab selected. The page has a navigation bar at the top with 'PROJECTS', 'LOCATIONS', 'SYSTEM ACTIVITY', 'ADMINISTRATION', and 'VISUALIZE'. The 'ADMINISTRATION' tab is active, and the 'System Settings' sub-tab is selected. Below the navigation bar, there are three tabs: 'Product Adapter Manager', 'Activation', and 'CyberArk'. The 'Activation' tab is active. The main content area contains four input fields: 'Licence Email', 'Licence Key', 'Licenced OSI', and 'Licence Expiry Date'. Below these fields is a blue button labeled 'Activate All Servers'. At the bottom, there is a table with three columns: 'Name', 'Installation ID', and 'Status'. The table is currently empty.

## 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

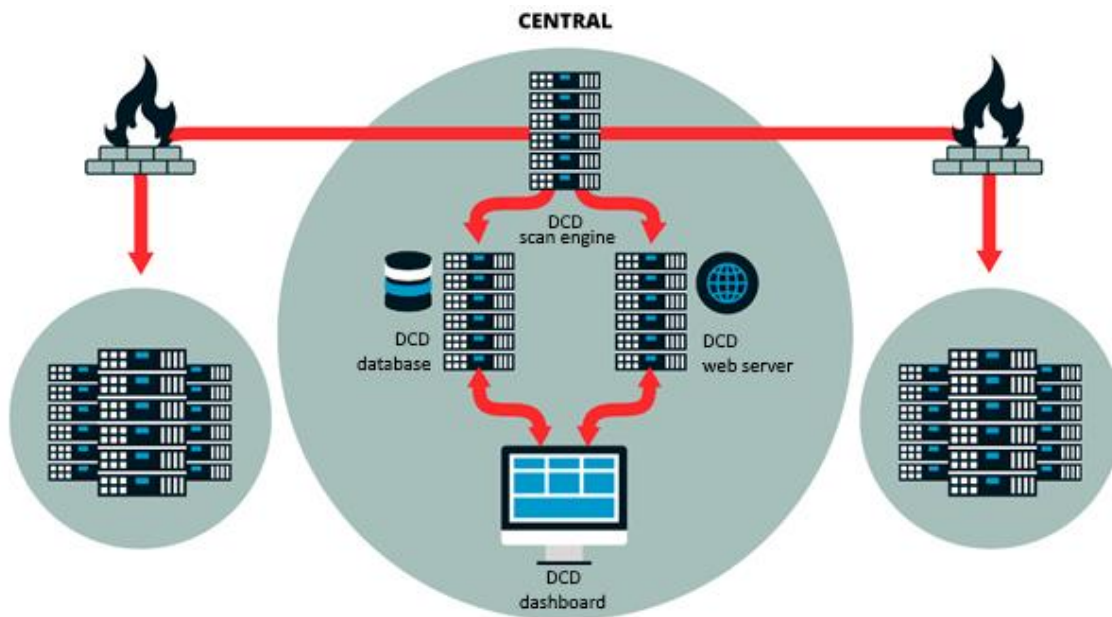
The rest of the document is composed of a number of use cases. These are complete configuration examples that walk you through the configuration of the scan engine UI. These use cases should act as a basis for deciding on the details of an actual on-site configuration.

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

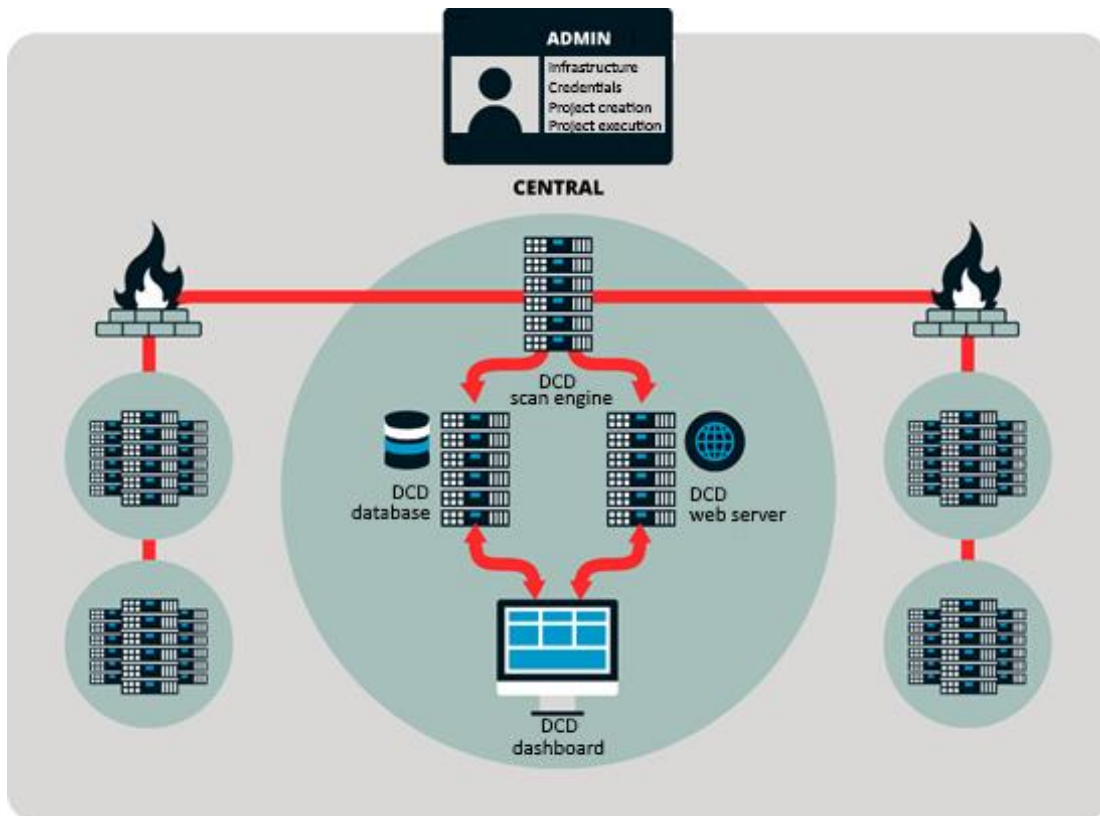
For a basic estate, the network infrastructure is composed of a relatively open network with no major restrictions in terms of firewalls, network latency, or bandwidth.



### 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.

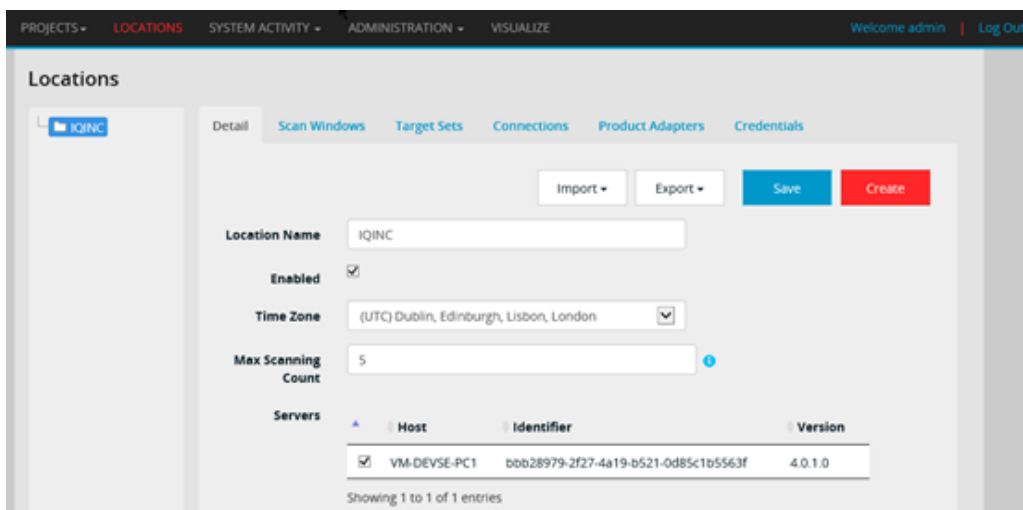


## Basic estate - Locations

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. Click the **Locations** menu in the dashboard to display 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.

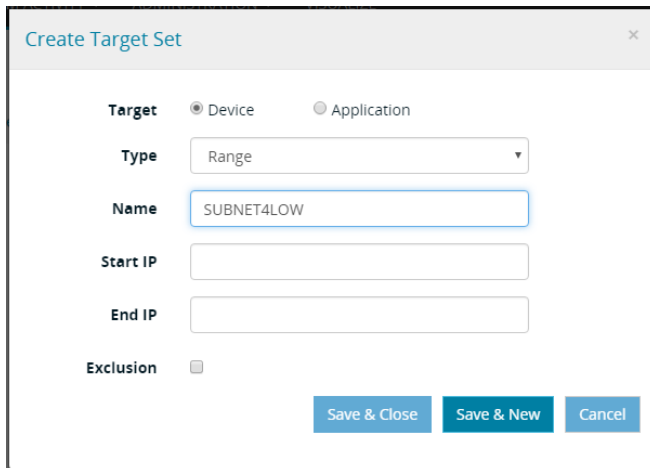
For a basic estate or POC, it's assumed that no restrictions will be applied. The Scan Windows settings can be ignored for this basic estate operation.

## Basic estate - Target Sets



**Target sets** 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**.

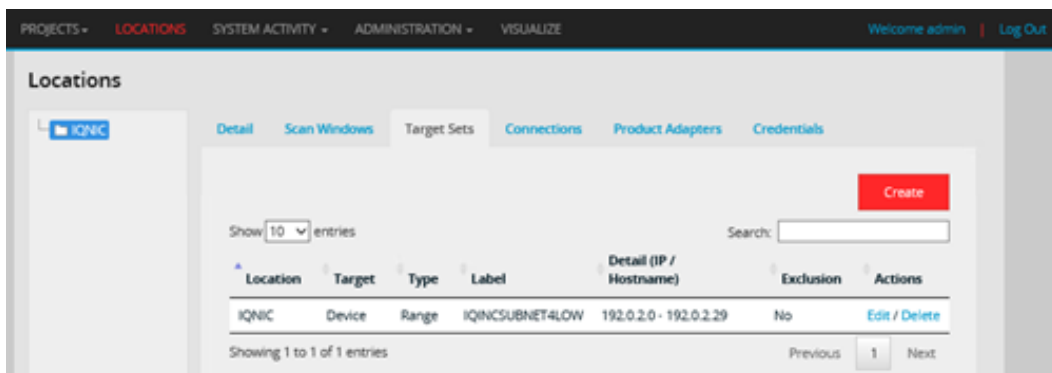
1. Select the top-level location.
2. Select the **Target Sets** tab.
3. Click the **Create** button to add a new target.
4. In the Create Target Set dialog, set the IP Range Type to **Range**.



The 'Create Target Set' dialog box contains the following fields and options:

- Target:** Radio buttons for 'Device' (selected) and 'Application'.
- Type:** A dropdown menu currently showing 'Range'.
- Name:** A text input field containing 'SUBNET4LOW'.
- Start IP:** An empty text input field.
- End IP:** An empty text input field.
- Exclusion:** An unchecked checkbox.
- Buttons:** 'Save & Close', 'Save & New', and 'Cancel' at the bottom right.

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 **Save & Close**.
10. Check that the new range is now associated with the location.



The screenshot shows the 'Locations' page with the 'Target Sets' tab selected. A table lists the created target set:

Location	Target	Type	Label	Detail (IP / Hostname)	Exclusion	Actions
IQNIC	Device	Range	IQINCSUBNET4LOW	192.0.2.0 - 192.0.2.29	No	Edit / Delete

Below the table, it says 'Showing 1 to 1 of 1 entries'. Navigation buttons for 'Previous', '1', and 'Next' are visible.

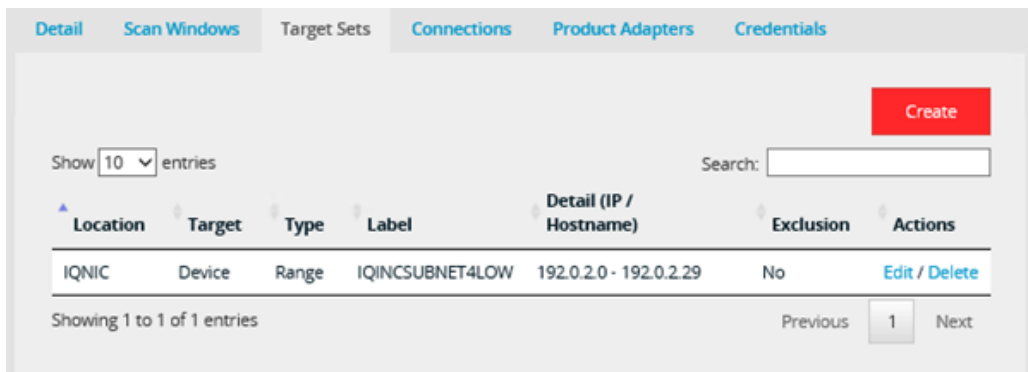
## Basic estate - Direct application scanning

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.



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

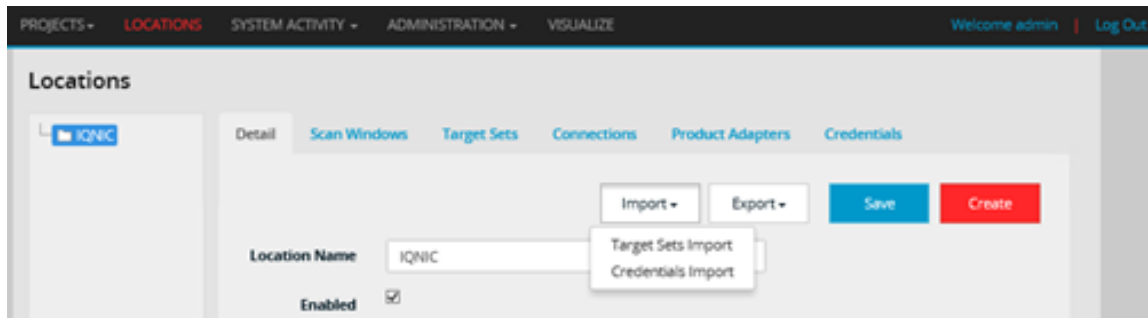
- For target, select **Application**, and then select the specific application type to be scanned.
- Issues to be considered for specific application types:
  - Instance Name is not required for vCenter type.
  - The default port will be used if none is specified.
  - Port needs to be specified for vCenter.
- 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.

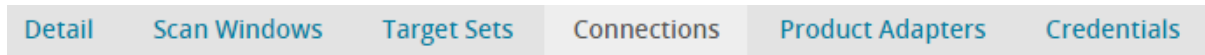
**Note:** If the application target is created in a location that doesn't have the required settings enabled for the target to be scanned successfully (e.g., required connection is not enabled), the target will still be created, but a warning message will appear, notifying you of the settings that need 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 > Detail** tab. The Import and Export menus provide the ability to import targets. Follow the instructions and file formats provided (a template is provided).



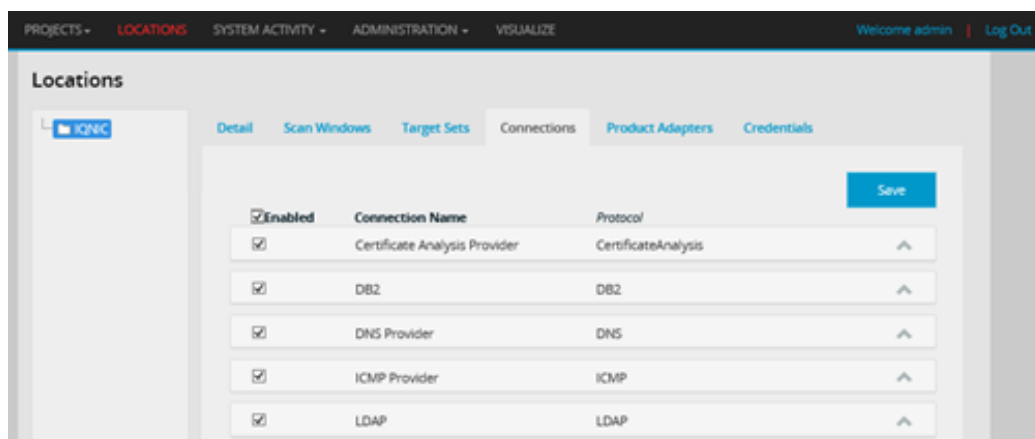
## Basic estate – Connections



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 *Data Center Discovery—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 arrow button to expand the options. The settings provided here must match those that were specified during the installation of the NavisphereCLI package.

The screenshot shows a configuration window titled 'NavisphereCLI'. It contains a list of settings, each with a label and a text input field:

- Ports:** 443
- commandtimeoutms:** 60000
- credentialscope:** 0
- ignoreinvalidcertificate:** false
- optionalnaviclientlocation:** (empty field)

- **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

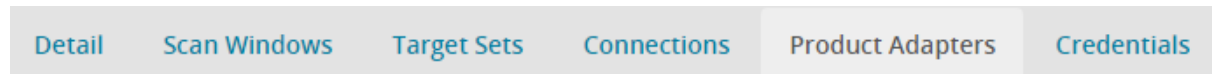
- **Command Prefix Code:** The connection type **SSH** can be used in with the command prefix **SUDO** to escalate your permissions to cover additional commands contained within the sudoers file. **SH** is used by default; to specify a custom command prefix, set **usecommandprefix** to **True**.
- **Use 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

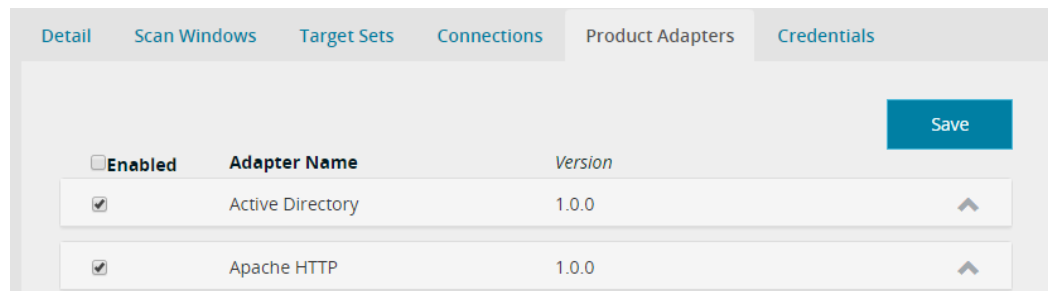
the number of attempts the scan engine will re-attempt the connection before the connection is abandoned for the given target. It supports Integer values.

## Basic estate - Product adapters



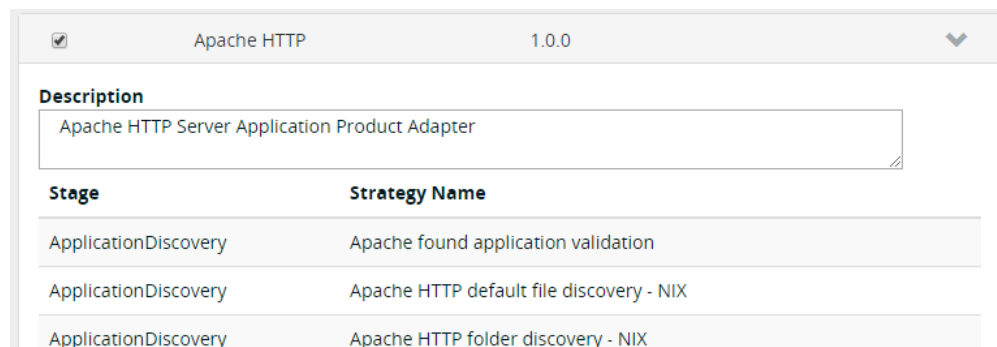
The **Product Adapters** functionality means that additional protocols, commands, and “transformation of scanned data” can be added to the core platform. This product development can be driven by customer requirements or emerging technology.

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



The expand arrow 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 arrow button again collapses the expanded product adapter.



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\Ivanti\DataCenterDiscovery ScanEngine 4.0)
2. Open the Ivanti.DataCenterDiscovery.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

**Detail**   **Scan Windows**   **Target Sets**   **Connections**   **Product Adapters**   **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 **Save & Close**.
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.

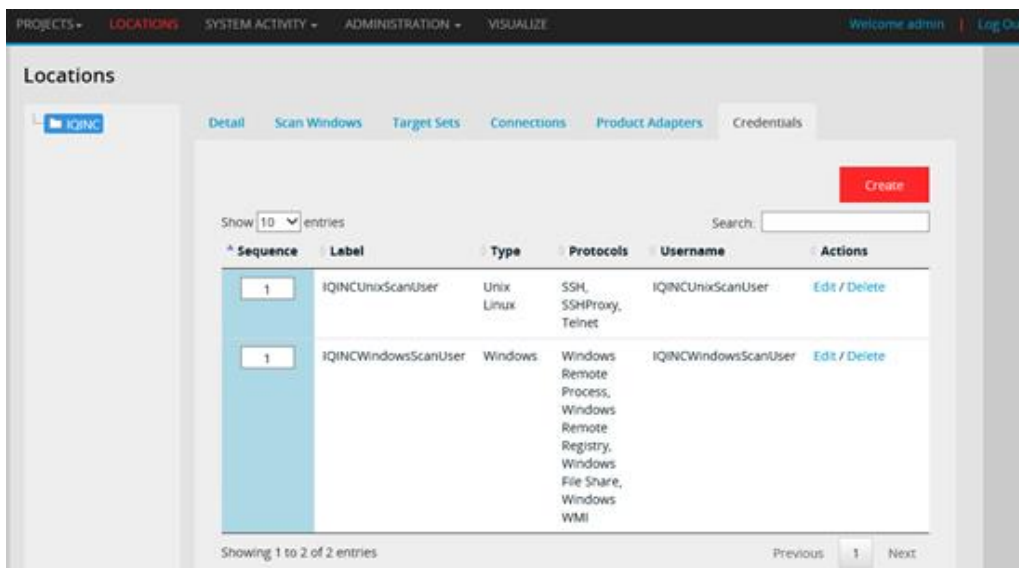
An SSH Proxy credential cannot be deleted if it's assigned to an existing UNIX Linux credential.

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 **Save & Close**.



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 *Data Center Discovery—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 **Save & Close**.
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 **Save & Close**.
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 **Save & Close**.
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.

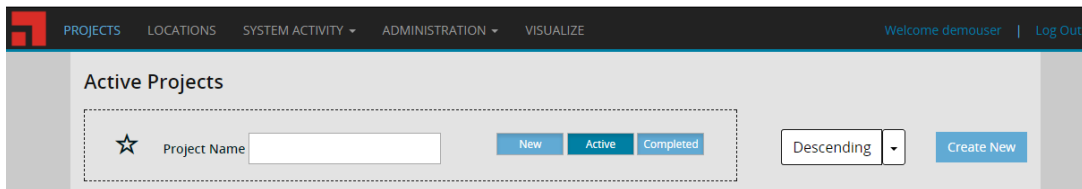
3. View the Create a Credential dialog that is opened.
4. See the Credential Type to **VMware**.
5. Set the Connection Type set to **VMware**.
6. Set the Label to **vSphereScanUser**.
7. Provide a sequence value for this credential. This is a relative value (i.e., sequence one (1) credentials will be 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 **Save & Close**.
11. Check that the new credential is now associated with the location.

Sequence	Label	Type	Protocols	Username	Actions
1	IQINCWindowsScanUser	Windows	Windows Remote Process, Windows Remote Registry, Windows File Share, Windows WMI	IQINC\iqdonarscanuser	Edit / Delete
2	IQINCOracleScanUser	Oracle Database	Oracle Database	IQINCOracleScanUser	Edit / Delete
3	IQINMsSqlScanUser	MS SQL Server	MS SQL server	IQINCMsSqlScanUser	Edit / Delete
4	IQINCInformixScanUser	Informix	Informix	IQINCInformixScanUser	Edit / Delete
5	IQINCvSphereScanUser	VMWare	VMware	IQINCvSphereScanUser	Edit / Delete

## 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:

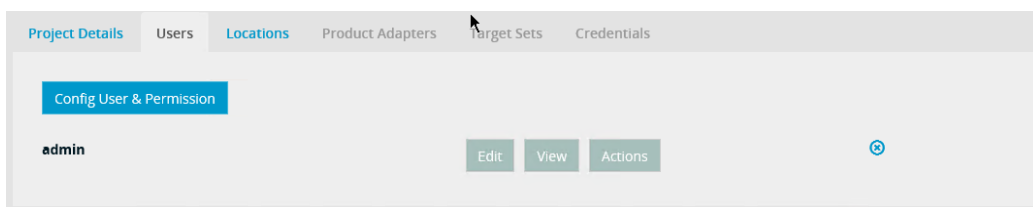
1. Select the **Projects** icon or click the **Projects** menu in the dashboard to display the currently available projects. By default, no projects are defined.



2. Click the **Create New** button to add a project.
3. In the Create Project dialog, set the Name to **Basic Estate**.
4. Set the Description to **How to scan a basic estate**.
5. Set the Start Time to the current time.
6. Click the **Next** button.

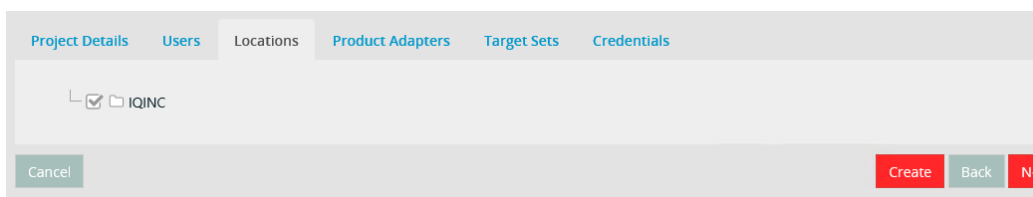
## Users tab

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.

## Target Sets tab

1. Ensure that the SUBNET4LOW IP Range is set to **On**.

2. Click the **Next** button.

Show  entries

Search:

Name	Location	Detail	Target/Exclusion	On / Off
IQINCSUBNET4LOW	IQINC	192.0.2.0 - 192.0.2.29	Target	<input checked="" type="checkbox"/>
Test Application	IQINC	vCenter 1.2.3.4:44	Target	<input checked="" type="checkbox"/>

Showing 1 to 2 of 2 entries

Previous  Next

## Credentials tab

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

Project Details Users Locations Product Adapters Target Sets **Credentials**

Show  entries

Search:

Label	Location	Type	Connections	On / Off
IQINCMsSqlScanUser	IQINC	MS_SQL_Server	MS SQL server	<input checked="" type="checkbox"/>
IQINCOracleScanUser	IQINC	Oracle_Database	Oracle Database	<input checked="" type="checkbox"/>
IQINCUnixScanUser	IQINC	Unix_Linux	Telnet	<input checked="" type="checkbox"/>
IQINCVsphereScanUser	IQINC	VMWare	VMware	<input checked="" type="checkbox"/>
IQINCWindowsScanUser	IQINC	Windows	Windows WMI	<input checked="" type="checkbox"/>

Showing 1 to 5 of 5 entries

Previous  Next

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

PROJECTS + LOCATIONS SYSTEM ACTIVITY + ADMINISTRATION + VISUALIZE

Welcome admin | Log Out

### Active Projects

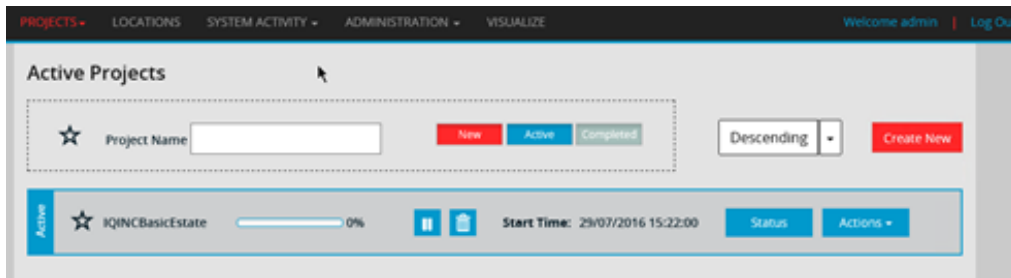
☆ Project Name

New	☆ IQINCBasicEstate	Waiting to be started	<input type="button" value="Run"/> <input type="button" value="Stop"/>	Start Time: 29/07/2016 15:22:00	<input type="button" value="Configure"/>
-----	--------------------	-----------------------	--	---------------------------------	--

## Basic estate - Start scan

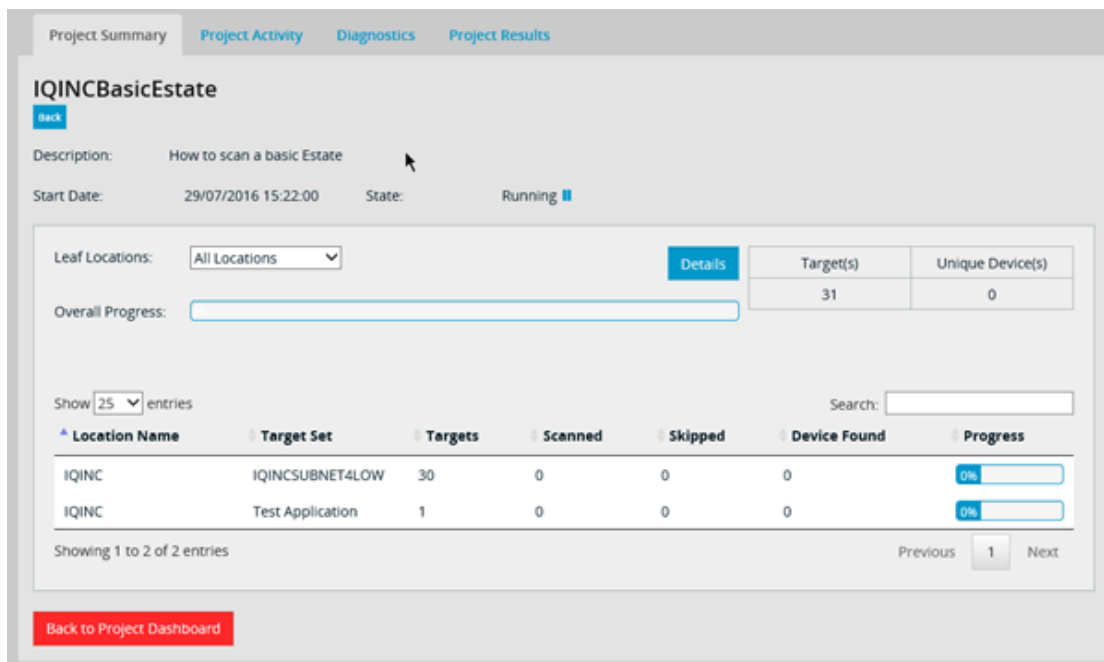
The final step of this process is to initiate a project scan. Projects are initiated from the Active Project tab.

1. Select the **Projects** icon or click the **Projects** drop-down menu.
2. Select the **Active** button.
3. Identify the **Basic Estate** 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.



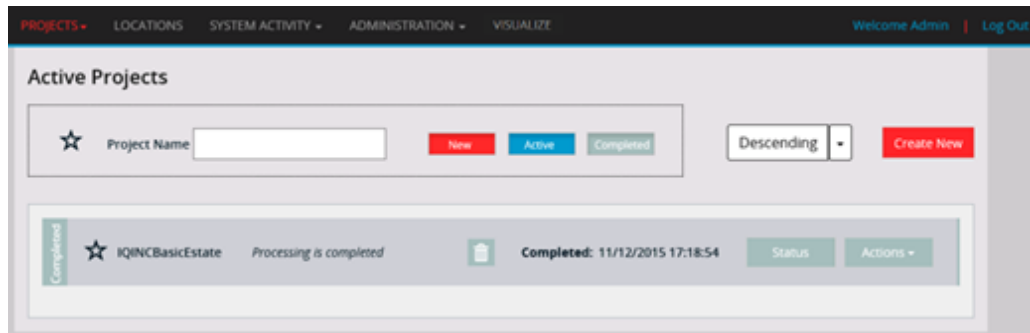
Refer to the “Project scan analysis” section for details about how to examine and diagnose the scanning operations.

## 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** button.
3. Identify the **Basic Estate** 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.

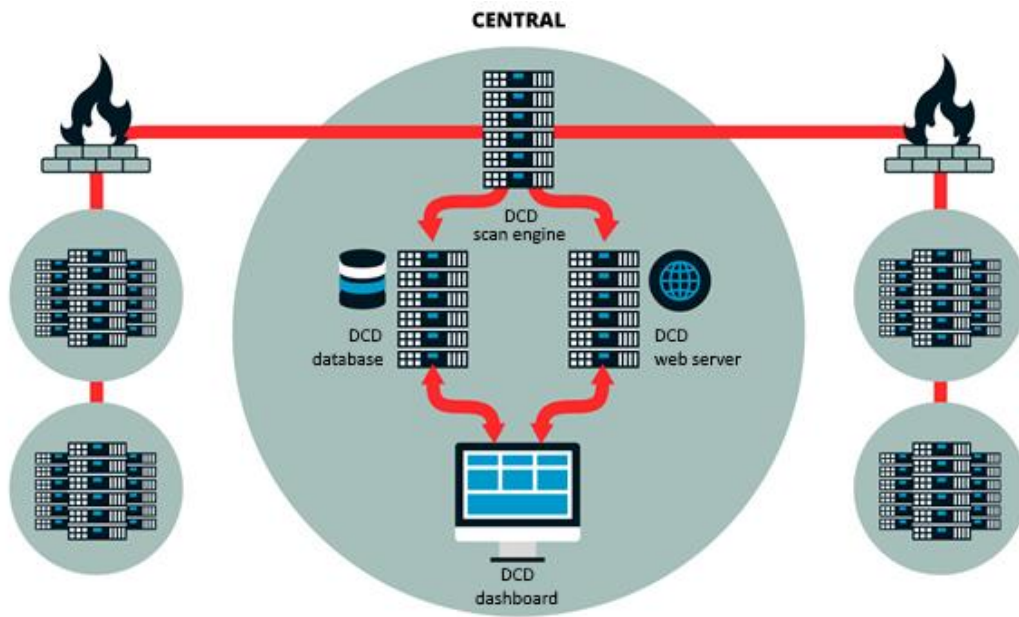
To support the project as described, the following items are required:

- **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

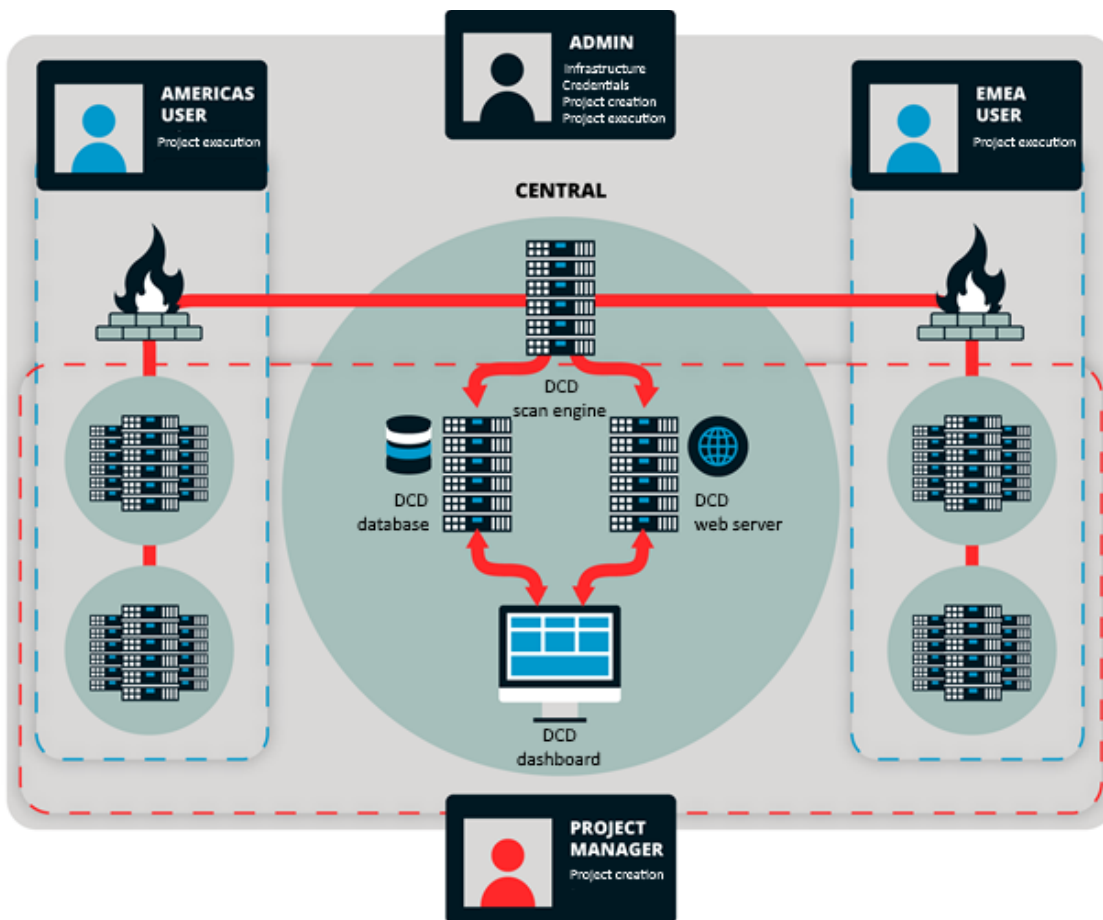
This network is composed of a relatively open network with no major restrictions in terms of firewalls, network latency, or bandwidth. The network structure is geographically dispersed into the Americas and EMEA. Each of these locations has a production and test set of devices.





## 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's 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

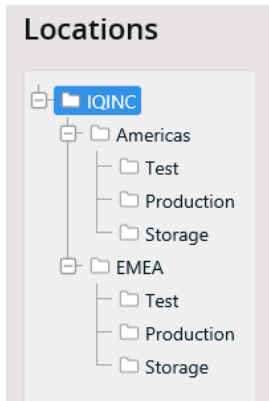
The medium-size company is split into two regional (scan) locations. Each region can be allowed to run its own scan projects (e.g., an Oracle audit may be done on a regional level at different times). Each location is also sub-divided into production and test devices and storage infrastructure as described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

Detail	Scan Windows	Target Sets	Connections	Product Adapters	Credentials
--------	--------------	-------------	-------------	------------------	-------------

**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).



**Target sets** 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 **Target Sets** tab.
5. Click the **Create** button to add a new target.
6. View the **Create Target** dialog.

**Create Target Set**

Target: ☒ Device ☐ Application

Type: Range

Name: SUBNET4LOW

Start IP:

End IP:

Exclusion: ☐

Save & Close Save & New Cancel

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 **Target Sets** 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 **Target Sets** 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.

**Locations**

Detail Scan Windows **Targets** Connections Product Adapters Credentials

Show 10 entries Search: range X

Location	Range Type	Label	Detail (IP / Hostname)	Target	Actions
IQINC Americas Production	Range	IQINC USPROD		Target	
IQINC Americas Test	Range	IQINC USTEST		Target	
IQINC EMEA Production	Range	IQINC EMEAPROD		Target	
IQINC EMEA Test	Range	IQINC EMEATEST		Target	

Showing 1 to 4 of 4 entries (filtered from 9 total entries) Previous 1 Next

**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

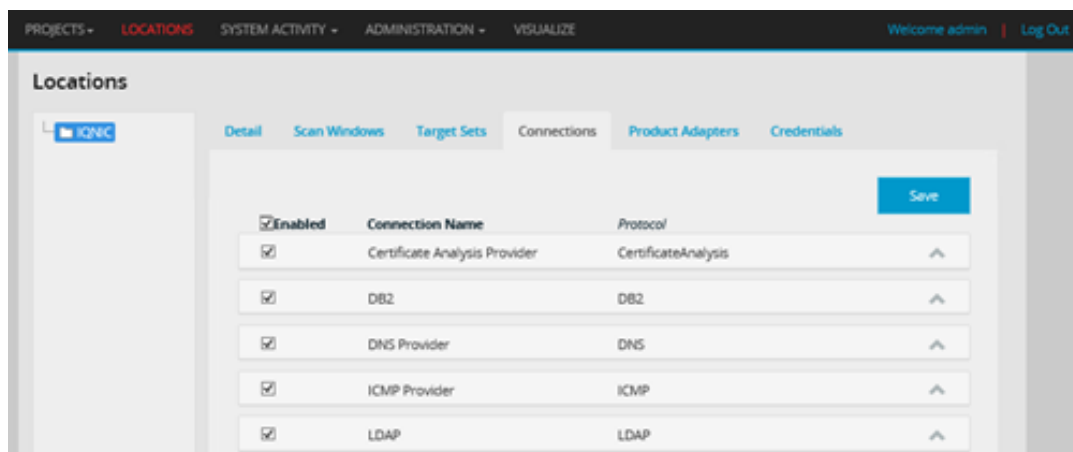
Login: Admin

Detail	Scan Windows	Target Sets	Connections	Product Adapters	Credentials
--------	--------------	-------------	-------------	------------------	-------------

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 *Data Center Discovery—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 arrow button to expand the options. The settings provided here must match those that were specified during the installation of the NavisphereCLI package.

NavisphereCLI	
Ports	443
commandtimeouts	60000
credentialscope	0
ignoreinvalidcertificate	false
optionalnaviclientlocation	

**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

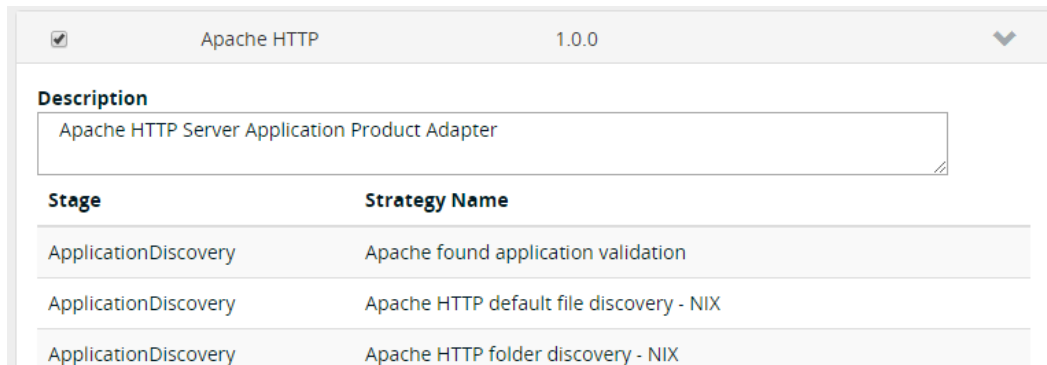
Detail	Scan Windows	Target Sets	Connections	Product Adapters	Credentials
--------	--------------	-------------	-------------	------------------	-------------

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:

Detail	Scan Windows	Target Sets	Connections	Product Adapters	Credentials					
<div> <input type="checkbox"/> Enabled           <table border="1"> <thead> <tr> <th>Adapter Name</th> <th>Version</th> </tr> </thead> <tbody> <tr> <td>Active Directory</td> <td>1.0.0</td> </tr> <tr> <td>Apache HTTP</td> <td>1.0.0</td> </tr> </tbody> </table> </div> <div>Save</div>					Adapter Name	Version	Active Directory	1.0.0	Apache HTTP	1.0.0
Adapter Name	Version									
Active Directory	1.0.0									
Apache HTTP	1.0.0									

The expand arrow 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\Ivanti\DataCenterDiscovery ScanEngine 4.0).
2. Open the Ivanti.DataCenterDiscovery.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

Detail	Scan Windows	Target Sets	Connections	Product Adapters	Credentials
--------	--------------	-------------	-------------	------------------	-------------

System credentials are used to provide access to an operating system (such as Windows or \*NIX) or an operating system component (such as 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 as 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.

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.

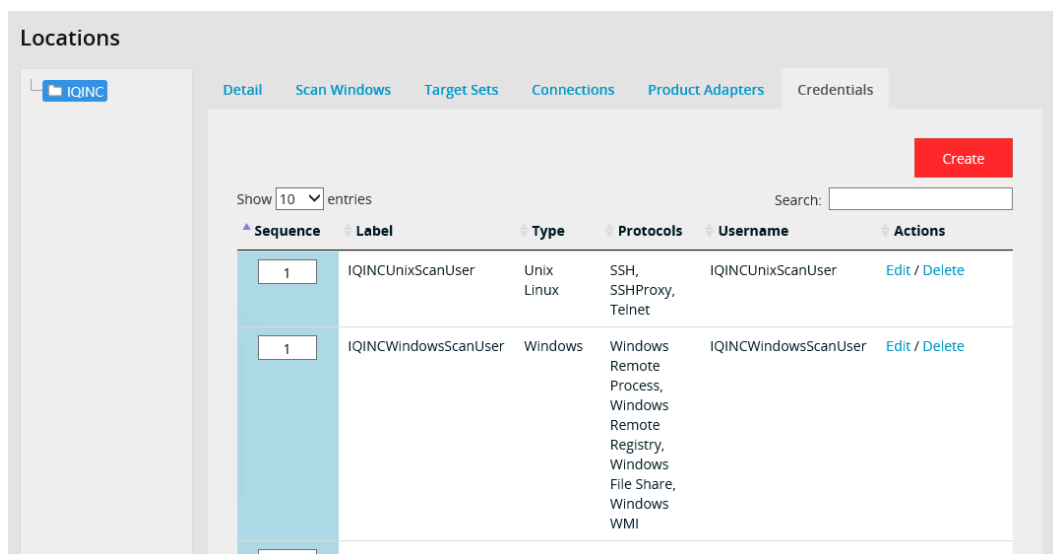
The screenshot shows a window titled "Add Credential". Inside, there are two radio buttons for "Managed": "Local" (which is selected) and "CyberArk". Below this is a dropdown menu for "Credential Type" with the text "-- Select Credential Type --". Underneath are several text input fields labeled "Connections:", "Label:", "Sequence:", "Username:", and "Password:". At the bottom of the window are three buttons: "Save & Close" (in red), "Save & New" (in blue), and "Cancel" (in grey).

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.

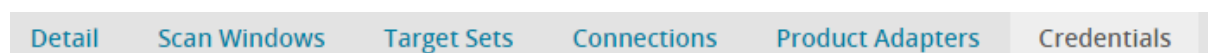
Repeat the process to add a **Windows** account credential:

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 *Data Center Discovery—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 *Data Center Discovery—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. Set 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 EMEAvmSphereScanUser 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 EMEAvmSphereScanUser 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.

**Manage User Role and Permission**

Manage User [Manage Role Permission](#)

Show  entries Search:  Create A New User

User Name	Firstname	Lastname	Email	Actions
admin				<a href="#">Edit Profile</a>   <a href="#">Reset Password</a>
America.user	America	User	america.user@iqinc.vom	<a href="#">Edit Profile</a>   <a href="#">Reset Password</a>   <a href="#">Delete</a>
Emea.user	Emea	User	emea.user@iqinc.com	<a href="#">Edit Profile</a>   <a href="#">Reset Password</a>   <a href="#">Delete</a>
Project Manager	Project	Manager	project.manager@iqinc.com	<a href="#">Edit Profile</a>   <a href="#">Reset Password</a>   <a href="#">Delete</a>

Showing 1 to 4 of 4 entries Previous  Next



## Multi-Departmental Estate – Project EMEA

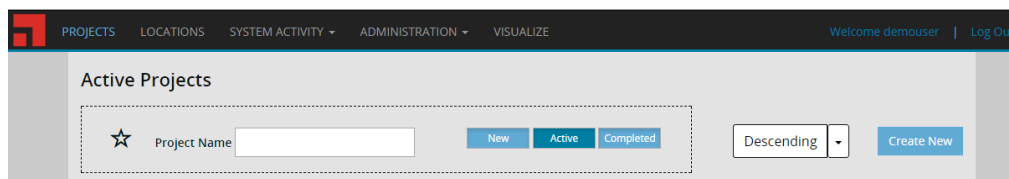
### Login: Project.Manager

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.

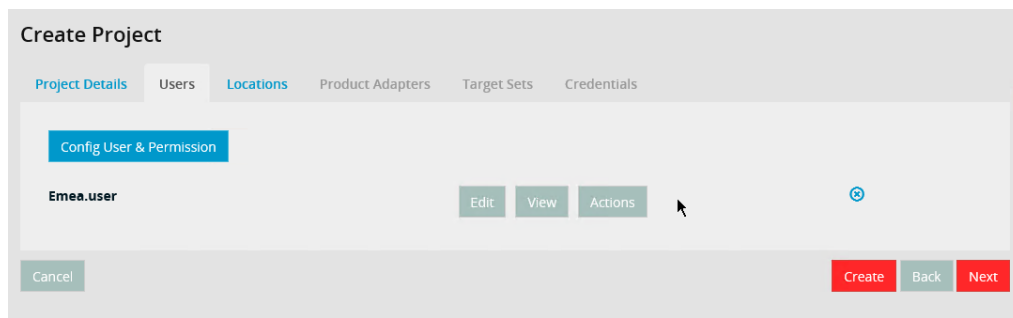


2. Select the **Active** button.
3. Click the **Create New** button to add a project.
4. View the Create Project dialog that is opened.
5. Set the Name to **MultiDeptEMEA**.
6. Set the Description to **Project Shared Between Multiple Users and Roles**.
7. Set the Start time to the current time.
8. Click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

### Users tab

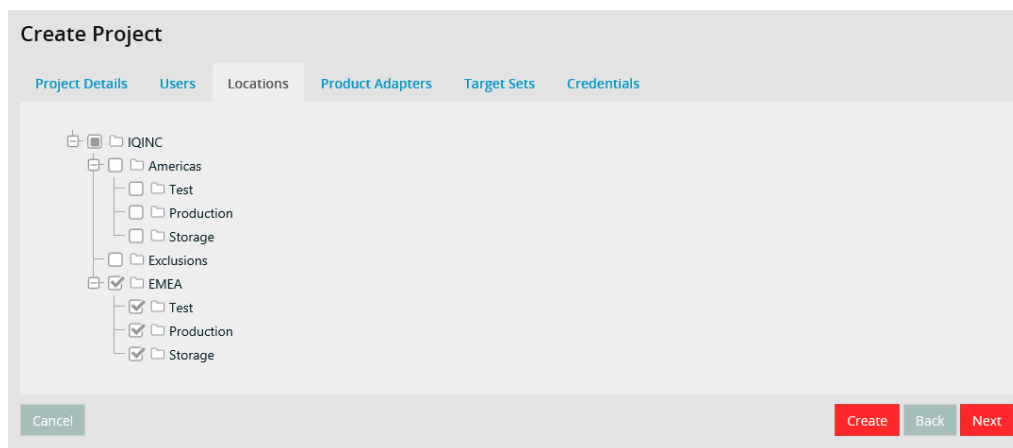
1. Click the **Config User & Permission** button.
2. Select the **EMEA.user** to be included with this project.

- Click the **Next** button.



## Locations tab

- Select the EMEA location.
- Click the **Next** button.



## Product Adapters tab

- Leave all the Product Adapters enabled.
- Click the **Next** button.

## Target Sets tab

- Ensure that the targets associated with the EMEA location are enabled.
- 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.

**Create Project**

Project Details Users Locations Product Adapters **Target Sets** Credentials

Show 10 entries Search:

Name	Location	Detail	Target/Exclusion	On / Off
IQINC EMEAPROD	IQINC EMEA Production	192.0.2.80	Target	<input checked="" type="checkbox"/>
IQINC EMEATEST	IQINC EMEA Test	192.0.2.30	Target	<input checked="" type="checkbox"/>

Showing 1 to 2 of 2 entries

Previous 1 Next

Cancel Create Back Next

- Click the **Next** button.

## Credentials tab

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

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

PROJECTS+ LOCATIONS SYSTEM ACTIVITY ADMINISTRATION VISUALIZE Welcome project manager Log Out

**Active Projects**

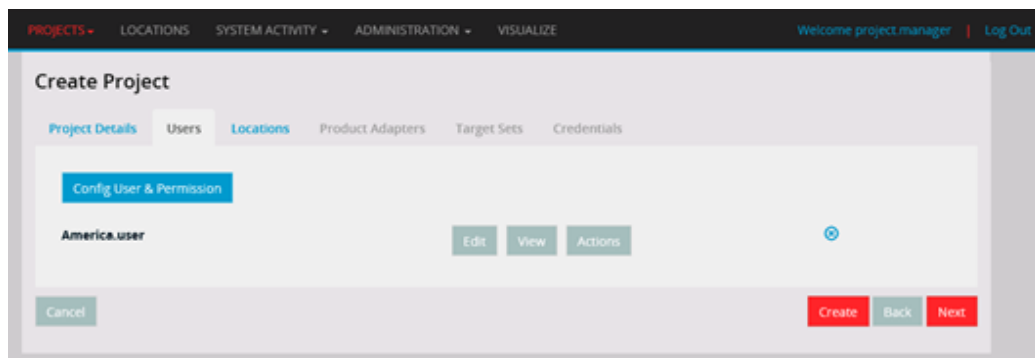
☆ Project Name  New Active Completed Descending - Create New

☆ IQINCMultiDeptEMEA Waiting to be started Start Time: 11/12/2015 23:54:00 Configure

- Select the **Active Projects**.
- Note that the previously created EMEA project is available.
- Click the **Create New** button to add a project.
- View the Create Project dialog that is opened.
- Set the Name to **MultiDeptAmericas**.
- Set the Description to **Americas Project Shared Between Multiple Users and Roles**.
- Set the Start Time to the current time.
- Click the **Next** button.

## Users tab

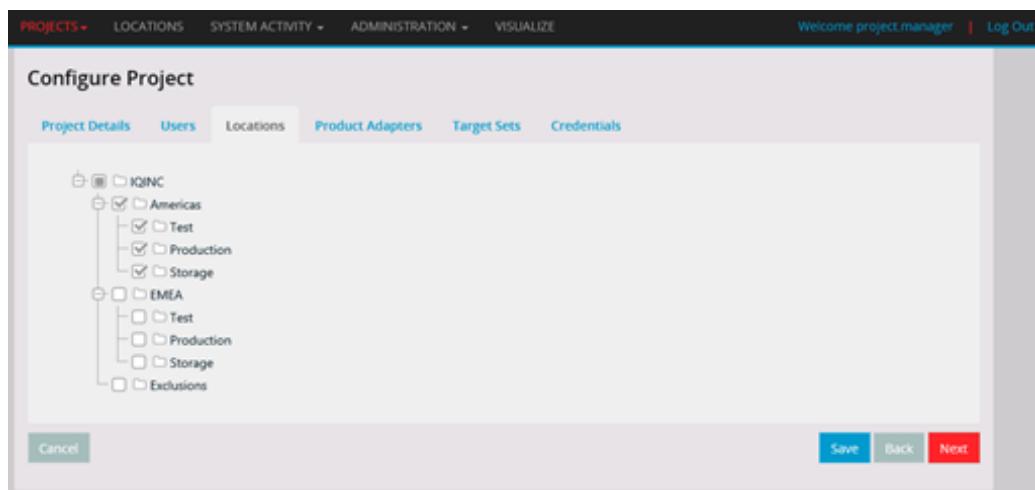
1. Click on the **Config User & Permission** button.
2. Select the **America.user** user to be included with this project.



3. Click the **Next** button.

## Locations tab

1. Select the **Americas** location.



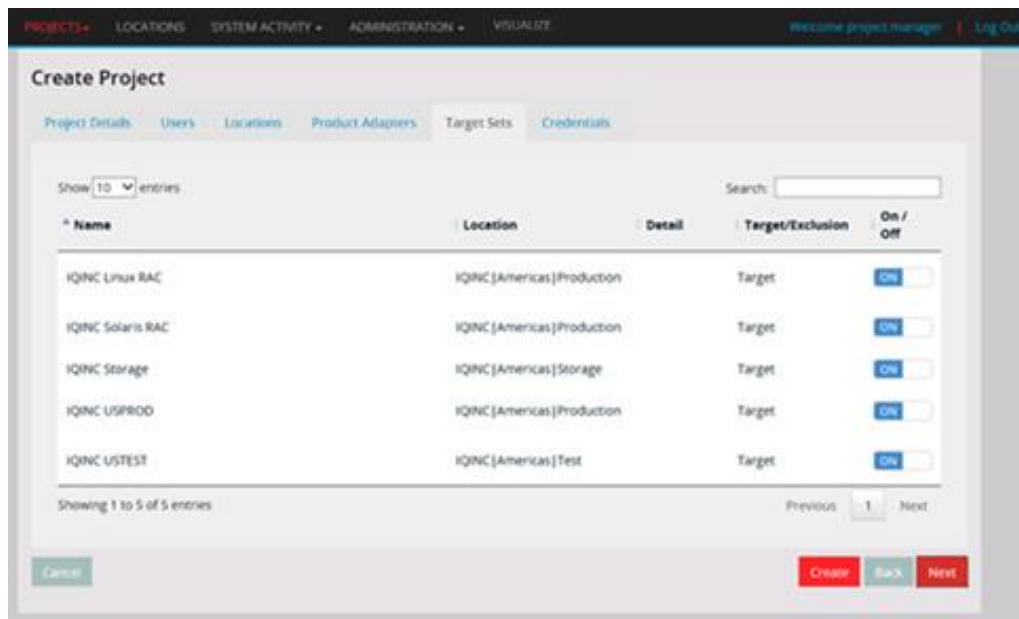
2. Note that all the sub-areas are also selected.
3. Click the **Next** button.

## Product Adapters tab

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

## Target Sets tab

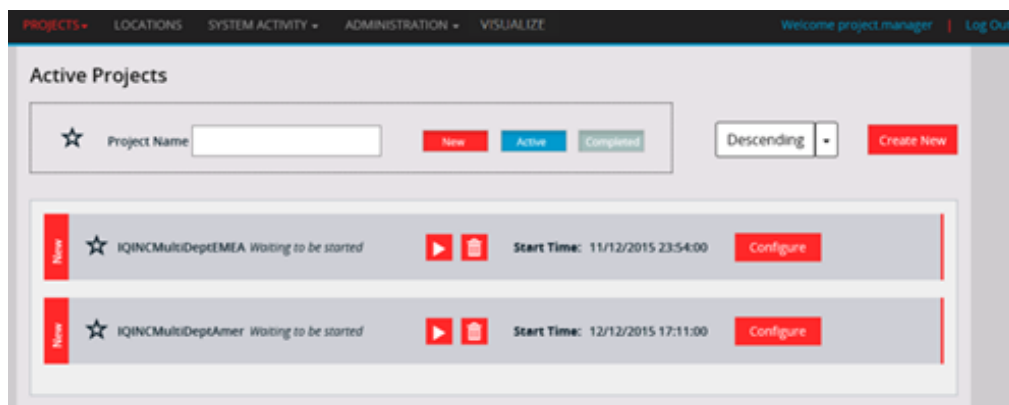
1. Ensure that the targets associated with the Americas are enabled.
2. Note that only targets that have been associated with the Americas location are listed. The association of locations with targets was provided by the admin user when describing the infrastructure.



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.

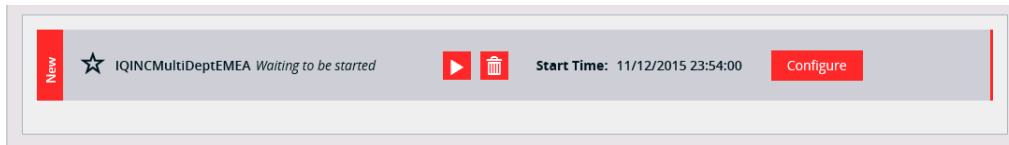
### Multi-departmental estate – Start EMEA scan

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** button.
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.

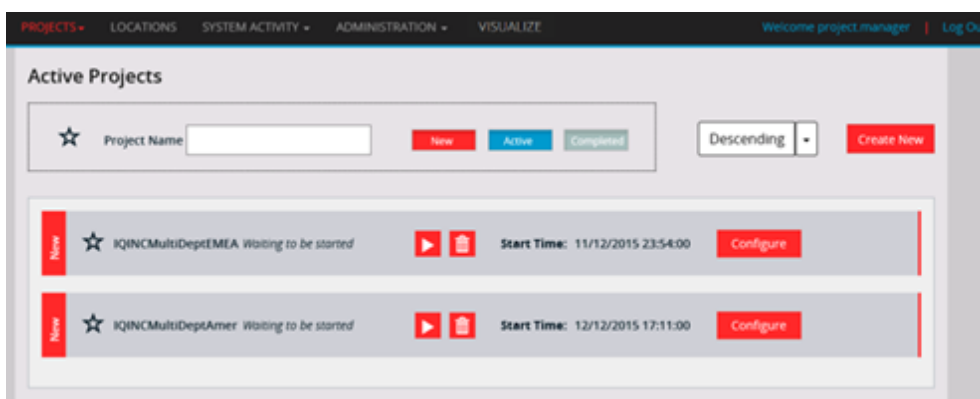
## Multi-departmental estate – Start Americas scan

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** button.
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** button.
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** button.
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.

#### 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:

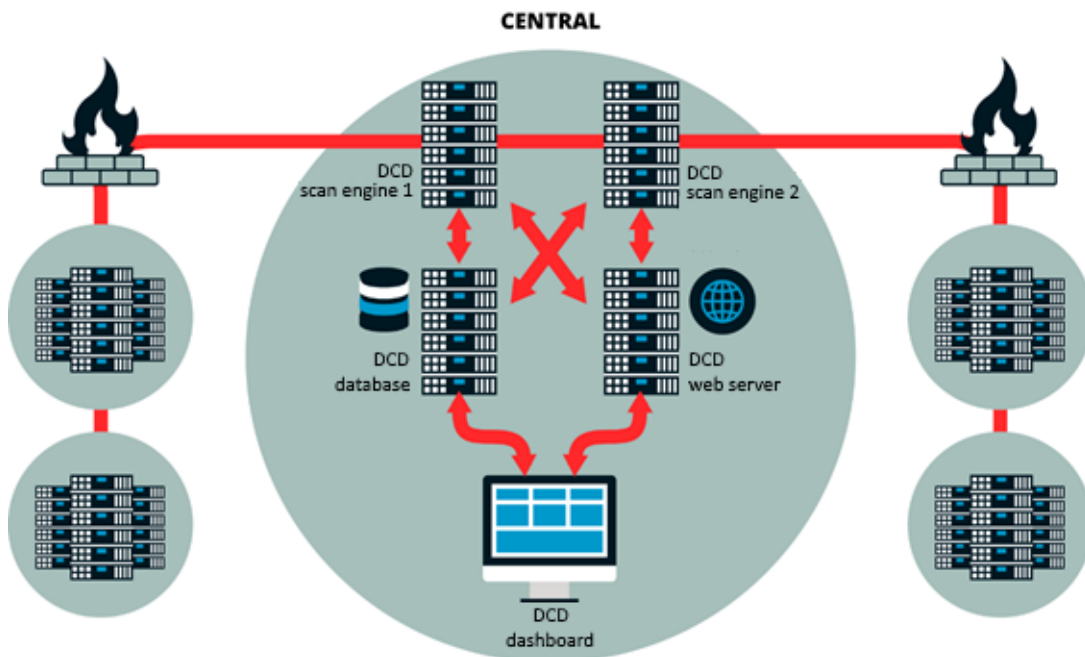
- **Global Infrastructure:** Identification and control of infrastructure globally. This "user" is responsible for the description of the infrastructure to be scanned, which includes IP address ranges, IP address range exclusions, Scan Windows and Connection types to be used.
- **Global Project Manager:** 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 installation guide to install multiple scan engines.

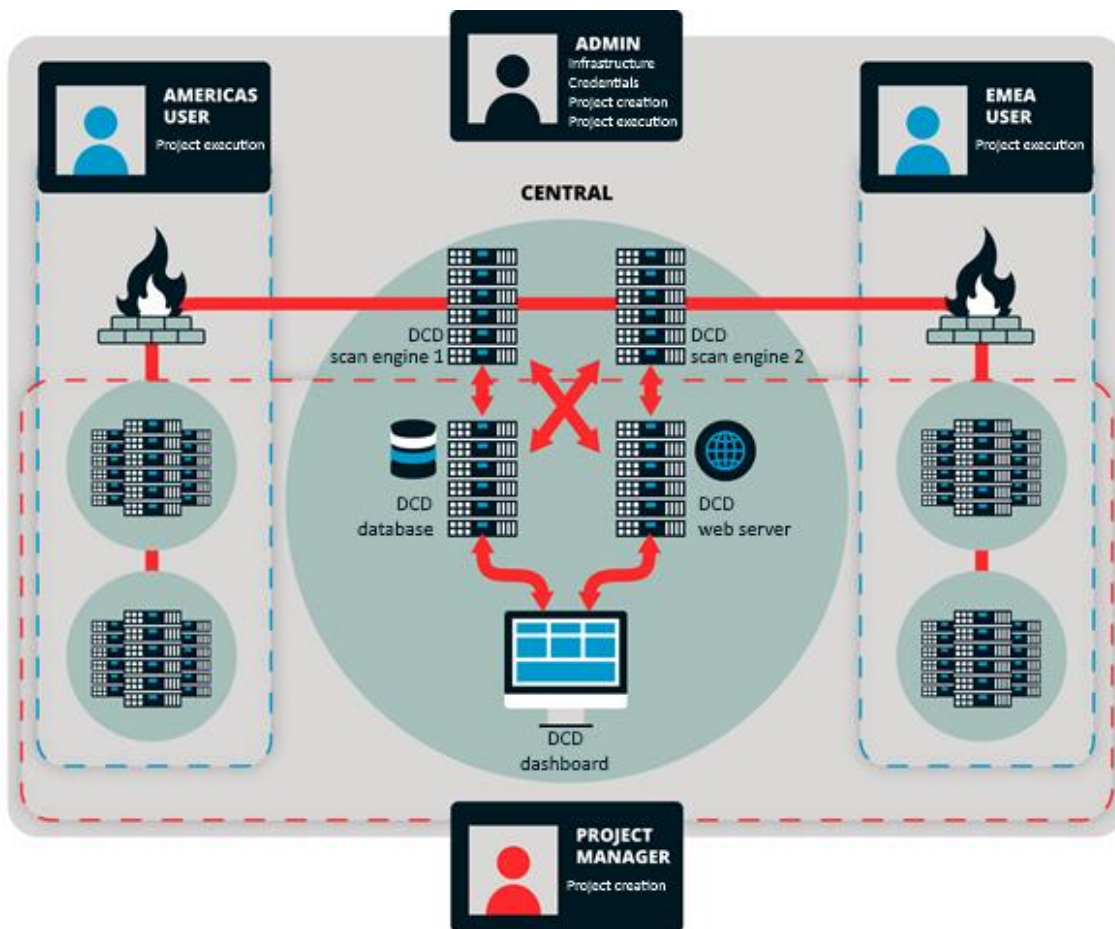
### Complex estate – Network infrastructure

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 *Data Center Discovery—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.
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

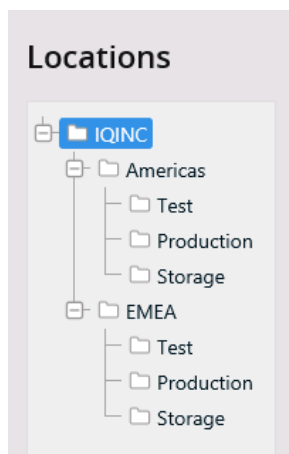
### Login: Admin

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:

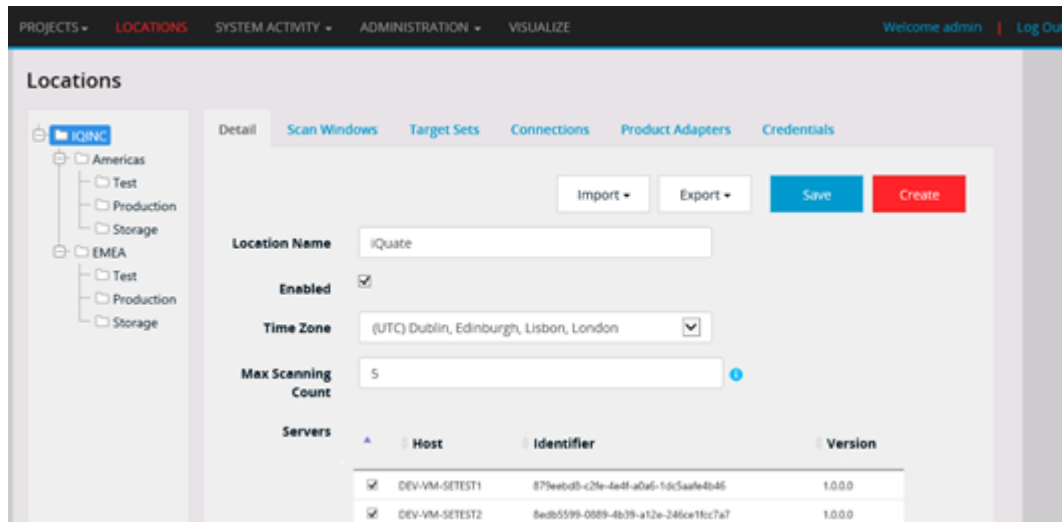
- Americas
  - Test
  - Production
  - Storage
- EMEA
  - Test
  - Production
  - Storage

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 top-level location.
4. Enable both scan engines for that 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 top-level 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.

Update Scan Window

**Scan Window Time**

Name: Not Working Hours

Start Date: 30/09/2015

Recurring Time: 09:00

Duration(mins): 480

Recurrence Type: ☐ Once ☒ Daily ☐ Weekly ☐ Monthly ☐ Yearly

Exclusion: ☒

**Recurrence - Daily**

☐ Recur Every 1 Day(s)

☒ Recur Every Weekday

Update Cancel

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.

Update Scan Window

**Scan Window Time**

Name: Financial Season

Start Date: 01/12/2015

Recurring Time: 00:00

Duration(mins): 1440

Recurrence Type: ☐ Once ☐ Daily ☒ Weekly ☐ Monthly ☐ Yearly

Exclusion: ☒

**Recurrence - Weekly**

Recur Every 1 Week(s) On

Sunday Monday Tuesday Wednesday Thursday Friday Saturday

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.

Detail

Scan Windows

Target Sets

Connections

Product Adapters

Credentials

Create

Name	Recurrence	Next Start	Duration (Mins)	Enabled	Exclusion	Action
Not Working Hours	Daily	10/08/2016 09:00:00	480	<input checked="" type="checkbox"/>	True	<a href="#">Edit / Delete</a>
Financial Season	Weekly	10/08/2016 00:00:00	1440	<input checked="" type="checkbox"/>	True	<a href="#">Edit / Delete</a>

## 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.

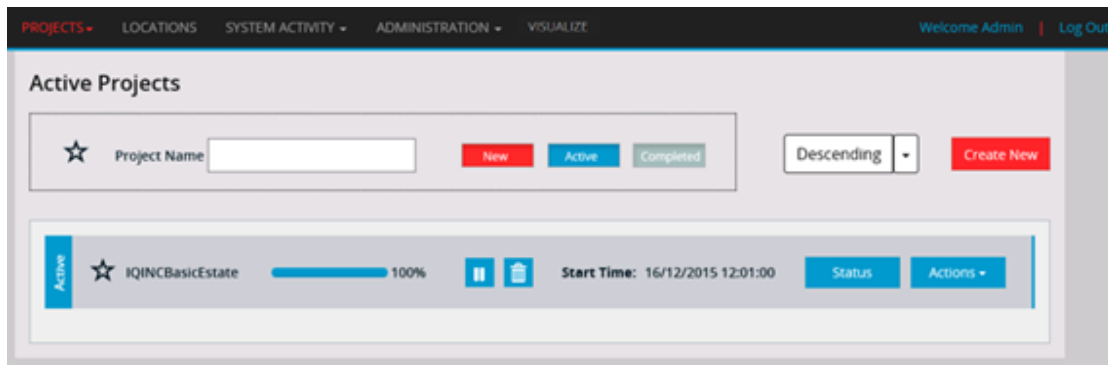
Complex estate section	Equivalent multi-departmental estate section
Complex estate – Targets	See Multi-departmental estate – Targets
Complex estate - Connections	See Multi-departmental estate – Connections
Complex estate – Product Adapters	See Multi-departmental estate – Product Adapters
Complex estate – 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

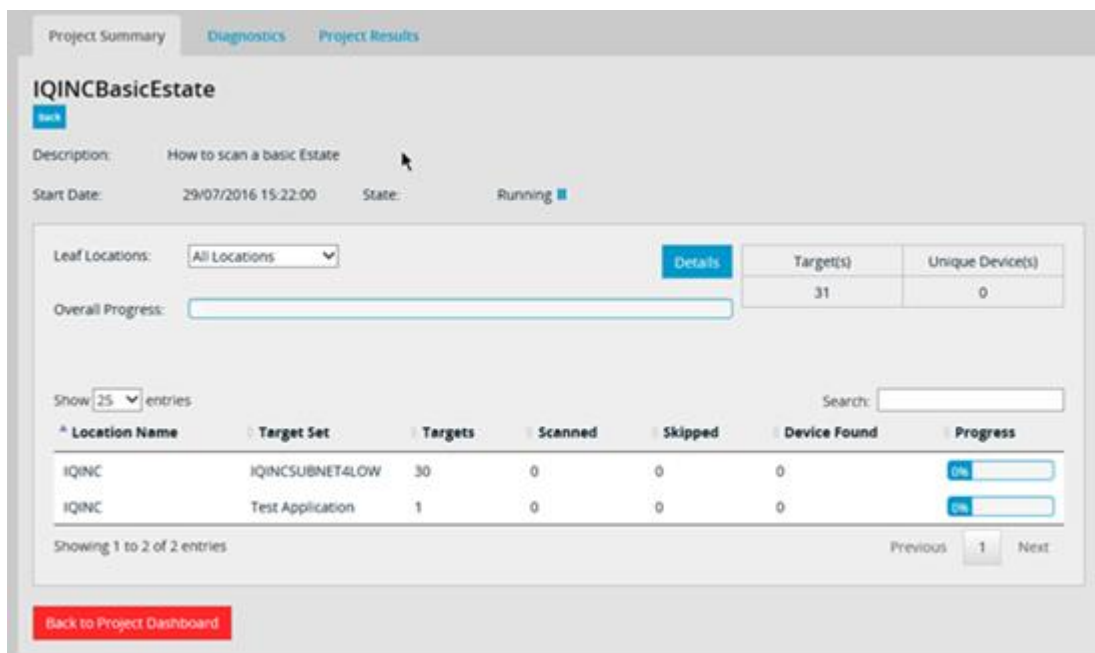
You can analyze the scanning operation from the UI interface. The analysis is carried out on a project by project basis. Under **Active Projects**, identify the project of interest.



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.



Additional detail is available for each target by clicking the **More** button, which displays the project Target Diagnostics window.

## Project diagnostics target – No credential(s) attempt

**Target Diagnostics:**

[Back](#)

[Rescan Target](#)

**Scan History**

Show  entries

Search:

Server Name	IP Address	Start Time	End Time	Status	Outcome
IQINC		16/12/2015 12:05:42	16/12/2015 12:07:54	Completed	No Credential(s) Attempt

Showing 1 to 1 of 1 entries

First Previous **1** Next Last

**Connection History**

Label	Location	Username	Attempts	Successful	Failed
> No Credential			8	1	7

**Stage History**

> TargetVerification

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.

**Target Diagnostics:**

[Back](#)

[Rescan Target](#)

**Scan History**

Show  entries

Search:

Server Name	IP Address	Start Time	End Time	Status	Outcome
IQINC		16/12/2015 12:05:42	16/12/2015 12:07:54	Completed	No Credential(s) Attempt

Showing 1 to 1 of 1 entries

First Previous **1** Next Last

**Connection History**

Label	Location	Username	Attempts	Successful	Failed
> No Credential			8	1	7

Show  entries

Search:

Connection	Port	Instance Name	Attempt Date	Outcome	Message
ICMP Provider	0		16/12/2015 12:05:44	Success	CONNECTION-UNSECURED-SUCCESSFUL
TCP Provider	22		16/12/2015 12:05:54	GeneralFailure	CONNECTION-UNSECURED-FAILURE

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.

Stage History					
TargetVerification					
Show <input type="text"/> entries		Search: <input type="text"/>			
Product Adapter	Strategy	Attempt Date	Duration	Outcome	Message
Device Discovery	TCP Discovery	5/4/2016 12:07:51 PM	0	Skipped	Skipping Strategy because of missing Protocol connection TCP (audit=Discovery@TV.1:DeviceDiscoveryTCP) <a href="#">Show</a>

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 diagnostics target – 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.

Stage History	
>	DeviceUniqueness
>	ApplicationDiscovery
>	DeviceDiscovery
>	ApplicationUniqueness
>	DeviceScanning
>	TargetVerification

## Target verification

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

▼ TargetVerification

Show 25 entries Search:

Product Adapter	Strategy	Attempt Date	Duration	Outcome	Message	
Device Discovery	Packet Analysis Discovery	23/09/2015 13:52:39	21013	NoResult	Strategy did not return a result" (audit=Discovery@TV.1:DeviceDiscoveryPacketAnalysis)	<a href="#">Show</a>
Device Discovery	TCP Discovery	23/09/2015 13:52:39	0	Success	Strategy returned a valid result (audit=Discovery@TV.1:DeviceDiscoveryTCP)	<a href="#">Show</a>
Device Discovery	Ping Discovery	23/09/2015 13:52:39	0	Success	Strategy returned a valid result (audit=Discovery@TV.3:DeviceDiscoveryPing)	<a href="#">Show</a>

Showing 1 to 3 of 3 entries First Previous **1** Next Last

## 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)	<a href="#">Show</a>
Device Discovery	TCP Open Ports	23/09/2015 13:52:51	0	Success	Strategy returned a valid result (audit=Discovery@DD.2:PortDiscoveryTCP)	<a href="#">Show</a>
Device Discovery	Certificate Discovery	23/09/2015 13:53:14	0	Success	Strategy returned a valid result (audit=Discovery@DD.4:CertificateDiscovery)	<a href="#">Show</a>
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>
Unix Variant	SSH/Telnet Hostname Identification	23/09/2015 13:53:15	0	Success	Strategy returned a valid result (audit=UNIX@DD.0:DeviceDiscoveryHostname)	<a href="#">Show</a>
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>

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. 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)	<a href="#">Show</a>
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>
Unix Variant	Device Hostname	23/09/2015 13:53:17	0	Success	Strategy returned a valid result (audit=UNIX@DU.2:DeviceHostname)	<a href="#">Show</a>
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>

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: <input type="text"/>			
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>
Unix Variant	SSH DNS Identification	23/09/2015 13:53:34	0	Success	Strategy returned a valid result (audit=UNIX@DS.0:DeviceDiscovery)	<a href="#">Show</a>
Unix Variant	Targetted Unix Variant Folders Index	23/09/2015 13:56:36	181271	GeneralFailure	Exception in strategy (audit=UNIX@DS.1:TargettedFolderIndex)	<a href="#">Show</a>
Unix Variant	HP-UX Device Uptime	23/09/2015 13:56:36	0	Success	Strategy returned a valid result (audit=UNIX@DS.1:HPUXUptime)	<a href="#">Show</a>
Unix Variant	HP-UX Device FQDN	23/09/2015 13:56:37	0	Success	Strategy returned a valid result (audit=UNIX@DS.1:HPDeviceFQDN)	<a href="#">Show</a>
Unix Variant	HP-UX Device Domain Name	23/09/2015 13:56:37	664	StrategyFailure	Strategy failed (audit=UNIX@DS.1:HPDeviceDomainName)	<a href="#">Show</a>
Unix Variant	HP-UX Process ProxyPort Information	23/09/2015 13:56:39	612	StrategyFailure	Strategy failed (audit=UNIX@DS.1:ProcessPorts)	<a href="#">Show</a>
Unix Variant	HP-UX Device Information	23/09/2015 13:56:39	0	Success	Strategy returned a valid result (audit=UNIX@DS.1:DeviceInformation)	<a href="#">Show</a>
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)	<a href="#">Show</a>
Unix Variant	HP-UX Process Information	23/09/2015 13:56:52	0	Success	Strategy returned a valid result (audit=UNIX@DS.1:Processes)	<a href="#">Show</a>

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: <input type="text"/>				
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>

The example above identifies that the Cognos TM1 product adapter successfully 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: <input type="text"/>				
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>
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)	<a href="#">Show</a>

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:

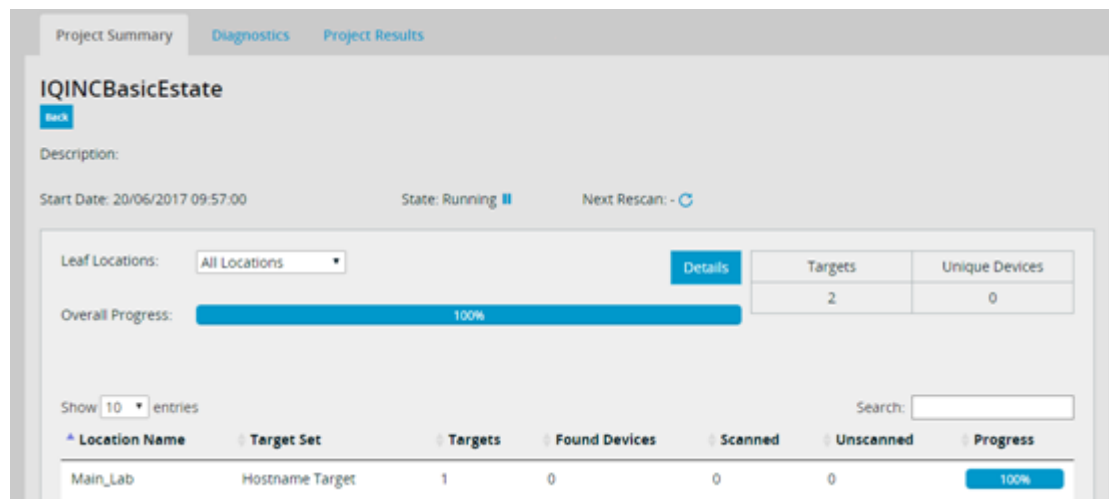
- Scan service logging
  - Filename: Service.log
  - Additional overflow filename: Service.log.N (where N is a number between 1 and 10).
  - The logs associated with the overall scan operation. When a file gets too large, a new file is created and the original file is renamed to service.log.N
- Individual 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\Ivanti\DataCenterDiscovery 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 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.

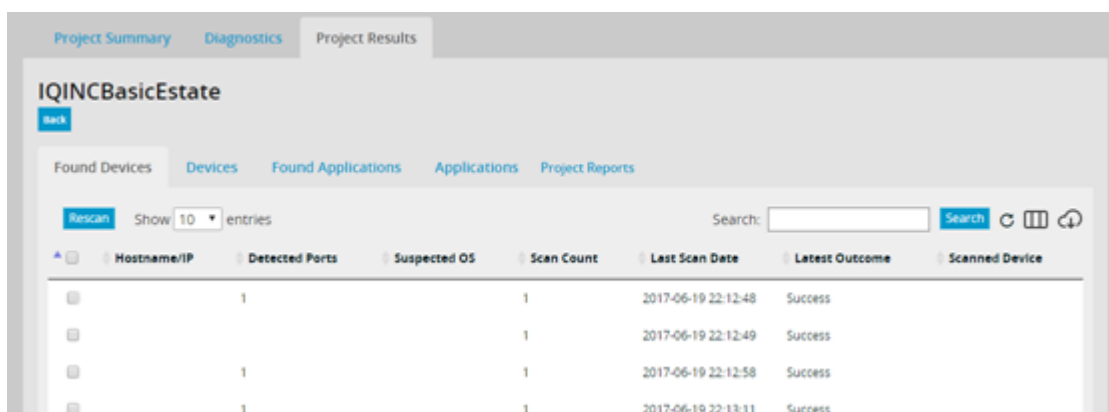
Each category is available as a separate tab for further examination, and each provides additional action buttons:

Button	Action
	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.



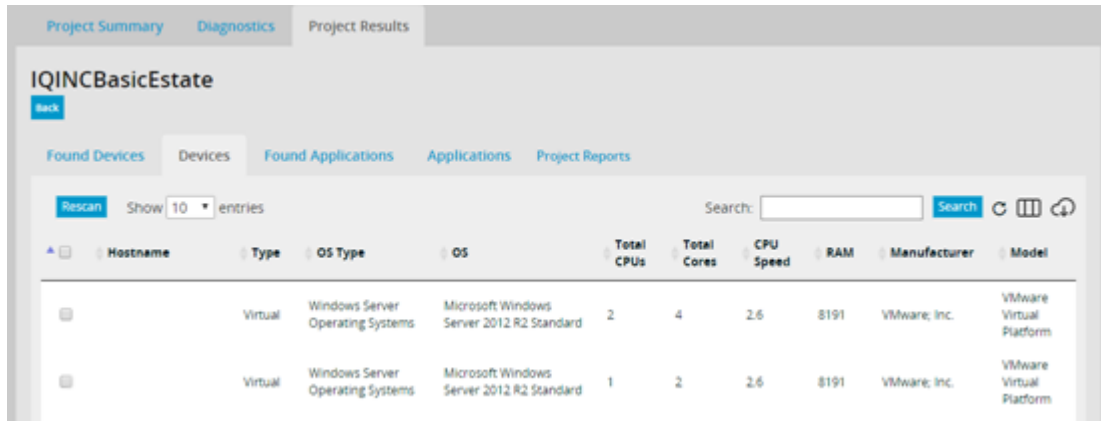
Hostname/IP	Detected Ports	Suspected OS	Scan Count	Last Scan Date	Latest Outcome	Scanned Device
	1		1	2017-06-19 22:12:48	Success	
			1	2017-06-19 22:12:49	Success	
	1		1	2017-06-19 22:12:58	Success	
	1		1	2017-06-19 22:13:11	Success	

## 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



Project Summary | Diagnostics | Project Results

**IQINCBasicEstate**

Back

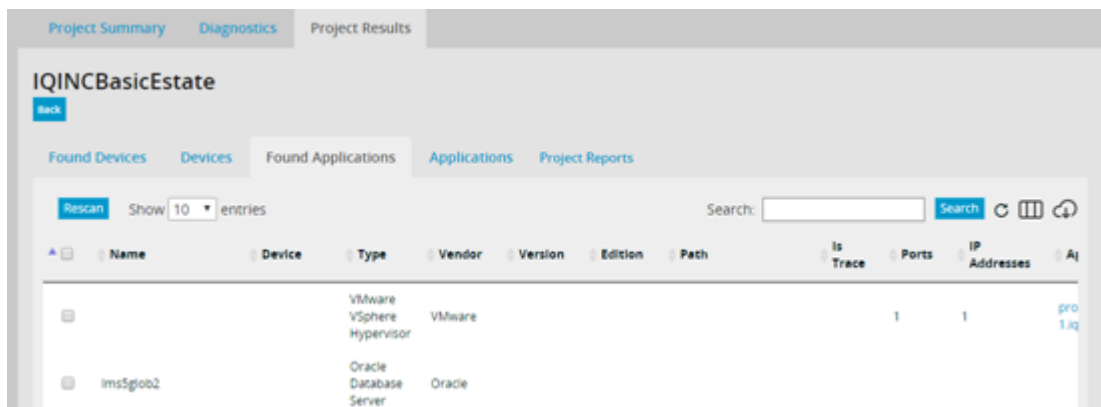
Found Devices | Devices | Found Applications | Applications | Project Reports

Rescan Show 10 entries Search: [ ] Search [ ] [ ] [ ]

Hostname	Type	OS Type	OS	Total CPUs	Total Cores	CPU Speed	RAM	Manufacturer	Model
	Virtual	Windows Server Operating Systems	Microsoft Windows Server 2012 R2 Standard	2	4	2.6	8191	VMware, Inc.	VMware Virtual Platform
	Virtual	Windows Server Operating Systems	Microsoft Windows Server 2012 R2 Standard	1	2	2.6	8191	VMware, Inc.	VMware Virtual Platform

## 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).



Project Summary | Diagnostics | Project Results

**IQINCBasicEstate**

Back

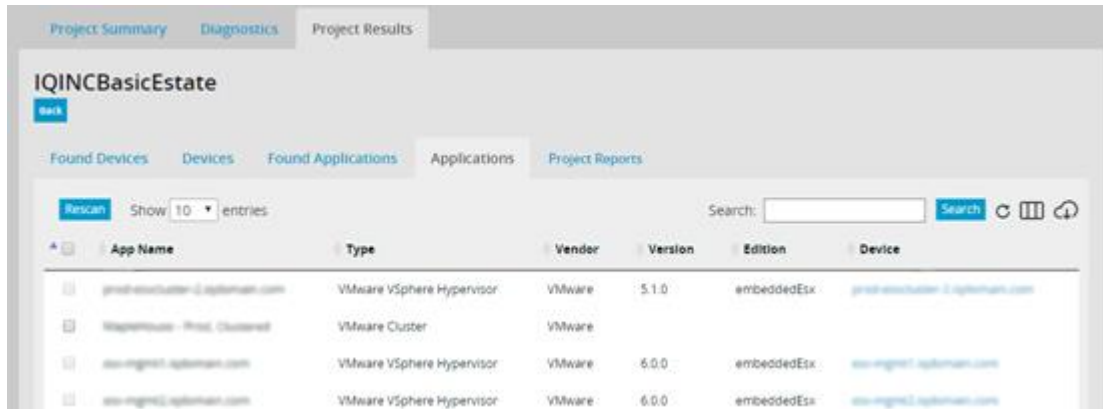
Found Devices | Devices | Found Applications | Applications | Project Reports

Rescan Show 10 entries Search: [ ] Search [ ] [ ] [ ]

Name	Device	Type	Vendor	Version	Edition	Path	Is Trace	Ports	IP Addresses	Aliases
	VMware	VMware VSphere Hypervisor	VMware					1	1	pro 1.iq
lms5job2		Oracle Database Server	Oracle							

## Applications

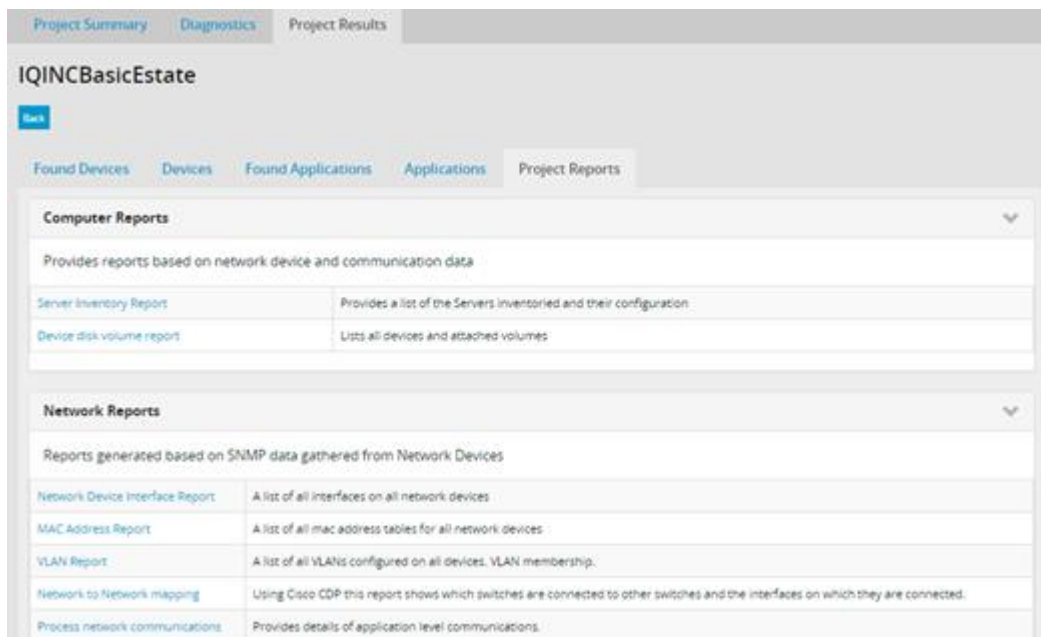
This is a successfully scanned application that represents an application distinct from all other applications (based on uniqueness).



## Project reports

This is a centralized location for downloading both network and computer reports. Currently available reports include network device interface, Mac address, VLAN, and network-to-network mapping.

To download a report, click its link in the Report name column.



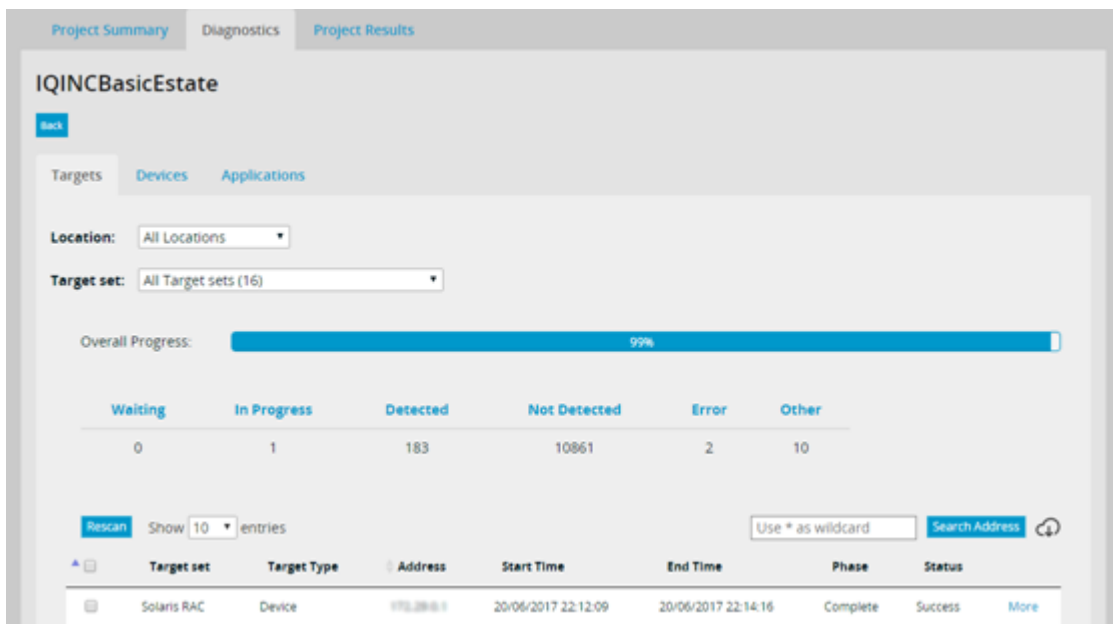
## Project status – Diagnostics

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.

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



Note the three tabs under Diagnostics—**Targets**, **Devices**, and **Applications**.

All three tabs have Location and Target Set fields, which enable you to filter and refresh the displayed data below. The Location field displays the same list of Leaf Locations as seen in the drop-down on the Project Summary page. None of these tabs will display any rows until scanning has commenced.

The Targets tab summarizes the targets for which scans were attempted and identifies different statuses such as waiting, in-progress, detected, not detected, error, and other:

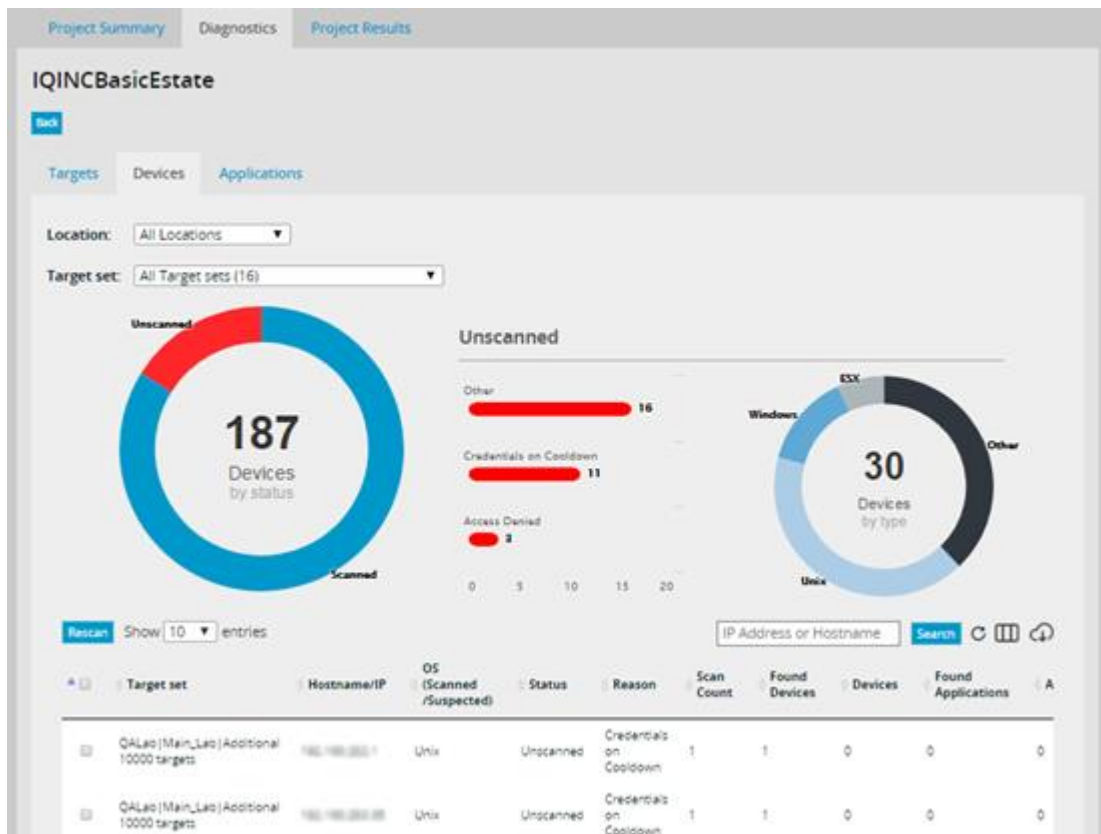
- Waiting and in-progress are for non-completed targets.
- Detected, not detected, error, and other are for scan-completed targets.

Clicking any of the status types causes the table contents to refresh and display corresponding targets for that specific status.

If a target is rescanned, it's changed from a completed target set status to an incomplete status. The target in the data table will reappear with the latest start time stamp and current target status.

If a target is excluded, then the Targets tab shows a status of other and a status of target excluded. If the target is then included, the Status and Phase fields will not update 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 can be further filtered by clicking on a colored slice.

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

- **Chart 2** (the bar chart in the center) 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.

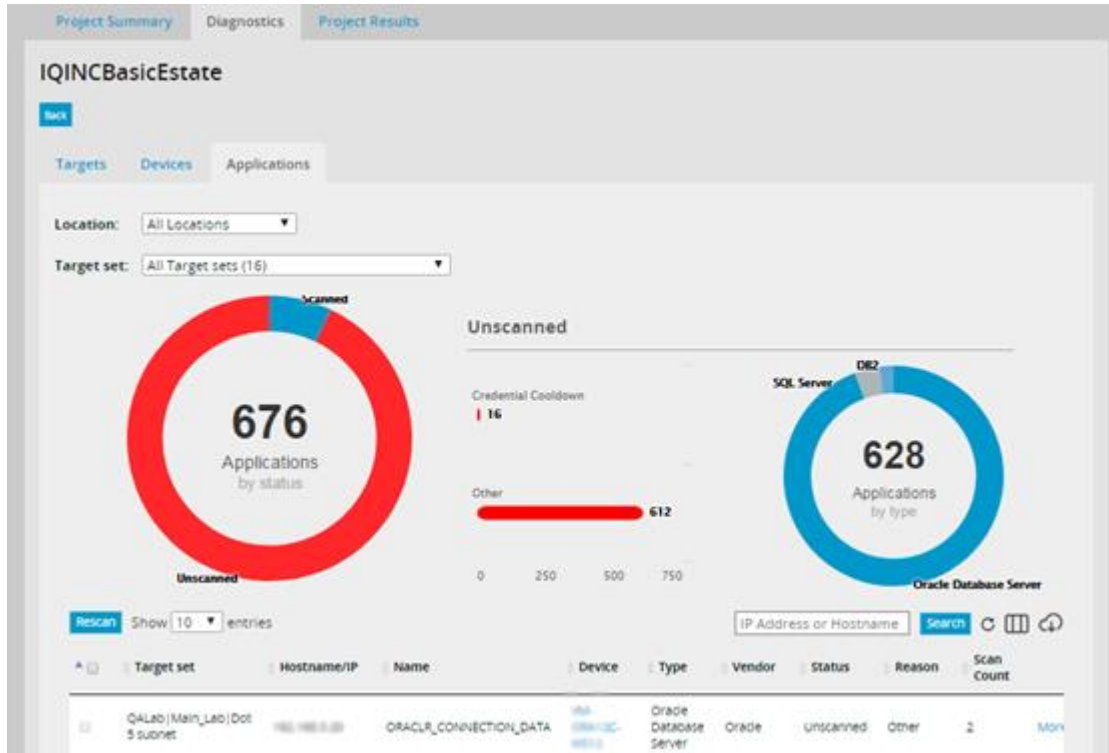
**The table** at the bottom of the page summarizes the scan results for each individual target. This table lists all the targets on which a scan has been attempted and summarizes how the scan went.

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 **Target Sets** 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** area 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.

Performance

Database Server

DB Server Name	Page Reads(sec.)	Page Writes(sec.)	Memory Usage%	CPU Usage%
vm-qase	0	0	1	0

Scanning Server

Show 10 entries

Search:

Name	Active Jobs	IO (In) %	IO (Out) %	Network (In) %	Network (Out) %	CPU %	Memory %	Activity
VM-QASE	0	0	0	0	0	0	40	Config

Showing 1 to 1 of 1 entries

Previous1Next

## 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.

Scanning Activity							
Show 10 entries		Search:					
Target	Server	Start Time	End Time	Source	Phase	Status	Action
192.28.0.1		16/12/2015 12:06:18	16/12/2015 12:06:58	Project	Complete	Success	More...
192.28.0.10		16/12/2015 12:05:38	16/12/2015 12:07:56	Project	Complete	Success	More...
192.28.0.11		16/12/2015 12:05:38	16/12/2015 12:07:56	Project	Complete	Success	More...
192.28.0.12		16/12/2015 12:05:38	16/12/2015 12:07:58	Project	Complete	Success	More...
192.28.0.13		16/12/2015 12:05:38	16/12/2015 12:07:59	Project	Complete	Success	More...
192.28.0.14		16/12/2015 12:05:38	16/12/2015 12:07:59	Project	Complete	Success	More...
192.28.0.2		16/12/2015 12:05:38	16/12/2015 12:06:12	Project	Complete	Success	More...
192.28.0.3		16/12/2015 12:05:38	16/12/2015 12:06:12	Project	Complete	Success	More...
192.28.0.33		16/12/2015 12:05:38	16/12/2015 12:06:42	Project	Complete	Success	More...

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.

**System Audit Log**

From: 09/12/2015 To: 16/12/2015 [Go](#)

Show 10 entries Search:

Changed Date	Username	Change Type	Object Type	Field Name	Old Value	New Value
16/12/2015 11:50	admin	Update	Location	Servers		IQINC(25/80%/80%/8...
16/12/2015 11:50	admin	Insert	LocationConnection...	IsEnabled		False
16/12/2015 11:50	admin	Insert	LocationConnection...	ConnectionConfigura...		Certificate Analysis P...
16/12/2015 11:50	admin	Insert	LocationConnection...	IsEnabled		False
16/12/2015 11:50	admin	Insert	LocationConnection...	ConnectionConfigura...		DB2
16/12/2015 11:50	admin	Insert	LocationConnection...	IsEnabled		False
16/12/2015 11:50	admin	Insert	LocationConnection...	ConnectionConfigura...		DNS Provider
16/12/2015 11:50	admin	Insert	LocationConnection...	IsEnabled		False
16/12/2015 11:50	admin	Insert	LocationConnection...	ConnectionConfigura...		ICMP Provider
16/12/2015 11:50	admin	Insert	LocationConnection...	IsEnabled		False

## 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.

**Tracing Log**

```
[ERROR] =====
OCCURED AT : 16 December 2015 12:56:40
LOGIN USER: application end
Url Request Path: ~
MESSAGE:

_shutDownMessage=HostingEnvironment initiated shutdown
HostingEnvironment caused shutdown

_shutDownStack= at System.Environment.GetStackTrace(Exception e, Boolean needFileInfo)
at System.Environment.get_StackTrace()
at System.Web.Hosting.HostingEnvironment.InitiateShutdownInternal()
at System.Web.Hosting.PipelineRuntime.StopProcessing()
----- STACKTRACE -----
```

[Download Log File](#)



## 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.

The screenshot shows the 'Scanning Server Configuration' interface. At the top, a dropdown menu 'Select A Server' is set to 'VM-PC3-10'. The interface is divided into two main sections: 'Status' and 'Configuration'.

**Status Section:**

- Server Name:** VM-PC3-10
- Installation ID:** 2ffe1ec1-fd03-44aa-a081-88b316cab71f
- Status:** Running (indicated by a green box)
- Product Adapters:** 45 (with a link to 'More Info...')

**Configuration Section:**

- Max Disk IO Usage Percent:** A slider set to 80 (range 1 to 100).
- Max Memory Usage Percent:** A slider set to 80 (range 1 to 100).
- Max CPU Usage Percent:** A slider set to 80 (range 1 to 100).
- Max Network IO Usage Percent:** A slider set to 80 (range 1 to 100).
- Max Active Jobs:** A slider set to 25 (range 1 to 100).
- Job Polling Count:** A slider set to 5 (range 1 to 50).
- Queue Processing Enabled:** A checkbox that is checked.

At the bottom right of the configuration section are two buttons: 'Update' and 'Copy To'.

- **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.
- **Job Polling Count:** The number of jobs the scan engine will start at any one time. The scan engine will continue polling this number of jobs until it has reached the max active jobs value.
- **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.



The screenshot shows the 'System Settings' dashboard with the 'Product Adapter Manager' tab selected. Below the tab are three sub-tabs: 'Activation', 'CyberArk', and 'Configuration'. The main content area displays a table with the following data:

Vendor	Adapter Name	Version	Enabled
Apache	Apache HTTP	1.0.0	<input checked="" type="checkbox"/>
Citrix	XenServer	1.0.0	<input checked="" type="checkbox"/>
IBM	IBM Business Process Manager	1.0.0	<input checked="" type="checkbox"/>
IBM	Cognos TM1	1.0.0	<input checked="" type="checkbox"/>
IBM	Content Manager	1.0.0	<input checked="" type="checkbox"/>
IBM	Content Manager OnDemand	1.0.0	<input checked="" type="checkbox"/>
IBM	DB2 Database	1.0.0	<input checked="" type="checkbox"/>

### 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 *Data Center Discovery—Scan Engine Prerequisites Guide* for CyberArk prerequisite details.

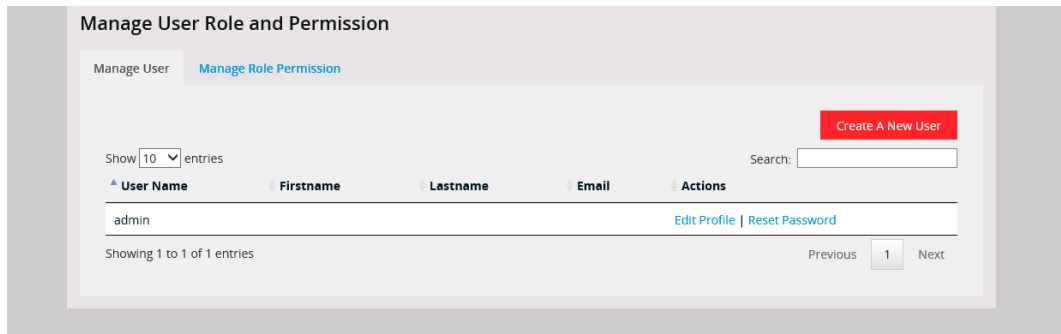
## User settings

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.

Reset User Password

Reset For  
admin

New Password

Confirm Password

Reset Cancel

## 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.

Update A User

Profile

Disabled ☐

Username admin

Firstname IQSonar

Lastname Administrator

Email iqsonar.administrator@iquate.com

Roles

☒ Administrator

Update Cancel

## 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.

**Create A User**

Profile

☒ Is Active Directory User ⓘ

Domain Name

Username

Firstname

Lastname

Email

Permissions

☒ Administrator

Create Cancel

### 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.

**Update A User**

Profile

Disabled ☐

Domain Name

Username

Firstname

Lastname

Email

Roles

☒ Administrator

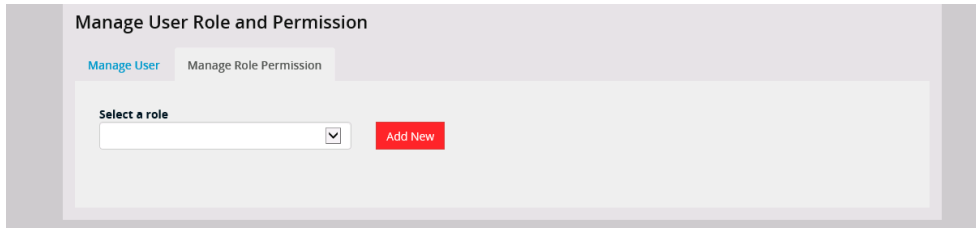
Update Cancel

## User settings – Manage role permission

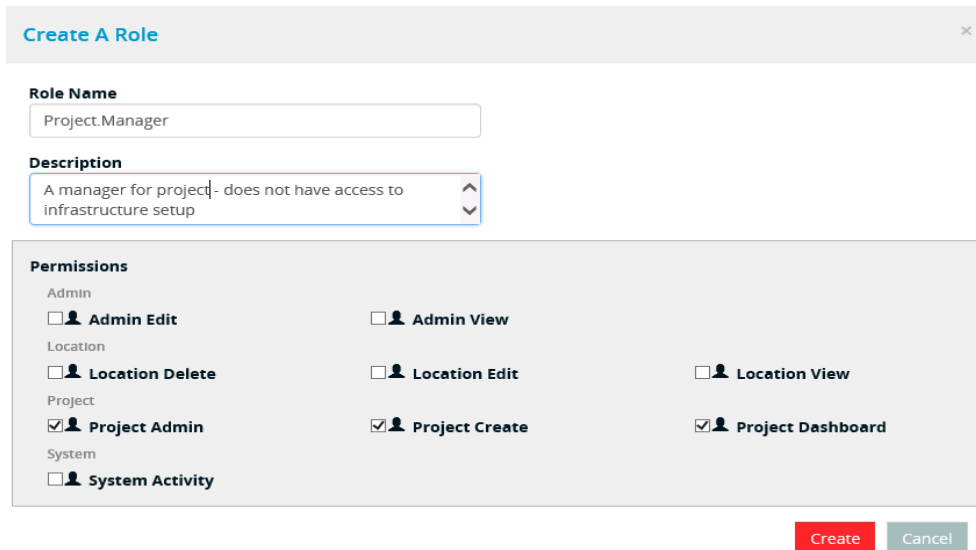
Roles allow for subsets of the functionality (provided by the dashboard) to be enabled or disabled on a per-user basis. This process also ties in with the creation of users described in the previous section. You can define a role that limits the dashboard functionality. Users can then be assigned this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

<b>Admin</b>		
<input type="checkbox"/> <b>Admin Edit</b>	<input type="checkbox"/> <b>Admin View</b>	
<b>Location</b>		
<input type="checkbox"/> <b>Location Delete</b>	<input type="checkbox"/> <b>Location Edit</b>	<input type="checkbox"/> <b>Location View</b>
<b>Project</b>		
<input checked="" type="checkbox"/> <b>Project Admin</b>	<input checked="" type="checkbox"/> <b>Project Create</b>	<input checked="" type="checkbox"/> <b>Project Dashboard</b>
<b>System</b>		
<input type="checkbox"/> <b>System Activity</b>		

**Create** **Cancel**

## Configuration settings

The screenshot shows the 'System Settings' window with tabs for 'Product Adapter Manager', 'Activation', 'CyberArk', and 'Configuration'. The 'Configuration' tab is active. A blue 'Update' button is in the top right. The 'Job Serving' section is expanded, showing the following settings:

Setting	Value	Help Icon
Enable Job Logging	OFF	?
Auto Deleted Job Log	ON	?
Target Expand Rate	2048	?
Max Count Multiple To Queue	1.5	?
Min Queued Threshold	0.66	?
Save Target XML	OFF	?

The 'Scanning' section is also expanded, showing:

Setting	Value	Help Icon
Jobs Timeout (mins)	120	?

You can modify the following configuration settings.

### Configuration settings - Job serving

- **Enable Job Logging:** When enabled (ON), job serving diagnostics are written to the jobs.t\_Log table. OFF indicates no diagnostic information will be written.
- **Auto Deleted Job Log:** When enabled (ON), job serving diagnostic data in the jobs.t\_Log table is automatically deleted once job logging is disabled. Set to OFF to keep this data after job serving logging has been disabled.
- **Target Expand Rate:** Determines the total number of IPs (from range and subnet target sets) to add to the queue upon execution of queue step 1. This stops the queue from becoming flooded when ranges are expanded more quickly than they can be served.
- **Max Count Multiple To Queue:** Determines the number of jobs to queue for each scan engine. The default is 1.5, which means for a scan engine with a max jobs limit of 100, 150 jobs (100 x 1.5) are queued for that server. This is to keep the scan engines operating at full capacity.
- **Min Queued Threshold:** When the number of jobs queued for a server is below a certain percentage of its max jobs setting, more jobs are queued for it. This prevents the queue from becoming flooded if the server has multiple long-running jobs.
- **Save Target XML:** When enabled (ON), the XML for each target is saved in the job table. Saving target XMLs results in massive data bloat, so this option is set to OFF by default.

### Configuration settings - Scanning

**Jobs Timeout (mins)** applies a time limit to each scan job. After the time limit expires, the job is terminated and any artifacts already discovered will be saved to the database. The job is assigned a status indicating it was completed after a timeout. The value of 0 indicates that no time limit should be applied to the job. The default value is 60 (mins).

## Appendix A: Key terms, emails, and links

Term	Description
CSV	Comma-separated values
IIS	Internet Information Services
Ivanti support	<a href="https://www.ivanti.com/support/ivanti-support">https://www.ivanti.com/support/ivanti-support</a>
Microsoft support for KB932370	<a href="https://support.microsoft.com/kb/932370">https://support.microsoft.com/kb/932370</a>
NETSTAT	A command on the command prompt to access ports.
Oracle Licensing Management Services (LMS)	<p>Oracle LMS is an organization that promotes the management, governance, and awareness of the proper use and distribution for Oracle systems through expert services.</p> <p>*as defined by Oracle</p>
Oracle Rac	Real Application Cluster
Partitioning (Hard)	<p>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.</p> <p>*as defined by Oracle</p>
Partitioning (Soft)	<p>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.</p> <p>*as defined by Oracle</p>
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