freshworks

Device42 Implementation Guide

Table of Contents

Version Number 1.0

Last Updated: December 3, 2025

Welcome

Welcome to the Device42 Implementation Guide, which will guide you through implementing Device42. This guide is based on our experience implementing Device42 for thousands of customers, and while each customer is unique, this guide presents the most commonly followed steps to help make you successful.

Who is this Guide For?

This guide is designed for those persons responsible for implementing Device42. This guide assumes these persons have:

- An understanding of Network Engineering as well as their IT environment
- Completed the following Device42 training modules available at **https://academy.device42.com/**
  - Device42 Certified Technical Administrator (DCT-A) Course
  - Implementation Fundamentals: Deployment
  - Implementation Fundamentals: Discovery

How do I use this Guide?

This Guide is designed to be viewed electronically, as it includes links to online documents. We recommend you open the guide on one monitor while you implement Device42 on another monitor.

What is Device42?

We refer to Device42 as an Advanced IT Asset Management, or Advanced ITAM solution. It will provide you insights into your infrastructure assets and enable you to manage and transform your IT environment with greater speed, efficiency, and reduced risk.

At its core, Device42 is a discovery system that automatically collects vast amounts of data from your entire IT environment, from network devices to software, applications, and storage, to build a comprehensive inventory of your IT assets in support of your Service Management needs.

What Comprises Device42?

Device42 comprises several modules that can either be purchased together as part of a solution or individually based on your needs.

Our **Core** product includes:

- Comprehensive Discovery: Device42 automatically finds and maps out virtually all of your IT infrastructure, whether it's located in your own data center, running on virtual machines, or hosted in various cloud environments. This "deep and wide" discovery gathers critical details about your physical servers, network devices, containers, and end-user devices. Most of this discovery is agentless, meaning it can gather information without requiring software agents to be installed on your devices. However, if you require it, Device42 has an agent that can be installed to collect data for these devices.
- Robust Data Center Infrastructure Management (DCIM) capabilities, allowing you to see the physical layout of your data centers, including rooms, racks, and cable management.
- Built-in Central IT Database (CMDB): All your discovered information is organized into a centralized Configuration Management Database (CMDB). Think of this as a single, highly accurate, and constantly updated master record for all your IT components.
- Intelligent Data Enrichment (EnrichAI): Device42 uses Artificial Intelligence (AI) through its EnrichAI feature to enhance your discovered data. This means it automatically adds valuable information from third-party sources, such as vendor details and operating system information. This helps you not just know what you have, but also when it might need attention or replacement.

Our **Software and License Management (SLM)** module helps you discover all installed software on Windows and Linux machines across your IT estate by cataloging installed packaged software and installed patches and versions. The module enables you to compare current software usage to license counts, enabling you to understand software utilization. The SLM module can also detect prohibited software, helps track license agreements and expiration dates, and can identify purchased versus installed software to ensure licensing compliance. Alerts can be configured to notify you of critical events, such as expiring licenses or the detection of prohibited software.

Our **Storage** module provides storage discovery, offering agentless, vendor-neutral visibility into various storage systems, showing how everything is configured. Storage Discovery also shows the compute systems that are dependent on the Storage Array which can help with Disaster Recovery planning and migration activities.

Our **Application Dependency Mapping (ADM)** module is a powerful Advanced ITAM module that provides crucial visibility into how your IT assets interconnect, especially focusing on application relationships. This goes beyond a simple inventory list to show the intricate web of dependencies that power your business services. ADM is based on Service-to-Service communications, with information collected via Netstat, which enables Device42 to build relationships between your servers over time.

Our **Netflow** module enhances visibility into network communication and connectivity within an IT environment. It augments data gathered by Device42's other auto-discovery methods, such as SNMP, WMI or WinRM for Windows, and SSH for Linux. Netflow works hand-in-hand with Device42's ADM module to provide crucial additional connection information from network devices to your business applications. It's particularly useful for capturing ephemeral connections that might not be consistently identified through ADM's regular sampling intervals.

Our **Resource Utilization** module gathers statistics on a machine's disk, network I/O, CPU, and memory utilization over time. This data is then leveraged by Device42's **Cloud Recommendation Engine (CRE)** to provide exact details needed to plan your next cloud deployment, including comparing costs across different cloud service providers to help with right-sizing your cloud deployment.

All of our modules leverage our **Insights+ Reporting and Dashboarding engine**. Device42 transforms the raw discovered data into consumable IT operational intelligence. It offers advanced visualizations, pre-built dashboards, and customizable reports that help IT teams make smarter business decisions based on real-time information.

What are Device42’s Key Benefits?

Device42 helps organizations large and small, across many industries. Below are some ways Device42 can benefit your organization:

Improved Planning: By providing a clear and comprehensive view of your entire IT estate, your organization can save time and money and better plan your capital expenditures (like hardware or cloud resources) more effectively.

Financial Savings: Customers have reported significant financial savings in areas such as IT equipment and software consolidation, with some seeing improvements of up to 30%.

Enhanced Compliance: Device42 makes it much easier for IT teams to meet internal and external regulatory compliances and pass audits. Having a complete and accurate inventory will help you proactively achieve continuous compliance with less disruption to business operations.

Reduced Risk and Better Decision-Making: By understanding the interdependencies between IT assets, your organization can decrease risks associated with planned changes and make informed decisions, ultimately improving IT agility.

In essence, Device42's Advanced ITAM provides a single, trusted source of truth for all your IT assets, giving you unparalleled visibility and actionable insights to efficiently manage your technology, plan for the future, and ensure compliance, thereby helping your organization run its IT operations more effectively.

What is the Scope for this Document?

As reviewed, Device42 comprises several modules. This document will help you implement Device42's **Core**, **Software License Management**, and **Storage** modules. The specific IT asset categories considered in scope for this guide are as follows:

- Network Devices
- Virtual environments
- Windows and Linux/Unix servers
- Software
- Cloud environments
- Storage environments
- Certificates
- Device Warranties

You can configure and run additional discovery jobs; they are accessible from the Device42 **Discover** menu within the UI. We recommend you run any of these jobs after you have run discovery for the relevant above-listed asset categories.

Note that some of the discovery jobs for the IT categories listed above include options that, when enabled, collect data for the **Application Dependency Mapping (ADM)** module. This guide does not include details to configure these discovery options; Device42 recommends enabling them approximately 30 days after discovery jobs have been running effectively. There is a separate User Guide for implementing ADM.

How is Device42 Implemented?

We view a Device42 implementation as occurring in four phases, what we refer to as "The 4 Ds of Device42". This structured approach is based upon best practices from thousands of implementations. These four phases are **Deploy**, **Discover**, **Data Validation**, and **Display**.

Deploy
Discover
Data Validation
Display

Deploy

The Deploy phase ensures you install and properly configure the required Device42 components to discover your infrastructure. You will install and configure the Device42 Main Appliance (MA), Remote Collectors (RCs), and the Windows Discovery Service (WDS) instances if Windows systems are in scope. While Device42 primarily performs agentless discovery, you may optionally install Device42 Discovery Agents onto your machines running Windows, Linux, UNIX, and macOS operating systems.

The Deploy phase also includes you properly configuring network settings and firewall rules to enable communication with all your relevant infrastructure components. Appropriate access permissions need to be granted to Device42, adhering to the principle of least privilege, after which you should perform connectivity tests to confirm proper functionality.

Discover

Once the Deploy phase is complete, as part of the Discover phase you will configure and execute discovery jobs to discover your IT environment. You will configure discovery job settings, including IP ranges, credentials, and schedules, for various components such as SNMP devices, Hypervisors, Windows and Linux servers, and cloud resources. At the beginning of this phase you will execute discovery jobs to identify and inventory your infrastructure. Then you will review discovery scores that provide you insight into the success and accuracy of these jobs. You will use these discovery scores to identify any discovery job issues that you will then remedy. Finally, you will schedule these discovery jobs to automatically run at specified time intervals.

Data Validation

The Data Validation phase follows the Discover phase, where you will ensure the discovered data is complete and accurate. You will perform sample checks comparing discovered data against other existing data sources to verify data accuracy, completeness, and consistency. You will resolve any data errors or inconsistencies.

Display

Once your discovered data is validated, you will make sure it is consumable by users and provides actionable insights so you and others can make impactful business decisions. You will verify the accuracy of all relevant data visualizations (charts, graphs, maps, etc.). You will configure reports or custom dashboards to display key metrics, and create and schedule reports that provide insights into infrastructure status, changes, and performance. In short, you will ensure you and others can leverage the data Device42 discovered about your IT environment to make better IT and business decisions.

What are Device42 Critical Success Factors?

We have helped thousands of customers implement Device42, and have not only learned the best way to implement Device42 but have also learned customer best practices that help ensure a quick and successful implementation. Please give careful consideration to each of the critical success factors below.

Have Clarity of Purpose

Gain internal consensus regarding your initial Device42 implementation goals, defining what “success” means. This will help focus the Device42 implementation.

Identify Supporting Departments and Persons

Your Device42 implementation will likely require support from persons residing in various other departments within your organization. This document details the information and tasks required to implement Device42, and **it is your responsibility to determine who to enlist for support and to help ensure their timely support**.

Leverage Executive Sponsors

Have Project Stakeholders and/or Executive Sponsors reach out to the leaders of departments from which you require assistance and convey the following:

- An overview of the project, including its goals
- The value the project will provide to the business
- The role their department will play in the project’s success

This step will help ensure you get the support you require.

Share Information and Documentation

Device42 provides a wealth of documentation at **https://docs.device42.com/**, including documentation and videos linked to in this guide. Encourage others to access this online documentation as it will likely include answers to questions they have. Device42 users also have access to **Device42 Academy**, which includes a variety of courses, including courses in implementing Device42. We encourage you to contact us and sign up for classes.

Get Project Management Assistance if necessary

It can sometimes be difficult to manage an implementation that requires coordination between different departments or persons, particularly when you are also the implementation Technical Lead. Project Managers can help facilitate meetings, can help hold persons accountable for deliverables, and can escalate to management when required.

Contact Device42 Support if you get stuck
You can contact Support via email, phone, or our Support Portal. Note that you can contact a Device42 Support agent Monday through Friday from 7am through 6pm ET, and again from 11pm through 6am ET. You can also access our Support Portal and Knowledge Base Portal at **https://support.device42.com/hc/en-us**, can email support at **support@device42.com**, and can call us at 1 (844) 424-2422.

Implementing Device42—the 4 D's

Preface

Each of the four Device42 Implementation phases is described in detail below. Each phase contains a series of tasks, and each of these tasks requires steps to complete. For each task you may find one or more of the following:

- A simplified list of steps—this will enable you to **understand** the steps, but may in some cases lack all the detail to complete the tasks
- A link to a web page—the web page typically includes all the detail you will need to **perform** the task, including options you may or may not choose to enable
- A link to a video—the video will enable you to **see** the task performed, along with related commentary

This document also includes Appendices that will be referenced later in this document. These Appendices contain more technical information you may need to reference yourself and/or provide to others involved in the implementation.

Phase 1—Deploy

In the Deploy phase you will deploy and configure the Device42 Main Appliance (MA) and Remote Collectors (RCs) as self-contained virtual appliances on your network, install and configure Windows Discovery Service (WDS) instances, and optionally install and configure Device42 Discovery Agents. Prior to performing these tasks you must understand each of these components, their prerequisites, and how they interoperate.

Device42 Technical Component Overview

Main Appliance: The Device42 Main Appliance (MA) is a self-contained and self-maintaining virtual appliance that serves as the core component of the Device42 system. It is a pre-configured virtual appliance (built on Linux) that your organization hosts, enabling full protection under your data center security architecture and policies.

Remote Collector: The Remote Collector (RC), is a lighter pre-configured virtual appliance (built on Linux), used to perform agentless discovery across network segments. It also provides scalability by offloading discovery workloads from the MA. The RC will connect to your non-Windows targets for discovery as well as hand Windows discovery jobs off to the WDS, if applicable. We require that you install at least 1 RC for any Device42 deployment.

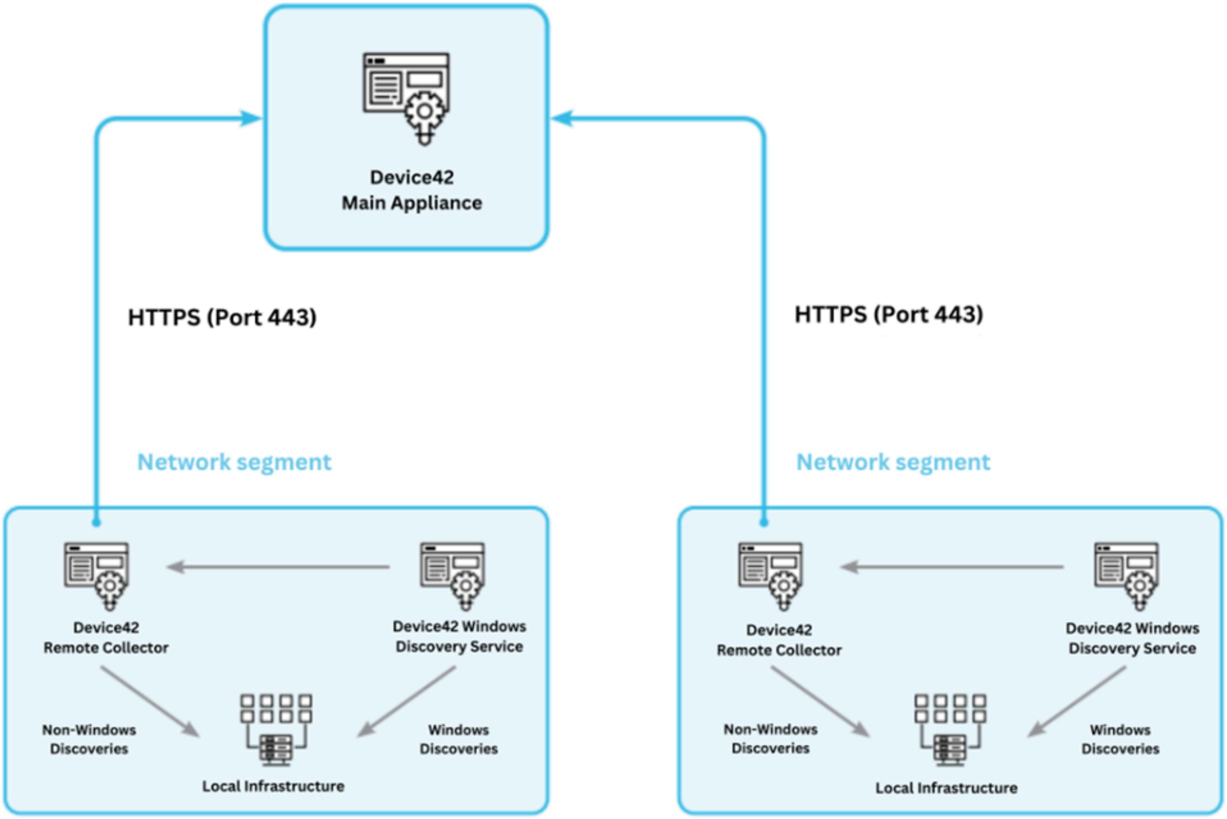
Windows Discovery Service: The Windows Discovery Service (WDS) is a .NET service which runs on a Windows system and makes WMI queries on behalf of the Linux-based RC and MA. If you'll be running Windows discoveries, you must deploy at least 1 WDS instance and connect it to an RC.

Discovery Agent: The Device42 Discovery Agent can be optionally deployed into your environment. It is typically deployed either on devices like laptops that are not consistently connected to your corporate network or in segmented network environments where agentless discovery is not permitted or possible. The Device42 Agent can run on Windows, macOS, Linux, and other Unix-based operating systems.

Device42 Reference Architecture

The Main Appliance, Remote Collectors, and Windows Discovery Service all play a role in discovering your IT environment. Device42 is deployed in a hub-and-spoke architecture; each RC/WDS collects data and syncs it back to the centralized MA. It is typically recommended for RCs and WDS instances to be deployed in pairs, if Windows discovery is required.

The image below depicts a Production environment consisting of one Main Appliance and two sets of Remote Collectors and Windows Discovery Service instances.



Click **here** to view a video describing the architecture depicted in the above image.

It is critical that network settings are correctly configured and firewall rules properly enabled to grant appropriate access permissions while adhering to the principle of least privilege. Once configured, we strongly recommend you perform connectivity tests to confirm these changes were successfully made.

A reference list of all ports used to gain access to targets to be discovered can be found **here**. **It is critical to provide this link to network personnel so they can ensure the necessary ports are open so Device42 can discover your infrastructure.**

Security Notes:

- All data in transit from WDS to RC and RC to MA is over SSL or HTTPS.
- All data stays at rest within the MA in an end-user environment.
- Only data voluntarily shared by the end user leaves the premises.

Deployment Component Sizing Recommendations

The table below includes Main Appliance, Remote Collectors, and Windows Discovery Service sizing recommendations.

Table 1—Component Sizing Recommendations

Device42 Component	Sizing/Notes
1 Main Appliance (virtual appliance)	Small to Medium Environments (<2500K devices): ● 4 vCPU ● 16GB RAM ● 150GB vDisk (SSD or flash disk recommended)
	Medium to Large Environments (>2500K devices): ● 16 vCPU ● 64GB RAM ● 150GB vDisk (SSD or flash disk recommended)
	**For **any** environments where Application Dependency Mapping (ADM), Resource Utilization (RU) and/or Storage discovery is included, we recommend following the guidelines for the Medium to Large Environments**
Remote Collector(s) (virtual appliance)	1 RC per 2,000-2,500 devices for basic discovery jobs (i.e. network or hardware scans); 1 RC per 1,000-1,200 devices when enabling ADM, RU, or Power Monitoring. ● 2 vCPU ● 4GB RAM ● 50GB vDisk
Windows Discovery Service (WDS) (.NET installer)	1 WDS instance per 2,000-2,500 devices for basic discovery jobs (i.e. network or hardware scans); 1 WDS instance per 1,000-1,200 devices when enabling ADM, RU, or Power Monitoring. ● 2 vCPU ● 8GB RAM ● 50GB vDisk (minimum)

We recommend a dedicated resource pool for the virtual appliance to ensure there is no resource contention. Additionally, as Device42 utilizes a database within the virtual appliance we recommend solid-state storage, or similar storage optimized for database operations.

For Windows infrastructure, Device42 requires a WDS to be installed on one machine per discovery segment/Remote Collector.

Deploy Tasks

Phase 1 Task 1: Deploy the Main Appliance

1.1.1. Size the Main Appliance Server

Device42 Main Appliance server sizing is based on the quantity of devices to be discovered. Refer to *Table 1—Component Sizing Recommendations* to properly size your Device42 Main Appliance server.

1.1.2. Install and Configure the Main Appliance

Main Appliance Prerequisites

Device42 operates with only five ports open to the virtual appliance:

- Port 80: Redirects to port 443
- Port 443: Web (HTTPS)
- Port 4242: Redirects to port 4343
- Port 4343: Appliance manager (HTTPS)
- Port 404: SSH for limited console menu operations

Make sure the appropriate network personnel are made aware of these requirements.

Main Appliance Installation and Configuration

The MA can be installed on virtual environments like VCenter, Microsoft HyperV, and Citrix Xen server, as well as cloud platforms like Amazon Web Services and Microsoft Azure. Click **here** to navigate to the main Device42 Installation web page, where you will find sub-pages that include MA installation instructions for all supported virtual environments.

Note:

- When following the installation steps in the above linked page, in addition to setting a static IP address, also set the **NTP Time settings** and **Time Zone**.

1.1.3. Apply Your License

After installing the MA you will be prompted to apply for your new license file. Perform these steps:

1. Click the **Choose File** button.
2. Select the file and click **Open**
3. Click the **Upload & Apply** button

1.1.4. Register the MA

You have 30 days after MA installation to register. When prompted, click the **Register Now** button.

1.1.5. Create a Passphrase to Encrypt Device42 Passwords

You must create a passphrase that will encrypt passwords within Device42. To create a passphrase, perform these steps:

1. Choose **Tools…Password Security**
2. Enter a passphrase and click the checkbox stating you will save the passphrase in a secure location
3. Click the **Save** button

To view a video on installing and configuring the MA, click **here**.

Phase 1 Task 2: Deploy the Remote Collectors

1.2.1. Size the Remote Collectors

Device42 Remote Collector server sizing is based on the quantity of workloads to be discovered. Refer to *Table 1—Component Sizing Recommendations* to properly size your Device42 Remote Collector servers.

1.2.2. Install and Configure the Remote Collectors

The Remote Collectors can be installed on the Hypervisor of your choice. Click **here** to link to the page where you can download the RC installer.

Note that while the above linked page includes an *Initial (First-Boot) Network Configuration* section for configuring the Remote Collector, **we recommend you instead reference *Appendix A- Configuring your Remote Collector* to configure the Remote Collector**.

To view a video on configuring the RCs, click **here**.

Phase 1 Task 3: Deploy the Windows Discovery Service

1.3.1. Size the Windows Discovery Service Servers

Windows Discovery Services server sizing is based on the quantity of workloads to be discovered. Refer to *Table 1—Component Sizing Recommendations* to properly size your Device42 Remote Collector servers.

1.3.2. Install the Windows Discovery Service

Click **here** to link to the page where you can both download the WDS installer and access WDS installation documentation.

To view a video on installing the WDS, click **here**.

Phase 1 Task 4: Deploy the Discovery Agent

We recommend you use agentless discovery whenever possible, as it makes deployment easier, minimizes impact on target systems, and reduces operational overhead for most environments. However, as mentioned, you may choose to install the Discovery Agent on devices like laptops that are not consistently connected to your corporate network or in segmented network environments where agentless discovery is not permitted or possible.

1.4.1. Discovery Agent Supported Platforms

Device42 autodiscovery agents are available for deployment on the following platforms:

- Windows 64-bit (Recommended)
- Windows 32-bit
- Mac—Intel
- Mac—ARM
- Linux 32-bit
- Linux 64-bit
- FreeBSD 32-bit
- FreeBSD 64-bit
- OpenBSD 32-bit
- OpenBSD 64-bit
- Solaris Sparc 64-bit

1.4.2. Install the Discovery Agent

The agent can be downloaded from the Main Appliance and can either be run from the command line or can be scheduled using a scheduling program. Click **here** to access the Device42 Discovery Agent main page that provides these instructions as well as additional agent information.

You can also install versions of the Windows and Mac discovery agent as a service. Click **here** for more information about the Windows Discovery Agent Service Wrapper.

The Windows or Linux Discovery Agent can also be leveraged in an *offline* mode, where it creates a log of discovered data, which is uploaded to a machine for processing, and is finally uploaded to your Device42 Main Appliance. Click **here** for more information about this option.

Optional Deploy Tasks

Below is a list of tasks that can be performed either now or in the future.

Phase 1 Task 5: Back up your Deployed Environment

You should back up your deployed environment so you can quickly restore a configuration in case of emergency.
To back up your environment, perform the following steps:

1. Hover over **Tools**, then choose **Appliance Manager** from the **Settings** section. This will take you to the Device42 Appliance Manager login screen.
2. Enter the Username and Password to log in (default Username is *d42admin* and default Password is *default*). We recommend changing these credentials once logged in.
3. Follow the steps listed **here** to configure your backup.

Phase 1 Task 6: Add Users

Adding users will help you better track user changes and define user permission levels.
To add new administrators, perform the following steps:

1. Hover over **Tools**, then choose **Administrators** from the **Admins & Permissions** section.
2. Click either **Create Local Admin** or **Create Active Directory Admin** (if AD is connected to the Main Appliance)
3. Fill out the Add Admin User page and click the **Save** button.

Click **here** for more information to add an Active Directory User as a Device42 Administrator. For information on setting up an Active Directory/LDAP User Sync click **here**, and for information on configuring Device42 Role-Based Access Control click **here**.

Phase 1 Task 7: Configure Audit Logs

Every change made to Device42 Configuration Items (CIs), via the user interface, autodiscovery jobs, RESTful API calls, or imports, is recorded as history, and this history is maintained in Audit Logs.
To change the log settings, perform the following steps:

1. Hover over **Tools**, then choose **Log Settings** from the **Settings** section.
2. Click the **Edit** button.
3. Edit the settings.
4. Click the **Save** button.

Note the longer the duration, the more disk space will be used. For long term storage, you may leverage webhooks (click **here** for more information about webhooks).

Click **here** for more information about Audit Logs.

Phase 1 Task 8: Set up a Mail Server

Setting up a mail server enables automated email notifications and alerts for events like discovery scans, system updates, backup completions, reports, and custom workflow actions.

Click **here** for instructions on adding mail server settings.

Deploy Phase Checklist

The Deploy phase is considered complete when:

- ☐ Device42 Infrastructure Installation is complete: The Device42 MA and RCs are properly deployed and configured; WDS/WMI is selected as the preferred path forward and WDS is installed on RCs (if Windows is in scope for the deployment); and the Discovery Agent is installed if required.
- ☐ Network Configuration is complete: Network settings and firewall rules are properly configured to allow Device42 to communicate with all relevant infrastructure components in scope for the deployment.
- ☐ Access and Permissions are granted: Appropriate access permissions are granted to Device42, ensuring it can access all necessary systems and devices across the various in-scope jobs the customer will be running.
- ☐ Initial Connectivity Checks have passed: Initial connectivity tests confirm that Device42 can communicate with key infrastructure components without errors.
- ☐ Device42 environment is backed up and scheduled for future backups. Main Appliance Meta Data, SSH key pair, System Configuration Files are backed up; Remote Collector Meta Data, TLS Key Pair, Configuration files, and Data Files are backed up. Future backups are scheduled to occur.
- ☐ Additional Admin users have been defined.
- ☐ Audit Log configuration is configured as desired.
- ☐ Mail Server is configured.

Deploy Phase Support

At the conclusion of Phase 1 your Device42 Main Appliance, Remote Collectors, and Windows Discovery Service should be deployed and configured. Your network should be configured with the proper access granted, and initial connectivity checks to your infrastructure components should be successful.

Should you have questions or issues, please first access *The Hitchhiker's Guide to Device42*, our online documentation page that can be accessed **here**. You can easily search this guide for any questions you may have. You may also access the Device42 Support page **here**, where you can submit a request, access our Knowledge Base, or access other general information.

Phase 2—Discover

In the Discover phase you will configure, execute, and schedule jobs that discover your IT landscape and collect and store the associated data.These discovery jobs systematically scan and inventory your IT infrastructure, using Device42's automatic discovery capabilities to populate the database. This includes everything from network devices to software, applications, and storage.
This phase is broken down into four tasks:

- Task 2.1—Prepare for Discovery Jobs
- Task 2.2—Create and Run Discovery Jobs
- Task 2.3—Validate Discovery Jobs
- Task 2.4—Schedule Discovery Jobs

Note that the **Validate** and **Schedule** tasks can be performed immediately following *Task 2.2—Create and Run Discovery Jobs* for **each** discovery job (vs. validating and scheduling after running **all** the discovery jobs).

Discovery Job Best Practices

Below is a list of basic discovery job Best Practices. While this list is long, discovery is the foundation of Device42, and it is therefore important that you understand and implement these best practices. We recommend you refer back to this list often.

Discovery Job Best Practices—Discovery Job Planning

1. Limit your discovery focus—there are a variety of discovery jobs and it is tempting to immediately run as many as possible. Focus on the jobs that will deliver the maximum value to your organization; these typically include jobs like SNMP, Virtualization, Windows, Linux and Unix, Cloud, Storage, and Certificate. You can run additional discovery jobs once the core jobs have been created and scheduled.
2. Organize your discovery jobs—there are different discovery job types (e.g. SNMP, Hypervisor, Windows, Linux, Cloud, Storage, etc.) and each of these will likely have multiple jobs based on location, Data Center, Region, etc. or due to the large number of items to be discovered. Consider how you want to organize each discovery job type. For example, you may conclude it is best to have a separate Windows discovery job for each location or Data Center. Take into account the recommended maximum number of devices a Remote Collector supports when organizing your jobs.
3. Adopt a standard discovery job naming convention—name each discovery job so they are easily understandable, are consistent, and can be sorted in a way that will be useful.

Discovery Job Best Practices—Discovery Job Configuration

1. Do not set up an autodiscovery scan using critical production account credentials; create a separate, dedicated account used only for discovery. Account lock-out could result in an otherwise avoidable outage depending on your permissions and configured password policies. You as a customer are responsible for any such behavior.
2. Always leverage a Remote Collector when performing discovery jobs. Note this is **required** when scanning networks larger than /24, using Nmap and leveraging any of our modular offerings such as: Application Dependency Mapping (ADM), Resource Utilization (RU), Storage Discovery, and Power and Environmental Monitoring.
3. For each discovery job, be as specific as possible in terms of defining your discovery targets (e.g. your devices), excluding any targets that should not be discovered. Doing so will reduce the number of discovery failures.
4. Do not exceed the largest recommended network range of /16, which includes 65,534 IP addresses. Adding more than the recommended range may either yield inconsistent discovery results or lengthen the time required for the discovery job to complete.
5. Break down larger subnets into smaller subnets, and leverage additional RCs to optimize discovery performance for larger environments.

Discovery Job Best Practices—Discovery Job Scheduling

1. Schedule your discovery jobs. Discovery jobs that are created, run once, and never scheduled to run again result in stale information and an inaccurate inventory.
2. Confirm job health before scheduling—make sure your discovery jobs return the expected data before you schedule them to run.
3. Schedule discovery jobs to run with the level of frequency required to keep your data current. Different jobs will require different frequencies based on their rate of data change.
4. Confirm that scheduled discovery jobs are complete before they are scheduled to run next. For example, a discovery job scheduled to run every four hours completes in less than four hours.
5. Avoid running jobs during high network traffic hours; this can reduce impact to network performance.
6. When running multiple jobs during a day, schedule them to run evenly throughout the day. If you cannot run jobs during primary business or production hours, spread them across non-peak, non-business hours as evenly as possible.
7. Regularly view the **Scheduled Job Distribution Status** report to ensure your jobs are not overloaded (**Insights+...System Administration…Scheduled Job Distribution Status**)

Discover Tasks

Phase 2 Task 1—Prepare for Discovery Jobs

2.1.1. Collect and Store Discovery Credentials

Credentials (Secrets) are frequently required when performing agentless Discovery; you specify them when creating discovery jobs. It is important to store the correct credentials in Device42 so you can reference them for jobs that require them. **Incorrect credentials is a common reason why discovery jobs do not successfully complete. Make sure you have the correct credentials and that you enter them correctly.**

Here are some examples of credentials required for common discovery jobs:

- **SNMP Discovery**—requires SNMP Community String (SNMP GET read account)
- **Linux Discovery**—requires SSH Login
- **Windows Discovery**—requires Windows Services Account (WMI access to devices)

Secrets are centrally stored in **Resources…Secrets…All Secrets**; note they are only visible to the user who created them but can be shared.

2.1.2. Create Subnets

Adding subnets helps you define the network scope as you discover your network(s) and also reduces the number of “undefined 0.0.0.0” network types.

To add your Subnets, perform the following steps:

1. Choose **Resources…All Subnets**
2. Click the **Create** button
3. Enter an IPv4 or IPv6 address into the Network field
4. Enter the Mask Bits (omit the “/”)
5. Enter the Service Level
6. Review the remaining options and choose the items that best fit your needs.
7. Click the Save button.

Click **here** for more information about subnets, including detailed instructions for adding or editing a subnet.

2.1.3. Configure Ports to Discovery Targets

It is critical that the ports used to access the targets are open in advance of running discovery jobs. Click **here** for a list of all ports that may be used to access targets for discovery, along with their directionality.

Phase 2 Task 2: Create and Run Discovery Jobs

Discovery Job Order

Device42 strongly recommends you run your first discovery jobs in the order listed below; you will achieve the best results and it will minimize future reconciliation work. **You can skip any jobs that are not applicable to your organization.**

Recommended Discovery Order		
Order	**Discovery**	**Description**
1	Network (SNMP)	Uses Simple Network Management Protocol (SNMP) to build your L2 Network landscape by discovering and gathering information from network devices such as switches, routers, and printers, collecting hardware and connectivity details. Use **this document** to get you started
2	Virtual Machine	V-Server auto-discovery collects data from hypervisors such as VMware, Citrix Xen, libvirt, and oVirt. Use **this document** to help get you started.
3	Windows/ Hyper-V	Brings in Windows and Hyper-V machines, performing deep discovery on Hypervisors, and Windows OS using WMI and WinRM protocols. It collects comprehensive hardware and software details and discovers virtualization platforms such as VMware, Hyper-V, and others. It gathers information about virtual machines, hosts, and their configurations. Use **this document** to help get you started.
4	Linux	Brings in host information, parts, OS, Service processes, and installed software and applications and configuration files for Linux and Unix machines. Use **this document** to help get you started.
5	Cloud	Brings in virtual machines and storage in Amazon Web Services, Microsoft Azure, Cloudstack, Openstack, and numerous other platforms. Discovers infrastructure and resources in various cloud environments such as AWS, Azure, Google Cloud, and Alibaba Cloud. It collects detailed information about the cloud assets and their configurations. Use **this document** to help get you started.
6	Storage	Discovers Storage Arrays for on premise storage solutions, using the appropriate API for the vendors required. Detailed information of Controllers, LUNs, Storage Pools and Disks in use. Connected to the appropriate hypervisors and file servers with a breakdown of usage. Use **this document** to help get you started.
7	Certificate	Scans and discovers SSL certificates across your network. It gathers information about the certificates and alerts you before they expire. Use **this document** to help get you started.
8	Warranty Sync	Syncs with vendors like Dell, IBM, Lenovo, and Meraki to pull in warranty information for discovered devices using their service tags and serial numbers. This helps in tracking device warranties and managing end-of-life replacements. Use **this document** to help get you started.
9	UCS/Load Balancer	Discovers Cisco Unified Computing System (UCS) and Application Centric Infrastructure (ACI) environments, as well as load balancers like F5. It collects detailed configuration and performance data. Use **this document** to help get you started.

2.2.1. Create SNMP Discovery Jobs

SNMP discovery jobs capture network equipment data per unique IP Address, CIDR block, or IP Range responding to SNMP *get requests* on Port 161.

SNMP discovery will discover network switches, storage switches, basic SAN details, management interfaces (iLO, iDRAC, etc.) and load balancer details. The Main Appliance will then federate newly discovered devices and details with other configuration items in Device42 allowing you to map connectivity across the network. The SAN discovery will also allow you to see which SANs are attached to a fiber switch when their WWNs are discovered. Discovery of various management interfaces will bring in BMC details and associate them with their affiliated hypervisor/bare-metal servers in Device42. Device42 supports SNMP v1, v2c and v3.

Port and Credential Requirements

Ports
UDP Port 161 should be accessible on any of the SNMP targets from the Device42 Remote Collectors.

Credentials
Read-only credentials are required for SNMP discovery jobs.

Steps to create and Run and SNMP Discovery Job

To create and run an SNMP Discovery Job, perform the following steps:

1. Navigate to **Discovery…SNMP**
2. Click the **Create** button
3. Enter the Job name
4. Select the Remote Collector
5. Enter the Server or Servers, CIDR Block, or IP Range
6. Review the remaining options and choose the items that best fit your needs.
7. Add the credentials.
8. Click the **Save** button.
9. Click the check box next to the discovery job(s) and choose **Actions…Run Selected Jobs**

Click **here** for more detail regarding SNMP Network Autodiscovery. This should be your first place to look when troubleshooting SNMP discovery job issues.

To view a video on creating an SNMP discovery job, click **here**.

2.2.2. Create Hypervisor Discovery Jobs

Hypervisor discovery jobs discover the Virtual Systems on the Hypervisor Platform, including ESX and ESXi, Citrix XenServer, HyperV, oVirt, Redhat, KVM/libvirt, OpenVZ, AIX HMC, Nutanix Prism, Nutanix Prism Central, Docker, and LXC.

Click **here** for a full list of supported Platforms.

Port and Credential Requirements

Ports
For **VMWare**, TCP port 443 should be accessible from the Remote Collectors to the Hypervisors. **Other Hypervisors** leverage APIs over HTTPS, or SSH over a user-definable port for discovery.

Credentials
For **VMWare**, Read-only API account with access to vCenter or the target infrastructure is sufficient.

Steps to create and Run a Hypervisor Discovery Job

To create and run a Hypervisor discovery job, perform the following steps:

1. Choose **Discovery…HyperVisors / *nix / Windows**
2. Click the **Create** button
3. Enter the Job name
4. Select the Remote Collector
5. Select the Hypervisor Platform (e.g. vmware)
6. Select the URL prefix (e.g. http or https)
7. Enter the Server or Servers, CIDR Block, or IP Range
8. Add the Discovery Target(s) Credential(s) (i.e. Username and Password)
9. Review the remaining options and choose the items that best fit your needs.
10. Click the **Save** button.
11. Click the check box next to the discovery job(s) and choose **Actions…Run Selected Jobs**

Click **here** for more detail regarding Hypervisor Autodiscovery. This should be your first place to look when troubleshooting Hypervisor discovery job issues.

To view a video that discusses Best Practices for Hypervisor discovery jobs, click **here**.

2.2.3. Create Windows Discovery Jobs

Windows discovery jobs provide an accurate inventory of the Windows devices on your target network.

While your virtual infrastructure can be discovered via VMWare, Hypervisor, etc. discovery jobs, Windows discovery jobs perform an OS-level discovery of your Windows devices, including your virtual Windows servers. Windows Discovery of physical infrastructure can be done either via

Windows Management Instrumentation (WMI), an older and less secure discovery method, or Windows Remote Management (WinRM), which is newer and more secure.

Port and Credential Requirements

There are a number of prerequisites and requirements for Windows discovery jobs to run properly, including WinRM Network Requirements, WMI Network Requirements, WMI and Windows Permissions, and Port Requirements. **It is imperative that the prerequisites and the requirements are met prior to running Windows discovery jobs.** Click here for these requirements and prerequisites, and also for more detailed instructions on creating and running Windows discovery jobs. This should be your first place to look when troubleshooting Windows discovery job issues.

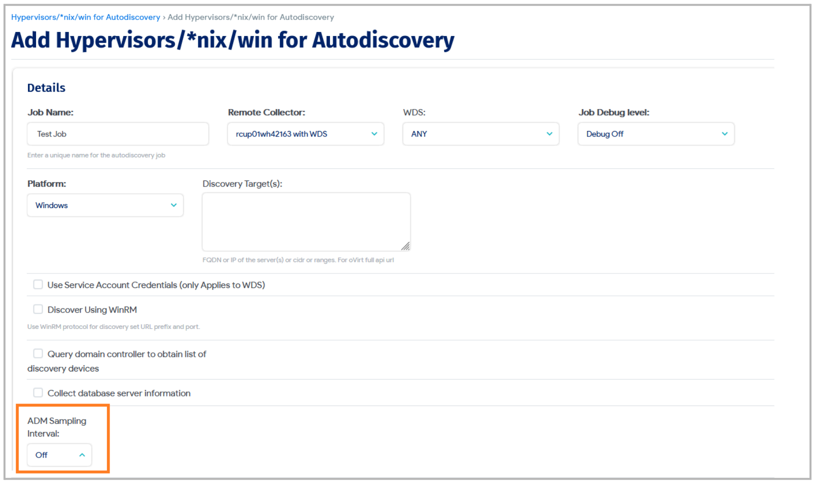
Steps to create and Run a Windows Discovery Job

To create and run a Windows discovery job, perform the following steps:

1. Choose **Discovery…HyperVisors / *nix / Windows**
2. Click the **Create** button
3. Enter the Job name
4. Select the Remote Collector
5. Select the **Windows** Platform
6. Enter the Server or Servers, CIDR Block, or IP Range
7. Add the Discovery Target(s) Credential(s) (i.e. Username and Password)
8. Review the remaining options and choose the items that best fit your needs.
9. Click the **Save** button.
10. Click the check box next to the discovery job(s) and choose **Actions…Run Selected Jobs**

Note:

- There are sometimes failures when discovering Windows operating system-based devices. Use *Appendix B—Windows Authentication Troubleshooting Checklist* to help you investigate and resolve these failures. If you are unable to resolve these failures, please contact Device42 Support for assistance.
- Organizations that have purchased the **Software License Management** module can include Software discovery when running Windows discovery jobs by clicking the **Discover Software** checkbox within the **Software and Applications** section of the job. For more information regarding Software License Management with Device42, see the *Software License Management Discovery Jobs* section later in this document.
- **Do not initially configure Windows discovery jobs to collect ADM information.** There are two reasons for this: 1) You may inadvertently consume your ADM licenses by discovering the wrong devices; 2) We recommend you wait~30 days before enabling ADM. See *Device42 ADM Implementation Guide* for instructions on to implement ADM
    - **Set ADM Sampling to “Off”**. Note: This is enabled by default when licensed for Enterprise Application Discovery and Services Discovery. **If you do not set ADM Sampling to “Off” you will have to perform multiple “cleanup” steps.**



Hypervisors/*nix/win for Autodiscovery › Add Hypervisors/*nix/win for Autodiscovery

Add Hypervisors/*nix/win for Autodiscovery

Details

Job Name: Test Job

Enter a unique name for the autodiscovery job

Remote Collector: rcup01wh42163 with WDS

WDS: ANY

Job Debug level: Debug Off

Platform: Windows

Discovery Target(s):

FQDN or IP of the server(s) or cidr or ranges. For oVirt full api url

□ Use Service Account Credentials (only Applies to WDS)

□ Discover Using WinRM

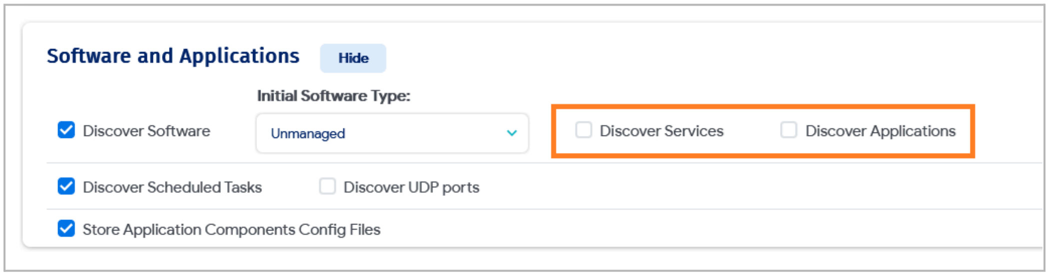
Use WinRM protocol for discovery set URL prefix and port.

□ Query domain controller to obtain list of discovery devices

□ Collect database server information

ADM Sampling Interval: Off

- In *Software and Applications*, click “Show” and make sure that **Discover Services** and **Discover Applications** checkboxes are **unchecked**.



Software and Applications

☑ Discover Software

Initial Software Type: Unmanaged

□ Discover Services

□ Discover Applications

☑ Discover Scheduled Tasks

□ Discover UDP ports

☑ Store Application Components Config Files

To view a video on creating a Windows discovery job, click **here**.

To view a video on troubleshooting common Windows discovery job issues, click **here**.

2.2.4. Create Linux and Unix Discovery Jobs

Linux and Unix discovery jobs provide an accurate inventory of the Linux and Unix devices on your target network and discover your *nix physical and virtual infrastructure.

Port and Credential Requirements

Ports

Device42 will, by default, use the standard SSH port 22 to target your Linux and Unix infrastructure. If your organization uses a non-standard SSH port you can specify this port in the discovery job.

Credentials

Several of the commands that are run invoke **sudo** for escalated privileges. This is avoided when possible, but is sometimes necessary to determine certain information for a comprehensive discovery.

Click **here** for more detail regarding Linux and Unix Autodiscovery. This should be your first place to look when troubleshooting Linux and Unix discovery job issues.

Steps to create and run a Linux/*nix Discovery Job

To create and run a Linux/*nix discovery job, perform the following steps:

1. Choose **Discovery…HyperVisors / *nix / Windows**
2. Click the **Create** button
3. Enter the Job name
4. Select the Remote Collector
5. Select the ***nix** Platform
6. Enter the Server or Servers, CIDR Block, or IP Range
7. Enter the Port (if default port 22 is not being used)
8. Add the Discovery Target(s) Credential(s) (i.e. Username and Password)
9. Review the remaining options and choose the items that best fit your needs.
10. Click the **Save** button.
11. Click the check box next to the discovery job(s) and choose **Actions…Run Selected Jobs**

Note:

- Organizations that have purchased the **Software License Management** module can include Software discovery when running *nix discovery jobs (as well as other platforms like Classic WinRM, IBM i/AS400, IBM z/OS, and SCCM) by clicking the **Discover Software** checkbox within the **Software and Applications** section of the job. For more information regarding Software License Management with Device42, see the *Software License Management Discovery Jobs* section later in this document.

To view a video on creating a Linux discovery job, click **here**.

2.2.5. Create Cloud Discovery Jobs

Cloud discovery jobs discover your infrastructure in AWS, Azure, Google Cloud, and other cloud providers and inventory your cloud infrastructure from available cloud solutions: AWS, Azure, GCP, Alibaba Cloud, Amazon API, Digital Ocean, Intune, Linode, Open stack, Oracle Cloud and Standalone Kubernetes.

Port and Credential Requirements

Ports
Cloud infrastructure discovery is performed using HTTPS over port 443.

Credentials

Required credentials vary by Cloud Provider.

- AWS
  - Dynamic and Static Account Discovery are supported using both IAM users and EC2 instance Profiles
- Microsoft Azure
  - Require Subscription ID (not required when performing Tenant wide discovery)
  - Tenant ID Credentials (Username/Password or Service Principle ClientID/Client Secret Value)
- Google Cloud
  - Project ID (leave blank if doing multi project discovery)
  - Service Account with viewer role and a Service Account key (JSON key file)
- Kubernetes Cluster
  - Basic Authentication (Username/Password) OR
  - Bearer Token (Username and token string) OR
  - The User / Service Account will need view permissions to any desired pods / applications or view cluster wide.

Click **here** for more detail regarding Cloud Autodiscovery. This should be your first place to look when troubleshooting Cloud discovery job issues.

Click the following links for discovery details for **AWS**, **MS Azure**, **Google Cloud**, and **Kubernetes** Cloud discovery jobs. Regarding Kubernetes, click **here** for information regarding provisioning a Service Account.

Steps to create and run a Cloud Discovery Job

To create and run a Cloud discovery job, perform the following steps:

1. Choose **Discovery…Cloud**
2. Click the **Create** button
3. Enter the Job name
4. Select the Cloud Type and Vendor(s)
5. Select the VRF Group
6. Select the Remote Collector
7. Enter the appropriate cloud credentials (varies depending on platform)
8. Enter the Server or Servers, CIDR Block, or IP Range
9. Review the remaining options and choose the items that best fit your needs.
10. Click the **Save** button.
11. Click the check box next to the discovery job(s) and choose **Actions…Run Selected Jobs**

2.2.6. Create Storage Array Discovery Jobs

Storage Array discovery jobs identify and return Storage Array resource details, related resources, and topology maps for a wide range of storage platforms.

Click **here** for more detail regarding Storage Arrays Autodiscovery, including the list of supported platforms. This page also contains links to additional information about access protocols and minimum permissions for **Dell/EMC Arrays, HP Arrays**, **IBM Arrays**, as well as **All Other Storage Arrays**. It also contains more detail on creating new Storage Array discovery jobs. This should be your first place to look when troubleshooting Storage Array discovery job issues.

Steps to create and run a Storage Arrays Discovery Job

To create and run a Storage Arrays discovery job, perform the following steps:

1. Choose **Discovery...Storage Arrays**
2. Click the **Create** button
3. Enter the Job name
4. Select the Remote Collector
5. Select the Platform (e.g. Netapp)
6. Enter the Server or Servers, CIDR Block, or IP Range
7. Select the Target Type (values dependent on selected Platform)
8. Select the Protocol Type (values dependent on selected Platform)
9. Check or uncheck Enable Performance Data Collection
10. Select the Performance Data Sampling Interval
11. Select the Action for Storage Array not found (keep or delete Array Resource)
12. Add the Discovery Target(s) Credential(s) (i.e. Username and Password)
13. Review the remaining options and choose the items that best fit your needs.
14. Click the **Save** button.
15. Click the check box next to the discovery job(s) and choose **Actions...Run Selected Jobs**

Click **here** to view more information about Storage Arrays, including viewing and editing storage arrays, viewing arrays mapped to devices, viewing storage resource maps and trend graphs, and importing and exporting Storage Array discovery jobs.

2.2.7. Create Certificates Discovery Jobs

Certificates discovery jobs provide detailed information on https SSL certificates, including expiration dates, which is helpful for business continuity.

Click **here** for more detail regarding Certificates Autodiscovery, including creating a Certificates discovery job, SSL Certificate Cipher Suite Discovery, and discovery risks when multitenancy is enabled. This should be your first place to look when troubleshooting Certificates discovery job issues.

Steps to create and run a Certificates Discovery Job

To create and run a Certificates discovery job, perform the following steps:

1. Choose **Discovery…Certificates**
2. Click the **Create** button
3. Enter the Job name
4. Select the Remote Collector
5. Provide the Server or Servers, CIDR Block or IP Range
6. Review the remaining options and choose the items that best fit your needs.
7. Click the **Save** button.
8. Click the check box next to the discovery job(s) and choose **Actions…Run Selected Jobs**

Click **here** for information on managing discovered certificates.

To view a video on viewing the results from Certificates discovery jobs, click **here**.

2.2.8. Create Warranty Discovery Jobs

Warranty discovery jobs enable you to discover and document your hardware warranties. Device42 currently supports warranty autodiscovery for the following vendors: Dell, IBM, Lenovo, Meraki, and Cisco (Preview).

Warranty Discovery Job Prerequisites

Device Field Prerequisites

The warranty discovery APIrequires both the device model and serial number fields be correctly entered, either manually or via discovery.

The Device42 **Hardware** field must include a vendor name that exactly equals a value of “Dell”, “IBM”, “Meraki”, and “Lenovo”. You can add vendor aliases if you choose. If you have multiple vendor entries for any of these vendors (e.g. “Dell”, “Dell Inc.”) we recommend merging these into a single vendor, using the abovementioned vendor names (see *Appendix C—Merge Vendor Steps* for instructions to merge multiple vendors).

API Prerequisites

Warranty Discovery requires vendor API keys. See the information below on how to receive API keys from each vendor.

- Dell API key: Register or log in at Dell TechDirect portal (**https://techdirect.dell.com**) and choose **Services…APIs** to request an API key; you will be provided with a Client ID and Client Secret for API access
- Meraki API key: Click **here** for Meraki instructions to receive your API key
- Lenovo API key: Large enterprise customers can request a warranty lookup API key from Lenovo Sales or Support Account Representatives.

- IBM API key: Click **here** to log in to your IBM account to access your warranty lookup information.

Steps to create and run a Warranty Discovery Job

To create and run a Warranty discovery Job, perform the following steps:

1. Choose **Discovery…Warranty Sync**
2. Click the **Create** button
3. Enter the Job name
4. Select the Remote Collector
5. Select the Vendor
   - For Dell, then specify the API Version then specify the Access Key and Secret Key
   - For Meraki, then specify the Access Key
   - For IBM or Lenovo, then specify the Access Key
6. Select the Order Number Type
7. Select the Debug level
8. Click the **Save** button.
9. Click the check box next to the discovery job(s) and choose **Actions…Run Selected Jobs**

Click **here** for more detail regarding Warranty Autodiscovery, including API Key details, configuration information, and prerequisites. It also includes information to configure the warranty script, as well as documenting the secure communication details between the Device42 UI and warranty script to the hardware vendor, and other information. This should be your first place to look when troubleshooting Warranty discovery job issues.

2.2.9. Create UCS/Load Balancer Discovery Jobs

UCS/Load Balancer discovery jobs map out virtual servers, pools, and their relationships to backend devices. Once you have run SNMP and Windows/*nix discovery jobs, you can create UCS/Load Balancer jobs to collect connectivity and dependency data.

Prerequisites

For F5 discovery, ensure you have the **username for a local account** with access to the F5 API. The API calls work with read-only access and do not require administrative privileges.

Note that F5 devices do not support username and password authentication for accounts that use external authentication providers, such as Active Directory, which uses token-based authentication.

Steps to create and run a Load Balancer and Cluster Device (UCS) Discovery Job

Given the variety of Discovery platforms, we recommend you click **here** to follow the steps to create these jobs. This page also includes prerequisites and discovery options. To run the created job, click the check box next to the discovery job(s) and choose **Actions…Run Selected Jobs**.

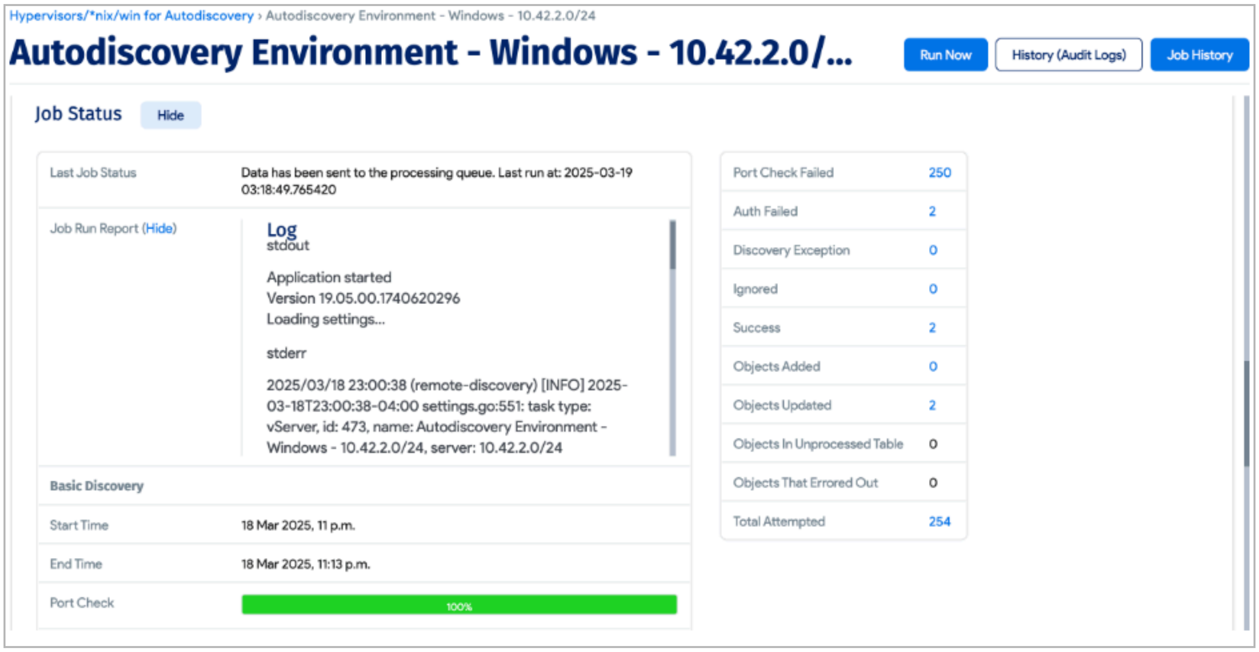
Phase 2 Task 3: Verify Discovery Jobs

There are a variety of ways for you to evaluate the success of a discovery job. These include:

- Discovery Job Results Status—provides a status of the overall job, displaying successes, failures, warnings, and other results.
- Discovery Scores—provides a score for one or all discovery jobs.
- Discovery Target Details—provides discovery results and scores for individual targets (e.g. server)

2.3.1. Discovery Job Results

After running a discovery job you will be presented with the Job Status It will look something like this:


Hypervisors/*nix/win for Autodiscovery › Autodiscovery Environment - Windows - 10.42.2.0/24
Run Now
History (Audit Logs)
Job History
Hide
100%

Autodiscovery Environment - Windows - 10.42.2.0/...

Job Status

Last Job Status	Data has been sent to the processing queue. Last run at: 2025-03-19 03:18:49.765420
Job Run Report (Hide)	Log
Basic Discovery	
Start Time	18 Mar 2025, 11 p.m.
End Time	18 Mar 2025, 11:13 p.m.
Port Check	100%

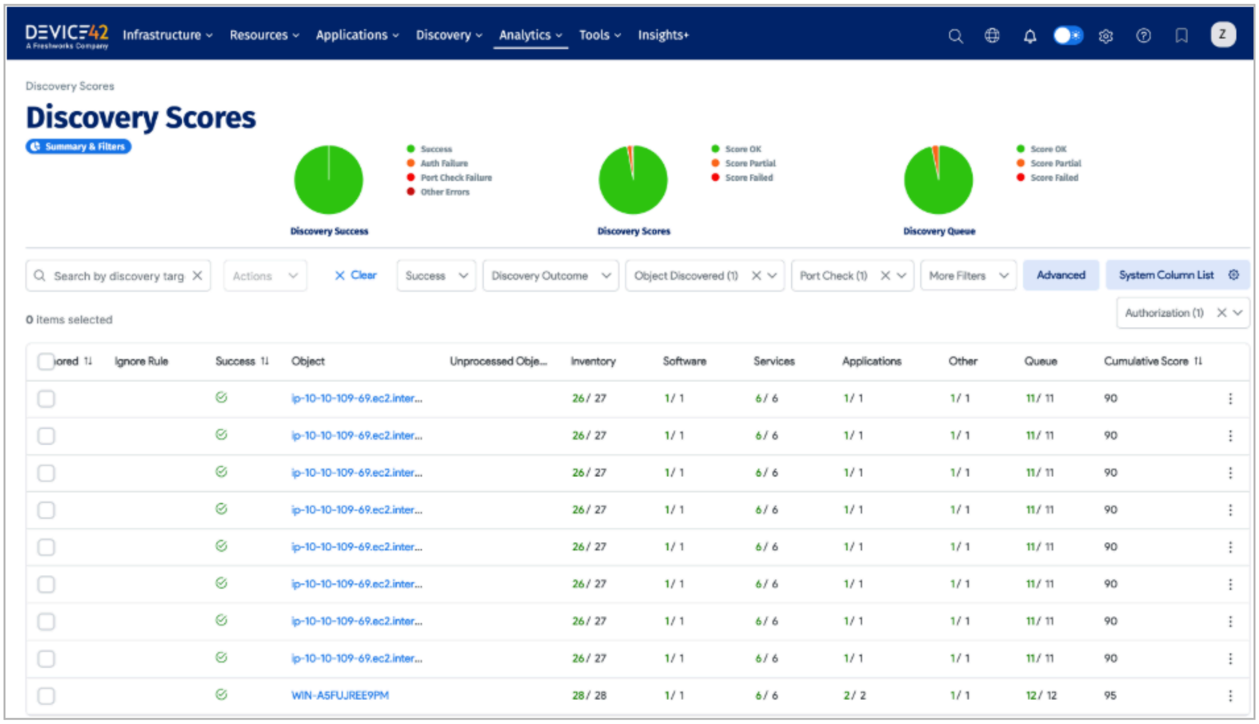
```
stdout

Application started
Version 19.05.00.1740620296
Loading settings...

stderr

2025/03/18 23:00:38 (remote-discovery) [INFO] 2025-03-18T23:00:38-04:00 settings.go:551: task type: vServer, id: 473, name: Autodiscovery Environment - Windows - 10.42.2.0/24, server: 10.42.2.0/24
```

Port Check Failed	250
Auth Failed	2
Discovery Exception	0
Ignored	0
Success	2
Objects Added	0
Objects Updated	2
Objects In Unprocessed Table	0
Objects That Errored Out	0
Total Attempted	254

- The Job Status section provides the **Last Job Status**, as well as **Basic Discovery** and **Detailed Discovery** results.
- You can click the **Show** link next to the **Job Run Report** to see the Job Report Log.
- You can see the Discover Breakdown (e.g. Port Check Failed, Auth Failed, etc.) and click the quantity value for these to link to the **Discovery Scores** for these items. From here you can link to the **Discovery Target Details** for each discovered item.

2.3.2. Discovery Scores

The Discovery Scores page enables you to view the success of your discovery jobs on a granular level. It provides an overall view of discovery success, discovery scores, and discovery queues. You can see each discovered device, the target IP it was discovered from (which is also a link to that job's page), the job name, cumulative score, and more.



0 items selected

☐	ored ⇅	Ignore Rule	Success ⇅	Object	Unprocessed Obje...	Inventory	Software	Services	Applications	Other	Queue	Cumulative Score ⇅	
☐			✓	ip-10-10-109-69.ec2.inter...		26 / 27	1 / 1	6 / 6	1 / 1	1 / 1	11 / 11	90	⋮
☐			✓	ip-10-10-109-69.ec2.inter...		26 / 27	1 / 1	6 / 6	1 / 1	1 / 1	11 / 11	90	⋮
☐			✓	ip-10-10-109-69.ec2.inter...		26 / 27	1 / 1	6 / 6	1 / 1	1 / 1	11 / 11	90	⋮
☐			✓	ip-10-10-109-69.ec2.inter...		26 / 27	1 / 1	6 / 6	1 / 1	1 / 1	11 / 11	90	⋮
☐			✓	ip-10-10-109-69.ec2.inter...		26 / 27	1 / 1	6 / 6	1 / 1	1 / 1	11 / 11	90	⋮
☐			✓	ip-10-10-109-69.ec2.inter...		26 / 27	1 / 1	6 / 6	1 / 1	1 / 1	11 / 11	90	⋮
☐			✓	ip-10-10-109-69.ec2.inter...		26 / 27	1 / 1	6 / 6	1 / 1	1 / 1	11 / 11	90	⋮
☐			✓	ip-10-10-109-69.ec2.inter...		26 / 27	1 / 1	6 / 6	1 / 1	1 / 1	11 / 11	90	⋮
☐			✓	WIN-A5FUJREE9PM		28 / 28	1 / 1	6 / 6	2 / 2	1 / 1	12 / 12	95	⋮

Discovery Scores can be accessed in a variety of ways, including **Analytics…Discovery Scores**.

Access Discovery Score Steps

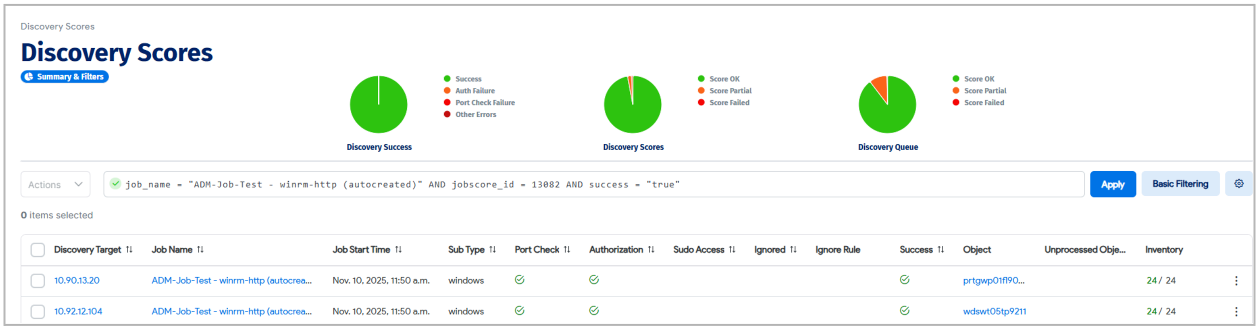
To access Discovery Scores, perform the following steps:

1. Chose **Analytics…Discovery Scores**
2. Hover over the pie charts to view summary data for each category. You can also click on a legend entry to filter in or out from the summary.
3. View the scrollable list of discovered devices, sorted from newest to oldest by default. Each device is displayed on its own line and provides information such as Discovery Target, Job Name, Job Timestamp, and a red or green Success indicator.
4. Click on any of the Discovered Targets to view the **Discovery Target Details** for that target.
5. Click on the **Job Name** to navigate to the discovery job to which that device was a part. Here you can see the status of the overall job.

Click here for more information about Discovery Scores.

2.3.3. Discovery Target Details

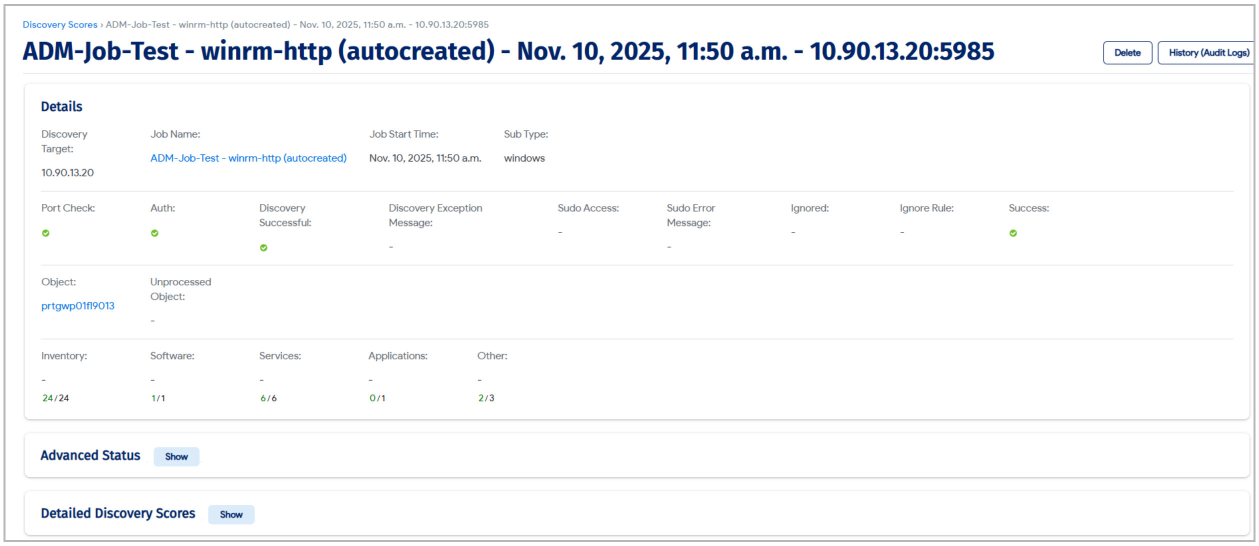
Discovery Target Details provide discovery information for a single Discovery target (e.g. an IP Address) within a specific discovery job (e.g. a specific Cloud discovery job). You can access Discovery Target Details by clicking on a Discovery Target within **Discovery Scores**.



```
job_name = "ADM-Job-Test - winrm-http (autocreated)" AND jobscore_id = 13082 AND success = "true"
```

0 items selected

Discovery Target	Job Name	Job Start Time	Sub Type	Port Check	Authorization	Sudo Access	Ignored	Ignore Rule	Success	Object	Unprocessed Obje...	Inventory
10.90.13.20	ADM-Job-Test - winrm-http (autocrea...	Nov. 10, 2025, 11:50 a.m.	windows	✓	✓				✓	prtgwp01fl90...		24 / 24
10.92.12.104	ADM-Job-Test - winrm-http (autocrea...	Nov. 10, 2025, 11:50 a.m.	windows	✓	✓				✓	wdswt05tp9211		24 / 24


Discovery Scores › ADM-Job-Test - winrm-http (autocreated) - Nov. 10, 2025, 11:50 a.m. - 10.90.13.20:5985
ADM-Job-Test - winrm-http (autocreated) - Nov. 10, 2025, 11:50 a.m. - 10.90.13.20:5985
Delete
History (Audit Logs)
Details

Discovery Target: 10.90.13.20
Job Name: ADM-Job-Test - winrm-http (autocreated)
Job Start Time: Nov. 10, 2025, 11:50 a.m.
Sub Type: windows

Port Check: ✓
Auth: ✓
Discovery Successful: ✓
Discovery Exception Message: -
Sudo Access: -
Sudo Error Message: -
Ignored: -
Ignore Rule: -
Success: ✓

Object: prtgwp01fl9013
Unprocessed Object: -

Inventory: - 24/24
Software: - 1/1
Services: - 6/6
Applications: - 0/1
Other: - 2/3

Advanced Status
Show
Detailed Discovery Scores
Show

- The Details section provides the Discovery Target, Job Name, Discovery Status (e.g. Port Check, Auth, etc.), and other information.
- You can click the **Show** link next to **Advanced Status**, **Detailed Discovery Scores**, and **Detailed Queue Scores** sections for additional details.

Phase 2 Task 4: Schedule Discovery Jobs

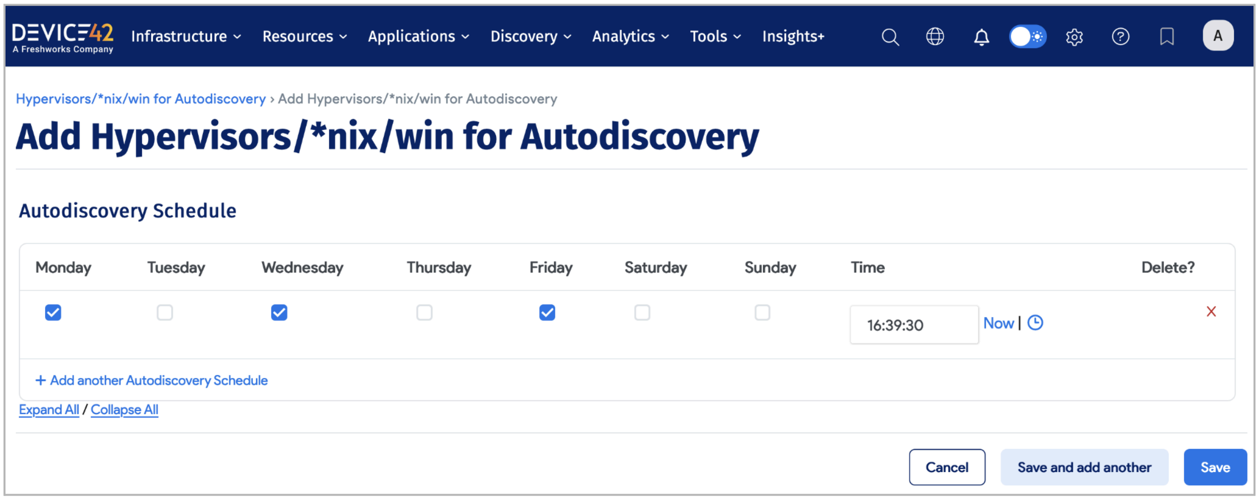
2.4.1. Scheduling a Discovery Job

Once a discovery job has been run and validated, it can be scheduled to automatically run. In the **Autodiscovery Schedule** section of each job, you can set as many different autodiscovery schedules as required to cover your environment. You can choose specific times and days of the week to run the autodiscovery job.

Steps to schedule a Discovery Job

To schedule an existing discovery job, perform the following steps:

1. Choose **Discovery**, then choose the type of discovery job you want to schedule.
2. Click the name of the job you want to schedule.
3. Click the **Edit** button.
4. Scroll to the **Autodiscovery Schedule** section and click the **+ Add another Autodiscover Schedule** link.
5. Specify the schedule you want.
6. Click the **Save** button.


DEVICE42
A Freshworks Company
Infrastructure
Resources
Applications
Discovery
Analytics
Tools
Insights+
A
Hypervisors/*nix/win for Autodiscovery › Add Hypervisors/*nix/win for Autodiscovery
Add Hypervisors/*nix/win for Autodiscovery
Autodiscovery Schedule

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Time	Delete?
☑	□	☑	□	☑	□	□	16:39:30 Now |	×

+ Add another Autodiscovery Schedule
Expand All / Collapse All
Cancel
Save and add another
Save

Discovery and Unprocessed Device Records

Unprocessed device records are discovered devices that could not be confidently matched to any existing device records based on the system’s device matching criteria. This most commonly happens when using "Moderate" or "Conservative" matching levels, in which the system considers multiple data points (such as hostname, IP address, MAC address, serial number, and UUID) and requires a certain combined score to merge with an existing record. If this threshold is not met, the discovered device ends up as "unprocessed" and requires manual review or action.

Users can review these records and either merge them with existing assets, create a new record, or delete them if they are outdated or incorrectly discovered.

To view Unprocessed Device Records, hover over **Discovery**, then choose **Unprocessed Device Records**.

Unprocessed Device Records Best Practices

1. Regularly check the **Unprocessed Device Records** page.
2. Merge records that clearly belong to existing assets, and delete old or stale records. Implement Auto Clean rules to delete old or stale records when appropriate.
3. Update discovery credentials and methods if frequent unprocessed records indicate incomplete data collection or matching failures.
4. In environments where matching is challenging, switching to "classic" device matching level can reduce the incidence of unprocessed records.

Click **here** for more information about Unprocessed Device Records, including defining matching levels, enabling Enhanced Device Matching, and other information.

To view a video providing more information about Unprocessed Device Records, click **here**.

Discovery and Auto Clean Rules

AutoClean Rules enable you to automatically manage old and possibly stale data based on specific criteria you set. Data pertaining to objects (e.g a device or an IP address) that is not found in subsequent autodiscovery jobs can be automatically deleted, architect, or otherwise modified. Auto Clean rules are particularly relevant for cleaning up IP Addresses, Devices, and Software. Click **here** for more information on adding Auto Clean rules, including instructions to create new rules.

To view a video on using Auto Clean rules, click **here**.

Additional Discovery Information

Click **here** to view the Autodiscovery main page, where you will find a wealth of autodiscovery information. This should be the first place to look for autodiscovery questions you may still have. It also includes a long list of sub-pages for each job discovery type.

Software License Management Discovery Jobs

Overview

As mentioned earlier in this document, Software License Management (SLM) is a separate Device42 module that among other things, scans Windows, Linux, and other device instances to detect installed software.
SLM is configured by enabling certain options within **Hypervisors / *nix / Windows** discovery jobs, specifically when the following **Platform** values are chosen:

- *nix
- Classic WinRM
- IBM i/AS400
- IBM z/OS
- SCCM
- Windows

To enable software discovery for these discovery jobs, click the **Software** checkbox within the **Software and Applications** section of the job.

Click **here** to link to a page providing information on how to configure the SLM module, view discovered software, enable software alerting, run software reports, and more.

Discover Phase Checklist

The Discover phase is considered complete when:

- ☐ You have defined your subnets.
- ☐ You have defined the discover jobs that will deliver the maximum return to your organization.
- ☐ You have determined how you want to organize and name your discovery jobs.
- ☐ You have created and run your discovery jobs, making sure to include only those targets relevant to each job, and making sure to limit the quantity of targets to ensure the jobs successfully complete.
- ☐ You have viewed your Unprocessed Device Records and have taken the appropriate actions (e.g. delete records, merge records).
- ☐ You have verified your discovery jobs were successful by reviewing Discovery Job results, Discovery Scores, and Discover Target Details.
- ☐ You have scheduled your discovery jobs, making sure to run them only as frequently as is needed, to schedule them during times when it will have minimal network impact, and to schedule jobs to run on different days and at different times so as to not overwhelm the Main Appliance.

Discover Phase Support

At the conclusion of Phase 2 you should have created and configured your relevant discovery jobs, validated that the jobs ran successfully, and scheduled those jobs to automatically run at specific intervals.

Should you have questions or issues, please first access *The Hitchhiker's Guide to Device42*, our online documentation page that can be accessed **here**. You can easily search this guide for any questions you may have. You may also access the Device42 Support page **here**, where you can submit a request, access our Knowledge Base, or access other general information.

Phase 3—Data Validation

In the Data Validation phase you will verify the quality and reliability of the discovered data. You will compare discovered data against existing reliable data sources in order to confirm the discovered data is accurate, complete, and consistent. If you find data that is missing (e.g. missing devices), blank (e.g. missing Model Name), or incorrect (e.g. incorrect hostname), we recommend you contact Device42 Support at **https://support.device42.com/** for help.

Data Validation Methods

There are three primary methods for reviewing discovered Device42 data, so that it can be compared against other data sources—viewing individual records, exporting data in bulk, and generating reports.

Viewing Individual Records

To view individual records, perform the following steps:

1. Hover over **Resources**, then click the item you wish to view (e.g. **All Devices**)
2. Click on the name of the item whose data you wish to view

Exporting Data in Bulk

To export data in bulk that can later be reviewed, perform the following steps:

1. Hover over **Tools**, then click **Exports (CSV)**
2. Click the name of the item whose data you want to export (e.g. **Device**)

Generating Reports

There are several useful reports to validate discovered data. To run these reports, perform the following steps:

1. Click **Insights+**
2. Click the folder and report you want to use; for example:
    a. **Modernization…Compute** to review Utilization, Hardware, and Operating System information
    b. **Compliance/Audit…Environmental Summary** to review physical and virtual devices, OS and version information, and installed software package information
    c. **IT Service Delivery…Insights+ Overview** to see an overall view of your IT enterprise

Data Validation and Data Import

While Device42's CMDB is primarily updated through discovery jobs, it can also be updated by way of manual entry, data import, or via API.

Manual Entry

To add or update data manually, perform the following steps:

1. Hover over **Resources**, click on the category of items you want to update (e.g. All Devices).
2. Click the item you want to update.
3. Click the **Edit** button.
4. Enter the information.
5. Click the **Save** button.

Data Import

To bulk import data, perform the following steps:

1. Hover over **Tools**, then choose **Imports/Exports (xls)** under the **Templates & Bulk Operations** section.
2. Either click the Sample File you want to use for import or download the **Current Data** for that data category.
3. Open the downloaded file and add or update the data.
4. Click the **Choose File** button and select the file containing the data you want to import.
5. Click the **Import** button.

Note:

- You can also bulk import your existing data from different spreadsheet formats by mapping columns to D42 fields using the tool linked **here**.

API Import

Restful APIs are supported in Device42 as one of the primary methods of entering, editing and retrieving data. Click **here** to access the Device42 API Guide.

Data Validation Phase Checklist

The Data Validation phase is considered complete when:

- ☐ You have reviewed the discovered data by reviewing individual records, by exporting data in bulk and reviewing this data, and/or by running reports
- ☐ You have compared the discovered data against existing, trusted data sources in an effort to confirm all data instances were discovered and that all data field values are as expected
- ☐ You have investigated and resolved any inconsistencies between the discovered data and your existing, trusted data sources
- ☐ You have imported any data you want in Device42 that was not able to be discovered.

Data Validation Phase Support

At the conclusion of Phase 3 you should have confirmed the accuracy of your discovered data.

Should you have questions or issues, please first access *The Hitchhiker's Guide to Device42*, our online documentation page that can be accessed **here.** You can easily search this guide for any questions you may have. You may also access the Device42 Support page **here**, where you can submit a request, access our Knowledge Base, or access other general information.

Data Validation and Data Integration

Customers often want to integrate Device42 discovered data with other systems, like Freshservice, Jira Service Management, ServiceNow, or others. We recommend you establish these integrations after you have completed the Data Validation phase. Once you have established these integrations, we recommend you use available mapping/schema data source information to confirm all relevant Device42 data has been successfully transferred to the destination platform.

Click **here** to navigate to the Device42 Integrations page, where you can view and access integration connectors to a variety of applications.

Phase 4—Display

In the Display phase you will translate your validated, discovered data into actionable intelligence through various reporting and visualization capabilities, empowering users to make informed business decisions and integrate Device42 into their operational workflows.

Report and Dashboard Overview

There are two main types of Device42 reporting: Standard and Insights+.

Standard Reports

Standard Reports is the first place you will look for information. You can use and modify pre-defined reports, list reports, guided reports, and even use our Device42 Object Query Language (DOQL) if you are so inclined. You can export and schedule Standard Reports.

Click **here** for more information about Standard Reports.

To view a video on ensuring success with Standard Reports, click **here**.

Insights+

Device42's Insights+ provides integrated analytics that leverage the breadth and depth of Device42 discovery to help you make sense of your data through visuals and dashboards so that you can make better, more informed business decisions.

Insights+ identifies patterns, trends, and outliers in data sets across your entire estate, elevating your performance with data understanding.

Click **here** for more information about Insights+.

To view a video on ensuring success with Insights+, click **here**.

Reports Summary

Below is a summary of each of the three Device42 reporting mechanisms:

- Standard Reports likely represent fundamental, day-to-day reporting
- Insights+ offers advanced visualizations and out-of-the-box dashboards to deliver comprehensive IT operational intelligence and support strategic business decisions

Reporting Reference Material

In addition to the above report links, below are links to additional reporting documentation:

- We have created a **Data Building Blocks Cookbook** that provides the "recipes” to more easily create and run report-based queries.
- The **Database Viewer Schema** page explains how to view Device42’s **Entity Relationship Diagram** and **Data Dictionary**.
- The **InsightsAI Chat** page explains how to use natural language descriptions to generate DOQL queries and tailored reports.

Key Customer Reporting Responsibilities

You and/or others in your organization will be responsible for completing specific tasks in order to ensure your organization receives tangible value from the data Device42 discovers. These responsibilities include the following:

- Complete Device42 Reporting Course: It is critical that you and/or others complete the Device42 Reporting course so you understand Device42’s reporting capabilities and methods.
- Define and Document Reporting Needs: Your organization invested in Device42 so it can provide visibility to address specific needs. By understanding those business needs, coupled with the knowledge of the data Device42 has discovered and the Device42 reporting capabilities, you or others must define and document the specific reports that will provide your organization with the required visibility. This is critical, whether these reports will be created by your organization, by Device42 Customer Success, or by a certified Device42 partner.
- Create and Customize Dashboards/Reports: Once your organization’s reporting needs are identified, you must facilitate the creation of these Dashboards and Reports.
- Review and Confirm Dashboards/Reports: You are responsible for reviewing the configured dashboards and reports to verify all necessary data visualizations (charts, graphs, maps) accurately represent the discovered infrastructure data.

Display Phase Checklist

The Display phase is considered complete when:

- □ You have a comprehensive understanding of Device42's reporting capabilities through the Device42 Academy's reporting training courses and by reviewing online Device42 reporting documentation.
- □ You have educated key stakeholders and main users regarding both Device42's standard reports plus its reporting capabilities
- □ You have defined and documented the key reporting requirements to address your organization's business needs.
- □ You have configured existing dashboards/reports and/or created new dashboards/reports to meet your organization's business needs.
- □ You have verified all dashboards (including charts, graphs, maps, etc.) and reports accurately reflect your discovered infrastructure.

Conclusion

Congratulations, You have completed the base Device42 implementation! Based on our experience working with customers, we expect you may have additional requirements, including integrating Device42 with other applications and systems, as well as expanding the use of Device42 to help your organization achieve additional objectives.

Please contact Device42 Support should you encounter any issues, and please contact your Account Representative or your Customer Success Manager should you require assistance with any non-support matters.

Please also use *Appendix D—Additional Customer Resources* for a list of links that can assist you with your Device42 journey.

Appendix A—Configuring your Remote Collector

Step 1: Change User Password

Perform the following steps:

1. Navigate to the Virtual Machine console of the Remote Collector Appliance
2. Login using the default credentials (Username is **client** and Password is **device42**)
3. Choose option (p) to enter the *Change Password (user client)* menu
4. Enter and verify the new password
5. Choose the **Save** button

Step 2: Specify Hostname

Perform the following steps:

1. Choose option (s) to enter the *Server Settings* menu
2. Enter a hostname
3. Choose the **Save** button

Step 3: Configure the Network Interface

Perform the following steps:

1. Choose option (u) to enter the *Network, Connectivity and Utilities* menu
2. Choose option (n) to enter the *Network Interfaces* menu
3. Select the default interface (highlighted in white) and press *Enter*
4. If using a Static IP, deselect *Use DHCP:* and enter the IP Address, Subnet, Gateway, and DNS server(s); if using IPv6, specify the IPv6 Address and Gateway
5. Choose **Save**, then **Exit**, then **Exit**

Step 4: Configure the NTP Settings

Perform the following steps:

1. Choose option (n) to enter the *NTP Client Settings* menu
2. Ensure Daily sync is chosen
3. Optionally choose to sync on reboot (this enables an admin to reboot the RC within the Device42 interface, which can help resolve unusual RC behavior)
4. Choose **Manual Sync** should you choose to perform a manual sync now, else choose the **Save** button

Step 5: Connect the Remote Collector to the Main Appliance

Perform the following steps:

1. Choose option (r) to enter the *Remote Collector Setup* menu
2. Enter the name of the Remote Collector
3. Enter either the Hostname or IP Address of the Main Appliance
4. Generate a One Time Password (OTP) from the Main Appliance, which will be entered later into this menu
    a. Log into the Main Appliance
    b. Choose **Discovery…Remote Collectors**
    c. Click the **Generate OTP** button
5. Enter the OTP
6. Choose the **Register** button. Note the Green acknowledgement text at the top of the main Appliance Management menu
7. Navigate back to the Main Appliance and confirm the RC in the Remote Collectors menu shows a **State** of “connected”

Appendix B—Windows Authentication Troubleshooting Checklist

Purpose: Use this checklist when your Device42 Windows Discovery jobs are failing due to **authentication**, **WMI/WinRM**, or **connectivity** issues.

1. Basic Environment & Discovery Setup

	Item	Notes
☐	Device42 Windows Discovery Job created	Use the correct discovery type (Windows/Hyper-V)
☐	At least one **Windows Discovery Service (WDS)** is installed and online	WDS should be registered in Device42
☐	Correct **WDS** selected in job (if applicable)	Job → Advanced Options
☐	Target hosts specified (IPs or FQDNs resolve properly)	Use valid DNS names or IPs
☐	Valid **Windows credentials** assigned to job	Either manual, or WDS "Service Account Credentials"
☐	Job logs show which credentials were attempted	Use debug mode if needed

2. Network Connectivity Checks

Run from WDS or discovery machine:

	Test	Command / Notes
□	Ping/Netstat Windows host	ping HOSTNAME or IP netstat HOSTNAME or IP
□	Test port 135 (for WMI)	PowerShell: Test-NetConnection -ComputerName HOST -Port 135
□	If using WinRM, test port 5985 (HTTP) or 5986 (HTTPS)	Test-NetConnection -ComputerName HOST -Port 5985
□	Hostname resolves correctly	nslookup HOSTNAME
□	If using IPs, DNS isn't required	Ensure IPs are pingable

3. Authentication Validation

	Check	Notes
□	Credentials are valid and **not expired/locked**	Try login via RDP to confirm
□	Domain credentials are fully qualified (e.g. DOMAIN\user)	Required for remote auth
□	If using gMSA, WDS service is running as the gMSA	Check Windows Service “Log On As”
□	For gMSA, discovery job set to “Use Service Account Credentials”	Only works with WDS

4. Firewall & Port Configuration

On **target** Windows host:

	Item	Command / Notes
☐	Port 135 allowed (for WMI/DCOM)	Windows Firewall inbound rule: “WMI (DCOM-In)”
☐	WMI rule enabled	“Windows Management Instrumentation (WMI-In)”
☐	Ephemeral port range not blocked	Allow dynamic ports or set custom port range for WMI
☐	WinRM enabled and allowed (if using WinRM)	Run: `winrm quickconfig` on target
☐	WinRM listener exists	`winrm enumerate winrm/config/listener`
☐	WinRM firewall rule enabled	“Windows Remote Management (HTTP-In)”

5. WMI / WinRM Functionality Tests

From WDS or discovery system:

WMI Test:

```
Get-WmiObject -Class Win32_OperatingSystem -ComputerName TARGET -Credential (Get-Credential)
```

WinRM Test:

```
Test-WSMan TARGET
```

Or:

```
winrm id -r:TARGET
```

	Result	Expect
☐	WMI command succeeds	Returns OS info
☐	WinRM test returns 200 OK	WinRM properly set up

6. Permission / Namespace Access

	Item	Notes
☐	Account has remote WMI permissions	Can use Device42 WMI Tester
☐	Can connect to \\TARGET\root\cimv2	Use Device42 WMI Tester
☐	Account is in **Distributed COM Users**	Or granted DCOM launch permissions manually
☐	Account is in **Performance Monitor/Log Users** (optional)	For perf counters
☐	Account is in **Event Log Readers** (optional)	For Windows events

7. Device42 Job-Specific Settings

	Check	Notes
☐	Discovery job set to correct **protocol** (WMI or WinRM)	WinRM recommended where possible
☐	Selected WDS is online and has connectivity	Test from same system
☐	Job runs with **Debug** enabled for verbose logs	Review log output in Job History
☐	Device42 not behind proxy blocking outbound port 443	For job report / updates

8. If the Job Still Fails…

	Step	Notes
☐	Use Device42 **WMI Test Tool**	**Download from Device42**
☐	Use WBEMTest locally	Connect to \\TARGET\root\cimv2 with credentials
☐	Review Device42 job logs for authentication errors	Check for "Access Denied" vs "RPC Unavailable" vs other
☐	Open support ticket with Device42	Include logs, test results, account details, and network path info

Appendix C—Merge Vendor Steps

To merge multiple vendor names into a single vendor name, perform the following steps:

1. Choose **Infrastructure…Vendors**.
2. Check the checkbox for the vendors you want to merge.
3. Choose **Actions…Merge**.
4. In the **Merge Vendor** dialog box, choose the vendor name you wish to assign to the selected vendor entries.
5. Optionally check the checkbox to automatically merge the vendor names for like named software.
6. Click the **Merge** button.

Appendix D—Additional Customer Resources

Below are links to commonly used customer resources. We recommend you bookmark these and other links in this guide for easy access.

- **Device42 Website**
- **The Hitchhiker's Guide to Device42** (i.e. Device42 Product Documentation navigation page)
- **Device42 Support Portal** (for ticket requests, access to Knowledgebase, etc.)
- **Device42 Release Notes**
- **Device42 Integrations Page**
- **Device42 API Guide**
- **Device42 Github**
- **Device42 Product Upgrade download site**
- **Device42 Upgrade Steps**
- **Device42 Academy**
- **Device42 Blog**
- **Device42 YouTube Channel**
- **Device42 LinkedIn Page**