Solution Brief

anuta networks

Multi-Vendor Network Compliance Management

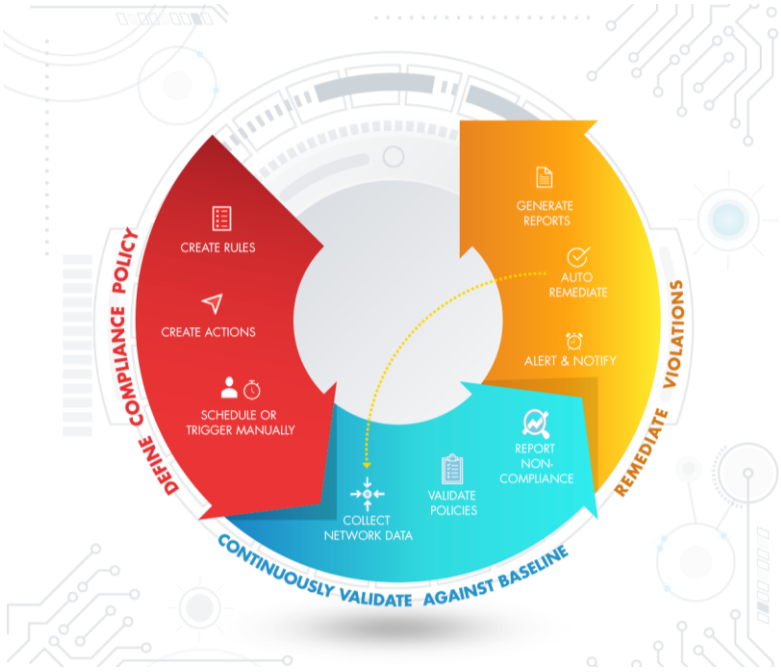
Configuration Management, Configuration Compliance, Service Compliance, Software Compliance

Key Capabilities

- Supports both legacy CLI & YANG based configuration compliance
- Maintains Service sanity with Service Compliance
- Ensures software compliance
- Offers RMA, Configuration Restoration & software upgrade workflows
- Get in-depth compliance analytics
- Schedule network audits
- Detailed reporting & dashboarding
- Enforces compliance through auto-remediation
- Implements compliance as a business process
- Quickly scale up to 1M+ devices across 45+ vendors

Managing configuration changes and enforcing compliance policies is a complex undertaking within large networks. A wide array of research indicates that a vast majority consider human error as the root cause of most network outages. Furthermore, manual network management and network automation scripting does not scale to meet the challenges of today's dynamic support of infrastructure, software, or policies. Organizations need an end-to-end automation solution that provides comprehensive configuration and compliance management capabilities.

Anuta Networks ATOM Multi-Vendor Configuration and Compliance management solution enable organizations to manage and monitor a diverse, multi-vendor network. It also provides an automated enforcement mechanism to ensure network consistency and business continuity.



Today's networks are fast and multi-dimensional, with an ever-increasing demand to move to smart and 100% compliant networks. Configuration and compliance management solutions combined with provisioning, analytics, telemetry, and closed-loop automation will enable organizations to achieve these objectives.

anuta networks

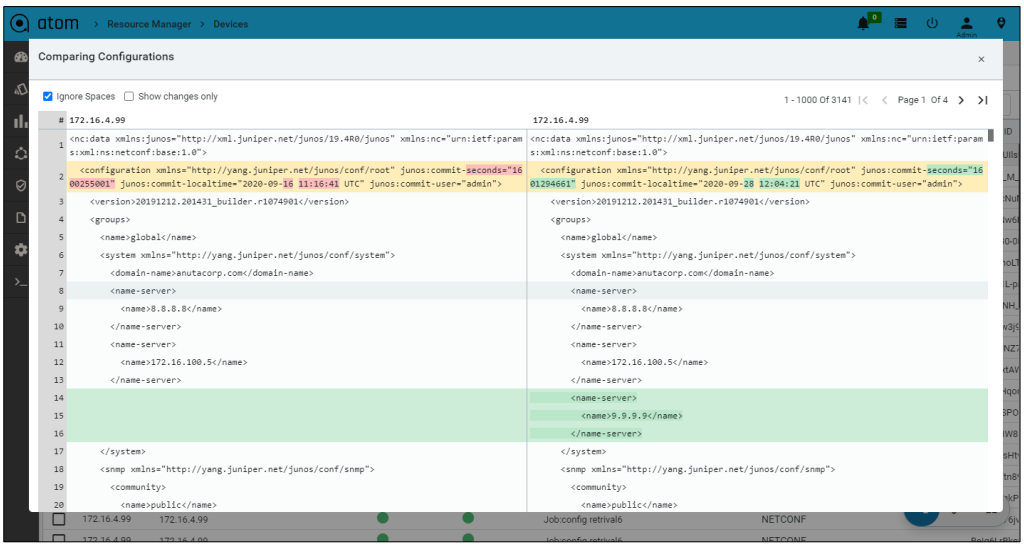
Configuration Management

ATOM offers extensive capabilities around Configuration Management of multi-vendor network devices. To begin with, ATOM allows supports on-demand, scheduled, and change-driven configuration archival. SNMP traps support the triggered retrieval of configuration. The configuration type includes CLI, NETCONF & API.

ATOM offers textual diff utility to compare configurations retrieved at various times. A corresponding changelog is also generated, enabling a more in-depth look at configuration differences from one version to another.

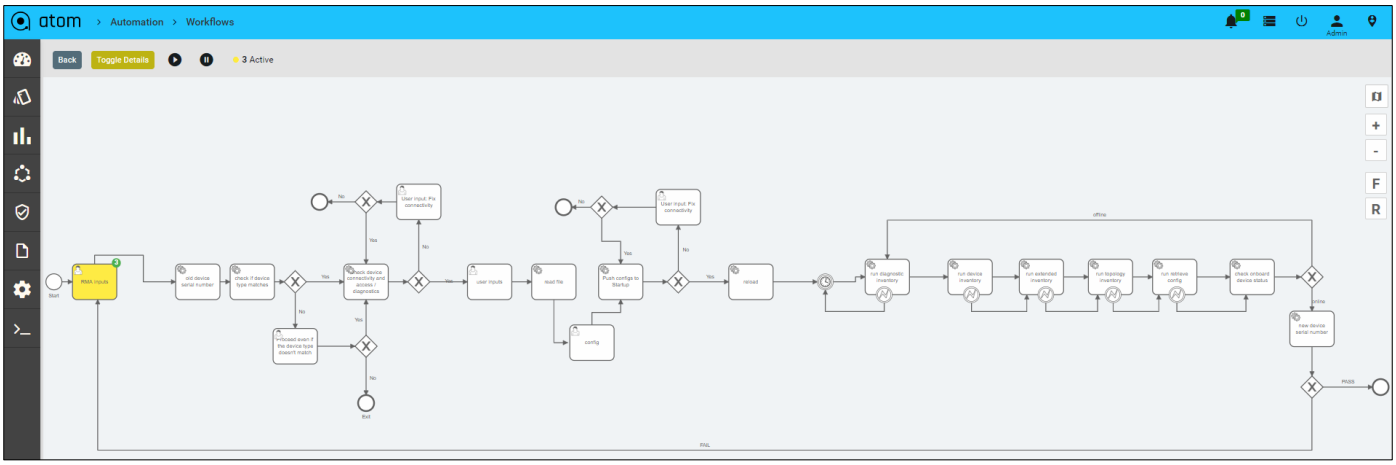
The retrieved configuration is parsed and mapped back to a data model based on YANG. The data model supported includes vendor native YANG and OpenConfig. ATOM parses the configuration and updates the data model each time a change is detected.

ATOM supports the versioning of configurations using tags. These tags will form an integral part of ATOM's RMA process workflow and Configuration restoration workflows that aids in massive scale network refresh.



Configuration diff utility

Configuration versioning



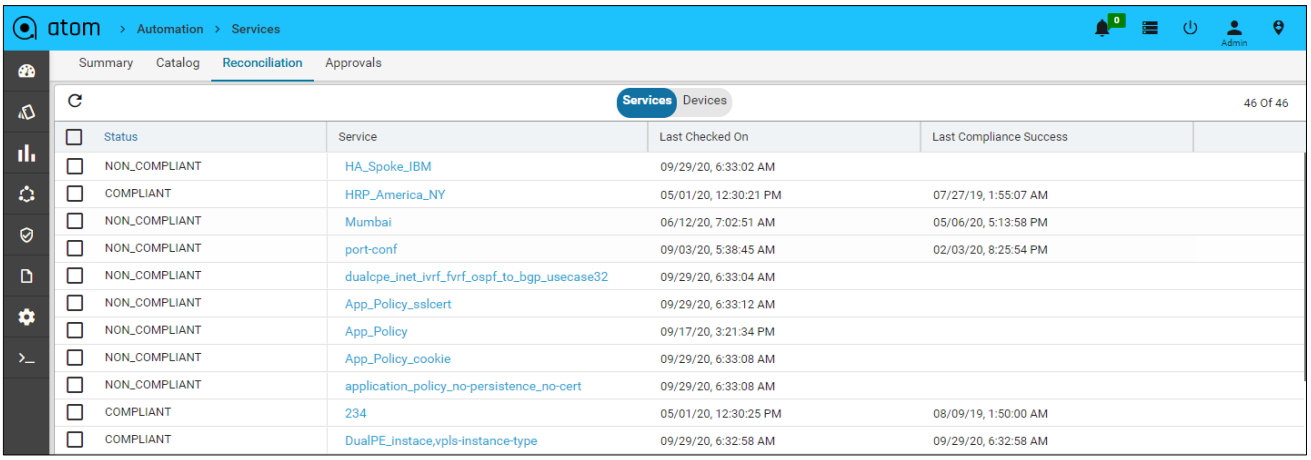
RMA/Config Restoration

Service Compliance

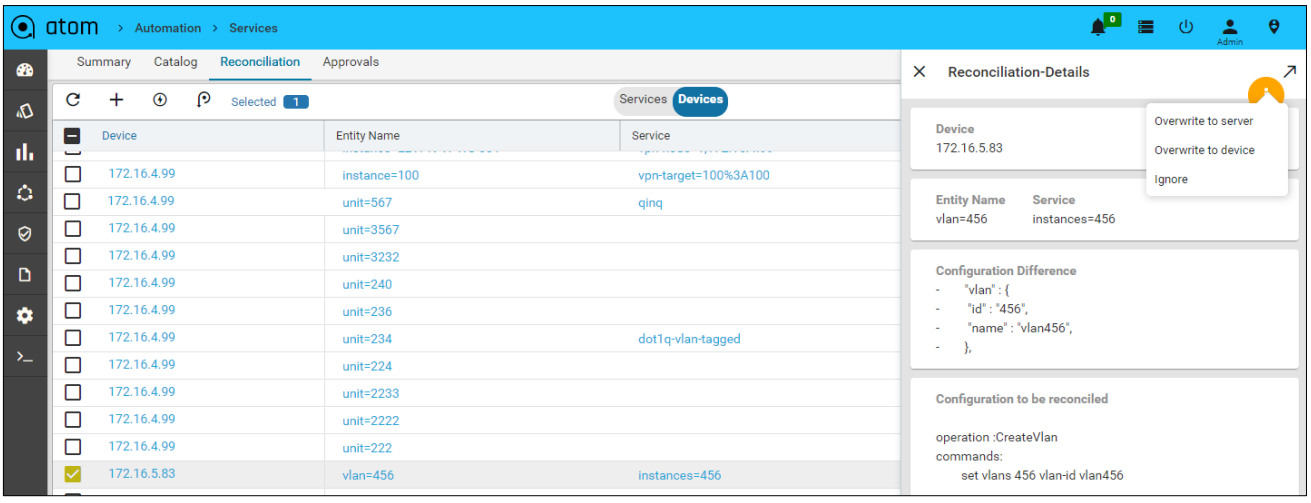
ATOM supports Service Models based on YANG. The stateful services such as L2/L3 VPN, EVPN-MPLS, EVPN-VXLAN, and much more are part of ATOM's rich catalog of Service models. In most cases, the services span across multiple devices, and platforms creating a service chain. Maintaining this service or service chain always is challenging, primarily due to the complexity involved.

Service compliance is built into the YANG service models in ATOM to maintain the sanity of the services at all times. In the wake of out-of-band change to the service configurations on the devices involved, ATOM gets notified via a scheduled configuration pull or SNMP trap. Post receiving the latest device configurations, ATOM runs a service inventory and flags any discrepancy to service configurations. Detailed view of configuration drifts and corresponding remediation configurations are captured and made available for one-click remediation.

The status of service is marked compliant once ATOM's service compliance remediates the service discrepancies.



Service Compliance



Configuration Drift

anuta networks

Configuration Compliance

While maintaining service configurations is essential, maintaining a standard across other sets of configurations is equally important. Regular and frequent network audits across a multi-vendor/multi-platform network can be a daunting task. The framework offered by Anuta ATOM enables an effortless definition and strict enforcement of golden standards, with smooth integration into the business processes of an organization.

Define complex policies with ease

ATOM offers an intuitive Policy Builder that facilitates the definition of simple & complex network, security, and other policies. It allows the administrator to define intent or baseline rules and remediation actions in the event of violations. Administrators can also create a parameterized baseline or standard configurations using strings or python-jinja for vendor platforms of their choice. The rule variables in the builder capture the default values for the templates. Multiple conditions form a policy to cater to complex scenarios where an expected configuration is pushed, or sometimes unexpected configurations are removed.

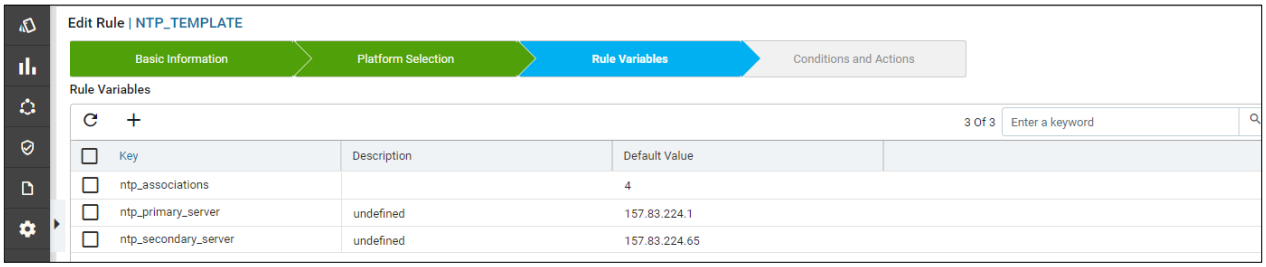
Policies for legacy CLI devices

Define CLI commands as golden templates using simple pattern matching using the ATOM's policy builder. The policy could be validated against a global configuration or a block of configuration, such as an Interface configuration block. A CLI compliance policy example shown below ensures a set of primary and secondary NTP servers in a network.

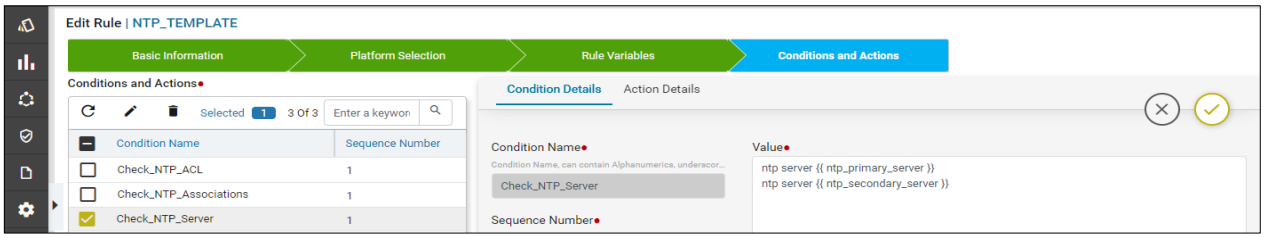
Another example shown ensures CDP/LLDP commands are disabled on all public-facing interfaces. The regular expression matches all the interfaces other than the Loopback and PortChannel interface with a public IP, checks for the CDP enable CLI under each identified interface, and lists them down.

The framework also allows setting a severity, message for non-compliance, and the definition of Fix CLIs that represents the golden configuration. For example, in the above example of disabling CDP commands, loops are defined to iterate over the identified public interfaces to set the *no cdp enable* command.

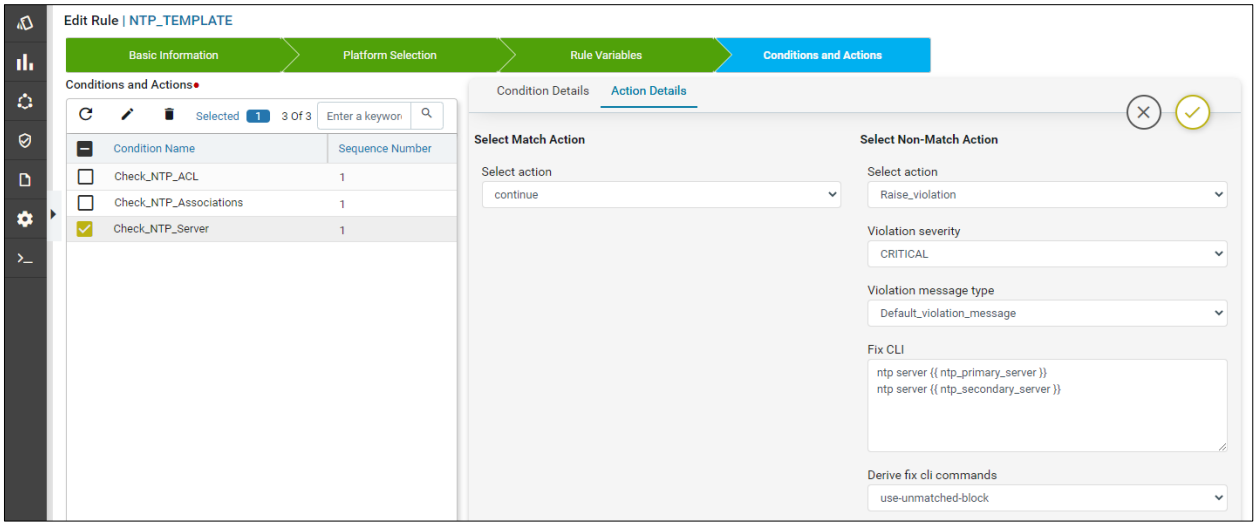
Example: NTP Golden Configurations



Rule Variables for Jinja templates

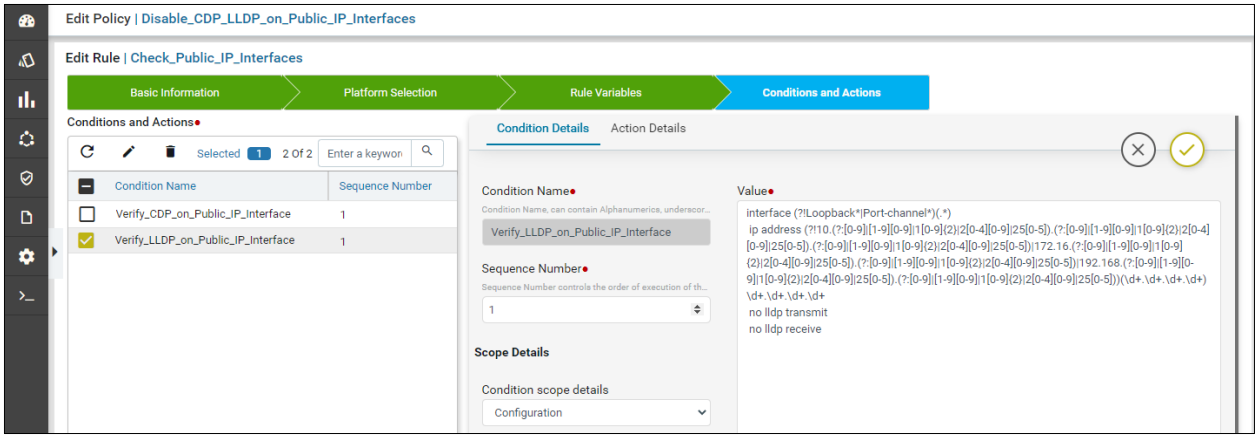


Policy definition

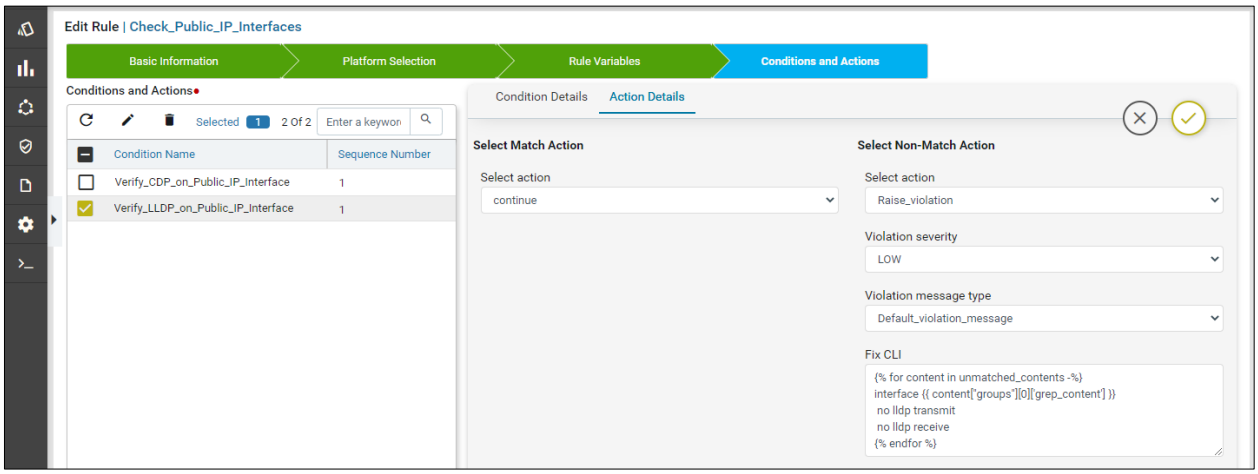


Remediation Config

Example: CDP/LLDP golden policy for public interfaces



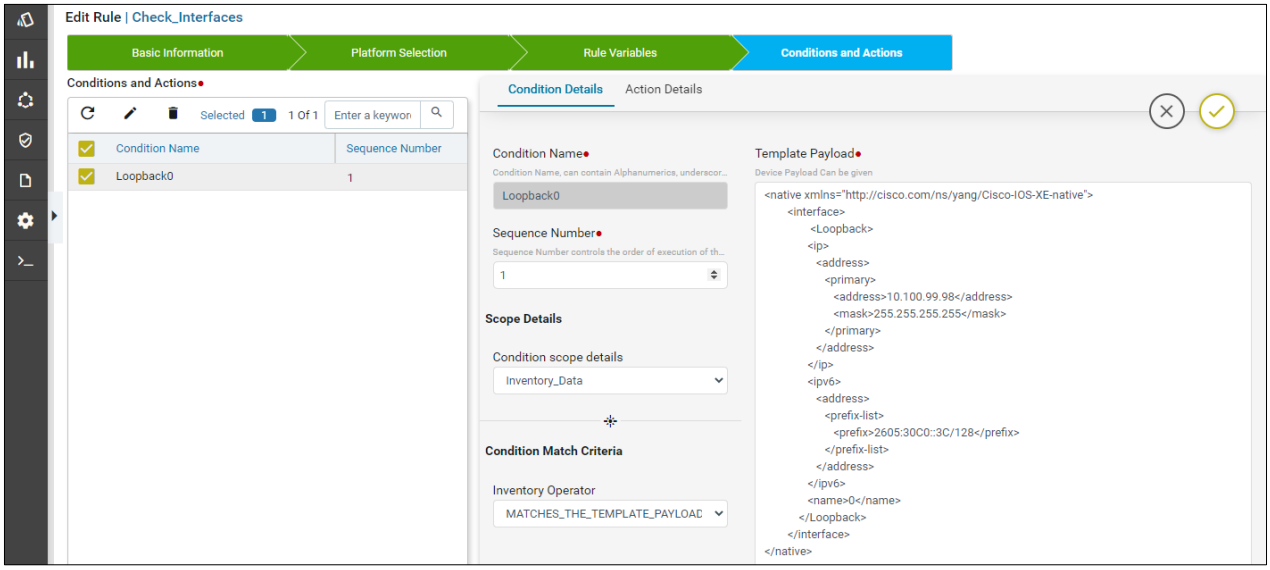
Pattern matching in Policy definition



Looping/Jinja in Fix Payload

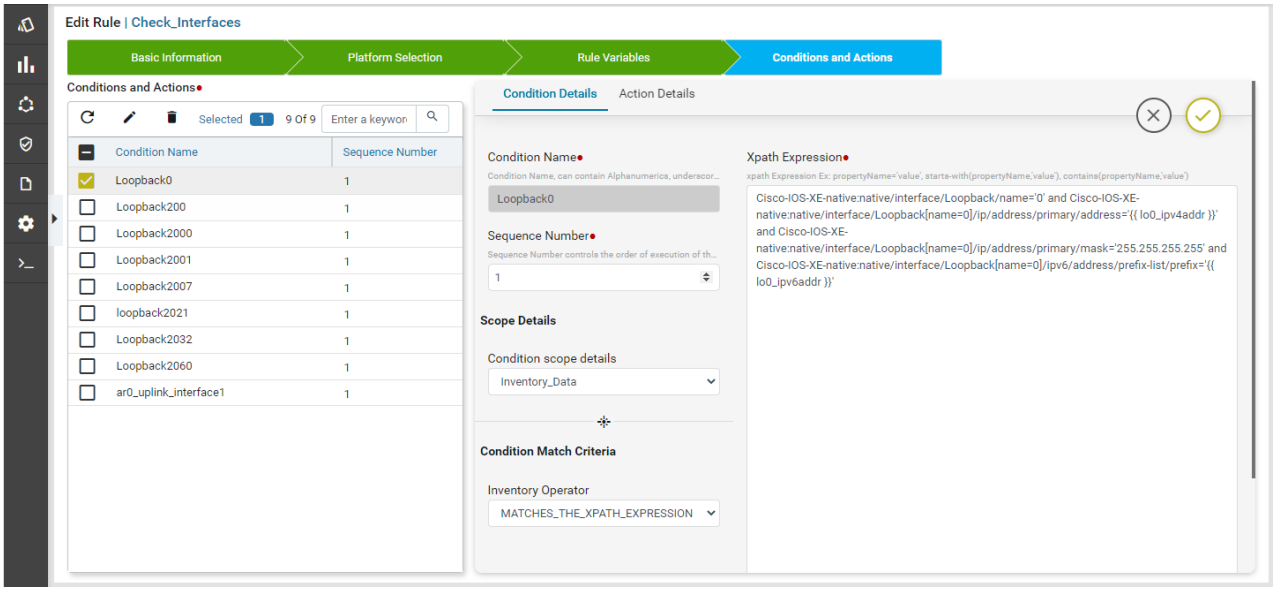
Policies for Native/OpenConfig YANG based devices

Define golden templates for native YANG or OpenConfig based devices using XML templates or X-path expressions using ATOM's policy builder. The example below ensures specific IPv4 and IPv6 IP addresses are always maintained on Loopback0.



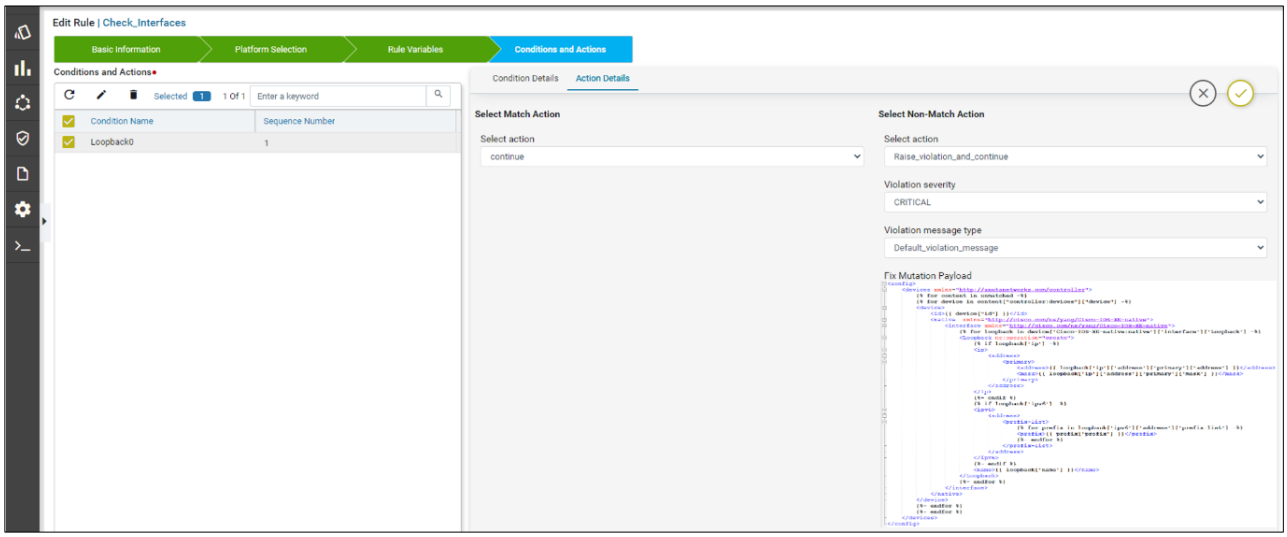
XML template payload for YANG based devices

The same policy defined as X-path expression is as shown below.



X-path expressions for YANG based devices

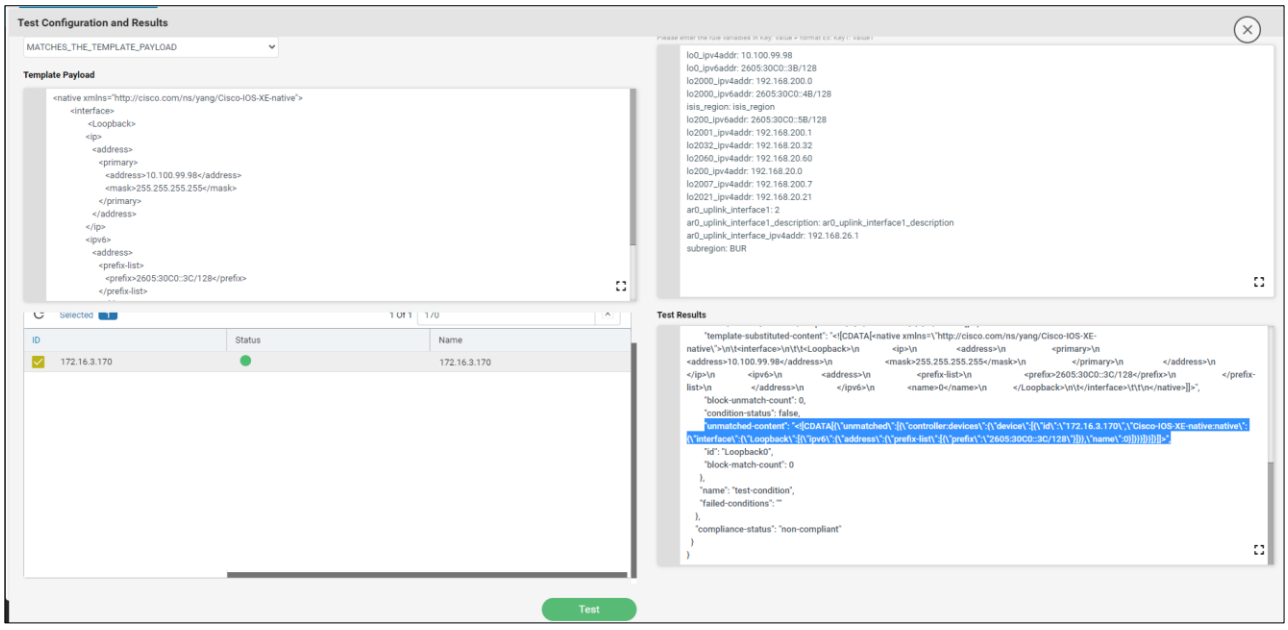
The Fix template for a non-match scenario for the above use case is shown below. The template generates XML payload using looping and conditional statements to ensure compliance with the defined policy.



Looping/Conditional constructs for complex use cases

Validate the policy definitions with In-built Test Engine

To aid in complex policy & Fix CLI/template definitions, ATOM offers a test engine for configuration compliance. A virtual framework of CLI policy or YANG policy, rule variables & devices helps users get real-time feedback on the policy definitions. An example of how the unmatched content returned by the device is used to create the Fix template payload is shown below.

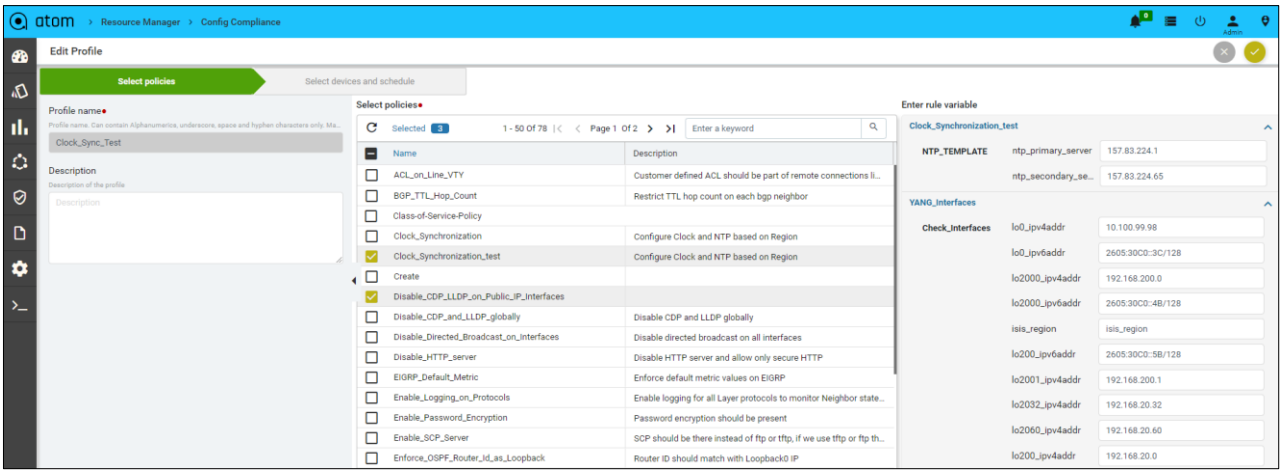


In-built test engine for testing & dry run

Apply policies to a group of devices

The policies defined in ATOM's policy builder can be applied to a set of devices using Profiles. ATOM offers a custom grouping of devices on platform-specific attributes using its Device Groups or a logical & hierarchical grouping based on location or other resources using its Resource Pools. Profiles in ATOM allows bundling of multiple policies. A profile, for example, may denote a group of policies for a group of devices in a region. One can choose to change the default values set in the rule variables of the policy in the profile, making it unique for a set of devices.

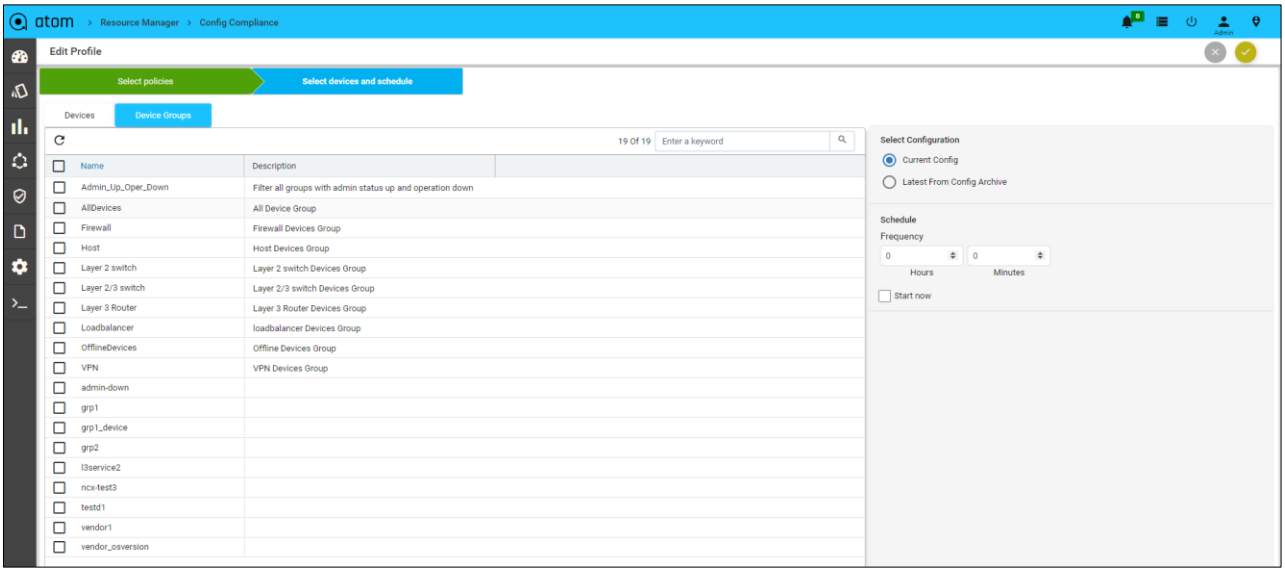
If the requirement is to have hierarchical policies, for example, a set of standards for Europe and a set of standards for Italy & Germany are present. If Italy and Germany's devices are to inherit the standards from Europe, their compliance profile will contain a combination of policies from Europe and their policies.



Bundle, create hierarchical policies & customize per device group

Schedule Compliance Audits

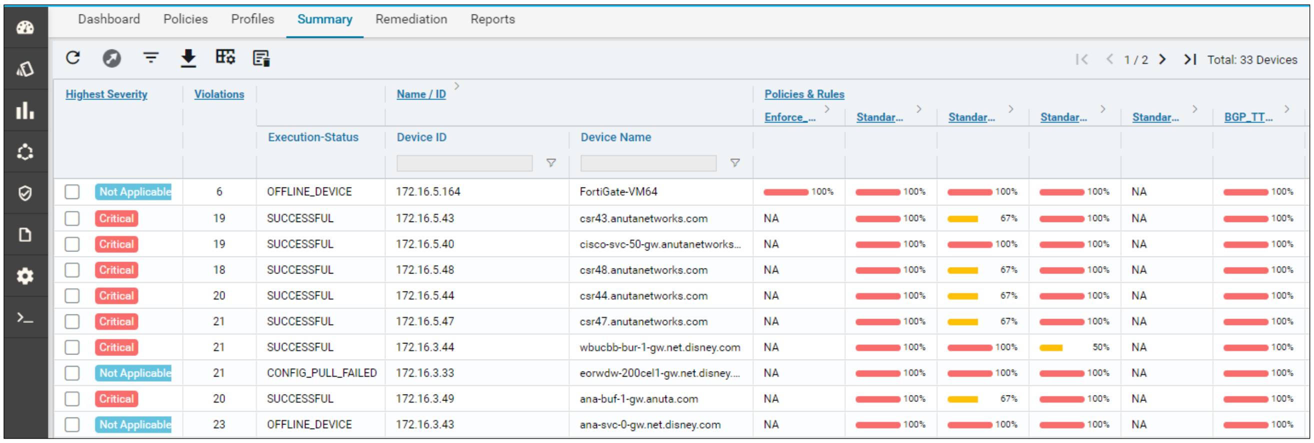
Schedule the compliance runs frequency to get a detailed view of the network compliance status. The compliance checks can be performed against the latest configuration or the latest archived configuration. Device-level audits can also be triggered from the device grid view.



Schedule compliance audits

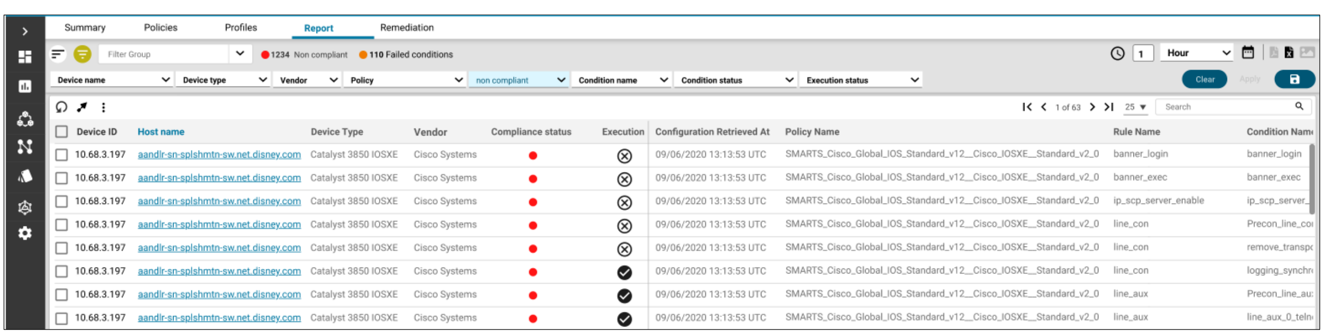
Exhaustive Reporting & Dashboarding

A detailed report & analytics on network compliance status is presented for business documentation. The dashboards offer deep insights through compliance status, trends, and Top N view of different focal points such as Vendor, Device, Device groups, Region, Policies, and Profiles. A detailed tabular report with compliance status is also made available. It can be scheduled, downloaded in various formats, or emailed directly from ATOM.



Detailed compliance status report

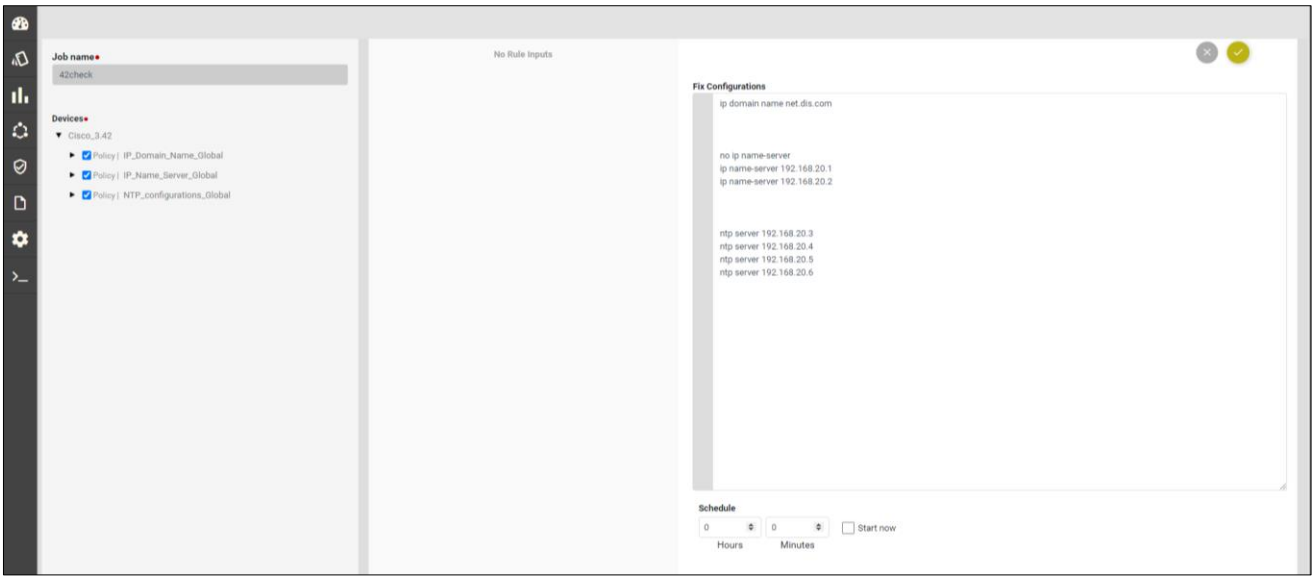
Business dashboards for compliance snapshot



On-demand & scheduled customizable reports

Remediate & stay network healthy

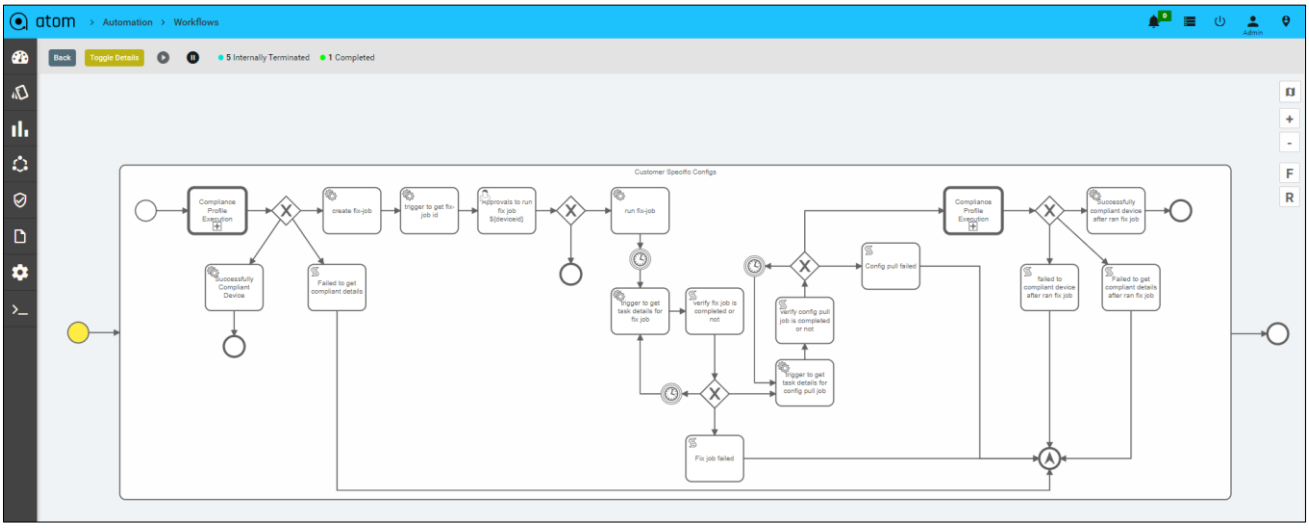
A remediation job can be triggered manually or scheduled by choosing the list of devices/device groups. The corresponding Fix CLIs/templates are executed, after which the reports and summary dashboards are updated to reflect the new compliance status of the devices.



Schedule remediation for compliance enforcement

Tie the compliance process into business workflows

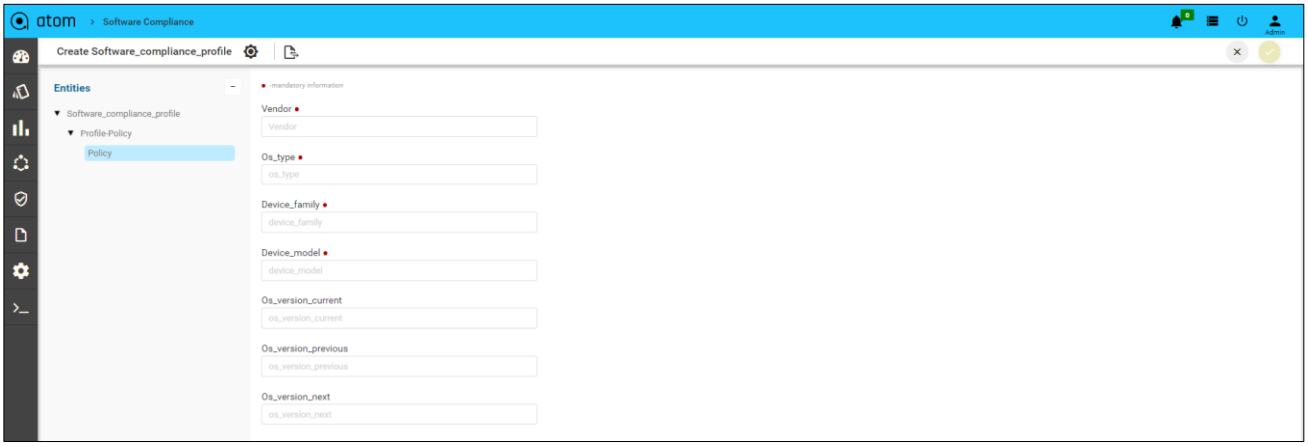
Utilize out-of-box Compliance workflows in ATOM and tie them into other workflows such as ZTP or other method-of-procedures (MOPs) to ensure Day-0 compliance on newly onboarded devices. The compliance workflows audit the chosen profiles and remediate non-compliance to ensure golden standards across the network as part of the business process.



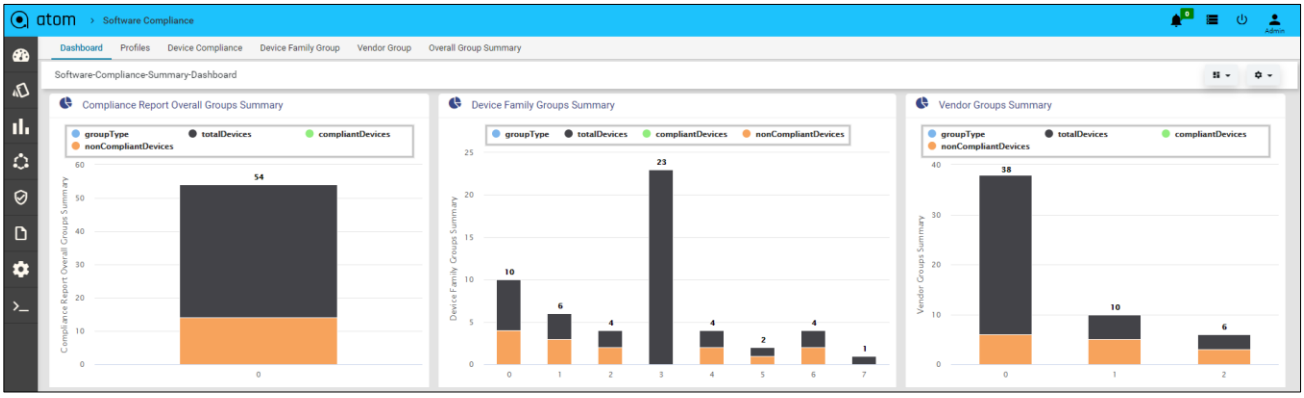
Compliance as a business process

Software Compliance

Most organization's wish list includes having a single software image across their network install base. ATOM's software compliance helps in maintaining software compliance across the network. ATOM offers the creation of multiple software compliance profiles to capture the vendor, platform, OS family, etc. to mark the golden software image of the network. A periodical assessment against the inventory data by ATOM results in a detailed dashboarding and compliance reporting on the vendor, device, device groups.



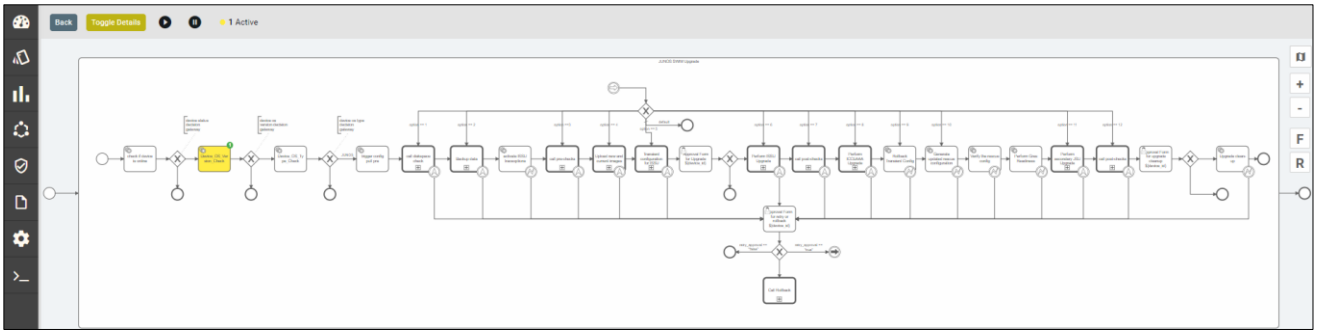
Define golden images per vendor/platform



Software compliance dashboard & reports

Ensure software compliance with ATOM's software upgrade workflows

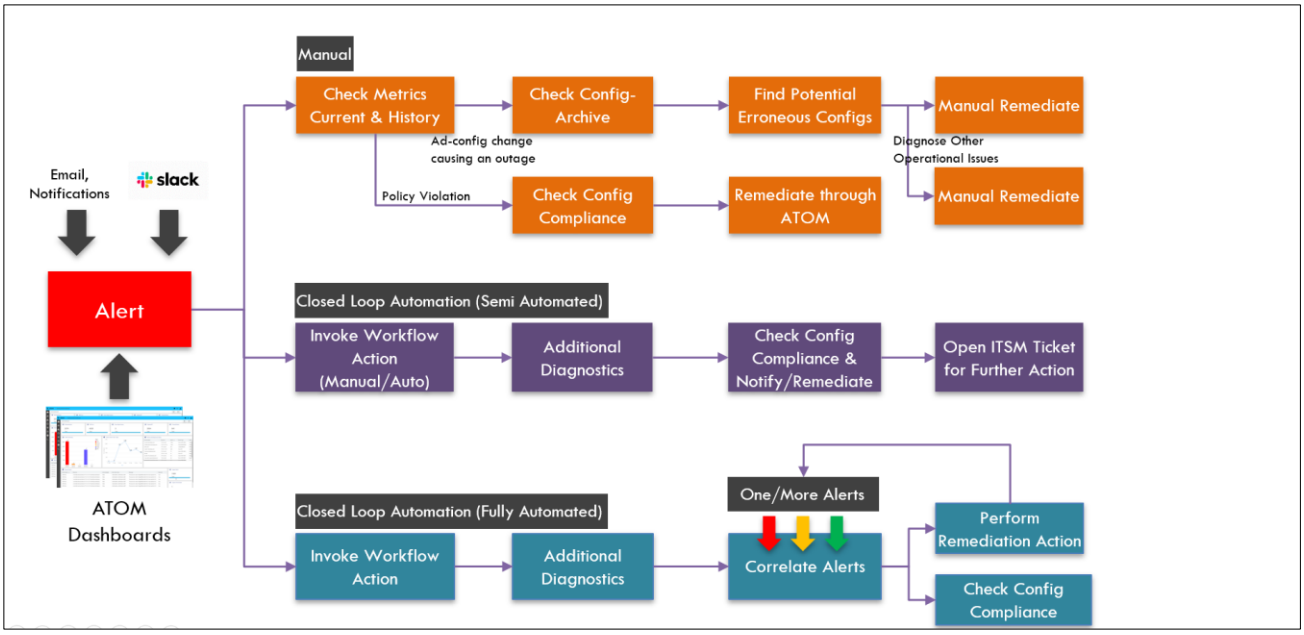
ATOM supports several flavors of vendor recommended software upgrade workflows to ensure software compliance across the network. The software upgrade workflows include pre-checks, contacting the image server (ATOM also has an image server), uploading the image to the device, activating the new package via a reboot, and post-checks to ensure a successful upgrade.



Software upgrade workflows

Ensuring Compliance – A step in ATOM's troubleshooting tool kit

ATOM's Alerting & Closed Loop Automation framework plays a crucial role in network troubleshooting. ATOM's compliance management forms a part of this troubleshooting exercise. An alert generated in ATOM always has an action associated with it. In most scenarios addressing complex issues, a diagnostic workflow that performs various validations ends up being the action to an alert. The first step in a diagnostic workflow is a compliance profile execution to validate if the vulnerability alert resulted from non-compliance of configuration, service, or software. Initial compliance checks aids in speeding up the triage and results in faster remediation.



Compliance for troubleshooting

Easily scale with ATOM's microservices architecture

Monitor and manage compliance of the entire network through a single pane of glass. Given its horizontally scalable microservices architecture, ATOM can enforce compliance across thousands of devices- up to 1M+!

Additional Resources

Video-on-demand on ATOM Compliance Management

To learn how Anuta Network's ATOM Multi-Vendor Configuration and Compliance management can help you simplify network audit procedures, contact us at https://www.anutanetworks.com