Customer Portal Release Notes

Release 3.1
31 August 2017
Revision 2

These Release Notes accompany Release 3.1 of the Customer Portal. They describe new and changed features in the software.

Contents

New and Changed Features

This section describes the new features or enhancements to existing features in Customer Portal Release 3.1.

SD-WAN

- **Support for managing and deploying SD-WAN policies**—From Customer Portal Release 3.1 onward, you can define and deploy SD-WAN policies for applications or application groups based on service-level agreement (SLA) requirements. SD-WAN policies help in optimum utilization of the WAN links and efficient distribution of traffic. Policies are applied at site, site group, or department level. You can also schedule your policy deployment for a later date and time.
- **Support for creating SLA profiles for applications and application groups**—From Customer Portal Release 3.1 onward, you can create tenant-level SLA profiles and associate the SLA profiles with applications or application groups. (In this context, the term *applications* refers to applications that do not need a Secure Sockets Layer (SSL) inspection.) An SLA profile consists of defined target metrics, which include the following:
  - Throughput, latency, packet loss, jitter, and delay
  - An assured class of service
  - Upstream and downstream rates for its applications
- **Support for four SD-WAN-enabled links per site**—Starting with Customer Portal Release 3.1, you can configure up to four WAN links per site that support SD-WAN. You can configure these links as MPLS or broadband links. In releases before Customer Portal Release 3.1, you can configure only two WAN links.
- **Support for monitoring SLA performance**—Customer Portal Release 3.1 supports the SLA-performance monitoring of tenants, sites, and applications that have met and those that have not met their defined SLA values in a specified period.
- **Support for monitoring SD-WAN events**—Customer Portal Release 3.1 supports the monitoring of SD-WAN events. SD-WAN events are triggered when the SLA requirements for a site are not met on its designated WAN link and the site switches WAN links to meet its SLA requirements.
- **Support for creating site groups**—Customer Portal Release 3.1 enables you to create site groups, which are a collection of one or more sites, for policy management. A site group enables you to apply a policy to all the sites in a group simultaneously. You create site groups from the Create Site Group page (**Site** > **Site Groups** > **Create Site Group**).

- **Viewing the bandwidth capacity of a WAN link**—From Customer Portal Release 3.1 onward, you can view the maximum bandwidth capacity of a WAN link. To view bandwidth capacity of a WAN link, hover over the WAN link connected to a site on the **WAN** tab of the *Site-Name* page (**Sites > Site Management > *Site-Name* > WAN**).
- **Support for grouping LAN segments into departments**—From Customer Portal Release 3.1 onward, you can group LAN segments within a site into departments. You use departments to apply specific policies to LAN segments that are members of a department. You can create, view, edit, or delete departments from the Departments page (**Configuration > Shared Objects > Departments**).

Security Management

- **Support for NAT policy management**—Customer Portal Release 3.1 enables you to create, modify, and delete Network Address Translation (NAT) policies and rules. In Customer Portal Release 3.1, only source-NAT and static-NAT management are supported.
- **Support for intent-based firewall policy**—Customer Portal Release 3.1 enables you to create, modify, and delete firewall intents associated with a firewall policy. Firewall policies are intent-based, which means that they can incorporate both Transport Layer (Layer 4) and Application Layer (Layer 7) application firewall constructs in a single intent. In addition, policies are automatically assigned to devices based on the endpoints chosen in the definition of the intent, and do not need to be assigned to specific devices manually. Firewall intents consist of source and destination endpoints; the endpoints can be applications (L7), sites, IP addresses, IP address groups, site groups, departments, and services. (In this context, the term *applications* refers to applications that do not need a Secure Sockets Layer (SSL) inspection.)
- **Support for schedules in firewall policy**—From Customer Portal Release 3.1 onward, you can create, modify, clone, and delete firewall policy schedules. A schedule enables you to run an intent for a specified period either on a one-time or on a recurring basis based on how the schedule is created.
- **Support for services in firewall and NAT policies**—From Customer Portal Release 3.1 onward, you can create, modify, clone, and delete services or service groups.

  A service refers to an application on a device, such as Domain Name System (DNS). Services are based on protocols and ports used by an application, and when added to a policy, a configured service can be applied across all devices. The protocols available to create a service include TCP, UDP, SUN-RPC, MS-RPC, ICMP, ICMPv6, and so on.

  You can combine services together to form a service group. Service groups are useful when you want to apply the same policy to multiple services because by doing this you can create and work with fewer policies.
- **Support for security dashboards**—From Customer Portal Release 3.1 onward, a security dashboard page displays information such as top events, top denials, top applications, top source and destination IP addresses, top traffic, and top infected hosts.
- **Support for application visibility**—From Customer Portal Release 3.1, you can view information about bandwidth consumption, session establishment, and the risks associated with your network applications. Analyzing your network applications provides

useful security management information, such as applications that can lead to data loss, bandwidth overconsumption, time-consuming applications, and personal applications that can elevate business risks.

- **Support for security alerts**—From Customer Portal Release 3.1, you can create, edit, and delete security alert definitions. Alerts are used to notify administrators about significant events within the system and warn them about problems in your monitored environment.

  An alert definition consists of data criteria for triggering an alert. An alert is triggered when the event threshold exceeds the defined data criteria.

- **Support for security events and system log messages**—From Customer Portal Release 3.1 onward, you can view security events associated with firewall, Web filtering, IPsec VPN, content filtering, antispam, antivirus, and IPS events.

  Security events include the system log messages of the device and critical information such as the number of events, virus instances found, interfaces that are down, attacks, CPU spikes, reboots, and sessions.

- **Ability to collect and view device events**—From Customer Portal Release 3.1 onward, you can troubleshoot a device by using device events. Device events include the following:

  - Routine operations—for example, user login into the configuration database
  - Failure and error conditions—for example, failure to access a configuration file
  - Emergency or critical conditions—for example, device power failure due to excessive temperature

- **Support for generating reports**—From Customer Portal Release 3.1 onward, you can generate reports to view the summary of network activity and overall network status of CPE devices. Using reports, you can:

  - Create, edit, delete, and clone reports, preview reports in PDF, and send reports by e-mail
  - Schedule reports based on the defined filters
  - Schedule reports based on the available default reports
  - Generate reports with multiple sections, where each section has its own criteria

- **Support for application signature management**—Customer Portal Release 3.1 enables you to create, modify, clone, delete, and view custom application signature groups, and view predefined application signatures.

- **Support for active database**—From Customer Portal Release 3.1, you can download and install the application firewall signature database to CPE devices. This database includes signature definitions of attacks and applications that can be used to identify applications for tracking firewall policies and quality of service prioritization.

- **Support for address management**—Customer Portal Release 3.1 enables you to create, edit, and delete addresses and address groups. Addresses and address groups are used in firewall and NAT services.

Customer Portal

- **Support for role-based access control (RBAC)**—Customer Portal Release 3.1 enables you to add, view, edit, and delete tenant users. The following roles are available:
  - **Tenant Administrator**—Users with the Tenant Administrator role have full access to the Customer Portal and APIs. They can add one or more users with Tenant Administrator or Tenant Operator roles.
  - **Tenant Operator**—Users with the Tenant Operator role have read-only access to the Customer Portal and APIs.
- **Security enhancements related to login credentials**—Customer Portal Release 3.1 includes the following security-related enhancements:
  - You can use the **Forgot Password** link on the Login page to reset your password.
  - After you log in for the first time, you are prompted to change your password.

    Passwords must conform to the password rules specified in the UI.
  - Your account is locked after five consecutive unsuccessful login attempts.
- **Customer Portal Dashboard**—From Customer Portal Release 3.1 onward, you can view a customized view of network services by using the widgets on the user-configurable Dashboard page.

  You can drag these widgets from the carousel at the top of your dashboard to your workspace, where you can add, remove, and rearrange them to meet your needs. The dashboard automatically adjusts the placement of the widgets to dynamically fit on your browser window without changing their order. You can manually reorder the widgets by using the drag and drop option. In addition, you can press and hold the top portion of the widget to move it to a new location.

Miscellaneous

- **Activation process for CPE devices**—From Customer Portal Release 3.1 onward, you can activate SRX300 Services Gateway and NFX250 Network Services Platform devices in the following ways:
  - By connecting a computer to the LAN port of the device and entering the activation code through your browser
  - By specifying the activation code in Customer Portal
- **Support for viewing devices**—From Customer Portal Release 3.1, you can use the Devices page (**Resources > Devices**) to view the list of available CPE devices at the customer premises. You can also view information about each CPE device in the network.
- **Support for viewing device images**—From Customer Portal Release 3.1 onward, you can view a list of uploaded device images on the Images page (**Resources > Images**).

- **Support for configuration deployment**—From Customer Portal Release 3.1 onward, you can deploy SD-WAN and security policies immediately or schedule the deployment for a later date and time.
- **Support for viewing policies at the device level and site level**—From Customer Portal Release 3.1 onward, you can view the policies assigned to a CPE device (**Resources** > **Devices** > ***Device-Name*** > **Policies**) and the policies assigned to a tenant site (**Sites** > **Site Management** > ***Site-Name*** > **Policies**). You can view the following information about policies:
  - List of all policies applicable to a tenant or site
  - Details about the tenant user who last updated the policy
  - Time when the policy was last updated
  - Deployment status of the policy
  - Number of intents applicable to the site compared to the total number of intents applicable to the tenant
- **Support for job management**—From Customer Portal Release 3.1 onward, you can view the list of jobs that are currently running and the jobs that are scheduled to run later. You can also specify whether you want to run a job immediately or schedule it for a later date and time.
- **Support for viewing licenses**—From Customer Portal Release 3.1 onward, you can view information about uploaded licenses on the Licenses page (**Administration > Licenses**).

Requesting Technical Support

Contact your service provider's organization for technical support.

Revision History

31 August 2017—Revision 2

21 August 2017—Revision 1, Customer Portal Release 3.1