

What's New in Juniper Networks Unified Access Control (UAC) 2.1

A description of the new features found in Juniper Networks UAC 2.1

Introduction

This document describes the new features available in version 2.1 of the Juniper Networks Unified Access Control (UAC) solution.

Scope

This document assumes familiarity with Juniper Networks UAC 1.2 and Juniper Networks UAC 2.0, as well as basic familiarity with Juniper's Odyssey[®] Access Client (OAC) 802.1X client and Steel-Belted Radius[®] (SBR) AAA/RADIUS servers.

Juniper Networks Unified Access Control (UAC) 2.1 Features

Juniper Networks Unified Access Control (UAC) 2.1 includes the following features:

Support for Additional Steel-Belted Radius (SBR) Capabilities

Supports additional RADIUS processing capabilities within the Juniper Infranet Controller (IC) to flexibly handle an increased number of deployment and usage scenarios. The additional SBR features integrated within UAC v2.1 include:

- Support for additional Extensible Authentication Protocol (EAP) types
- Support for RADIUS proxy
- The ability to upload RADIUS dictionaries to the Infranet Controller

Extended Support for Different Device Types

Extends support for unmanageable devices and cross-platform endpoints to include:

- The ability to dynamically address unmanageable devices through Media Access Control (MAC) address white listing or blacklisting, and integration with an existing backend database or asset discovery or profiling solution
- A NAC-enabled Layer 2/Layer 3 UAC Agent for the Microsoft Vista platform
- Support for a persistent Layer 3 agent on Apple[®] Macintosh[®] and Linux platforms

Extended Endpoint Assessment/Remediation Support

Improves endpoint compliance based access control by:

- Extending endpoint assessment capabilities to incorporate pre-defined patch management checks
- Extending automatic remediation capabilities
- Supporting Java-based IMCs/IMVs for standards-based integration of endpoint software on non-Windows platforms

Coordinated Threat Control and Dynamic Threat Management

Introduces the ability to leverage Intrusion Detection and Prevention (IDP) and Unified Threat Management (UTM) capabilities for dynamic network protection, providing the:

Copyright ©2007 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

- Ability to leverage IDP network and application level threats to dynamically quarantine a user for real-time network protection
- Ability to apply role-based security policies for users with Juniper firewalls/IDP

Flexible, Scalable, Secure Access Control

Provides additional access control security and functionality, including :

- Configurable UAC Agent on the Infranet Controller
- Role-based UAC Agent download
- Limit simultaneous user logins for the same user
- Licensing changes

Additional Features Added in 2.1R3 maintenance release

- OAC Client Manager Control of Balloon Notification Updates
- Configurable Coordinated Threat Control Remediation Messages
- OAC Windows Password Change Improvements
- OAC System Tray Status Icon Changes

Support for Additional Steel-Belted Radius (SBR) Capabilities

Supports additional RADIUS processing capabilities within the Infranet Controller to flexibly handle an increased number of deployment and usage scenarios.

- **Support for Additional Extensible Authentication Protocol (EAP) Types in the Infranet Controller**

Juniper Networks Unified Access Control (UAC) 2.1 offers support for additional EAP types on all Infranet Controllers (IC 4000 and IC 6000). By supporting additional EAP types in the Infranet Controller, customers are able to control access to their network at the Access Layer for a diverse array of deployment scenarios.

The additional EAP types supported include:

- Outer methods, such as:
 - PAP
 - CHAP
 - MSCHAP
 - MSCHAPv2
 - EAP-MSCHAPv2
 - EAP-MD5
 - EAP-GTC
 - EAP-TTLS
 - EAP-PEAP
 - EAP-TLS
- Inner methods, including:
 - EAP-MSCHAPv2
 - EAP-MD5
 - EAP-GTC
 - EAP-JUAC

Benefits: Enables customers to control access to their network at the Access Layer for a wide variety of deployment scenarios including, for example UAC Agent with GINA enabled, or user authentication for guests accessing the network with a 3rd party supplicant.

Availability: Available on all Infranet Controller products.

- **Support for RADIUS Proxy**

Juniper's UAC enables administrators to proxy inner and additional authentication types to a backend RADIUS server. Available on all Infranet Controller models, this feature enables customers to support deployments where certain authentications require a backend RADIUS server. The RADIUS proxy authentication is supported at the realm level.

Benefits: Enables customers to support deployments where certain authentications have to be supported by a backend RADIUS server.

Availability: Available on all Infranet Controller products.

- **Upload RADIUS dictionaries to Infranet Controller**

Juniper's UAC enables administrators to upload to the Infranet Controller new RADIUS dictionaries to support any RADIUS clients – such as switches and access points – that the Infranet Controller does not natively support. This enables customers to preserve their existing network topology and configurations by supporting value added attributes being sent to switches, even those that the IC does not support out of the box.

Benefits: Enables customers to preserve their existing network topology and configurations by supporting value added attributes being sent to switches and access points, even those that the Infranet Controller does not support natively.

Availability: Available on all Infranet Controller products.

Expanded Support for Different Device Types

UAC extends its support for unmanageable devices and cross-platform endpoints.

- **Dynamically Addresses Unmanageable Devices**

Juniper Networks Infranet Controller supports the dynamic provisioning of access control rules for unmanageable devices – including networked printers, barcode scanners, terminals, and so on. Through support for Media Access Control (MAC) address authentication via RADIUS, in combination with MAC address white listing and blacklisting on the Infranet Controller, the Infranet Controller can dynamically identify a device as an unmanageable device and assign it to the appropriate VLAN for access to the network.

The Infranet Controller now also includes the ability to query a backend database via Lightweight Directory Access Protocol (LDAP) interfaces or alternately an asset discovery or profiling solution as part of the authentication sequence for an unmanageable device, obtaining the device's true identity and using any profiles or attributes returned by the backend database or asset discovery or profiling solution to map the device to the appropriate VLAN for network access. This enables customers to save time and cost by allowing them to employ their existing policy and profile stores, providing deep integration to leverage user profiles and attributes for role- and resource-based access control.

Benefits: Enables customers to leverage their existing policy and profile stores by providing deep integration for leveraging user profiles and attributes for role and resource based access control.

Availability: Available on all Infranet Controller products.

- **NAC-Enabled Layer 2/Layer 3 Agent for Microsoft® Windows Vista™ Platforms**

Juniper Networks is introducing a full-featured Odyssey® Access Client (OAC) for Microsoft Windows Vista platforms, providing user authentication, endpoint assessment, IPsec and client-side enforcement capabilities. This new member of the OAC 802.1X client family enjoys feature parity with the edition of OAC for the Microsoft Windows® XP and Windows 2000 operating system platforms. It can be dynamically provisioned by the Infranet Controller or configured as an .msi package by the Odyssey Client Administrator and pre-installed on user devices, enabling customers to deploy a unified agent for seamless and comprehensive access control across their entire installed base of user devices and operating system platforms, including the growing number of Windows Vista deployments.

Benefits: Enables customers to deploy a unified agent for seamless and comprehensive access control across their entire infrastructure, including emerging Microsoft Windows Vista deployments.

Availability: Available on all Infranet Controller products. Also available on all applicable Odyssey Access Client editions (with an upgrade to the latest OAC version).

- **Persistent Layer 3 Agent for Apple[®] Macintosh[®] and Linux Platforms**

Juniper Networks introduces a persistent Layer 3 agent for Apple Macintosh and Linux platforms, enabling customers to deploy UAC at Layer 3 and more easily support their heterogeneous endpoint infrastructure (Microsoft Windows, Apple[®] Mac OS[®], Linux, etc). The persistent Layer 3 agent does not require a browser window to remain open to achieve Layer 3 network connectivity, and can be used to log in and out of the Infranet Controller to gain access to network resources.

Benefits: Enables customers to more easily deploy UAC in Layer 3 mode to support their heterogeneous endpoint infrastructure (Windows, Macintosh, Linux, etc.).

Availability: Available on all Infranet Controller products.

Extended Endpoint Assessment/Remediation Support

UAC continues to extend its endpoint compliance-based access control capabilities.

- **Pre-Defined Patch Management Checks**

Juniper Networks UAC extends its endpoint assessment capabilities to now include in the Infranet Controller the ability to support predefined patch management checks through its integration of Shavlik NetChk[®] Protect predefined patch management assessment checks. Available now on all Infranet Controller products, UAC's pre-defined endpoint patch management checks include the ability to inspect the endpoint for targeted operating system or application hot fixes, enabling UAC customers to easily define policies that can be directly linked to the presence or absence of specific hot fixes for defined operating systems and/or applications. The pre-defined patch management checks can also be performed according to the severity level of the vulnerability (critical, high, medium, low, etc.) and can be used to enforce access to certain roles or deny access to certain roles.

Benefits: Enables customers to more easily define policies that ensure access control is tied to the presence or absence of certain critical hot fixes for operating systems and applications.

Availability: Available on all Infranet Controller products.

- **Extended Automatic Remediation Support**

Juniper Networks UAC extends its auto-remediation capabilities for non-compliant devices, enabling customers to remediate automatically those devices that do not meet policy prior to allowing them on to their network, minimizing support calls from users of non-compliant endpoints.

UAC's extended auto-remediation capabilities include:

- For all antivirus applications supported by UAC:
 - Launching an antivirus process, if it's not already running
 - Launching an antivirus scan
 - Downloading a virus definition file, if the antivirus definition file isn't recent enough
 - Invoking real time protection, if it's not already enabled
- Firewall auto-remediation for Microsoft Windows XP and 2000 and Windows Vista, turning the firewall on, if it is not running
- Automatically modifying registry settings to pre-defined values as specified by policy for compliance

Benefits: Enables the solution to auto-remediate endpoints before allowing them on to the network, minimizing the support calls from noncompliant users.

Availability: Available on all Infranet Controller products. Also available in all Odyssey Access Client (OAC) editions (with an upgrade to the latest OAC version) in a UAC environment.

- **Support for Java-based IMC/IMV Pairs**

Juniper Networks UAC adds the ability to support the integration of 3rd party endpoint software for compliance checks on non-Microsoft Windows platforms (Mac OS, Linux, Solaris) by including support for Java-based IMC/IMV pairs. This allows for the creation of custom endpoint assessment checks on platforms other than Microsoft Windows, and for those checks to be leveraged as part of an UAC deployment. This is available in agent-less mode only for Apple Macintosh (Apple Mac OS), Linux, and Solaris platforms, and is available on all Infranet Controller products. Please note that the Java IMCs/IMVs complement the native endpoint assessment capabilities already provided by UAC for Macintosh, Linux, and Solaris platforms in agent-less mode.

Benefits: Enables the development of custom endpoint assessment checks on non-Microsoft Windows platforms and to have them leveraged and accessible as part of an UAC deployment.

Availability: Available on all Infranet Controller products, in agent-less mode only for Apple Macintosh (Apple Mac OS), Linux, and Solaris platforms.

Coordinated Threat Control and Dynamic Threat Management

UAC introduces Coordinated Threat Control with the ability to leverage Juniper's Intrusion Detection and Prevention (IDP) and Unified Threat Management (UTM) products to deliver dynamic network protection.

- **Leverage IDP Network and Application Level Threats for Dynamic User Quarantines**

Juniper's UAC now enables enterprises to leverage the deep packet, application level threat intelligence of Juniper Networks standalone Intrusion Detection and Prevention (IDP) platforms as part of its framework. When a standalone Juniper IDP detects a network threat of a particular type – policies can be configured on several attributes including attack category, attack protocol, attack strings, actions taken, destination or source addresses/ports – it can signal the Infranet Controller, which after receiving the signal and information from the IDP can narrow the threat to a specific user or device. UAC can then implement a configurable policy action, including the following flexible options: quarantining the user (or device) by placing them in a restricted VLAN; changing roles and denying access to certain applications; terminating the user session; or even disabling the user session until an administrator can re-enable it. UAC can also be configured to take no action but to just log the event. Through these actions, UAC ties access control not only to endpoint integrity and user identity, but also to actual traffic through the network.

Available on all Infranet Controller products – but requiring a separate license – this feature enables customers to leverage their Juniper IDP as part of their access control deployment for dynamic threat management, bringing security enforcement deeper into the network's core in addition to the network's edge for ubiquitous protection.

Benefits: Enables customers to leverage their standalone Juniper IDP platform as part of their access control deployment for dynamic threat management. Also enables enterprises to bring security enforcement deeper into the core of the network and to the edge of the network for more ubiquitous protection.

Availability: Available on all Infranet Controller products; **HOWEVER**, requires a separate license, 1 per platform on the Infranet Controller (IC4000-ADD-TCTRL and IC6000-ADD-TCTRL).

- **Apply Role-based Security Policies for Juniper Firewall/IDP Users**

UAC introduces the ability for all of its Infranet Controller products to not only apply role-based network and application access control policies, but also role-based threat management policies – like network IDP, network antivirus, network spyware, and/or network URL filtering. Enterprises can now leverage UAC for not only dynamic access control, but also dynamic threat control. As an example, an un-trusted user no longer must simply be placed into quarantine or remediation; UAC can also turn on security services in the network to ensure that the user's access to the network and networked applications is rendered secure. This functionality is available on all Juniper firewalls (with UTM enabled) or on Juniper's ISG-IDP or SSG platforms (with UTM enabled).

- Benefits:** Enables enterprises to leverage UAC for not only dynamic access control but also dynamic threat control.
- Availability:** Available on all Infranet Controller products

Flexible, Scalable, Secure Access Control

Providing additional access control security and functionality.

- **Configurable, Dynamically Downloadable Odyssey Access Client (OAC) UAC Edition (UE)**

A Layer 2/Layer 3 Odyssey Access Client (OAC) UAC Edition (UE) agent has been introduced as part of Juniper's UAC solution. This dynamically downloadable OAC UAC Edition agent introduces new features and can be configured on any Infranet Controller for a tighter control over user-exposed features and settings. This allows customers to enable access control in their infrastructure without the expense and deployment and management issues of pre-installed client software.

The new, downloadable OAC UAC Edition now supports client lock down, where the Infranet Controller can be used to lock down agent settings that should not be exposed to users. The Infranet Controller also supports additional configurations on the OAC UAC Edition such as configuring profiles that include, as example login names for use, wired and/or wireless adapter configuration, authentication protocols, network SSIDs, and IC URLs, that can be pre-configured and dynamically downloaded. Also, the Infranet Controller can be used to prevent the Odyssey Client Administrator and license management settings from being exposed to users.

Benefits: Allows customers to enable access control in their infrastructure without requiring the pre-installation of client software. Also enables enterprises to preserve their ability for dynamic download while still tightly controlling the settings of the agent.

Availability: Available on all Infranet Controller products.

- **Role-based UAC Agent Download**

Juniper Networks' introduces the ability for the UAC Agent download to be role-based. Through this feature, the Infranet Controller can now dynamically determine the role of the user on login and, based on the requirements for that role the Infranet Controller can dynamically deliver the client in the appropriate manner (agent-based or agent-less). This enables customers to tie agent-less or agent-based access dynamically to a user or device identity, instead of to realms that force users to make an upfront selection. If the role does not require a client, the user will be able to attempt network access through UAC's agent-less method.

Benefits: Enables customers to tie agent-less or agent-based access dynamically to user and/or device identity instead of tying it to realms that force users to make an upfront selection.

Availability: Available on all Infranet Controller products.

- **Limit Simultaneous Logins for the Same User**

Juniper Networks UAC has instituted the ability to limit simultaneous user logins, allowing only a set number of logins per user at any given point in time. This enables customers to enforce simultaneous user login limits should they choose to mandate this limit as a security policy. The user login limit is configurable. When the user exceeds the simultaneous individual login limit, they are presented with an option to either continue, which drops the previous session(s), or to cancel the current authentication process, preserving the older session(s). User session limit support is available in both UAC Agent and agent-less modes.

Benefits: Enables customers to enforce limits on simultaneous user logins should their security policies mandate this as a requirement.

Availability: Available on all Infranet Controller products in UAC Agent or agent-less modes.

- **New Licenses Adding Coordinated Threat Control to UAC**

Juniper Networks is introducing 2 new licenses for UAC, the IC4000-ADD-TCTRL and IC6000-ADD-TCTRL. These new licenses add the ability for UAC to communicate with Juniper IDP products for Coordinated Threat Control based on Juniper IDP intelligence, providing enterprises with a flexible option to leverage additional access control and security capabilities with their UAC deployment.

Benefits: Provides enterprises with a flexible option to layer more capabilities on their UAC deployment.

Availability: Available on all Infranet Controller products; **HOWEVER**, requires a separate license, 1 per platform on the Infranet Controller (IC4000-ADD-TCTRL and IC6000-ADD-TCTRL).

Additional Features Added in 2.1R3 maintenance release

- **OAC Client Manager Control of Balloon Notification Updates**

2.1R3 adds several new options to the OAC Client Manager (OCM), allowing end users to control the notifications that they receive from Odyssey related to authentication and endpoint integrity issues. This capability was previously available to administrators through hidden registry settings, but can now be controlled by end users if desired. Specifically, the end user can control whether or not to see these notifications, the display of the notifications (dialog box vs system tray balloon), as well as the duration and time between display of the notifications.

Benefits: Provides end users with greater control over their Odyssey Access Client experience, allowing them to tailor their interaction with OAC.

Availability: Available on all Infranet Controller products. Also available in all Odyssey Access Client (OAC) editions in a UAC environment.

- **Configurable Coordinated Threat Control Remediation Messages**

The 2.1R3 release adds additional administrator control over end user remediation messages when using the Coordinated Threat Control functionality with Juniper IDP products. When the IDP sensor event results in the Infranet Controller changing a user's network access, the end user will receive messages similar to those received when their machine has failed one or more endpoint security (Host Checker) policies. A default message is provided, but administrators are now able to fully customize these messages in order to provide the end user with a clear indication of the issue and how it will affect them. If the Coordinated Threat Control policy stipulates that the user should be disconnected, OAC will handle this event in the same manner that any other OAC disconnect is handled.

Benefits: Allows administrators to customize the end user experience in order to reduce any end user confusion and to minimize helpdesk calls.

Availability: Available on all Infranet Controller products. Also available in all Odyssey Access Client (OAC) editions in a UAC environment.

- **OAC Windows Password Change Improvements**

This feature improves the OAC behavior after a successful password change event. When a user changes their password, OAC will now capture the new password and use it during re-authentication, allowing a more seamless experience for the end user. This change applies when the user changes their password via the CTRL-ALT-DEL menu, to Windows password changes via OAC at GINA login time, and to password changes during authentication (post-GINA).

Benefits: Improves the end user experience by providing a seamless re-authentication event via OAC, even after the password has been changed.

Availability: Available on all Infranet Controller products. Also available in all Odyssey Access Client (OAC) editions in a UAC environment.

- **OAC System Tray Status Icon Changes**

This change improves the user experience when OAC cannot connect to an Infranet Controller. The system tray icon in this situation will now display a black "connecting..." icon rather than a red "authentication failed" icon. Please reference the

Odyssey Access Client User's Guide or Administrator's Guide for further information on the balloon status icons and their meaning.

- Benefits:** Provides more useful and accurate information to the end user when they are unable to connect to an Infranet Controller.
- Availability:** Available on all Infranet Controller products. Also available in all Odyssey Access Client (OAC) editions in a UAC environment.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.