

Service Description

The Nova Datacom Juniper Networks Unified Access Control (UAC) Implementation service provides specialized support by Certified Juniper Networks Engineers who have the skills and experience to help you implement and optimize UAC solutions with Layer 2 and/or Layer 3 enforcement quickly, securely, and efficiently at your operation centers. This implementation service also includes onsite knowledge transfer and 5 calendar days of post-installation deployment support during which engineers are available for follow-up questions.

The implementation service is intended for all Juniper Unified Access Control and is delivered in five phases:

Phase 1: Pre-Qualification and Recommendations

Our certified Juniper engineer gathers the following information from your organization:

- Product requirements
- Existing physical and logical network topology
- Deployment options: Stand alone or Clustered for Redundancy/Load Balancing
- Centralized Management option
- Authentication Integration options: LDAP/Active Directory/PKI - Certificates, Smart Cards, DoD Common Access Card -CAC
- Enforcement Methods: Layer 2 Enforcement via 802.1X, Layer 3 Enforcement via ScreenOS/JUNOS
- End point Security: Host checker
- Security Certification requirements: FIPS, Common Criteria

The engineer will then make recommendations about:

- Placement in network
- Access Method considerations
- Features to be used, licensing requirements and best practices recommendations
- Any special setup needed based on the applications and resources

Phase 2: Implementation Planning

When you receive your customized Unified Access Control Implementation Plan, it addresses:

- Network placement and connection to surrounding network gear
- Cluster Architecture (if applicable)
- NSM (Network Security Manager) Design Architecture and integration (if applicable)
- Realm and Role design (Up to 5)
- Resource profiles and policy design (Up to 10)
- Endpoint Security
- Monitoring and administration (Syslog/SNMP)
- Recommended test plan

Phase 3: Implementation

The engineer identifies the recommended Unified Access Control OS release for the device and begins the implementation. Activities include:

- System configuration
- Application of License Key
- Installation of server certs and or configuration of Certificate Signing Request

Cage: 4RLJ8
DUNS: 169242760
GSA: GS35F0322U Schedule 70

SBA-certified 8(a)
Minority Woman-Owned
SDB

- ❑ Importing Trusted Certificate Authority
- ❑ Configuration of Authentication Integration
- ❑ Configuration of Clustering
- ❑ Configuration of NSM Integration
- ❑ Configuration of Realm and Role design (Up to 5)
- ❑ Configuration of Resource profiles and policy design (Up to 10)
- ❑ Configuration of Layer 2 Enforcement (Up to 10)
- ❑ Configuration of Layer 3 Enforcement (Up to 10)
- ❑ Configuration of Endpoint Security
- ❑ Configuration of Appliance monitoring and administration
- ❑ Verifying access and functionality
- ❑ Providing 'As-built' configuration guide
- ❑ Providing Flowchart of data flow
- ❑ Providing exported configuration in XML format
- ❑ The following steps may be initiated remotely and completed during the onsite visit:
 - Perform Initial Configuration (IP Addresses, DNS, Routing)
 - Load recommended Unified Access Control OS release onto the device
 - Configuration of Layer 2/Layer 3 Enforcement
 - Assist in post-deployment monitoring while customer executes test plan

Phase 4: Knowledge Transfer

During the onsite phase, your engineer provides informal knowledge transfer. Topics covered during this information exchange may include:

- ❑ Review of Architecture and Device Configuration
- ❑ Basic troubleshooting
- ❑ Monitoring of event and access logs
- ❑ Centralized Management via NSM

Phase 5: Post-Installation Support

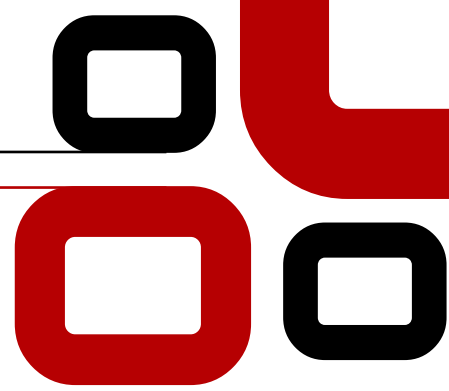
Once deployed, your organization receives support for 5 calendar days. During this phase, you can pose IDP configuration-related questions to our Engineering staff by phone or e-mail. These Firewall engineers are available Monday through Friday, through 9 am to 5 pm local time and have one business day to respond,



OPERATE
SERVICE SPECIALIST



IMPLEMENT
SERVICE SPECIALIST



Nova Datacom responsibility

Provide a Certified Juniper Networks Engineer to:

- ❑ Help deploy and configure the Unified Access Control at your Operation Center
- ❑ Provide Daily Status update
- ❑ Provide As-built configuration
- ❑ Provide knowledge transfer for customer engineers
- ❑ Be available for 5 days of remote post-installation support
- ❑ Be part of a designated team available for follow-up questions during normal business hours as agreed upon in SOW

Customer Responsibility

- ❑ Complete and submit pre-implementation questionnaire prior to the scheduling of Nova Datacom's onsite resource
- ❑ Provide a designated project manager or point-of-contact to interface with Nova Datacom for daily issues and coordination of resources
- ❑ Provide access to applications, databases, and technical resources as required
- ❑ Provide all power and interface cabling to the equipment
- ❑ Provide network resource and connectivity
- ❑ Have a test plan for all critical applications

Nova Datacom, LLC

4501 Singer Ct. Suite 350 Chantilly, VA 20151
www.novadatacom.com • info@novadatacom.com
Tel: 888.205.4062 • Fax: 703.234.9040

© 2011 Nova Datacom, LLC. All rights reserved. All other company and product names are trademarks of their respective owners.