



BorderGuard[™] Management Console

**Release Notes
MC Version 2.6-2861**

September 2007

Blue Ridge Networks, Inc.
14120 Parke Long Court
Chantilly, VA 20151

1.0 Introduction

The BorderGuard™ Management Console Release Notes highlight the new features found in the Blue Ridge Networks BorderGuard Management Console (MC) component. A more complete description of the MC capabilities can be found in the Management Console System Setup Guide.

The MC has been created to facilitate setup of Blue Ridge Networks VPN solutions. It is deployed as a preconfigured, headless appliance and is accessed by an administrator using a standard web browser. The initial releases of the MC specifically focused on enabling X.509-based remote access and site-to-site VPN solutions which featured DoD PKI interoperability and leveraged the x.509 features available in the BorderGuard 6000 series models. Subsequent MC releases have added support for site-to-site solutions based on the use of pre-placed public keys with BorderGuard 5000 series and Compact BorderGuard 100/550 models. The MC also supports RemoteLink™ solutions for Remote Access using BorderGuard 5000 series and BorderGuard 6000 series as the server component.

2.0 MC Hardware

The MC is deployed as a pre-loaded, 1-U server appliance. The appliance is Intel-based and uses a 3.0 GHz Xeon processor with 800 MHz front side bus. It is configured with 2 GB DDR SDRAM and a 200 GB, 7200 RPM, hot-swappable SATA drive. The MC is equipped with two network interface cards (NICs) to facilitate enterprise setup and management of the appliance.

3.0 MC Release Features

MC software is based on open standards and open source components such as Apache Tomcat, J2EE, Struts framework and Linux OS. MC applications provide capabilities to setup and manage BorderGuards in VPN configurations.

3.1 MC Release 2.6-2861 (September 2007)

The following sections summarize the new features incorporated in the 2.6-2861 version of the Management Console.

3.1.1 Increased Flexibility in Handling VPN Configuration Changes

Previously, the MC-enforced VPN configuration consistency by blocking all configuration changes to a VPN where one or more of its BorderGuards were offline. With the changes in MC version 2.6, updates are no longer blocked and, in fact, the current configuration status for each device is tracked as it compares to the configuration of other BorderGuards participating in the VPN.

NOTE: This feature is not applicable to changes in the VPN Management Policy which will affect the Remote Manager device and remotely managed BorderGuards.

3.1.2 Improvements to Certificate Validation Process (OCSP)

An MC Admin can now specify multiple OCSP servers (multiple URLs) and an OCSP policy for a trusted root certificate. The OCSP interface has been enhanced to handle the situation where the MC is requesting status for single certificate that is being authenticated, but an external OCSP responder/repeater responds with status for multiple certificates. In addition, the MC will verify signed OCSP responses from an external OCSP server when an OCSP server certificate or Self-signed CA certificate has been added on the Trusted Root page.

When multiple OCSP servers have been entered, the MC will contact the OCSP servers in the order that they appear in the list. (The MC considers the first server in the list as the Primary OCSP server and will use its response for respective certificate during the certificate-validation process. If there is NO response from the Primary OCSP server, then the MC will contact the next server (Backup OCSP server) in the list.

The OCSP policy options are used to fine tune system behavior associated with end users ID certificate validation status from an OCSP server. The policy options include:

- *High* (If the OCSP server is unavailable, the certificate status will be assumed to be “revoked” and access will be denied),
- *Medium* (If the OCSP server is unavailable, the MC-cached values for certificate validation will be checked and if there is no information on the certificate, its status will be assumed to be “revoked” and access will be denied. If there is a cached value for this certificate, the system will use that cached result.)
- *Low* (If the OCSP server is unavailable, the MC-cached values for certificate validation will be checked and if there is a cached value for this certificate, the system will use that cached result. If there is no information on the certificate, its status will be assumed to be “good” and access will be allowed. If desired, the Administrator can request a notification email for every case where Low policy is selected and an end user is allowed access, but the OCSP server is unavailable and there is no cached result.)

The default OCSP policy is *High*.

3.1.3 New Features for MC-Signed Certificates

MC version 2.6 has added several new features that enhance the use of MC-signed certificates in certificate-based Remote Access VPNs.

An Admin can now create, save and use Certificate Templates to assist in generating MC-signed ID certificates. Multiple values can be assigned to a certificate field. The display of ID certificates (Audit Certificates page) has been improved with a tabular layout highlighting the subject field, expiration date, the issuer and an icon representation for the certificate status. An Admin can filter/view MC-signed certificates by expiration date, valid/not-valid certificate status, or using a Certificate Template. The certificate listing pages for CA cert, Trusted Root cert, Audit cert, and Cached cert also use this improved display format.

The new MC has added a “Certificates” tab on the Remote Access Group page to view a list of ID certificates that will satisfy the group’s mapping criteria. A count of these certificates is shown on the title bar for the “Related Certificates” table.

The VPN Overview page has been restructured to provide linked views of deployed VPNs/Policies, BorderGuard devices and the associated connected users or sessions. VPN Notes can be created and associated with VPNs or devices.

3.1.4 External Backup and Backup/Restore Enhancements

A new capability has been added on the System Backup page to enable use of an external server for manual or scheduled (periodical) upload of backup files to Windows shares (using SMB).

During the standard backup processing a “waiting” screen is shown and when backup is complete, the backup files are listed. The file size of each backup is also shown in this Backup Files listing which can be sorted by file name and file date.

The MC Backup / Restore facility has been improved to use a “custom” format that results in faster backups and restores.

3.1.5 Audit Improvements

Audit subtypes have been added to enhance the detail captured by audit messages. For example, audit data can indicate that changes were made to a VPN Policy or to a Logical Device configuration, and an LDAP audit subtype can identify error conditions that may occur during a check of the LDAP server’s connection.

New audit log messages aid in capturing the LDAP query/authentication process and the text of log messages have been improved to better indicate whether they are for internal OCSP communication (between BG and MC) or external OCSP communication (between MC and external OCSP server).

RemoteLink session performance statistics have been added to the system data collected. These statistics are provided by the BorderGuard logger for each active session on every BG that is participating in an RL Policy.

3.1.6 Check Access to Servers (OCSP/LDAP)

Improved logic for the "Check Access to Servers" button on Trusted Root Authority (TRA) page selects one of the following certificates - cached ID cert, Intermediate CA cert, Trusted Root cert (in the order listed on the TRA page) - to check server connectivity for the LDAP and OCSP server(s). Along with the status, it will display the certificate used for checking the server connectivity.

3.1.7 Other Improvements

Several other changes and fixes have been applied to the MC. They include:

Syslog: A syslog export feature has been added to the MC. This feature converts MC audit messages to syslog format and allows export to an external syslog server.

Client Policy: RA VPN policy settings have been added to reflect options for smart card authentication, VNIC MTU and VLAN tagging.

RL Policy: A drop-down selection has been added to the RemoteLink Policy tunnel parameters page (with Mode 3) which allows Administrators to assign specific parameters applicable to an RA Server BG. In addition, RemoteLink Policy tunnel parameters for encryption are limited to IDEA, AES128, AES192, AES256, TDES, ESP-TDES, NONE.

GUI/Wizard improvements: A sidebar ("third frame") now displays the "Wizard Steps and Progress" for the respective VPN Wizard. Wizard logic has been improved to better allow modifying an existing VPN Policy versus creating a new policy.

Fixed MC Token Utility and Added Error Handling: Resolved issues with certain characters in userID/password when attempting to login to the MC Token Utility. The solution required URL encoding to ensure accurate transfer of UserID/Password characters between RemoteLink Token Utility and the MC). A validation check and display of the error message was added to the token utility to alert the Admin to suscriptoin creation problems while programming KeyGuard tokens.

Added Error Check to BorderGuard Naming: A check is now made when a BorderGuard name is entered to ensure it does not exceed the BorderGuard limit of 64 characters.

3.2 MC Release 2.4-2421 (March 2007)

The following sections summarize the new features incorporated in the 2.4-2421 version of the Management Console.

3.2.1 Improved X.509 RA OCSP Checking

The MC has improved the ability to identify the issuer for cached certificates. It has also enhanced the OCSP status messages for cached certificates where an OCSP server is not specified on the Trusted Root Certificate.

Additional log messages have been provided to increase the audit coverage of communication between the MC and OCSP servers as well as communication between the MC and LDAP servers.

Additional parameters have been added to the CA Settings GUI to allow administrative adjustments to OCSP Time Variance (skew) and OCSP External Server Timeout . These parameters help the system better handle message delays for OCSP responses and cases where there is no OCSP response.

3.3 MC Release 2.4-2351 (February 2007)

The following sections summarize the new features incorporated in the 2.4-2351 version of the Management Console.

3.3.1 Default User ID

The MC's default system administrator account has been renamed from "root" to "suadmin". The default password has not been changed.

3.3.2 Support for "Enclave" Routing Policy

Site-to-site VPNs can now be configured to enable a special routing policy. An administrator can choose an "enclave" option to force all traffic destined for external to be routed through the VPN secure tunnel. This is especially useful for central star site-to-site deployments where traffic for the internet is routed securely from the star "remote" sites to the central site. An administrator can select this optional routing policy for hub and spoke as well as central star topologies.

3.3.3 Enable / Disable ICMP Ping

MC administrators can explicitly enable or disable the ability of a BorderGuard to respond to ICMP pings. This can be very valuable to enable ICMP ping response when troubleshooting a deployment, but then disable the response for more security.

3.3.4 Enhanced RemoteLink™ Token Handling

The MC GUI has added tabs to display fields in a programmed RemoteLink KeyGuard without having to reload the "package" (.brz) file with the token utility. In addition, the "package" filename is now automatically assigned based on end user name and RemoteLink policy.

3.3.5 VPN Tunnel Names

The convention for naming VPN tunnels has been modified to provide shorter names.

NOTE: This change will only impact existing deployments that are upgrading an MC from 2.4-2190 where RemoteLink users were deployed. For those deployments, new subscriptions need to be created for your existing RemoteLink end users. After you have upgraded the MC to 2.4-2351 and after the RA servers have been uploaded with an updated configuration (including the new tunnel names), all older RemoteLink KeyGuard tokens will need to be re-programmed or new tokens can be issued so that the subscriptions reflect the new naming convention.

3.4 MC Release 2.4-2190 (December 2006)

The following sections summarize the features incorporated in the 2.4-2190 version of the Management Console.

3.4.1 Support for "Classic" Remote Access using RemoteLink™

The Management Console now supports configuration of Remote Access VPNs using RemoteLink™ (RL) devices, RL static subscriptions and a pre-placed public key deployment model. BorderGuard 5000 series models, Compact BorderGuards and BorderGuard 6000 series models can be used for these VPNs. Several features have been added to the MC in support of this new capability:

- An administrator can define modify and delete Named End-Users and End-User Groups that can be used in RemoteLink™ policies.

- RemoteLink™ VPN policies can be defined to support all RemoteLink™ modes of operation. These policies can be customized to indicate individual tunnel parameters associated with a specific RA BorderGuard server. This is useful when programming a token with multiple subscriptions.
- Multiple Remote Access BorderGuard servers can be combined to create a “Pooled Device”. This concept is used to enable redundancy and load-spreading for RemoteLink™ connections.
- A downloadable “Token Utility” is provided with the MC. This utility can be installed on a PC running Win2K, XP or Server 2003 and is used to program KeyGuard tokens with RemoteLink™ subscriptions (policy and keys) that have been encrypted and packaged at the MC. The utility communicates with the MC via an administrator login (https protocol) to enable the MC to audit KeyGuard programming events.
NOTE: In order to download the “Token Utility” from the MC, an administrator must have at least “Read” permission for the “Manage End-User Tokens” privilege. This minimum permission is also required for the person programming the KeyGuards.
- A standard RA RemoteLink™ connection report has been added to the default report package on the MC.

3.4.2 MC GUI and Audit Enhancements

Several enhancements have been added to the MC GUI. Navigational links are now shown at the top of a web page to show a history of MC activity. Visual feedback on web pages has been added by enabling and disabling the “Save/Update” button. Validation checks are now performed on Device and End-User names to only allow letters, numbers, underscores and spaces as character entries.

Background audit messages have been corrected to indicate the owner is “system process” rather than “unknown user” or “no logged on user”.

3.4.3 S2S Traffic Filter

An administrator can now update or copy an individual S2S traffic filter. The MC has also added the ability to do DNS lookup and set default traffic filters on the Device or on a VPN policy.

3.5 MC Release 2.3-2100 (December 2006)

The following sections summarize the features incorporated in the 2.3-2100 version of the Management Console.

3.5.1 Customize VPN Configuration

Several additional features have been added to allow an administrator to customize the configuration of a Remote Access or Site-to-Site VPN:

- Define additional routes/networks/hosts that will participate in a VPN.
- Customize Site-to-Site VPN policy by creating admin-defined “Traffic Filters” to control processing of Site-to-Site traffic.

- An administrator can select a BorderGuard and view a textual description summarizing the effect of the BorderGuard filters that are being applied to VPN traffic.
- Administrator can now designate a specific BorderGuard to serve as a Remote Manager, acting as a “Secure Gateway” to manage remotely deployed BorderGuards.
- Sleeve timeouts can be modified on Remote Access and Site-to-Site policy screens.

3.5.2 Verify Connectivity to External Servers

The MC has added a facility to help Administrators verify that the MC can access servers that have been designated as LDAP (CRL) and OCSP responders. This can be used during system setup and can assist in operational troubleshooting.

3.5.3 BorderGuard Settings

More BorderGuard control has been provided to administrators:

- The MC allows an administrator to set a BorderGuard’s password. The password is case sensitive and must be at least 4 characters long and less than 32 characters. The MC will accept and apply any combination of printable password characters except ‘ (single quote) and \ (back slash).
- When the BorderGuard is used as a DHCP server, the MC adds a 5 second delay after DHCP startup to ensure secure tunnel setup is complete.
- An administrator can modify BorderGuard interface port speed and duplex settings. In addition, a BorderGuard can be configured to use any UDP port between 1 and 65535.

NOTE: The ability to set a UDP port between 1 and 512 requires that the BorderGuard use firmware 7.4-12 or later.

3.5.4 CA Certificate Management

Administrators can pre-load DoD PKI CA certificates to the MC’s list of trusted root certs. They can also view and delete cached CA certs or CRLs, and they can generate a new signing CA certificate if the settings of the built-in Certificate Authority have been modified.

3.5.5 Enhancements for X.509 Remote Access

Several enhancements have been added to the X.509 Remote Access functionality:

- In defining the X.509 Remote Access “group definition” used in the Remote Access VPN and/or “Red List”, multiple values can be used for the mapping. For example, many certificates have multiple CNs, DCs, etc in the certificate’s “Distinguished Name” field. Mappings can be created to match against these repeated tags.
- (Green List) The MC allows an administrator to import user-specific cert identifiers that can be associated in group mappings. One initial application of this capability is the import of EDI-PI attributes from Active Directory, and use of these attributes to define specific membership in RA groups. Because these

attributes are also found in user's certificates, this constitutes a type of access list or "Green List" to grant VPN access based on a match with this parameter. Other parsing templates can be loaded to expand the uses of this feature.

NOTE: Full "Green List" functionality requires the use of firmware 7.4-15 or later.

3.5.6 Export Audit and Logger Data

An administrator can export displayed audit or logger records in csv format.

3.6 MC Release 2.1-1310 (June 2006)

The following sections summarize the features incorporated in the 2.1-1310 version of the Management Console.

3.6.1 Management Sleeve Parameters

An administrator can modify the sleeve parameters associated with management sleeves.

3.6.2 UDP Destination Port

The default UDP destination port can be modified for Site-to-Site and Remote Access policies.

3.6.3 Wireless Remote Access

The MC now supports a template configuration for 3-port Wireless Remote Access deployments.

3.7 MC Release 2.1-1039 (February 2006)

The following sections summarize the features incorporated in the 2.1-1039 version of the Management Console.

3.7.1 Time Sync BorderGuards

The MC has been upgraded to force a time sync with all BorderGuards it is managing every 15 minutes to avoid possibility of time drift in deployed units.

3.7.2 Modified BorderGuard Default Logout

Default logout time for a managed BorderGuard is now set to 10 minutes.

3.7.3 Multi-Staged Initializations

Improved application of VPN configurations with multi-stage initialization approach to BorderGuard uploads. This approach reduces the possibility of an incomplete initialization.

3.7.4 Remote Access with DHCP Wizard

The Remote Access Wizard has been upgraded to support DHCP setup on the BorderGuard during the wizard steps.

3.7.5 Reload BorderGuard Configuration

A “Reload Configuration” button has been added to the Firmware tab of Physical BG screen. This enables a manual forced upload of the configuration files.

3.8 MC Release 2.1-990 (January 2006)

The following sections summarize the features incorporated in the 2.1-990 version of the Management Console.

3.8.1 Additional Site-to-Site Topology Options in the VPN Wizard

Previous releases provided the ability to deploy a Central Star Site-to-Site VPN. This release adds a Mesh Site-to-Site VPN option, and adds the ability to convert between a Central Star and a Mesh topology.

3.8.2 Support for Additional BorderGuard Models

The Management Console now supports configuration of Site-to-Site VPNs using BorderGuard 5000 series models as well as BorderGuard 6000 series models. Compact BorderGuard models, such as BG100 and BG550 are also supported using BorderGuard 5000 series authentication options. The following table illustrates VPN constraints based on model types:

VPN Type	BG 6000 Series		BG5000 Series		Comments
	Certs	Keys	Certs	Keys	
RA – X.509	Required	Allowed	NA	NA	X.509 RA only available on BG6000 series
RA – “Classic”	NA	NA	NA	NA	MC Does Not Support “static subscription” RA
S2S – X.509	Required	Allowed	NA	NA	X.509 S2S only available on BG6000 series
S2S – “Classic”	Allowed	Required	Prohibited	Required	Key exchange is focus of “Classic” S2S

3.8.3 Configure BorderGuard as DHCP Server

The Management Console can be used to set up the BorderGuard’s built in DHCP server to provide IP addresses for the VPN client.

3.8.4 Advanced Data Streaming Link to BorderGuard

Administrators can activate a live telnet session to the BorderGuard from within their web browser. This provides real time data reflecting current BorderGuard status and supports system troubleshooting.

3.8.5 Project/Site Option for Grouping Devices

Administrators can associate VPN devices with Projects and Sites. This option allows grouping BorderGuard devices to mirror a deployment environment and supports display of devices according to the VPN in which they are participating or according to their site grouping.

3.8.6 Session Timeout

Configurable session timeouts have been added to automatically log a user off the MC after a specified time of user inactivity.

3.8.7 Default Logger Settings

This feature allows temporary configuration of the logger for more detailed event capture, and can automatically reset the logger back to the default settings after a specified amount of time. This will prevent unintended flooding of the system with unwanted event data.

3.8.8 MC Environment Update Facility

The MC Restore facility has been extended to handle software and database updates. This enables system version upgrades and data migration.

3.8.9 Basic reports

This feature provides three pre-defined types of reports: MC/System Report, Remote Access Connection Report and Remote Access Red-List Report. The reports automatically run every night.

3.8.10 BorderGuard Passwords

Administrators (with the appropriate permission) can create and update BorderGuard passwords.

3.8.11 Reset to Factory Default

This feature allows an administrator to restore the MC's database to factory default state. This can be useful when conducting system tests prior to actual deployment.

3.9 MC Release 2.1-595 (August 2005)

The following sections summarize the features incorporated in the 2.1-595 MC. This release is the first version to fully support X.509 remote access and X.509 site-to-site (central star topology) using the BorderGuard 6000 models.

The X.509 standard refers to a very commonly encountered form of digital certificates, where an X.509 digital certificate contains the holder's public key as well as the holder's identity information such as name, organization, etc. In X.509 deployments, a Certificate Authority, or CA, is responsible for verifying the identity of certificate holders, publishing the public key certificate for previously issued certificates, responding to authenticated requests for certificate revocation, and providing notification of any certificate revocations.

The BorderGuard 6000 family uses the Management Console (MC) to provide CA functionality and to proxy enterprise information requests to external CAs. The MC provides information to the BorderGuard 6000 about the status of X.509 certificates that are presented from other BorderGuards or from VPN Client software. The BG6000 MC can be configured to use either CRL (Certificate Revocation Lists) or OCSP (Online Certificate Status Protocol) or both to perform certificate status checking.

3.9.1 Management Setup and Configuration

The MC provides the means for an IT administrator to initially setup the MC, to create Admin users and roles, to setup Certificate Services, and to configure Audit and Backup/Restore operations.

3.9.2 Remote Access Using Standard (X.509) Certificates

After the MC has been installed and configured, the MC provides a wizard-based approach to setup of remote access VPNs that use standard (X.509) certificates. Both locally managed and remote managed configurations are supported.

3.9.3 Site-To-Site (Central Star) Using Standard (X.509) Certificates

After the MC has been installed and configured, the MC provides a wizard-based approach to setup of site-to-site VPNs that use standard (X.509) certificates. Per the features in MC configuration of Certificate Services, the MC can either act as the CA for the VPN or the MC can proxy requests for an external CA.

3.9.4 System Status

After the MC has been installed and configured, the IT admin can use the MC to review audit data and logged information.