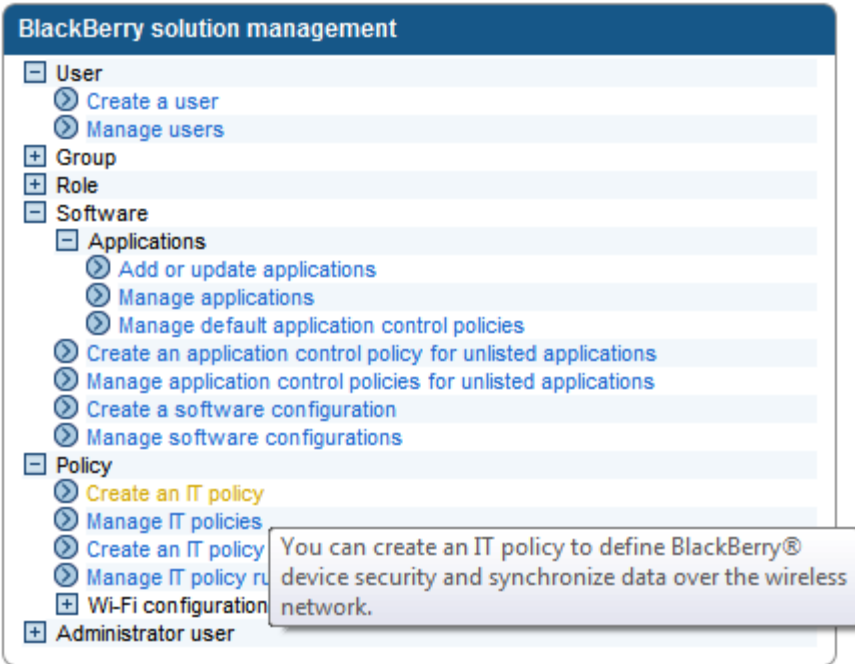


Recommended setting for Idle Timer

NOTE: If the customer already has an IT Policy in place or want to change their “default” policy for Third party apps. They need only to “Allow Resetting Idle Timer” to “yes” in the security tab of that policy.



BlackBerry solution management

- [-] User
 - Create a user
 - Manage users
- [+] Group
- [+] Role
- [-] Software
 - [-] Applications
 - Add or update applications
 - Manage applications
 - Manage default application control policies
 - Create an application control policy for unlisted applications
 - Manage application control policies for unlisted applications
 - Create a software configuration
 - Manage software configurations
- [-] Policy
 - **Create an IT policy**
 - Manage IT policies
 - Create an IT policy
 - Manage IT policy rules
- [+] Wi-Fi configuration
- [+] Administrator user

You can create an IT policy to define BlackBerry® device security and synchronize data over the wireless network.

Policy > Create an IT policy

Create an IT policy

IT policy rules help you control BlackBerry® devices in your organization. You can create an IT policy to define BlackBerry device security and synchronize data over the wireless network. You can configure IT policies, assign IT policies to users or groups, and more.

IT policy information	
Name:	Telenav Security Policy
Description:	Telenav Policy

Save
Cancel

Copyright © 1997 - 2011 Research In Motion Limited. All rights reserved.
Version: 5.0.2.28

Manage IT policies

You can rename IT policies, view a list of users with specific IT policies, assign IT policies to users and groups, edit IT policies, delete IT policies, and more.

Policy information	
Name:	Telenav Security Policy
Description:	Telenav Policy

Edit IT policy
View complete IT policy
Copy IT policy
Delete IT policy
View users with IT policy
View IT policies list

Copyright © 1997 - 2011 Research In Motion Limited. All rights reserved.
Version: 5.0.2.28

Disable IP Modem	<input type="checkbox"/>	Specify whether the Internet Protocol (IP) modem feature on applicable More...
Allow Smart Card Password Caching	<input type="checkbox"/>	Specify whether the smart card password can be cached.
Disable GPS	<input type="checkbox"/>	If this rule is set to More... Specify whether the GPS functionality on the BlackBerry device is turned More...
Force Content Protection of Master Keys	<input type="checkbox"/>	Specify whether the BlackBerry device, when locked, prevents the radio and More...
Force LED Blinking When Microphone Is On	<input type="checkbox"/>	Specify whether the BlackBerry device indicates that its microphone is on (for More...
Content Protection of Contact List	<input type="checkbox"/>	Specify whether the Include Contacts option on the BlackBerry device is set to More...
Disable State Certificate Status Checks	<input type="checkbox"/>	Specify whether to prevent the BlackBerry device from displaying warnings and More...
Disable External Memory	<input type="checkbox"/>	Specify whether to prevent the expandable memory (microSD) feature from working More...
Disable USB Mass Storage	<input type="checkbox"/>	Specify whether to prevent the USB Mass Storage feature or the Media Transfer More...
External File System Encryption Level	<input type="text"/>	Specify the level of file system encryption that the BlackBerry device uses to More...
Disable Media Manager FTP Access	<input type="checkbox"/>	Specify whether to disable access to the file transfer protocol channel from More...
Disable Smart Password Entry	<input type="checkbox"/>	Specify whether to prevent the user from using smart password entry on the More...
Force Smart Card Two Factor Challenge Response	<input type="checkbox"/>	Specify whether the user must choose a smart card certificate for use with More...
Secure Wipe If Low Battery	<input type="checkbox"/>	Specify whether the BlackBerry device securely wipes all of its user data if More...
Secure Wipe Delay After IT Policy Received	<input type="text"/>	Specify the length of time, in hours, after receiving an IT policy update that More...
Secure Wipe Delay After Lock	<input type="text"/>	Specify the length of time, in hours, after the BlackBerry device locks that More...
Firewall Block Incoming Messages	<input type="checkbox"/> SMS Messages <input type="checkbox"/> MMS Messages <input type="checkbox"/> BlackBerry Internet Service Messages <input type="checkbox"/> PN Messages (Public) <input type="checkbox"/> PN Messages (Corporate) <input type="checkbox"/> Enterprise Messages	Specify whether the firewall on the BlackBerry device blocks, and prevents the More...
Required Password Pattern	<input type="text"/>	Specify the permitted structure of the BlackBerry device password. A character More...
Require Secure APB Messages	<input type="checkbox"/>	Specify whether the BlackBerry device can receive unsecured messages, including More...
Password Required for Application Download	<input type="checkbox"/>	Specify whether the BlackBerry device will prompt the user for their password More...
Allow Resetting of Idle Timer	<input checked="" type="checkbox"/>	Specify whether the BlackBerry will allow third party applications to reset the More...
Reset to Factory Defaults on Wipe	<input type="checkbox"/>	Specify whether the BlackBerry device resets itself to factory default settings More...
Allow Screen Shot Capture	<input type="checkbox"/>	Specify whether the BlackBerry device will allow applications to capture screen More...
Disable Public Photo Sharing Applications	<input type="checkbox"/>	Specify whether to prevent public photo sharing applications (for example, More...
Disable Geo-Tagging of Photos	<input type="checkbox"/>	Specify whether to prevent the BlackBerry device from adding geographical More...
Message Classification Title	<input type="text"/>	Specify the message classification title that BlackBerry devices will include More...
Firewall Whitelist Addresses	<input type="text"/>	Specify the list of email addresses that the BlackBerry device firewall allows. More...
Weak Digest Algorithms	<input type="checkbox"/> MD2 <input type="checkbox"/> MD4	Specify the digest algorithms that the BlackBerry device considers weak. The More...

Manage IT policies

You can rename IT policies, view a list of users with specific IT policies, assign IT policies to users and groups, edit IT policies, delete IT policies, and more.

Policy information	Application Center	BlackBerry App World	BlackBerry Messenger	BlackBerry Smart Card Reader	BlackBerry Unite!	Bluetooth	Browser	Camera	Certificate Synchronization	Certification Authority Profile															
Chalk Pushcast	Common	Date and Time	Desktop	Desktop only	Device IOT Application	Device only	Documents To Go	Email Messaging	Enterprise Voice Client	External Display	Firewall	Global	Instant Messaging												
Location Based Services	MDS Integration Service	Memory Cleaner	On-Device Help	PGP Application	PM Synchronization	Password	Phone	RIM Value-Added Applications	S/MIME Application	S/M Application Toolkit	Secure Email	Security	Service Exclusivity	Smart Dialing	TCP	TLS Application	User Feedback	User defined	VPN	Visual Voice Mail	VoP	WTLS Application	Wi-Fi	Wired Software Updates	Wireless Software Upgrades

Policy information	
Name:	Telenav Security Policy
Description:	Telenav Policy
<input type="button" value="Save all"/> <input type="button" value="Cancel and return to view"/>	
<small>Copyright © 1997 - 2011 Research In Motion Limited. All rights reserved. Version: 5.0.2.28</small>	

Manage IT policies

You can rename IT policies, view a list of users with specific IT policies, assign IT policies to users and groups, edit IT policies, delete IT policies, and more.

Name	Description
Default	The Default IT policy includes all the standard IT policy rules that are set on the BlackBerry Enterprise Server.
Basic Password Security	Similar to the Default IT policy, the Basic Password Security IT policy also requires that users have a basic password that they can use to log in to the BlackBerry device. Users must change their passwords regularly. The IT policy includes a set password timeout that locks the BlackBerry device.
Medium Password Security	Similar to the Default IT policy, the Medium Password Security also requires a complex password that users can use to log in to the BlackBerry device. Users must change their passwords at regular intervals. The IT policy includes a maximum password history and turns off Bluetooth technology on the BlackBerry device.
Advanced Security	Similar to the Default IT policy, the Advanced Security IT policy also requires a complex password that a user must change frequently, a set password timeout that locks the BlackBerry device, and a maximum password history. The IT policy restricts Bluetooth technology on the BlackBerry device, turns on strong content protection, turns off USB mass storage, and requires the BlackBerry device to encrypt external file systems.
Medium Security with No 3rd Party Applications	Similar to the Medium Password Security, the Medium Security with No 3rd Party Applications IT policy requires a complex password that a user must change frequently, a set password timeout that locks the BlackBerry device, and a maximum password history. The IT policy prevents users from making their BlackBerry devices discoverable by other Bluetooth-enabled devices and turns off the ability to download third-party applications.
Advanced Security with No 3rd Party Applications	Similar to the Advanced Security IT policy, the Advanced Security with No 3rd Party Applications IT policy requires a complex password that a user must change frequently, a set password timeout that locks the BlackBerry device, and a maximum password history. The IT policy restricts Bluetooth technology on the BlackBerry device, turns on strong content protection, turns off USB mass storage, requires the BlackBerry device to encrypt external file systems, and turns off the ability to download third-party applications.
Individual-Liable Devices	Similar to the Default IT policy, the Individual-Liable Device IT policy prevents BlackBerry device users from accessing organizer data in social networking applications on their BlackBerry devices. In addition, users can access other calendar services and email messaging services, update the BlackBerry Device Software using update methods that exist outside your organization, make calls when the devices are locked, and out, copy, and paste text. Users are prevented from forwarding messages from one email messaging service to another.
Telenav Security Policy	Telenav Policy

-
-
-

BlackBerry solution management

- [-] User
 - ⌕ Create a user
 - ⌕ Manage users
- [+] Group
- [+] Role
- [-] Software
 - [-] Application
 - ⌕ Add or update applications
 - ⌕ Manage applications
 - ⌕ Manage default application control policies
 - ⌕ Create an application control policy for unlisted applications
 - ⌕ Manage application control policies for unlisted applications
 - ⌕ Create a software configuration
 - ⌕ Manage software configurations
- [-] Policy
 - ⌕ Create an IT policy
 - ⌕ Manage IT policies
 - ⌕ Create an IT policy rule
 - ⌕ Manage IT policy rules
 - [+] Wi-Fi configuration
- [+] Administrator user

You can update user information, add or change the groups and roles that users are assigned to, delete users, and more.

Manage users

You must search for a user to manage. You can update user information, add or change the groups and roles that a user is assigned to, and delete users.

User Information	Groups	Roles	Wi-Fi profiles	VPN profiles	VoIP profiles	Software tokens	Component information	Access control rules	Software configuration	Policies
------------------	--------	-------	----------------	--------------	---------------	-----------------	-----------------------	----------------------	------------------------	----------

User information

Display name: User ID:

Authentication type	User name	Password
Active Directory	The entered data retrieved a user identification from the Active Directory system. The authentication will use the associated Active Directory credentials.	

Associated device properties

PN	Device model
Home Carrier	Current Carrier
Phone number	Software version
Associated BlackBerry Enterprise Server	Last message sent
Last contact date	Result of last transaction to the device
Device IT policy	Delivered to device
Queued IT policy status	Password policy for Telenav
	Applied successfully
	Device IT policy time

Messaging configuration

Configuration	Description
Default configuration	The default configuration is created automatically when the BlackBerry Enterprise Server is installed.

- Edit user
- Send message to user
- Back to search
- Back to previous search results

- BlackBerry Enterprise Server status**
- Switch BlackBerry user to different BlackBerry Enterprise Server
 - Disable as BlackBerry user

- Status**
- Delete user
 - Reload user




- Device activation**
- Specify an activation password
 - Generate an activation email
 - Clear activation password
 - Specify new device password and lock device

- Device deployment**
- Resend service books to a device
 - Resend IT policy to a device
 - View tasks

Manage users

You must search for a user to manage. You can update user information, add or change the groups and roles that a user is assigned to, and delete users.

User information	Groups	Roles	Wi-Fi profiles	VPN profiles	VoIP profiles	Software tokens	Component information	Access control rules	Software configuration	Policies
IT policy name			Description					Assigned to		
Default			The Default IT policy includes all the standard IT policy rules that are set on the BlackBerry Enterprise Server.					User assigned		
Resolved IT policy name			Description					Assigned to		
Default			The Default IT policy includes all the standard IT policy rules that are set on the BlackBerry Enterprise Server.							

-  Edit user
-  Back to search
-  Back to previous search results

Copyright © 1997 - 2011 Research In Motion Limited. All rights reserved.
Version: 5.0.2.28

Manage users


You must search for a user to manage. You can update user information, add or change the groups and roles that a user is assigned to, and delete users.


User information	Groups	Roles	Wi-Fi profiles	VPN profiles	VoIP profiles	Software tokens	Component information	Access control rules	Software configuration	Policies
------------------	--------	-------	----------------	--------------	---------------	-----------------	-----------------------	----------------------	------------------------	----------

IT policy

IT policy:

- Default
- Basic Password Security
- Medium Password Security
- Advanced Security
- Medium Security with No 3rd Party Applications
- Advanced Security with No 3rd Party Applications
- Individual-Liable Devices
- Telenav Security Policy**

 Save all

 Cancel and return to view