BlackBerry Enterprise Server Express

Versione: 5.0
Service Pack: 4

Guida di riferimento ai criteri IT

BlackBerry®

Pubblicato: 29/10/2012
SWD-20121029114627124

Indice

1 Risorse correlate 10

2 Novità in questa versione 11

Nuova impostazione di configurazione 11

Nuove regole dei criteri di controllo applicazioni 11

3 Criteri IT 12

Criterio IT predefinito 12

Valori predefiniti per le regole dei criteri IT 12

4 Regole dei criteri IT 18

Gruppo criteri Solo dispositivo 18

Regola dei criteri IT Consenti messaggi peer-to-peer 18

Regola dei criteri IT Consenti messaggi di testo 18

Regola dei criteri IT: Attiva timeout a lungo termine 19

Regola dei criteri IT: Abilita configurazione WAP 19

Regola dei criteri IT Giacenza max password 20

Regola dei criteri IT: Timeout di protezione massimo 20

Regola dei criteri IT: Lunghezza minima della password 21

Regola dei criteri IT Modelli password 22

Regola dei criteri IT: Password obbligatoria 22

Regola dei criteri IT: L'utente può modificare il timeout 23

Regola dei criteri IT: L'utente può disattivare la password 23

Gruppo criteri Globale 24

Regola dei criteri IT: Consenti browser 24

Regola dei criteri IT: Consenti telefono 24

Gruppo criteri BlackBerry App World 25

Regole dei criteri IT: Attiva fatturazione provider di servizi wireless 25

Gruppo criteri Bluetooth 26

Regola dei criteri IT Bluetooth 26

Regola dei criteri IT: Disattiva bypass wireless 26

Gruppo criteri Browser 27

Regola dei criteri IT Disattiva JavaScript nel browser 27

Regola dei criteri IT per i Domini browser MDS 28

Gruppo criteri Fotocamera 28

Regola dei criteri IT: Disattiva fotocamera 28

Regola dei criteri IT: Disattiva videocamera 29

Gruppo criteri comuni 29

Regola dei criteri IT Disattiva MMS ... 29
Regola dei criteri IT Disattiva registrazione note vocali ... 30
Gruppo criteri Messaggi di posta elettronica ... 30
Regola dei criteri IT: Conferma download immagini esterne ... 30
Regola dei criteri IT: Disattiva download manuale di immagini esterne ... 31
Regola dei criteri IT: Disattiva funzioni di inoltro e risposta a messaggi crittografati in formato nativo di Notes ... 31
Regola dei criteri IT Disattiva contenuti multimediali e-mail ... 32
Regola dei criteri IT: Dimensioni massime di singoli allegati nel formato nativo MFH ... 33
Regola dei criteri IT: Dimensioni totali massime degli allegati nel formato nativo MFH ... 34
Regola dei criteri IT: Dimensioni massime di singoli allegati nel formato nativo MFH ... 34
Regola dei criteri IT: Timeout password di crittografia nativa di Notes ... 35
Regola dei criteri IT: Richiede la crittografia nativa di Notes per i messaggi in uscita ... 35
Gruppo criteri Password ... 36
Regola dei criteri IT: Password vietate ... 36
Regola dei criteri IT: Cronologia massima password ... 37
Regola dei criteri IT: Intervallo periodico ... 37
Regola dei criteri IT: Imposta numero massimo di tentativi password ... 38
Regola dei criteri IT: Imposta Timeout password ... 39
Regola dei criteri IT: Annulla eco password ... 39
Gruppo criteri Dispositivi personali ... 40
Regola dei criteri IT Disattiva Inoltro di contenuto di lavoro utilizzando canali personali ... 40
Regola dei criteri IT: Consenti la separazione di contenuto di lavoro ... 41
Regola dei criteri IT Richiedi risorse di lavoro per l'esecuzione delle attività ... 42
Regola dei criteri IT Domini aziendali ... 42
Gruppo criteri sincronizzazione PIM ... 43
Regola dei criteri IT: Disattiva tutte le sincronizzazioni wireless ... 43
Gruppo criteri applicazione PGP ... 44
Regola dei criteri IT: Crittografie del contenuto consentite per PGP ... 44
Regola dei criteri IT Modalità crittografia allegato consentita per PGP ... 45
Regola dei criteri IT: Tipi di crittografia consentiti per PGP ... 45
Regola dei criteri IT: Forza firma digitale per PGP ... 46
Regola dei criteri IT: Forza crittografia per messaggi PGP ... 47
Regola dei criteri IT: Lunghezza minima della chiave DH forte per PGP ... 47
Regola dei criteri IT: Lunghezza minima della chiave DSA forte per PGP ... 48
Regola dei criteri IT: Lunghezza minima della chiave RSA forte per PGP ... 49
Regola dei criteri IT: Modalità PGP parti successive e invio ... 49
Regola dei criteri IT: Metodo di registrazione al PGP ... 50
Regola dei criteri IT: Timeout cache criteri di PGP Universal ... 51
Regola dei criteri IT: Indirizzo del PGP Universal Server ... 51
Gruppo criteri Applicazioni RIM a valore aggiunto ... 52

Regola dei criteri IT Disabilita l'accesso ai dati dell'agenda elettronica per le applicazioni di social networking 52
Gruppo criteri di protezione 53
Regola dei criteri IT: Consenti connessioni esterne 53
Regola dei criteri IT Consenti la reimpostazione del timer di inattività 53
Regola dei criteri IT: Consenti connessioni Split-Pipe 54
Regola dei criteri IT: Consenti l'utilizzo della porta seriale alle applicazioni di terzi 54
Regola dei criteri IT Livello di protezione del contenuto 55
Regola dei criteri IT: Disattiva 3DES Transport Crypto 56
Regola dei criteri IT: Disattiva memoria esterna 56
Regola dei criteri IT: Disattiva GPS 57
Regola dei criteri IT: Disattiva modem IP 57
Regola dei criteri IT Disattiva memorizzazione di massa USB 58
Regola dei criteri IT Vieta download di applicazioni di terzi 59
Regola dei criteri IT: Applica crittografia ai file multimediali sulla memoria su scheda del dispositivo 60
Regola dei criteri IT: Livello di crittografia file system esterno 60
Regola dei criteri IT: Forza blocco nella custodia 61
Regola dei criteri IT: Modello password obbligatorio 61
Regola dei criteri IT: Reimposta valori predefiniti durante pulizia della memoria 62
Regola dei criteri IT: Convertitore di sicurezza hash file .cod 63
Gruppo criteri applicazione S/MIME 63
Regola dei criteri IT: Indirizzo e-mail EMS (Entrust Messaging Server) 64
Regola dei criteri IT: Crittografie del contenuto consentite per S/MIME 64
Regola dei criteri IT: Modalità crittografia allegato consentita per S/MIME 65
Regola dei criteri IT: Tipi di crittografia consentiti per S/MIME 66
Regola dei criteri IT: Forza firma digitale per S/MIME 66
Regola dei criteri IT: Forza crittografia per messaggi S/MIME 67
Regola dei criteri IT: Lunghezza minima della chiave DH forte per S/MIME 68
Regola dei criteri IT: Lunghezza minima della chiave DSA forte per S/MIME 68
Regola dei criteri IT: Lunghezza minima della chiave ECC forte per S/MIME 69
Regola dei criteri IT: Lunghezza minima della chiave RSA forte per S/MIME 70
Regola dei criteri IT: Modalità S/MIME parti successive e invio 70
Gruppo criteri VPN 71
Regola dei criteri IT: Nome utente VPN 71
Regola dei criteri IT: Password utente VPN 72
Gruppo criteri Wi-Fi 72
Regola dei criteri IT Disattiva Wi-Fi 72
Wired Software Updates policy group 73
Regola dei criteri IT: Consenti caricamento software basato su Web 73
Regola dei criteri IT: Backup servizi di crittografia 74
Gruppo criteri aggiornamenti software wireless 74

Regola dei criteri IT: Vieta download patch su roaming WAN ... 74

5 Impostazioni di configurazione ... 76

Impostazioni di configurazione per i profili Wi-Fi ... 76

Impostazione di configurazione Autorità di certificazione dei certificati associati ... 76

Impostazione di configurazione Profilo VPN associato ... 76

Consenti handover tra punti di accesso Wi-Fi ... 77

Impostazione di configurazione Consenti modifiche Wi-Fi sul dispositivo ... 77

Impostazione di configurazione Consenti salvataggio password Wi-Fi ... 77

Impostazione di configurazione Tipo canale per Wi-Fi ... 78

Impostazione di configurazione Modalità di accesso Wi-Fi a BlackBerry Infrastructure su rete Wi-Fi ... 78

Impostazione di configurazione Gateway predefinito della Wi-Fi ... 79

Impostazione di configurazione dell'ID chiave Wi-Fi predefinito ... 79

Impostazione di configurazione Configurazione DHCP della Wi-Fi ... 80

Impostazione di configurazione Disattiva convalida certificato server Wi-Fi ... 80

Impostazione di configurazione Suffisso dominio per Wi-Fi ... 81

Impostazione di configurazione Metodo di provisioning Wi-Fi ... 81

Impostazione di configurazione Attiva pagina autenticazione per Wi-Fi ... 82

Impostazione di configurazione Token hardware Wi-Fi richiesto ... 82

Impostazione di configurazione Modalità autenticazione interna per Wi-Fi ... 83

Impostazione di configurazione del percorso di accesso Internet Wi-Fi ... 83

Impostazione di configurazione Indirizzo IP Wi-Fi ... 84

Impostazione di configurazione Protezione collegamento Wi-Fi ... 84

Impostazione di configurazione Livello di protezione minimo per chiavi di crittografia di certificati EAP-TLS per Wi-Fi ... 85

Impostazione di configurazione Chiave Wi-Fi pre-condivisa ... 86

Impostazione di configurazione DNS primario della Wi-Fi ... 86

Impostazione di configurazione Modifica profilo Wi-Fi ... 87

Impostazione di configurazione Visibilità profilo Wi-Fi ... 87

Impostazione di configurazione Soglia roaming Wi-Fi ... 88

Impostazione di configurazione DNS secondario della Wi-Fi ... 88

Impostazione di configurazione SAN server per Wi-Fi ... 89

Impostazione di configurazione Oggetto server per Wi-Fi ... 89

Impostazione di configurazione SSID Wi-Fi ... 89

Impostazione di configurazione Subnet mask Wi-Fi ... 90

Impostazione di configurazione Numero di serie token Wi-Fi ... 90

Impostazione di configurazione Nome utente Wi-Fi ... 90

Impostazione di configurazione Password utente Wi-Fi ... 91

Impostazione di configurazione Chiave WEP 1 per Wi-Fi ... 91

Impostazione di configurazione Chiave WEP 2 per Wi-Fi ... 92

Impostazione di configurazione Chiave WEP 3 per Wi-Fi ... 92

Impostazione di configurazione Chiave WEP 4 per Wi-Fi ... 92
Impostazioni di configurazione per i profili VPN ... 93
Impostazione di configurazione Autorità di certificazione dei certificati associati ... 93
Impostazione di configurazione Abilita VPN ... 93
Impostazione della configurazione Modalità di divisione del tunnel ... 94
Impostazione di configurazione Annulla banner VPN ... 94
Impostazione di configurazione Utilizza Xauth per VPN ... 95
Impostazione di configurazione Consenti modifiche VPN sul dispositivo ... 95
Impostazione di configurazione Consenti salvataggio password VPN ... 96
Impostazione di configurazione Disattiva convalida certificato server VPN ... 96
Impostazione di configurazione Configurazione DNS VPN ... 97
Impostazione di configurazione Nome dominio VPN ... 97
Impostazione di configurazione Indirizzo gateway VPN ... 98
Impostazione di configurazione Nome gruppo VPN ... 98
Impostazione di configurazione Password gruppo VPN ... 98
Impostazione di configurazione Token hardware VPN richiesto ... 99
Impostazione di configurazione Crittografia IKE per VPN ... 99
Impostazione di configurazione Gruppo DH IKE per VPN ... 100
Impostazione di configurazione Hash IKE per VPN ... 100
Impostazione di configurazione Indirizzo IP VPN ... 101
Impostazione di configurazione Crittografia e hash IPSec per VPN ... 101
Impostazione di configurazione Livello di protezione minimo per chiavi di crittografia di certificati per VPN ... 102
Impostazione di configurazione Durata attività NAT VPN ... 103
Impostazione di configurazione PFS per VPN ... 103
Impostazione di configurazione DNS primario della VPN ... 103
Impostazione di configurazione Visibilità profilo VPN ... 104
Impostazione di configurazione Modifica profilo VPN ... 104
Impostazione di configurazione DNS secondario della VPN ... 105
Impostazione della configurazione Indirizzo IP subnet VPN 1 ... 105
Impostazione della configurazione Subnet mask VPN 1 ... 106
Impostazione della configurazione Indirizzo IP subnet VPN 2 ... 106
Impostazione della configurazione Subnet mask VPN 2 ... 106
Impostazione della configurazione Indirizzo IP subnet VPN 3 ... 107
Impostazione della configurazione Subnet mask VPN 3 ... 107
Impostazione di configurazione Subnet mask VPN ... 107
Impostazione di configurazione Numero di serie token VPN ... 108
Impostazione di configurazione Nome utente VPN ... 108
Impostazione di configurazione Password utente VPN ... 109
Impostazione di configurazione Tipo fornitore VPN ... 109
Impostazione di configurazione Tipo Xauth per VPN ... 110

6 Regole dei criteri di controllo applicazioni ... 111
Regola dei criteri di controllo applicazioni: Connessioni di rete esterne consentite ... 111
Regola dei criteri di controllo applicazioni: Connessioni di rete interne consentite ... 112
Regola dei criteri di controllo delle applicazioni: Le connessioni locali sono consentite? ... 113
Regola dei criteri di controllo applicazioni Le impostazioni del dispositivo possono essere modificate? ... 113
Regola dei criteri di controllo applicazioni Consentire il ripristino del timer di protezione? ... 114
Regola dei criteri di controllo applicazioni Visualizza informazioni quando bloccato ... 115
Regola dei criteri di controllo applicazioni: Disposizione ... 115
Regola dei criteri di controllo delle applicazioni: L'accesso all'API filtri browser è consentito? ... 116
Regola dei criteri di controllo applicazioni L'accesso ai dati aziendali è consentito? ... 117
Regola dei criteri di controllo delle applicazioni: L'accesso all'API posta elettronica è consentito? ... 117
Regola dei criteri di controllo applicazioni L'accesso all'API avvio evento è consentito? ... 118
Regola dei criteri di controllo applicazioni L'accesso all'API file è consentito? ... 118
Regola dei criteri di controllo applicazioni L'accesso all'API GPS è consentito? ... 119
Regola dei criteri di controllo applicazioni L'accesso all'archivio chiavi del dispositivo è consentito? ... 120
Regola dei criteri di controllo delle applicazioni: L'accesso all'API di comunicazione tra i processi è consentito? ... 120
Regola dei criteri di controllo applicazioni: Accesso all'API contenuto multimediale consentito ... 121
Regola dei criteri di controllo delle applicazioni: L'accesso all'API di gestione modulo è consentito? ... 122
Regola dei criteri di controllo applicazioni: L'accesso a NFC (Near Field Communication) è autorizzato? ... 122
Regola dei criteri di controllo applicazioni: L'accesso all'API PIM è consentito? ... 123
Regola dei criteri di controllo applicazioni: L'accesso all'API telefono è consentito? ... 124
Regola dei criteri di controllo applicazioni: L'accesso alle API di acquisizione schermo, microfono e video è consentito? ... 124
Regola dei criteri di controllo applicazioni: L'accesso all'elemento protetto è autorizzato? ... 125
Regola dei criteri di controllo applicazioni: L'accesso all'API SPP (Serial Port Profile) per Bluetooth è consentito? ... 126
Regola dei criteri di controllo applicazioni: L'accesso all'API autenticatore utente è consentito? ... 126
Regola dei criteri di controllo applicazioni: L'accesso all'API Wi-Fi è consentito? ... 127
Regola dei criteri di controllo applicazioni: Protezione media archivio chiavi consentita ... 128
Regola dei criteri di controllo applicazioni Gestione connessioni consentita ... 128
Regola dei criteri di controllo applicazioni Controllo contenuto multimediale consentito ... 129
Regola dei criteri di controllo applicazioni: I dati temi sono consentiti? ... 129
Regola dei criteri di controllo applicazioni: Elenco dei domini filtro browser ... 130
Regola dei criteri di controllo applicazioni: Elenco dei domini esterni ... 130
Regola dei criteri di controllo applicazioni: Elenco dei domini interni ... 131
7 Esempi dei livelli di protezione ... 132
Richiesta dell'utilizzo di una password su un dispositivo ... 132
Come evitare l'utilizzo non autorizzato di un dispositivo ... 133
Crittografia dei dati su un dispositivo ... 133
Limitazione della messaggistica su un dispositivo ... 134
Precauzioni per evitare i pericoli derivanti da virus o utenti malintenzionati ... 135
Limitazione delle risorse a cui può accedere un'applicazione di terzi su un dispositivo ... 135

Limitazione del controllo utente in applicazioni di terzi installate sui dispositivi BlackBerry 136
Blocco dell'esecuzione di applicazioni RIM a valore aggiunto su dispositivi BlackBerry 137
8 Glossario 138
9 Note legali 140

Risorse correlate

1

Per leggere le guide seguenti o il materiale aggiuntivo connesso, visitare il sito all'indirizzo www.blackberry.com/go/serverdocs.

Guida	Informazioni
Novità del BlackBerry Enterprise Server Express Materiale di supporto di 5.0 SP4	• Riepilogo delle nuove funzionalità
Guida di aggiornamento di BlackBerry Enterprise Server Express	• Riepilogo degli aggiornamenti delle guide per gli amministratori per BlackBerry Enterprise Server Express 5.0 SP4
Note sulla versione per BlackBerry Enterprise Server Express	• Descrizione di problemi noti e delle potenziali soluzioni temporanee
Guida di installazione e configurazione di BlackBerry Enterprise Server Express	• Requisiti di sistema • Istruzioni relative all'installazione
Guida all'aggiornamento di BlackBerry Enterprise Server Express	• Requisiti di sistema • Istruzioni relative all'aggiornamento

Novità in questa versione

2

Nuova impostazione di configurazione

Tipo di profilo	Impostazioni	BlackBerry Device Software (requisiti minimi)
VPN	Autorità di certificazione dei certificati associati	5.0

Nuove regole dei criteri di controllo applicazioni

Regola	BlackBerry Device Software (requisiti minimi)
L'accesso a NFC (Near Field Communication) è autorizzato?	7.0
L'accesso all'elemento protetto è consentito?	7.0

Criteri IT

3

È possibile assegnare i criteri IT ai dispositivi BlackBerry per soddisfare i requisiti di protezione dell'organizzazione e le necessità degli utenti BlackBerry. Ad esempio, è possibile creare un criterio IT, configurare le regole del criterio IT per soddisfare i requisiti di protezione, aggiungere utenti a un gruppo e assegnare il criterio IT al gruppo.

Per ulteriori informazioni sulla creazione di un criterio IT, sulla configurazione delle regole dei criteri IT e sull'assegnazione di un criterio IT a un account utente o a un gruppo, consultare la *Guida all'amministrazione di* BlackBerry Enterprise Server Express.

Criterio IT predefinito

BlackBerry Enterprise Server Express include un criterio IT predefinito. Quando si installa , le regole dei criteri IT nel criterio IT predefinito non contengono alcun valore. Se non si specifica un valore per una regola dei criteri IT, viene utilizzato il valore predefinito. Si può configurare e applicare il criterio IT predefinito agli account utente o si possono creare criteri IT nuovi e assegnarli agli account utente per controllare i dispositivi BlackBerry nell'ambiente dell'organizzazione.

Valori predefiniti per le regole dei criteri IT

Gruppo di criteri IT	Regola dei criteri IT	Valore predefinito
Elementi solo per il dispositivo	Consenti messaggi peer-to-peer	Sì
Elementi solo per il dispositivo	Consenti SMS	Sì
Elementi solo per il dispositivo	Attiva timeout a lungo termine	Sì
Elementi solo per il dispositivo	Attiva configurazione WAP	Sì

Gruppo di criteri IT	Regola dei criteri IT	Valore predefinito
Elementi solo per il dispositivo	Giacenza max password	Valore nullo
Elementi solo per il dispositivo	Timeout di protezione massimo	Valore nullo
Elementi solo per il dispositivo	Lunghezza minima della password	Valore nullo
Elementi solo per il dispositivo	Modelli password	Nessuna restrizione
Elementi solo per il dispositivo	Password obbligatoria	No
Elementi solo per il dispositivo	L'utente può modificare il timeout	Sì
Elementi solo per il dispositivo	L'utente può disattivare la password	Sì
Elementi globali	Consenti browser	Sì
Elementi globali	Consenti telefono	Sì
BlackBerry App World	Attiva fatturazione provider di servizi wireless	No
Bluetooth	Disattiva Bluetooth	No
Bluetooth	Disattiva bypass wireless	Sì
Browser	Disattiva JavaScript nel browser	No
Browser	Domini browser MDS	Valore nullo
Fotocamera	Disattiva fotocamera	No
Fotocamera	Disattiva videocamera	No
Comune	Disattiva MMS	No
Comune	Disattiva registrazione note vocali	No
Messaggi di posta elettronica	Conferma download immagini esterne	No

Gruppo di criteri IT	Regola dei criteri IT	Valore predefinito
Messaggi di posta elettronica	Disattiva download manuale di immagini esterne	No
Messaggi di posta elettronica	Disattiva funzioni di inoltro e risposta a messaggi crittografati in formato nativo di Notes	No
Messaggi di posta elettronica	Disattiva contenuti multimediali posta elettronica	No
Messaggi di posta elettronica	Dimensioni massime di singoli allegati nel formato nativo MFH	3.145.728 byte (3 MB)
Messaggi di posta elettronica	Dimensioni totali massime degli allegati nel formato nativo MFH	5 MB
Messaggi di posta elettronica	Dimensioni massime di singoli allegati nel formato nativo MTH	10.240 KB
Messaggi di posta elettronica	Timeout password di crittografia nativa di Notes	-1
Messaggi di posta elettronica	Richiedi la crittografia nativa di Notes per i messaggi in uscita	No
Password	Password vietate	Valore nullo
Password	Cronologia massima password	0
Password	Intervallo periodico	Sì (60 minuti)
Password	Imposta numero massimo di tentativi password	10
Password	Imposta Timeout password	2 minuti (versioni di BlackBerry Device Software precedenti alla 4.7) 30 minuti (BlackBerry Device Software 4.7 e versioni successive)
Password	Annulla eco password	Sì
Dispositivi personali	Disattiva inoltro contenuto di lavoro utilizzando canali personali	No

Gruppo di criteri IT	Regola dei criteri IT	Valore predefinito
Dispositivi personali	Consenti la separazione di contenuto di lavoro	No
Dispositivi personali	Richiedi risorse di lavoro per l'esecuzione delle attività	No
Dispositivi personali	Domini aziendali	Valore nullo
Sincronizzazione PIM	Disattiva tutte le sincronizzazioni wireless	No
Applicazione PGP	Crittografie del contenuto consentite per PGP	Utilizzare tutti gli algoritmi supportati
Applicazione PGP	Modalità crittografia allegato consentita per PGP	Automatico
Applicazione PGP	Tipi di crittografia consentiti per PGP	Entrambi
Applicazione PGP	Forza firma digitale per PGP	No
Applicazione PGP	Forza crittografia per messaggi PGP	No
Applicazione PGP	Lunghezza minima della chiave DH forte di PGP	1024 bit
Applicazione PGP	Lunghezza minima della chiave DSA forte di PGP	1024 bit
Applicazione PGP	Lunghezza minima della chiave RSA forte di PGP	1024 bit
Applicazione PGP	Modalità PGP parti successive e invio	Manuale
Applicazione PGP	Metodo di iscrizione di PGP Universal	Iscrizione basata su e-mail
Applicazione PGP	Timeout cache criteri di PGP Universal	24 ore
Applicazione PGP	Indirizzo di PGP Universal Server	Valore nullo
Applicazioni RIM Value-Added	Disattiva l'accesso ai dati dell'agenda elettronica per le applicazioni di social networking	Sì
Protezione	Consenti connessioni esterne	Sì
Protezione	Consenti la reimpostazione del timer di inattività	No
Protezione	Consenti connessioni simultanee	No
Protezione	Consenti l'utilizzo della porta seriale ad applicazioni di terzi	Sì
Protezione	Livello di protezione del contenuto	Valore nullo

Gruppo di criteri IT	Regola dei criteri IT	Valore predefinito
Protezione	Disattiva 3DES Transport Crypto	No
Protezione	Disattiva memoria esterna	No
Protezione	Disattiva GPS	No
Protezione	Disattiva modem IP	No
Protezione	Disattiva memorizzazione di massa USB	No
Protezione	Vieta download di applicazioni di terzi	No
Protezione	Applica crittografia ai file multimediali sulla memoria su scheda del dispositivo	Autorizzazione concessa
Protezione	Livello di crittografia file system esterno	Non richiesto
Protezione	Forza blocco nella custodia	No
Protezione	Modello password obbligatorio	Valore nullo
Protezione	Reimposta valori predefiniti durante pulizia della memoria	No
Protezione	Convertitore di sicurezza hash file .cod	Valore nullo
Applicazione S/MIME	Indirizzo e-mail EMS (Entrust Messaging Server)	Valore nullo
Applicazione S/MIME	Crittografie del contenuto consentite per S/MIME	Utilizzare tutti gli algoritmi supportati
Applicazione S/MIME	Modalità crittografia allegato consentita per S/MIME	Automatico
Applicazione S/MIME	Tipi di crittografia consentiti per S/MIME	Entrambi
Applicazione S/MIME	Forza firma digitale per S/MIME	No
Applicazione S/MIME	Forza crittografia per messaggi S/MIME	No
Applicazione S/MIME	Lunghezza minima della chiave DH forte per S/MIME	1024 bit
Applicazione S/MIME	Lunghezza minima della chiave DSA forte per S/MIME	1024 bit
Applicazione S/MIME	Lunghezza minima della chiave ECC forte per S/MIME	163 bit
Applicazione S/MIME	Lunghezza minima della chiave RSA forte per S/MIME	1024 bit

Gruppo di criteri IT	Regola dei criteri IT	Valore predefinito
Applicazione S/MIME	Modalità S/MIME parti successive e invio	Manuale
VPN	Nome utente VPN	Valore nullo
VPN	Password utente VPN	Valore nullo
Wi-Fi	Disattiva Wi-Fi	No
Aggiornamenti software cablati	Consenti caricamento software basato su Web	No
Aggiornamenti software cablati	Backup servizi di crittografia	Sì
Aggiornamenti wireless del software	Vieta download patch su roaming WAN	No

Regole dei criteri IT

4

BlackBerry Enterprise Server Express include regole dei criteri IT, che possono essere configurate per soddisfare i requisiti di protezione dell'organizzazione e le esigenze degli utenti BlackBerry.

Gruppo criteri Solo dispositivo

Regola dei criteri IT Consenti messaggi peer-to-peer

Descrizione	Questa regola consente di specificare se un utente BlackBerry può inviare messaggi PIN. Questa regola non impedisce all'utente di ricevere messaggi PIN.
Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT Consenti messaggi di testo

Descrizione	Questa regola consente di specificare se un utente BlackBerry può inviare messaggi di testo. Questa regola non impedisce all'utente di ricevere messaggi SMS. Questa regola non impedisce all'utente di inviare e ricevere messaggi MMS. Per impedire all'utente di inviare e ricevere messaggi MMS, è possibile utilizzare la regola dei criteri IT Disattiva MMS.

Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Attiva timeout a lungo termine

Descrizione	Questa regola consente di specificare se il dispositivo BlackBerry deve bloccarsi dopo un periodo di tempo predefinito, indipendentemente dal fatto che l'utente BlackBerry stia utilizzando il dispositivo.
Regole collegate	La regola dei criteri IT Intervallo periodico influenza questa regola. Utilizzare la regola dei criteri IT Intervallo periodico per ridurre o ampliare l'intervallo di timeout.
Valori possibili	• Sì • No
Valori predefiniti	• No nel Criterio IT predefinito
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Abilita configurazione WAP

Descrizione	Questa regola consente di specificare se un utente BlackBerry può utilizzare il browser WAP su un dispositivo BlackBerry. Se il browser WAP viene disattivato e il provider dei servizi di rete dell'organizzazione utilizza il servizio WAP per la messaggistica MMS, non sarà possibile inviare e ricevere messaggi MMS.

Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP3

Regola dei criteri IT Giacenza max password

Descrizione	Questa regola consente di specificare il numero di giorni fino alla scadenza della password di un dispositivo BlackBerry, dopodiché il dispositivo BlackBerryrichiede all'utente di impostarne una nuova. Se si imposta questa regola su 0, la password del dispositivo non scadrà mai.
Regole dei criteri IT collegate	La regola dei criteri IT Password obbligatoria influenza questa regola. Un dispositivo utilizza questa regola solo se la regola dei criteri IT Password obbligatoria è configurata su Sì.
Valori possibili	• Da 0 a 65.535 giorni
Valori predefiniti	• 0 giorni nel criterio IT Predefinito
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Timeout di protezione massimo

Descrizione	Questa regola consente di specificare il tempo massimo che un utente BlackBerry può impostare come valore di timeout di protezione. Il valore di timeout di protezione rappresenta il numero di minuti di inattività al termine del quale il dispositivo BlackBerry viene bloccato.

Regole collegate	La regola dei criteri IT Password obbligatoria influisce su questa regola. Il dispositivo utilizza questa regola solo se la regola dei criteri IT Password obbligatoria è configurata su Sì. La regola dei criteri IT L'utente può modificare il timeout influisce su questa regola. Un utente può impostare qualsiasi valore di timeout inferiore rispetto a quello impostato dall'amministratore, a meno che la regola dei criteri IT L'utente può modificare il timeout non sia impostata su No.
Valori possibili	• Da 10 a 480 minuti
Valori predefiniti	• Valore null nel criterio IT Predefinito
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Lunghezza minima della password

Descrizione	Questa regola consente di specificare il numero minimo di caratteri richiesti per la password di un dispositivo BlackBerry. Questa regola non controlla il numero massimo di caratteri per la password. Il numero massimo è 32 caratteri.
Regole collegate	La regola dei criteri IT Password obbligatoria influisce su questa regola. Un dispositivo utilizza questa regola solo se la regola dei criteri IT Password obbligatoria è configurata su Sì.
Valori possibili	• Da 4 a 14 caratteri
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT Modelli password

Descrizione	Questa regola consente di verificare se i caratteri della password di un dispositivo BlackBerry soddisfano i requisiti di specifici modelli preimpostati. Per impostazione predefinita, un dispositivo impedisce ad un utente BlackBerry di configurare una password che utilizza una sequenza naturale di caratteri o di numeri. Il dispositivo accetterà invece la password se viene inserito un simbolo all'interno di una sequenza naturale.
Regole collegate	La regola dei criteri IT Password obbligatoria influisce su questa regola. Il dispositivo utilizza questa regola solo se la regola dei criteri IT Password obbligatoria è configurata su Sì.
Valori possibili	• Almeno 1 carattere alfabetico e 1 numerico • Almeno 1 carattere alfabetico, 1 numerico e 1 speciale • Almeno 1 carattere alfabetico maiuscolo, 1 alfabetico minuscolo, 1 numerico e 1 speciale • Nessuna restrizione
Valori predefiniti	• Nessuna restrizione nel criterio IT Predefinito
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Password obbligatoria

Descrizione	Questa regola consente di specificare se un utente BlackBerry deve configurare una password su un dispositivo BlackBerry.
Valori possibili	• Sì • No
Valori predefiniti	• No nel Criterio IT predefinito
Requisiti minimi	• BlackBerry Device Software 3.6

Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: L'utente può modificare il timeout

Descrizione	Questa regola consente di specificare se un utente BlackBerry può sovrascrivere il valore di timeout di protezione.
Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: L'utente può disattivare la password

Descrizione	Questa regola consente di specificare se un utente BlackBerry può disattivare l'obbligo di una password di protezione per il dispositivo BlackBerry. Questa regola è obsoleta in BlackBerry Device Software 4.0 e versioni successive.
Regole collegate	La regola dei criteri IT Password obbligatoria influisce su questa regola. Un dispositivo utilizza questa regola solo se la regola dei criteri IT Password obbligatoria è configurata su Sì.
Valori possibili	• Sì • No
Valori predefiniti	• Sì nel criterio IT Predefinito
Requisiti minimi	• BlackBerry Device Software 3.6

Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Gruppo criteri Globale

Regola dei criteri IT: Consenti browser

Descrizione	Questa regola consente di specificare se rendere disponibile o meno BlackBerry Browser sul dispositivo BlackBerry. Questa regola non si applica agli altri browser.
Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Consenti telefono

Descrizione	Questa regola consente di specificare se il telefono è disponibile su un dispositivo BlackBerry.
Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 3.6

Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Gruppo criteri BlackBerry App World

Regole dei criteri IT: Attiva fatturazione provider di servizi wireless

Descrizione	Questa regola consente di specificare se un utente BlackBerry può acquistare applicazioni dallo storefront BlackBerry App World utilizzando il piano di acquisto per il provider di servizi wireless dell'organizzazione.
Esempio	Si deve gestire BlackBerry Enterprise Server Express presso un'agenzia immobiliare. Molti degli utenti BlackBerry dell'agenzia hanno notato diverse applicazioni sullo BlackBerry App Worldche potrebbero aiutarli nella ricerca di nuovi appartamenti. Si dispone dell'approvazione da parte del team di gestione a consentire che i dipendenti possano acquistare le applicazioni utilizzando il piano di acquisto del provider di servizi wireless dell'agenzia.
Valori possibili	• Sì • No
Valori predefiniti	• No
Requisiti minimi	• BlackBerry Device Software 4.5
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Gruppo criteri Bluetooth

Per ulteriori informazioni sulla protezione Bluetooth® sui dispositivi BlackBerry, consultare il documento *Panoramica delle caratteristiche tecniche - Protezione di BlackBerry Enterprise Solution* e *Protezione per i dispositivi BlackBerry con tecnologia wireless Bluetooth* .

Regola dei criteri IT Bluetooth

Descrizione	Questa regola consente di specificare se disattivare o meno il supporto per la tecnologia Bluetooth® su un dispositivo BlackBerry. Se la tecnologia Bluetooth è attivata quando un dispositivo BlackBerry riceve questa regola, l'utente deve reimpostare il dispositivo affinché la modifica venga implementata.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 3.8
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Disattiva bypass wireless

Descrizione	Questa regola consente di specificare se impedire di utilizzare il bypass wireless tramite la tecnologia Bluetooth® su un dispositivo BlackBerry.
Esempio	Molti dipendenti dispongono di computer con tecnologia Bluetooth. Bluetooth Tale tecnologia consente agli utenti di connettere i computer ai dispositivi che supportano Bluetooth tramite una connessione Bluetooth wireless. È possibile consentire agli utenti di sincronizzare i dispositivi BlackBerry Desktop Softwaretramite una connessione Bluetooth invece di utilizzare la rete del provider di servizi wireless dell'organizzazione. È, inoltre, possibile consentire alle connessioni Bluetooth di contribuire alla riduzione dell'utilizzo della rete wireless nell'ambiente dell'organizzazione.

Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 4.1
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP3

Gruppo criteri Browser

Le regole nel gruppo criteri Browser interessano tutte le configurazioni del browser sul dispositivo BlackBerry.

Regola dei criteri IT Disattiva JavaScript nel browser

Descrizione	Questa regola specifica se consentire o meno l'esecuzione del codice JavaScript su un dispositivo BlackBerry.
Esempio	Alcuni utenti BlackBerry riferiscono che BlackBerry Browser è lento durante l'esplorazione di siti Web specifici. I siti Web potrebbero utilizzare JavaScript, un linguaggio di scripting utilizzato per una vasta gamma di funzioni, incluse finestre a comparsa, la convalida dell'input utente o la creazione di un'interfaccia dinamica. È possibile utilizzare questa regola per evitare l'elaborazione di JavaScript da parte dei dispositivi. Questa regola disattiva la funzionalità JavaScript sui siti Web, ma potrebbe accelerare l'esplorazione.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.0

Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT per i Domini browser MDS

Descrizione	Questa regola consente di specificare un elenco di indirizzi Web che un dispositivo BlackBerry deve recuperare mediante BlackBerry Browser e BlackBerry MDS Connection Service. È necessario separare gli indirizzi Web con una virgola (,). Se si desidera consentire a BlackBerry Browser di recuperare i sottodomini di un indirizzo Web, far precedere il nome di dominio da un punto (.). Ad esempio, digitare ".esempio.com" per consentire a BlackBerry Browser di recuperare tutti i sottodomini di esempio.com (ad esempio mail.esempio.com, www.example.ca).
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2
Introduzione alla regola	• BlackBerry Enterprise Server Express per Microsoft Exchange 5.0 SP2 MR1 • BlackBerry Enterprise Server Express per IBM Lotus Domino 5.0 SP2

Gruppo criteri Fotocamera

Regola dei criteri IT: Disattiva fotocamera

Descrizione	Questa regola consente di specificare se attivare o meno la fotocamera su un dispositivo BlackBerry.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.2

Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Disattiva videocamera

Descrizione	Questa regola consente di specificare se attivare o meno la videocamera su un dispositivo BlackBerry.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.3
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Gruppo criteri comuni

Regola dei criteri IT Disattiva MMS

Descrizione	Questa regola consente di specificare se un utente BlackBerry può inviare e ricevere messaggi MMS. Per ulteriori informazioni, vedere *Panoramica delle caratteristiche tecniche - Protezione di BlackBerry Enterprise Solution* .
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.0.2

Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT Disattiva registrazione note vocali

Descrizione	Questa regola consente di specificare se l'applicazione di registrazione note vocali è disponibile su un dispositivo BlackBerry.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.3
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Gruppo criteri Messaggi di posta elettronica

Le regole nel gruppo criteri Messaggi e-mail controllano la riconciliazione wireless dei messaggi e la visualizzazione degli allegati.

Regola dei criteri IT: Conferma download immagini esterne

Descrizione	Questa regola consente di specificare se un dispositivo BlackBerry visualizza una finestra di dialogo di conferma quando un utente BlackBerry fa clic sul collegamento Scarica immagini in un messaggio e-mail in formato HTML. Il messaggio visualizzato nella finestra di dialogo di conferma informa gli utenti che potrebbero esporre i propri indirizzi e-mail in caso di download dell'immagine da Internet.
Valori possibili	• Sì

	• No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 5.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Disattiva download manuale di immagini esterne

Descrizione	Questa regola consente di specificare se l'utente BlackBerry può richiedere manualmente la visualizzazione di contenuti (ad esempio immagini) che fanno riferimento a URL incorporati nei messaggi e-mail.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.5
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Disattiva funzioni di inoltro e risposta a messaggi crittografati in formato nativo di Notes

Descrizione	Questa regola consente di specificare se impedire o meno a un utente BlackBerry di inoltrare e rispondere a messaggi e-mail crittografati di IBM Lotus Domino su un dispositivo BlackBerry. Per

	impostazione predefinita, gli utenti che dispongono di un dispositivo che supporta la lettura dei messaggi e-mail crittografati di IBM Lotus Domino possono inoltrare e rispondere ai messaggi crittografati ricevuti, decrittografati e decompressi sul dispositivo. BlackBerry Messaging Agent esegue la decrittografia dei messaggi e-mail prima che vengano inviati dal dispositivo al destinatario come testo normale. Per ulteriori informazioni relative alla lettura di messaggi e-mail crittografati di IBM Lotus Domino sui dispositivi, consultare il documento *Panoramica delle caratteristiche tecniche - Protezione di BlackBerry Enterprise Solution* .
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.2.1
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP3

Regola dei criteri IT Disattiva contenuti multimediali e-mail

Descrizione	Questa regola consente di specificare se un dispositivo BlackBerry può ricevere messaggi e-mail in formato RTF o HTML.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.5
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Dimensioni massime di singoli allegati nel formato nativo MFH

Descrizione	Questa regola consente di specificare la dimensione massima di un allegato che un utente BlackBerry può inviare da un dispositivo BlackBerry. Questa regola si applica agli allegati le cui dimensioni superano 60 KB. Se si imposta questa regola su 0, il dispositivo non può inviare alcun allegato più grande di 60 KB. Il dispositivo può inviare allegati più piccoli di 60 KB. Il dispositivo comprime gli allegati più piccoli di 60 KB e include gli allegati nel corpo del messaggio e-mail. Se si modifica il valore del campo Dimensioni massime caricamento allegati singoli (in KB) o il campo Dimensioni massime caricamento allegati su 0, il dispositivo non può caricare alcun allegato più grande di 60 KB.
Esempio	Molti utenti inviano ai propri collaboratori messaggi e-mail che includono allegati di grandi dimensioni e questo può influenzare le prestazioni di BlackBerry Enterprise Server Express. È possibile limitare la dimensione degli allegati del messaggio che gli utenti possono inviare dai dispositivi per consentire il controllo del traffico di rete.
Regole collegate	In BlackBerry Enterprise Server Express 5.0 SP1 o versione successiva, questa regola interagisce con il campo Dimensioni massime caricamento allegati singoli (in KB) in BlackBerry Administration Service. Se si configura questo campo, BlackBerry Enterprise Server Express invia i valori al dispositivo mediante i dati di configurazione. Il dispositivo non può inviare un allegato che supera la dimensione specificata nel campo.
Valori possibili	• Da 0 a 3.145.728 byte
Valore predefinito	• 3.145.728 byte
Requisiti minimi	• BlackBerry Device Software 4.2
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Dimensioni totali massime degli allegati nel formato nativo MFH

Descrizione	Questa regola consente di specificare la dimensione totale di tutti gli allegati standard che è possibile caricare da un dispositivo BlackBerry.
Esempio	Molti utenti BlackBerry inviano ai propri colleghi messaggi e-mail contenenti uno o più allegati di grandi dimensioni, il che può influire sulle prestazioni di BlackBerry Enterprise Server Express. Per aiutare a controllare il traffico di rete, è possibile limitare la dimensione totale degli allegati che gli utenti possono inviare dai loro dispositivi.
Valori possibili	• Da 0 a 5.242.880 byte
Valore predefinito	• 5.242.880 byte
Requisiti minimi	• BlackBerry Device Software 4.2
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Dimensioni massime di singoli allegati nel formato nativo MFH

Descrizione	Questa regola consente di specificare la dimensione massima di un allegato che un utente BlackBerry può inviare da un dispositivo BlackBerry. Impostare questa regola su 0 per impedire all'utente di scaricare gli allegati sul dispositivo.
Esempio	Molti utenti BlackBerry effettuano il download degli allegati dei messaggi sui propri dispositivi. Il personale IT si preoccupa dell'utilizzo delle risorse delle rete extra e dei rischio potenziale per la sicurezza causato dal download degli allegati, in quanto il mittente potrebbe non essere sempre un dipendente fidato. È possibile impedire agli utenti di effettuare il download degli allegati sui propri dispositivi. Gli allegati possono comunque essere aperti e visualizzati dagli utenti.
Valore possibile	• Da 0 a 1.048.576 KB

Valore predefinito	• 10.240 KB
Requisiti minimi	• BlackBerry Device Software 4.5
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Timeout password di crittografia nativa di Notes

Descrizione	Questa regola consente di specificare per quanto tempo al massimo un dispositivo BlackBerry potrà memorizzare le password .id di IBM Lotus Notes digitate dall'utente BlackBerry. Configurare questa regola su 0 per impedire al dispositivo di memorizzare la password digitata da un utente su un dispositivo.
Valori possibili	• Da 1 a 32.767 minuti
Valore predefinito	• -1
Requisiti minimi	• BlackBerry Device Software 4.3
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP3

Regola dei criteri IT: Richiede la crittografia nativa di Notes per i messaggi in uscita

Descrizione	Questa regola consente di specificare se un utente BlackBerry può inviare messaggi e-mail crittografati tramite la crittografia di IBM Lotus Notes. Se necessario, il dispositivo BlackBerry richiede all'utente le password di crittografia di IBM Lotus Notes. Un dispositivo non esegue la crittografia di IBM Lotus Notes, ma configura i messaggi e-mail inviati dal dispositivo per la crittografia di IBM Lotus Notes eseguita da BlackBerry Enterprise Server Express. Questa regola non viene applicata ai messaggi inviati da un dispositivo che utilizza servizi e-mail che non supportano la crittografia di IBM Lotus Notes.

Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 5.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP3

Gruppo criteri Password

Un dispositivo BlackBerry usa le regole dei criteri IT nel gruppo criteri Password solo se, nel gruppo di criteri Solo dispositivo, la regola dei criteri IT Password obbligatoria viene configurata su Sì. Per ulteriori informazioni sull'utilizzo delle password nei dispositivi BlackBerry, vedere *BlackBerry Enterprise Solution Protezione di BlackBerry Enterprise Solution*.

Regola dei criteri IT: Password vietate

Descrizione	Questa regola consente di specificare le password che non possono essere utilizzate da un utente BlackBerry. Separare la lista delle password con la virgola (,). Per impostazione predefinita, un dispositivo BlackBerry impedisce all'utente di configurare password che utilizzano una sequenza naturale di caratteri o di numeri. Il dispositivo impedisce automaticamente le sostituzioni delle lettere comuni. Ad esempio, se si include la parola "password" nell'elenco delle password vietate, gli utenti non possono utilizzare le parole "p@ssw0rd", "pa$zword", o "password123" sul dispositivo.
Regole collegate	La regola dei criteri IT Password obbligatoria influisce su questa regola. Il dispositivo utilizza questa regola solo se si imposta la regola dei criteri IT Password obbligatoria su Sì.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.1
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Cronologia massima password

Descrizione	Questa regola consente di specificare il numero massimo di password già utilizzate che vengono controllate da un dispositivo BlackBerry al momento di creare nuove password per impedire a un utente BlackBerry di riutilizzare password precedenti.
Regole collegate	La regola dei criteri IT Password obbligatoria influisce su questa regola. Il dispositivo utilizza questa regola solo se si imposta la regola dei criteri IT Password obbligatoria su Sì.
Esempio	Si supponga di aver notato che molti utenti riutilizzano password già utilizzate in precedenza quando viene richiesto di creare una nuova password per i loro dispositivi. In tal caso, è possibile forzare gli utenti a creare nuove password ogni volta che viene richiesto per aumentare la sicurezza delle password. Impostare questa regola su 15 per fare in modo che, quando un utente digita una nuova password, questa sia diversa dalle ultime 15 password specificate dall'utente.
Valori possibili	• Da 0 a 15 password
Valori predefiniti	• 0
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Intervallo periodico

Descrizione	Questa regola consente di specificare l'intervallo di timeout di protezione prima del quale un dispositivo BlackBerry si blocca e richiede all'utente BlackBerry di digitare la password. Questa impostazione non considera se il dispositivo è stato attivo durante questo intervallo.
Regole collegate	La regola dei criteri IT Password obbligatoria influisce su questa regola. Il dispositivo utilizza questa regola solo se si imposta la regola dei criteri IT Password obbligatoria su Sì. La regola dei criteri IT L'utente può modificare il timeout influisce su questa regola. Impostare la regola dei criteri IT L'utente può modificare il timeout su No per impedire agli utenti di modificare le impostazioni di timeout sul dispositivo.

	La regola dei criteri IT Attiva timeout a lungo termine influisce su questa regola. Per impostazione predefinita, se si imposta la regola dei criteri IT Attiva timeout a lungo termine su Sì, l'intervallo del timeout di protezione viene attivato e impostato su 60 minuti.
Valori possibili	• Da 1 a 1440 minuti
Valore predefinito	• 60 minuti
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Imposta numero massimo di tentativi password

Descrizione	Questa regola consente di specificare il numero di volte in cui un utente BlackBerry può tentare di immettere una password prima che un dispositivo BlackBerry elimini in modo permanente tutti i dati delle applicazioni.
Regole collegate	La regola dei criteri IT Password obbligatoria influisce su questa regola. Il dispositivo utilizza questa regola solo se si imposta la regola dei criteri IT Password obbligatoria su Sì.
Valori possibili	• Da 3 a 10
Valore predefinito	• 10
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Imposta Timeout password

Descrizione	Questa regola consente di specificare il tempo di inattività prima del quale un utente BlackBerry deve digitare la password per sbloccare un dispositivo BlackBerry. Questa regola definisce il valore predefinito per il timeout di protezione.
Regole collegate	La regola dei criteri IT L'utente può modificare il timeout influisce su questa regola. Se si imposta la regola dei criteri IT L'utente può modificare il timeout su No, il dispositivo utilizza il timeout di protezione configurato in questa regola.
Valori possibili	• Da 0 a 60 minuti
Valore predefinito	• 2 minuti per BlackBerry Device Software 4.6 e versioni precedenti • 30 minuti per BlackBerry Device Software 4.7 e versioni successive
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Annulla eco password

Descrizione	Questa regola consente di specificare se i caratteri digitati dall'utente BlackBerry nella finestra di dialogo Password vengono visualizzati sul dispositivo BlackBerry dopo un certo numero di immissioni errate della password.
Regole collegate	La regola dei criteri IT Password obbligatoria influisce su questa regola. Il dispositivo utilizza questa regola solo se è configurata una password sul dispositivo. Per richiedere una password, configurare la regola dei criteri IT Password obbligatoria su Sì. La regola dei criteri IT Imposta numero massimo di tentativi password influisce su questa regola. Per specificare il numero di volte in cui l'utente può digitare la password errata prima che i caratteri vengano visualizzati sulla schermata, configurare la regola dei criteri IT Imposta numero massimo di tentativi password.
Valori possibili	• Sì • No

Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Gruppo criteri Dispositivi personali

Regola dei criteri IT Disattiva Inoltro di contenuto di lavoro utilizzando canali personali

Descrizione	Questa regola consente di specificare se un utente BlackBerry può inviare i dati di lavoro ai contatti utilizzando risorse personali (ad esempio, messaggi di testo SMS, messaggi MMS o messaggi e-mail da account e-mail personali).
Regole collegate	La regola dei criteri IT Consenti la separazione di contenuto di lavoro influisce su questa regola. Un dispositivo BlackBerry utilizza solo questa regola se la regola dei criteri IT Consenti la separazione di contenuto di lavoro viene impostata su Sì.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry 6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP3

Regola dei criteri IT: Consenti la separazione di contenuto di lavoro

Descrizione	Questa regola consente di specificare se un dispositivo BlackBerry distingue tra dati di lavoro e dati personali e se solo le applicazioni autorizzate sul dispositivo possono accedere ai dati di lavoro. Se questa regola viene impostata su Sì e un utente BlackBerry tenta di eliminare i dati di configurazione desktop, il dispositivo richiede all'utente di eliminare i dati di lavoro in esso contenuti.
Esempio	L'organizzazione gestisce informazioni riservate che non possono essere condivise con fonti esterne. Tutti gli utenti BlackBerry dell'organizzazione dispongono di un'applicazione personalizzata sui propri dispositivi che può essere utilizzata per rilevare e condividere le informazioni sui clienti. È possibile utilizzare questa regola e la regola dei criteri di controllo applicazioni "L'accesso all'API dei dati aziendali è consentito?" per garantire all'applicazione personalizzata l'accesso al contenuto di lavoro e impedire a tutte le altre applicazioni di terzi sul dispositivo di accedere al contenuto di lavoro, come messaggi e-mail, informazioni sul contatto e informazioni del calendario.
Regole collegate	La regola dei criteri di controllo applicazioni "L'accesso all'API dei dati aziendali è consentito?" influenza questa regola. La regola dei criteri di controllo applicazioni "L'accesso all'API dei dati aziendali è consentito?" consente di specificare se un'applicazione di terzi o un'applicazione aggiuntiva sono autorizzate ad accedere ai dati di lavoro. Per consentire a questa regola di influire sulle applicazioni di terzi, è necessario impostare la regola dei criteri di controllo applicazioni "L'accesso all'API dei dati aziendali è consentito?" su Autorizzazione non concessa per l'applicazione di terzi.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry 6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP3

Regola dei criteri IT Richiedi risorse di lavoro per l'esecuzione delle attività

Descrizione	Questa regola consente di specificare se un dispositivo BlackBerry deve utilizzare le risorse di lavoro (ad esempio, account e-mail o calendari aziendali) quando un utente BlackBerry conduce le attività di lavoro (ad esempio, l'invio di un messaggio e-mail a un contatto di lavoro o la pianificazione di un appuntamento di lavoro).
Regole collegate	La regola dei criteri IT Consenti la separazione di contenuto di lavoro influisce su questa regola. Il dispositivo utilizza solo questa regola se la regola dei criteri IT Consenti la separazione di contenuto di lavoro viene impostata su Sì.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry 6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP3

Regola dei criteri IT Domini aziendali

Descrizione	Questa regola consente di specificare un elenco di risorse (ad esempio, nomi dominio, nomi server e domini e-mail) che un dispositivo BlackBerry identifica come risorse di lavoro. Se si elenca un dominio, tutti i sottodomini del dominio sono compresi automaticamente. Se si elencano più risorse, separare le risorse con una virgola (,), punto e virgola (;) o uno spazio. Ad esempio, se l'organizzazione dispone di più domini, digitare example.com, example.net, example.org. Se si imposta questa regola, il dispositivo avvisa l'utente BlackBerry quando un messaggio e-mail include un indirizzo e-mail che non appartiene a un dominio aziendale. Il dispositivo evidenzia in giallo gli indirizzi e-mail che non appartengono al dominio aziendale. Se l'utente tenta di inoltrare un messaggio e-mail di lavoro a un indirizzo e-mail che non appartiene al dominio aziendale o che include un indirizzo che non appartiene al dominio aziendale in una risposta, il dispositivo visualizza anche un messaggio di avviso.

Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry 6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP3

Gruppo criteri sincronizzazione PIM

Regola dei criteri IT: Disattiva tutte le sincronizzazioni wireless

Descrizione	Questa regola consente di attivare o meno la sincronizzazione wireless dei dati. Impostare questa regola su Sì per disattivare completamente la sincronizzazione wireless dei dati, con l'eccezione della risoluzione dei conflitti e-mail wireless. Questa regola impedisce di effettuare le seguenti operazioni: • Sincronizzazione wireless delle voci di contatto, voci del calendario, filtri e-mail, attività e memo • Sincronizzazione wireless di tutte le informazioni di registrazione • Backup wireless di dati, compresi i dati di configurazione per i dispositivi BlackBerry • Caricamenti wireless • Attivazione dei dispositivi tramite la rete wireless
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.0

Gruppo criteri applicazione PGP

Le regole dei criteri IT del gruppo criteri Applicazione PGP si applicano ai dispositivi BlackBerry che dispongono di PGP Support Package per smartphone BlackBerry. Per ulteriori informazioni sull'utilizzo di PGP Support Package per smartphone BlackBerry, consultare il documento *Panoramica delle caratteristiche tecniche di protezione di PGP Support Package per dispositivi BlackBerry* .

Regola dei criteri IT: Crittografie del contenuto consentite per PGP

Descrizione	Questa regola consente di specificare gli algoritmi di crittografia che un dispositivo BlackBerry può utilizzare per crittografare i messaggi protetti con PGP. Per mantenere la compatibilità con la maggior parte dei client PGP, utilizzare la crittografia Triple DES e CAST. Per impostazione predefinita, un dispositivo è progettato per crittografare i messaggi e-mail utilizzando la crittografia Triple DES quando non conosce i metodi di decrittografia a disposizione di un destinatario.
Esempio	L'organizzazione ha implementato la tecnologia PGP per proteggere i messaggi e-mail e altri dati elettronici inviati e ricevuti dai dipendenti. Si installa PGP Support Package per smartphone BlackBerry sui dispositivi per consentire agli utenti BlackBerry di inviare e ricevere messaggi e-mail e PIN protetti da PGP. L'organizzazione supporta esclusivamente l'uso degli standard AES e Triple DES, pertanto si utilizza questa regola per permettere ai dispositivi di utilizzare queste crittografie del contenuto solo per crittografare messaggi PGP.
Valori possibili	• AES (256 bit) • AES (192 bit) • AES (128 bit) • CAST (128 bit) • Triple DES
Requisiti minimi	• PGP Support Package per smartphone BlackBerry 4.1 • BlackBerry Device Software 4.1

Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT Modalità crittografia allegato consentita per PGP

Descrizione	Questa regola consente di specificare la modalità utilizzata per recuperare le informazioni degli allegati protette con PGP su un dispositivo BlackBerry.
Esempio	Gli standard di protezione dell'organizzazione indicano che gli utenti dovrebbero aprire gli allegati dei messaggi crittografati con PGP sui computer solo in un ambiente di lavoro altamente protetto. È possibile utilizzare questa regola per impedire agli utenti di recuperare gli allegati crittografati con PGP sui loro dispositivi.
Valori possibili	• Nessuno • Manuale • Automatico
Valore predefinito	• Automatico
Requisiti minimi	• BlackBerry Device Software 4.5
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Tipi di crittografia consentiti per PGP

Descrizione	Questa regola consente di specificare i tipi di crittografia che un dispositivo BlackBerry può utilizzare per i messaggi protetti con PGP.
Esempio	L'organizzazione gestisce informazioni che richiedono un livello di protezione elevato. È possibile utilizzare questa regola per supportare la crittografia PGP e quella convenzionale per i messaggi e-mail inviati e ricevuti sui dispositivi.

Valori possibili	• Solo basato su chiave PGP • Solo convenzionale • Entrambi
Valore predefinito	• Entrambi
Requisiti minimi	• PGP Support Package per smartphone BlackBerry 4.0 • BlackBerry Device Software 4.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Forza firma digitale per PGP

Descrizione	Questa regola consente di specificare se un dispositivo BlackBerry inserisce la firma digitale in tutti i messaggi protetti con PGP inviati. Se viene applicata questa regola, è possibile sovrascrivere le impostazioni del criterio di protezione e-mail sul PGP Universal Server.
Esempio	L'organizzazione ha implementato la tecnologia PGP per proteggere i messaggi e-mail e altri dati elettronici inviati e ricevuti dai dipendenti. Si installa PGP Support Package per smartphone BlackBerry sui dispositivi per consentire agli utenti BlackBerry di inviare e ricevere messaggi e-mail e PIN protetti da PGP. Gli standard di protezione dell'organizzazione richiedono l'aggiunta di una firma digitale a tutti i messaggi e-mail. Una firma digitale consente di verificare che il messaggio è stato inviato dall'utente corretto. È possibile utilizzare questa regola per aggiungere firme digitali a tutti i messaggi PGP inviati dai dispositivi.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• PGP Support Package per smartphone BlackBerry 4.1 • BlackBerry Device Software 4.1

Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Forza crittografia per messaggi PGP

Descrizione	Questa regola consente di specificare se un dispositivo BlackBerry esegue la crittografia di tutti i messaggi protetti con PGP inviati. Se viene applicata questa regola, è possibile sovrascrivere le impostazioni del criterio di protezione e-mail sul PGP Universal Server.
Esempio	L'organizzazione ha implementato la tecnologia PGP per proteggere i messaggi e-mail e altri dati elettronici inviati e ricevuti dai dipendenti. Si installa PGP Support Package per smartphone BlackBerry sui dispositivi per consentire agli utenti BlackBerry di inviare e ricevere messaggi e-mail e PIN protetti da PGP. Per soddisfare i requisiti stabiliti dall'organizzazione in materia di protezione delle comunicazioni mobili, è possibile utilizzare questa regola per fare in modo che i dispositivi eseguano la crittografia di tutti i messaggi e-mail inoltrati o inviati come risposta mediante la crittografia PGP.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• PGP Support Package per smartphone BlackBerry 4.1 • BlackBerry Device Software 4.1
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Lunghezza minima della chiave DH forte per PGP

Descrizione	Questa regola consente di specificare la dimensione minima della chiave Diffie-Hellman da utilizzare con i messaggi protetti con PGP.

Esempio	I dispositivi BlackBerry utilizzano chiavi pubbliche PGP e chiavi private PGP per crittografare e decrittografare i messaggi e-mail. Le chiavi PGP possono utilizzare l'algoritmo DH per la crittografia e la decrittografia. La lunghezza della chiave in bit è un fattore importante che incide sull'efficacia della chiave. L'organizzazione supporta la lunghezza minima della chiave di 512 bit per le chiavi che utilizzano l'algoritmo DH, pertanto si imposta questa regola su 512 bit per permettere ai dispositivi di supportare chiavi PGP di lunghezza uguale o superiore a tale valore.
Valori possibili	• Da 512 a 4096 bit
Valore predefinito	• 1024 bit
Requisiti minimi	• PGP Support Package per smartphone BlackBerry 4.1 • BlackBerry Device Software 4.1
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Lunghezza minima della chiave DSA forte per PGP

Descrizione	Questa regola consente di specificare la dimensione minima della chiave DSA da utilizzare con i messaggi protetti con PGP. L'intervallo consentito va da 512 a 1024 bit.
Esempio	I dispositivi BlackBerry utilizzano chiavi pubbliche PGP e chiavi private PGP per crittografare e decrittografare i messaggi e-mail. Le chiavi PGP possono utilizzare l'algoritmo DSA per la crittografia e la decrittografia. La lunghezza della chiave in bit è un fattore importante che incide sull'efficacia della chiave. L'organizzazione supporta la lunghezza minima della chiave di 512 bit per le chiavi che utilizzano l'algoritmo DSA, pertanto si imposta questa regola su 512 bit per permettere ai dispositivi di supportare chiavi PGP di lunghezza uguale o superiore a tale valore.
Valori possibili	• Da 512 a 1024 bit
Valore predefinito	• 1024 bit
Requisiti minimi	• PGP Support Package per smartphone BlackBerry 4.1 • BlackBerry Device Software 4.1

Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Lunghezza minima della chiave RSA forte per PGP

Descrizione	Questa regola consente di specificare la dimensione minima della chiave RSA da utilizzare con i messaggi protetti con PGP.
Esempio	I dispositivi BlackBerry utilizzano chiavi pubbliche PGP e chiavi private PGP per crittografare e decrittografare i messaggi e-mail. Le chiavi PGP possono utilizzare l'algoritmo RSA per la crittografia e la decrittografia. La lunghezza della chiave in bit è un fattore importante che incide sull'efficacia della chiave. L'organizzazione supporta la lunghezza minima della chiave di 512 bit per le chiavi che utilizzano l'algoritmo RSA, pertanto si imposta questa regola su 512 bit per permettere ai dispositivi di supportare chiavi PGP di lunghezza uguale o superiore a tale valore.
Valori possibili	• Da 512 a 4096 bit
Valore predefinito	• 1024 bit
Requisiti minimi	• PGP Support Package per smartphone BlackBerry 4.1 • BlackBerry Device Software 4.1
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Modalità PGP parti successive e invio

Descrizione	Questa regola consente di specificare la modalità utilizzata da un dispositivo BlackBerry per recuperare il testo completo di un messaggio e-mail quando un utente BlackBerry inoltra o risponde a un messaggio e-mail.
Esempio	Per impostazione predefinita, l'utente BlackBerry deve richiedere il testo completo dei messaggi e-mail per l'inoltro o la risposta come messaggi PGP dal proprio dispositivo. È possibile utilizzare questa

	regola per consentire ai dispositivi di recuperare e visualizzare automaticamente il testo completo dei messaggi e-mail per consentire la risposta o l'inoltro come messaggi PGP.
Valori possibili	• Automatico • Manuale • Nessuna
Valore predefinito	• Manuale
Requisiti minimi	• BlackBerry Device Software 5.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Metodo di registrazione al PGP

Descrizione	Questa regola specifica il metodo utilizzato da un utente BlackBerry per effettuare la registrazione al PGP Universal Server su un dispositivo BlackBerry. L'utente deve fornire le informazioni di registrazione al PGP Universal Server prima di poter inviare e ricevere i messaggi PGP protetti sul dispositivo.
Esempio	Per supportare la crittografia PGP con PGP Universal Server, gli utenti BlackBerry devono effettuare l'iscrizione dei propri dispositivi con PGP Universal Server dell'organizzazione. Per impostazione predefinita, l'iscrizione dei dispositivi con PGP Universal Server viene effettuata tramite e-mail. Per soddisfare i requisiti di protezione dell'organizzazione, è possibile utilizzare questa regola per applicare un metodo alternativo che richieda agli utenti di specificare il nome utente e la password di dominio per l'iscrizione dei dispositivi.
Valori possibili	• Iscrizione con nome utente/password dominio • Iscrizione basata su e-mail
Valore predefinito	• Iscrizione basata su e-mail
Requisiti minimi	• PGP Support Package per smartphone BlackBerry 4.1 • BlackBerry Device Software 4.1

Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Timeout cache criteri di PGP Universal

Descrizione	Questa regola consente di specificare per quanto tempo un dispositivo BlackBerry memorizza gli indirizzi del PGP Universal Server nella cache.
Esempio	I dispositivi BlackBerry recuperano il criterio e-mail di PGP Universal Server per determinare se firmare, crittografare o firmare e crittografare i messaggi e-mail. Se il criterio e-mail non viene cambiato frequentemente, è possibile impostare questa regola in modo da consentire ai dispositivi di recuperare il criterio e-mail di PGP Universal Server ogni 48 ore.
Valori possibili	• Da 4 a 48 ore
Valore predefinito	• 24 ore
Requisiti minimi	• PGP Support Package per smartphone BlackBerry 4.1 • BlackBerry Device Software 4.1
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Indirizzo del PGP Universal Server

Descrizione	Questa regola consente di specificare l'indirizzo del PGP Universal Server della propria organizzazione. Il PGP Universal Server applica i criteri di protezione e-mail configurati dall'amministratore del PGP Universal Server. Configurare questa regola per richiedere all'utente BlackBerry di effettuare la registrazione sul PGP Universal Server. Un dispositivo BlackBerry registrato su PGP Support Package per smartphone BlackBerry assicura la conformità ai criteri di protezione e-mail di tutti i messaggi e-mail.
Valore predefinito	• Valore null

Requisiti minimi	• PGP Support Package per smartphone BlackBerry 4.1 • BlackBerry Device Software 4.1
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Gruppo criteri Applicazioni RIM a valore aggiunto

Regola dei criteri IT Disabilita l'accesso ai dati dell'agenda elettronica per le applicazioni di social networking

Descrizione	Questa regola consente di specificare se un dispositivo BlackBerry deve impedire alle applicazioni di social networking di accedere ai dati dell'agenda elettronica.
Esempio	Il personale addetto all'assistenza di un'università utilizza Facebook per smartphone BlackBerry per condividere informazioni sui corsi, sulla pianificazione delle esercitazioni e sui contatti di assistenza. È possibile consentire alle applicazioni di social networking di accedere alle informazioni del calendario e dei contatti sui dispositivi per far sì che il personale addetto all'assistenza possa condividere tali informazioni con gli studenti che utilizzano l'applicazione.
Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 4.2.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP3

Gruppo criteri di protezione

Regola dei criteri IT: Consenti connessioni esterne

Descrizione	Questa regola consente di specificare se le applicazioni, comprese quelle di terzi, possono instaurare connessioni esterne (ad esempio, ad un gateway WAP).
Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT Consenti la reimpostazione del timer di inattività

Descrizione	Questa regola consente di specificare se un dispositivo BlackBerry consente ad applicazioni di terzi di riconfigurare il valore di timeout inattività su un dispositivo e di ignorare il valore di timeout per la password del dispositivo. Per ulteriori informazioni sul timeout inattività, visitare il sito www.blackberry.com/go/apiref e consultare la classe EventInjector e il metodo Backlight.enable() nella documentazione di riferimento sulle API per BlackBerry Java Development Environment.
Valori possibili	• Sì • No

Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.2.1
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Consenti connessioni Split-Pipe

Descrizione	Questa regola consente di specificare se le applicazioni, comprese quelle di terzi, possono stabilire contemporaneamente connessioni interne ed esterne su un dispositivo BlackBerry. Un'applicazione potrebbe costituire una minaccia alla protezione se stabilisce contemporaneamente connessioni interne ed esterne in quanto potrebbe raccogliere dati all'interno del firewall e inviarli al di fuori di esso.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Consenti l'utilizzo della porta seriale alle applicazioni di terzi

Descrizione	Questa regola consente di specificare se le applicazioni di terzi possono utilizzare la porta seriale, la porta IrDA o la porta USB del dispositivo BlackBerry.
Esempio	Gli utenti BlackBerry all'interno dell'organizzazione utilizzano un'applicazione personalizzata che consente loro di caricare nei propri computer i dati dei clienti, raccolti durante le visite in loco. L'applicazione richiede l'utilizzo della porta USB sui dispositivi per la connessione ai computer. È

	possibile utilizzare questa regola per consentire all'applicazione di utilizzare la porta di USB sui dispositivi.
Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT Livello di protezione del contenuto

Descrizione	Questa regola consente di specificare il livello di crittografia utilizzato da un dispositivo BlackBerry per la protezione del contenuto dei dati ricevuti quando è bloccato. Quando viene specificato un valore per questa regola, la protezione del contenuto viene attivata. Se questa regola viene impostata su Forte, il dispositivo utilizza una chiave pubblica ECC a 160 bit. Se questa regola viene impostata su Più forte, il dispositivo utilizza una chiave pubblica ECC a 283 bit. Se questa regola viene impostata su Massima, il dispositivo utilizza una chiave pubblica ECC a 571 bit. Per i dispositivi con BlackBerry Device Software 5.0 e versioni successive con memoria del dispositivo integrata, questa regola applica la crittografa anche a tale memoria con la password utente e la chiave generata dal dispositivo BlackBerry. I file multimediali nella memoria del dispositivo integrata non sono crittografati se non si imposta la regola dei criteri IT Applica crittografia ai file multimediali sulla memoria su scheda del dispositivo. Per i dispositivi con BlackBerry Device Software 4.7 e versioni precedenti, è possibile configurare la regola dei criteri IT Livello di crittografia file system esterno per crittografare i file multimediali presenti nella scheda di memoria.
Regole collegate	La regola dei criteri IT Password obbligatoria influisce su questa regola. Il dispositivo utilizza questa regola solo se la regola dei criteri IT Password obbligatoria è impostata su Sì. Questa regola influenza la regola dei criteri IT Lunghezza minima della password. Se questa regola viene impostata su Più forte, è necessario impostare la regola dei criteri IT Lunghezza minima della password su 12 caratteri. Se questa regola viene impostata su Massima, è necessario impostare la regola dei criteri IT Lunghezza minima della password su 21 caratteri.

Valori possibili	• Forte • Più forte • Massima
Valori predefiniti	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Disattiva 3DES Transport Crypto

Descrizione	Questa regola consente di impedire a un dispositivo BlackBerry di utilizzare l'algoritmo Triple DES per crittografare e decrittografare i dati.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Disattiva memoria esterna

Descrizione	Questa regola consente di specificare se impedire o meno a un utente BlackBerry di accedere alla scheda di memoria su un dispositivo BlackBerry.
Valori possibili	• Sì • No

Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.2
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Disattiva GPS

Descrizione	Questa regola consente di specificare se attivare o meno la funzionalità GPS su un dispositivo BlackBerry. Se questa regola viene impostata su Sì, BlackBerry Maps non sarà in grado di funzionare e le applicazioni non potranno accedere alle API GPS del dispositivo
Regole collegate	Questa regola influenza l'impostazione L'accesso all'API GPS è consentito? della regola dei criteri di controllo applicazioni. Questa regola sovrascrive l'impostazione L'accesso all'API GPS è consentito? della regola dei criteri di controllo applicazioni.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.3
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Disattiva modem IP

Descrizione	Questa regola consente di specificare se rendere disponibile il modem IP su un dispositivo BlackBerry.
Valori possibili	• Sì • No

Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT Disattiva memorizzazione di massa USB

Descrizione	Questa regola consente di attivare o meno la memorizzazione di massa USB e il protocollo di trasporto multimediale. Il protocollo di trasporto multimediale consente a un utente BlackBerry di trasferire file multimediali da un computer o da BlackBerry Desktop Manager a un dispositivo BlackBerry o una scheda di memoria. Quando si trasferiscono file tramite il protocollo di trasporto multimediale, il dispositivo non applica la protezione del contenuto ai file e non crittografa i dati sulla scheda di memoria, anche se è stata configurata la regola dei criteri IT Livello di crittografia file system esterno. Questa funzione non è disponibile per BlackBerry Desktop Manager 4.2.2 poiché Roxio Media Manager utilizza il protocollo di trasporto multimediale per trasferire i file. Per ulteriori informazioni sulla protezione dei dati memorizzati su una scheda di memoria in un dispositivo, consultare *Panoramica delle caratteristiche tecniche - Protezione di BlackBerry Enterprise Solution* .
Valori possibili	• Sì • No
Valori predefiniti	• Sì nel criterio IT Predefinito.
Requisiti minimi	• BlackBerry Device Software 4.2
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT Vieta download di applicazioni di terzi

Descrizione	Questa regola consente di specificare se un utente BlackBerry può installare o aggiornare le applicazioni su un dispositivo BlackBerry utilizzando BlackBerry Browser o BlackBerry App World. Se questa regola viene impostata su Sì, l'utente non può installare o aggiornare le applicazioni sul dispositivo utilizzando BlackBerry Browser o BlackBerry App World. L'utente può installare o aggiornare un'applicazione che Research In Motion crea utilizzando BlackBerry Desktop Software. Questa regola non è applicabile alle applicazioni aggiuntive RIM nelle configurazioni software. Se si imposta questa regola su Sì, BlackBerry Administration Service impedisce di utilizzare una configurazione software per installare applicazioni di terzi firmate digitalmente con chiavi di firma codice sul dispositivo. Una volta applicata questa regola, qualunque applicazione di terzi firmata viene rimossa dal dispositivo e non può essere reinstallata dall'utente.
Regole collegate	Questa regola influenza la regola dei criteri IT Regola limitazioni applicazioni. Se questa regola viene impostata su Sì, questa regola ha priorità sulla regola dei criteri IT Regola limitazioni applicazioni. Questa regola influenza la regola dei criteri IT Regola limitazioni categorie. Se questa regola viene impostata su Sì, questa regola ha priorità sulla regola dei criteri IT Regola limitazioni categorie. Questa regola è interessata dalla regola dei criteri IT Metodi di installazione delle applicazioni. Se specifici metodi di applicazione vengono vietati tramite la regola Metodi di installazione delle applicazioni, tale regola ha la precedenza su BlackBerry 7.1 e dispositivi successivi.
Valori possibili	• Sì • No
Valori predefiniti	• No nel criterio IT Predefinito
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Applica crittografia ai file multimediali sulla memoria su scheda del dispositivo

Descrizione	Questa regola consente di specificare se i file multimediali presenti nella scheda di memoria di un dispositivo BlackBerry sono crittografati con la password e la chiave generata dall'utente BlackBerry.
Regole collegate	La regola dei criteri IT Livello di protezione del contenuto influisce su questa regola. Il dispositivo utilizza questa regola dei criteri IT solo se viene configurata anche la regola dei criteri IT Livello di protezione del contenuto.
Valori possibili	• Autorizzazione concessa • Indispensabile • Autorizzazione non concessa
Valore predefinito	• Autorizzazione concessa
Requisiti minimi	• BlackBerry Device Software 5.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Livello di crittografia file system esterno

Descrizione	Questa regola consente di specificare il livello di crittografia utilizzato da un dispositivo BlackBerry per crittografare file archiviati su una scheda di memoria. È possibile utilizzare questa regola per richiedere al dispositivo di crittografare una scheda di memoria, includendo o meno i file memorizzati nella scheda di memoria. Non è possibile utilizzare questa regola per crittografare i file che un utente BlackBerry trasferisce manualmente nella scheda di memoria (ad esempio, da un dispositivo di memorizzazione di massa USB). Le chiavi master per la scheda di memoria sono archiviate nella scheda di memoria. Il dispositivo è progettato per utilizzare le chiavi master per decrittografare e crittografare file nella scheda di memoria. Il dispositivo crittografa le chiavi master utilizzando la propria chiave principale, una password inserita dall'utente o entrambe.

Valori possibili	• Crittografa con la password dell'utente (directory multimediali escluse) • Crittografa con la password dell'utente (directory multimediali incluse) • Crittografa con la chiave del dispositivo (directory multimediali escluse) • Crittografa con la chiave del dispositivo (directory multimediali incluse) • Crittografa con password dell'utente e chiave del dispositivo (directory multimediali escluse) • Crittografa con password dell'utente e chiave del dispositivo (directory multimediali incluse) • Non richiesto
Valori predefiniti	• Non richiesto
Requisiti minimi	• BlackBerry Device Software 4.2
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Forza blocco nella custodia

Descrizione	Questa regola consente di specificare se un dispositivo BlackBerry deve bloccarsi quando l'utente BlackBerry lo inserisce in una custodia.
Valori possibili	• Sì • No
Valori predefiniti	• No nel criterio IT Predefinito
Requisiti minimi	• BlackBerry Device Software 3.6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Modello password obbligatorio

Descrizione	Questa regola consente di specificare il formato richiesto per una password del dispositivo BlackBerry. Un carattere nel modello di password ne specifica il tipo e la posizione consentiti. Le password

	possono contenere soltanto caratteri nella codifica Latin-1. Se questa regola viene configurata, l'utente può impostare una password di lunghezza maggiore o uguale rispetto a quella del modello di un dispositivo BlackBerry. I caratteri della password che superano la lunghezza del formato possono essere lettere, numeri o simboli di qualsiasi tipo. È possibile utilizzare i seguenti caratteri per specificare il formato della password: • a: consente qualsiasi lettera • A: consente solo una lettera maiuscola • c: consente qualsiasi consonante • C: consente solo una consonante maiuscola • v: consente qualsiasi vocale • V: consente solo una vocale maiuscola • N, n o #: consente solo un numero • S, s o @: consente solo un simbolo • ?: consente qualsiasi lettera, numero o simbolo
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Reimposta valori predefiniti durante pulizia della memoria

Descrizione	Questa regola consente di specificare se ripristinare o meno i valori predefiniti del dispositivo BlackBerry quando quest'ultimo riceve il comando di amministrazione IT Elimina tutti i dati e disattiva dispositivo tramite la rete wireless. Per i dispositivi con BlackBerry Device Software e versioni successive, questa regola viene applicata in modalità remota (quando un amministratore cancella i dati su un dispositivo in modalità remota) e in locale (ad esempio, quando l'utente BlackBerry supera i tentativi massimi di immissione della password o cancella tutti i dati sul dispositivo). Per i dispositivi con BlackBerry Device Software 4.7 e versioni precedenti, questa regola viene applicata solo quando un amministratore cancella i dati in modalità remota.

Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.2.2
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Convertitore di sicurezza hash file .cod

Descrizione	Questa regola consente di specificare gli hash per i file. cod di un convertitore richiesto da un dispositivo BlackBerry per registrare il convertitore. Impostare ogni hash nel formato esadecimale e separare più valori con una virgola (,).
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.5
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP3

Gruppo criteri applicazione S/MIME

Le regole dei criteri IT del gruppo criteri Applicazione S/MIME si applicano ai dispositivi BlackBerry che dispongono di S/MIME Support Package per smartphone BlackBerry. Per ulteriori informazioni sull'utilizzo di S/MIME Support Package per smartphone BlackBerry, consultare il documento *Panoramica delle caratteristiche tecniche di protezione di S/MIME Support Package per i dispositivi BlackBerry* .

Regola dei criteri IT: Indirizzo e-mail EMS (Entrust Messaging Server)

Descrizione	Questa regola consente di specificare l'indirizzo e-mail del server di messaggistica Entrust Entelligence Messaging Server utilizzato dalla propria organizzazione.
Esempio	L'organizzazione utilizza un Entrust Entelligence Messaging Server per proteggere i messaggi e-mail inviati dai propri dipendenti. È possibile utilizzare questa regola per consentire ai dispositivi BlackBerry di comunicare con l'EMS e supportare la funzionalità EMS integrata nei dispositivi.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.0 • S/MIME Support Package per smartphone BlackBerry 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Crittografie del contenuto consentite per S/MIME

Descrizione	Questa regola consente di specificare gli algoritmi di crittografia che un dispositivo BlackBerry può utilizzare per crittografare i messaggi e-mail con protezione S/MIME. Per mantenere la compatibilità con la maggior parte dei client S/MIME, utilizzare l'algoritmo Triple DES e uno degli RC2. Per impostazione predefinita, il dispositivo è progettato per crittografare i messaggi e-mail tramite l'algoritmo Triple DES quando non conosce i metodi di decrittografia a disposizione del destinatario.
Esempio	Si installa S/MIME Support Package per smartphone BlackBerry sui dispositivi per permettere agli utenti di inviare e ricevere messaggi e-mail e PIN firmati con S/MIME e firmati e crittografati con S/MIME. L'organizzazione supporta esclusivamente l'utilizzo della crittografia AES e Triple DES, pertanto si utilizza questa regola per permettere ai dispositivi di utilizzare queste crittografie del contenuto solo per crittografare messaggi S/MIME.

Valori possibili	• AES (256 bit) • AES (192 bit) • AES (128 bit) • CAST (128 bit) • RC2 (128 bit) • Triple DES • RC2 (64 bit) • RC2 (40 bit)
Valore predefinito	• AES (256 bit), AES (192 bit), AES (128 bit), CAST (128 bit), RC2 (128 bit) e Triple DES
Requisiti minimi	• BlackBerry Device Software 3.6 • S/MIME Support Package per smartphone BlackBerry 1.5
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Modalità crittografia allegato consentita per S/MIME

Descrizione	Questa regola consente di specificare la modalità utilizzata per recuperare le informazioni degli allegati protette con S/MIME su un dispositivo BlackBerry.
Esempio	Gli standard di protezione dell'organizzazione indicano che gli utenti BlackBerry dovrebbero aprire gli allegati dei messaggi crittografati con S/MIME sui computer solo in un ambiente di lavoro altamente protetto. È possibile utilizzare questa regola per impedire agli utenti di recuperare gli allegati crittografati con S/MIME sui loro dispositivi.
Valori possibili	• Automatico • Manuale • Nessuno
Valore predefinito	• Automatico

Requisiti minimi	• BlackBerry Device Software 4.5
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Tipi di crittografia consentiti per S/MIME

Descrizione	Questa regola consente di specificare i tipi di crittografia che un dispositivo BlackBerry può utilizzare con i messaggi e-mail con protezione S/MIME.
Esempio	Alcuni utenti dell'organizzazione stanno pianificando un progetto riservato e desiderano proteggere i propri messaggi e-mail. Si installa S/MIME Support Package per smartphone BlackBerry sui dispositivi per permettere agli utenti BlackBerry di inviare e ricevere messaggi e-mail e PIN firmati con S/MIME e firmati e crittografati con S/MIME. È possibile configurare questa regola dei criteri IT in modo che sia obbligatorio utilizzare una password condivisa per crittografare e decrittografare i messaggi e-mail.
Valori possibili	• Crittografia basata su certificato • Crittografia basata su password • Entrambi
Valore predefinito	• Entrambi
Requisiti minimi	• BlackBerry Device Software 4.6 • S/MIME Support Package per smartphone BlackBerry 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Forza firma digitale per S/MIME

Descrizione	Questa regola consente di specificare se un dispositivo BlackBerry invia tutti i messaggi e-mail con protezione S/MIME con una firma digitale.

Esempio	Sui dispositivi, viene installato S/MIME Support Package per smartphone BlackBerry in modo da consentire agli utenti di inviare e ricevere messaggi e-mail e PIN firmati con S/MIME e firmati e crittografati con S/MIME. Gli standard di protezione dell'organizzazione richiedono l'aggiunta di una firma digitale a tutti i messaggi e-mail. Una firma digitale consente di verificare che il messaggio è stato inviato dall'utente corretto. È possibile utilizzare questa regola per aggiungere firme digitali a tutti i messaggi S/MIME inviati dai dispositivi.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 3.6 • S/MIME Support Package per smartphone BlackBerry 1.5
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Forza crittografia per messaggi S/MIME

Descrizione	Questa regola consente di specificare se un dispositivo BlackBerry crittografa tutti i messaggi e-mail che un utente BlackBerry invia tramite la crittografia S/MIME.
Esempio	Si installa S/MIME Support Package per smartphone BlackBerry sui dispositivi per permettere agli utenti di inviare e ricevere messaggi e-mail e PIN firmati con S/MIME e firmati e crittografati con S/MIME. Per soddisfare i requisiti stabiliti dall'organizzazione in materia di protezione delle comunicazioni mobili, è possibile utilizzare questa regola per fare in modo che i dispositivi eseguano la crittografia di tutti i messaggi e-mail inoltrati o inviati come risposta mediante la crittografia S/MIME.
Valori possibili	• Sì • No
Valore predefinito	• No

Requisiti minimi	• BlackBerry Device Software 3.6 • S/MIME Support Package per smartphone BlackBerry 1.5
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Lunghezza minima della chiave DH forte per S/MIME

Descrizione	Questa regola consente di specificare la dimensione minima della chiave Diffie-Hellman da utilizzare con i messaggi protetti con S/MIME.
Esempio	I dispositivi BlackBerry utilizzano chiavi pubbliche S/MIME e chiavi private S/MIME per crittografare e decrittografare i messaggi e-mail. Le chiavi S/MIME possono utilizzare l'algoritmo DH per la crittografia e la decrittografia. La lunghezza della chiave in bit è un fattore che incide sull'efficacia della chiave. L'organizzazione supporta la lunghezza minima della chiave di 512 bit per le chiavi che utilizzano l'algoritmo DH, pertanto si imposta questa regola su 512 bit per permettere ai dispositivi di supportare chiavi S/MIME di lunghezza uguale o superiore a tale valore.
Valori possibili	• Da 512 a 4096 bit
Valore predefinito	• 1024 bit
Requisiti minimi	• BlackBerry Device Software 3.6 • S/MIME Support Package per smartphone BlackBerry 1.5
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Lunghezza minima della chiave DSA forte per S/MIME

Descrizione	Questa regola consente di specificare la dimensione minima della chiave DSA utilizzata da un dispositivo BlackBerry con i messaggi e-mail con protezione S/MIME.

Esempio	I dispositivi BlackBerry utilizzano chiavi pubbliche S/MIME e chiavi private S/MIME per crittografare e decrittografare i messaggi e-mail. Le chiavi S/MIME possono utilizzare l'algoritmo DSA per la crittografia e la decrittografia. La lunghezza della chiave in bit è un fattore che incide sull'efficacia della chiave. L'organizzazione supporta la lunghezza minima della chiave di 512 bit per le chiavi che utilizzano l'algoritmo DSA, pertanto si imposta questa regola su 512 bit per permettere ai dispositivi di supportare chiavi S/MIME di lunghezza uguale o superiore a tale valore.
Valori possibili	• Da 512 a 1024 bit
Valore predefinito	• 1024 bit
Requisiti minimi	• BlackBerry Device Software 3.6 • S/MIME Support Package per smartphone BlackBerry 1.5
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Lunghezza minima della chiave ECC forte per S/MIME

Descrizione	Questa regola consente di specificare la dimensione minima della chiave ECC utilizzata da un dispositivo BlackBerry con i messaggi e-mail con protezione S/MIME.
Esempio	I dispositivi BlackBerry utilizzano chiavi pubbliche S/MIME e chiavi private S/MIME per crittografare e decrittografare i messaggi e-mail. Le chiavi S/MIME possono utilizzare l'algoritmo ECC per la crittografia e la decrittografia. La lunghezza della chiave in bit è un fattore che incide sull'efficacia della chiave. L'organizzazione supporta la lunghezza minima della chiave di 160 bit per le chiavi che utilizzano l'algoritmo ECC, pertanto si imposta questa regola su 160 bit per permettere ai dispositivi di supportare chiavi S/MIME di lunghezza uguale o superiore a tale valore.
Valori possibili	• Da 163 a 571 bit
Valore predefinito	• 163 bit
Requisiti minimi	• BlackBerry Device Software 3.6 • S/MIME Support Package per smartphone BlackBerry 1.5

Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Lunghezza minima della chiave RSA forte per S/MIME

Descrizione	Questa regola consente di specificare la dimensione minima della chiave RSA utilizzata da un dispositivo BlackBerry con i messaggi e-mail con protezione S/MIME.
Esempio	I dispositivi BlackBerry utilizzano chiavi pubbliche S/MIME e chiavi private S/MIME per crittografare e decrittografare i messaggi e-mail. Le chiavi S/MIME possono utilizzare l'algoritmo RSA per la crittografia e la decrittografia. La lunghezza della chiave in bit è un fattore che incide sull'efficacia della chiave. L'organizzazione supporta la lunghezza minima della chiave di 512 bit per le chiavi che utilizzano l'algoritmo RSA, pertanto si imposta questa regola su 512 bit per permettere ai dispositivi di supportare chiavi S/MIME di lunghezza uguale o superiore a tale valore.
Valori possibili	• Da 512 a 4096 bit
Valore predefinito	• 1024 bit
Requisiti minimi	• BlackBerry Device Software 3.6 • S/MIME Support Package per smartphone BlackBerry 1.5
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Regola dei criteri IT: Modalità S/MIME parti successive e invio

Descrizione	Questa regola consente di specificare la modalità utilizzata da un dispositivo BlackBerry per recuperare il testo completo di un messaggio e-mail se un utente BlackBerry inoltra o risponde a un messaggio e-mail.
Esempio	Per impostazione predefinita, l'utente BlackBerry deve richiedere il testo completo dei messaggi e-mail per l'inoltro o la risposta come messaggi S/MIME dai propri dispositivi. È possibile utilizzare

	questa regola per fare in modo che i dispositivi recuperino e visualizzino automaticamente il testo completo dei messaggi e-mail per consentire la risposta o l'inoltro come messaggi S/MIME.
Valori possibili	• Automatico • Manuale • Nessuna
Valore predefinito	• Manuale
Requisiti minimi	• BlackBerry Device Software 5.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP2

Gruppo criteri VPN

Regola dei criteri IT: Nome utente VPN

Descrizione	Questa regola consente di specificare il nome utente predefinito utilizzato da un dispositivo BlackBerry per eseguire la registrazione sul server VPN dell'organizzazione. Configurare un valore per questa regola per creare un nome utente predefinito per tutti gli account utente. Se si immette manualmente un nome utente su un dispositivo BlackBerry, gli aggiornamenti dei criteri IT sovrascrivono o eliminano il valore digitato dall'utente. Per conservare il valore immesso dall'utente sul dispositivo, verificare che la regola aggiornata utilizzi lo stesso valore di questa regola.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Password utente VPN

Descrizione	Questa regola consente di specificare la password predefinita utilizzata dal dispositivo BlackBerry per la connessione al server VPN dell'organizzazione. Specificare un valore per questa regola per configurare una password predefinita per tutti gli account utente. Se un utente BlackBerry immette manualmente una password su un dispositivo, gli aggiornamenti dei criteri IT sovrascrivono o eliminano il valore digitato dall'utente. Per conservare il valore immesso dall'utente sul dispositivo, verificare che la regola aggiornata utilizzi lo stesso valore di questa regola.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Gruppo criteri Wi-Fi

Il nome precedente di questo gruppo criteri era Gruppo criteri WLAN.

Regola dei criteri IT Disattiva Wi-Fi

Descrizione	Questa regola consente di specificare se un utente BlackBerry può accedere a una rete Wi-Fi da un dispositivo BlackBerry abilitato Wi-Fi.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.2.1

Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Wired Software Updates policy group

IT policy rules in the Wired Software Updates policy group apply to the BlackBerry Device Software update process when a BlackBerry device user connects a BlackBerry device to a computer.

Regola dei criteri IT: Consenti caricamento software basato su Web

Descrizione	Questa regola consente di specificare se l'utente BlackBerry può aggiornare BlackBerry Device Software mediante la funzione di caricamento del software su Internet.
Esempio	L'organizzazione dispone di personale IT ridotto. Si desidera che i dipendenti siano in grado di aggiornare BlackBerry Device Software sui propri dispositivi senza dover richiedere un aggiornamento al reparto IT. È possibile utilizzare questa regola per consentire agli utenti di aggiornare BlackBerry Device Software tramite il sito Web di aggiornamento BlackBerry Device Software (www.blackberry.com/update).
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 5.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri IT: Backup servizi di crittografia

Descrizione	Questa regola consente di specificare se il dispositivo BlackBerry può eseguire il backup dei dati dei servizi di crittografia quando un utente BlackBerry aggiorna BlackBerry Device Software. Un servizio di crittografia è un servizio che utilizza una chiave crittografica per proteggere le comunicazioni sul dispositivo. Se si consente al dispositivo di eseguire il backup dei dati dei servizi di crittografia, il dispositivo può continuare a utilizzare il servizio di crittografia al termine del processo di caricamento del software senza che l'utente debba riattivare il dispositivo manualmente.
Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 5.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Gruppo criteri aggiornamenti software wireless

Regola dei criteri IT: Vieta download patch su roaming WAN

Descrizione	Questa regola consente di specificare se impedire o meno a un dispositivo BlackBerry di scaricare aggiornamenti per BlackBerry Device Software tramite una connessione WAN durante il roaming.
Esempio	Si supponga di voler impedire agli utenti BlackBerry di effettuare l'aggiornamento di BlackBerry Device Softwaretramite la rete wireless utilizzando una connessione WAN in roaming, perché questo tipo di connessione non soddisfa i requisiti di protezione e gli standard di utilizzo della rete

	dell'organizzazione. È possibile utilizzare questa regola per impedire agli utenti di effettuare l'aggiornamento di BlackBerry Device Software mediante una connessione WAN in roaming.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.5
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Impostazioni di configurazione 5

Impostazioni di configurazione per i profili Wi-Fi

Impostazione di configurazione Autorità di certificazione dei certificati associati

Descrizione	Questa impostazione consente di specificare il nome del profilo dell'autorità di certificazione nella regola dei criteri IT Nome profilo autorità di certificazione. Il profilo dell'autorità di certificazione è composto da credenziali che il dispositivo BlackBerry può utilizzare per avviare il processo di iscrizione dei certificati. Dopo aver associato un profilo dell'autorità di certificazione a un profilo Wi-Fi, è possibile assegnare il profilo Wi-Fi a un account utente e inviarlo a un dispositivo.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 5.0

Impostazione di configurazione Profilo VPN associato

Descrizione	Questa impostazione consente di specificare il nome del profilo VPN da associare al profilo Wi-Fi.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2.0

Consenti handover tra punti di accesso Wi-Fi

Descrizione	Questa impostazione consente di specificare se il dispositivo BlackBerry può eseguire l'handover Wi-Fi tra punti di accesso wireless.
Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione Consenti modifiche Wi-Fi sul dispositivo

Descrizione	Questa impostazione consente di specificare se un utente BlackBerry può modificare le impostazioni dei criteri Wi-Fi sul dispositivo BlackBerry.
Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 4.0

Impostazione di configurazione Consenti salvataggio password Wi-Fi

Descrizione	Questa impostazione consente di specificare se un utente BlackBerry può salvare le password per l'autenticazione in una rete Wi-Fi sul dispositivo BlackBerry.

Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione Tipo canale per Wi-Fi

Descrizione	Questa impostazione consente di specificare i tipi di canale in base a cui configurare i punti di accesso wireless di un SSID specifico.
Valori possibili	• 802.11 a/b/g • 802.11 b/g • 802.11 a • 802.11 b
Valore predefinito	• 802.11 a/b/g
Requisiti minimi	• BlackBerry Device Software 4.2.2

Impostazione di configurazione Modalità di accesso Wi-Fi a BlackBerry Infrastructure su rete Wi-Fi

Descrizione	Questa impostazione specifica se un dispositivo BlackBerry si può connettere a BlackBerry Infrastructure tramite la rete Wi-Fi.
Impostazioni collegate	Questa impostazione di configurazione influenza la regola dei criteri IT Modalità di accesso Wi-Fi a BlackBerry Infrastructure. Se si modifica questa impostazione, la regola dei criteri IT Modalità di accesso BlackBerry Infrastructure a Wi-Fi viene ignorata. È possibile utilizzare questa impostazione per configurare la modalità di accesso di una rete Wi-Fi specifica, nonché utilizzare la regola dei criteri IT per configurare la modalità di accesso di altre reti Wi-Fi.

	La regola dei criteri IT Modalità di accesso Wi-Fi a BlackBerry Infrastructure influenza questa impostazione di configurazione. Se si disattiva l'accesso a BlackBerry Infrastructure tramite una rete Wi-Fi mediante la regola dei criteri IT Modalità di accesso Wi-Fi a BlackBerry Infrastructure, non è possibile ignorare la regola dei criteri IT tramite questa impostazione di configurazione.
Valori possibili	• Accesso senza VPN • Accesso con VPN • Accesso disattivato
Valore predefinito	• Accesso senza VPN
Requisiti minimi	• BlackBerry Device Software 5.0

Impostazione di configurazione Gateway predefinito della Wi-Fi

Descrizione	Questa regola consente di specificare il gateway predefinito nel formato dell'indirizzo IP (ad esempio 10.0.0.1) che il dispositivo BlackBerry può utilizzare se il protocollo DHCP sul dispositivo è disattivato.
Impostazioni collegate	L'impostazione di configurazione Configurazione DHCP della Wi-Fi influenza questa impostazione di configurazione. Il dispositivo utilizza questa impostazione solo se si modifica l'impostazione Configurazione DHCP della Wi-Fi su No.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione dell'ID chiave Wi-Fi predefinito

Descrizione	Questa impostazione consente di specificare l'ID predefinito della chiave WEP. Verificare che l'ID della chiave WEP corrisponda all'ID del punto di accesso WEP e alla chiave WEP corrispondente.

Valori possibili	• Da 1 a 4
Valore predefinito	• 1
Requisiti minimi	• BlackBerry Device Software 4.0

Impostazione di configurazione Configurazione DHCP della Wi-Fi

Descrizione	Questa impostazione consente di specificare se la propria organizzazione utilizza il protocollo DHCP per la configurazione dinamica della rete. Se l'organizzazione utilizza una rete Wi-Fi che comprende sottoreti, attivare il protocollo DHCP per consentire il roaming tra le sottoreti.
Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Disattiva convalida certificato server Wi-Fi

Descrizione	Questa impostazione consente di specificare se il dispositivo BlackBerry richiede il certificato di un'autorità di certificazione per l'autenticazione del server quando si utilizza un metodo di autenticazione PEAP, EAP-TLS o EAP-TTLS per connettersi a una rete Wi-Fi. Se si cambia questa impostazione su Sì, non è richiesto un certificato di origine per il metodo di autenticazione PEAP, EAP-TLS o EAP-TTLS.
Valori possibili	• Sì • No

Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 5.0

Impostazione di configurazione Suffisso dominio per Wi-Fi

Descrizione	Questa impostazione consente di specificare il suffisso per il nome del dominio interno in formato FQDN.
Impostazioni collegate	L'impostazione di configurazione Configurazione DHCP della Wi-Fi influenza questa impostazione di configurazione. Configurare questa impostazione solo se si modifica l'impostazione di configurazione Configurazione DHCP della rete Wi-Fi su Falso per non rendere disponibile il protocollo DHCP Wi-Fi
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione Metodo di provisioning Wi-Fi

Descrizione	Questa impostazione consente di specificare il tipo di metodo di provisioning utilizzato dal dispositivo BlackBerry quando esegue l'autenticazione su una rete Wi-Fi mediante il metodo EAP-FAST con file PAC. Se si desidera consentire al server di eseguire l'autenticazione del dispositivo tramite il nome utente e la password dell'account utente e un certificato di origine quando il dispositivo effettua la connessione per la prima volta, selezionare l'opzione Autenticato. Il dispositivo non si connette al server se quest'ultimo non fornisce un certificato di origine al dispositivo stesso. Se si desidera che il server esegua l'autenticazione del dispositivo utilizzando il nome utente e la password dell'account utente senza l'autenticazione del server, selezionare l'opzione Anonimo. Se si desidera consentire al server di eseguire l'autenticazione del dispositivo utilizzando il nome utente e la password dell'account utente e, inoltre, si desidera che le impostazioni sul server stabiliscano se effettuare l'autenticazione del server, selezionare l'opzione Entrambi. Se il server

	fornisce un certificato di origine, il dispositivo effettua la verifica del server tramite il certificato di origine selezionato. Se il server non presenta un certificato di origine, il dispositivo non esegue l'autenticazione del server.
Valori possibili	• Anonimo • Autenticato • Entrambi
Valore predefinito	• Anonimo
Requisiti minimi	• BlackBerry Device Software 5.0

Impostazione di configurazione Attiva pagina autenticazione per Wi-Fi

Descrizione	Questa impostazione consente di specificare se il browser di accesso Wi-Fi è disponibile sul dispositivo BlackBerry. Modificare questa impostazione su Sì per permettere a un utente BlackBerry di accedere a un Captive Portal utilizzando il dispositivo.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.0

Impostazione di configurazione Token hardware Wi-Fi richiesto

Descrizione	Questa impostazione consente di specificare se il dispositivo BlackBerry richiede un token hardware per l'autenticazione. Modificare questa impostazione su Sì se il dispositivo richiede un token hardware (ad esempio, RSA SecurID) per l'autenticazione della password.

Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione Modalità autenticazione interna per Wi-Fi

Descrizione	Questa impostazione consente di specificare la modalità di autenticazione utilizzata dal dispositivo BlackBerry per la protezione EAP con tunnel.
Valori possibili	• Nessuno • EAP-MSCHAPV2 • EAP-GTC • PAP • CHAP • MSCHAP • MSCHAPV2 • EAP-MD5
Valore predefinito	• Nessuno
Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione del percorso di accesso Internet Wi-Fi

Descrizione	Questa impostazione consente di specificare in che modo un dispositivo BlackBerry deve accedere a Internet per i profili Wi-Fi configurati per l'organizzazione.

Valori possibili	• Accesso tramite Wi-Fi • Accesso tramite BlackBerry MDS Connection Service • Selezione automatica
Valore predefinito	• Selezione automatica
Requisiti minimi	• BlackBerry 6

Impostazione di configurazione Indirizzo IP Wi-Fi

Descrizione	Questa impostazione consente di specificare l'indirizzo IP (ad esempio 10.0.0.1) che il dispositivo BlackBerry può utilizzare se il protocollo DHCP sul dispositivo è disattivato.
Impostazioni collegate	L'impostazione di configurazione Configurazione DHCP della Wi-Fi influenza questa impostazione di configurazione. Il dispositivo utilizza questa impostazione solo se si modifica l'impostazione Configurazione DHCP della Wi-Fi su No.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Protezione collegamento Wi-Fi

Descrizione	Questa impostazione specifica il metodo di autenticazione che un dispositivo BlackBerry richiede per accedere a una rete Wi-Fi.
Valori possibili	• Protezione Wi-Fi aperta • WEP • PSK • EAP-PEAP • EAP-LEAP

	• ESP-TLS • EAP-FAST • EAP-TTLS • EAP-SIM • EAP-AKA
Valore predefinito	• Protezione Wi-Fi aperta
Requisiti minimi	• BlackBerry Device Software 4.0

Impostazione di configurazione Livello di protezione minimo per chiavi di crittografia di certificati EAP-TLS per Wi-Fi

Descrizione	Questa impostazione consente di specificare il livello minimo di protezione per le chiavi utilizzato da un metodo di autenticazione EAP con un certificato client. Se si configura questa impostazione su Protezione media, il dispositivo BlackBerry richiede all'utente BlackBerry di immettere la password dell'archivio chiavi solo una volta, per recuperare la chiave privata e crittografare i messaggi. Dopo il recupero della chiave privata da parte del dispositivo, quest'ultimo la recupera di nuovo solo dopo il ripristino del dispositivo da parte del'utente. Il dispositivo memorizza la chiave privata nella cache della memoria, ma non insieme al profilo Wi-Fi. Se si configura questa impostazione su Protezione alta, il dispositivo richiede sempre all'utente la password dell'archivio chiavi quando deve accedere alla chiave privata e crittografare i messaggi e-mail. Il dispositivo non memorizza la chiave privata non crittografata insieme al profilo Wi-Fi. Se si configura questa impostazione su Protezione bassa, il dispositivo richiede all'utente di immettere la password dell'archivio chiavi solo una volta, per recuperare la chiave privata e crittografare i messaggi e-mail. Il dispositivo memorizza la chiave privata non crittografata insieme al profilo Wi-Fi.
Valori possibili	• Protezione bassa • Protezione alta • Protezione media
Valore predefinito	• Protezione bassa

Requisiti minimi	• BlackBerry Device Software 4.0

Impostazione di configurazione Chiave Wi-Fi pre-condivisa

Descrizione	Questa impostazione consente di specificare una PSK se nell'organizzazione vengono utilizzate PSK per eseguire l'autenticazione per le reti Wi-Fi.
Impostazioni collegate	L'impostazione di configurazione Protezione collegamento Wi-Fi influenza questa impostazione di configurazione. Il dispositivo BlackBerry utilizza questa impostazione solo se si configura l'impostazione di configurazione Protezione collegamento Wi-Fi su PSK.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.0

Impostazione di configurazione DNS primario della Wi-Fi

Descrizione	Questa impostazione consente di specificare il DNS primario nel formato dell'indirizzo IP (ad esempio 10.0.0.1) che il dispositivo BlackBerry può utilizzare se il protocollo DHCP sul dispositivo è disattivato.
Impostazioni collegate	L'impostazione di configurazione Configurazione DHCP della Wi-Fi influenza questa impostazione di configurazione. Il dispositivo utilizza questa impostazione solo se si modifica l'impostazione Configurazione DHCP della rete Wi-Fi su No.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Modifica profilo Wi-Fi

Descrizione	Questa impostazione consente di specificare se un utente BlackBerry può modificare le impostazioni del profilo Wi-Fi su un dispositivo BlackBerry. Se si modifica questa impostazione su Nessuna modifica, l'utente non può modificare alcuna impostazione nel profilo Wi-Fi. Se si modifica questa impostazione su Modifica credenziali, l'utente può modificare solo le credenziali utente nel profilo Wi-Fi.
Valori possibili	• Modifica completa • Nessuna modifica • Modifica credenziali
Valore predefinito	• Modifica completa
Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione Visibilità profilo Wi-Fi

Descrizione	Questa impostazione consente di specificare se un utente BlackBerry può visualizzare le impostazioni del profilo Wi-Fi. Se si configura questa impostazione su Visibilità limitata, il dispositivo BlackBerry visualizza solo il nome del profilo. Se si configura questa impostazione su Visibilità credenziali, il dispositivo visualizza solo il nome del profilo e le informazioni di accesso dell'utente.
Valori possibili	• Visibilità completa • Visibilità limitata • Visibilità credenziali
Valore predefinito	• Visibilità completa
Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione Soglia roaming Wi-Fi

Descrizione	Questa impostazione specifica con quale frequenza il ricetrasmettitore Wi-Fi di un dispositivo BlackBerry ricerca i punti di accesso wireless nelle vicinanze e si collega a uno di tali punti di accesso se la qualità del segnale è migliore di quella del punto di accesso utilizzato al momento. Se si configura questa impostazione su Bassa, il dispositivo esegue il roaming solo se la qualità del segnale è molto bassa. Se si configura questa impostazione su Media, il dispositivo esegue il roaming solo se la qualità del segnale è media o bassa. Se si configura questa impostazione su Alta, il dispositivo esegue il roaming forzato ai punti di accesso che offrono una potenza del segnale migliore. Se si configura questa impostazione su Automatico, il dispositivo seleziona automaticamente le soglie di roaming.
Valori possibili	• Automatico • Basso • Media • Alto
Valore predefinito	• Automatico
Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione DNS secondario della Wi-Fi

Descrizione	Questa impostazione consente di specificare il DNS secondario nel formato dell'indirizzo IP (ad esempio 10.0.0.1) che il dispositivo BlackBerry può utilizzare se il protocollo DHCP sul dispositivo è disattivato.
Impostazioni collegate	L'impostazione di configurazione Configurazione DHCP della Wi-Fi influenza questa regola. Il dispositivo utilizza questa impostazione solo se si modifica l'impostazione Configurazione DHCP della Wi-Fi su No.
Valore predefinito	• Valore null

Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione SAN server per Wi-Fi

Descrizione	Questa impostazione consente di specificare un campo SAN per il certificato ricevuto dal server. Se non si specifica un campo SAN per il certificato del server, un dispositivo BlackBerry accetta qualsiasi certificato del server valido.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione Oggetto server per Wi-Fi

Descrizione	Questa impostazione consente di specificare il campo "Oggetto" per il certificato ricevuto dal server. Se non si specifica il campo Oggetto per un certificato del server, un dispositivo BlackBerry accetta qualsiasi certificato del server valido.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione SSID Wi-Fi

Descrizione	Questa impostazione consente di specificare il nome di una rete Wi-Fi e i relativi punti di accesso wireless. L'SSID è sensibile alla distinzione tra maiuscole e minuscole e non può superare i 32 caratteri.
Valore predefinito	• Valore null

Requisiti minimi	• BlackBerry Device Software 4.0

Impostazione di configurazione Subnet mask Wi-Fi

Descrizione	Questa impostazione consente di specificare la subnet mask nel formato dell'indirizzo IP (ad esempio 10.0.0.1) che il dispositivo BlackBerry può utilizzare se il protocollo DHCP sul dispositivo è disattivato.
Impostazioni collegate	L'impostazione di configurazione Configurazione DHCP della Wi-Fi influenza questa regola. Il dispositivo utilizza questa impostazione solo se si modifica l'impostazione Configurazione DHCP della Wi-Fi su No.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Numero di serie token Wi-Fi

Descrizione	Se il dispositivo BlackBerry richiede che un token software faccia parte della password per l'autenticazione, questa impostazione consente di specificare il numero di serie del token software attribuito al dispositivo.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione Nome utente Wi-Fi

Descrizione	Questa impostazione consente di specificare il nome utente per l'autenticazione PEAP o LEAP su un dispositivo BlackBerry. Configurare questa impostazione se si desidera creare un valore predefinito per tutti gli utenti BlackBerry. Se l'utente immette manualmente un nome utente sul dispositivo, gli aggiornamenti dei criteri IT sovrascrivono o eliminano il valore digitato dall'utente. Per conservare il

	valore specificato dall'utente sul dispositivo, verificare che il profilo Wi-Fi aggiornato utilizzi lo stesso valore del profilo Wi-Fi sul dispositivo.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.0

Impostazione di configurazione Password utente Wi-Fi

Descrizione	Questa impostazione consente di specificare la password per l'autenticazione PEAP o LEAP su un dispositivo BlackBerry. Configurare questa impostazione se si desidera creare un valore predefinito per tutti gli utenti BlackBerry. Se l'utente immette manualmente una password sul dispositivo, gli aggiornamenti dei criteri IT sovrascrivono o eliminano il valore digitato dall'utente. Per conservare il valore specificato dall'utente sul dispositivo, verificare che il profilo Wi-Fi aggiornato utilizzi lo stesso valore del profilo Wi-Fi sul dispositivo.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Chiave WEP 1 per Wi-Fi

Descrizione	Questa impostazione consente di specificare la password per la chiave WEP 1 utilizzando il formato *xx:xx:xx:xx:xx*. Questa impostazione di configurazione supporta 5 o 13 coppie di cifre esadecimali (da 0 a 9 e da A a F) separate da due punti (:). Ad esempio, AB:CD:EF:01:23 o AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.0

Impostazione di configurazione Chiave WEP 2 per Wi-Fi

Descrizione	Questa impostazione consente di specificare la password per la chiave WEP 2 utilizzando il formato *xx:xx:xx:xx:xx*. Questa impostazione di configurazione supporta 5 o 13 coppie di cifre esadecimali (da 0 a 9 e da A a F) separate da due punti (:). Ad esempio, AB:CD:EF:01:23 o AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.0

Impostazione di configurazione Chiave WEP 3 per Wi-Fi

Descrizione	Questa impostazione consente di specificare la password per la chiave WEP 3 utilizzando il formato *xx:xx:xx:xx:xx*. Questa impostazione di configurazione supporta 5 o 13 coppie di cifre esadecimali (da 0 a 9 e da A a F) separate da due punti (:). Ad esempio, AB:CD:EF:01:23 o AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.0

Impostazione di configurazione Chiave WEP 4 per Wi-Fi

Descrizione	Questa impostazione consente di specificare la password per la chiave WEP 4 utilizzando il formato *xx:xx:xx:xx:xx*. Questa impostazione di configurazione supporta 5 o 13 coppie di cifre esadecimali (da 0 a 9 e da A a F) separate da due punti (:). Ad esempio, AB:CD:EF:01:23 o AB:CD:EF:01:23:45:67:89:AB:CD:EF:01:23.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.0

Impostazioni di configurazione per i profili VPN

Impostazione di configurazione Autorità di certificazione dei certificati associati

Descrizione	Questa impostazione consente di specificare il nome del profilo dell'autorità di certificazione nella regola dei criteri IT Nome profilo autorità di certificazione. Il profilo dell'autorità di certificazione è composto da credenziali che il dispositivo BlackBerry può utilizzare per avviare il processo di iscrizione dei certificati. Dopo aver associato un profilo dell'autorità di certificazione a un profilo VPN, è possibile assegnare il profilo VPN a un account utente e inviarlo a un dispositivo.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 5.0 • BlackBerry Enterprise Server Express 5.0 SP4

Impostazione di configurazione Abilita VPN

Descrizione	Questa impostazione consente di specificare se il client VPN di un dispositivo BlackBerry è attivato. Se si modifica questa impostazione su Sì, il dispositivo deve utilizzare un server VPN per accedere a una rete Wi-Fi. Se si modifica questa impostazione su No, il dispositivo potrebbe non essere in grado di utilizzare una rete Wi-Fi che richiede l'accesso VPN o potrebbe richiedere l'uso di una modalità alternativa di controllo dell'accesso.
Valori possibili	• Sì • No
Valore predefinito	• No

Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione della configurazione Modalità di divisione del tunnel

Descrizione	Questa impostazione specifica se un dispositivo BlackBerry può utilizzare la divisione del tunnel per bypassare una connessione VPN attiva.
Valori possibili	• Attiva su tutte le reti • Disattiva sulle reti aziendali • Disattiva su tutte le reti
Valore predefinito	• Disattiva su tutte le reti
Requisiti minimi	• BlackBerry Device Software 5.0

Impostazione di configurazione Annulla banner VPN

Descrizione	Questa impostazione consente di specificare se la finestra di dialogo VPN viene visualizzata su un dispositivo BlackBerry una volta connesso al server VPN.
Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione Utilizza Xauth per VPN

Descrizione	Questa impostazione consente di specificare se il client VPN di un dispositivo BlackBerry deve utilizzare i certificati Xauth per eseguire l'autenticazione sul gateway VPN dell'organizzazione.
Impostazioni collegate	L'impostazione di configurazione Attiva VPN influenza questa impostazione di configurazione. È necessario modificare l'impostazione di configurazione Attiva VPN su Sì per consentire al dispositivo di utilizzare questa impostazione di configurazione.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Consenti modifiche VPN sul dispositivo

Descrizione	Questa impostazione consente di specificare se l'utente BlackBerry può modificare tutte le regole dei criteri VPN su un dispositivo BlackBerry. Se si modifica questa impostazione su No, l'utente può continuare a modificare nome utente e password VPN sul dispositivo.
Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 4.0

Impostazione di configurazione Consenti salvataggio password VPN

Descrizione	Questa impostazione consente di specificare se un utente BlackBerry può salvare la password VPN su un dispositivo BlackBerry.
Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Disattiva convalida certificato server VPN

Descrizione	Questa impostazione consente di specificare se un dispositivo BlackBerry deve richiedere un certificato per l'autenticazione con i gateway VPN che supportano l'autenticazione basata su PKI mediante i certificati. Questa impostazione è applicabile ai seguenti gateway VPN che supportano l'autenticazione basata su PKI mediante i certificati: Cisco Secure PIX Firewall, Cisco IOS with Easy VPN Server, NetScreen Series Security Systems e Nortel Networks Contivity VPN Switch.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 5.0

Impostazione di configurazione Configurazione DNS VPN

Descrizione	Questa impostazione consente di specificare la configurazione DNS della VPN aziendale. Per richiedere che il dispositivo BlackBerry recuperi le impostazioni DNS dal gateway VPN, cambiare questa impostazione su Sì. Per richiedere al dispositivo di utilizzare le impostazioni statiche specificate nelle impostazioni di configurazione DNS primario VPN, DNS secondario VPN e Nome dominio VPN, modificare questa impostazione su No.
Impostazioni collegate	L'impostazione di configurazione Attiva VPN influenza questa impostazione di configurazione. È necessario modificare l'impostazione di configurazione Attiva VPN su Vero per consentire al dispositivo di utilizzare questa impostazione di configurazione.
Valori possibili	• Sì • No
Impostazione predefinita	• Sì
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Nome dominio VPN

Descrizione	Questa impostazione consente di specificare il suffisso per il nome dominio dell'azienda in formato FQDN.
Impostazioni collegate	L'impostazione di configurazione Attiva VPN influenza questa impostazione di configurazione. È necessario modificare l'impostazione di configurazione Attiva VPN su Sì per consentire al dispositivo BlackBerry di utilizzare questa impostazione di configurazione. L'impostazione di configurazione Configurazione DNS VPN influenza questa impostazione di configurazione. È necessario modificare l'impostazione di configurazione Configurazione DNS VPN su No per consentire al dispositivo di utilizzare questa impostazione di configurazione.
Valore predefinito	• Valore null

Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Indirizzo gateway VPN

Descrizione	Questa impostazione consente di specificare l'indirizzo IP o il suffisso FQDN del server VPN aziendale.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Nome gruppo VPN

Descrizione	Questa impostazione consente di specificare il nome gruppo del server VPN aziendale. Specificare il nome gruppo del server VPN dell'organizzazione solo se il client VPN lo richiede.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Password gruppo VPN

Descrizione	Questa impostazione consente di specificare la password di gruppo del server VPN dell'organizzazione. Specificare la password di gruppo del server VPN dell'organizzazione solo se il client VPN lo richiede.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Token hardware VPN richiesto

Descrizione	Questa impostazione consente di specificare se il server VPN richiede che un dispositivo BlackBerry utilizzi un token hardware come parte della password per l'autenticazione.
Valori possibili	• Sì • No
Valore predefinito	• No
Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione Crittografia IKE per VPN

Descrizione	Questa impostazione consente di specificare l'algoritmo di crittografia utilizzato da un dispositivo BlackBerry per autenticare gli scambi IKE. Cambiare questa impostazione solo se l'algoritmo di crittografia non supporta AES128.
Valori possibili	• DES • 3DES • AES128 • AES192 • AES256
Valore predefinito	• AES128
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Gruppo DH IKE per VPN

Descrizione	Questa impostazione consente di specificare il gruppo DH utilizzato da un dispositivo BlackBerry per la generazione delle chiavi. Cambiare questa impostazione solo se il gruppo DH non utilizza ECC.
Impostazioni collegate	L'impostazione di configurazione Attiva VPN influenza questa regola. È necessario modificare l'impostazione di configurazione Attiva VPN su Sì per consentire al dispositivo di utilizzare questa impostazione.
Valori possibili	• Gruppo 1 • Gruppo 2 • Gruppo 5 • Gruppo 7 • Gruppo 9
Valore predefinito	• Gruppo 7
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Hash IKE per VPN

Descrizione	Questa impostazione consente di specificare il codice HMAC (Hash Message Authentication Code) utilizzato da un dispositivo BlackBerry. Modificare questa impostazione solo se il codice HMAC (Hash Message Authentication Code) non supporta SHA-1 a 160 bit.
Valori possibili	• MD5 a 128 bit • SHA1 a 160 bit
Valore predefinito	• SHA1 a 160 bit
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Indirizzo IP VPN

Descrizione	Questa impostazione consente di specificare l'indirizzo IP della VPN.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione Crittografia e hash IPSec per VPN

Descrizione	Questa impostazione consente di specificare gli algoritmi di crittografia e hash utilizzati da un dispositivo BlackBerry per le SA (Security Association) IPSec. Modificare questa impostazione solo se le opzioni di crittografia e hash IPSec non sono impostate su Hash SHA1 e Crittografia AES-128.
Valori possibili	• Hash MD5 senza crittografia • Hash SHA1 senza crittografia • Nessun Hash con crittografia DES • Hash MD5 e crittografia DES • Hash SHA1 e crittografia DES • Nessun Hash e crittografia 3DES • Hash MD5 e crittografia 3DES • Hash SHA1 e crittografia 3DES • Nessun Hash e crittografia AES128 • Hash MD5 e crittografia AES128 • Hash SHA1 e crittografia AES128 • Nessun Hash e crittografia AES192 • Hash MD5 e crittografia AES192 • Hash SHA1 e crittografia AES192 • Nessun Hash e crittografia AES256 • Hash MD5 e crittografia AES256

	• Hash SHA1 e crittografia AES256
Valore predefinito	• Hash SHA1 e crittografia AES128
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Livello di protezione minimo per chiavi di crittografia di certificati per VPN

Descrizione	Questa impostazione consente di specificare il livello minimo di protezione per le chiavi private utilizzate da un dispositivo BlackBerry per i metodi di autenticazione che richiedono certificati client. Se si modifica questa impostazione su Protezione alta, il dispositivo BlackBerry richiederà sempre all'utente la password dell'archivio chiavi per accedere alla chiave privata. Tale richiesta può verificarsi frequentemente, anche se l'utente ha appena immesso la password. Le chiavi private non vengono memorizzate assieme al profilo VPN. Se si modifica questa impostazione su Protezione media, il dispositivo richiede all'utente la password dell'archivio chiavi solo la prima volta, quindi la richiede solo se l'utente reimposta il dispositivo. Le chiavi private vengono conservate nella cache della memoria, ma non assieme al profilo VPN. Se si modifica questa impostazione su Protezione bassa, il dispositivo richiede solo una volta all'utente di immettere la password dell'archivio chiavi. Il dispositivo recupera e archivia in formato non crittografato la chiave privata insieme al profilo VPN.
Valori possibili	• Protezione bassa • Protezione alta • Protezione media
Valore predefinito	• Protezione bassa
Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione Durata attività NAT VPN

Descrizione	Questa impostazione consente di specificare la frequenza di durata dell'attività del NAT. Specificare l'intervallo dopo il quale un dispositivo BlackBerry invia al VPN Concentrator un pacchetto per mantenere attiva la connessione.
Valori possibili	• Da 1 a 1439 minuti
Valore predefinito	• 1 minuto
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione PFS per VPN

Descrizione	Questa impostazione consente di specificare se la PFS è attiva per un dispositivo BlackBerry. Cambiare questa impostazione solo se la propria organizzazione non supporta la PFS.
Valori possibili	• Sì • No
Valore predefinito	• Sì
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione DNS primario della VPN

Descrizione	Questa impostazione consente di specificare l'impostazione statica per l'indirizzo IP del server DNS primario aziendale.

Impostazioni collegate	L'impostazione di configurazione Attiva VPN influenza questa impostazione di configurazione. È necessario modificare l'impostazione di configurazione Attiva VPN su Sì per fare in modo che il dispositivo BlackBerry utilizzi questa impostazione di configurazione. L'impostazione di configurazione Configurazione DNS VPN influenza questa impostazione di configurazione. È necessario modificare l'impostazione di configurazione Configurazione DNS VPN su No in modo che il dispositivo utilizzi questa impostazione di configurazione.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Visibilità profilo VPN

Descrizione	Questa impostazione consente di specificare se l'utente BlackBerry può visualizzare le impostazioni di configurazione del profilo VPN su un dispositivo BlackBerry.
Valori possibili	• Visibilità completa • Visibilità limitata • Visibilità credenziali
Valore predefinito	• Visibilità completa
Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione Modifica profilo VPN

Descrizione	Questa impostazione consente di specificare se l'utente BlackBerry può modificare le impostazioni di configurazione del profilo VPN su un dispositivo BlackBerry.
Valori possibili	• Modifica completa • Nessuna modifica • Modifica credenziali

Valore predefinito	• Modifica completa
Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione DNS secondario della VPN

Descrizione	Questa impostazione consente di specificare l'impostazione statica per l'indirizzo IP del server DNS secondario aziendale.
Impostazioni collegate	L'impostazione di configurazione Attiva VPN influenza questa impostazione di configurazione. È necessario modificare l'impostazione di configurazione Attiva VPN su Sì per consentire ad un dispositivo BlackBerry di utilizzare questa impostazione. L'impostazione di configurazione Configurazione DNS VPN influenza questa impostazione di configurazione. È necessario modificare l'impostazione di configurazione Configurazione DNS VPN su No per consentire al dispositivo di utilizzare questa impostazione di configurazione.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione della configurazione Indirizzo IP subnet VPN 1

Descrizione	Questa impostazione specifica l'indirizzo IP della subnet 1 per i gateway VPN per i quali il dispositivo BlackBerry deve definire una subnet. Immettere l'indirizzo IP in notazione decimale a punti (ad esempio, 192.0.2.1).
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.6

Impostazione della configurazione Subnet mask VPN 1

Descrizione	Questa impostazione specifica la subnet mask della subnet 1 per i gateway VPN per i quali il dispositivo BlackBerry deve definire una subnet.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.6

Impostazione della configurazione Indirizzo IP subnet VPN 2

Descrizione	Questa impostazione specifica l'indirizzo IP della subnet 2 per i gateway VPN per i quali il dispositivo BlackBerry deve definire una subnet. Immettere l'indirizzo IP in notazione decimale a punti (ad esempio, 192.0.2.1).
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.6

Impostazione della configurazione Subnet mask VPN 2

Descrizione	Questa impostazione specifica la subnet mask della subnet 2 per i gateway VPN per i quali il dispositivo BlackBerry deve definire una subnet.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.6

Impostazione della configurazione Indirizzo IP subnet VPN 3

Descrizione	Questa impostazione specifica l'indirizzo IP della subnet 3 per i gateway VPN per i quali il dispositivo BlackBerry deve definire una subnet. Immettere l'indirizzo IP in notazione decimale a punti (ad esempio, 192.0.2.1).
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.6

Impostazione della configurazione Subnet mask VPN 3

Descrizione	Questa impostazione specifica la subnet mask della subnet 3 per i gateway VPN per i quali il dispositivo BlackBerry deve definire una subnet.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.6

Impostazione di configurazione Subnet mask VPN

Descrizione	Questa impostazione consente di specificare l'indirizzo IP per la subnet mask della VPN.
Impostazioni collegate	Questa impostazione di configurazione influenza l'impostazione di configurazione Attiva VPN. Se si modifica questa impostazione di configurazione, è necessario modificare l'impostazione di configurazione Attiva VPN su Sì. Questa impostazione di configurazione influenza l'impostazione di configurazione Configurazione DNS VPN. Se si modifica questa impostazione di configurazione, è necessario modificare l'impostazione di configurazione Configurazione DNS VPN su No.
Impostazione predefinita	• Valore null

Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione Numero di serie token VPN

Descrizione	Se il server VPN richiede a un dispositivo BlackBerry di utilizzare un token software come parte della password per l'autenticazione, questa impostazione consente di specificare il numero di serie del token software attribuito al dispositivo.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2.1

Impostazione di configurazione Nome utente VPN

Descrizione	Questa impostazione consente di specificare il nome utente predefinito utilizzato da un dispositivo BlackBerry per eseguire la registrazione sul server SIP dell'organizzazione. Configurare questa impostazione per creare un nome utente predefinito per tutti gli account utente. Se si immette manualmente un nome utente su un dispositivo BlackBerry, gli aggiornamenti dei criteri IT sovrascrivono o eliminano il valore digitato dall'utente. Per conservare il valore immesso dall'utente sul dispositivo, verificare che l'impostazione di configurazione aggiornata utilizzi lo stesso valore di questa impostazione.
Impostazioni collegate	L'impostazione di configurazione Attiva VPN influenza questa impostazione di configurazione. È necessario modificare l'impostazione di configurazione Attiva VPN su Sì per consentire al dispositivo di utilizzare questa impostazione.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Password utente VPN

Descrizione	Questa impostazione consente di specificare la password predefinita utilizzata da un dispositivo BlackBerry per eseguire la registrazione sul server VPN dell'organizzazione. Configurare questa impostazione per creare una password predefinita per tutti account utente. Se un utente BlackBerry immette manualmente una password sul dispositivo, gli aggiornamenti dei criteri IT sovrascrivono o eliminano il valore digitato dall'utente. Per conservare il valore immesso dall'utente sul dispositivo, verificare che l'impostazione di configurazione aggiornata utilizzi lo stesso valore di questa impostazione.
Impostazioni collegate	L'impostazione di configurazione Attiva VPN influenza questa impostazione di configurazione. È necessario modificare l'impostazione di configurazione Attiva VPN su Sì per consentire al dispositivo di utilizzare questa impostazione di configurazione.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Tipo fornitore VPN

Descrizione	Questa impostazione consente di specificare il tipo di client VPN emulato su un dispositivo BlackBerry.
Impostazioni collegate	L'impostazione di configurazione Attiva VPN influenza questa impostazione di configurazione. È necessario modificare l'impostazione di configurazione Attiva VPN su Sì per consentire al dispositivo di utilizzare questa impostazione di configurazione.
Valori possibili	• Alcatel 7130 Secure VPN Gateway Family • Avaya VSU(TM) Series • Check Point(TM) Software Technologies VPN-1 • Cisco VPN Concentrator serie 3000 • Cisco Secure PIX Firewall VPN • Cisco IOS with Easy VPN Server • Cosine IPX VPN Gateway

	• Cylink Nethawk • Intel®) Netstructure(TM) 3100 Series • Lucent Firewall Brick Family • Netscreen Systems • Nortel Networks Contivity VPN Switch Series • ReefEdge Connect Server • Secure Computing Sidewinder(TM) Firewall • Symantec Raptor Firewall and PowerVPN
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.2

Impostazione di configurazione Tipo Xauth per VPN

Descrizione	Questa impostazione specifica il tipo di autenticazione che gli utenti BlackBerry devono utilizzare per il server VPN dell'organizzazione.
Impostazioni collegate	L'impostazione di configurazione Attiva VPN influenza questa impostazione di configurazione. Cambiare l'impostazione di configurazione Attiva VPN su Sì per fare in modo che un dispositivo BlackBerry utilizzi questa impostazione di configurazione.
Valori possibili	• Nome utente e password richiesti • SecurID richiesto
Valore predefinito	• Nome utente e password richiesti
Requisiti minimi	• BlackBerry Device Software 4.2

Regole dei criteri di controllo applicazioni

6

Per informazioni sulla configurazione delle regole dei criteri di controllo applicazioni, consultare la documentazione *Guida per l'amministratore di BlackBerry Enterprise Server Express*

Regola dei criteri di controllo applicazioni: Connessioni di rete esterne consentite

Descrizione	Questa regola consente di specificare se un'applicazione può stabilire connessioni di rete esterne. È possibile configurare questa regola per impedire a un'applicazione di inviare o ricevere dati su un dispositivo BlackBerry tramite un protocollo esterno (ad esempio, WAP o TCP). È, inoltre, possibile configurare questa regola in modo da consentire ad un'applicazione di richiedere l'autorizzazione dell'utente BlackBerry prima di stabilire connessioni esterne tramite il firewall del dispositivo.
Regole collegate	La regola dei criteri di controllo applicazioni Elenco dei domini esterni influenza questa regola. La regola dei criteri di controllo applicazioni Elenco dei domini esterni ha priorità sulla regola dei criteri di controllo applicazioni.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa • Richiesto dall'utente
Valore predefinito	• Richiesto dall'utente
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni: Connessioni di rete interne consentite

Descrizione	Questa regola consente di specificare se un'applicazione può stabilire connessioni di rete interne. È possibile configurare questa regola per impedire all'applicazione di inviare o ricevere dati a e dal dispositivo BlackBerry utilizzando un protocollo interno (ad esempio BlackBerry MDS Connection Service). È, inoltre, possibile configurare questa regola in modo da consentire ad un'applicazione di richiedere l'autorizzazione dell'utente BlackBerry prima di stabilire connessioni interne tramite il firewall del dispositivo.
Regole collegate	La regola dei criteri di controllo applicazioni Elenco dei domini interni influenza questa regola. La regola dei criteri di controllo applicazioni Elenco dei domini interni ha priorità sulla regola dei criteri di controllo applicazioni.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa • Richiesto dall'utente
Valore predefinito	• Richiesto dall'utente
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo delle applicazioni: Le connessioni locali sono consentite?

Descrizione	Questa regola consente di specificare se un'applicazione può stabilire connessioni alla rete locale (ad esempio, connessioni al dispositivo BlackBerry utilizzando una porta seriale o USB).
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa
Valore predefinito	• Autorizzazione concessa
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni Le impostazioni del dispositivo possono essere modificate?

Descrizione	Questa regola consente di specificare se un'applicazione può modificare le impostazioni di configurazione e utente BlackBerry su un dispositivo BlackBerry.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa

	• Richiesto dall'utente
Valore predefinito	• Autorizzazione concessa
Requisiti minimi	• BlackBerry Device Software 4.2.1
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni Consentire il ripristino del timer di protezione?

Descrizione	Questa regola consente di specificare se un'applicazione può reimpostare il tempo che deve trascorrere prima di bloccare automaticamente un dispositivo BlackBerry.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa • Richiesto dall'utente
Valore predefinito	• Autorizzazione non concessa
Requisiti minimi	• BlackBerry Device Software 4.2.1
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni Visualizza informazioni quando bloccato

Descrizione	Questa regola consente di specificare se un'applicazione può visualizzare informazioni su una schermata del dispositivo BlackBerry quando il dispositivo è bloccato.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa • Richiesto dall'utente
Valore predefinito	• Autorizzazione non concessa
Requisiti minimi	• BlackBerry 6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP3

Regola dei criteri di controllo applicazioni: Disposizione

Descrizione	Questa regola consente di specificare se la presenza di un'applicazione sul dispositivo BlackBerry è opzionale, richiesta o non consentita. È possibile utilizzare questa regola per impostare sul dispositivo una determinata applicazione come richiesta o per impedire che sul dispositivo vengano installate applicazioni non specificate o non attendibili.
Valori possibili	• Opzionale • Indispensabile • Autorizzazione non concessa

Valore predefinito	• Opzionale
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo delle applicazioni: L'accesso all'API filtri browser è consentito?

Descrizione	Questa regola consente di specificare se un'applicazione può accedere all'API filtri browser per registrare un filtro del browser su un dispositivo BlackBerry. È possibile utilizzare questa regola per consentire alle applicazioni di terzi di applicare filtri del browser personalizzati al contenuto di pagine Web su un dispositivo.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa
Valore predefinito	• Autorizzazione non concessa
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni L'accesso ai dati aziendali è consentito?

Descrizione	Questa regola consente di specificare se un'applicazione di terzi o un'applicazione aggiuntiva sviluppata da Research In Motion può accedere ai dati di lavoro su un dispositivo BlackBerry. È possibile configurare questa regola per impedire alle applicazioni di terzi o alle applicazioni aggiuntive sviluppate da RIM di accedere ai dati di lavoro sul dispositivo. Il dispositivo controlla la presenza di questa regola per determinare quali applicazioni possono accedere ai dati di lavoro.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa
Valore predefinito	• Autorizzazione concessa
Requisiti minimi	• BlackBerry 6
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP3

Regola dei criteri di controllo delle applicazioni: L'accesso all'API posta elettronica è consentito?

Descrizione	Questa regola consente di specificare se un'applicazione può inviare e ricevere messaggi e-mail su un dispositivo BlackBerry.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa

Valore predefinito	• Autorizzazione concessa
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni L'accesso all'API avvio evento è consentito?

Descrizione	Questa regola consente di specificare se un'applicazione può simulare eventi di input su un dispositivo BlackBerry, come ad esempio la pressione di tasti o movimenti della trackball.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa
Valore predefinito	• Autorizzazione concessa
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni L'accesso all'API file è consentito?

Descrizione	Questa regola consente di specificare se un'applicazione può accedere, modificare, eliminare e spostare file su un dispositivo BlackBerry.

Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa
Valore predefinito	• Autorizzazione concessa
Requisiti minimi	• BlackBerry Device Software 4.2
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni L'accesso all'API GPS è consentito?

Descrizione	Questa regola consente di specificare se un'applicazione può accedere alle API GPS su un dispositivo BlackBerry. È possibile configurare questa regola per impedire all'applicazione di accedere alle API GPS sul dispositivo o per far sì che richieda l'autorizzazione all'utente BlackBerry.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa • Richiesto dall'utente
Valore predefinito	• Richiesto dall'utente
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni L'accesso all'archivio chiavi del dispositivo è consentito?

Descrizione	Questa regola consente di specificare se un'applicazione può accedere alle API dell'archivio chiavi su un dispositivo BlackBerry.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa
Valore predefinito	• Autorizzazione concessa
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo delle applicazioni: L'accesso all'API di comunicazione tra i processi è consentito?

Descrizione	Questa regola consente di specificare se un'applicazione può eseguire operazioni di comunicazione tra applicazioni. È possibile utilizzare questa regola per permettere a due o più applicazioni di condividere dei dati o ad un'applicazione di utilizzare le autorizzazioni di connessione di un'altra applicazione.

Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa
Valore predefinito	• Autorizzazione concessa
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni: Accesso all'API contenuto multimediale consentito

Descrizione	Questa regola consente di specificare se un'applicazione può eseguire o creare file multimediali su un dispositivo BlackBerry.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa
Valore predefinito	• Autorizzazione concessa
Requisiti minimi	• BlackBerry Device Software 4.3
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo delle applicazioni: L'accesso all'API di gestione modulo è consentito?

Descrizione	Questa regola consente di specificare se un'applicazione può aggiungere, modificare o eliminare file .cod Java su un dispositivo BlackBerry.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa
Valore predefinito	• Autorizzazione concessa
Requisiti minimi	• BlackBerry Device Software 4.3
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni: L'accesso a NFC (Near Field Communication) è autorizzato?

Descrizione	Questa regola consente di specificare se un'applicazione può accedere a NFC su un dispositivo BlackBerry.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa

	• Richiesto dall'utente
Valore predefinito	• Autorizzazione concessa
Requisiti minimi	• BlackBerry 7
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP4

Regola dei criteri di controllo applicazioni: L'accesso all'API PIM è consentito?

Descrizione	Questa regola consente di specificare se un'applicazione può accedere alle API PIM del dispositivo BlackBerry, che controllano l'accesso alle informazioni personali dell'utenteBlackBerry, come quelle della rubrica, sul dispositivo. Se si consente a un'applicazione di accedere alle API dei dati PIM e di utilizzare i protocolli di connessione di rete, l'applicazione potrebbe inviare tutte le informazioni personali dell'utente dal dispositivo.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa
Valore predefinito	• Autorizzazione concessa
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni: L'accesso all'API telefono è consentito?

Descrizione	Questa regola consente di specificare se un'applicazione può effettuare e ricevere chiamate e accedere ai registri delle chiamate su un dispositivo BlackBerry. È possibile configurare questa regola per impedire ad un'applicazione di effettuare chiamate su un dispositivo o per richiedere a un utente BlackBerry se desidera consentire la chiamata prima di far eseguire l'operazione all'applicazione.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa • Richiesto dall'utente
Valore predefinito	• Richiesto dall'utente
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni: L'accesso alle API di acquisizione schermo, microfono e video è consentito?

Descrizione	Questa regola consente di specificare se un'applicazione può registrare elementi multimediali, come audio e video, tramite BlackBerry Browser o altre applicazioni su un dispositivo BlackBerry.
Valori possibili	• Autorizzazione non concessa

	• Autorizzazione concessa • Richiesto dall'utente
Valore predefinito	• Autorizzazione non concessa
Requisiti minimi	• BlackBerry Device Software 4.2.1
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni: L'accesso all'elemento protetto è autorizzato?

Descrizione	Questa regola consente di specificare se un'applicazione può accedere all'elemento protetto su un dispositivo BlackBerry.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa • Richiesto dall'utente
Valore predefinito	• Autorizzazione concessa
Requisiti minimi	• BlackBerry 7
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP4

Regola dei criteri di controllo applicazioni: L'accesso all'API SPP (Serial Port Profile) per Bluetooth è consentito?

Descrizione	Questa regola consente di specificare se un'applicazione può accedere all'API del profilo Bluetooth® SPP (Serial Port Profile).
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa
Valore predefinito	• Autorizzazione concessa
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni: L'accesso all'API autenticatore utente è consentito?

Descrizione	Questa regola consente di specificare se un'applicazione può accedere all'API del framework dell'autenticatore utente. Il framework dell'autenticatore utente consente la registrazione di driver che, tramite l'autenticazione a due fattori, possono sbloccare il dispositivo BlackBerry. La regola viene applicata a BlackBerry Device Software e alle applicazioni Java di terzi.

	Per i dispositivi con BlackBerry Device Software 5.0 e versioni successive, questa regola viene applicata ai driver per smart card reader e ai metodi di autenticazione a due fattori personalizzati, che vengono creati dagli sviluppatori dell'organizzazione. Per i dispositivi con BlackBerry Device Software 4.7 e versioni precedenti, questa regola viene applicata solo ai driver per smart card.
Valori possibili	• Non consentire • Autorizzazione concessa
Valore predefinito	• Autorizzazione concessa
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni: L'accesso all'API Wi-Fi è consentito?

Descrizione	Questa regola consente di specificare se un'applicazione su un dispositivo BlackBerry può inviare e ricevere dati tramite una connessione Wi-Fi e accedere alle informazioni sulla rete Wi-Fi.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa • Richiesto dall'utente
Valore predefinito	• Richiesto dall'utente
Requisiti minimi	• BlackBerry Device Software 4.2.1
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni: Protezione media archivio chiavi consentita

Descrizione	Questa regola consente di specificare se un'applicazione può accedere alle voci dell'archivio chiavi con un livello di protezione medio. L'applicazione richiederà all'utente BlackBerry la password dell'archivio chiavi la prima volta che accede alla chiave privata o nel momento in cui scade la password della chiave privata.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa
Valore predefinito	• Autorizzazione concessa
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni Gestione connessioni consentita

Descrizione	Questa regola consente di specificare se un'applicazione può gestire le connessioni e le informazioni relative alla connessione su un dispositivo BlackBerry.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa
Valore predefinito	• Autorizzazione concessa

Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP3

Regola dei criteri di controllo applicazioni Controllo contenuto multimediale consentito

Descrizione	Questa regola consente di specificare se un'applicazione può aprire o gestire file multimediali su un dispositivo BlackBerry.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa • Richiesto dall'utente
Valore predefinito	• Autorizzazione concessa
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP3

Regola dei criteri di controllo applicazioni: I dati temi sono consentiti?

Descrizione	Questa regola consente di specificare se un utente BlackBerry può utilizzare applicazioni personalizzate sviluppate con Plazmic Content Developer's Kit su un dispositivo BlackBerry.
Valori possibili	• Autorizzazione non concessa • Autorizzazione concessa

Valore predefinito	• Autorizzazione concessa
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni: Elenco dei domini filtro browser

Descrizione	Questa regola consente di specificare l'elenco dei domini per cui un'applicazione può applicare i filtri del browser relativi al contenuto delle pagine Web sul dispositivo BlackBerry. Ad esempio, è possibile decidere di applicare i filtri ai motori di ricerca specificando www.google.com e www.yahoo.com.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni: Elenco dei domini esterni

Descrizione	Questa regola consente di specificare i nomi dei domini esterni ai quali un'applicazione può connettersi. Questa regola non supporta i caratteri jolly. Separare i diversi domini con un punto e virgola (;). È possibile configurare questa regola dei criteri di controllo dell'applicazione e una regola pull che BlackBerry MDS Connection Service utilizza per controllare se un utenteBlackBerry può accedere a

	un dominio esterno. Se vengono configurate questa regola e una regola pull per un dominio esterno, l'utente non può accedere al dominio esterno, a meno che non sia consentito l'accesso da questa regola e dalla regola pull.
Regole collegate	Questa regola influenza la regola dei criteri di controllo applicazioni Le connessioni di rete esterne sono consentite? L'applicazione su un dispositivo BlackBerry può connettersi ai domini specificati in questa regola anche se la regola dei criteri di controllo applicazioni Le connessioni di rete esterne sono consentite? viene impostata su Autorizzazione non concessa.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Regola dei criteri di controllo applicazioni: Elenco dei domini interni

Descrizione	Questa regola consente di specificare i nomi dei domini interni ai quali un'applicazione può connettersi. Questa regola non supporta i caratteri jolly. Separare i diversi domini con un punto e virgola (;).
Regole collegate	Questa regola influenza la regola dei criteri di controllo applicazioni Le connessioni di rete interne sono consentite? L'applicazione su un dispositivo BlackBerry può connettersi ai domini specificati in questa regola anche se la regola dei criteri di controllo applicazioni Le connessioni di rete interne sono consentite? viene impostata su Autorizzazione non concessa.
Valore predefinito	• Valore null
Requisiti minimi	• BlackBerry Device Software 4.0
Introduzione alla regola	• BlackBerry Enterprise Server Express 5.0 SP1

Esempi dei livelli di protezione 7

Richiesta dell'utilizzo di una password su un dispositivo

Scenario	Regola dei criteri IT	Gruppo di criteri IT	Valore
Estendere il criterio delle password dell'organizzazione ai dispositivi BlackBerry.	Password obbligatoria	Gruppo criteri Solo dispositivo	Sì
	Giacenza max password	Gruppo criteri Solo dispositivo	30
	Lunghezza minima della password	Gruppo criteri Solo dispositivo	8
	Modelli password	Gruppo criteri Solo dispositivo	Almeno 1 carattere alfabetico, 1 numerico e 1 speciale
	Imposta Timeout password	Gruppo criteri Password	5
	L'utente può modificare il timeout	Gruppo criteri Solo dispositivo	No
Eliminare i dati di tutti gli utenti sul dispositivo se un utente BlackBerry digita la password in modo errato.	Imposta numero massimo di tentativi password	Gruppo criteri Password	10
Non consentire ad un utente di riutilizzare una password scaduta.	Cronologia massima password	Gruppo criteri Password	10

Come evitare l'utilizzo non autorizzato di un dispositivo

Scenario	Regola dei criteri IT	Gruppo criteri	Valore
Bloccare il dispositivo BlackBerry automaticamente, qualunque sia l'attività dell'utente.	Attiva timeout a lungo termine	Gruppo criteri Solo dispositivo	Sì
Richiedere ad un utente BlackBerry di digitare la password periodicamente.	Intervallo periodico	Gruppo criteri Password	60
Bloccare il dispositivo automaticamente dopo un periodo di inattività dell'utente.	Timeout di protezione massimo	Gruppo criteri Solo dispositivo	10

Crittografia dei dati su un dispositivo

Scenario	Regola dei criteri IT	Gruppo criteri	Valore
Proteggere l'utente e i dati delle applicazioni BlackBerry sul dispositivo BlackBerry.	Livello di protezione del contenuto	Protezione	Massima
Specificare gli algoritmi che il dispositivo utilizza per crittografare e decrittografare i messaggi codificati con PGP.	Crittografie del contenuto consentite per PGP	Applicazione PGP	AES (192 bit), AES (256 bit), AES (128 bit) e Triple DES
Specificare gli algoritmi che il dispositivo utilizza per crittografare e decrittografare i messaggi codificati con S/MIME.	Crittografie del contenuto consentite per S/MIME	Applicazione S/MIME	AES (192 bit), AES (256 bit), AES (128 bit) e Triple DES

Limitazione della messaggistica su un dispositivo

Scenario	Regola dei criteri IT	Gruppo criteri	Valore
Limitare la messaggistica su un dispositivo BlackBerry per i servizi di messaggistica che l'organizzazione può controllare.	Consenti altri servizi browser	Esclusività servizi	No
	Consenti altri servizi di messaggistica	Esclusività servizi	No
	Consenti messaggi peer-to-peer	Solo dispositivo	No
	Consenti SMS	Solo dispositivo	No
	Disattiva inoltro tra servizi	Protezione	Sì
	Disattiva Taglia/Copia/Incolla	Protezione	Sì
Richiedere che un utente BlackBerry invii i messaggi e-mail crittografati dal dispositivo.	Forza crittografia per messaggi S/MIME	Applicazione S/MIME	Sì
	PGP	Applicazione PGP	Sì
Impedire all'utente di inviare messaggi PIN.	Consenti messaggi peer-to-peer	Solo dispositivo	No
Impedire all'utente di inviare messaggi di testo SMS.	Consenti SMS	Solo dispositivo	No
Impedire all'utente di inoltrare o rispondere ai messaggi e-mail utilizzando un diverso servizio di messaggistica.	Disattiva inoltro tra servizi	Protezione	Sì

Precauzioni per evitare i pericoli derivanti da virus o utenti malintenzionati

Utilizzare le regole dei criteri IT e di controllo applicazioni per bloccare i pericoli derivanti da virus o altri attacchi di utenti malintenzionati.

Limitazione delle risorse a cui può accedere un'applicazione di terzi su un dispositivo

Scenario	Regola dei criteri di controllo applicazioni di esempio	Valore
Impedire alle applicazioni Java di terzi di accedere a un elenco di domini utilizzando BlackBerry Browser.	Elenco dei domini filtro browser	Indirizzi dei domini
Consentire a un'applicazione Java di terzi di inviare e ricevere messaggi su un dispositivo BlackBerry.	L'accesso all'API e-mail è consentito?	Autorizzazione concessa
Rimuovere un'applicazione Java di terzi dai dispositivi BlackBerry attraverso la rete wireless.	Disposizione	Autorizzazione non concessa
Consentire a un'applicazione Java di terzi di accedere all'applicazione telefono sui dispositivi BlackBerry.	L'accesso all'API telefono è consentito?	Autorizzazione concessa
Consentire a un'applicazione Java di terzi di creare connessioni di rete esterne pubbliche e consentire le connessioni ai domini esterni senza richiedere agli utenti la password sui propri dispositivi BlackBerry.	Le connessioni di rete esterne sono consentite?	Autorizzazione concessa
	Elenco dei domini esterni	Indirizzi dei domini esterni
Consentire a un'applicazione Java di terzi di stabilire connessioni ai dispositivi Bluetooth.	L'accesso all'API SPP (Serial Port Profile) per Bluetooth è consentito?	Autorizzazione concessa
	Le connessioni di rete esterne sono consentite?	Autorizzazione concessa

Scenario	Regola dei criteri di controllo applicazioni di esempio	Valore
Impedire agli utenti di attivare un tema personalizzato creato utilizzando Plazmic Content Developer's Kit.	I dati temi sono consentiti?	Autorizzazione non concessa
Impedire agli utenti di sbloccare i propri dispositivi BlackBerry utilizzando BlackBerry Smart Card Reader e una password di autenticazione.	L'accesso all'API autenticatore utente è consentito?	Autorizzazione non concessa

Limitazione del controllo utente in applicazioni di terzi installate sui dispositivi BlackBerry

Scenario	Regola dei criteri d'esempio	Valore
Impedire che le applicazioni di terzi possano accedere a porte seriali o USB sui dispositivi BlackBerry.	Consenti l'utilizzo della porta seriale ad applicazioni di terzi (regola dei criteri IT)	No
Impedire agli utenti di scaricare applicazioni di terzi o temi sui propri dispositivi BlackBerry.	Vieta download di applicazioni di terzi (Regola dei criteri IT)	Sì
Impedire agli utenti di rimuovere un'applicazione Java di terzi sui propri dispositivi BlackBerry.	Disposizione (regola dei criteri di controllo applicazioni)	Indispensabile
Impedire agli utenti di installare un'applicazione Java di terzi sui propri dispositivi BlackBerry.	Disposizione (regola dei criteri di controllo applicazioni)	Autorizzazione non concessa
Rimuovere un'applicazione Java di terzi dai dispositivi BlackBerry attraverso la rete wireless.	Disposizione (regola dei criteri di controllo applicazioni)	Autorizzazione non concessa
Impedire agli utenti di attivare un tema personalizzato creato utilizzando BlackBerry Theme Studio.	La regola dei criteri di controllo applicazioni personalizzate Dati temi è consentito?	Indispensabile
Impedire agli utenti di sbloccare i propri dispositivi BlackBerry utilizzando BlackBerry Smart Card Reader e una password di autenticazione.	L'accesso all'API autenticatore utente (regola dei criteri di controllo applicazioni) è consentito?	Indispensabile
Impedire agli utenti autenticati attraverso una connessione VPN di utilizzare applicazioni di terzi sui propri dispositivi BlackBerry.	L'accesso all'API autenticatore utente (regola dei criteri di controllo applicazioni) è consentito?	Indispensabile

Blocco dell'esecuzione di applicazioni RIM a valore aggiunto su dispositivi BlackBerry

È possibile utilizzare regole dei criteri di controllo applicazioni e regole dei criteri IT per controllare se le applicazioni Research In Motion a valore aggiunto sono disponibili sui dispositivi BlackBerry. Le applicazioni RIM a valore aggiunto includono BlackBerry Wallet ed il motore di ottimizzazione contenuti E-commerce per BlackBerry Browser.

Per impedire l'esecuzione di applicazioni RIM a valore aggiunto su BlackBerry Device Software in versioni antecedenti alla 4.5, è possibile bloccare tutte queste applicazioni utilizzando la regola dei criteri IT Disattiva Applicazioni RIM a valore aggiunto oppure è possibile bloccare specifiche applicazioni RIM a valore aggiunto utilizzando regole dei criteri IT per applicazioni specifiche.

Per impedire l'esecuzione delle applicazioni RIM a valore aggiunto su BlackBerry Device Software versione 4.5 o successive, è possibile utilizzare uno qualsiasi dei seguenti metodi specifici dell'applicazione:

Applicazione	Metodo
BlackBerry Wallet	• Configurare la regola dei criteri IT Disattiva BlackBerry Wallet su Sì. • Applicare un criterio di controllo applicazioni per bloccare tutte le applicazioni di terze parti o applicare un criterio di controllo delle applicazione per bloccare specifiche applicazioni RIM a valore aggiunto se si desidera rimuovere le applicazioni RIM a valore aggiunto dai dispositivi BlackBerry. • Configurare la regola dei criteri IT Disattiva applicazioni RIM a valore aggiunto su Sì.
motore ottimizzazione contenuti E-commerce per BlackBerry Browser	• Configurare la regola dei criteri IT Disattiva Motore ottimizzazione contenuti E-Commerce su Sì. • Applicare una regola di controllo applicazioni per bloccare tutte le applicazioni di terzi, o applicare una regola di controllo per bloccare specifiche applicazioni RIM a valore aggiunto se si desidera rimuovere le applicazioni RIM a valore aggiunto dai dispositivi BlackBerry. • Configurare la regola dei criteri IT Disattiva applicazioni RIM a valore aggiunto su Sì.

È possibile applicare la proprietà Disposizione dei criteri di controllo applicazioni solo alle applicazioni RIM a valore aggiunto. Altre regole dei criteri di controllo applicazioni non si applicano alle applicazioni RIM a valore aggiunto.

Glossario

8

AES	Advanced Encryption Standard
API	Application Programming Interface
BIP	Protocollo BIP (Bearer Independent Protocol)
CAST	Computer Assisted Seriation Test
DES	Data Encryption Standard
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
EAP-LEAP	Extensible Authentication Protocol Lightweight Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography (crittografia a curva ellittica)
FTP	Protocollo di trasferimento dei file
Gateway Message Envelope (GME)	Il protocollo Gateway Message Envelope è un protocollo proprietario di Research In Motion che consente il trasferimento di dati compressi e crittografati tra la rete wireless e i dispositivi BlackBerry. Questo protocollo definisce un livello di instradamento che specifica i tipi di contenuto dei messaggi consentiti e le informazioni di indirizzamento dei dati. I gateway e altri componenti di instradamento utilizzano queste informazioni per identificare il tipo e l'origine dei dati dei dispositivi BlackBerry, nonché per stabilire il servizio di destinazione appropriato al quale indirizzarli.
GPS	Global Positioning System
HTML	Hypertext Markup Language
IP	Internet Protocol
IT	Information Technology
MFH	messaggio dal dispositivo
MMS	Multimedia Messaging Service (servizio di messaggistica multimediale)
MTH	messaggio al dispositivo
NFC	Near Field Communication
PIM	Personal Information Management

PIN	Personal Identification Number (numero identificativo personale)
RC	Rivest's Cipher
S/MIME	Secure Multipurpose Internet Mail Extensions
SMS	Short Message Service (servizio messaggi brevi)
SPP	Profilo porta seriale
TCP	Transmission Control Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network (rete privata virtuale)
WAN	Wide Area Network (rete geografica)
WAP	Wireless Application Protocol
xAuth	Extended Authentication (autenticazione estesa)

Note legali

9

©2012 Research In Motion Limited. Tutti i diritti riservati. BlackBerry®, RIM®, Research In Motion® e i relativi marchi, nomi e logo sono di proprietà di Research In Motion Limited e sono registrati e/o utilizzati negli Stati Uniti e in altri Paesi.

Bluetooth è un marchio di Bluetooth SIG. Entrust e Entrust Entelligence sono marchi di Entrust, Inc. IrDA è un marchio di Infrared Data Association. PGP è un marchio di PGP Corporation. Plazmic è un marchio di Plazmic, Inc. Roxio è un marchio di Sonic Solutions. RSA e RSA SecurID sono marchi di RSA Security. IBM, Domino, Lotus e Lotus Notes sono marchi registrati di International Business Machines Corporation. Java e JavaScript sono marchi di Oracle America, Inc. Wi-Fi è un marchio di Wi-Fi Alliance. Tutti gli altri marchi sono di proprietà dei rispettivi titolari.

La presente documentazione, compresa tutta la documentazione ivi allegata come riferimento, ad esempio la documentazione fornita o resa disponibile sul sito www.blackberry.com/go/docs, viene fornita o resa accessibile "COSÌ COM'È" e "SE DISPONIBILE" e senza alcuna condizione, approvazione, garanzia o dichiarazione di alcun tipo da parte di Research In Motion Limited e delle relative società affiliate ("RIM") e RIM non si assume alcuna responsabilità per errori tipografici, tecnici o per altre imprecisioni, errori od omissioni presenti nella documentazione. Al fine di tutelare le informazioni proprietarie e riservate e/o i segreti commerciali di RIM, è possibile che alcuni aspetti delle tecnologie di RIM vengano descritti in modo generico nella presente documentazione. RIM si riserva il diritto di modificare periodicamente le informazioni contenute nella presente documentazione, senza alcun obbligo di distribuzione agli abbonati di modifiche, aggiornamenti, miglioramenti o aggiunte al documento in tempo utile.

La presente documentazione potrebbe contenere riferimenti a fonti di informazioni, hardware o software, prodotti o servizi di terzi, compresi componenti e contenuti protetti da copyright e/o siti Web di terzi (collettivamente denominati "Prodotti e servizi di terzi"). RIM non controlla né è responsabile per eventuali Prodotti e servizi di terzi, inclusi, senza alcuna limitazione, il contenuto, l'accuratezza, la conformità al copyright, le prestazioni, la compatibilità, l'affidabilità, la legalità, la decenza, i collegamenti o qualsiasi altro aspetto dei Prodotti e servizi di terzi. La presenza di riferimenti a Prodotti e servizi di terzi nella presente documentazione non implica in nessun caso l'approvazione da parte di RIM dei Prodotti e servizi di terzi o dei terzi.

A MENO CHE LE LEGGI APPLICABILI NELLA GIURISDIZIONE VIGENTE LO PROIBISCANO, CON IL PRESENTE DOCUMENTO SI ESCLUDONO TUTTE LE CONDIZIONI, APPROVAZIONI, GARANZIE, DICHIARAZIONI IMPLICITE O ESPLICITE DI OGNI GENERE, COMPRESE, SENZA ALCUNA LIMITAZIONE, LE CONDIZIONI, APPROVAZIONI, GARANZIE, DICHIARAZIONI O GARANZIE DI DURATA, IDONEITÀ A UN PARTICOLARE SCOPO O USO, COMMERCIABILITÀ, QUALITÀ, NON VIOLAZIONE, QUALITÀ SODDISFACENTE O TITOLO, OVVERO DERIVANTI DA STATUTI O USANZE COMMERCIALI O USI DI COMMERCIO, O ANCORA CORRELATE ALLA DOCUMENTAZIONE O ALL'USO DI QUESTA, OVVERO ALLE PRESTAZIONI O ALLE MANCATE PRESTAZIONI DI SOFTWARE, HARDWARE, SERVIZI O QUALSIASI TIPO DI PRODOTTI E SERVIZI DI TERZI IVI NOMINATI. L'UTENTE POTREBBE INOLTRE GODERE DI ULTERIORI DIRITTI A SECONDA DELLO STATO O DELLA PROVINCIA DI APPARTENENZA. È POSSIBILE CHE ALCUNE GIURISDIZIONI NON CONSENTANO L'ESCLUSIONE O LA LIMITAZIONE DI GARANZIE E CONDIZIONI IMPLICITE. NEI LIMITI CONSENTITI DALLA LEGGE, TUTTE LE GARANZIE E CONDIZIONI IMPLICITE IN RELAZIONE ALLA PRESENTE DOCUMENTAZIONE, CONSIDERANDO CHE LA LORO ESCLUSIONE NON È CONCESSA, IN BASE A QUANTO SPECIFICATO PRIMA, MENTRE LA LORO

LIMITAZIONE È CONCESSA, VENGONO QUI LIMITATE A NOVANTA (90) GIORNI A PARTIRE DALLA DATA DI ACQUISTO DELLA DOCUMENTAZIONE O L'ELEMENTO OGGETTO DELLA LAMENTELA.

ENTRO I LIMITI MASSIMI CONSENTITI DALLE LEGGI APPLICABILI NELLA GIURISDIZIONE VIGENTE, RIM NON PUÒ ESSERE IN NESSUN CASO RITENUTA RESPONSABILE DI QUALSIASI TIPO DI DANNI RELATIVI ALLA PRESENTE DOCUMENTAZIONE O ALL'USO DI QUESTA, OVVERO ALLE PRESTAZIONI O MANCATE PRESTAZIONI DI QUALSIASI SOFTWARE, HARDWARE, SERVIZIO O QUALSIASI DEI PRODOTTI E SERVIZI DI TERZI DI CUI SOPRA, COMPRESI, SENZA LIMITAZIONE, I DANNI SEGUENTI: DIRETTI, CONSEQUENZIALI, ESEMPLARI, INCIDENTALI, INDIRETTI, SPECIALI, PUNITIVI O AGGRAVATI, DANNI DERIVANTI DALLA PERDITA DI RICAVI O PROFITTI, MANCATA REALIZZAZIONE DEI GUADAGNI PREVISTI, INTERRUZIONE DELL'ATTIVITÀ COMMERCIALE, PERDITA DI INFORMAZIONI COMMERCIALI, PERDITA DI OPPORTUNITÀ COMMERCIALI OVVERO DANNEGGIAMENTO O PERDITA DI DATI, MANCATA TRASMISSIONE O RICEZIONE DI DATI, PROBLEMI ASSOCIATI A QUALSIASI DELLE APPLICAZIONI UTILIZZATE CON I PRODOTTI O I SERVIZI RIM, COSTI DERIVANTI DA TEMPI MORTI, MANCATO USO DEI PRODOTTI O DEI SERVIZI RIM O DI PARTI DI ESSI OVVERO DI QUALSIASI SERVIZIO DI DISPONIBILITÀ, COSTO DI SERVIZI SOSTITUTIVI, COSTI DI COPERTURA, STRUTTURE O SERVIZI, COSTI DI CAPITALE OVVERO ALTRE PERDITE DI CARATTERE PECUNIARIO DI TALE TIPO, SIA NEL CASO IN CUI TALI DANNI SIANO PREVISTI CHE NEL CASO IN CUI NON LO SIANO, E ANCHE QUALORA RIM SIA STATA AVVISATA DELLA POSSIBILITÀ DEL VERIFICARSI DI TALI DANNI.

NEI LIMITI MASSIMI CONSENTITI DALLE LEGGI APPLICABILI NELLA GIURISDIZIONE VIGENTE, RIM NON HA NESSUN ALTRO OBBLIGO, DOVERE O RESPONSABILITÀ RELATIVAMENTE ALL'ADEMPIMENTO DEL CONTRATTO, NEGLIGENZA O ALTRO NEI CONFRONTI DELL'UTENTE, COMPRESA LA RESPONSABILITÀ PER NEGLIGENZA O COMPATIBILITÀ.

LE LIMITAZIONI, ESCLUSIONI ED ESCLUSIONI DI RESPONSABILITÀ RIPORTATE NEL PRESENTE DOCUMENTO SI APPLICANO: (A) INDIPENDENTEMENTE DALLA NATURA DELLA CAUSA DELL'AZIONE, DELLA RICHIESTA O DELL'AZIONE INTRAPRESA DALL'UTENTE, COMPRESE, SENZA LIMITAZIONE, LA VIOLAZIONE DEL CONTRATTO, LA NEGLIGENZA, LE AZIONI LESIVE, LA COMPATIBILITÀ O QUALSIASI ALTRO DANNO CONTEMPLATO DALLA LEGGE E RIMARRANNO IN VIGORE IN SEGUITO A VIOLAZIONI DI FONDO O AL MANCATO ADEMPIMENTO DELLO SCOPO ALLA BASE DEL PRESENTE CONTRATTO O DI QUALSIASI CLAUSOLA IN ESSO PRESENTE; E (B) A RIM E ALLE RELATIVE SOCIETÀ AFFILIATE, AI SUCCESSORI DI QUESTE, AI CESSIONARI, AGLI AGENTI, AI FORNITORI (IVI COMPRESI I PROVIDER DI SERVIZI), AI RIVENDITORI AUTORIZZATI RIM (IVI COMPRESI I PROVIDER DI SERVIZI) E AI RISPETTIVI DIRETTORI, DIPENDENTI E COLLABORATORI INDIPENDENTI.

OLTRE ALLE LIMITAZIONI ED ESCLUSIONI DI CUI SOPRA, IN NESSUN CASO SUI DIRETTORI, I DIPENDENTI, GLI AGENTI, I RIVENDITORI, I FORNITORI, I COLLABORATORI INDIPENDENTI DI RIM O TUTTI GLI AFFILIATI DI RIM RICADRÀ LA RESPONSABILITÀ DERIVANTE DA O CORRELATA ALLA PRESENTE DOCUMENTAZIONE.

Prima della sottoscrizione, dell'installazione o dell'utilizzo di Prodotti e servizi di terzi, è responsabilità dell'utente assicurarsi che il provider di servizi garantisca il supporto di tutte le relative funzioni. Alcuni provider di servizi potrebbero non offrire la funzionalità di esplorazione in Internet con un abbonamento a BlackBerry® Internet Service. Verificare con il provider di servizi la disponibilità, le disposizioni di roaming, i piani di servizio e le funzionalità. Per l'installazione o l'utilizzo di Prodotti e servizi di terzi con prodotti e servizi RIM potrebbero essere necessari uno o più brevetti, marchi, copyright o licenze di altro tipo al fine di evitare violazioni dei diritti di terzi. L'utilizzo di Prodotti e servizi di terzi e l'eventuale necessità di licenze di terzi sono responsabilità esclusive dell'utente. Nel caso in cui sia necessario, l'utente è responsabile del relativo acquisto. L'utente non deve installare o utilizzare Prodotti e servizi di terzi fino all'acquisto delle relative licenze richieste. Tutti i Prodotti e servizi di terzi forniti con i prodotti e i servizi RIM hanno lo scopo di offrire maggiore comodità all'utente e vengono forniti "COSÌ COME SONO", senza condizioni, approvazioni, garanzie, dichiarazioni espresse o implicite di qualsiasi tipo da parte di RIM. RIM non si assume nessun tipo di responsabilità a tale riguardo. L'utilizzo da

parte dell'utente di Prodotti e servizi di terzi deve essere sottoposto e soggetto all'accettazione da parte dell'utente stesso dei termini di licenze indipendenti e altri contratti ivi applicabili con terzi, salvo quanto espressamente coperto da eventuali licenze o altri contratti stipulati con RIM.

Alcune funzionalità illustrate nella presente documentazione richiedono una versione minima del software BlackBerry® Enterprise Server, BlackBerry® Desktop Software, e/o BlackBerry® Device Software.

I termini di utilizzo di tutti i prodotti o servizi RIM vengono definiti in una licenza o in un altro contratto indipendente stipulato con RIM ivi applicabile. NESSUNA AFFERMAZIONE CONTENUTA NELLA PRESENTE DOCUMENTAZIONE PUÒ SOSTITUIRE CONTRATTI O GARANZIE SCRITTE ESPLICITE FORNITE DA RIM PER PARTI DI PRODOTTI O SERVIZI RIM DIVERSI DA QUELLI INDICATI NELLA PRESENTE DOCUMENTAZIONE.

Research In Motion Limited
295 Phillip Street
Waterloo, ON N2L 3W8
Canada

Research In Motion UK Limited
Centrum House
36 Station Road
Egham, Surrey TW20 9LF
Regno Unito

Pubblicato in Canada