

# Blockbit UTM versão 1.2.0

A tabela a seguir lista as melhorias realizadas no release do Blockbit UTM versão 1.2.0

<b>Controle de acesso para visitantes no Captive Portal</b> É possível especificar para qual rede o Captive Portal pode ser habilitado.
<b>Melhoria e Reestruturação do Dashboard</b> Adicionamos novos widgets para visualização de informações e reformulamos o dashboard. Criamos um novo dashboard para mostrar informações do sistema.
<b>Integração com Servidor RADIUS</b> Agora é possível autenticar usuários do BLOCKBIT UTM em servidores RADIUS (Remote Authentication Dial In User Service).
<b>HA com persistência de sessão</b> O recursos de alta disponibilidade (HA – high availability) agora tem suporte ao sincronismo de sessão de conexões e logins.
<b>Identificador de complexidade de senhas</b> A interface mostra agora o nível de complexidade na senha escolhida pelo usuário durante o cadastro.
<b>Notificação de atualizações na base do IPS</b> As atualizações da base do IPS (Intrusion Prevention System) agora contam com alertas automáticos de sistema para notificar o administrador.
<b>Agrupamento de Políticas</b> Para melhorar o gerenciamento das políticas de segurança, implementamos o agrupamento de políticas, que podem ser implementadas em conjunto para diferentes recursos.
<b>Antimalware para HTTP/S</b> O BLOCKBIT UTM agora possui recursos antimalware nos protocolos HTTP e HTTPS, bloqueando o download de arquivos infectados e a execução de arquivos PUA maliciosos. O novo recurso inclui detecção com análise heurística e varredura de arquivos protegidos por senha.
<b>Relatório de Varredura Antimalware</b> Implementamos a criação de um relatório com os resultados da varredura de arquivos executada pelo recurso antimalware.
<b>Quarentena de Antimalware</b> O novo recurso de quarentena permite armazenar arquivos marcados como suspeitos pelo antimalware. O download pelo usuário só é liberado após a varredura do conteúdo e confirmação de que não há ameaças.
<b>Monitor de sessões</b> Implementamos um novo recurso de monitoria de sessões em tempo real que registra o tráfego de e para as conexões de rede do ambiente.
<b>Filtro de conteúdo HTTPS através da Autoridade Certificadora</b> Permite fazer filtro de conteúdo através da autoridade certificadora (CN, DN e O).
<b>Desativação da Sumarização de Aplicativos Web</b> Agora é possível desabilitar a sumarização de aplicativos web por política o que possibilita máximo desempenho geral do sistema.
<b>Desativação Global para o Serviço de Decriptação SSL</b> Agora é possível desabilitar a decriptação SSL do sistema de acordo com as regras de negócio, permitindo o uso de políticas de segurança sem a aplicação de certificados.
<b>Desativação do Update Automático</b> O administrador agora pode optar por desabilitar os updates automáticos do sistema.
<b>Serviço SSO com RADIUS</b> O novo recurso permite realizar SSO (Single Sign-on) através de servidores de autenticação RADIUS (Remote Authentication Dial In User Service) – RSSO.
<b>Desativação de Sumarização de Serviços</b> O novo recurso permite desabilitar a sumarização de serviços para obter o máximo de desempenho (throughput) em uma rede.
<b>Desativação de Interceptação SSL por Domínio</b> Agora é possível realizar bypass da interceptação SSL através de domínio.
<b>Link Aggregation em VLAN</b> O novo recurso permite suporte ao protocolo de link aggregation em interfaces VLAN.
<b>Objeto de Content-Type</b> Realizamos uma modificação que permite a interface de gerenciamento de content-type suportar extensão de arquivos.
<b>DHCP Relay</b> Agora foi Incluído o suporte a DHCP Relay no serviço de DHCP.