Material Técnico

BluePex® Endpoint Control

BluePex®

Endpoint Control

O Endpoint Control é responsável pelo monitoramento dos dados do computador do usuário. Estes dados são coletados e enviados para a Suíte a fim de exibi-los de uma forma centralizada e simples ao administrador.

Além do monitoramento, o Endpoint Control, também pode realizar algumas ações, como instalar o Endpoint Protection, remover programas, desligar, reiniciar, abrir o acesso remoto, entre outras.

Instalação

Ao realizar o download do instalador do Endpoint Control, ele virá com o seguinte formato de nomenclatura: Setup_1234abcd123abc12ab1a.msi , onde não deve ser renomeado em hipótese alguma, visto que " o que está escrito após o **Setup**_", é o serial da empresa e qualquer alteração nestes dados pode fazer com que o dispositivo não se comunique corretamente com a Suíte.

A instalação é simples, basta clicar no executável que ele irá realizar a instalação, porém é preciso ter acesso administrativo para realizar a instalação.

O dispositivo deve possuir pelo menos a versão .NET Framework 4.5.2 para que seja realizado a instalação, porém recomendamos ao menos a versão 4.7.2 para que o acesso remoto funcione corretamente.

As versões do Windows homologadas para o funcionamento do Endpoint Control são: Windows 7, Windows 8, Windows 10, Server 2008 R2, Server 2012, Server 2016 e Server 2019, nas plataformas i386 e x64.

Existe também uma versão para XP, Vista e Server 2008, no entanto ela apenas realiza o monitoramento, porém esta versão não será abordado neste momento.

Ao instalar o Endpoint Control, é gerado um ID para o dispositivo que é único, inclusive, mesmo desinstalando o programa, este ID é mantido em caso de uma nova reinstalação.

Será instalado no dispositivo um executável com interface gráfica, que ficará em execução na área de notificação da barra de tarefas do Windows. Após a instalação é recomendado executar o atalho na área de trabalho chamado "BluePex Endpoint", para que este executável seja aberto, porém o instalador já define como um programa que será aberto toda vez que o Windows seja iniciado. Após aberto este programa está sempre em execução, não sendo possível fechá-lo pela interface (ele será ficará novamente na área de notificação da barra de tarefas).

Outro recurso que serão instalado e ficará em execução é o serviço do Endpoint Control. Ele é executado automaticamente, não sendo necessário nenhuma interação para sua execução.

Endpoint Control (Serviço)

O serviço do endpoint control é responsável pela coleta de dados e execução dos comandos e seu funcionamento se dá da seguinte maneira:

Quando o serviço se inicializa, ele cria um agendamento para verificar o status da execução desse serviço à cada 30 minutos, garantindo que se caso o serviço para de executar por algum motivo, ele seja iniciado novamente. Além disso, ele inicializa após 60 segundos os sub-serviços, esses responsáveis pelas coletas, comandos, verificações e outros.

Coleta de inventário

A coleta de inventário é executada na inicialização e após isso uma vez a cada 24 horas de forma automática, porém é possível coletar novamente de forma manual pela Suíte.

Coleta de dados

A coleta geral de dados é executada em média a cada 2 minutos, porém este tempo pode variar caso o dispositivo esteja com a capacidade de processamento ou memória com bastante uso no momento, fazendo com que a coleta leve mais tempo do que o normal. Nestes casos o serviço se ajusta para manter uma média de execução, de acordo com a capacidade do dispositivo. É possível configurar na Suíte o tempo de inatividade de acordo com o dispositivo, para que ele não seja exibido como offline em casos que leve um tempo maior para esta coleta.

Execução de Comandos

É mantida uma conexão via socket com nossos servidores em que ao receber um comando, o serviço inicializa a execução do mesmo e ao mesmo tempo informa ao servidor o status da execução deste comando. Caso a conexão caia, é feita uma nova tentativa de conexão a cada 60 segundos.

Diagnóstico

A cada 10 minutos é feita uma verificação do status das conexões com os nossos servidores e caso apresente alguma falha, é exibido tanto no log quanto na interface gráfica do Endpoint Control.

Produtividade

Caso o módulo de produtividade esteja habilitado (o módulo é habilitado por padrão), será feito o envio dos dados de produtividade para a Suíte à cada 5 minutos. Os dados são obtidos e gerados pela interface gráfica do Endpoint Control, portanto é necessário que ele esteja em execução para esta coleta.

Caso não seja possível o envio dos dados, devido a algum problema de conexão, os dados são salvos para envio posterior, ocorrendo após o envio com sucesso dos dados novos.

Template

Quando o serviço do Endpoint Control é inicializado, após 5 minutos ele irá verificar se existe algum template gerado para o território (no Cloud Suíte) em que este endpoint encontra-se e caso exista, ele irá aplicar este template. Uma vez aplicado esta verificação não ocorrerá novamente.

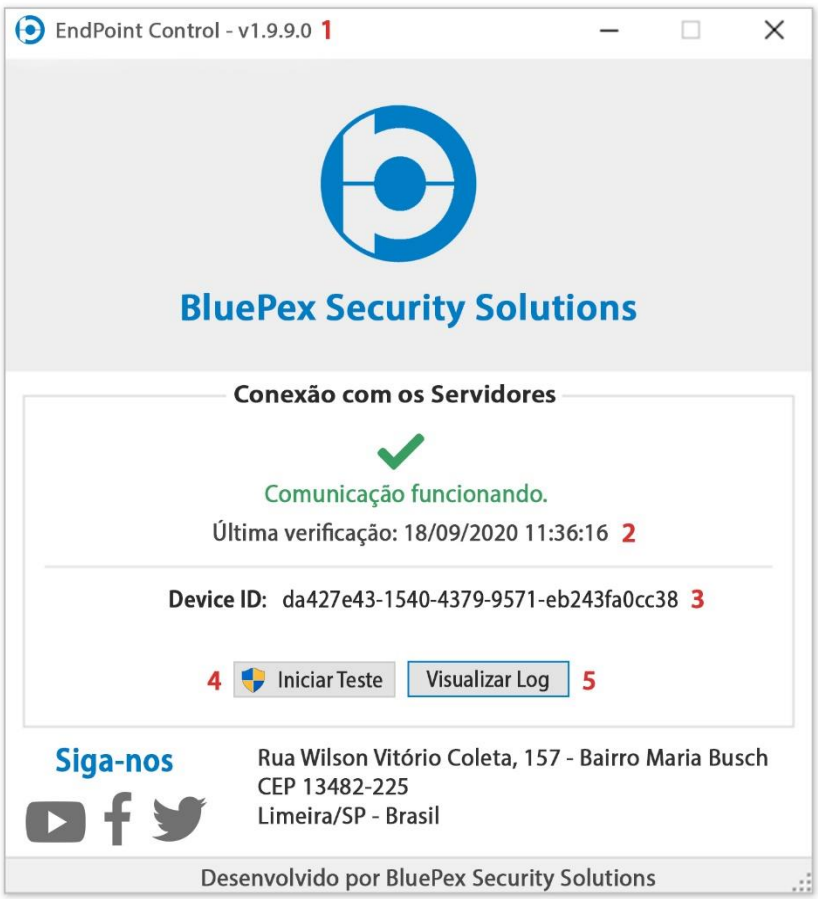
O template é configurado no Cloud Suíte através das políticas e caso queira forçar a aplicação do template, basta enviar o comando de aplicar política pelo Cloud Suíte que o template será executado novamente.

Atualmente o template irá configurar se o módulo de produtividade será habilitado ou desabilitado (o padrão é habilitado) e também irá realizar a instalação do Endpoint Protection caso definido para instalar (o padrão é não instalar).

Endpoint Control (Interface Gráfica)

A interface gráfica do Endpoint Control é inicializada automaticamente junto com a inicialização do sistema operacional, bem como é inicializada de forma minimizada, sendo localizada na área de notificação da barra de tarefas do Windows, e podendo ser aberto clicando sobre este ícone ou sobre o ícone “BluePex Endpoint” localizado na área de trabalho.

O Endpoint Control possui a seguinte identidade visual:



1) No título do programa é exibido a versão instalada em seu dispositivo, no caso v.1.9.9.0.
2) Neste local aparece o diagnóstico da conexão do dispositivo com os nossos servidores, quando tudo está funcionando aparece como na imagem, caso não haja a conexão com um ou mais servidores, será exibido a seguinte mensagem:
   “Comunicação falhou para X de 4 servidores” (Os detalhes da falha pode ser visualizado no log). A data e hora exibida é a data e hora em que foi realizado o último teste de conexão em nossos servidores.
3) Exibe o Device ID do dispositivo. Esse ID é único por dispositivo e não pode ser alterado. Ao clicar 2x sobre o ID o valor é copiado para a área de transferência. Esse ID pode ser utilizado para localizar o dispositivo na Suíte.
4) O botão “Iniciar Teste” realiza um novo teste manual na conexão com os servidores. É preciso ter permissão administrativa para executar esta ação.
5) O botão “Visualizar Log” abre uma janela contendo o log do dia. Esta nova janela não é atualizada automaticamente, sendo necessário fechar e abrir novamente para ver o log atualizado.

Atualização

O Endpoint Control é atualizado automaticamente quando lançado uma nova versão, não sendo necessário nenhuma ação manual para isto. A interface gráfica do Endpoint Control não é aberta automaticamente após a atualização, portanto é necessário abrir novamente manualmente ou reiniciar o computador.

Possíveis problemas e soluções

O Endpoint Control foi instalado e não comunica com a Suíte

Após a instalação, o dispositivo deverá aparecer na Suíte em torno de 10 minutos, se após este tempo ele não aparecer efetue as seguintes verificações:

1. Verifique se o serial é válido:

   É possível verificar essa informação pela interface gráfica, caso o serial seja inválido, será exibido “Serial Inválido” em vermelho logo abaixo do Device ID.

   Caso esta mensagem esteja aparecendo, basta baixar novamente o instalador, verificar se a nomenclatura está correta, desinstalar a versão atual e instalar novamente.

2. Verificar o horário do dispositivo:

   O dispositivo deve estar com o horário correto.

3. Verificar o status das conexões:

   Para que o dispositivo se comunique com a Suíte, é preciso que ele esteja conseguindo conectar aos nossos servidores de dados. É possível verificar o status da conexão na interface gráfica, se aparece falha para 1 ou mais conexões, pode estar havendo algum bloqueio ou outro problema.

   Verifique se há algum bloqueio nas conexões, se possuir proxy, é preciso efetuar a liberação dos seguintes endereços:

   suiteapi.bluepex.com.br
   cdn.bluepex.com.br
   mq.bluepex.com.br
   endpointchat.bluepex.com.br

   Para testar novamente a conexão, basta clicar no botão ”Iniciar Teste” na interface gráfica.

4. Verificar se o Windows está fornecendo acesso aos dados para coleta:

   Acessar o prompt de comando executando como administrador

   Acessar o caminho: C:\Program Files\Bluepex Security Solutions\Bluepex Endpoint

   Executar o seguinte comando: SuiteTasker.exe /logs json

   Caso dê tudo certo, aparecerá após alguns minutos a seguinte mensagem:

   Updating json file...
   01-Uptime
   02-IP
   03-Disk
   04-Public Interfaces
   05-Private Interfaces
   06-Top Process
   07-Datetime
   08-Services
   09-Memory
   10-CPU
   11-User
   12-Antivirus
   13-WinLicense
   14-Policies
   15-Colect Antimalware info All
   items collected
   json file updated

* Pode aparecer uma falha no item 15 caso você não possua o nosso Endpoint Protection instalado, mas isso não afeta em nada.

Caso não fique desta forma, ou se travar em algum item (o item 6 e 13 demoram mais para sua coleta, mas isso não é um problema, porém normalmente o travamento se dá no item 6), onde é necessário executar o seguinte comando para que o Windows reconstrua todos os contadores de desempenho e seja possível coletar os dados novamente:

lodctr /r

Após a execução, o processo leva alguns segundos e aparecerá a seguinte mensagem em caso de sucesso:

Info: Configuração do contador de desempenho reconstruída com sucesso a partir do repositório de backup do sistema

Feito isso, basta rodar novamente o comando “SuiteTasker.exe /logs json“ e assim verificar se gerou corretamente desta vez.

5. Reiniciar o dispositivo:

Esta etapa pode ser necessária caso tenha sido efetuado o item 3 e mesmo assim não houve a comunicação.

É possível reiniciar o serviço do Endpoint Control também, mas somente faça isso caso não seja possível reiniciar o dispositivo.

Para reiniciar o serviço, basta executar o comando como administrador “services.msc”. Nesta tela, localize e selecione o serviço “BluePex Endpoint” e clique em Reiniciar o serviço.

O Endpoint Control parou de comunicar-se com a Suíte

Se por algum motivo o endpoint parou de se comunicar com a Suíte, ou seja, ele está ligado porém na Suíte consta como sem comunicação, efetue os seguintes procedimentos:

1. Verifique o status da conexão conforme descrito em “O Endpoint Control foi instalado e não comunica com a Suíte”.

2. Verificar o horário do dispositivo:

O dispositivo deve estar com o horário correto.

3. Verifique se o dispositivo está levando muito tempo para gerar os dados:

   O Endpoint Control, leva uma média de 2 minutos para coletar os dados do dispositivo e enviá-los para a Suíte, porém este tempo pode variar caso o dispositivo esteja com a capacidade de processamento ou memória com bastante uso no momento, aumentando assim o tempo para a coleta e envio de dados. Acessando o log é possível verificar os envios pelo seguinte registro:

   2020-09-18 11:36:16.3585 - INFO: Information successfully published

   Neste caso, a informação foi publicada às 11:36:16 do dia 18/09/2020, a próxima execução deverá ocorrer em aproximadamente 2 minutos após esta, porém se o intervalo de envio estiver muito grande é possível que a média de tempo tenha sido alterada em algum momento, esta informação é registrada no log, porém a maneira mais simples de verificar o tempo médio é o seguinte:

   Acessar o prompt de comando executando como administrador.

   Acessar o caminho: C:\Program Files\Bluepex Security Solutions\Bluepex Endpoint

   Executar o seguinte comando: SuiteTasker.exe /diag show

   Serão exibidos alguns dados, mas o importante neste caso é o seguinte dado:

   Current avgInterval: 33910

   Se este valor for maior do que 120000 (2 minutos), então é este o intervalo que estão sendo coletados os dados. Este valor está em milissegundos, portanto basta dividir por 60000 para saber o valor em segundos.

   Caso o tempo esteja elevado, ao ponto de passar de horas, por exemplo, o ideal é reiniciar o dispositivo ou o serviço, a fim de que este valor seja resetado ao seu valor original, porém existe uma verificação para que se o intervalo seja maior do que 1 hora, ele é resetado automaticamente para o intervalo padrão de 2 minutos.

   É importante salientar que o próprio Endpoint Control realiza ajustes neste intervalo baseado no tempo de coleta, que irá diminuir ou aumentar conforme o próprio dispositivo, mas nunca será menor do que 2 minutos.

4. Verificar se o Windows está fornecendo acesso aos dados para coleta conforme descrito em “O Endpoint Control foi instalado e não comunica com a Suíte”.

5. Verificar no arquivo de log se o seguinte conjunto de erros está aparecendo:
   INFO: Starting Install Service
   ERROR: Installation failure with unknown error
   ERROR: Não é possível parar o serviço SimAgent no computador '.'.

Neste caso, o controlador de serviço do Windows congelou o processo do Endpoint Control então o sistema de reinício do serviço não consegue ser efetuado com sucesso.

Este problema pode ser resolvido apenas reiniciando o dispositivo (No Windows 10, desligar o dispositivo não faz o reinício dos processos, visto que ele suspende a execução e ativa novamente quando liga, como um processo de hibernação para acelerar o início do sistema operacional).

Se, por algum motivo, não for possível reiniciar o dispositivo, é possível fazer o processo manualmente, da seguinte forma:

- Acesse o Regedit como administrador
- Acesse o seguinte caminho:
  Dispositivos x64:
  HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Bluepex Security Solutions\SimAgent
  Dispositivos i386:
  HKEY_LOCAL_MACHINE\SOFTWARE\Bluepex Security Solutions\simagent
- Verifique a chave NeedRestart, se estiver em 1, mude para 0 e salve.
- Abra o gerenciador de tarefas, e finalize a tarefa “SimAgent.exe”, aguarde alguns segundos que o processo iniciará novamente, não estando mais congelado.

Verificação de Log

O Endpoint Control armazena diariamente arquivos de logs contendo os principais eventos, falhas e erros caso ocorram. O arquivo de log pode ser visualizado através da interface gráfica do Endpoint Control, no botão “Visualizar Log”, já os logs mais antigos ficam armazenados no seguinte diretório: %programdata%\Bluepex

O arquivo do dia possui o nome BluePexEP.log, já os demais apresentam desta forma: BluePexEP_2020-05-08.00.log (O arquivo foi renomeado no dia 18, porém o conteúdo é do dia anterior, no caso dia 17, ou seja, o nome é sempre do dia posterior ao log gerado).

Através do log é possível observar vários eventos que ajudam na verificação de possíveis problemas caso esteja ocorrendo.

Segue os principais eventos e seus significados:

- INFO: Information successfully published
  Os dados do dispositivo foram enviados para a Suíte com sucesso.

- INFO: Publishing Hardware and Software inventory
  O sistema está iniciando a coleta de inventário.

- INFO: Hardware and Software inventory was published
  O inventário foi publicado com sucesso.

- INFO: Checking new version of agent and view
  Está sendo verificado se existe uma nova versão do Endpoint Control.

- INFO: There is a new version for Bluepex Endpoint, starting upgrade!
  Existe uma nova versão, e foi inicializado o processo de upgrade.

- INFO: Start Diagnostic Check
  Iniciado o processo de diagnóstico de conexão com os servidores.

- INFO: Checking Server API
  Está sendo verificado pelo Diagnostic Check o servidor de API, caso ocorra algum erro, este estará abaixo deste registro.

- INFO: Checking Server CDN
  Está sendo verificado pelo Diagnostic Check o servidor de CDN, caso ocorra algum erro, este estará abaixo deste registro.

- INFO: Checking Server MQ
  Está sendo verificado pelo Diagnostic Check o servidor de MQ, caso ocorra algum erro, este estará abaixo deste registro.

- INFO: End Diagnostic Check
  Fim do processo de diagnóstico de conexão.

- INFO: WebSocket - Connected
  A conexão com o WebSocket foi realizada.

- INFO: WebSocket - Communication finished
  A conexão com o WebSocket foi finalizada. Isso pode acontecer quando o dispositivo estiver sendo desligado ou se houver uma queda na conexão, no caso de queda, o serviço irá reconectar novamente após 60 segundos.

- INFO: Scheduled a Installation Health Check with action: C:\Program Files\Bluepex Security Solutions\Bluepex Endpoint\\SuiteTasker.exe /check
  Ao inicializar o serviço, foi agendado o Health Check que verifica a cada 30 minutos se o serviço está em execução, ou caso ocorra algum travamento do serviço, para que ele seja reiniciado automaticamente.

- INFO: Bluepex Endpoint service successfully restarted
  O serviço do Endpoint Control foi reiniciado com sucesso.

- INFO: The computer is about to enter a suspended state
  O computador está sendo desligado (Windows 10) ou está entrando em modo de Suspensão.

- INFO: Command: get-inventory, Status: starting
  Informação sobre um comando enviado e seu status.

- INFO: Post Online
  Informa a Suíte que o dispositivo está Online.

- INFO: Post Offline
  Informa a Suíte que o dispositivo está Offline.

- INFO: Productivity newer successfully published
  Os novos dados de produtividade foram enviados para a Suíte com sucesso

- INFO: Productivity prod_AAAAMMDD successfully published
  Os dados antigos de produtividade foram enviados para a Suíte com sucesso

- WARN: The time elapsed to get information was above the default, elapsed: 130950,4513, default: 120000.
  O intervalo para coleta de dados foi alterado de 120000 milissegundos (2 minutos) para 130950 milissegundos (2min18seg).

- WARN: Bluepex Endpoint service needs to restart, working on it
  O serviço precisa ser reiniciado e está trabalhando nisto.

- WARN: Bluepex Endpoint service is not Running, trying to start it
  O serviço não está rodando e será reiniciado.

- WARN: Falha: BrokerUnreachable, ao conectar ao host
  Não foi possível conectar ao servidor MQ.
  Se ocorrer com frequência, verifique sua conexão e também um possível bloqueio por Firewall/Antivírus.

- WARN: Message: O nome remoto não pôde ser resolvido: 'suiteapihom.bluepex.com.br', Dica: verifique se nenhum Firewall/Antivírus está bloqueando o acesso!
  Não foi possível conectar ao servidor de API.
  Se ocorrer com frequência, verifique sua conexão e também um possível bloqueio por Firewall/Antivírus.

- WARN: Message: O nome remoto não pôde ser resolvido: 'cdn.bluepex.com.br', Dica: verifique se nenhum Firewall/Antivírus está bloqueando o acesso!
  Não foi possível conectar ao servidor de CDN.
  Se ocorrer com frequência, verifique sua conexão e também um possível bloqueio por Firewall/Antivírus.

- WARN: Can not send newer productivity to queue
  Não foi possível enviar os novos dados de produtividade para a Suíte

- WARN: Can not connect to send older productivity to queue
  Não foi possível enviar os dados antigos de produtividade para a Suíte

- ERROR: Message: O tempo limite da operação foi atingido
  Ocorreu um timeout durante a execução da operação para acesso ao servidor da API.
  Se ocorrer com frequência, verifique sua conexão e também um possível bloqueio por Firewall/Antivírus.

- ERROR: Message: O servidor remoto retornou um erro: (502) Gateway Incorreto.
  O servidor pode ter falhado na entrega do conteúdo.
  Se ocorrer com frequência, verifique sua conexão e também um possível bloqueio por Firewall/Antivírus.