



Troubleshooting Epsoft DLP

By [infraestructura](#)



Troubleshooting Epsoft DLP

Preparação

Definição de canais de comunicação

Equipe do Projeto Epsoft:

Suporte e apoio:

Suporte Epsoft	suporte@epsoft.com.br
----------------	--

Instalação do FlashSafe DLP - Client

Pacote de Instalação em cada máquina que será monitorada.

Pré-requisitos:

4Gb Memória

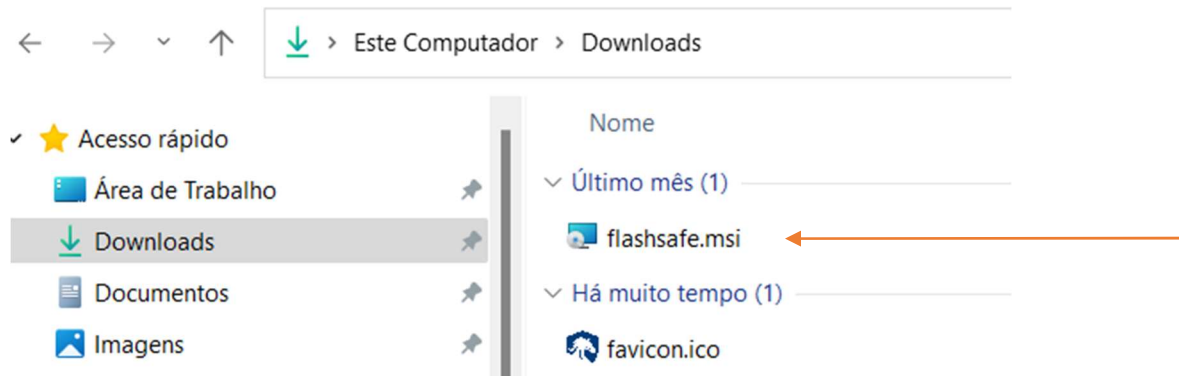
Windows 7 ou superior

Plugin Java JRE

Permissão de Administrador

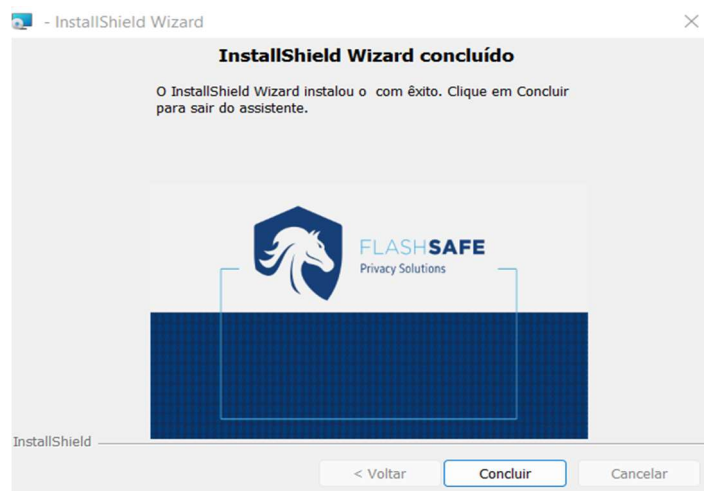
Passos da Instalação:

Execute o instalador como administrador.

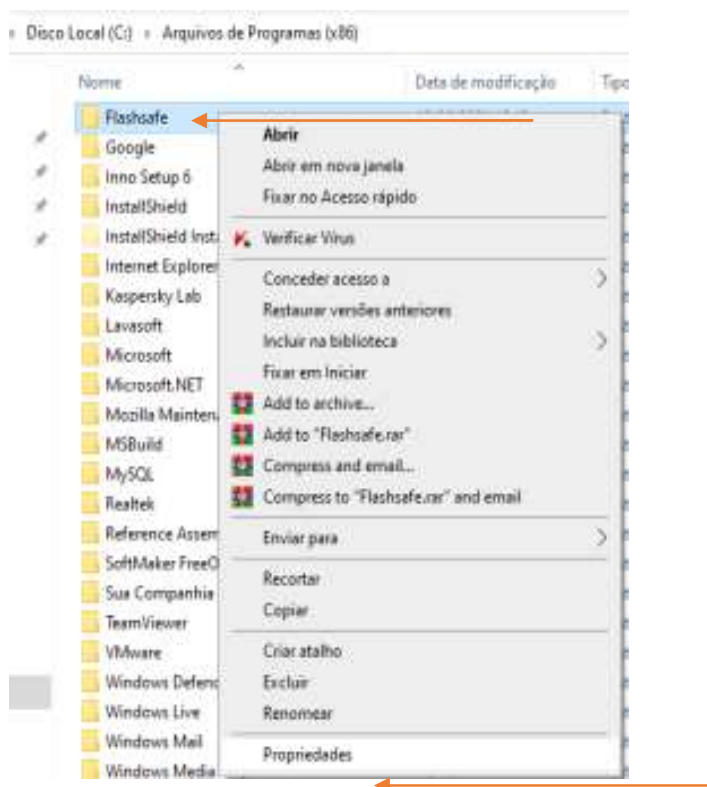


Obs: Caso não consiga executar o instalador a partir de Downloads devido a propriedades do sistema Windows fazer a cópia para meus documentos ou outro diretório que desejar.

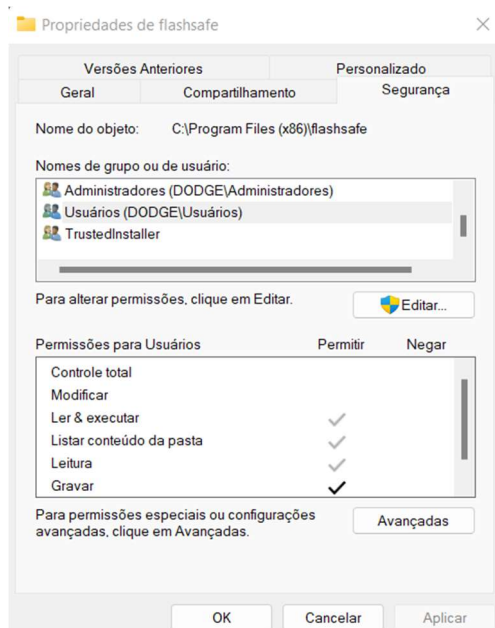




Navegue drive C:\Arquivos de programas (x86)\ e clique com o **botão direito** sobre a pasta onde o Cliente Dlp foi instalado. Em seguida clique no item de menu Propriedades.



Verificar se foi concedido as permissões para usuários do computador, caso não tenha, selecione o grupo Usuários, em seguida clique em Permitir para “gravar ou modificar”, para salvar clique no Aplicar e depois botão OK.



Verificando problemas com a inicialização do DLP Epssoft

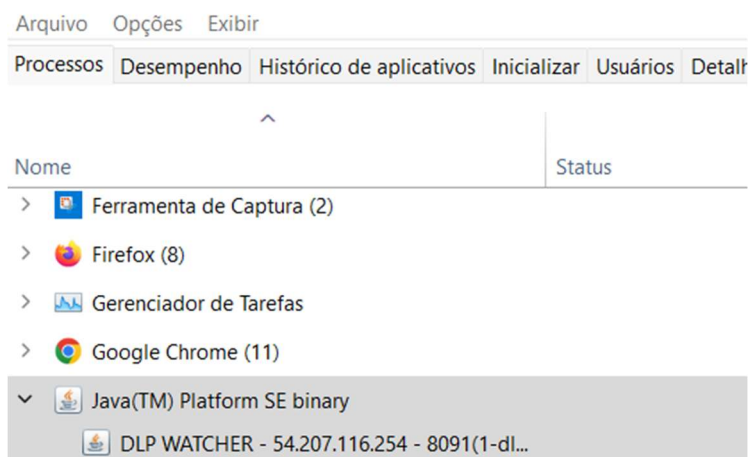
Necessário checar e instalação do Plugin Java.

Java 8 (update 371) 64 bits ou Versão mais atualizada

Link para Download.

<https://java.com>

Para checar se o Cliente está em atividade após cerca de 2 minutos da máquina inicializada verificar em gerenciamento de tarefas se o processo java(TM) Plataforma SE Binary encontra-se em execução.



Caso não ocorra a inicialização automática do aplicativo e a máquina do usuário correspondente não esteja sendo visualizada no front pelo DPO, este problema pode ser verificado via Regedit conforme caminho abaixo.

Verifique a existência do atalho na pasta flashsafe: dlpwatchstart

> OS (C:) > Arquivos de Programas (x86) > flashsafe

Nome	Data de modificação	Tipo	Tamanho
d	02/08/2022 09:11	Pasta de arquivos	
dlpAudit	02/08/2022 09:13	Pasta de arquivos	
dlpCliente	02/08/2022 09:13	Pasta de arquivos	
j	02/08/2022 09:11	Pasta de arquivos	
java	02/08/2022 09:11	Pasta de arquivos	
log	02/08/2022 09:13	Pasta de arquivos	
trab	02/08/2022 09:13	Pasta de arquivos	
v	02/08/2022 09:11	Pasta de arquivos	
220802.txt	02/08/2022 09:14	Documento de Texto	1 KB
DiscoveryAtivoDbg.cmd	09/10/2021 20:22	Script de Comandos do Windows	1 KB
dlpWatchStart.cmd	12/07/2022 16:47	Script de Comandos do Windows	1 KB
dlpWatchStart	29/12/2021 16:56	Atalho	2 KB
dlpWatchStart.vbs	29/12/2021 13:40	Arquivo de script do VBScript	1 KB
dlpWatchStartDbg.cmd	12/07/2022 16:47	Script de Comandos do Windows	1 KB

Atalho DlpwatchStar

Acessar o caminho via regedit:

Computador\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\
CurrentVersion\Run

Verifique a existência da chave de registro.

\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run

Nome	Tipo	Dados
(Padrão)	REG_SZ	(valor não definido)
dlp	REG_SZ	C:\Program Files (x86)\Flashsafe\dlpWatchStart.lnk
SunJavaUpdateSched	REG_SZ	"C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe"

Opção 1:

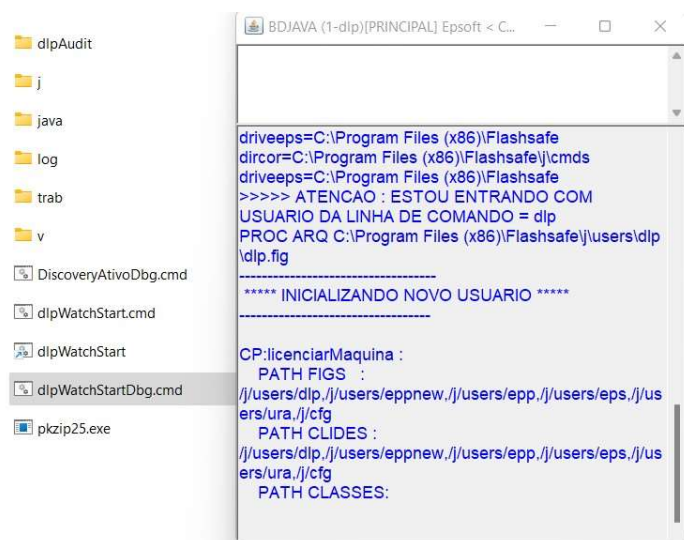
Caso não exista Desinstale o Software através do painel de controle adicionar e remover programas e instale novamente, após reinstalação verifique se a chave de registro foi criada.

Configuração finalizada.

Executando pela primeira vez o DLP.

Para melhor acompanhamento na primeira instalação do DLP recomenda-se realizar a execução através do

“DlpWatcherStartDbg.cmd” conforme figura abaixo.



Realizar o acompanhamento desta fase permite visualizar se ocorrerá algum problema de Comunicação do DLP com o Servidor Cloud, atividade de interferência do Antivírus local,

Liberação de porta de comunicação IP no Firewall.

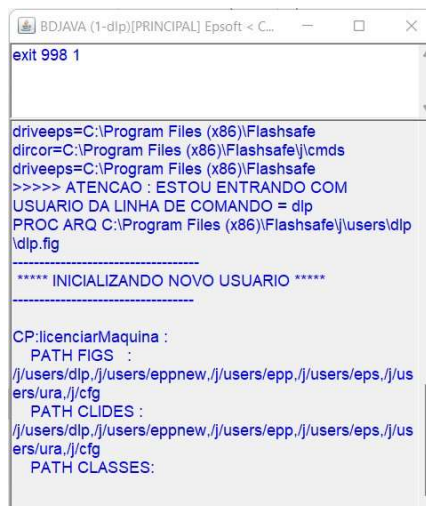
Comando: StatusDlp permite verificar se as configurações estão corretas identificando as portas de comunicação

Para fechar o modo debug executar o commando "exit 998 1"



```
DLP WATCHER - 52.67.242.215 - 8027(1...
StatusDlp

[>>>>statusDlp
ipCloud      =52.67.242.215
portaCloud   =8027
$ipExterno   =
$portaExterna =
$ipDlp       =
portaDlp     =8028
pid          =21052@DODGE
driveeps     =C:\Program Files (x86)\Flashsafe
loopArquivos thread 2
loopWork 16
arquivos recentes thread 17
procFilaSendInfo thread 18
amostragemMonitoracaoAnexos checa filhos thread 19
executador de comandos thread 20
monitor de mouse thread 21
análise de dados sensíveis thread 22
monitor de keys thread 23
controle de dispositivos externos 24
----- DISCOVERY -----
```



```
BDJ\JAVA (1-dlp)[PRINCIPAL] Epsoft < C...
exit 998 1

driveeps=C:\Program Files (x86)\Flashsafe
dircor=C:\Program Files (x86)\Flashsafe\cmds
driveeps=C:\Program Files (x86)\Flashsafe
>>>>> ATENCAO : ESTOU ENTRANDO COM
USUARIO DA LINHA DE COMANDO = dlp
PROC ARQ C:\Program Files (x86)\Flashsafe\users\dlp
\dlp.fig

***** INICIALIZANDO NOVO USUARIO *****

CP:licenciarMaquina :
  PATH FIGS :
    /j/users/dlp./j/users/eppnew./j/users/epp./j/users/eps./j/us
ers/ura./j/cfg
  PATH CLIDES :
    /j/users/dlp./j/users/eppnew./j/users/epp./j/users/eps./j/us
ers/ura./j/cfg
  PATH CLASSES:
```

Obs: Recomendamos Este procedimento somente para pessoal técnico envolvidos na instalação do DLP.

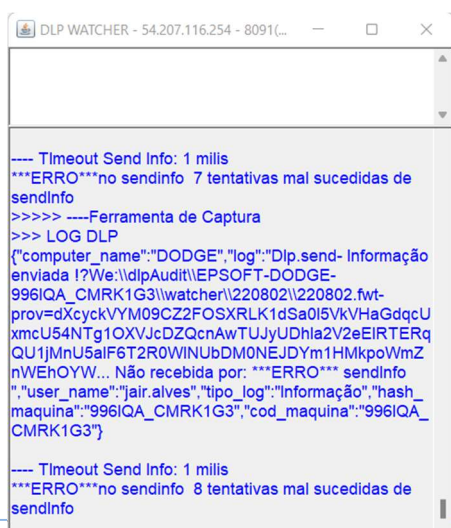
“Muito Importante”

Realizar a verificação das configurações de firewall, para ambientes que possuam algum tipo de bloqueio de portas.

Para comunicação do cliente com o servidor Cloud e necessário o desbloqueio da porta Cloud Especificada neste exemplo usando a porta 8027 somente para Saída.

Caso este bloqueio ocorra teremos falha de comunicação com o Servidor Cloud.

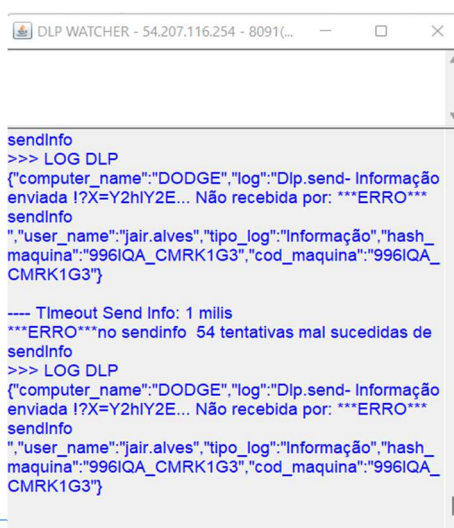
Exemplos:



```
DLP WATCHER - 54.207.116.254 - 8091(1...

---- Timeout Send Info: 1 millis
***ERRO***no sendinfo 7 tentativas mal sucedidas de
sendInfo
>>>>> ----Ferramenta de Captura
>>> LOG DLP
{"computer_name":"DODGE","log":"Dlp.send- Informação
enviada !?We:\dlpAudit\EPSON-DODGE-
996IQA_CM RK1G3\lwatcher\220802\220802.fwt-
prov=dXcyckVYM09CZ2FOSXRLK1dSa0I5VkvHaGdqC4
xmcU54NTg1OXVJcDZQcnAwTUJyUDhla2V2eEIRTERq
QU1jMnU5aIF6T2R0WINUbDM0NEJDYm1HMkpoWmZ
nWEhOYW... Não recebida por: ***ERRO*** sendInfo
{"user_name":"jair.alves","tipo_log":"Informação","hash_
maquina":"996IQA_CM RK1G3","cod_maquina":"996IQA_
CM RK1G3"}

---- Timeout Send Info: 1 millis
***ERRO***no sendinfo 8 tentativas mal sucedidas de
sendInfo
```



```
DLP WATCHER - 54.207.116.254 - 8091(1...

sendInfo
>>> LOG DLP
{"computer_name":"DODGE","log":"Dlp.send- Informação
enviada !?X=Y2hiY2E... Não recebida por: ***ERRO***
sendInfo
{"user_name":"jair.alves","tipo_log":"Informação","hash_
maquina":"996IQA_CM RK1G3","cod_maquina":"996IQA_
CM RK1G3"}

---- Timeout Send Info: 1 millis
***ERRO***no sendinfo 54 tentativas mal sucedidas de
sendInfo
>>> LOG DLP
{"computer_name":"DODGE","log":"Dlp.send- Informação
enviada !?X=Y2hiY2E... Não recebida por: ***ERRO***
sendInfo
{"user_name":"jair.alves","tipo_log":"Informação","hash_
maquina":"996IQA_CM RK1G3","cod_maquina":"996IQA_
CM RK1G3"}
```


Após Verificação ou correção dos itens de configuração acima descritos realizar acesso ao front para verificar

se a maquina e os dados estão chegando ao servidor.

Todas: 11

Em Atividade: 3

Sem Atividade: 8

Total

Busca

20

Total de Registros: 1

Pesquise no resultado

por página

1

AÇÕES	STATUS	GRUPO DLP	CÓDIGO DE MÁQUINA	NOME DA MÁQUINA	USUÁRIO	DISCOS	ÚTIMA ATIVIDADE
<div><div></div><div></div><div></div><div></div></div>	<div></div>	epsoft	0BX31U_2VRT9R2	VOLVO	tatiana.toniolo	<div>-- Selecione uma unidade de Disco --</div>	01/08/2022 - 17:02:32
<div><div></div><div></div><div></div><div></div></div>	<div></div>	epsoft	20U3PPB_FMRK1G3	GOROLLA	leandro.oliveira	<div>-- Selecione uma unidade de Disco --</div>	01/08/2022 - 12:30:03
<div><div></div><div></div><div></div><div></div></div>	<div></div>	epsoft	576HXW_PE08EL96	SKYLINE	henrique.aurelio	<div>-- Selecione uma unidade de Disco --</div>	02/08/2022 - 10:20:21
<div><div></div><div></div><div></div><div></div></div>	<div></div>	epsoft	996IQA_CMRK1G3	DODGE	jair.alves	<div>-- Selecione uma unidade de Disco --</div>	02/08/2022 - 10:20:22
<div><div></div><div></div><div></div><div></div></div>	<div></div>	epsoft	9DALGPF_FMRK1G3	GOROLLA	leandro.oliveira	<div>-- Selecione uma unidade de Disco --</div>	29/07/2022 - 18:18:44

Validação Realizada.

Pontos Importantes para instalação:

Instalação por GPO.

Segue recomendações:

Ao implementar o DLP Epsoft, recomendamos realizar testes prévio em uma pequena quantidade de maquinas para que se observe o comportamento da implementação.

Checar instalação em cada maquina se foi realiza com sucesso.

Checar Atuação do programa antivirus local em experiências passadas foi detectado algum tipo de intervenção do antivirus Fazendo com que o instalador seja executado parcialmente assim não contendo toda os diretorios necessários para a total Funcionalidade do DLP.

Caso esteja executando o instalador a partir de Downloads para versões atualizadas de Windows 10, 11 e antivirus Necessário copia-lo para outro diretorio exemplo, meus documentos a assim executa-lo.

Os diretórios que devem contemplar a instalação serem os seguintes?

OS (C:) > Arquivos de Programas (x86) > flashsafe

Nome	Data de modificação	Tipo	Tamanho
d	02/01/2023 12:35	Pasta de arquivos	
j	02/01/2023 12:35	Pasta de arquivos	
java	02/01/2023 12:35	Pasta de arquivos	
v	02/01/2023 12:35	Pasta de arquivos	
DiscoveryAtivoDbg.cmd	09/10/2021 20:22	Script de Comand...	1 KB
dIpWatchStart.cmd	05/12/2022 11:21	Script de Comand...	1 KB
dIpWatchStart	29/12/2021 16:56	Atalho	2 KB
dIpWatchStart.vbs	29/12/2021 13:40	Arquivo de script ...	1 KB
dIpWatchStartDbg.cmd	05/12/2022 11:22	Script de Comand...	1 KB
pkzip25.exe	20/07/2018 18:23	Aplicativo	332 KB

Após instalação deve ficar assim:

Verificando qualquer coisa diferente deste cenário realizar a verificação do Antivírus local:

Caso isto aconteça aconselhável inserir instalador flashsafe.msi em exceções no painel de configurações
Do seu antivírus ou desativá-lo somente nesta etapa retornando a sua configuração normal
Após concluí-las.

> OS (C:) > Arquivos de Programas (x86) > flashsafe >

Nome	Data de modificação	Tipo	Tamanho
d	02/01/2023 12:41	Pasta de arquivos	
dIpAudit	02/01/2023 12:40	Pasta de arquivos	
dIpCliente	02/01/2023 12:40	Pasta de arquivos	
j	02/01/2023 12:35	Pasta de arquivos	
java	02/01/2023 12:35	Pasta de arquivos	
log	02/01/2023 12:40	Pasta de arquivos	
log_testes	02/01/2023 12:41	Pasta de arquivos	
trab	02/01/2023 12:40	Pasta de arquivos	
v	02/01/2023 12:35	Pasta de arquivos	
230102.txt	02/01/2023 12:40	Documento de Te...	1 KB
DiscoveryAtivoDbg.cmd	09/10/2021 20:22	Script de Comand...	1 KB
dIpWatchStart.cmd	05/12/2022 11:21	Script de Comand...	1 KB
dIpWatchStart	29/12/2021 16:56	Atalho	2 KB
dIpWatchStart.vbs	29/12/2021 13:40	Arquivo de script ...	1 KB
dIpWatchStartDbg.cmd	05/12/2022 11:22	Script de Comand...	1 KB
pkzip25.exe	20/07/2018 18:23	Aplicativo	332 KB

Checar porta de comunicação Cloud utilizada pelo Cliente se está liberado acesso para saída e seu IP.

Caso tenha que desinstalar o DLP que faça pelo Painel de controle mesmo que o cliente esteja rodando existe funções que param a execução para que seja feita a desinstalação, OBS, Necessário que usuário tenha direitos de Adm Para Execução desta tarefa.

**Todo o canal de comunicação sera efetuado pelo Email corporativo
suporte@epsoft.com.br**

