

Configurando o Cisco Secure UNIX e Secure ID (SDI Client)

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Instalação de um SDI Client \(Secure ID\) em uma máquina Cisco Secure UNIX](#)

[Exame inicial do ID seguro e CSUNIX](#)

[ID seguro e CSUNIX: Perfil TACACS+](#)

[Como o perfil funciona](#)

[Combinações de senha de CSUnix TACACS+ que não trabalham](#)

[Debugando exemplos de perfil de CSUnix TACACS+ SDI](#)

[Raio CSUnix](#)

[Autenticação de login com CSUnix e RAI0](#)

[PPP e autenticação pap com CSUnix e RAI0](#)

[Conexão e PAP de PPP de rede de discagem](#)

[Dicas de debug e verificação](#)

[RADIUS, PPP e PAP do Cisco Secure](#)

[ID seguro e CSUNIX](#)

[Informações Relacionadas](#)

[Introdução](#)

Para executar a configuração neste documento, você precisa toda a versão segura de Cisco que apoiar Secure ID s do Security Dynamics Incorporated (SDI) '.

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

[Convenções](#)

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

Instalação de um SDI Client (Secure ID) em uma máquina Cisco Secure UNIX

Nota: O Secure ID está instalado geralmente antes que Cisco UNIX seguro (CSUnix) esteja instalado. Estas instruções descrevem como instalar o cliente de SDI depois que CSUnix foi instalado.

1. No servidor SDI, execute o **sdadmin**. Diga o servidor SDI que a máquina de CSUnix é um cliente e especifique que os usuários SDI na pergunta estão ativados no cliente de CSUnix.
2. Use o **nslookup #.#.#.#** ou o comando **nslookup <hostname>** certificar-se que o cliente de CSUnix e o servidor SDI podem fazer para a frente e consulta reversa de se.
3. Copie o arquivo de `/etc/sdace.txt` do servidor SDI ao arquivo de `/etc/sdace.txt` do cliente de CSUnix.
4. Copie o arquivo `sdconf.rec` do servidor SDI ao cliente de CSUnix; este arquivo pode residir em qualquer lugar no cliente de CSUnix. Contudo, se é colocado na mesma estrutura do diretório no cliente de CSUnix como era no servidor SDI, `sdace.txt` não tem que ser alterado.
5. `/etc/sdace.txt` ou `VAR_ACE` devem apontar ao trajeto onde o arquivo `sdconf.rec` é encontrado. Para verificar isto, execute o `cat /etc/sdace.txt`, ou verifique a saída do `env` para ter certeza que `VAR_ACE` esteja definido no perfil da raiz enquanto a raiz começa.
6. Suporte o `CSU.cfg` do cliente de CSUnix, a seguir altere a seção dos `config_external_authen_symbols AUTHEN` com estas linhas:
7. Recicle CSUnix pela execução de **K80CiscoSecure** e de **S80CiscoSecure**.
8. Se `$BASE/utills/psg` mostra que Cisco se fixa o processo do processo de servidor AAA era ativo antes que o arquivo `csu.cfg` esteve alterado mas não mais tarde, a seguir os erros foram feitos na revisão do arquivo `csu.cfg`. Restaure o arquivo `csu.cfg` original e tente-o fazer as mudanças esboçadas na etapa 6 outra vez.

Exame inicial do ID seguro e CSUNIX

Para testar o ID seguro e CSUNIX, execute estas etapas:

1. Certifique-se de que um usuário diferente de SDI pode telnet ao roteador e para ser autenticado com CSUnix. Se isto não trabalha, o SDI não trabalhará.
2. Teste a Autenticação SDI básica no roteador e execute este comando:

```
aaa new-model aaa authentication login default tacacs+ none
```

Nota: Isto supõe que os comandos **tacacs-server** são já ativos no roteador.
3. Adicionar um usuário SDI da linha de comando `csunix` para incorporar este comando

```
$BASE/CLI/AddProfile -p 9900 -u sdi_user -pw sdi
```
4. Tente autenticar como um usuário. Se esse usuário trabalha, o isoperacional SDI, e você podem adicionar a informação adicional aos perfis de usuário.
5. Os usuários SDI podem ser testados com o perfil do `unknown_user` em CSUnix. (Os usuários não têm que explicitamente ser alistados em CSUnix se eles que todos estão passados fora ao SDI e todos têm o mesmo perfil.) Se há um perfil de usuário desconhecido já exista, suprima `d` com a ajuda deste comando:

```
$BASE/CLI/DeleteProfile -p 9900 -u unknown_user
```

6. Use este comando adicionar um outro perfil de usuário desconhecido:

```
$BASE/CLI/AddProfile -p 9900 -u unknown_user -pw sdi
```

 Este comando passa fora de todos os usuários desconhecidos ao SDI.

ID seguro e CSUNIX: Perfil TACACS+

1. Execute um teste inicial sem o SDI. Se este perfil de usuário não trabalha sem uma senha do SDI para a autenticação de login, o protocolo de autenticação de cumprimento do desafio (RACHADURA), e o protocolo password authentication (PAP), não trabalhará com uma

```
senha do SDI:# ./ViewProfile -p 9900 -u cse
```

```
User Profile Information
user = cse{
password = chap "chappwd"
password = pap "pappwd"
password = clear,"clearpwd"
default service=permit
service=shell {
}
service=ppp {
protocol=lcp {
}
protocol=ip {
}
}
}
```

2. Uma vez que o perfil trabalha, adicionar o “sdi” ao perfil no lugar de “claro” segundo as indicações deste exemplo:# ./ViewProfile -p 9900 -u cse

```
User Profile Information
user = cse{
password = chap "chappwd"
password = pap "pappwd"
password = sdi default service=permit service=shell { } service=ppp { protocol=lcp { }
protocol=ip { } } }
```

Como o perfil funciona

Este perfil permite que o usuário entre com estas combinações:

- Telnet ao roteador e ao uso SDI. (Isto supõe que o comando **aaa authentication login default tacacs+** esteve executado no roteador.)
- Conexão PPP da rede de comunicação dial-up e PAP. (Isto supõe que os comandos **aaa authentication ppp default if-needed tacacs e ppp authen pap** estiveram executados no roteador).**Nota:** No PC, na rede de comunicação dial-up, certifique-se que o “Accept any authentication que inclui o texto claro” está verificado. Antes de disar, incorpore uma destas combinações de nome de usuário/senha à janela terminal:
username: cse*code+card
password: pap (must agree with profile)

```
username: cse
password: code+card
```

- Conexão PPP e RACHADURA da rede de comunicação dial-up. (Isto supõe que os comandos **aaa authentication ppp default if-needed tacacs e ppp authen chap** estiveram executados no roteador).**Nota:** No PC, na rede de comunicação dial-up, ou o “Accept any authentication que inclui o texto claro” ou “aceita somente a autenticação criptografada” deve

ser verificado. Antes de discar, incorpore este nome de usuário e senha à janela

```
terminal:username: cse*code+card
password: chap (must agree with profile)
```

Combinações de senha de CSUnix TACACS+ que não trabalham

Estas combinações produzem estes CSUnix debugam erros:

- RACHE e não senha do “texto não criptografado” no campo de senha. O usuário incorpora o `code+card` em vez da senha do “texto não criptografado”. [O RFC 1994 na RACHADURA](#) exige o armazenamento da senha de texto sem formatação.

```
username: cse password: code+card CiscoSecure INFO - User cse, No tokencard password
received CiscoSecure NOTICE - Authentication - Incorrect password;
```

- RACHADURA e uma senha ruim da RACHADURA.

```
username: cse*code+card password: wrong chap password (O usuário passa fora ao SDI, e o SDI
passa o usuário, mas CSUnix falha o usuário porque a senha da RACHADURA é
ruim.)CiscoSecure INFO - The character * was found in username:
```

```
username=cse,passcode=1234755962
```

```
CiscoSecure INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
```

```
CiscoSecure INFO - sdi_verify: cse authenticated by ACE Srvr
```

```
CiscoSecure INFO - sdi: cse free external_data memory,state=GET_PASSCODE
```

```
CiscoSecure INFO - sdi_verify: rtn 1
```

```
CiscoSecure NOTICE - Authentication - Incorrect password;
```

- PAP e uma senha de PAP ruim.

```
username: cse*code+card password: wrong pap password (O usuário passa fora ao SDI, e o SDI
passa o usuário, mas CSUnix falha o usuário porque a senha da RACHADURA é
ruim.)CiscoSecure INFO - 52 User Profiles and 8 Group Profiles loaded into Cache.
```

```
CiscoSecure INFO - The character * was found in username:
```

```
username=cse,passcode=1234651500
```

```
CiscoSecure INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
```

```
CiscoSecure INFO - sdi_verify: cse authenticated by ACE Srvr
```

```
CiscoSecure INFO - sdi: cse free external_data memory,state=GET_PASSCODE
```

```
CiscoSecure INFO - sdi_verify: rtn 1
```

```
CiscoSecure NOTICE - Authentication - Incorrect password;
```

Debugando exemplos de perfil de CSUnix TACACS+ SDI

- O usuário precisa de fazer a RACHADURA e a autenticação de login; O PAP falha.#

```
./ViewProfile -p 9900 -u cse
```

```
User Profile Information
```

```
user = cse{
```

```
password = chap "*****"
```

```
password = sdi
```

```
default service=permit
```

```
service=shell {
```

```
}
```

```
service=ppp {
```

```
protocol=lcp {
```

```
}
```

```
protocol=ip {
```

```
}
```

```
}
```

- O usuário precisa de fazer o PAP e a autenticação de login; A RACHADURA falha.#

```
./ViewProfile -p 9900 -u cse
```

```
User Profile Information
```

```
user = cse{
```

```

member = admin
password = pap "*****"
password = sdi
default service=permit
service=shell {
}
service=ppp {
protocol=lcp {
}
protocol=ip {
}
}
}

```

Raio CSUnix

Estas seções contêm procedimentos do raio CSUnix.

Autenticação de login com CSUnix e RAIO

Execute estas etapas à autenticação de teste:

1. Execute um teste inicial sem o SDI. Se este perfil de usuário não trabalha sem uma senha do SDI para a autenticação de login, não trabalhará com uma senha do SDI: # ./ViewProfile

```

-p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2="whatever" } reply_attributes= { 6=6 } } }

```

2. Uma vez que este perfil trabalha, substitua “o que quer que” com “sdi” segundo as

```

indicações deste exemplo: # ./ViewProfile -p 9900 -u cse
User Profile Information
user = cse{
radius=Cisco {
check_items= {
2=sdi } reply_attributes= { 6=6 } } }

```

PPP e autenticação pap com CSUnix e RAIO

Execute estas etapas à autenticação de teste:

Nota: A autenticação PPP chap com CSUnix e RAIO não é apoiada.

1. Execute um teste inicial sem o SDI. Se este perfil de usuário não trabalha sem uma senha do SDI para a autenticação PPP/PAP e “modo assíncrono dedicado,” não trabalhará com uma senha do SDI: # ./ViewProfile -p 9900 -u cse

```

user = cse {
password = pap "pappass"
radius=Cisco {
check_items = {
}
reply_attributes= {
6=2
7=1

```

```
}  
}  
}
```

2. Uma vez os trabalhos acima do perfil, adicionam a **senha = o sdi** ao perfil e adicionam o atributo **200=1** segundo as indicações deste exemplo (este ajusta Cisco_Token_Immediate ao yes.):# ./ViewProfile -p 9900 -u cse

```
user = cse {  
password = pap "pappass"  
password = sdi  
radius=Cisco {  
check_items = {  
200=1  
}  
reply_attributes= {  
6=2  
7=1  
}  
}  
}
```

3. No "GUI avançado, a seção do server," **certifica-se que o " habilitar cache de token "** está ajustado. Isto pode ser confirmado do comando line interface(cli) com: \$BASE/CLI/ViewProfile -p 9900 -u SERVER.#.#.#.#
!--- Where #.#.#.# is the IP address of the CSUnix server. TokenCachingEnabled="yes"

[Conexão e PAP de PPP de rede de discagem](#)

Supõe-se que os **comandos aaa authentication ppp default if-needed tacacs e PPP authen PAP** estiveram executados no roteador. Incorpore este nome de usuário e senha à janela terminal antes que você disque.:

```
username: cse  
password: code+card
```

Nota: No PC, na rede de comunicação dial-up, certifique-se que o "Accept any authentication que inclui o texto claro" está verificado.

[Dicas de debug e verificação](#)

Estas seções contêm pontas para dicas de debug e verificação.

[RADIUS, PPP e PAP do Cisco Secure](#)

Este é um exemplo de um debug correto:

```
CiscoSecure DEBUG - RADIUS ; Outgoing Accept Packet id=133 (10.31.1.6)  
  User-Service-Type = Framed-User  
  Framed-Protocol = PPP  
CiscoSecure DEBUG - RADIUS ; Request from host alf0106 nas (10.31.1.6)  
  code=1 id=134 length=73  
CiscoSecure DEBUG - RADIUS ; Incoming Packet id=134 (10.31.1.6)  
  Client-Id = 10.31.1.6  
  Client-Port-Id = 1  
  NAS-Port-Type = Async  
  User-Name = "cse"  
  Password = "?\235\306"  
  User-Service-Type = Framed-User  
  Framed-Protocol = PPP
```

```
CiscoSecure DEBUG - RADIUS ; Authenticate (10.31.1.6)
CiscoSecure DEBUG - RADIUS ; checkList: ASCEND_TOKEN_IMMEDIATE = 1
CiscoSecure DEBUG - RADIUS ; User PASSWORD type is Special
CiscoSecure DEBUG - RADIUS ; authPapPwd (10.31.1.6)
CiscoSecure INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
CiscoSecure DEBUG - profile_valid_tcaching FALSE ending.
CiscoSecure DEBUG - Token Caching. IGNORE.
CiscoSecure INFO - sdi_verify: cse authenticated by ACE Srvr
CiscoSecure INFO - sdi: cse free external_data memory,state=GET_PASSCODE
CiscoSecure INFO - sdi_verify: rtn 1
CiscoSecure DEBUG - RADIUS ; Sending Ack of id 134 to alf0106 (10.31.1.6)
```

ID seguro e CSUNIX

Debugar é armazenado no arquivo especificado em /etc/syslog.conf para local0.debug.

Nenhum usuários pode autenticar - SDI ou de outra maneira:

Depois que você adiciona o Secure ID, certifique-se de que nenhum erro esteve feito quando você altera o arquivo csu.cfg. Fixe o arquivo csu.cfg ou reverta ao arquivo csu.cfg alternativo.

Este é um exemplo de um debug correto:

```
Dec 13 11:24:22 rtp-evergreen.rtp.cisco.com CiscoSecure:
  INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
Dec 13 11:24:22 rtp-evergreen.rtp.cisco.com CiscoSecure:
  INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
Dec 13 11:24:31 rtp-evergreen.rtp.cisco.com CiscoSecure:
  INFO - sdi_verify: cse authenticated by ACE Srvr
Dec 13 11:24:31 rtp-evergreen.rtp.cisco.com CiscoSecure:
  INFO - sdi_verify: cse authenticated by ACE Srvr
Dec 13 11:24:31 rtp-evergreen.rtp.cisco.com CiscoSecure:
  INFO - sdi: cse free external_data memory,state=GET_PASSCODE
Dec 13 11:24:31 rtp-evergreen.rtp.cisco.com CiscoSecure:
  INFO - sdi: cse free external_data memory,state=GET_PASSCODE
Dec 13 11:24:31 rtp-evergreen.rtp.cisco.com CiscoSecure:
  INFO - sdi_verify: rtn 1
Dec 13 11:24:31 rtp-evergreen.rtp.cisco.com CiscoSecure:
  INFO - sdi_verify: rtn 1
```

Este é um exemplo de um debug ruim:

CSUnix encontra o perfil de usuário e envia-o ao servidor SDI, mas o servidor SDI falha o usuário porque a senha é ruim.

```
Dec 13 11:26:22 rtp-evergreen.rtp.cisco.com CiscoSecure:
  INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
Dec 13 11:26:22 rtp-evergreen.rtp.cisco.com CiscoSecure:
  INFO - sdi_challenge: rtn 1, state=GET_PASSCODE, user=cse
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
  WARNING - sdi_verify: cse denied access by ACE Srvr
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
  WARNING - sdi_verify: cse denied access by ACE Srvr
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
  INFO - sdi: cse free external_data memory,state=GET_PASSCODE
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
  INFO - sdi: cse free external_data memory,state=GET_PASSCODE
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
  INFO - sdi_verify: rtn 0
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
  INFO - sdi_verify: rtn 0
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:
```

```
NOTICE - Authentication - Incorrect password;  
Dec 13 11:26:26 rtp-evergreen.rtp.cisco.com CiscoSecure:  
NOTICE - Authentication - Incorrect password;
```

Esta é uma mostra do exemplo que o server de Ace está para baixo:

Incorpore a **parada de ./aceserver** no servidor SDI. O usuário não recebe “incorpora a mensagem da SENHA”.

```
Dec 13 11:33:42 rtp-evergreen.rtp.cisco.com CiscoSecure:  
ERROR - sdi_challenge error: sd_init failed cli/srvr comm init (cse)  
Dec 13 11:33:42 rtp-evergreen.rtp.cisco.com CiscoSecure:  
ERROR - sdi_challenge error: sd_init failed cli/srvr comm init (cse)  
Dec 13 11:33:42 rtp-evergreen.rtp.cisco.com CiscoSecure:  
INFO - sdi: cse free external_data memory,state=RESET  
Dec 13 11:33:42 rtp-evergreen.rtp.cisco.com CiscoSecure:  
INFO - sdi: cse free external_data memory,state=RESET
```

[Informações Relacionadas](#)

- [Cisco Secure ACS para página de suporte do UNIX](#)
- [Field Notice para o Cisco Secure ACS para UNIX](#)
- [Suporte Técnico - Cisco Systems](#)