

Guia de projeto e implementação de TokenCaching

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configurar a entrada do nome de usuário e senha](#)

[Configurar o TokenCaching no CiscoSecure ACS Windows](#)

[Configurar o TokenCaching no CiscoSecure ACS UNIX](#)

[Verificar](#)

[Troubleshooting](#)

[Debugar o TokenCaching no CiscoSecure ACS UNIX](#)

[Informações Relacionadas](#)

[Introdução](#)

O espaço deste documento é discutir a instalação e pesquisá-lo defeitos do TokenCaching. As sessões do Point-to-Point Protocol (PPP) para usuários do adaptador terminal de ISDN (TA) são terminadas tipicamente no usuário PC. Isto permite que o usuário controle a sessão de PPP da mesma forma como uma conexão dialup do async (modem), que signifique conecte e desligue a sessão como necessária. Isto permite o usuário usar o protocolo password authentication (PAP) a fim incorporar a senha de uma vez (OTP) para o transporte.

Contudo, se o segundo canal B é projetado vir acima automaticamente, o usuário deve ser alertado para um OTP novo para o segundo canal B. O software PPP PC não recolhe o segundo OTP. Em lugar de, o software tenta usar a mesma senha usada para o canal B preliminar. O servidor de placa token nega a reutilização de um OTP pelo projeto. O CiscoSecure ACS para Unix (Versão 2.2 e mais recente) e o CiscoSecure ACS for Windows (2.1 e mais tarde) executam o TokenCaching a fim apoiar o uso do mesmo OTP no segundo canal B. Esta opção exige o server do Authentication, Authorization, and Accounting (AAA) manter a informação de estado sobre a conexão do usuário de token.

Refira [senhas de uma única vez NO ISDN de apoio](#) para mais informação.

[Pré-requisitos](#)

Requisitos

Este documento supõe que você já tem estes configurados corretamente:

- Um modem dialup que funcione corretamente.
- O servidor do acesso de rede (NAS) configurado corretamente, com AAA que aponta ao CiscoSecure ACS UNIX ou às janelas de ACS.
- O ACE/SDI já setup com CiscoSecure ACS UNIX ou janelas de ACS, e trabalha corretamente.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- CiscoSecure ACS UNIX 2.2 ou mais atrasado
- 2.1 de Windows do CiscoSecure ACS ou mais tarde

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Configurar

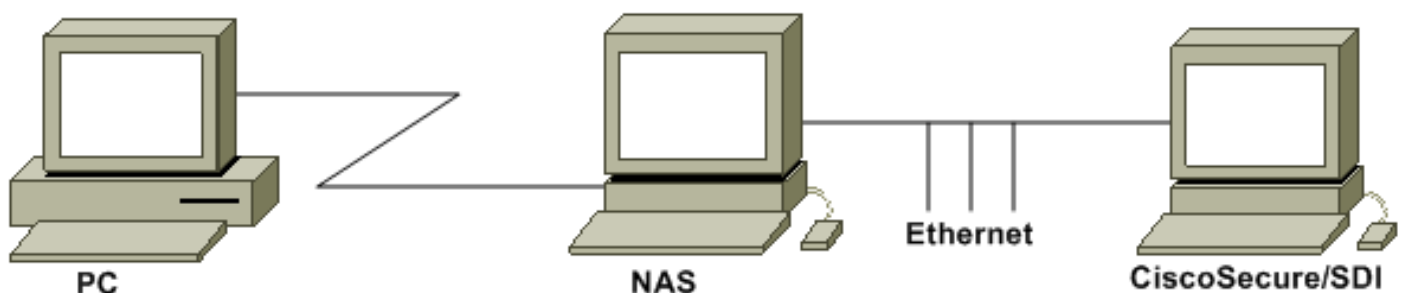
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a [Command Lookup Tool](#) ([somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Um PC disca em um NAS e no modem ISDN, e é configurado para o **comando ppp multilink**.



Configurações

Este documento utiliza as seguintes configurações:

- [Configurar a entrada do nome de usuário e senha](#)
- [Configurar o TokenCaching no CiscoSecure ACS Windows](#)
- [Configurar o TokenCaching no CiscoSecure ACS UNIX](#)

Configurar a entrada do nome de usuário e senha

Neste documento, o protocolo de autenticação de cumprimento do desafio dos usos NAS (RACHADURA) para a sessão de PPP junto com a senha de uma vez SDI. Se você usa a RACHADURA, incorpore a senha a este formulário:

- **username** — fadi*pin+code (note * no username)
- **senha** — chappassword

Um exemplo deste é: o username = o fadi, a senha da rachadura = Cisco, pino = 1234, e o código que mostra no token são 987654. Consequentemente, o usuário entra neste:

- **username** — fadi*1234987654
- **senha** — Cisco

Nota: Se o CiscoSecure e o NAS foram configurados para o PAP, o username e o token podem ser incorporados como este:

- **username** — username*pin+code
- **senha**—

Ou:

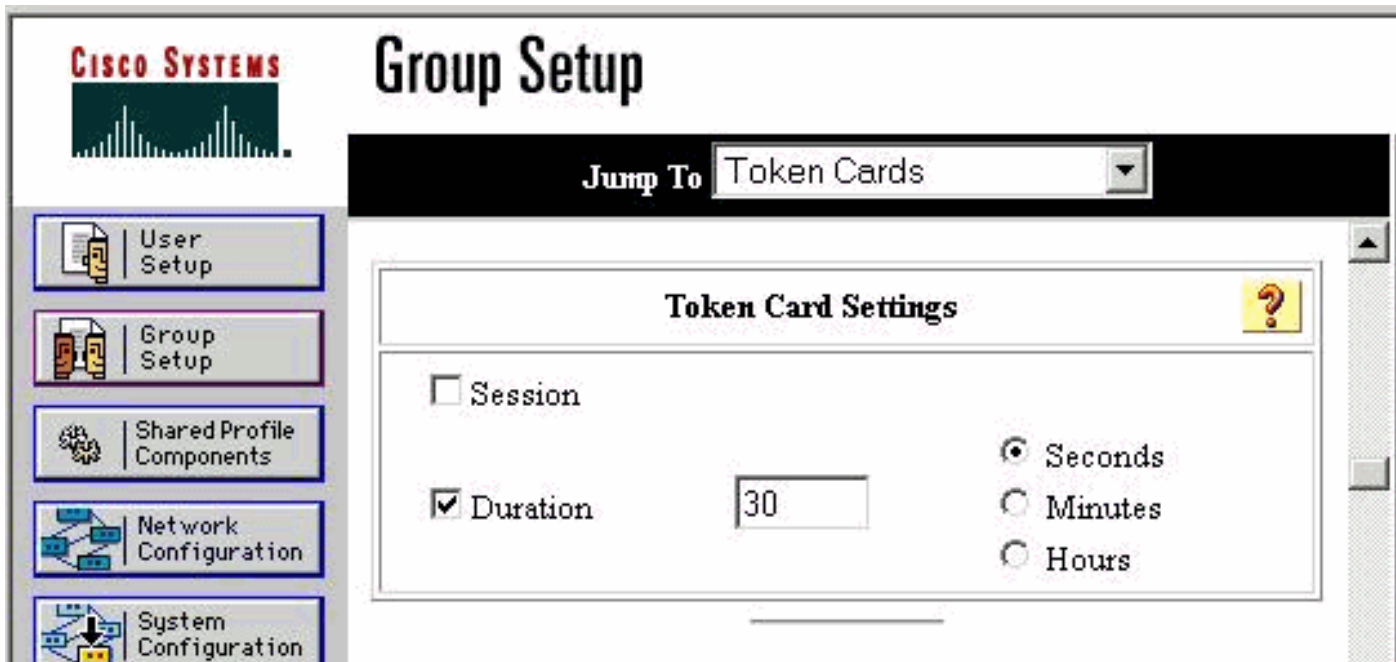
- **nome de usuário** nome de usuário
- **senha** — pin+code

Configurar o TokenCaching no CiscoSecure ACS Windows

O usuário ou o grupo de Windows do CiscoSecure ACS são usual estabelecido, com o IP PPP e o PPP LCP verificados se você usa o TACACS+. Se você usa o RAI0, estes devem ser configurados:

- Atributo 6 = **Service_Type = Framed**
- Atributo 7 = **Framed_Protocol =PPP**

Além, os parâmetros do TokenCaching podem ser verificados para ver se há o grupo segundo as indicações deste exemplo:



[Configurar o TokenCaching no CiscoSecure ACS UNIX](#)

Há quatro atributos do TokenCaching. O atributo do `config_token_cache_absolute_timeout` (nos segundos) é ajustado no arquivo `$install_directory/config/CSU.cfg`. Outros três atributos (`set server token-caching`, `set server token-caching-expire-method`, e `set server token-caching-timeout`) são ajustados no usuário ou nos perfis de grupo. Para este documento, o global attribute `config_token_cache_absolute_timeout` é ajustado a este no arquivo `$install_directory/config/CSU.cfg`:

```
NUMBER config_token_cache_absolute_timeout = 300;
```

Os perfis do atributo do TokenCaching do usuário e do server do grupo são configurados segundo as indicações deste exemplo:

Group Profile:

```
Group Profile Information
group = sdi{
profile_id = 42
profile_cycle = 5
default service=permit
set server token-caching=enable
set server token-caching-expire-method=timeout
set server token-caching-timeout=30
set server max-failed-login-count=1000

}
```

User Profile:

```
user = fadi{
profile_id = 20
set server current-failed-logins = 0
profile_cycle = 168
member = sdi
profile_status = enabled
password = chap "*****"
password = sdi
password = pap "*****"
password = clear "*****"
```

```
default service=permit
set server max-failed-login-count=1000
!--- The TACACS+ section of the profile. service=ppp { default protocol=permit protocol=ip {
set addr=1.1.1.1 } protocol=lcp { } !--- This allows the user to use the ppp multilink command.
protocol=multilink { } } service=shell { default attribute=permit } !--- The RADIUS section of
the profile. radius=Cisco12.05 { check_items= { 200=0 } }
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Debugar o TokenCaching no CiscoSecure ACS UNIX

Este log do CiscoSecure UNIX mostra uma autenticação bem sucedida com TokenCaching, quando a autenticação ocorre em dois canais BRI:

```
Jun 14 13:44:29 cholera CiscoSecure: DEBUG - AUTHENTICATION START request
(e7079cae)
!--- Detects the * in the username. Jun 14 13:44:29 cholera CiscoSecure: INFO - The character *
was found in username: username=fadi,passcode=3435598216 !--- Initializes ACE modules in
CiscoSecure. Jun 14 13:44:29 cholera CiscoSecure: DEBUG - sdi_challenge response timeout 5 Jun
14 13:44:29 cholera CiscoSecure: DEBUG - AceInit() Jun 14 13:44:29 cholera CiscoSecure: DEBUG -
AceInit(17477), ace rc=150, ed=1039800 Jun 14 13:44:29 cholera CiscoSecure: DEBUG -
acsWaitForSingleObject (17477) begin Jun 14 13:44:29 cholera CiscoSecure: DEBUG - aceCB(17477)
Jun 14 13:44:29 cholera CiscoSecure: DEBUG - aceCB(17477) AceGetUserData, ace rc=1, ed=1039800
Jun 14 13:44:29 cholera CiscoSecure: DEBUG - aceCB(17477): AceGetAuthenticationStatus, ace rc=1,
acm rc=0 Jun 14 13:44:29 cholera CiscoSecure: DEBUG - aceCB(17477): return Jun 14 13:44:29
cholera CiscoSecure: DEBUG - acsWaitForSingleObject(0) (17477) Jun 14 13:44:29 cholera
CiscoSecure: DEBUG - acsWaitForSingleObject (17477) end, rc=0 Jun 14 13:44:29 cholera
CiscoSecure: DEBUG - AceInit(17477), continue, acm rc=0 Jun 14 13:44:29 cholera CiscoSecure:
DEBUG - AceSetUsername(17477), username=fadi Jun 14 13:44:29 cholera CiscoSecure: DEBUG -
AceSetUsername(17477), ace rc=1 Jun 14 13:44:29 cholera CiscoSecure: INFO -
sdi_challenge(17477): rtn 1, state=GET_PASSCODE, user=fadi Jun 14 13:44:29 cholera CiscoSecure:
DEBUG - Token Caching. timeout_value is: 30 Jun 14 13:44:29 cholera CiscoSecure: DEBUG - Token
Caching. timeout enabled value: 30 Jun 14 13:44:29 cholera CiscoSecure: DEBUG -
profile_valid_tcaching TRUE ending. Jun 14 13:44:29 cholera CiscoSecure: DEBUG - Token Caching.
MISS. Jun 14 13:44:29 cholera CiscoSecure: DEBUG - AceSetPasscode(17477), passcode=3435598216
Jun 14 13:44:29 cholera CiscoSecure: DEBUG - AceSetPasscode(17477), ace rc=1 !--- Checks
credentials with ACE server. Jun 14 13:44:29 cholera CiscoSecure: DEBUG - AceCheck(17477) Jun 14
13:44:29 cholera CiscoSecure: DEBUG - AceCheck(17477), ace rc=150 Jun 14 13:44:29 cholera
CiscoSecure: DEBUG - acsWaitForSingleObject (17477) begin Jun 14 13:44:31 cholera CiscoSecure:
DEBUG - aceCB(17477) Jun 14 13:44:31 cholera CiscoSecure: DEBUG - aceCB(17477) AceGetUserData,
ace rc=1, ed=1039800 Jun 14 13:44:31 cholera CiscoSecure: DEBUG - aceCB(17477):
AceGetAuthenticationStatus, ace rc=1, acm rc=0 Jun 14 13:44:31 cholera CiscoSecure: DEBUG -
aceCB(17477): return Jun 14 13:44:31 cholera CiscoSecure: DEBUG - acsWaitForSingleObject(0)
(17477) Jun 14 13:44:31 cholera CiscoSecure: DEBUG - acsWaitForSingleObject (17477) end, rc=0
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - AceCheck(17477), continue, acm rc=0 Jun 14 13:44:31
cholera CiscoSecure: INFO - sdi_verify(17477): fadi authenticated by ACE Srvr Jun 14 13:44:31
cholera CiscoSecure: DEBUG - AceClose(17477) Jun 14 13:44:31 cholera CiscoSecure: INFO -
sdi(17477): fadi free external_data memory, state=GET_PASSCODE !--- The TokenCaching timeout is
set to 30 seconds. Jun 14 13:44:31 cholera CiscoSecure: DEBUG - Token Caching. timeout_value is:
30 Jun 14 13:44:31 cholera CiscoSecure: DEBUG - Token Caching. timeout enabled value: 30 Jun 14
13:44:31 cholera CiscoSecure: DEBUG - profile_valid_tcaching TRUE ending. !--- The TokenCaching
takes place. Jun 14 13:44:31 cholera CiscoSecure: DEBUG - cache_insert (key<4>,
```

```
val<10><3435598216>, port_type<3>) Jun 14 13:44:31 cholera CiscoSecure: DEBUG - Cisco Cached  
Tokens : 1 Jun 14 13:44:31 cholera CiscoSecure: INFO - sdi_verify(17477): rtn 1 Jun 14 13:44:31  
cholera CiscoSecure: DEBUG - Authentication - LOGIN successful; [NAS=lynch.cisco.com,  
Port=BRI0:1, User=fadi, Priv=1] !--- The authentication of the second BRI channel begins. Jun 14  
13:44:31 cholera CiscoSecure: DEBUG - AUTHENTICATION START request (76f91a6c) Jun 14 13:44:31  
cholera CiscoSecure: INFO - The character * was found in username:  
username=fadi,passcode=3435598216 Jun 14 13:44:31 cholera CiscoSecure: DEBUG - sdi_challenge  
response timeout 5 Jun 14 13:44:31 cholera CiscoSecure: DEBUG - AceInit() Jun 14 13:44:31  
cholera CiscoSecure: DEBUG - AceInit(29111), ace rc=150, ed=1039984 Jun 14 13:44:31 cholera  
CiscoSecure: DEBUG - acsWaitForSingleObject (29111) begin Jun 14 13:44:31 cholera CiscoSecure:  
DEBUG - aceCB(29111) Jun 14 13:44:31 cholera CiscoSecure: DEBUG - aceCB(29111) AceGetUserData,  
ace rc=1, ed=1039984 Jun 14 13:44:31 cholera CiscoSecure: DEBUG - aceCB(29111):  
AceGetAuthenticationStatus, ace rc=1, acm rc=0 Jun 14 13:44:31 cholera CiscoSecure: DEBUG -  
aceCB(29111): return Jun 14 13:44:31 cholera CiscoSecure: DEBUG - acsWaitForSingleObject(0)  
(29111) Jun 14 13:44:31 cholera CiscoSecure: DEBUG - acsWaitForSingleObject (29111) end, rc=0  
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - AceInit(29111), continue, acm rc=0 Jun 14 13:44:31  
cholera CiscoSecure: DEBUG - AceSetUsername(29111), username=fadi Jun 14 13:44:31 cholera  
CiscoSecure: DEBUG - AceSetUsername(29111), ace rc=1 Jun 14 13:44:31 cholera CiscoSecure: INFO -  
sdi_challenge(29111): rtn 1, state=GET_PASSCODE, user=fadi Jun 14 13:44:31 cholera CiscoSecure:  
DEBUG - Token Caching. timeout_value is: 30 Jun 14 13:44:31 cholera CiscoSecure: DEBUG - Token  
Caching. timeout enabled value: 30 Jun 14 13:44:31 cholera CiscoSecure: DEBUG -  
profile_valid_tcaching TRUE ending. !--- Checks with the cached token for the user "fadi". Jun  
14 13:44:31 cholera CiscoSecure: DEBUG - Token Caching. USER : fadi Jun 14 13:44:31 cholera  
CiscoSecure: DEBUG - PASSWORD : 3435598216 len: 10 Jun 14 13:44:31 cholera CiscoSecure: DEBUG -  
hashval_str: 3435598216 len: 10 Jun 14 13:44:31 cholera CiscoSecure: DEBUG - port_type : BRI  
len: 3 Jun 14 13:44:31 cholera CiscoSecure: DEBUG - Token Caching. HIT. Jun 14 13:44:31 cholera  
CiscoSecure: DEBUG - AceClose(29111) Jun 14 13:44:31 cholera CiscoSecure: INFO - sdi(29111):  
fadi free external_data memory, state=GET_PASSCODE Jun 14 13:44:31 cholera CiscoSecure: INFO -  
sdi_verify(29111): rtn 1 Jun 14 13:44:31 cholera CiscoSecure: DEBUG - Authentication - LOGIN  
successful; [NAS=lynch.cisco.com, Port=BRI0:2, User=fadi, Priv=1] !--- After 30 seconds the  
cached token expires. Jun 14 13:45:03 cholera CiscoSecure: DEBUG - Expiring Cisco Token Cache  
Entry Jun 14 13:45:03 cholera CiscoSecure: DEBUG - Cisco Cached Tokens : 0
```

Informações Relacionadas

- [Recomendações de Segurança da Cisco, respostas, e observações](#)
- [Página de Suporte do Produto CiscoSecure UNIX](#)
- [Página de Suporte do Produto CiscoSecure ACS for Windows](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)