# Design- und Implementierungsleitfaden für TokenCaching

## Inhalt



## Einführung

In diesem Dokument wird die Einrichtung und Fehlerbehebung von TokenCaching erläutert. Point-to-Point Protocol (PPP)-Sitzungen für Benutzer des ISDN-Terminaladapters (TA) werden in der Regel am Benutzer-PC beendet. Dadurch kann der Benutzer die PPP-Sitzung auf die gleiche Weise wie eine asynchrone (Modem-)DFÜ-Verbindung steuern, d. h. die Sitzung bei Bedarf verbinden und trennen. Dadurch kann der Benutzer das Password Authentication Protocol (PAP) verwenden, um das einmalige Kennwort (OTP) für die Übertragung einzugeben.

Wenn jedoch der zweite B-Kanal automatisch gestartet werden soll, muss der Benutzer zur Eingabe eines neuen OTP für den zweiten B-Kanal aufgefordert werden. PC PPP-Software sammelt kein zweites OTP. Stattdessen versucht die Software, das gleiche Kennwort zu verwenden, das für den primären B-Kanal verwendet wird. Der Token Card-Server verweigert die Wiederverwendung eines OTP-Dienstprogramms. Cisco Secure ACS für UNIX (Version 2.2 und höher) und Cisco Secure ACS für Windows (2.1 und höher) führen TokenCaching aus, um die Verwendung desselben OTP auf dem zweiten B-Kanal zu unterstützen. Diese Option erfordert den AAA-Server (Authentication, Authorization, Accounting), um Statusinformationen über die Verbindung des Tokenbenutzers zu erhalten.

Weitere Informationen finden Sie unter Unterstützen von Einmalkennwörtern auf ISDN.

## Voraussetzungen

## Anforderungen

In diesem Dokument wird davon ausgegangen, dass Sie diese bereits korrekt konfiguriert haben:

- Ein DFÜ-Modem, das ordnungsgemäß funktioniert.
- Der ordnungsgemäß konfigurierte Network Access Server (NAS) mit AAA, der auf Cisco Secure ACS UNIX oder ACS Windows verweist.
- ACE/SDI ist bereits mit Cisco Secure ACS UNIX oder ACS Windows eingerichtet und funktioniert ordnungsgemäß.

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Secure ACS Unix 2.2 oder höher
- Cisco Secure ACS Windows 2.1 oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

# Konfigurieren

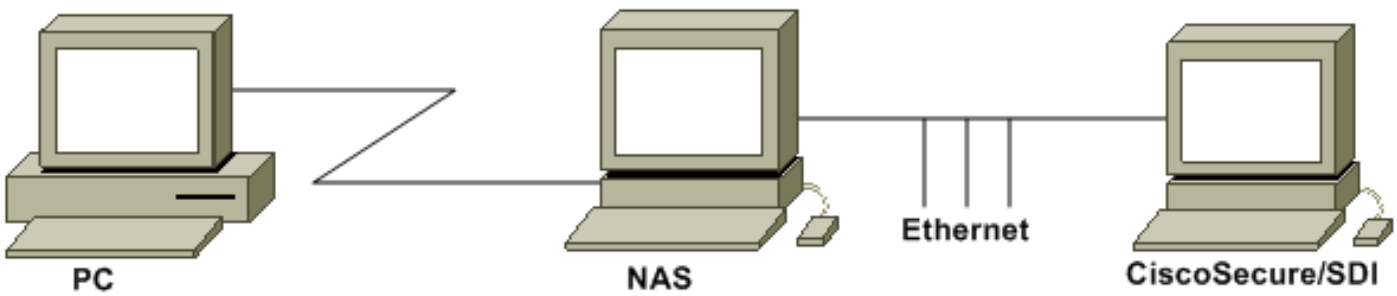
In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

**Hinweis:** Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

## Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:

Ein PC wählt sich in ein NAS- und ISDN-Modem ein und ist für den **ppp-Multilink-**Befehl konfiguriert.



## Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Konfigurieren der Eingabe von Benutzernamen und Kennwort
- TokenCaching auf CiscoSecure ACS Windows konfigurieren
- TokenCaching in CiscoSecure ACS UNIX konfigurieren

## Konfigurieren der Eingabe von Benutzernamen und Kennwort

In diesem Dokument verwendet das NAS-Gerät Challenge Handshake Authentication Protocol (CHAP) für die PPP-Sitzung zusammen mit dem einmaligen SDI-Kennwort. Wenn Sie CHAP verwenden, geben Sie das Kennwort in diesem Formular ein:

- **username** - fadi*pin+code (beachten Sie das * im Benutzernamen)
- **Kennwort** - Kennwort

Ein Beispiel hierfür ist: username = fadi, chap password = cisco, pin = 1234 und der Code, der auf dem Token angezeigt wird, ist 987654. Daher gibt der Benutzer Folgendes ein:

- **Benutzername** - fadi*1234987654
- **password** - cisco

**Hinweis:** Wenn CiscoSecure und das NAS-Gerät für PAP konfiguriert wurden, können der Benutzername und das Token wie folgt eingegeben werden:

- **Benutzername** - Benutzername*Pin+Code
- **Kennwort**:

Oder:

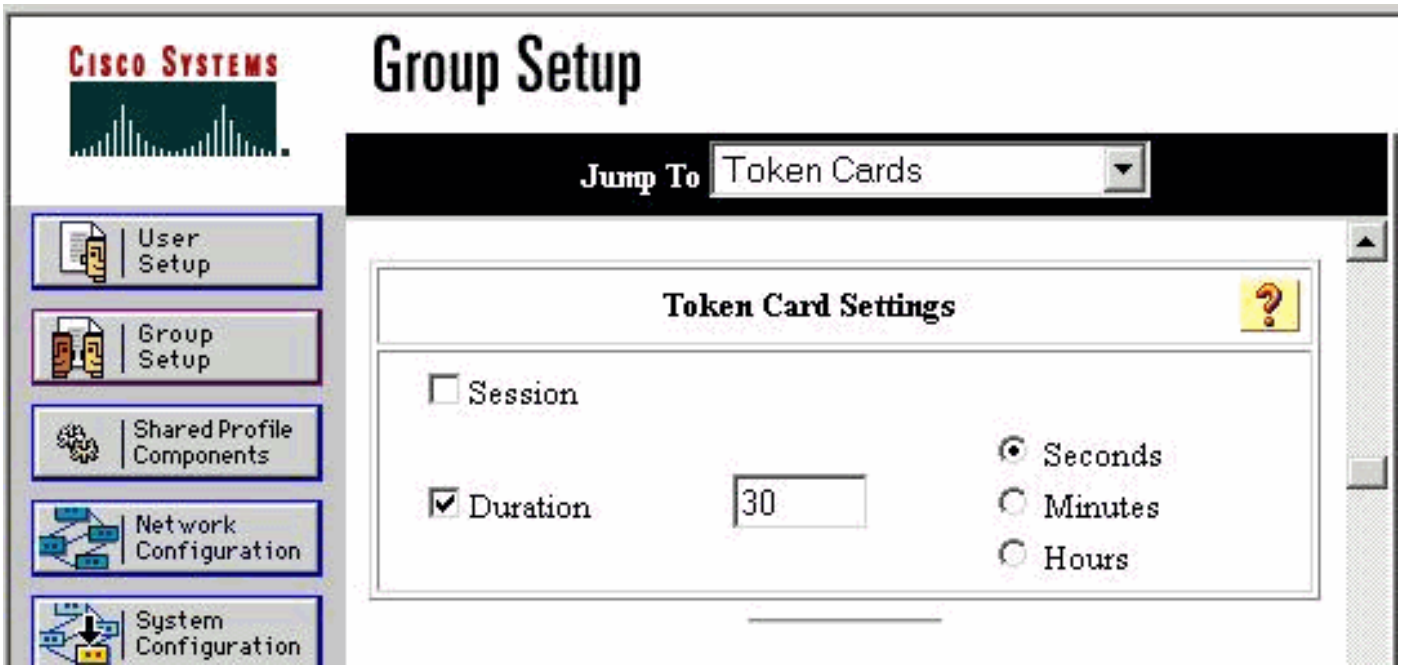
- **Benutzername** - Benutzername
- **Kennwort**: pin+code

## TokenCaching auf CiscoSecure ACS Windows konfigurieren

Der Cisco Secure ACS-Windows-Benutzer oder die -Gruppe ist wie gewohnt eingerichtet, wobei PPP-IP und PPP-LCP bei Verwendung von TACACS+ aktiviert sind. Wenn Sie RADIUS verwenden, müssen diese konfiguriert werden:

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

Darüber hinaus können die TokenCaching-Parameter für die Gruppe überprüft werden, wie in diesem Beispiel gezeigt:




## TokenCaching in CiscoSecure ACS UNIX konfigurieren

Es gibt vier TokenCaching-Attribute. Das Attribut config_token_cache_absolute_timeout (in Sekunden) wird in der Datei $install_directory/config/CSU.cfg festgelegt. Die anderen drei Attribute (Festlegen der Token-Zwischenspeicherung für Server, Festlegen der Methode für das Zwischenspeichern von Servertoken, Festlegen der Methode für das Zwischenspeichern von Servertoken, Festlegen der Methode für das Zwischenspeichern von Servertoken und Festlegen des Timeouts für das Zwischenspeichern von Servertoken) werden in den Benutzer- oder Gruppenprofilen festgelegt. Für dieses Dokument wird das globale Attribut config_token_cache_absolute_timeout in der Datei $install_directory/config/CSU.cfg auf Folgendes festgelegt:

```
NUMBER config_token_cache_absolute_timeout = 300;
```

Die TokenCaching-Attributprofile des Benutzer- und Gruppenservers werden wie in diesem Beispiel gezeigt konfiguriert:

```
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 } } }
```

# Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

# Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

## Debuggen von TokenCaching auf CiscoSecure ACS UNIX

Dieses CiscoSecure UNIX-Protokoll zeigt eine erfolgreiche Authentifizierung mit TokenCaching, wenn die Authentifizierung auf zwei BRI-Kanälen erfolgt:

```
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
```

# Zugehörige Informationen

- Cisco Sicherheitsempfehlungen, Antworten und Benachrichtigungen
- Support-Seite für CiscoSecure UNIX-Produkte
- Support-Seite für CiscoSecure ACS für Windows-Produkte
- Technischer Support und Dokumentation - Cisco Systems