

TokenCaching Design and Implementation Guide

Document ID: 10220

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations
- Configure Username and Password Input
- Configure TokenCaching on CiscoSecure ACS Windows
- Configure TokenCaching in CiscoSecure ACS UNIX

Verify

Troubleshoot

- Debug TokenCaching on CiscoSecure ACS UNIX

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

The scope of this document is to discuss the setup and troubleshoot of TokenCaching. Point-to-Point Protocol (PPP) sessions for ISDN terminal adapter (TA) users are typically terminated at the user PC. This allows the user to control the PPP session in the same manner as an async (modem) dialup connection, which means connect and disconnect the session as needed. This permits the user to use Password Authentication Protocol (PAP) in order to enter the one-time password (OTP) for transport.

However, if the second B channel is designed to come up automatically, the user must be prompted for a new OTP for the second B channel. PC PPP software does not collect the second OTP. Instead, the software tries to use the same password used for the primary B channel. The Token Card server denies the re-use of an OTP by design. CiscoSecure ACS for UNIX (version 2.2 and later) and CiscoSecure ACS for Windows (2.1 and later) perform TokenCaching in order to support the use of the same OTP on the second B channel. This option requires the authentication, authorization, and accounting (AAA) server to maintain state information about the connection of the token user.

Refer to Supporting One-time Passwords on ISDN for more information.

Prerequisites

Requirements

This document assumes that you already have these configured correctly:

- A dialup modem that works properly.
- The Network Access Server (NAS) configured properly, with AAA that points to CiscoSecure ACS UNIX or ACS Windows.
- ACE/SDI is already setup with CiscoSecure ACS UNIX or ACS Windows, and works properly.

Components Used

The information in this document is based on these software and hardware versions:

- CiscoSecure ACS Unix 2.2 or later
- CiscoSecure ACS Windows 2.1 or later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Configure

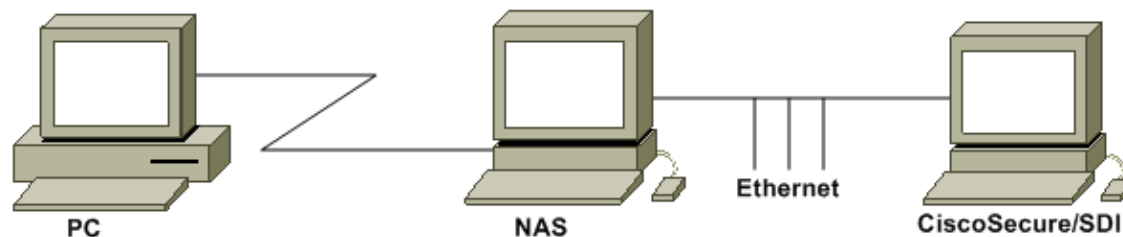
In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:

A PC dials into a NAS and the ISDN modem, and is configured for the **ppp multilink** command.



Configurations

This document uses these configurations:

- Configure Username and Password Input
- Configure TokenCaching on CiscoSecure ACS Windows
- Configure TokenCaching in CiscoSecure ACS UNIX

Configure Username and Password Input

In this document, the NAS uses Challenge Handshake Authentication Protocol (CHAP) for the PPP session along with the SDI one-time password. If you use CHAP, enter the password in this form:

- **username** fadi*pin+code (note the * in the username)
- **password** chappassword

An example of this is: username = fadi, chap password = cisco, pin = 1234, and the code that shows on the token is 987654. Therefore, the user enters this:

- **username** fadi*1234987654
- **password** cisco

Note: If CiscoSecure and the NAS were configured for PAP, the username and token can be entered as this:

- **username** username*pin+code
- **password**

Or:

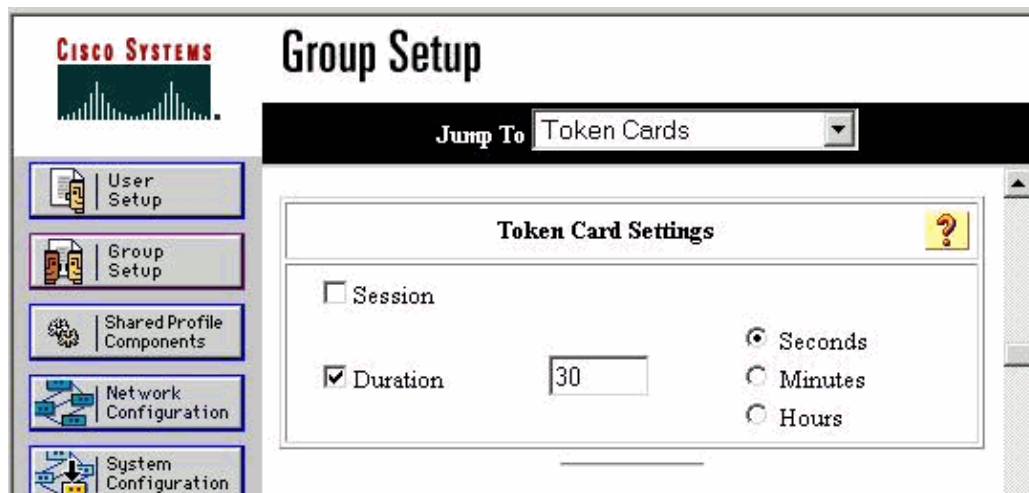
- **username** username
- **password** pin+code

Configure TokenCaching on CiscoSecure ACS Windows

The CiscoSecure ACS Windows user or group is set up as usual, with PPP IP and PPP LCP checked if you use TACACS+. If you use RADIUS, these must be configured:

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

In addition, the TokenCaching parameters can be checked for the group as shown in this example:



Configure TokenCaching in CiscoSecure ACS UNIX

There are four TokenCaching attributes. The `config_token_cache_absolute_timeout` (in seconds) attribute is set in the `$install_directory/config/CSU.cfg` file. The other three attributes (`set server token-caching`, `set server token-caching-expire-method`, and `set server token-caching-timeout`) are set in the user or group profiles. For this document, the global attribute `config_token_cache_absolute_timeout` is set to this in the `$install_directory/config/CSU.cfg` file:

```
NUMBER config_token_cache_absolute_timeout = 300;
```

The user and group server TokenCaching attribute profiles are configured as shown in this example:

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
}
}
}
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Debug TokenCaching on CiscoSecure ACS UNIX

This CiscoSecure UNIX log shows a successful authentication with TokenCaching, when authentication occurs on two BRI channels:

```
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: 1
Jun 14 13:44:31 cholera CiscoSecure: DEBUG - hashval_str: 3435598216 len: 1
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
```

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [CiscoSecure ACS for UNIX](#)
- [Cisco Security Advisories, Responses, and Notices](#)
- [CiscoSecure UNIX Product Support Page](#)
- [Cisco Secure ACS for Windows](#)
- [CiscoSecure ACS for Windows Product Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 24, 2007

Document ID: 10220
