# Eigenschappen draadloze LAN-controller voor IDS-handtekeningen

## Inhoud



## Inleiding

Dit document beschrijft hoe u inbraakdetectiesysteem (IDS)-handtekeningen kunt configureren in Cisco Wireless LAN (WLAN) Controller software release 3.2 en eerdere releases.

## Voorwaarden

### Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de WLAN-softwarerelease 3.2 en hoger.

### Conventies

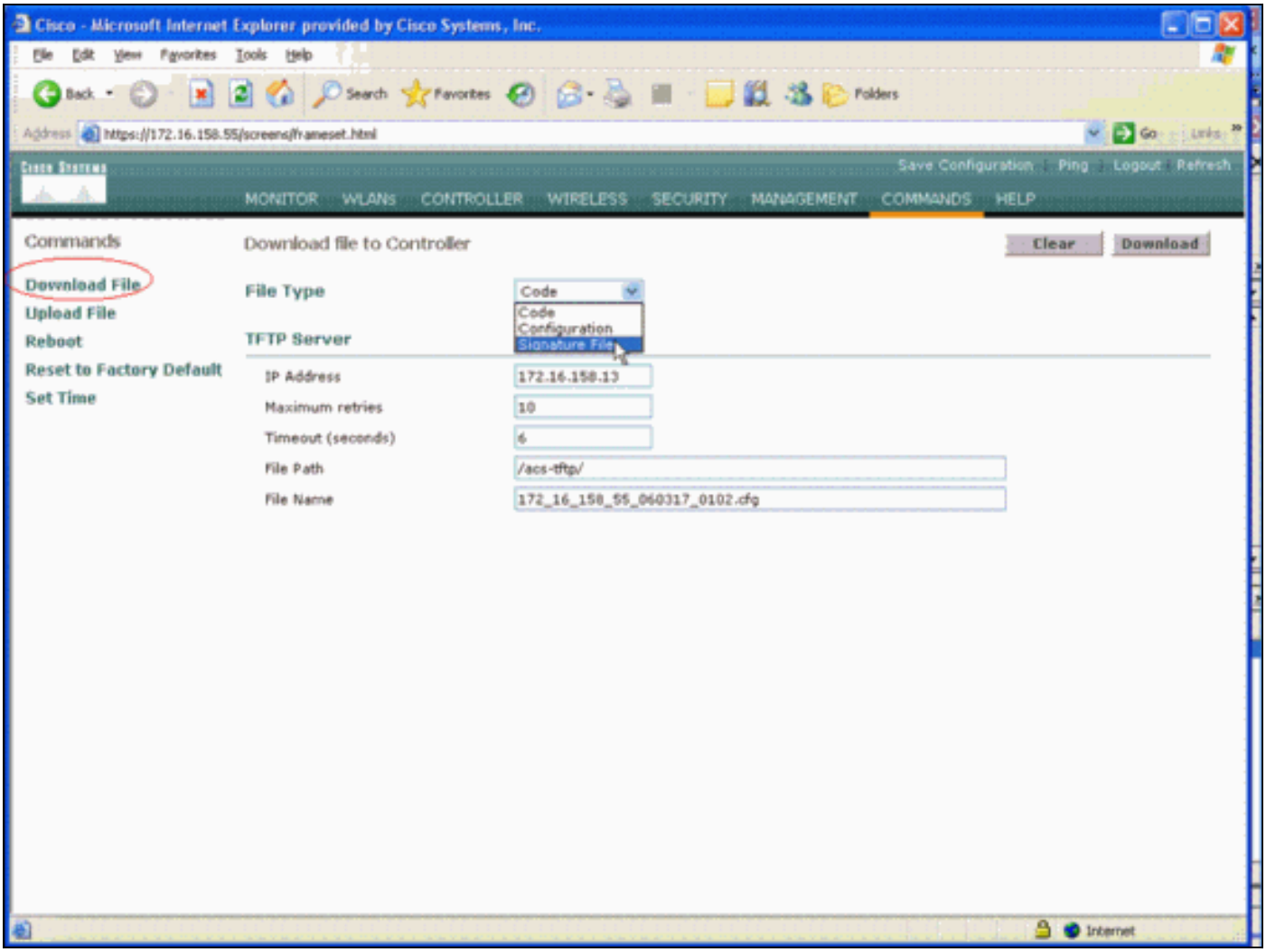
Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

## Achtergrondinformatie

U kunt het IDS-bestand voor handtekening uploaden, dat u kunt bewerken (of voor documentatiebeoordeling). Kies **Opdrachten > Upload File > Signaalbestand**. Om een gewijzigd IDS-bestand te downloaden selecteert u **Opdrachten > Bestand > Handelsbestand**. Nadat u een

bestand met handtekeningen aan de controller hebt gedownload, worden alle toegangspunten (AP's) die op de controller zijn aangesloten, in real time verververst met de nieuw bewerkte signatuurparameters.

Dit venster toont hoe u het bestand met handtekeningen kunt downloaden:




Het IDS-tekstbestand heeft negen parameters voor elke IDS-handtekening. U kunt deze tekenparameters wijzigen en nieuwe aangepaste handtekeningen schrijven. Zie het formaat dat de sectie Controller IDS-parameters van dit document biedt.

## Controller IDS-parameters

Alle handtekeningen *moeten* in deze indeling beschikken:

```
Name = <str>, Ver = <int>, Preced = <int>, FrmType = <frmType-type>, Pattern =
<pattern-format>, Freq = <int>, Interval = <int>, Quiet = <int>, Action = <action-val>,
Desc = <str>
```

De maximale lengte van de regel is 1000 tekens. Lijnen die langer zijn dan 1000 worden niet correct geparseerd.

Alle regels die beginnen met # in het IDS-tekstbestand worden als opmerkingen beschouwd en worden overgeslagen. Wordt ook overgeslagen in alle lege regels, die lijnen met slechts whitespace of newline zijn. De eerste niet-commentaar, niet-blanke regel *moet* de sleutelrevisie

hebben. Als het bestand een door Cisco meegeleverd bestand voor handtekeningen is, mag u de waarde van de herziening niet wijzigen. Cisco gebruikt deze waarde om te beheren of signatuurbestanden worden vrijgegeven. Als het bestand handtekeningen bevat die door de eindgebruiker zijn gemaakt, *moet* de waarde van de herziening op maat zijn (Revision = douane).

De negen parameters voor IDS-handtekening die u kunt wijzigen zijn:

- **Naam** = handtekening Dit is een unieke string die de signatuur identificeert. De maximum lengte van de naam is 20 tekens.
- **Vooraf** = signatuur. Dit is een unieke ID die de voorrang aangeeft van de handtekening onder alle handtekeningen die in het bestand voor handtekeningen zijn gedefinieerd. Er *moet* één penning per handtekening zijn.
- **FrmType** = type frame. Deze parameter kan waarden uit de lijst <frmType-val>halen. Er *moet* één FrmType-token zijn. Het <frmType-val> kan slechts één van deze twee zoekwoorden zijn:steungegevensHet <frmType-val> geeft aan of deze handtekening gegevens of beheerframes detecteert.
- **Patroon** = signatuur. De symbolische waarde wordt gebruikt om pakketten te detecteren die overeenkomen met de handtekening. Er *moet* ten minste één Patronentoken per handtekening zijn. Er kunnen wel vijf van zulke penningen per handtekening zijn. Als de handtekening meer dan één dergelijke token heeft, moet een pakje overeenkomen met de waarden van alle penningen zodat het pakje overeenkomt met de handtekening.Wanneer AP een pakket ontvangt, neemt AP de byte stroom die bij <offset> begint, en met het <masker>, en vergelijkt het resultaat met <patroon>. Als AP een overeenkomst vindt, overweegt AP het pakket met de handtekening. Het <patroon-formaat> kan worden voorafgegaan door de onderhandelaar "!". In dat geval, worden alle pakketten die FAIL de overeenkomende werking vertonen die deze sectie beschrijft, beschouwd als een overeenkomst met de handtekening.
- **Freq** = pakketfrequentie in pakketten/interval. De waarde van deze token geeft aan hoeveel pakketten per meetinterval aan deze handtekening moeten voldoen voordat de signatuur Actie wordt uitgevoerd. Een waarde van 0 geeft aan dat de signatuur Actie wordt genomen elke keer dat een pakje bij de handtekening aansluit. De maximale waarde voor deze token is 65.535. Er *moet* één Freq-token per handtekening zijn.
- **Intervaal** = meetinterval in seconden. De waarde van deze token geeft de periode aan die de drempel (d.w.z. de Freq) aangeeft. De standaardwaarde voor dit token is 1 seconde. De maximale waarde voor dit token is 3600.
- **Stil** = stille tijd in seconden. De waarde van deze token geeft de hoeveelheid tijd aan die moet doorgeven terwijl AP geen pakketten ontvangt die overeenkomen met de handtekening voordat AP bepaalt dat de aanval waarvan de handtekening aangeeft, is neergestort. Als de waarde van het Freq token 0 is, wordt deze token genegeerd. Er *moet* één Quiet token zijn per handtekening.
- **Actie** = Handeling tot ondertekening. Dit geeft aan wat AP moet doen als een pakje met de handtekening overeenkomt. Deze parameter kan waarden uit de lijst <action-val> halen. Er *moet* één Action token zijn per handtekening. Het <action-val> kan slechts één van deze twee zoekwoorden zijn:geen = niets doen .rapport = rapporteert de partij aan de switch .
- **Desc** = beschrijving van de handtekening. Dit is een string die het doel van de signatuur beschrijft. Wanneer een signatuur overeenkomt met een Simple Network Management Protocol (SNMP)-val, wordt deze string aan de val geleverd. De maximale lengte van de beschrijving is 100 tekens. Er *moet* één Desc-token zijn per handtekening.

# IDS-standaardhandtekeningen voor controllers

Deze IDS-handtekeningen verzenden met de controller als "standaard IDS-handtekeningen". U kunt al deze signatuurparameters wijzigen, zoals de sectie Controller IDS-parameters beschrijft.

```
Revision = 1.000
Name = "Bcast deauth", Ver = 0, Preced= 1, FrmType = mgmt, Pattern = 0:0x00C0:0x03FF,
Pattern = 4:0x01:0x01, Freq=30, Quiet = 300, Action = report, Desc="Broadcast
Deauthentication Frame"

Name = "NULL probe resp 1", Ver = 0, Preced = 2, FrmType = mgmt, Pattern =
0:0x0050:0x03FF, Pattern = 36:0x0000:0xFFFF, Freq=1, Quiet = 300, Action = report, Desc =
"NULL Probe Response - Zero length SSID element"

Name = "NULL probe resp 2", Ver = 0, Preced = 3, FrmType = mgmt, Pattern =
0:0x0050:0x03FF, Pattern = !36:0x00:0xFF, Freq=1, Quiet = 300, Action = report, Desc =
"NULL Probe Response - No SSID element"

Name = "Assoc flood", Ver = 0, Preced= 4, FrmType = mgmt, Pattern = 0:0x0000:0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Association Request flood"

Name = "Auth Flood", Ver = 0, Preced= 5, FrmType = mgmt, Pattern = 0: 0x00b0: 0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Authentication Request flood"

Name = "Reassoc flood", Ver = 0, Preced= 5, FrmType = mgmt, Pattern = 0:0x0020:0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Reassociation Request flood"

Name = "Broadcast Probe flood", Ver = 0, Preced= 6, FrmType = mgmt, Pattern =
0:0x0040:0x03FF, Pattern = 4:0x01:0x01, Pattern = 24:0x0000:0xFFFF, Freq=50, Quiet = 600,
Action = report, Desc="Broadcast Probe Request flood"

Name = "Disassoc flood", Ver = 0, Preced= 7, FrmType = mgmt, Pattern = 0:0x00A0:0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Disassociation flood"

Name = "Deauth flood", Ver = 0, Preced= 8, FrmType = mgmt, Pattern = 0:0x00C0:0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Deauthentication flood"

Name = "Res mgmt 6 & 7", Ver = 0, Preced= 9, FrmType = mgmt, Pattern = 0:0x0060:0x03EF,
Freq=5, Quiet = 600, Action = report, Desc="Reserved management sub-types 6 and 7"

Name = "Res mgmt D", Ver = 0, Preced= 10, FrmType = mgmt, Pattern = 0:0x00D0:0x03FF,
Freq=5, Quiet = 600, Action = report, Desc="Reserved management sub-type D"

Name = "Res mgmt E & F", Ver = 0, Preced= 11, FrmType = mgmt, Pattern = 0:0x00E0:0x03EF,
Freq=5, Quiet = 600, Action = report, Desc="Reserved management sub-types E and F"

Name = "EAPOL flood", Ver = 0, Preced= 12, FrmType = data, Pattern = 0:0x0108:0x03FF,
Pattern = 30:0x888E:0xFFFF, Freq=50, Quiet = 300, Action = report, Desc="EAPOL Flood
Attack"

Name = "NetStumbler 3.2.0", Ver = 0, Preced= 13, FrmType = data, Pattern =
0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Pattern =
36:0x466c7572:0xFFFFFFFF, Freq = 1, Quiet = 300, Action = report, Desc="NetStumbler 3.2.0"

Name = "NetStumbler 3.2.3", Ver = 0, Preced= 14, FrmType = data, Pattern =
0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Pattern =
36:0x416C6C20:0xFFFFFFFF, Freq = 1, Quiet = 600, Action = report, Desc="NetStumbler 3.2.3"

Name = "NetStumbler 3.3.0", Ver = 0, Preced= 15, FrmType = data, Pattern =
0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Pattern =
```

```
36:0x20202020:0xFFFFFFFF, Freq = 1, Quiet = 600, Action = report, Desc="NetStumbler 3.3.0"

Name = "NetStumbler generic", Ver = 0, Preced= 16, FrmType = data, Pattern =
0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Freq = 1,
Quiet = 600, Action = report, Desc="NetStumbler"

Name = "Wellenreiter", Ver = 0, Preced= 17, FrmType = mgmt, Pattern = 0:0x0040:0x03FF,
Pattern = 24:0x001d746869735f69735f757365645f666f725f77656c6c656e726569:
0xffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff, Freq = 1, Quiet = 600,
Action = report, Desc="Wellenreiter"
```

## IDS-berichten

Dankzij versie 4.0 van de draadloze LAN-controller krijgt u dit IDS-bericht mogelijk.

```
Big NAV Dos attack from AP with Base Radio MAC 00:0f:23:xx:xx:xx,
Slot ID 0 and Source MAC 00:00:00:00:00:00
```

Dit IDS-bericht geeft aan dat het veld 802.11 Network Allocation Vector (NAV) in het Wireless 802.11-frame te groot is en dat het draadloze netwerk onder een DOS-aanval kan vallen (of dat er een verkeerde client is).

Nadat u dit IDS-bericht hebt ontvangen, is de volgende stap de betreffende client te traceren. U moet de client lokaliseren op basis van de signaalsterkte met een draadloze snuiver in het gebied rond het access point of de locatieserver gebruiken om de positie ervan te bepalen.

Het NAV-veld is het virtuele drager-zintuig dat wordt gebruikt om aanrijdingen tussen verborgen terminals (draadloze klanten die de huidige draadloze client niet kan detecteren wanneer deze wordt verzonden) te verzachten bij 802.11-transmissies. De verborgen terminals creëren problemen omdat het toegangspunt pakketten van twee cliënten kan ontvangen die naar het toegangspunt kunnen verzenden maar niet de uitzendingen van elkaar kunnen ontvangen. Wanneer deze klanten gelijktijdig verzenden, botsen hun pakketten op het toegangspunt en dit resulteert in het toegangspunt dat geen van beide pakketten duidelijk ontvangt.

Wanneer een draadloze client een gegevenspakket naar het access point wil verzenden, geeft hij feitelijk een vierpakketsequentie over, de RTS-CTS-DATA-ACK pakketsequentie. Elk van de vier 802.11 frames heeft een NAV-veld dat het aantal microseconden aangeeft dat het kanaal gereserveerd is voor een draadloze client. Tijdens de handdruk RTS/CTS tussen de draadloze client en het access point, verstuurt de draadloze client een klein RTS-kader dat een NAV-interval omvat dat groot genoeg is om de gehele sequentie te voltooien. Dit omvat het CTS-kader, het gegevenskader en het daaropvolgende herkenningskader vanuit het access point.

Wanneer de draadloze client het RTS-pakket met de NAV-set doorgeeft, wordt de overgedragen waarde gebruikt om de NAV-timers in te stellen op alle andere draadloze clients die gekoppeld zijn aan het access point. Het toegangspunt antwoordt op het RTS-pakket van de client met een CTS-pakket dat een nieuwe NAV-waarde bevat die is bijgewerkt om rekening te houden met de tijd die al tijdens de pakketreeks is verstreken. Nadat het CTS-pakket is verzonden, heeft elke draadloze client die vanaf het access point kan ontvangen, hun NAV-timer bijgewerkt en alle transmissies tot hun NAV-timer 0 bereikt. Dit houdt het kanaal vrij voor de draadloze client om het proces van het verzenden van een pakket naar het access point te voltooien.

Een aanvaller zou dit virtuele drager-zintuig kunnen exploiteren door op het NAV-veld een grote tijd te eisen. Dit voorkomt dat andere klanten pakketten verzenden. De maximumwaarde voor NAV is 32767, of grofweg 32 milliseconden op 802.11b netwerken. In theorie hoeft een aanvaller alleen maar ruwweg 30 pakketten per seconde te verzenden om alle toegang tot het kanaal te

blokkeren.

## Gerelateerde informatie

- Cisco 4400 Series draadloze LAN-controllers
- Cisco 4100 Series draadloze LAN-controllers
- Cisco 2000 Series draadloze LAN-controllers
- Cisco-signaalmotoren voor inbraakdetectiesysteem, versie 3.1
- Technische ondersteuning en documentatie – Cisco Systems