

2.2 هقي ببطتو ليمعلا دادعإ نيوكت

تايوت حمل

[عمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[عمدختسملا تانوكملا](#)

[نيوكتلا](#)

[تاننيوكتلا](#)

[ليمعلا دادمإ نيوكت 1. بابلا](#)

[AnyConnect عمزح ليمحت 1. ةوطخللا](#)

[AnyConnect قفاوت ةدحو ليزنت 2. ةوطخللا](#)

[عضولا فيرعت فلم عاشنا 3. ةوطخللا](#)

[AnyConnect نيوكت عاشنا 4. ةوطخللا](#)

[ليمعلا دادمإ تاسايس نيوكت 5. ةوطخللا](#)

[CP ل ليوختلا فيرعت فلم عاشنا 6. ةوطخللا](#)

[ليوختلا تاسايس نيوكت 7. ةوطخللا](#)

[عضولا نيوكت 2. بابلا](#)

[عضولا شيحت 1. ةوطخللا](#)

[قيبطت طرش عاشنا 2. ةوطخللا](#)

[عضولا تابلطتم عاشنا 3. ةوطخللا](#)

[عضولا جهن عاشنا 4. ةوطخللا](#)

[قرمتسملا ةبقارملا لينمزللا لصالا ريغت \(ةيرايتخ\) 5. ةوطخللا](#)

[تاقيبطتلا عم قفاوت عاشنا \(ةيرايتخ\) 6. ةوطخللا](#)

[ةحصللا نم ققحتلا](#)

[LiveLog](#)

[ةياهنلا ةطقن](#)

[عضولا ةسايس رصانع](#)

[ريراقت](#)

[ةلاجل بسح عضولا مييقت](#)

[ةياهنلا ةطقن بسح عضولا مييقت](#)

[اهجالص او اطاخألا فاشكتسا](#)

[ISE نم](#)

[AnyConnect نم](#)

[ةعئاشلا تالكشملا](#)

[ISE ل لوصولا AnyConnect ل رع رذعتي](#)

[EP ضرع ةقيرط نم تاقيبطتلا عم قفاوتلا عاشنا دنع "لاخ" اطاخ ISE ي قولي](#)

عمدقملا

Identity Service Engine ل رع قيبطتلا ةيؤر ةينامإ نيوكت ةيفيك دننتمسما اذه حضوي ةبقارم ةينامإ تاقيبطتلا ةيؤر ةينامإ كل حيتت. اهجالص او اهئاخأ فاشكتسا او 2.2 (ISE) ، تامولعمل هذه ل دننست تاسايس عاشنا و، ةياهنلا طاقن ل رع ةتبثملا تاقيبطتلا

طورش ب يفت تناك اذا عضولا نم ققحتل تايلمع اءنثا اهت ب ثت ةلازا وا تاق ي ب طتلا لتقو تاق ي ب طتلاب ةمئاق مادختساب ISE لى تامولعم يرود لكشب AnyConnect لسري . ةدحم عيمج لوح تامولعم عمج AnyConnect ل نكمي . اهلي غشت يراجلا / ةت ب ثملا تايلمعلاو (كلذ لى امو ، يرفشتلاو اضرتسملا) ةدحم تائف نم تاق ي ب طتلا وا تاق ي ب طتلا

ةيساسألا تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملاب ةيساسأ ةفرعم كي دل نوكت نأب Cisco ي صوت

- Cisco نم ةيوهلا ةمدخ كرحم
- لي مءلا دادم
- ISE Posture

ةمدختسملا تانوكملا

ةيلاتلا ةي دامل تانوكملاو جماربلا تارادصا لى دن تسملا اذ ة دراو لا تامولعمل دن تست

- Cisco Identity Service Engine ، رادصا 2.2.0.470
- Cisco AnyConnect 4.4.00243
- AnyConnect 4.2.468.0 عم قفاوتلا ةدحو
- Windows 7 لي غشتلا ماظن ل 1 ةمدخل ةمزح

نيوكتلا

تانويوكتلا

لي مءلا دادم نيوكت 1. بابلا

AnyConnect ةمزح لي مءلا 1. ةوطخلا

ISE لى عئائتنلا > لي مءلا دادم > عئائتنلا > ةسايسلا رصانع > ةسايسلا لى لقتنا 1. لي لحملا صرقل نم لي كولا دراوم > ةفاضا قوف رقنا

2. (AnyConnect مةزح) فلم رتخاو Cisco نم مةمدم مةزح ةئفلا دح:

Agent Resources From Local Disk

Category ⓘ

anyconnect-w...ploy-k9.pkg

▼ AnyConnect Uploaded Resources

| Name | Type | Version | Description |
|------------------------------------|--------------------------|-----------|------------------------------------|
| AnyConnectDesktopWindows 4.4.24... | AnyConnectDesktopWindows | 4.4.243.0 | AnyConnect Secure Mobility Clie... |

تاريغتلا ظفحل لاسرا قوف رقنا.

غلابل مةنراق. اهل مةمحت مةت يتلا مةزحلل ةيعةجرملا غلابملا ديكأت كنم بلطي نأ بجي ةمزلال فلت مدم نامضل بيولا لىل Cisco عقوم لىل مةمدملا ققحتلا

AnyConnect قفاوت ةدحو ليزنت 2. ةوطخلا

ىت Cisco عقوم نم لىل كول دراوم > ةفاضل قوف رقنا، لىل عملا ريفوت جئاتن ةحفص لىل ةيطم نل قفاوتلا ةدحو دح. ةرفوتلا ةيطم نل تادحولا لىل يوتحت ةذفان قثبنت ظفح قوف رقناو Windows لىل غشتلا ماظنل AnyConnect ل ةبولطملا

كب صاخلا ISE لىل غشتلا ماظن لىل تنرتنلا لىل اصتا كىدل نكى مل اذا، كذل نم ال دب ماظن لىل اهل مةمحتو Cisco.com نم قفاوتلا ةيطم نل ةدحو دح لىل زنت كنكم لىل AnyConnect مةزح ةقيرط سفنب كب صاخلا ISE لىل غشتلا

> تاداعلا > ماظنلا > ةرادلا لىل اهل مةمحت مةمق، كتكبش لىل كول ةحفص لىل كول ةحفص

عضولاء فيرعت فلم ءاشن | 3. ةوطخل

AnyConnect فيصوت وأ NAC لئكو > ةفاض | لعل رقنا لئمعلءا ءاءم | ءئائن ةءفص لعل
عضولاء لئكو فيرعت فلم ءاءاع | نم AnyConnect ءءو Posture

Posture Agent Profile Settings

Select a Category ▼
Select a Category
AnyConnect
NAC Agent

فلم ظءءل لاسر | لعل رقنا . ةبولطم لاء ءبعل لاء صئصء لاء فلم لوقء ءئم سءب مق
فئرعل.

AnyConnect نئوك ءاشن | 4. ةوطخل

ءئال ءمزل ءءو AnyConnect نئوك > ةفاض | لعل رقنا لئمعلءا رئفوء ءئائن ةءفص لعل
1: ةوطخل لعل فءل لئمءمء

* Select AnyConnect Package:

ظءءل لاسر | قوف رقنا ءبولطم لاء لوقء لاء لك ءبعل سءب مق . ءئفءاض لاء ءاراءل لئمءم بءئ
ءارئفءل:

* Select AnyConnect Package: AnyConnectDesktopWindows 4.4.243.0
* Configuration Name: AnyConnect Configuration
Description:
DescriptionValue
* Compliance Module: AnyConnectComplianceModuleWindows 4.2.468.0

AnyConnect Module Selection

- ISE Posture
- VPN
- Network Access Manager
- Web Security
- AMP Enabler
- ASA Posture
- Network Visibility
- Umbrella Roaming Security
- Start Before Logon
- Diagnostic and Reporting Tool

Profile Selection

* ISE Posture: AnyConnect Posture
VPN
Network Access Manager
Web Security
AMP Enabler
Network Visibility
Umbrella Roaming Security
Customer Feedback

Customization Bundle
Localization Bundle

(ةللاتلة ووطخال) ليمعلا دادعإ جهن في اذه مادختسإ متي . نيوكتلا مسا - نيوكتلا مسا

2. ووطخال في اهليزنت مت يتلا ءدحملا قفاوتلا ءحو - قفاوتلا ءحو

ةيعضو) AnyConnect Posture فيرعت فلم دح - ((ISE) ءوهلا تامدخ كرحم ءيعضو) ISE Posture
3. ووطخال في هؤاشنإ مت يذلا ((ISE) ءوهلا تامدخ كرحم

ليمعلا دادمإ تاسايس نيوكت 5. ووطخال

ديدحتو ، Windows ل دوجوم جهن ريرحت وأ ديدج جهن ءاشنإ . ليمعلا دادمإ > ءسايسلا للى لقتنا
لكلذ ءچيتن هؤاشنإ مت يذلا AnyConnect نيوكت

CP ل ليوختلا فيرعت فلم عاشن | 6. ةوطخلا

رقناو ليوختلا تافي صوت > ليوختلا > جئاتنلا > ةسايسلا رصانع > ةسايسلا لىل لقتنا
ليعمل دادم لخدم لىل هيوتلا ةداعال هن يكتب مق .ديج صي صخت فلم عاشن ل ةفاصل

Authorization Profiles > **New Authorization Profile**

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP) i

ACL

Value

Static IP/Host name/FQDN

Auto Smart Port

Advanced Attributes Settings

= - +

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=ISE-REDIRECT
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=4cb1f740-e371-11e6-92ce-005056873bd0&action=cpp

في صوتلا ظفحل لاسر لىل رقنا .

يذلا لاثملا اذه في (هيوتلا ةداعال لوصولا في مكحتلا ةمئاق عاشن | بجي هنأ ركذت
هيوتلا ةداعال لىل لوصولل (ةكبشلا لىل لوصولا زاغ) NAD لىل (ISE-Redirect) يمسي

ة كرح هيجوتللا ةداعإل ةيساسألل لوصولل ي ف مكحتللا ةمئاق ضررتت ال ب جي . ةبسانملا و HTTP رورم ة كرح هيجوت ةداعإ ب جي و . اهليل و DHCP و DNS و ISE PSN دق نم رورملا تادنتسمللا هذه ي ف (ACL) لوصولل ي ف مكحتللا مئاق ةني ع ىل ع روثعلا نكمي . HTTPS : [بيولل ةيزك رملل](#) ةقداصملا و [WLC](#) و [ISE](#) نيوكت لاثم ىل ع [بيولل ةيزك رملل](#) ةقداصملا [ةي وهلا تامدخ كرحم نيوكت لاثم و لوجم عم](#)

ليوختللا تاسايس نيوكت . 7 ةوطخللا

ةلاح نم ققحتللا عم تاسايسلا نم نيونثا ءاشناب مقو ، ضيوفت > ةسايس ىل لقتنا ع ضوللا :

| | | | |
|-------------------------------------|--------------|---|-------------------|
| <input checked="" type="checkbox"/> | POSTURED | if Session:PostureStatus EQUALS Compliant | then PermitAccess |
| <input checked="" type="checkbox"/> | CPP_REDIRECT | if Session:PostureStatus NOT_EQUALS Compliant | then CPP_REDIRECT |

نم هتنت مل و ا ةياهن ةطقن ىل ع AnyConnect تي ببت متي مل اذا ، نيوكتلا اذه مادختساب يئاهنلا مدختسملل نكمي . ليمعلا دادم لخدم ىل ا هيجوت ةداعإ متيس ف ، دع ب عضوللا ISE عضو نم ققحتللا و ISE فاشتك AnyConnect ل نكمي و ISE نم AnyConnect تي ببت

ظفة ققط

عضوللا نيوكت . 2 بابلا

عضوللا شي دحت . 1 ةوطخللا

يوتحي وهو . ةلاحلا شي دحتل ناللا شي دحت رقن او تاشي دحت > ةي عضو > تاداعإ > ةرادا ىل لقتنا ع تاسايسلا عضول بولطم وهو تاقبي بطتل OPSWAT ماظنل تافيرعت و تاططم ىل ع

رأ ليزنت كنكمي ف ، كب صاخلا ISE ىل ع تنرتن ا لاصتا كي دل نكي مل اذا ، كلذ نم ال دب م <https://www.cisco.com/web/secure/pmbu/posture-offline.html> نم عضوللا تاشي دحت ددحو لصتم ريغ ددح ، تاشي دحتلا > عضوللا > تاداعإلا > ماظنلا > ةراداللا ىل لاقتناللا فلملا ليمحتل ناللا شي دحت قوف رقنا . عضوللا تاشي دحت عم هليزنت مت يذلا فلملا عضوللا تاشي دحت تي ببت و

قبي بطت طارش ءاشناب . 2 ةوطخللا

راي عم عم قفاوتلا ةدحو عم طقف ةتبتمللا تاقبي بطتللا لوح تامولعم عم مجب AnyConnect موقبي (ثدخاللا و) 4.x .

نأينعي اذهو) طقف ققحتلا تاي لمع ءارج نكمي Compliance Module نم 3.x رادصالا عم
AnyConnect (ال ما ليغشتلا ديقة ددحمالا ءي لمعلا تناك اذا ام ققحتي AnyConnect).

تاعومجملا هذو نيوكت نكمي قيبطتلا ءلاح عم

- يراجلا تاي لمعلا لوح تامولعم عيمجتب AnyConnect موقوي - ليغشتلا ديقة + تبثم
تبثتلا تامولعم عمج لالخنم ايلا اهلغشت
- طقف تبثتلا تامولعم عمجي AnyConnect - لمعي ال + تبثم

ءئفلا و مسالا، ءيش لك :ءئفلا لك تبسح ريفوت عم

- تاقيبطتلا عيمج لوح تامولعم عمج AnyConnect لواحيسف ءيش لك ديقت ءلاح يفة
تبثتلا
- لاثملا لبيس ىلع .جهنلل نعيم قيبطت ديقت نكمي، مسالا ديقت ءلاح يفة

Provision by

At least one category must be selected *

- | | | |
|---------------------------------------|--|---|
| <input type="checkbox"/> Unclassified | <input type="checkbox"/> Data Loss Prevention | <input type="checkbox"/> Data Storage |
| <input type="checkbox"/> Browser | <input type="checkbox"/> Backup | <input type="checkbox"/> Patch Management |
| <input type="checkbox"/> Encryption | <input checked="" type="checkbox"/> Antiphishing | <input type="checkbox"/> VPN Client |
| <input type="checkbox"/> Anti-Malware | <input type="checkbox"/> Virtual Machine | <input type="checkbox"/> Firewall |
| <input type="checkbox"/> Messenger | <input type="checkbox"/> Public File Sharing | <input type="checkbox"/> Health Agent |

Vendor *

At least one product must be selected *

Selected Rows/Page 3 / 1 3 Total Rows

Refresh

Filter

| <input type="checkbox"/> | Product Name | Version |
|-------------------------------------|---------------------|---------|
| <input checked="" type="checkbox"/> | Anvi Smart Defender | 1.x |
| <input type="checkbox"/> | Anvi Smart Defender | 2.x |
| <input type="checkbox"/> | Anvi Smart Defender | ANY |

- ءئفلا نم ءزهجالا عيمج لوح تامولعم عيمجتب موقوي AnyConnect نإف، ءئف ديقت مت اذا
لاثملا لبيس ىلع .ءدحمالا

Provision by

At least one category must be selected *

- | | | |
|--|---|---|
| <input type="checkbox"/> Unclassified | <input type="checkbox"/> Data Loss Prevention | <input type="checkbox"/> Data Storage |
| <input type="checkbox"/> Browser | <input type="checkbox"/> Backup | <input type="checkbox"/> Patch Management |
| <input type="checkbox"/> Encryption | <input type="checkbox"/> Antiphishing | <input type="checkbox"/> VPN Client |
| <input checked="" type="checkbox"/> Anti-Malware | <input type="checkbox"/> Virtual Machine | <input type="checkbox"/> Firewall |
| <input type="checkbox"/> Messenger | <input type="checkbox"/> Public File Sharing | <input type="checkbox"/> Health Agent |

رصانع > جهنلا يف اهلي غشت متي يتلا ةتبتمل تاقي بطتلا لوح تامولعم عمج لجأ نم ةئبعتو ديدج طرش عاشنإل ةفاضل قوف رقنا ، قيبطتلا ةلاح > عضولا > طورشلا > جهنلا :حضوم وه امك ةبولطملا لوقحلا

Application Condition > New

Name *

Description

Operating System *

Compliance module

Check By *

Application State * Installed Running

Provision by

عضولا تابلطتم عاشنإ. 3. ةوطخل

ببلمت عاشنإب مق تابلطتملا > عضولا > جهناتنلا > ةسايسلا رصانع > ةسايسلا يف اهواشنإ متي يتلا قيبطتلا ةلاح عم ديدج

| Name | Operating Systems | Compliance Module | Stealth Mode | Conditions | Remediation Actions |
|-------------------------|-------------------|----------------------|----------------|------------------------|-----------------------------|
| USB_Block | for Windows All | using 4.x or later | using Disabled | met if USB_Check | then USB_Block |
| Apps_collection | for Windows All | using 4.x or later | using Disabled | met if Apps_Collection | then Message Text Only |
| Any_AV_Installation_Mac | for Mac OSX | using 3.x or earlier | using Disabled | met if ANY_av_mac_inst | then Message Text Only |
| Any_AV_Definition_Mac | for Mac OSX | using 3.x or earlier | using Disabled | met if ANY_av_mac_def | then AnyAVDefRemediationMac |
| Any_AS_Installation_Mac | for Mac OSX | using 3.x or earlier | using Disabled | met if ANY_as_mac_inst | then Message Text Only |
| Any_AS_Definition_Mac | for Mac OSX | using 3.x or earlier | using Disabled | met if ANY_as_mac_def | then AnyASDefRemediationMac |

عضولا جهن عاشنإ. 4. ةوطخل

تابلطتملا دحأ ني مضت بجي ، تاقي بطتلا لوح تامولعم عمج نم AnyConnect و ISE ني كم تل دق Posture > جهنلا يف عضولا جهن عاشنإ نكمي .عضولا جهن يف قيبطتلا طورش دحأ عم مادختسالا نم ديزمل تامولعم عمج يف بغرت تنك اذا قيقدت هنا يلعبلطتملا ني عت متي

Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

| Status | Rule Name | Identity Groups | Operating Systems | Compliance Module | Stealth mode | Other Conditions | Requirements |
|-------------------------------------|-----------|-----------------|-------------------|-------------------|--------------|-----------------------|-----------------|
| <input checked="" type="checkbox"/> | Apps | Any | Windows | 4.x or later | Disabled | (Optional) Dictionary | Apps_collection |

Apps_collection

- Mandatory
- Optional
- Audit

قمرتسملا ةبقارملا لمنزلا لصال ريغت (ةرياختا) 5 ةوطخلا

لوح تاثيرحت لاسر AnyConnect لىع اهيف بجي يتل تارملا دد نيوكتب كل ISE حمسي نكميو قئاقدا 5 لىل لمنزلا لصال نيغت متي يضارثفا لكشب ISE. لىل تاثيرحت لىل ةماع تاداع | > ةيعضو > تاداع | > ةرادا | ف هريغت

Posture General Settings

| | | |
|---|-----------|---------|
| Remediation Timer | 4 | Minutes |
| Network Transition Delay | 3 | Seconds |
| Default Posture Status | Compliant | |
| <input type="checkbox"/> Automatically Close Login Success Screen After | 0 | Seconds |
| <input checked="" type="checkbox"/> Continuous Monitoring Interval | 5 | Minutes |
| Acceptable Use Policy in Stealth Mode | Block | |

Posture Lease

Perform posture assessment every time a user connects to the network

Perform posture assessment every Days

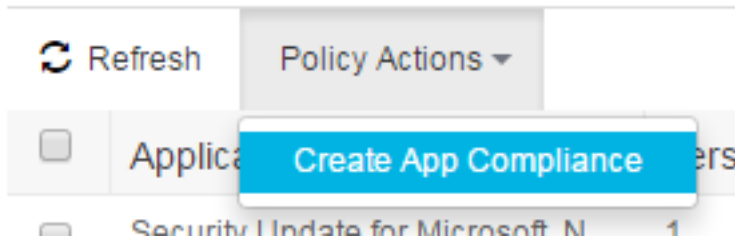
تاثيرحت لىل عم قفاوت عاشن | (ةرياختا) 6 ةوطخلا

ةيؤري ف تاثيرحت لىل عم قفاوت عاشن | نكمي، ةياهنلا ةطقن نم تانايبلا عيحت دعب [ةياهنلا ةطقن] > ةياهنلا طاقن > قايصل

1. قيبطت ديح:

| File Name | Version | Manufacturer | Product | Path |
|---|----------------|-----------------------|----------------------|--|
| Windows media player | 12.0.7593.2201 | Microsoft Corporation | Windows Media Player | C:\Program Files\Windows Media Player\wmplayer.exe |
| <input checked="" type="checkbox"/> FileZilla | 3.8.1.0 | FileZilla Project | FileShare | C:\Program Files (x86)\FileZilla\filezilla.exe |
| Security Update for Microsoft Windows 7 for x64-based Systems (KB2919442) | 1 | Microsoft Corporation | Windows Update | C:\Windows\SoftwareDistribution\Download\2919442\wuauclt.exe |

2. تاثيرحت لىل عم قفاوت عاشن | > جهنلا تاعارج | قوف رونا



3. ةقثب نم ةذفان يف لوقحلا ةئبعت:

Create Posture Application Compliance

Application Names *

Version 3.8.1.0 ANY

Compliance Name *

Description

Operating System * MacOSX Windows

Compliance module

Condition

Application State * Installed Running

Remediation

Remediation Type

Interval *

Retry Count *

Remediation Option * Uninstall Kill Process

Note: By default the above Condition & Remediation would be linked as a requirement.

Posture Policy
Posture Policy will be defined by configuring rules based on operating system and/or other conditions.

Identity Groups *

Cancel
Save Policy

4. ةجال عم ءارج اءضولا قيبطت طرش: ةيلالاتلا رصانعلا ءاشنإ بجي، ءهنلا ظفح قوف رقنا
ءضولا ءهن ءضولا بلطتم ءضولا قيبطت

ةحصللا نم ققحتلا

ءحص لكشب نيوكتلا لمع ءيكأتل مسقلا اءه مءءءسا.

LiveLog

ءي ءوتلا ءءاع + ءءاصملا: ءاءءملا ءضولا قفءء لثم قفءءلا وءبءي RADIUS LiveLog يف
قفءءملا ءضولا ءسائس ءقءاطم > (CoA) ضي وفتلا ربيءء > ءيوزتلا لءءملا

| Time | Status | Details | Repeat ... | Identity | Endpoint ID | Posture St... | Endpoint P... | Authenticat... | Authorizati... | Authorizati... | IP Address |
|------------------------------|--------------------------------------|---------|------------|----------|-------------------|---------------|----------------|-----------------|-----------------|----------------|---------------|
| Jan 04, 2017 07:59:07 655 PM | ● | | 1 | cisco | C0-4A:00:15:75:C8 | Compliant | Microsoft-W... | Default >> D... | Default >> p... | PermiAccess | 10.62.148.162 |
| Jan 04, 2017 07:19:16 732 PM | ✓ | | | cisco | C0-4A:00:15:75:C8 | Compliant | Microsoft-W... | Default >> D... | Default >> p... | PermiAccess | |
| Jan 04, 2017 07:19:16 097 PM | ✓ | | | | C0-4A:00:15:75:C8 | Compliant | | | | | |
| Jan 04, 2017 07:19:02 205 PM | ✓ | | | cisco | C0-4A:00:15:75:C8 | Pending | Microsoft-W... | Default >> D... | Default >> C... | CPP | |

ةياهنلا ةطقن

ةبقارملا ةرتف ننيوكتو (لبق نم AnyConnect ريفوت متي مل اذا) ليمعلا دادم دع رقنا .ةياهنلا طاقن > قايسلا ةيؤري فانايبلل عمج ةيلمع نم ققحتل نكمي ،ةرمتسملا لعل يوتحي .ةياهنلا ةطقن ةحفص حتفت نا بجيو ،ةياهنلا ةطقنل MAC ناونع قوف افسن ةياهنلا ةطقن لعل ةتبتلمل تاقيبطتلا لوح تامولعم

C0: >8

MAC Address: C0:4 8
 Username: cisco
 Endpoint Profile: Microsoft-Workstation
 Current IP Address: 10 62
 Location: Location → All Locations

Applications Attributes Authentication Threats Vulnerabilities

Refresh Policy Actions Filter

| Application Name | Version | Vendor | Running process | Category | Install Path |
|-------------------------------------|-----------------|---------------------------------|-----------------|----------------------|---------------------------|
| Security Update for Microsoft .N... | 1 | Microsoft Corporation | | Unclassified | |
| Security Update for Microsoft .N... | 1 | Microsoft Corporation | | Unclassified | |
| Microsoft .NET Framework 4.6.1 | 4.6.3105 | Microsoft Corporation | | Unclassified | C:\Windows\Microsoft... |
| Google Update Helper | 1.3.24.15 | Google Inc. | | Unclassified | |
| Windows Update Agent | 7.6.7601.19161 | Microsoft Corporation | | PatchManagement | C:\Windows\System32\ |
| Cisco AnyConnect ISE Complia... | 4.2.468.0 | Cisco Systems, Inc | | Unclassified | C:\Program Files (x86)... |
| DAEMON Tools Lite | 4.49.1.0356 | Disc Soft Ltd | | Unclassified | C:\Program Files (x86)... |
| Tftp32 Standalone Edition (re... | 0.0 | | | Unclassified | |
| Security Update for Microsoft .N... | 1 | Microsoft Corporation | | Unclassified | |
| VMware Tools | 9.4.15.2827462 | VMware, Inc. | 2 | Unclassified | C:\Program Files\VMW... |
| BitLocker Drive Encryption | 6.1.7600.16385 | Microsoft Corporation | | DiskEncryption | C:\Windows\System32\ |
| Cisco AnyConnect Diagnostics ... | 4.4.00209 | Cisco Systems, Inc. | | Unclassified | C:\Program Files (x86)... |
| Cisco AnyConnect Secure Mobi... | 4.4.00209 | Cisco Systems, Inc. | 5 | Unclassified | C:\Program Files (x86)... |
| Java Auto Updater | 2.8.91.15 | Oracle Corporation | | Unclassified | |
| Mozilla Firefox | 47.0.2 | Mozilla Corporation | | AntiPhishing_Browser | C:\Program Files (x86)... |
| Microsoft Visual C++ 2008 Redi... | 9.0.30729.4148 | Microsoft Corporation | | Unclassified | |
| Java 8 Update 91 | 8.0.910.15 | Oracle Corporation | | Unclassified | C:\Program Files (x86)... |
| Google Chrome | 55.0.2883.87 | Google Inc. | | AntiPhishing_Browser | C:\Program Files (x86)... |
| Cisco AnyConnect Profile Editor | 4.1.08005 | Cisco Systems, Inc. | | Unclassified | C:\Program Files (x86)... |
| Java | 8.0.910.15 | Oracle Corporation | | Unclassified | C:\Program Files (x86)... |
| Internet Explorer | 11.0.9600.18524 | Microsoft Corporation | | AntiPhishing_Browser | C:\Program Files\Inter... |
| Wireshark | 1.10.7 | The Wireshark developer comm... | | Unclassified | C:\Program Files (x86)... |
| Windows Backup and Restore | 6.1.7600.16385 | Microsoft Corporation | | BackupClient | C:\Windows\System32\ |
| Windows Media Player | 12.0.7601.23517 | Microsoft Corporation | 1 | Unclassified | C:\Program Files\Wind... |
| FileZilla | 3.8.1.0 | FileZilla Project | | FileShare | C:\Program Files (x86)... |
| Security Update for Microsoft .N... | 2 | Microsoft Corporation | | Unclassified | |
| Java 7 Update 79 | 7.0.790 | Oracle | | Unclassified | C:\Program Files (x86)... |

لعل طغضاو ننيترم ةياهنلا ةطقن لعل لوصولا لعل جاتحتس ، CSCve82743 ببسب تاقيبطتلا لودج مي دقتل شي دحت

عضول ةسايس رصانع

تاقىب طتل عم قفاوتل ءاشن راىخ مادختساب رصانع ال هذه ءاشن بجى

- عضول قىب طت طرش
- عضول قىب طت ةجل اع م ءارچ
- عضول بل طت م
- عضول چهن

فى طورشل دجوت ISE GUI ةيموسرل م دختسمل ةه او نم انه نم لك نم ققحتل نكمى و قىب طتل ةلاح > عضول > طورشل > ةسايس رصانع > ةسايس ال

Application Condition

Rows/Page 25 / 1 / 1 Go 11 Total Rows

| Name | Description | Application State | Compliance module | Categories | Check |
|---------------------|-------------|-----------------------|-------------------|---------------------|--------|
| Apps_Collection | | Installed | 4.x or later | Anti-Malware | APPLIC |
| FileZilla-Uninstall | | Installed | 4.x or later | Public File Sharing | APPLIC |
| Notepadplus | | Installed and Running | 4.x or later | Unclassified | APPLIC |

> ةجل اع م ال تاءارچ > عضول > چئائتل > ةسايس رصانع > ةسايس ال فى دجوم چال ال قىب طتل حال صا

Application Remediation

Rows/Page 2 / 1 / 1 Go 2 Total Rows

| Name | Description | Application State | Compliance module | Categories |
|---------------------------------|-------------|-------------------|-------------------|------------|
| Notepadplus_Remediation | | | 4.x or later | |
| FileZilla-Uninstall_Remediation | | | 4.x or later | |

تابل طتل م ال > عضول > چئائتل > ةسايس رصانع > ةسايس ال فى تابل طتل م دجوت

| FileZilla-Uninstall_Requirement | for Windows All | using 4.x or later | using Standard | met if FileZilla-Uninstall | then FileZilla-Uninstall_Remediation |
|---------------------------------|-----------------|--------------------|----------------|----------------------------|--------------------------------------|
| FileZilla-Uninstall_Requirement | for Windows All | using 4.x or later | using Standard | met if FileZilla-Uninstall | then FileZilla-Uninstall_Remediation |

عضول > ةسايس ال فى تاسايس ال دجوت

Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

| Status | Rule Name | Identity Groups | Operating Systems | Compliance Module | Stealth mode | Other Conditions | Requirements |
|---------|----------------------------|-----------------|-------------------|-------------------|--------------|------------------|---------------------------------|
| Enabled | FileZilla-Uninstall_Policy | Any | Windows All | 4.x or later | Disabled | | FileZilla-Uninstall_Requirement |

ريراق

> تاسايس ال م هصحف نكمى و ISE لى EndPoint لك نم ةلاح ريرقت لك نيزخت م تى ريراق ال ريراق ال م ةفلتخم لكشأ كانه ريراق ال

- ةياهن ةطقنل عضول قفاوت لوح لى صافات رفوى - ةياهنل ةطقن بسح عضول م يى قت ةنى عم
- ضرعى وهف. عضول ةسايس طورشل لوح لى صافات رفوى - ةلاح بسح عضول م يى قت ةيه مزل ال طورشل ضرعى م تى. اهرى رمت م تى ال طورشل او تلش فى ال طورشل طقف ةيراق ال او

ةلاجل بسح عضولا مبيقت

طورشلل دحلش في، لامل اذه في. حضوم وه امك ةلاجل بسح عضولا مبيقت رهظي
قفاوتم ريغ لىل عضولا ةلاجل بسح مبيقت لىل اذى:

Posture Assessment by Condition

From 2017-01-23 00:00:00.0 to 2017-01-30 10:24:16.683

+ My Reports Export To Schedule

| Time | Status | User | IP | Result | Policy | Location |
|------------------------|--------|-------|-------------------|--------|-----------------------------|---------------|
| 2017-01-24 17:20:57... | Failed | alice | C0.4A.00:15:75:C8 | Passed | uc_visRun_v4_Notepad_ANY | All Locations |
| 2017-01-24 17:05:59... | Failed | alice | C0.4A.00:15:75:C8 | Failed | fs_visInst_v4_FileZilla_ANY | All Locations |
| 2017-01-24 17:05:59... | Failed | alice | C0.4A.00:15:75:C8 | Passed | uc_visRun_v4_Notepad_ANY | All Locations |
| 2017-01-24 17:01:22... | Failed | alice | C0.4A.00:15:75:C8 | Failed | fs_visInst_v4_FileZilla_ANY | All Locations |
| 2017-01-24 17:01:22... | Failed | alice | C0.4A.00:15:75:C8 | Passed | uc_visRun_v4_Notepad_ANY | All Locations |
| 2017-01-24 16:56:44... | Failed | alice | C0.4A.00:15:75:C8 | Failed | fs_visInst_v4_FileZilla_ANY | All Locations |
| 2017-01-24 16:56:44... | Failed | alice | C0.4A.00:15:75:C8 | Passed | uc_visRun_v4_Notepad_ANY | All Locations |
| 2017-01-24 16:52:08.77 | Failed | alice | C0.4A.00:15:75:C8 | Failed | fs_visInst_v4_FileZilla_ANY | All Locations |
| 2017-01-24 16:52:08.77 | Failed | alice | C0.4A.00:15:75:C8 | Passed | uc_visRun_v4_Notepad_ANY | All Locations |
| 2017-01-24 16:17:24.78 | Passed | alice | C0.4A.00:15:75:C8 | Passed | uc_visRun_v4_Notepad_ANY | All Locations |
| 2017-01-24 15:46:33.24 | Passed | alice | C0.4A.00:15:75:C8 | Passed | uc_visRun_v4_Notepad_ANY | All Locations |
| 2017-01-24 15:45:57... | Passed | alice | C0.4A.00:15:75:C8 | Passed | uc_visRun_v4_Notepad_ANY | All Locations |
| 2017-01-24 13:45:04... | Passed | alice | C0.4A.00:15:75:C8 | Passed | uc_visRun_v4_Notepad_ANY | All Locations |
| 2017-01-24 12:43:45... | Passed | alice | C0.4A.00:15:75:C8 | Passed | uc_visRun_v4_Notepad_ANY | All Locations |
| 2017-01-24 12:43:10... | Passed | alice | C0.4A.00:15:75:C8 | Passed | uc_visRun_v4_Notepad_ANY | All Locations |
| 2017-01-24 12:42:35... | Passed | alice | C0.4A.00:15:75:C8 | Passed | uc_visRun_v4_Notepad_ANY | All Locations |
| 2017-01-24 12:41:59.22 | Passed | alice | C0.4A.00:15:75:C8 | Passed | uc_visRun_v4_Notepad_ANY | All Locations |
| 2017-01-24 11:41:14... | Passed | alice | C0.4A.00:15:75:C8 | Passed | uc_visRun_v4_Notepad_ANY | All Locations |

Rows/Page 100 / 11 / 12 / 1116 Total Rows

ةياهنللا ةطقن بسح عضولا مبيقت

ةياهنللا ةطقن بسح عضولا مبيقت:

Posture Assessment by Endpoint

From 2017-01-23 00:00:00.0 to 2017-01-30 10:27:40.80

+ My Reports Export To Schedule

| Time | Status | Endpoint | User | IP | Policy | Location |
|-------------------------|--------|----------|-------|-------------------|-----------------------------|---------------|
| 2017-01-24 18:17:40.993 | Failed | N/A | alice | C0.4A.00:15:75:C8 | Windows 7 Enterprise 64-bit | All Locations |
| 2017-01-24 18:10:44.127 | Failed | N/A | alice | C0.4A.00:15:75:C8 | Windows 7 Enterprise 64-bit | All Locations |
| 2017-01-24 18:00:57.393 | Failed | N/A | alice | C0.4A.00:15:75:C8 | Windows 7 Enterprise 64-bit | All Locations |
| 2017-01-24 17:55:39.642 | Failed | N/A | alice | C0.4A.00:15:75:C8 | Windows 7 Enterprise 64-bit | All Locations |
| 2017-01-24 17:46:25.969 | Failed | N/A | alice | C0.4A.00:15:75:C8 | Windows 7 Enterprise 64-bit | All Locations |
| 2017-01-24 17:40:35.05 | Failed | N/A | alice | C0.4A.00:15:75:C8 | Windows 7 Enterprise 64-bit | All Locations |
| 2017-01-24 17:25:38.766 | Failed | N/A | alice | C0.4A.00:15:75:C8 | Windows 7 Enterprise 64-bit | All Locations |
| 2017-01-24 17:20:57.331 | Failed | N/A | alice | C0.4A.00:15:75:C8 | Windows 7 Enterprise 64-bit | All Locations |
| 2017-01-24 17:05:59.534 | Failed | N/A | alice | C0.4A.00:15:75:C8 | Windows 7 Enterprise 64-bit | All Locations |
| 2017-01-24 17:01:22.737 | Failed | N/A | alice | C0.4A.00:15:75:C8 | Windows 7 Enterprise 64-bit | All Locations |
| 2017-01-24 16:56:44.516 | Failed | N/A | alice | C0.4A.00:15:75:C8 | Windows 7 Enterprise 64-bit | All Locations |
| 2017-01-24 16:52:08.77 | Failed | N/A | alice | C0.4A.00:15:75:C8 | Windows 7 Enterprise 64-bit | All Locations |
| 2017-01-24 16:17:24.78 | Passed | N/A | alice | C0.4A.00:15:75:C8 | Windows 7 Enterprise 64-bit | All Locations |
| 2017-01-24 15:46:33.24 | Passed | N/A | alice | C0.4A.00:15:75:C8 | Windows 7 Enterprise 64-bit | All Locations |
| 2017-01-24 15:45:57.783 | Passed | N/A | alice | C0.4A.00:15:75:C8 | Windows 7 Enterprise 64-bit | All Locations |
| 2017-01-24 13:45:04.109 | Passed | N/A | alice | C0.4A.00:15:75:C8 | Windows 7 Enterprise 64-bit | All Locations |
| 2017-01-24 12:43:45.326 | Passed | N/A | alice | C0.4A.00:15:75:C8 | Windows 7 Enterprise 64-bit | All Locations |
| 2017-01-24 12:43:10.551 | Passed | N/A | alice | C0.4A.00:15:75:C8 | Windows 7 Enterprise 64-bit | All Locations |

Rows/Page 100 / 6 / 580 Total Rows

ليصافاتلا ريرقت ةنوقيأ لىل رقنلاب عضولل ققحت لك ليصافات نم ققحتلا نكمي

اهجالصوا ءاطخالا فاشكتسا

اهجالصوا نيوكتلا ءاطخا فاشكتسال اهم ادختسا كنكمي تامولعم مسقلا اذه رفوي

نم ISE

ءاطخالا حيحصت كلذي في امب، عضولاب ةقلعتملا تامولعملا عيمج لىل ISE-psc.log يوتحي

لجس نيوكت > ليجستال > مازنل > ةرادلل ي ف عضولا اطاخأ ححصت نيكمت نكمي posture: وه نوكملا مسا ححصتال

Node List > ise22-pri.example.com
Debug Level Configuration

| Component Name | Log Level | Description |
|------------------------|-----------|--|
| PassiveID | INFO | PassiveID events and messages |
| policy-engine | INFO | Policy Engine 2.0 related messages |
| portal | INFO | Portal (Guest, Hotspot, BYOD, CP) debug messages |
| portal-session-manager | INFO | Portal Session Manager debug messages |
| portal-web-action | INFO | Base Portal debug messages |
| posture | DEBUG | Posture debug messages |
| previewportal | INFO | Preview Portal debug messages |

ISE ققحتي، تترثي ةكبش ب AnyConnect لاصتاو ةكبش لاب ةياهن ةطقن ليصوت درجم بادصا فشتكي امك، اهن نيوكت مت يتال عضولا صحف تاي لمع لباقم EP صحف بجي هنأ نم موقبي، ةمجملا تامولعمل ال اذانتسا EP. لعل اهتيتبثت مت يتال ةيظمنل قفاوتل ادحو اذه ISE لسري، اقحال. هرفشتو xml NAC ليجم - EP ل عضولا مالعتسا عاشناب ISE ال AnyConnect ال مالعتسال.

```

2017-01-04 19:19:13,686 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco::- About to query posture policy for user
cisco with endpoint mac C0-4A-00-15-75-C8
2017-01-04 19:19:13,687 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PostureManager -:cisco::- agentCMVersion=4.2.468.0,
agentType=AnyConnect Posture Agent, groupName=OESIS_V4_Agents -> found agent group with
displayName=4.x or later
2017-01-04 19:19:13,687 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- User cisco belongs to groups NAC
Group:NAC:IdentityGroups:Endpoint Identity Groups:Profiled:Workstation,NAC
Group:NAC:IdentityGroups:Any
2017-01-04 19:19:13,687 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- About to retrieve posture policy
resources for os 7 Enterprise, agent group 4.x or later and identity groups [NAC
Group:NAC:IdentityGroups:Endpoint Identity Groups:Profiled:Workstation, NAC
Group:NAC:IdentityGroups:Any]
2017-01-04 19:19:13,687 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- Evaluate resourceId NAC
Group:NAC:Posture:PosturePolicies:Apps by agent group with FQN NAC
Group:NAC:AgentGroupRoot:ALL:OESIS_V4_Agents
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- The evaluation result by agent group for
resourceId NAC Group:NAC:Posture:PosturePolicies:Apps is Permit
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- Evaluate resourceId NAC
Group:NAC:Posture:PosturePolicies:Apps by OS group with FQN NAC
Group:NAC:OsGroupRoot:ALL:WINDOWS_ALL:WINDOWS_7_ALL:WINDOWS_7_ENTERPRISE_ALL
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- stealth mode is 0
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- The evaluation result by os group for
resourceId NAC Group:NAC:Posture:PosturePolicies:Apps is Permit
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- Evaluate resourceId NAC
Group:NAC:Posture:PosturePolicies:Apps by Stealth mode NSF group with FQN NAC
Group:NAC:StealthModeStandard
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]

```

```
cisco.cpm.posture.runtime.PosturePolicyUtil --:cisco:::- Procesing obligation with posture policy
resource with id NAC Group:NAC:Posture:PosturePolicies:Apps
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil --:cisco:::- Found obligation id
urn:cisco:cepm:3.3:xacml:response-qualifier for posture policy resource with id NAC
Group:NAC:Posture:PosturePolicies:Apps
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil --:cisco:::- Found obligation id PostureReqs for
posture policy resource with id NAC Group:NAC:Posture:PosturePolicies:Apps
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil --:cisco:::- Posture policy resource id Apps has
following associated requirements []
2017-01-04 19:19:13,720 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cpm.posture.runtime.agent.AgentXmlGenerator --:cisco:::- policy enforcemnt is 2
2017-01-04 19:19:13,720 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cpm.posture.runtime.agent.AgentXmlGenerator --:cisco:::- simple condition: [Name=Apps_Collection,
Description=null, Application State =installed,runnning, Provision By =Everything, monitory
Categories = []]
2017-01-04 19:19:13,720 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cpm.posture.runtime.agent.AgentXmlGenerator --:cisco:::- check type is ApplicationVisibility
2017-01-04 19:19:13,800 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PostureHandlerImpl --:cisco:::- NAC agent xml <?xml version="1.0"
encoding="UTF-8"?><cleanmachines>
  <version>ISE: 2.2.0.423</version>
  <encryption>0</encryption>
  <package>
    <id>12</id>
    <name>Apps_collection</name>
    <description>Apps Check</description>
    <version/>
    <type>3</type>
    <optional>2</optional>
    <action>3</action>
    <check>
      <id>Apps_Collection</id>
      <category>12</category>
      <type>1202</type>
      <monitor>ALL</monitor>
      <evaluation>periodic</evaluation>
    </check>
    <criteria>(Apps_Collection)</criteria>
  </package>
</cleanmachines>

2017-01-04 19:19:13,800 INFO [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.util.StatusUtil --:cisco:::- StatusUtil - getPosturePolicyHTML
[<cleanmachines><version>ISE:
2.2.0.423</version><encryption>0</encryption><package><id>12</id><name>Apps_collection</name><de
scription>Apps
Check</description><version/><type>3</type><optional>2</optional><action>3</action><check><id>Ap
ps_Collection</id><category>12</category><type>1202</type><monitor>ALL</monitor><evaluation>peri
odic</evaluation></check><criteria>(Apps_Collection)</criteria></package></cleanmachines>]
2017-01-04 19:19:13,800 INFO [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.util.StatusUtil --:cisco:::- StatusUtil -getPosturePolicyHTML - do encrypt
2017-01-04 19:19:13,800 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.util.StatusUtil --:cisco:::- Encrypting policy using AES key.
2017-01-04 19:19:13,800 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.util.CipherUtil --:cisco:::- Encrypting message using AES.
2017-01-04 19:19:13,800 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.util.StatusUtil --:cisco:::- IV Base 64: AeUQGbj6CP/jMB+cTIGIGQ==
2017-01-04 19:19:13,801 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.util.StatusUtil --:cisco:::- StatusUtil.getPosturePolicyHTML() returns <!--X-
Perfigo-UserKey=--><!--X-Perfigo-Provider=Device Filter--><!--X-Perfigo-UserName=cisco--><!--
error=1010--><!--X-Perfigo-DM-Error=1010--><!--user role=--><!--X-Perfigo-OrigRole=--><!--X-
```



```
Perfigo-DM-Scan-Req=0--><!--X-ISE-IV=AeUQGbj6CP/jMB+cTIGIGQ===><!--X-Perfigo-DM-Software-
List=f5aGq8rU5wx7hFS9WnugNhy/6HaSxNtKesoqAjYkecEk56t+I/J93PtAYU0XLq451NXQhReuFktImYEPENWwOs1bV5o
OTuTsY3kEbcuR4p5Sp0cfz/j98YEubNtSKDCUGt5U8dhpOJqMYTV4UcaSP/D0FXym10gFEjPxpPghyWcplzYwcpehIX+2vOY
OSzPTEvM2kDdHTkof+/UYvBfGv8Y7YkK9P6lupfSedIqdynyxUbeqknXkoCaWvUawJLVWiXAJs2atsCwJjXitwNHYZCuH/mB
z/Y9AUvblCB/cutCeyVCl7ij8wtXUAt2NpKqeEj0COOxnp5B35JTBfOSXHFVJL29E5JALaun6RR8yJlkd4ap7qflnjsu451
CHY/SbKTMnqjV5bNwXfucBF++X6X/mh0nwk+r2iWhJfYqnmNxBm2BvcJAJXOKOV7xHIhgmLj+etF4Sss/zwnFT4+WTzKI+Bp
brVdnZjUP7+uvbQbIPtRFqJVI5StjZlIP4vLzFWKbWXI+itTX6hjqvNhiT2zwtvIboUZZXaBV6yS5/+5cYMU3+EhWxIx/UVO
0o7sX--><!--X-Perfigo-DM-Session-Time=240-->
2017-01-04 19:19:13,801 DEBUG [http-bio-10.48.26.60-8443-exec-9][
cisco.cpm.posture.runtime.PosturePolicyUtil --:cisco::- User cisco belongs to groups NAC
Group:NAC:IdentityGroups:Endpoint Identity Groups:Profiled:Workstation,NAC
Group:NAC:IdentityGroups:Any
2017-01-04 19:19:13,801 DEBUG [http-bio-10.48.26.60-8443-exec-9][
cisco.cpm.posture.runtime.PostureHandlerImpl --:cisco::- Sending response to endpoint C0-4A-00-
15-75-C8 http response [ [ <!--X-Perfigo-UserKey=--><!--X-Perfigo-Provider=Device Filter--><!--X-
Perfigo-UserName=cisco--><!--error=1010--><!--X-Perfigo-DM-Error=1010--><!--user role=--><!--X-
Perfigo-OrigRole=--><!--X-Perfigo-DM-Scan-Req=0--><!--X-ISE-IV=AeUQGbj6CP/jMB+cTIGIGQ===><!--X-
Perfigo-DM-Software-
List=f5aGq8rU5wx7hFS9WnugNhy/6HaSxNtKesoqAjYkecEk56t+I/J93PtAYU0XLq451NXQhReuFktImYEPENWwOs1bV5o
OTuTsY3kEbcuR4p5Sp0cfz/j98YEubNtSKDCUGt5U8dhpOJqMYTV4UcaSP/D0FXym10gFEjPxpPghyWcplzYwcpehIX+2vOY
OSzPTEvM2kDdHTkof+/UYvBfGv8Y7YkK9P6lupfSedIqdynyxUbeqknXkoCaWvUawJLVWiXAJs2atsCwJjXitwNHYZCuH/mB
z/Y9AUvblCB/cutCeyVCl7ij8wtXUAt2NpKqeEj0COOxnp5B35JTBfOSXHFVJL29E5JALaun6RR8yJlkd4ap7qflnjsu451
CHY/SbKTMnqjV5bNwXfucBF++X6X/mh0nwk+r2iWhJfYqnmNxBm2BvcJAJXOKOV7xHIhgmLj+etF4Sss/zwnFT4+WTzKI+Bp
brVdnZjUP7+uvbQbIPtRFqJVI5StjZlIP4vLzFWKbWXI+itTX6hjqvNhiT2zwtvIboUZZXaBV6yS5/+5cYMU3+EhWxIx/UVO
0o7sX--><!--X-Perfigo-DM-Session-Time=240--> ]
2017-01-04 19:19:13,959 DEBUG [http-bio-10.48.26.60-8443-exec-5][
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- receiving request from client
C0:4A:00:15:75:C8 10.62.148.162 bcu5ksw0
2017-01-04 19:19:13,966 DEBUG [http-bio-10.48.26.60-8443-exec-5][
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Found the ipAddress that matched the http
request remote address 10.62.148.162 and corresponding client mac address C0-4A-00-15-75-C8
2017-01-04 19:19:13,966 DEBUG [http-bio-10.48.26.60-8443-exec-5][
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for Radius session with input
values : sessionId: 0a3e946500000066586d3c42, MacAddr: C0-4A-00-15-75-C8, ipAddr: 10.62.148.162
2017-01-04 19:19:13,966 DEBUG [http-bio-10.48.26.60-8443-exec-5][
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for session using session ID:
0a3e946500000066586d3c42, IP addrs: [10.62.148.162], mac Addrs [C0-4A-00-15-75-C8]
2017-01-04 19:19:13,966 DEBUG [http-bio-10.48.26.60-8443-exec-5][
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- Found session using sessionId
0a3e946500000066586d3c42
```

تاقېب طتال ةفاك لوح تامول عم ىلع ريرقتال اذھ يوتحي AnyConnect. نم لمالكال ريرقتال
اھني وكت مت يتي قيبطتال ةلاح قباطت يتلا و اھي لعل روثع ال مت يتي

```
2017-01-04 19:19:37,358 DEBUG [http-bio-10.48.26.60-8443-exec-3][
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- UDID is
766bb955e51e4ab063fd478c63acee81260ca592 for end point C0-4A-00-15-75-C8
2017-01-04 19:19:37,358 DEBUG [http-bio-10.48.26.60-8443-exec-3][
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- os version from user agent is 1.2.1.6.1.4
2017-01-04 19:19:37,358 DEBUG [http-bio-10.48.26.60-8443-exec-3][
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Received posture request [parameters:
reqtype=, userip=10.62.148.162, clientmac=C0-4A-00-15-75-C8, os=, osVerison=1.2.1.6.1.4,
architecture=, provider=, state=, userAgent=Mozilla/4.0 (compatible; WINDOWS; 1.2.1.6.1.4;
AnyConnect Posture Agent v.4.4.00209), session_id=
2017-01-04 19:19:37,358 DEBUG [http-bio-10.48.26.60-8443-exec-3][
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Found a session info for endpoint C0-4A-00-
15-75-C8 cisco
2017-01-04 19:19:37,358 DEBUG [http-bio-10.48.26.60-8443-exec-3][
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Got userid cisco from cache for endpoint C0-
4A-00-15-75-C8/
2017-01-04 19:19:37,358 DEBUG [http-bio-10.48.26.60-8443-exec-3][
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Report IV in Base64:
JjneGgZcJbmjqMKQcy8kJg==
```

2017-01-04 19:19:37,359 DEBUG [http-bio-10.48.26.60-8443-exec-3][
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Using AES shared secret to decrypt report.
2017-01-04 19:19:37,359 DEBUG [http-bio-10.48.26.60-8443-exec-3][
cisco.cpm.posture.util.CipherUtil -::::- Decrypting message using AES.
2017-01-04 19:19:37,359 DEBUG [http-bio-10.48.26.60-8443-exec-3][
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- **Decrypted report** [
<report><version>1000</version><package><id>12</id><status>1</status><check><chk_id>Apps_Collect
ion</chk_id><diff>0</diff><application><diff>0</diff><id></id><name>Adobe Flash Player 23
NPAPI</name><vendor>Adobe Systems
Incorporated</vendor><version>23.0.0.207</version><category>Unclassified</category></application
><application><diff>0</diff><id>104</id><name>Adobe Flash Player</name><vendor>Adobe Systems
Inc.</vendor><version>23.0.0.207</version><path>C:\Windows\SysWOW64\Macromed\FIash</path><categ
ory>Unclassified</category></application><application><diff>0</diff><id>873</id><name>BitLocker
Drive Encryption</name><vendor>Microsoft
Corporation</vendor><version>6.1.7600.16385</version><path>C:\Windows\System32</path><category>
DiskEncryption</category></application><application><diff>0</diff><id></id><name>Cisco
AnyConnect Diagnostics and Reporting Tool</name><vendor>Cisco Systems,
Inc.</vendor><version>4.4.00209</version><path>C:\Program Files (x86)\Cisco\Cisco AnyConnect
Secure Mobility
Client\DART</path><category>Unclassified</category></application><application><diff>0</diff><id
></id><name>Cisco AnyConnect ISE Compliance Module</name><vendor>Cisco Systems,
Inc</vendor><version>4.2.468.0</version><path>C:\Program Files (x86)\Cisco\Cisco AnyConnect
Secure Mobility
Client\opswat</path><category>Unclassified</category></application><application><diff>0</diff><
id></id><name>Cisco AnyConnect ISE Posture Module</name><vendor>Cisco Systems,
Inc.</vendor><version>4.4.00209</version><path>C:\Program Files (x86)\Cisco\Cisco AnyConnect
Secure Mobility
Client</path><category>Unclassified</category><process><diff>0</diff><pid>704</pid><path>c:\pro
gram files (x86)\cisco\cisco anyconnect secure mobility
client\vpnagent.exe</path><hash>7D7502DE53F0282A7AFC98BE89F54D39FDEC3FAC2A1F32674C76967ADC695E09
</hash></process><process><diff>0</diff><pid>1296</pid><path>c:\program files (x86)\cisco\cisco
anyconnect secure mobility
client\aciseagent.exe</path><hash>7E156520C184334D473506FFE8A482997581ACF6ABD34231FDEDC2B9A3A120
66</hash></process><process><diff>0</diff><pid>3076</pid><path>c:\program files
(x86)\cisco\cisco anyconnect secure mobility
client\vpnu.exe</path><hash>0131258625A16B78125EB2081E8D5678671B6DE52DDA9E0813D4674618177DC3</h
ash></process><process><diff>0</diff><pid>3384</pid><path>c:\program files (x86)\cisco\cisco
anyconnect secure mobility
client\acise.exe</path><hash>8636F5761663A0EB9EDE263609B6AEF0EA52292E5B093AD4C453097583F365DD</h
ash></process><process><diff>0</diff><pid>15924</pid><path>c:\program files (x86)\cisco\cisco
anyconnect secure mobility
client\aciseposture.exe</path><hash>7FA4B3B6F688642E800AD53B865DBDCC163FBCA92D83482248DB068BA421
92EA</hash></process></application><application><diff>0</diff><id></id><name>Cisco AnyConnect
Profile Editor</name><vendor>Cisco Systems,
Inc.</vendor><version>4.1.08005</version><path>C:\Program Files (x86)\Cisco\Cisco AnyConnect
Profile
Editor</path><category>Unclassified</category></application><application><diff>0</diff><id></id
><name>Cisco AnyConnect Secure Mobility Client </name><vendor>Cisco Systems,
Inc.</vendor><version>4.4.00209</version><category>Unclassified</category></application><applica
tion><diff>0</diff><id></id><name>Cisco AnyConnect Secure Mobility Client</name><vendor>Cisco
Systems, Inc.</vendor><version>4.4.00209</version><path>C:\Program Files (x86)\Cisco\Cisco
AnyConnect Secure Mobility
Client</path><category>Unclassified</category><process><diff>0</diff><pid>704</pid><path>c:\pro
gram files (x86)\cisco\cisco anyconnect secure mobility
client\vpnagent.exe</path><hash>7D7502DE53F0282A7AFC98BE89F54D39FDEC3FAC2A1F32674C76967ADC695E09
</hash></process><process><diff>0</diff><pid>1296</pid><path>c:\program files (x86)\cisco\cisco
anyconnect secure mobility
client\aciseagent.exe</path><hash>7E156520C184334D473506FFE8A482997581ACF6ABD34231FDEDC2B9A3A120
66</hash></process><process><diff>0</diff><pid>3076</pid><path>c:\program files
(x86)\cisco\cisco anyconnect secure mobility
client\vpnu.exe</path><hash>0131258625A16B78125EB2081E8D5678671B6DE52DDA9E0813D4674618177DC3</h
ash></process><process><diff>0</diff><pid>3384</pid><path>c:\program files (x86)\cisco\cisco
anyconnect secure mobility
client\acise.exe</path><hash>8636F5761663A0EB9EDE263609B6AEF0EA52292E5B093AD4C453097583F365DD</h

ash></process><process><diff>0</diff><pid>15924</pid><path>c:\program files (x86)\cisco\cisco
anyconnect secure mobility
client\aciseposture.exe</path><hash>7FA4B3B6F688642E800AD53B865DBDCC163FBCA92D83482248DB068BA421
92EA</hash></process></application><application><diff>0</diff><id></id><name>Cisco NAC Agent
</name><vendor>Cisco Systems, Inc.</vendor><version>4.9.5.10</version><path>C:\Program Files
(x86)\Cisco\Cisco NAC
Agent</path><category>Unclassified</category><process><diff>0</diff><pid>1444</pid><path>c:\pro
gram files (x86)\cisco\cisco nac
agent\nacagent.exe</path><hash>502EF2A864254A2DF555E029BE2C39E94B111E8B01534D7161826650DE4CEB4D<
</hash></process><process><diff>0</diff><pid>2320</pid><path>c:\program files (x86)\cisco\cisco
nac
agent\nacagentui.exe</path><hash>DC617419F082BEAF26521E48CB410282631F93F1359E604A4D3D181A04FEE1F
B</hash></process></application><application><diff>0</diff><id>293</id><name>DAEMON Tools
Lite</name><vendor>Disc Soft Ltd</vendor><version>4.49.1.0356</version><path>C:\Program Files
(x86)\DAEMON Tools
Lite</path><category>Unclassified</category></application><application><diff>0</diff><id></id><
name>Digital Operatives PAINT
Beta</name><vendor></vendor><version>0.0</version><category>Unclassified</category></application
><application><diff>0</diff><id></id><name>FileZilla Server</name><vendor>FileZilla
Project</vendor><version>beta 0.9.44</version><path>C:\Program Files (x86)\FileZilla
Server</path><category>Unclassified</category><process><diff>0</diff><pid>1408</pid><path>c:\pr
ogram files (x86)\filezilla server\filezilla
server.exe</path><hash>E8DB1409DB694A90C759F418346AE5D71014AE3513A8B865B50923AD0DFEE395</hash></
process><process><diff>0</diff><pid>2348</pid><path>c:\program files (x86)\filezilla
server\filezilla server
interface.exe</path><hash>F57B0A7F4A9EBAACC1A67323EBB93D96FA910524FAE842953551DBA103EF71C5</hash
></process></application><application><diff>0</diff><id>180</id><name>FileZilla</name><vendor>Fi
leZilla Project</vendor><version>3.8.1.0</version><path>C:\Program Files (x86)\FileZilla FTP
Client</path><category>FileShare</category></application><application><diff>0</diff><id>39</id>
<name>Google Chrome</name><vendor>Google
Inc.</vendor><version>55.0.2883.87</version><path>C:\Program Files
(x86)\Google\Chrome\Application</path><category>AntiPhishing, Browser</category></application><a
pplication><diff>0</diff><id></id><name>Google Update Helper</name><vendor>Google
Inc.</vendor><version>1.3.24.15</version><category>Unclassified</category></application><applica
tion><diff>0</diff><id>100</id><name>Internet Explorer</name><vendor>Microsoft
Corporation</vendor><version>11.0.9600.18524</version><path>C:\Program Files\Internet
Explorer</path><category>AntiPhishing, Browser</category></application><application><diff>0</dif
f><id></id><name>Java 7 Update
79</name><vendor>Oracle</vendor><version>7.0.790</version><path>C:\Program Files
(x86)\Java\jre7</path><category>Unclassified</category></application><application><diff>0</diff
><id></id><name>Java 8 Update 91</name><vendor>Oracle
Corporation</vendor><version>8.0.910.15</version><path>C:\Program Files
(x86)\Java\jre1.8.0_91</path><category>Unclassified</category></application><application><diff>
0</diff><id></id><name>Java Auto Updater</name><vendor>Oracle
Corporation</vendor><version>2.8.91.15</version><category>Unclassified</category></application><
application><diff>0</diff><id>111</id><name>Java</name><vendor>Oracle
Corporation</vendor><version>7.0.790.15</version><path>C:\Program Files
(x86)\Java\jre7\bin</path><category>Unclassified</category></application><application><diff>0</
diff><id>111</id><name>Java</name><vendor>Oracle
Corporation</vendor><version>8.0.910.15</version><path>C:\Program Files
(x86)\Java\jre1.8.0_91\bin</path><category>Unclassified</category></application><application><d
iff>0</diff><id></id><name>Microsoft .NET Framework 4.6.1</name><vendor>Microsoft
Corporation</vendor><version>4.6.01055</version><path>C:\Windows\Microsoft.NET\Framework64\v4.0.
30319\SetupCache\v4.6.01055</path><category>Unclassified</category></application><application><
diff>0</diff><id></id><name>Microsoft Network Monitor 3.4</name><vendor>Microsoft
Corporation</vendor><version>3.4.2350.0</version><category>Unclassified</category></application>
<application><diff>0</diff><id></id><name>Microsoft Network Monitor: NetworkMonitor Parsers
3.4</name><vendor>Microsoft
Corporation</vendor><version>3.4.2350.0</version><category>Unclassified</category></application>
<application><diff>0</diff><id></id><name>Microsoft Visual C++ 2008 Redistributable - x64
9.0.30729.4148</name><vendor>Microsoft
Corporation</vendor><version>9.0.30729.4148</version><category>Unclassified</category></applicat
ion><application><diff>0</diff><id></id><name>Microsoft Visual C++ 2008 Redistributable - x86
9.0.30729.4148</name><vendor>Microsoft

Corporation</vendor><version>9.0.30729.4148</version><category>Unclassified</category></applicat
ion><application><diff>0</diff><id>44</id><name>Mozilla Firefox</name><vendor>Mozilla
Corporation</vendor><version>47.0.2</version><path>C:\Program Files (x86)\Mozilla
Firefox\</path><category>AntiPhishing,Browser</category><process><diff>0</diff><pid>8292</pid><p
ath>c:\program files (x86)\mozilla
firefox\firefox.exe</path><hash>47F80E4FC4C43FAF468D94F5D51AAC78A125CC720FCBEA0B88B5F29D06719CE9
</hash></process></application><application><diff>0</diff><id></id><name>Mozilla Maintenance
Service</name><vendor>Mozilla</vendor><version>47.0.2.6148</version><category>Unclassified</cate
gory></application><application><diff>0</diff><id>298</id><name>Notepad++</name><vendor>Notepad+
+ Team</vendor><version>6.63</version><path>C:\Program Files
(x86)\Notepad++\</path><category>Unclassified</category></application><application><diff>0</diff
><id></id><name>Security Update for Microsoft .NET Framework 4.6.1
(KB3122661)</name><vendor>Microsoft
Corporation</vendor><version>1</version><category>Unclassified</category></application><applicat
ion><diff>0</diff><id></id><name>Security Update for Microsoft .NET Framework 4.6.1
(KB3127233)</name><vendor>Microsoft
Corporation</vendor><version>1</version><category>Unclassified</category></application><applicat
ion><diff>0</diff><id></id><name>Security Update for Microsoft .NET Framework 4.6.1
(KB3136000v2)</name><vendor>Microsoft
Corporation</vendor><version>2</version><category>Unclassified</category></application><applicat
ion><diff>0</diff><id></id><name>Security Update for Microsoft .NET Framework 4.6.1
(KB3142037)</name><vendor>Microsoft
Corporation</vendor><version>1</version><category>Unclassified</category></application><applicat
ion><diff>0</diff><id></id><name>Security Update for Microsoft .NET Framework 4.6.1
(KB3143693)</name><vendor>Microsoft
Corporation</vendor><version>1</version><category>Unclassified</category></application><applicat
ion><diff>0</diff><id></id><name>Security Update for Microsoft .NET Framework 4.6.1
(KB3164025)</name><vendor>Microsoft
Corporation</vendor><version>1</version><category>Unclassified</category></application><applicat
ion><diff>0</diff><id></id><name>TP-LINK TL-WDN3200 Driver</name><vendor>TP-
LINK</vendor><version>1.1.0</version><path>C:\Program Files (x86)\TP-LINK\TP-LINK Wireless
Configuration Utility and
Driver\</path><category>Unclassified</category></application><application><diff>0</diff><id></id
><name>Tftpd32 Standalone Edition (remove
only)</name><vendor></vendor><version>0.0</version><category>Unclassified</category></applicatio
n><application><diff>0</diff><id></id><name>VMware Tools</name><vendor>VMware,
Inc.</vendor><version>9.4.15.2827462</version><path>C:\Program Files\VMware\VMware
Tools\</path><category>Unclassified</category><process><diff>0</diff><pid>952</pid><path>c:\prog
ram files\vmware\vmware
tools\vmtoolsd.exe</path><hash>5C642EF7F4EF65A0445B2C2CD227F9431835712EE7F1BD4D01D1F7472199DE47<
</hash></process><process><diff>0</diff><pid>1516</pid><path>c:\program files\vmware\vmware
tools\vmtoolsd.exe</path><hash>5C642EF7F4EF65A0445B2C2CD227F9431835712EE7F1BD4D01D1F7472199DE47<
</hash></process></application><application><diff>0</diff><id></id><name>WinPcap
4.1.3</name><vendor>Riverbed Technology,
Inc.</vendor><version>4.1.0.2980</version><category>Unclassified</category></application><applic
ation><diff>0</diff><id>300</id><name>WinPcap</name><vendor>Riverbed Technology,
Inc.</vendor><version>4.1.0.2980</version><path>C:\Program Files
(x86)\WinPcap\</path><category>Unclassified</category></application><application><diff>0</diff><
id>923</id><name>Windows Backup and Restore</name><vendor>Microsoft
Corporation</vendor><version>6.1.7600.16385</version><path>C:\Windows\System32\</path><category>
BackupClient</category></application><application><diff>0</diff><id>362</id><name>Windows
Defender</name><vendor>Microsoft
Corporation</vendor><version>6.1.7600.16385</version><path>C:\Program Files\Windows
Defender\</path><category>AntiMalware</category></application><application><diff>0</diff><id>283
</id><name>Windows Firewall</name><vendor>Microsoft
Corporation</vendor><version>6.1.7600.16385</version><path>C:\Windows\System32\</path><category>
FireWall</category></application><application><diff>0</diff><id>1612</id><name>Windows Media
Player</name><vendor>Microsoft
Corporation</vendor><version>12.0.7601.23517</version><path>C:\Program Files\Windows Media
Player\</path><category>Unclassified</category><process><diff>0</diff><pid>1596</pid><path>c:\pr
ogram files\windows media
player\wmpnetwk.exe</path><hash>306467D280E99D0616E839278A4DB5BED684F002AE284C3678CABB5251459CB3
</hash></process></application><application><diff>0</diff><id>1587</id><name>Windows Security
Health Agent</name><vendor>Microsoft

```
Corporation</vendor><version>6.1.7600.16385</version><path>C:\Windows\System32</path><category>HealthAgent</category></application><application><diff>0</diff><id>1090</id><name>Windows Update Agent</name><vendor>Microsoft Corporation</vendor><version>7.6.7601.19161</version><path>C:\Windows\System32</path><category>PatchManagement</category></application><application><diff>0</diff><id>1106</id><name>Windows VPN Client</name><vendor>Microsoft Corporation</vendor><version>6.1.7600.16385</version><path>C:\Windows\System32</path><category>VPNClient</category></application><application><diff>0</diff><id>207</id><name>Wireshark</name>< vendor>The Wireshark developer community</vendor><version>1.10.7</version><path>C:\Program Files (x86)\Wireshark\</path><category>Unclassified</category></application></check></package></report > ]]
```

قسنم ريرقت جذومن XML لسالس يه ريرقتلا ةفاك:

```
<report>
<version>1000</version>
<package>
<id>12</id>
<status>1</status>
<check>
<chk_id>Apps_Collection</chk_id>
<diff>0</diff>
<application>
<diff>0</diff>
<id>104</id>
<name>Adobe Flash Player</name>
<vendor>Adobe Systems Inc.</vendor>
<version>23.0.0.207</version>
<path>C:\Windows\SysWOW64\Macromed\FIash\</path>
<category>Unclassified</category>
</application>
...
<application>
<diff>0</diff>
<id></id>
<name>Cisco AnyConnect ISE Posture Module</name>
<vendor>Cisco Systems, Inc.</vendor>
<version>4.4.00209</version>
<path>C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\</path>
<category>Unclassified</category>
<process>
<diff>0</diff>
<pid>704</pid>
<path>c:\program files (x86)\cisco\cisco anyconnect secure mobility client\vpnagent.exe</path>
<hash>7D7502DE53F0282A7AFC98BE89F54D39FDEC3FAC2A1F32674C76967ADC695E09</hash>
</process>
<process>
<diff>0</diff>
<pid>1296</pid>
<path>c:\program files (x86)\cisco\cisco anyconnect secure mobility client\aciseagent.exe</path>
<hash>7E156520C184334D473506FFE8A482997581ACF6ABD34231FDEDC2B9A3A12066</hash>
</process>
<process>
<diff>0</diff>
<pid>3076</pid>
<path>c:\program files (x86)\cisco\cisco anyconnect secure mobility client\vpnuui.exe</path>
<hash>0131258625A16B78125EB2081E8D5678671B6DE52DDA9E0813D4674618177DC3</hash>
</process>
<process>
<diff>0</diff>
<pid>3384</pid>
<path>c:\program files (x86)\cisco\cisco anyconnect secure mobility client\acise.exe</path>
```

```
<hash>8636F5761663A0EB9EDE263609B6AEF0EA52292E5B093AD4C453097583F365DD</hash>
</process>
<process>
<diff>0</diff>
<pid>15924</pid>
<path>c:\program files (x86)\cisco\cisco anyconnect secure mobility
client\aciseposture.exe</path>
<hash>7FA4B3B6F688642E800AD53B865DBDCC163FBCA92D83482248DB068BA42192EA</hash>
</process>
</application>
... </check> </package> </report>
```

طوق ف تاريغيغتلا لسرت اهنا امك . طوق ف لاصتا لوأ دنع ةلماك ريراقت AnyConnect لسري
تقولا ضعب دعب Notepad++ ليريغشت ادب مت ، لاثملا ليربس لىلع

```
2017-01-04 19:24:37,929 DEBUG [http-bio-10.48.26.60-8443-exec-7][[]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Received posture request [parameters:
reqtype=, userip=10.62.148.162, clientmac=C0-4A-00-15-75-C8, os=, osVerison=1.2.1.6.1.4,
architecture=, provider=, state=, userAgent=Mozilla/4.0 (compatible; WINDOWS; 1.2.1.6.1.4;
AnyConnect Posture Agent v.4.4.00209), session_id=
2017-01-04 19:24:37,929 DEBUG [http-bio-10.48.26.60-8443-exec-7][[]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Found a session info for endpoint C0-4A-00-
15-75-C8 cisco
2017-01-04 19:24:37,929 DEBUG [http-bio-10.48.26.60-8443-exec-7][[]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Got userid cisco from cache for endpoint C0-
4A-00-15-75-C8/
2017-01-04 19:24:37,929 DEBUG [http-bio-10.48.26.60-8443-exec-7][[]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Report IV in Base64:
JjneGgZcJbmjqMKQcy8kJg==
2017-01-04 19:24:37,929 DEBUG [http-bio-10.48.26.60-8443-exec-7][[]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Using AES shared secret to decrypt report.
2017-01-04 19:24:37,929 DEBUG [http-bio-10.48.26.60-8443-exec-7][[]
cisco.cpm.posture.util.CipherUtil -::::- Decrypting message using AES.
2017-01-04 19:24:37,930 DEBUG [http-bio-10.48.26.60-8443-exec-7][[]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Decrypted report [[
<report><version>1000</version><package><id>12</id><status>1</status><check><chk_id>Apps_Collect
ion</chk_id><diff>1</diff><application><diff>2</diff><id>298</id>
```

```
<vendor>Notepad++ Team</vendor><version>6.63</version><path>C:\Program Files
(x86)\Notepad++\</path><category>Unclassified</category><process><diff>0</diff>
```

```
<path>c:\program files
(x86)\notepad++\notepad++.exe</path><hash>43E9F528CD2405E6DD117857D440A634769C6E11C4D986605354C2
605B6E7D84</hash></process></application></check></package></report> ]]
```

قس نم:

```
<report>
<version>1000</version>
<package>
<id>12</id>
<status>1</status>
<check>
<chk_id>Apps_Collection</chk_id>
<diff>1</diff>
<application>
```

<diff>2</diff>
<id>298</id>

<vendor>Notepad++ Team</vendor>
<version>6.63</version>
<path>C:\Program Files (x86)\Notepad++\</path>
<category>Unclassified</category>
<process>
<diff>0</diff>

<path>c:\program files (x86)\notepad++\notepad++.exe</path>
<hash>43E9F528CD2405E6DD117857D440A634769C6E11C4D986605354C2605B6E7D84</hash>
</process>
</application>
</check>
</package>
</report>

AnyConnect نم

ءاطخألا حىحصتو ةلصللا تاذ تالجال عىمى لىل ع AnyConnect_ISEPosture.txt فللمل اىوتحى لاثم انه . ةياهن ةطقن لىل ع اءعىمىم تىل ل DART ةمزح فى فللمل اذى لىل ع روثعل نكمى ل AES256 مءاخس اب هرىفش ت م تى ، رىرور رىرقتل

Date : 01/04/2017
Time : 19:34:38
Type : Unknown
Source : acise

Description : Function: Authenticator::bldMonitorReport
Thread Id: 0xD3C
File: Authenticator.cpp
Line: 724
Level: info

Monitor Report:
&user_key=dummykey&cm=10&ops=1&mac_list=C0%3a4A%3a00%3a15%3a75%3aC8&ip_list=10%2e62%2e148%2e162&hostname=TSOPREK%2dWIN7%2dl&udid=766bb955e51e4ab063fd478c63acee81260ca592&dm_report_client_IV=JjneGgZcJbmjqMKQcy8kJg%3d%3d&dm_report=2yWwY7QzHWCY%2fdVEESSAabEZtYltxNE7Qgy00a85Dgo2Ts4ok8sIrBM37S2%2fe2Hs0URCP4KkfY4Ap8%2bh%2fqS%2biw50CZe jKG%2bVbF7RTRqZyrg2veWAwVEDsSb%2bqWRRdzvZfsjS3G4ApQi07qnfExwN1IvCqrVOp1j17TAcVXEht8NkDg00T9jM%2fTNH%2fMK1lc0o6Ha5juJo4YtWDWY%2bnOancw%3d%3d.

Date : 01/04/2017
Time : 19:34:38
Type : Unknown
Source : acise

Description : Function: Authenticator::buildAndSendHttpMsg

Thread Id: 0xD3C
File: Authenticator.cpp
Line: 196
Level: debug

```
MSG_SN_HTTP_REQUEST, {{url="https://ise22-pri.example.com:8443/auth/perfigo_validate.jsp"},  
{server="ise22-pri.example.com"}, {method="post"}, {object_path=""}, {reuse_existing=1},  
{close_when_done=0},  
{pkt="&user_key=dummykey&cm=10&ops=1&mac_list=C0%3a4A%3a00%3a15%3a75%3aC8&ip_list=10%2e62%2e148%  
2e162&hostname=TSOPREK%2dWIN7%2d1&udid=766bb955e51e4ab063fd478c63acee81260ca592&dm_report_client  
_IV=JjneGgZcJbmjqMKQcy8kJg%3d%3d&dm_report=2yWwY7QzHWCY%2fDVEESSAabEZtYltxNE7Qgy0Oa85Dgo2Ts4ok8s  
IrBM37S2%2fe2Hs0URCP4KkfY4Ap8%2bh%2fqS%2biw50CZe jKG%2bVbF7RTRqZyrg2veWAwwEDsSb%2bqWRRdzvZfSjS3G4  
ApQi07qnfExwN1IvCqrVOp1j17TAcVXEht8NkDg00T9jM%2fTNH%2fMK1lc0o6Ha5juJo4YtWDWY%2bnOancw%3d%3d"},  
{path=""}, {type=1}}.
```

Date : 01/04/2017
Time : 19:34:39
Type : Unknown
Source : acise

Description : Function: HttpHandler::createOutgoingHTTPSMessage
Thread Id: 0xD3C
File: HttpHandler.cpp
Line: 295
Level: debug

```
MSG_NS_HTTP_RESPONSE, {{success=1}, {pkt="<!--error=0--><!--X-Perfigo-DM-Error=0--><!--X-  
Perfigo-Monitoring-Interval=5-->"}, {type=1}}.
```

ةعئاشللا تالكشمللا

ISE لى لوصول AnyConnect لى رذعتي

ءاطخ لى AnyConnect_ISEPosture.txt يوتحي ةلجالل هذه ي

Date : 01/04/2017
Time : 20:04:40
Type : Unknown
Source : acise

Description : Function: Authenticator::buildAndSendHttpMsg
Thread Id: 0xD3C
File: Authenticator.cpp
Line: 196
Level: debug

```
MSG_SN_HTTP_REQUEST, {{url="https://ise22-pri.example.com:8443/auth/perfigo_validate.jsp"},  
{server="ise22-pri.example.com"}, {method="post"}, {object_path=""}, {reuse_existing=1},  
{close_when_done=0},  
{pkt="&user_key=dummykey&cm=10&ops=1&mac_list=C0%3a4A%3a00%3a15%3a75%3aC8&ip_list=10%2e62%2e148%  
2e162&hostname=TSOPREK%2dWIN7%2d1&udid=766bb955e51e4ab063fd478c63acee81260ca592&dm_report_client  
_IV=JjneGgZcJbmjqMKQcy8kJg%3d%3d&dm_report=2yWwY7QzHWCY%2fDVEESSAabEZtYltxNE7Qgy0Oa85Dgo2Ts4ok8s  
IrBM37S2%2fe2Hs0URCP4KkfY4Ap8%2bh%2fqS%2biw50CZe jKG%2bVbF7RTRqZyrg2veWAwwEDsSb%2bqWRRdzvZfSjS3G4  
ApQi07qnfExwN1Pdu7AztTn%2f3VYph9WNF1jG1jXSuTFmr38e%2bVDXQnx7avYHs9meVItYqA6MecAJK3WdkBNSrK1bYjmI  
vzkAPqR2LuoflnA9IcNOTZQ9iN%2fknOjllQsiV5eV6j1MSUeOakKsTwylgbPsFz99eKdtaCMv1F%2fSAmvLApjpk0IMKor  
XXkvpJURtAtOMK751tXdykC85ihgHcI10JW7mlpvIppk5MbcZjihQbXldr5%2fQVdpB8eRqMhF1iCK1gx961wwdzBSfr%2bg  
rcF4072fYYNOa9cYnTFShgU%2bxrnBDcJ1GUoYE9K5nTfGQ01p4NrcbLjpm79e14v14YgfQhmSfktwxFA8pY7A6jmL3BIp30
```


9gmQVnoTqaaccqkW76uT%2bPkjV0YrOgdG0CYuUwUMVqpctGKorxxlC3IwXhBWUmvRY9p2LRdePRqnCN8hpiesyk%2bzTnyX
00aNdHD6%2bGEMGo9QjQvwrL9dcvrUxxHtlQcJPekXajXPfn98FpC8z%2b966tcz4DfMN6giSlEfK6y5%2bMpk0oAL%2fV4X
Mg296PDocGaeTK1OUR7Qkl%2b7S2fv%2fCfZdiQaTndZ6zHWuimq5JBRElmuKI9hWRN2cPERcDn64ISZZSiz9yPoJPlPPpFs
fggkc2PdS00EETMiM%2bBjNKcFx2Tcsq76eYfDtvDq9tGzjST8opInlIiXdAzdbeWsJCAerCvS73xg2vd2DHfpFlrd5lVa3q
wo3Vov3nFiAz4l3IrIlfOHjAE7rCZTy2dWU455icOjM0%2bCVAS3SzwCea4fZu3fAhmIhAVQKElCFZ4CyyBv89340Vw62Bxu
5ij0wbHOSTA8TSbxJXyuGBw8cqTPfuUtqPLx6nWtcrZ6p13MuQTq%2bKZLZ7hwY2Urf1o1gi9OPGyo5zuJZAUQInU%2bkJKU
6ycXHZo17Uti3DITCy0%2fG%2bQ2gixzBIpmJctekKJO243rZiU1wbOUPWLzGum8ydRu3im2LiDisXquAu7ipY5P0D475AZN
3Cd6nlIPP5Mora493QhX4I139q%2birT1%2f5F7tI%2fKLv20fWFC%2fjKbfu%2bFe4QIbdtiSCvLkyZ%2bWdWBMWSXHGE11
CoErbj4LJP3h4oqLto17riGcYmB%2bRHZXXNJA2bwjcfgy4w2FE4hrL0cC6D3YgZxHHpUeT4gMXoXj0EJwODxQwElc9yfoe%2
bdGj4Fy6%2fXc0ymDFYU7oOouAc0nwPKZwhZn4Q3mMZIG5aeOFcx9IM6M47IcMMbo0r78aUk8M94h5f4sK6JxHz75B6JyTx3
H%2bxFDJ3j5UtUYjloir4CLQJgR8ABhMDGxqhAN4c4wa4y790bh2F5PxxVXMGYb4ghFNt3jIHGXRMENPTYkelnd0falnmMhJ
UXE%2fVashJ8aZwcGCU%2fNhSkCATRXb5UDameasKwe3m4bcRtFbBNZ115CNQVH8ZPZsK1GCNPd6dOYkSxa%2fErYqImEzm
9itwSzUuJQXI%2f8%2f%2fKewc9jeBujwHqnjuIYg5sJbjk%2bqc%2fwy5hKHTbxFacnFJlvgJhHt3mht8oRC9EbbsULOAK1
fvLe4%2fe%2bqfJ0e02bw4sQuuLssMKxLsNQMCTIZFzh10K6BZdfolRonKG0MEG1K%2ftSDNC4eyQw9ewYhgpzDvHwlyprp
VY9UgcTvFVSh0Vy%2bwde4b0dtmPdhhQhvvsQOSgnxIX6a8GN4AwXEOE7CoP6%2fFZiTAJTuxUKMjC1m8iAsrAurJugnEgaK
KugSNk19y7bgSiYB6zkthDclEyBFwclrAecfH6oMJs59aJodXnPSAA9FuyqLCWB%2f3WFZ03efhTviz2101G8%2fswMxR0w%
2fR56oNH2wzUwkmh9oczFaYlPJPz6k47ohlzmDJraqyvWgzZfPIipa7EKK8Yvsu04BCFGMrDZtYZnCO6B9CFoKDCNJE9Wxl
%2bhTdzFCA4GpeLE4nT7y1j113iTV%2faWyImNLaRMU2ZiwuKy%2bd2OH55LqnLBCxrUUIMH7Ku4Mhd%2fYvwlNVpcZZ0L%2
bWOkMoephk2XXE4OQAY7Rk%2f%2fRncbbHlFOVQmEVOoxNneBElleaJK%2fxX6C0BZBaebAVYluwdGkkktvgQ5gUvzMiyyqbs
vzyUMzq%2fhgKY7vVMWUeyCsBnybuGPSILJIKMgdgjiz%2baUZsOyZsUE%2b7PPyiqphqXNRfQ6tj8wTzq7a2Z5XgCYI10Pi
qjlmg6hY1TiRYuPanyBqh6lLFKxblkpQJX2339ppqB4RBOzF4%2f3CsvfjU302NSU9fypX5dBYubAZt80DOBe84FSnQIX3pfx
2%2fw9LqclYWbxC2QSOfoHoe6TgkCiOall%2fqUHWqeOogbgLO5s5ffBoNmUCxhJW%2fh1EqKcsFzA%2ba%2f2Q0%2bs2m99R
qlxdd55bg67LXVPGFkH2dbVHjghXj090nLEtVwCfs8oMUIg%2bmnip%2fdA7wDz4Nsma2W0ugEh0jpfFbL2TxHLhE0r%2bwy
3t%2bosvtaxNJZg84LJKpt3J%2bmc0pnIBH5S5H7zrNDKUnIYXY8BD5n1clZi4wwkRIp62avJw7lN22zNHsjp7NUjTYw9X%2
f1Iti1TKxjPZuitU%2bITeCRRHzeoaeGbzE1E%2bGSSqemw7F1wx4w9JXHDAjH%2bY4iX7z2Y4OrY1JQQleeS9KWzw5HdiCp
uHmhMtLMSpz%2fGagw7KeaLEe9FwxrOYILS%2fXuBSTz1XOpbQHilH0ZdQbv2I%2bA%2f3j3GvalSul%2f0YVWlPPPIC2Ogk
SSbd4HyXXh9TEB8dhDmfucy5VEZ5MsuOTgytkALNSK0t9cyvsAcWTQf0uVAMnyBeaMPJAvdE9fXUiH628eMD9PHvt3cL0GYd
RR9WBUCszIFTJNIA5AXj7abdbC6VZ8DqX4YfJ1xgTqg2qKSJqXvtbi5BJU49BGaxu01Ta6eBo2ABltgBxKzb8DYNyqyqRB%2
bYkgr5YdU6z6va15jQJYGUJYVwZ8xDsKvYHz1fUFAHldzxkq44myNAjD1H0DoYhQaXU120UXkg09w5kBqTfmKj9DOJhs5Q88
ilebAbHHxm3GTZSJPp51jQjsPSU13doX3Mz8E7W5pYptxtW1XPwSshkxuhWjbVKKQRTgM5uSXCPQ0PDAqcc6NybV2t1BK3G
hQSPzsQ5k3wklDK7CYuUWMPKTMNLZDVF8i25DoGpA0K5m5s3VMAukLA9Gob5ysU%2fsu2TVBrJZD0sa3L%2bNoF2b01f8BC3
2e.

Date : 01/04/2017
Time : 20:04:41
Type : Unknown
Source : acise

Description : Function: hs_transport_winhttp_post
Thread Id: 0xD3C
File: hs_transport_winhttp.c
Line: 5776
Level: debug

unable to send request: 12029.

Date : 01/04/2017
Time : 20:04:41
Type : Unknown
Source : acise

Description : Function: HttpHandler::createOutgoingHTTPMessage
Thread Id: 0xD3C
File: HttpHandler.cpp
Line: 295
Level: debug

MSG_NS_HTTP_RESPONSE, {{success=0}, {pkt=""}, {type=1}}.

Date : 01/04/2017
Time : 20:04:41
Type : Error
Source : acise

Description : Function: Authenticator::parsePostureData
Thread Id: 0xD3C
File: Authenticator.cpp
Line: 257
Level: error

Failed to communicate with CAS..

Date : 01/04/2017
Time : 20:04:41
Type : Error
Source : acise

Description : Function: SMNavPosture::SMP_handleMonitorResp
Thread Id: 0xD3C
File: SMNavPosture.cpp
Line: 495
Level: error

Failed to parse monitor response.

EP ضرع ةقيرط نم تاقيرطتلا عم قفاوتلا ءاشنإ دنع "لاخ" أطخ ب ISE يقيرلي

ةقيرط نم تاقيرطتلا عم قفاوتلا ءاشنإ ءانثأ "ةيلاخ" ةلاسردوجول اعويش رثكألا ببسلا رادصإ ثدحأ لىل ءضولا ثيدحت موقى نأ بجي . ةبولطملا OPSWAT تاطخم بايغ وه EP ضرع ةقيرطتلا هذه حالصإب .

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إلمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل