ExtremeConnect® User Guide
Version 8.5

7/2020
9036795-00
Subject to Change Without Notice

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, Enterasys Networks, Inc., reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: www.extremenetworks.com/company/legal/trademarks/

Contact

If you require assistance, contact Extreme Networks using one of the following methods.

- Global Technical Assistance Center (GTAC) for Immediate Support
  - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or 1-603-952-5000. For the Extreme Networks support phone number in your country, visit: www.extremenetworks.com/support/contact
  - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This

community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

- Support Portal – Manage cases, downloads, service contracts, product licensing, and training and certifications.

Extreme Networks® Software License Agreement

This Extreme Networks Software License Agreement is an agreement ("Agreement") between You, the end user, and Extreme Networks, Inc. ("Extreme"), on behalf of itself and its Affiliates (as hereinafter defined and including its wholly owned subsidiary, Enterasys Networks, Inc. as well as its other subsidiaries). This Agreement sets forth Your rights and obligations with respect to the Licensed Software and Licensed Materials. BY INSTALLING THE LICENSE KEY FOR THE SOFTWARE ("License Key"), COPYING, OR OTHERWISE USING THE LICENSED SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE LICENSE KEY TO EXTREME OR YOUR DEALER, IF ANY, OR DO NOT USE THE LICENSED SOFTWARE AND CONTACT EXTREME OR YOUR DEALER WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A REFUND. IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT EXTREME, Attn: LegalTeam@extremenetworks.com.

1. DEFINITIONS. "Affiliates" means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. "Server Application" shall refer to the License Key for software installed on one or more of Your servers. "Client Application" shall refer to the application to access the Server Application. "Licensed Materials" shall collectively refer to the licensed software (including the Server Application and Client Application), Firmware, media embodying the software, and the documentation. "Concurrent User" shall refer to any of Your individual employees who You provide access to the Server Application at any one time. "Firmware" refers to any software program or code imbedded in chips or other media. "Licensed Software" refers to the Software and Firmware collectively.
2. TERM. This Agreement is effective from the date on which You install the License Key, use the Licensed Software, or a Concurrent User accesses the Server Application. You may terminate the Agreement at any time by destroying the Licensed Materials, together with all copies, modifications and merged portions in

any form. The Agreement and Your license to use the Licensed Materials will also terminate if You fail to comply with any term of condition herein.

3. GRANT OF SOFTWARE LICENSE. Extreme will grant You a non-transferable, non-exclusive license to use the machine-readable form of the Licensed Software and the accompanying documentation if You agree to the terms and conditions of this Agreement. You may install and use the Licensed Software as permitted by the license type purchased as described below in License Types. The license type purchased is specified on the invoice issued to You by Extreme or Your dealer, if any. YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.
4. LICENSE TYPES.
    - *Single User, Single Computer*. Under the terms of the Single User, Single Computer license, the license granted to You by Extreme when You install the License Key authorizes You to use the Licensed Software on any one, single computer only, or any replacement for that computer, for internal use only. A separate license, under a separate Software License Agreement, is required for any other computer on which You or another individual or employee intend to use the Licensed Software. A separate license under a separate Software License Agreement is also required if You wish to use a Client license (as described below).
    - *Client*. Under the terms of the Client license, the license granted to You by Extreme will authorize You to install the License Key for the Licensed Software on your server and allow the specific number of Concurrent Users shown on the relevant invoice issued to You for each Concurrent User that You order from Extreme or Your dealer, if any, to access the Server Application. A separate license is required for each additional Concurrent User.
5. AUDIT RIGHTS. You agree that Extreme may audit Your use of the Licensed Materials for compliance with these terms and Your License Type at any time, upon reasonable notice. In the event that such audit reveals any use of the Licensed Materials by You other than in full compliance with the license granted and the terms of this Agreement, You shall reimburse Extreme for all reasonable expenses related to such audit in addition to any other liabilities You may incur as a result of such non-compliance, including but not limited to additional fees for Concurrent Users over and above those specifically granted to You. From time to time, the Licensed Software will upload information about the Licensed Software and the associated devices to Extreme. This is to verify the Licensed Software is being used with a valid license. By using the Licensed Software, you consent to the transmission of this information. Under no circumstances, however, would Extreme employ any such

measure to interfere with your normal and permitted operation of the Products, even in the event of a contractual dispute.

6. RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS. Except as expressly permitted in this Agreement, You may not copy or otherwise reproduce the Licensed Materials. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile, disassemble, electronically transfer, or reverse engineer the Licensed Software, or to translate the Licensed Software into another computer language.

   The media embodying the Licensed Software may be copied by You, in whole or in part, into printed or machine readable form, in sufficient numbers only for backup or archival purposes, or to replace a worn or defective copy. However, You agree not to have more than two (2) copies of the Licensed Software in whole or in part, including the original media, in your possession for said purposes without Extreme's prior written consent, and in no event shall You operate more copies of the Licensed Software than the specific licenses granted to You. You may not copy or reproduce the documentation. You agree to maintain appropriate records of the location of the original media and all copies of the Licensed Software, in whole or in part, made by You. You may modify the machine-readable form of the Licensed Software for (1) your own internal use or (2) to merge the Licensed Software into other program material to form a modular work for your own use, provided that such work remains modular, but on termination of this Agreement, You are required to completely remove the Licensed Software from any such modular work. Any portion of the Licensed Software included in any such modular work shall be used only on a single computer for internal purposes and shall remain subject to all the terms and conditions of this Agreement. You agree to include any copyright or other proprietary notice set forth on the label of the media embodying the Licensed Software on any copy of the Licensed Software in any form, in whole or in part, or on any modification of the Licensed Software or any such modular work containing the Licensed Software or any part thereof.

7. TITLE AND PROPRIETARY RIGHTS

   a. The Licensed Materials are copyrighted works and are the sole and exclusive property of Extreme, any company or a division thereof which Extreme controls or is controlled by, or which may result from the merger or consolidation with Extreme (its "Affiliates"), and/or their suppliers. This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.

b. You further acknowledge that in the event of a breach of this Agreement, Extreme shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of this Agreement, Extreme shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Extreme.

8. PROTECTION AND SECURITY. In the performance of this Agreement or in contemplation thereof, You and your employees and agents may have access to private or confidential information owned or controlled by Extreme relating to the Licensed Materials supplied hereunder including, but not limited to, product specifications and schematics, and such information may contain proprietary details and disclosures. All information and data so acquired by You or your employees or agents under this Agreement or in contemplation hereof shall be and shall remain Extreme's exclusive property, and You shall use your best efforts (which in any event shall not be less than the efforts You take to ensure the confidentiality of your own proprietary and other confidential information) to keep, and have your employees and agents keep, any and all such information and data confidential, and shall not copy, publish, or disclose it to others, without Extreme's prior written approval, and shall return such information and data to Extreme at its request. Nothing herein shall limit your use or dissemination of information not actually derived from Extreme or of information which has been or subsequently is made public by Extreme, or a third party having authority to do so.

   You agree not to deliver or otherwise make available the Licensed Materials or any part thereof, including without limitation the object or source code (if provided) of the Licensed Software, to any party other than Extreme or its employees, except for purposes specifically related to your use of the Licensed Software on a single computer as expressly provided in this Agreement, without the prior written consent of Extreme. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized personnel shall have access thereto and that no unauthorized copy, publication, disclosure, or distribution, in whole or in part, in any form shall be made, and You agree to notify Extreme of any unauthorized use thereof. You acknowledge that the Licensed Materials contain valuable confidential information and trade secrets, and that unauthorized use, copying and/or disclosure thereof are harmful to Extreme or its Affiliates and/or its/their software suppliers.

9. MAINTENANCE AND UPDATES. Updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of an Extreme Service and Maintenance Agreement, if Extreme and You enter into such an agreement. Except as specifically set forth in such agreement, Extreme shall not be

under any obligation to provide Software Updates, modifications, or enhancements, or Software maintenance and support services to You.

10. DEFAULT AND TERMINATION. In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Extreme, or in the event that you become insolvent or seek protection, voluntarily or involuntarily, under any bankruptcy law, Extreme may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Extreme and You.
    a. Immediately after any termination of the Agreement or if You have for any reason discontinued use of Software, You shall return to Extreme the original and any copies of the Licensed Materials and remove the Licensed Software from any modular works made pursuant to Section 3, and certify in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been returned to Extreme.
    b. Sections 1, 7, 8, 10, 11, 12, 13, 14 and 15 shall survive termination of this Agreement for any reason.
11. EXPORT REQUIREMENTS. You are advised that the Software is of United States origin and subject to United States Export Administration Regulations; diversion contrary to United States law and regulation is prohibited. You agree not to directly or indirectly export, import or transmit the Software to any country, end user or for any Use that is prohibited by applicable United States regulation or statute (including but not limited to those countries embargoed from time to time by the United States government); or contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or Use.
12. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The Licensed Materials (i) were developed solely at private expense; (ii) contain "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Extreme and/or its suppliers. For Department of Defense units, the Licensed Materials are considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.
13. LIMITED WARRANTY AND LIMITATION OF LIABILITY. The only warranty that Extreme makes to You in connection with this license of the Licensed Materials is that if the media on which the Licensed Software is recorded is defective, it will be replaced without charge, if Extreme in good faith determines that the media and

proof of payment of the license fee are returned to Extreme or the dealer from whom it was obtained within ninety (90) days of the date of payment of the license fee. NEITHER EXTREME NOR ITS AFFILIATES MAKE ANY OTHER WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSED MATERIALS, WHICH ARE LICENSED "AS IS". THE LIMITED WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE EXPRESSLY DISCLAIMED, AND STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR FIRM ARE VOID. ONLY TO THE EXTENT SUCH EXCLUSION OF ANY IMPLIED WARRANTY IS NOT PERMITTED BY LAW, THE DURATION OF SUCH IMPLIED WARRANTY IS LIMITED TO THE DURATION OF THE LIMITED WARRANTY SET FORTH ABOVE. YOU ASSUME ALL RISK AS TO THE QUALITY, FUNCTION AND PERFORMANCE OF THE LICENSED MATERIALS. IN NO EVENT WILL EXTREME OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF DATA OR PROFITS OR FOR INABILITY TO USE THE LICENSED MATERIALS, TO ANY PARTY EVEN IF EXTREME OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL EXTREME OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS. Some states do not allow limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply to You. This limited warranty gives You specific legal rights, and You may also have other rights which vary from state to state.

14. JURISDICTION. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the State of California, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

15. GENERAL.

    a. This Agreement is the entire agreement between Extreme and You regarding the Licensed Materials, and all prior agreements, representations, statements, and undertakings, oral or written, are hereby expressly superseded and

canceled.

b. This Agreement may not be changed or amended except in writing signed by both parties hereto.

c. You represent that You have full right and/or authorization to enter into this Agreement.

d. This Agreement shall not be assignable by You without the express written consent of Extreme. The rights of Extreme and Your obligations under this Agreement shall inure to the benefit of Extreme's assignees, licensors, and licensees.

e. Section headings are for convenience only and shall not be considered in the interpretation of this Agreement.

f. The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto.

g. Extreme's waiver of any right shall not constitute waiver of that right in future. This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement.

h. Should You have any questions regarding this Agreement, You may contact Extreme at the address set forth below. Any notice or other communication to be sent to Extreme must be mailed by certified mail to the following address:

Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 95134 United States
ATTN: General Counsel

Table of Contents

ExtremeConnect Overview

Use the Extreme Management Center **Connect** tab to integrate third-party software with Extreme Management Center's ExtremeControl solution.

The **Menu** icon (☰) at the top of the screen provides links to additional information about your version of Extreme Management Center.

Extreme Management Center's ExtremeControl solution lets you monitor end systems and configure the appropriate experience for users accessing your network based on a variety of criteria. Network administrators may also have a variety of other tools to help monitor and control the user experience. ExtremeConnect bridges the gap between these tools and lets you control your network configurations from Extreme Management Center.

ExtremeConnect Requirements

ExtremeConnect requires an Extreme Management Center advanced license (NMS-ADV).

Navigating the Connect Tab

The tab contains three subtabs:

- **Configuration** – Allows you to enable, disable, and configure all available ExtremeConnect modules.
- **Diagnostics** – Provides information about all end-systems managed by any ExtremeConnect module and their associated end-system groups. Also provides performance statistics per ExtremeConnect module.
- **Services API** – Lets you explore or test the web service provided by ExtremeConnect.

Related Information

For information on related tabs:

- Configuration
- Diagnostics

ExtremeConnect Installation

Tips

- Installation of the ExtremeConnect plugin requires stopping the Extreme Management Center server service. In production environments, a maintenance window is highly recommended for this installation.
- ExtremeConnect already comes packaged with Extreme Management Center 7.0 and does not need to be installed manually. The following instructions are only for reference if a manual installation or update is required for an older version of Extreme Management Center.

Installation of the ExtremeConnect plugin is performed using an installation script. The following table outlines information required during installation of the ExtremeConnect plugin.

Description	Default Value
Installation Directory	/usr/local/Extreme_Networks/Extreme Management Center
Installation Mode	Update

Installation

To perform the installation:

1. Use SCopy application (WinSCP) to download the ExtremeConnect JAR file (NMS_Connect_x.xx_xx.jar) to the root directory.

2. Open an SSH session to the Extreme Management Center server. Change to the following directory:

```
cd/usr/local/Extreme_Networks/Extreme Management Center
```

3. To stop the Extreme Management Center service, enter the following command:

   ```
   service nsserver stop
   ```

   Note: Your Extreme Management Center prompts and version numbers may be different than what is shown here.

4. To initiate the installation script, enter the following command:

   ```
   java/bin/java -jar /NMS_Connect_x.xx_xx.jar –console
   ```

   Caution: NMS_Connect_*x.xx_xx*.jar is the name of the jar file you are installing. Use care with cutting and pasting because the hyphen (-) in the command (`–console`) may change to a period (.). Move the cursor and replace the symbols if needed.

5. Complete installation by following instructions provided in the script. Once the **Starting to unpack** message appears, the installation takes about a minute to complete.

6. Press 1, [Enter] and read the installation instructions that follow.

7. Press 1, [Enter]. Then press [Enter] or enter the target path if different from the default shown.

8. To select **install if no previous version of Extreme Connect is present**, press 0, [Enter].
   To update an existing ExtremeConnect installation and preserves configuration data, select 1.
   To clear the data, select 0.
   To redisplay and confirm your selection, press 3, [Enter].

9. To continue and start the installation, press 1, [Enter]. The installation process will show **Console installation done** when it is finished.

Once the console prompt appears, the installation is complete.

10. To start the Extreme Management Center server service, enter the following command:

```
service nsserver start
```

Post-Installation

After an installation, all modules except the Extreme Management Center module are disabled by default. Each module must be configured and enabled individually. The Extreme Management Center module creates the default end system groups in the Extreme Management Center database (if they do not already exist).

1. To access the ExtremeConnect configuration page, select **OneView > Connect**. The dashboard most likely displays without any data available initially.

2. Each module has its own configuration panel with parameters specific to each of them. You must define the parameter for each value that starts with a $ after a text install before enabling the module.
3. Verify for each plugin that you want to enable that there are no $ variables left before enabling the plugin.
4. After making changes to any variable in the configuration files, select **Save**. Configuration changes are indicated by a red triangle after each save action.
5. Enable the plugins that you want to integrate with Extreme Management Center.

ExtremeControl Configuration

In addition to base connectivity, the ExtremeControl configuration the ability to control the overall behavior of ExtremeConnect. To do so, the ExtremeControl module must be configured to integrate with ExtremeConnect.

Module Configuration

General Module Configuration	Description
Poll interval in seconds	Number of seconds between connections to the Extreme Management Center server.
Module log level	Verbosity of the module. Logs are stored in Extreme Management Center server.log file.
Module enabled	Whether the module is enabled.
Push update to remote service	If set to *true*, the data from other modules will be pushed to the service.
Update local data from remote service	If set to *true*, the data from the remote service will be used to update the internal end system table.
Pending approval end-system group:	The default end system group name to use, if an end system is not approved yet.
Enable Data Persistence	Enabling this option will force the module to store end system data, end system group data, and VLAN data to a file after each cycle. If this option is disabled, the module forgets all of the data after a service is restarted. However, to clean the existing data, the corresponding .dat files must be deleted.

Service-Specific Configuration	Description
Add end-systems to end-system groups	If this is set to *true*, the MAC of the end system will be added to an end system group in Extreme Management Center.
Update custom fields for end-systems	If set to *true*, the custom field data will be updated for each end system.
Update Kerberos username for end-systems	If set to *true*, the username will be updated for each end system and a Kerberos reauthentication will be triggered.
Update devicetype for end-systems	If set to *true*, the device type data will be updated for each end system.
Reauthorize end-system after update	If set to *true*, the end system will be reauthorized after it has been added to an end system group.
Remove end-system from existing groups	If set to *true*, the end system MAC will be removed from all other end system groups, if present.

Service-Specific Configuration	Description
Import End-system Groups	If this is set to *true*, all preconfigured MAC end system groups will be retrieved from Extreme Management Center. All groups with the values `vlan=#NUMBER# approval=#true|false#` in their description field will be used automatically by all other modules (for example, vSphere will create port groups for vSwitches using these values).

Verification

To verify the integration:

1. From OneView, select the **Identity and Access** tab.
2. Navigate to the **End Systems** list.
3. Find an end system that is updated by ExtremeConnect.
4. Navigate to the custom field that you chose during the installation. You should see information such as *vmName=MyVirtualMachine;vmGuestFullName=Ubuntu 5...* or similar information, based on your data sources. The information that displays depends on the module that reports the data to Extreme Management Center.
5. (Optional) To provide a more useful headline, you can rename the custom field in the NAC Manager under **Tools > Options**.

Identity and Access - End System Information

Related Information

For information on related tabs:

ExtremeConnect Overview

ExtremeConnect Configuration

Login Credentials and Module Navigation

To access the Connect **Configuration** tab, log in to Extreme Management Center using an account that is member of the built-in Extreme Management Center Administrators user group.

Each module provides its own specific configuration found under **Connect > Configuration > *Module Name***.

Configuration Tab

The **Configuration** tab provides information about the end systems and end system groups connecting to your network.

Using third-party software (known as modules) in conjunction with the network monitoring and access control functionality found in the Extreme Management Center ExtremeControl solution, the **Configuration** tab provides the most thorough information available about devices accessing your network. Additionally, the **Configuration** tab lets you control end system access to your network using each supported module's functionality.

The **Configuration** tab contains the following subtabs, each providing information about end systems:

- Dashboard – Provides an overview of the end systems monitored by each module and the end systems groups accessing your network.
- End-Systems – Displays the end systems detected for each module.
- End-System Groups – Displays the end system groups detected for each module.
- Administration – Lets you configure how Extreme Management Center communicates with each module and the behavior of the module in Extreme Management Center.
- Statistics – Displays various statistics about the time end systems have spent performing certain operations on the network.
- About – Provides basic information about your version of ExtremeConnect, the number of modules being used by your network, and basic information detected by modules in use.

Dashboard

The **Dashboard** tab provides a top-level overview of the end systems detected on your network. End systems are grouped by the modules that detected them and the end system groups to which they are assigned.

End Systems

The **End-Systems** tab provides information about the end systems connecting to your network.

Left Panel

The left panel of the tab shows all of the modules available in the **Connect** tab.

The **Enabled** column indicates whether the module is enabled:

- Check icon () – Module enabled on your network.
- X icon () – Module not enabled on your network.

Right Panel

The right panel of the tab shows a table with information about the end systems. Add or remove a column by selecting the down arrow at the right of a column header and selecting a checkbox associated with a column from the Columns menu.

End System Groups

The **End-System Groups** tab provides information about the end system groups connecting to your network.

Left Panel

The left panel of the tab shows all of the modules available in the **Connect** tab.

The **Enabled** column indicates whether the module is enabled:

- Check icon () – Module enabled on your network.
- X icon () – Module not enabled on your network.

Right Panel

The right panel of the tab shows a table with information about the end system groups. Add or remove a column by selecting the down arrow at the right of a column header and selecting a checkbox associated with a column from the Columns menu.

Administration

In the **Administration** tab, enter the information that details how Extreme Management Center connects to the module server and configure the module in Extreme Management Center.

The tab contains two subtabs:

- **Services** – A service outlines to Extreme Management Center how it connects to the server of the module you select. This includes the login credentials, IP, and port information for the module.
- **Configuration** – Lets you configure how the module gathers end system information and controls network access in Extreme Management Center and how that information is presented.

Services

Access the **Services** tab to specify information detailing how Extreme Management Center contacts the module's server. The **Services** tab lets you specify multiple services for modules that have more than one server.

Left Panel

The left panel of the tab shows all of the modules available in the **Connect** tab.

The **Enabled** column indicates whether the module is enabled:

- Check icon () – Module enabled on your network.
- X icon () – Module not enabled on your network.

Right Panel

The right panel displays a table containing the services saved for the selected module. The information in this panel varies depending on the module selected in the left panel. The information below is an example using the **Fiberlink MaaS360** module.

ID
A unique identifier for each service. This field cannot be edited.

Username
The username used to access the module's server.

Password
The password used to access the module's server.

apiUrl
The URL that provides access to the module's server.

billingIdEncrypt
The billing account ID used for the module.

appId
The application ID used to contact the module's web service.

appVersion
The application version of the module.

platformId
The platform ID of the module.

accessKey
The key used to communicate with the module server.

Add Service
This button adds a new row in the Services table from which you can create a new service for the module.

Remove Service
This button removes the selected row from the Services table.

Save
This button saves any changes made to services in the Services table.

Refresh
This button updates the table with any changes.

Configuration

The **Configuration** tab lets you specify the information you want the module to gather from end systems in Extreme Management Center as well as the module's access control behavior on the network.

Left Panel

The left panel of the tab shows all of the modules available in the **Connect** tab.

The **Enabled** column indicates whether the module is enabled:

- Check icon () – Module enabled on your network.
- X icon () – Module not enabled on your network.

Right Panel

The right panel displays two tables:

- **General Configuration** – Lets you configure certain general Extreme Management Center criteria.
- **Specific Configuration** – Lets you configure module-specific functionality.

Each module you select in the left panel displays different configurations, depending on the functionality available when using the module.

Name
The name of the configuration. This column cannot be edited.

Description
A brief description of the configuration and how it affects Extreme Management Center. This column cannot be edited.

Save
Select this button to save your changes to any of the configurations on the tab.

Refresh
Select this button to update the **Configuration** tab with any changes you made.

Statistics

Select the **Statistics** tab to view end system statistics for each module.

Left Panel

The left panel of the tab shows all of the modules available in the **Connect** tab.

The **Enabled** column indicates whether the module is enabled:

- Check icon () – Module enabled on your network.
- X icon () – Module not enabled on your network.

Right Panel

The right panel contains a table of the end system statistics captured by the module and a bar graph displaying an average of the statistical entries contained in the table.

About

The **About** tab contains basic information about your version of ExtremeConnect, how it is configured on your network, and information about the end systems, end system groups, VLANs, and scheduled deletions that ExtremeConnect detected on your network.

Module Configuration

There are many different ways to configure ExtremeConnect due to the different third-party software available.

NOTE: For each module configuration, you must select **Save** before proceeding to next module.

Module Configuration	Description
Poll interval in seconds	Number of seconds between connections to the Extreme Management Center server.
Module log level	Verbosity of the module. Logs are stored in the Extreme Management Center server.log file.
Module enabled	Whether the module is enabled.
Push update to remote service	If this is set to *true*, data from other modules is pushed to the service.
Update local data from remote service	If this is set to *true*, data from the remote service is used to update the internal end system table.
Pending Approval end-system group	The default end system group name to use if an end system is not approved yet.
Enable Data Persistence	Enabling this option forces the module to store end system data, end system group data, and VLAN data to a file after each cycle. If this option is disabled, the module forgets all of the data after a service restarts. However, to clean existing data, the corresponding .dat files must be deleted.

Service-Specific Configuration	Description
Add end-systems to end-system groups	If this is set to *true*, the MAC of the end system is added to an end system group in Extreme Management Center.
Update custom fields for end-systems	If this is set to *true*, the custom field data is updated for each end system.
Update Kerberos username for end-systems	If this is set to *true*, the username is updated for each end system and a Kerberos reauthentication is triggered.
Update devicetype for end-systems	If this is set to *true*, the device type data is updated for each end system.
Reauthorize end-system after update	If this is set to *true*, the end system is reauthorized after it has been added to an end system group.
Remove end-system from existing groups	If this is set to *true*, the end system MAC will be removed from all other end system groups, if it is present.
Import End-system Groups	If this is set to *true*, all preconfigured MAC end system groups are retrieved from Extreme Management Center. All groups with the values `vlan=#NUMBER# approval=#true|false#` in their description field will be used automatically by all other modules (for example, vSphere will create port groups for vSwitches using these values).

Verification

To verify whether ExtremeConnect is successfully pushing data from third-party data sources to Extreme Management Center:

1. Open Extreme Management Center's **Control > End-Systems** tab.
2. Find an end system updated by ExtremeConnect and navigate to the custom field. The field displays *vmName=MyVirtualMachine;vmGuestFullName=Ubuntu 5…*or something similar, depending on your data sources. The information displayed here differs a bit depending on the module that reports the data to Extreme Management Center.
3. Make sure that the end system list is displaying the custom field that you have chosen during installation.

NOTE: You can rename the **Custom** field on the **Administration** > **Options** > **Access Control** tab.

Related Information

For information on related tabs:

- Data Center/Cloud Configuration
- Security Configuration
- Mobility Configuration
- Management / IT Operations Configuration
- Data Center Manager (DCM) System Configuration
- Convergence Configuration
- Mobile Device Management (MDM) System Configuration
- ExtremeConnect Assessment Configuration
- Troubleshooting and FAQs

Data Center and Cloud Configuration

The various integrations for Data Center and Cloud focus on the automation of provisioning highly mobile end systems, such as virtual machines (VMs), or providing user information for virtual desktops. Depending on the capabilities of the third-party product, the automation can include the creation of virtual networks and VLAN configuration in the respective product.

- Amazon Web Services
- Google Compute Engine
- Citrix XenServer
- Citrix XenDesktop
- Microsoft Azure
- Microsoft System Center Virtual Machine Manager (SCVMM)
- Microsoft Hyper-V
- VMware vSphere
- VMware View

Amazon Web Services

The Amazon Web Services (AWS) integration provides automation and enhanced security for AWS EC2 instances and security groups. The main use cases are:

- Manage AWS security groups using policies in Extreme Management Center
- Assign AWS EC2 instances automatically to managed security groups
- Import AWS instances to Extreme Management Center
- Import virtual subnets as switches in the Extreme Management Center topology
- Provide reports on data retrieved from the Amazon cloud

Goals

The goals of this integration are to:

1. Import virtual machine (VM) instances from AWS to Extreme Management Center as end systems
2. Import the following items:
    a. AWS subnets to create Extreme Management Center switches
    b. AWS instance interfaces to create Extreme Management Center switch ports
3. Use the following switch data in Extreme Management Center to:
    a. Update the switch nickname, serial number, location, and contact field
    b. Update the switch port name and description field
4. Use the data on the Extreme Management Center end systems to:
    a. Update the custom fields, state, authorization, device family, hostname, IP address
    b. Map them to their connected switch (=AWS subnet) and port (=instance interface on that subnet)
5. Manage security groups based on Extreme Management Center policies:
    a. Import security groups from managed VPCs, as defined in the ExtremeConnect configuration
    b. Compare the corresponding policies from managed policy domains
    c. Create and update security groups based on policies, services, or rules
6. Manage the assignment of EC2 instances to security groups, based on manual Extreme Management Center end system group assignments

7. Provide custom reports on networks, subnetworks, availability zones, and instances

Prerequisites

The following prerequisites must be met:

- Install Extreme Management Center:
  - The minimum version required is Extreme Management Center version 8.2 (some features, like assigning devices and end systems to sites, require version 8.3)
  - The NMS-ADV advanced license must be deployed to enable this and other ExtremeConnect integrations
  - Internet access (ExtremeConnect runs on the Extreme Management Center server and requires access to the AWS cloud)

• Amazon Web Services Account

Integration Overview

The overall architecture is centered around the Extreme Management Center policy domain. Customers can create a dedicated policy domain with policies, service, and rules that they want to use to protect their virtual instances. The ExtremeConnect module's configuration must mention this policy domain as a managed domain and map it to one or more AWS accounts and VPC networks.

Once this domain gets enforced, ExtremeConnect will:

- Compare the policy rules with the existing security groups in the configured account's network
- Convert policy rules to security group rules, and create and update security groups as needed
- Create and update Extreme Management Center end system groups for each managed domain and policy.

  Group names: policyDomain__policyName

After an administrator assigns an Extreme Management Center end system to one of the managed groups, ExtremeConnect assigns the corresponding security groups to the corresponding AWS instance in the cloud to apply the corresponding security group rules.

Multi-Account Support

The integration supports synchronization with multiple AWS accounts. ExtremeConnect pulls all of the instances from all of the configured AWS accounts into Extreme Management Center. It synchronizes the configured list of managed Extreme policy domains to the configured list of AWS VPC networks (configurable per account).

The following diagram shows a setup where two policy domains are created. One policy domain provides a set of standard policies that is synchronized to two AWS cloud accounts. (Not all VPC networks in those two accounts receive those policies.) The other policy domain provides a set of special policies that is synchronized to (a different) one AWS account only .

Managed Domains, ES Groups, and Security Groups

The minimum configuration for this solution requires that you define at least one managed policy domain and map it to at least one account and VPC network (within that account). A managed policy domain is simply a standard policy domain in Extreme Management Center that becomes a managed policy domain by adding it to the ExtremeConnect module's configuration.

ExtremeConnect does not manage or modify the policy domain. Only the Extreme Management Center administrator modifies it. However, these domains are used by ExtremeConnect to:

- Create Extreme Management Center end system groups for each policy
- Create AWS security groups for each policy in the list of configured VPC networks

Those automatically created Extreme Management Center end system groups and AWS security groups are considered managed because they can be created, updated, and deleted by ExtremeConnect. **Important:** They should not be modified manually.

Regarding managed Extreme Management Center end system groups, ExtremeConnect only creates one end system group for each managed policy domain and contained policy, no matter how many accounts are being synchronized. This is because the end system groups represent exactly one policy and even if that policy is exported to multiple accounts, it still represents the same policy.

Mapping Domains to VPC Networks

When configuring how to map a managed domain to a VPC network in AWS the following rules apply:

- One managed policy domain is mapped or exported to one or more VPC networks
- No VPC network can be assigned to more than one policy domain
- Policy domains that are not configured in ExtremeConnect will not be synchronized with AWS
- VPCs that are not configured in ExtremeConnect will not be altered (unmanaged VPCs)
- Customers can manually create additional security groups in managed VPC networks
- Changes to managed security groups will be overwritten on next policy enforce

The following diagram visualizes valid and invalid configurations:

- **Valid:**
  - Map policy domain Custom App1 to VPC network Custom App1
  - Map policy domain Standard Apps to two VPC networks
  - This will create the exact same security groups in both VPC networks
  - Useful for rules that you want to apply to all or most of your VPC networks, as they apply some basic set of common rules
  - Avoids configuration errors, especially when the same rules have to be managed for many VPC networks
- **Not valid:** The red arrow indicates a configuration error since the destination VPC network (FinTech) is already a managed network from the Standard Apps policy domain. A VPC network cannot be fed by more than one policy domain.

VMs with Multiple Interfaces

AWS lets you create a VM with multiple NICs, which allows ExtremeConnect to apply different security groups for each interface of such a VM.

The following image shows two Extreme Management Center end systems that belong to a single AWS VM. ExtremeConnect creates an Extreme Management Center end system for each NIC on an AWS VM. Based on the different group assignments in Extreme Management Center (one end system is assigned to the Cloud__WebServer

group and the other to the Cloud__AppServer group) the corresponding security groups are applied per instance interface in AWS.

Naming Convention

When creating Extreme Management Center end system groups and AWS security groups, ExtremeConnect follows these naming conventions.

Security Group Name & Description

The name of each managed security group uses this syntax:

```
extremePolicyDomain__extremePolicy
```

Example:

```
Hospital__Doctor
```

AWS does not use the name of a security group as its unique identifier, so it is allowed to use the same names on different VPCs. However, ExtremeConnect will never create the same security group name in the same VPC. The security group ID is its identifier and is automatically generated by AWS when a new group is created.

ExtremeConnect also sets the description field of all managed groups. The description is not used by ExtremeConnect, and is meant to be useful for administrators to understand that those groups are managed by ExtremeConnect and should not be edited manually.

Example:

Managed by Extreme Connect - Referenced Domain / Policy: Hospital / Test

The following image shows an example of a security group name and how it is built based on the corresponding Extreme Management Center policy.

Security Group Tag

ExtremeConnect adds two tags to each managed security group that it creates:

- **Name:** Indicates the name of the group (it is not used for anything else).
- **ExtremePolicyId:** This tag is a key identifier used by ExtremeConnect. Each AWS security group that contains this tag is considered a managed group by

ExtremeConnect. **Important:** Do not delete or modify this tag manually. It encodes the policy domain and the policy name that it is based on (refers to).

Example: ExtremePolicyId tag

Hospital__Doctor

This tag is eventually used by ExtremeConnect to identify the correct security group to be applied to an instance.

This visualization shows an example of the security group tags and how they are built based on the corresponding Extreme Management Center policy.

Extreme End System Groups

Each managed Extreme end system group name uses this syntax:

`extremePolicyDomain----extremePolicy`

Example:

`Hospital__Patient`

These end system groups represent a specific policy that you want to apply to a cloud-based instance (which is represented by an end system in Extreme Management Center). The description field lists the accounts and VPC networks that this end system group is used for.

Example:

Managed by Connect for AWS accounts and VPCs: VPCs for account id snappy-bucksaw-168120: [datalab-network], VPCs for account id analytics-research-199618: [kurt-vpc-1, kurt-vpc-2]

This example also shows that it is a valid configuration to synchronize one policy domain with multiple AWS accounts and even multiple VPC networks within a single account.

Sites

Manage Extreme Management Center Sites

Once enabled, this integration creates the following site location automatically:

/World/Cloud

This is the main site node that contains all of the devices that are retrieved from any cloud provider (AWS, Azure and GCP). The node that will hold all of the AWS related devices is created under the main site node automatically. The path is as follows:

/World/Cloud/AWS

The following image shows what the user interface looks like when all three cloud integrations are enabled:

Assign Devices

When you select the /World/Cloud/AWS list item, the list of all retrieved AWS regions displays as subsites and the list of all devices is filtered automatically for those coming from AWS. Each device shows the site it belongs to:

Assign End Systems

Because the end systems are assigned to a switch and that switch belongs to a site, end systems are assigned automatically to the corresponding sites (the AWS region they run in).

Topology - Extreme Management Center Switches

ExtremeConnect creates one device (switch) in Extreme Management Center for each subnet found in AWS (from all configured accounts). ExtremeConnect then creates one switch port for each instance interface that is connected to an AWS subnet. Those switches and ports are used to connect the end systems (instances) virtually, providing a sense of location for each AWS instance.

Creating Devices

The following image shows a section of Extreme Management Center devices that have been created (based on AWS subnets) and shows some of the corresponding AWS subnets.

Before trying to create switches, ExtremeConnect pulls the current list of switches from Extreme Management Center and tries to parse data from their nickname, location, contact, and user data fields. The data encoded is as follows:

- **Nickname:**
  - If the subnet has a Name tag defined in AWS, then the Name tag is used as the nickname
  - If no Name tag is defined, the AWS subnet ID is used as the nickname
- **Site:** The Extreme Management Center site location of the device (region of the subnet)
- **Location:** Zone name of the subnet
- **Contact:** Account name ID (that this subnet is pulled from)
- **User Data 1:** Always shows `cp=aws` (a reference that this device originates from AWS)
- **User Data 2:** AWS VPC ID
- **User Data 3:** AWS subnet ID

Caution!

These fields should never be modified manually.

After creating the switch, ExtremeConnect creates a switch port for each instance interface that is connected to this subnet.

ExtremeConnect encodes data in the following switch port fields:

- **Name:** MAC address of the instance interface
- **Description:** Instance Name and Instance ID

Caution

These fields should never be modified manually.

Automatically Generate Switch IP

The IP addresses are automatically generated based off of the CIDR range provided by AWS for each subnet. Since AWS lets you have the same subnet (with the same CIDR

range) in multiple regions, the switch IP is auto-incremented starting at the first IP in the given CIDR range.

The automatically generated switch IP addresses are not relevant (they are not accessible and cannot be used by Extreme Management Center to talk to any AWS switch) but need to be provided to Extreme Management Center.

Removing and Resynchronizing Extreme Management Center Devices

If a subnet in AWS gets deleted, the corresponding Extreme Management Center switch will be deleted also.

If an Extreme Management Center device gets deleted, and that deleted device corresponds to an existing AWS subnet, ExtremeConnect will re-create this switch.

Updating Extreme Management Center Switch Ports

If a new instance interface is connected to a subnet in AWS, the corresponding Extreme Management Center switch will get a new switch port. Conversely, if an existing instance interface is removed from a subnet in AWS, the corresponding switch port in Extreme Management Center is removed.

Extreme Management Center End Systems

Creating End Systems

This integration creates an end system entry in Extreme Management Center for each AWS instance's network interface.

The following table shows the attributes mapping from AWS instances to Extreme Management Center end systems:

AWS Instance	Extreme Management Center End System
Taken from the instance's network interface's *association* attribute. If a public DNS is provided, then use a public DNS name and public IP address. Otherwise, use a private DNS name and private IP address.	Hostname and IP address
Instance type	Device family

AWS Instance	Extreme Management Center End System
State	State: • RUNNING = ACCEPT • Everything else = DISCONNECTED
Subnet	Switch IP: The Extreme Management Center device IP is automatically generated based on the CIDR of the corresponding AWS subnet
Instance interface	Connected Switch Port: Also shows the zone and instance interface MAC address

All end systems are shown in Extreme Management Center as they are discovered through automatic tracking. By assigning end systems to the corresponding switches, they will also be assigned to the corresponding site.

Updating End Systems

The ExtremeConnect module holds a cache of already synchronized end systems to avoid having to re-create all of the end systems during each poll interval. Therefore, if an AWS instance is already in that cache, tests will be executed on the following end system properties before an update message is sent to the Extreme Management Center API:

- IP address (network interface IP; public IP is preferred)
- Hostname (network interface DNS name; public DNS name is preferred)
- Switch IP (used if the feature to synchronize AWS subnets to Extreme Management Center devices is enabled)
- State
- Authorization

If any of these tests show that an update is required, ExtremeConnect updates the corresponding end system in Extreme Management Center.

Updating Custom Fields

The ExtremeConnect module updates two custom fields for each end system or instance imported from AWS:

- One custom field contains general data about the corresponding instance. The content and syntax of this custom field can be modified through a configuration option, but modifying it will most likely make the reports unavailable. The following data and variables are available:
  - Available variables from an instance (to which the interface belongs): *instanceId*, *instanceState*, *instanceType*, *instanceName*, *tags*
  - Available variables from the instance interface: *mac*, *interfaceId*, *interfaceStatus*, *vpcId*, *subnetId*, *subnetName*, *publicIpAddress*, *privateIpAddress*, *ipAddress*, *publicDnsName*, *privateDnsName*, *description*, *securityGroups*

    The default configuration for this parameter is:

    ```
    iName=#
    instanceName
    #;iStatus=#
    instanceState
    #;nwIfNetwork=#
    vpcId
    #;nwIfSubnet=#
    subnetName
    #;iZone=#
    availabilityZone
    #;nwIfIp=#ipAddress#;iType=#instanceType#
    ```

- Another custom field contains data that is used to identify the AWS instance, its interface, and the account name to which it belongs. **Important:** Do not manually modify the content of this custom field.

  Example content:

  ```
  cp=aws;iId=i-0b4845152d087a585;nwIfId=eni-
  216dc071;accName=MainAccount;vpc=vpc-f2ad7195
  ```

This data can be used to search and filter for end systems.

Removing End Systems

This section describes the mechanisms available to handle end systems that have been removed, deleted, or aged from AWS and therefore do not appear in the result list retrieved via the AWS API.

The following actions can be taken (all of these are configurable):

- Move a deleted end system to the deletion group. You can configure a deletion group on the ExtremeConnect module. Once a synchronized instance has been deleted from AWS, its corresponding MAC address is deleted from any end system group in EAC and added to this end system group. You can use this group to track which end systems are now considered outdated according to AWS.
- Delete end systems from Extreme Management Center. Delete the end system using its MAC address. This does not remove any group memberships, but it does delete the end system from Extreme Management Center.

Extreme Management Center End System Groups

ExtremeConnect uses Extreme Management Center end system groups (MAC-based) for two purposes:

1. As a catch-all group that can be configured to put all instance MACs into a single end system group for awareness. You can use this group to simplify searches, grouping, and filtering.

2. For each managed policy (from all managed domains), ExtremeConnect creates an end system group. When an end system MAC gets added to such an end system group, the corresponding AWS instance gets assigned to the corresponding security group. Pushing Extreme Management Center end systems to groups enforces security groups in AWS.

If those end systems get added to MAC groups that are not managed by ExtremeConnect, no change to the corresponding instances' security group assignment is performed.

If you configure a valid (existing) MAC-based end system group for the feature *Default endsystem group for all instances*, be aware that if you have done all three of the following actions:

- Manually deleted entries from this group
- Enabled the feature *Assign AWS security groups based on XMC end-system groups*
- Enabled the feature *Overwrite manual security group assignment*

ExtremeConnect removes any previously, manually configured security group assignment from the corresponding AWS instance, which can lead to communication issues with that instance. ExtremeConnect only keeps automatically assigned security groups on that instance. Additionally, if the corresponding end system has only been in that default catch-all group and is not member of any other group, ExtremeConnect removes all of the security group assignments from that instance (except for the default security group from its VPC) that could impact its connectivity.

Configuration

Verify that you have met the prerequisites before configuring the module.

AWS API Access

To retrieve any data from the AWS API, the following parameters are required:

- Access key ID
- Access key secret
- Default region

You can generate the access key and secret access key by following these directions located at this URL:

http://docs.aws.amazon.com/IAM/latest/UserGuide/ManagingCredentials.html#Using_CreateAccessKey

Make sure that the user you base this API access key from has sufficient permissions to use the API, manage both security groups and managed security groups assigned to instances, and pull data on security groups, instances, zones, subnets and managed security groups.

The following steps are a summary (from the AWS documentation) of how to create, modify, or delete a users' access key and secret:

1. Sign in to the AWS Management Console. Open the IAM console at https://console.aws.amazon.com/iam/.
2. From the navigation pane, select **Users**.
3. Select the name of the preferred user, and select the **Security credentials** tab.

4. If needed, expand the **Access keys** section and do any of the following:
    a. To create an access key, select **Create access key**. To save the access key ID and secret access key to a CSV file on your computer, select **Download .csv file**. Store the file in a secure location.
    Important: You will not have access to the secret access key again after this dialog closes.

    After you have downloaded the CSV file, select **Close**.
    b. To disable an active access key, select **Make inactive**.
    c. To re-enable an inactive access key, select **Make active**.
    d. To delete an access key, select its **X** button at the far right of the row. Select **Delete**.

AWS Default Region

The default region is required for some API calls (that are not region-specific) and is set to *us-east-1* by default.

All available regions can be found at this URL:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

Configure ExtremeConnect

The best practice is to perform the configuration from the Extreme Management Center web user interface on the **Connect** tab. (Customers should not have to use the configuration file directly. For informational purposes, on an XMC v8.1 server, the file is located at /usr/local/Extreme_Networks/NetSight/wildfly/standalone/configuration/connect /AwsHandler.xml)

AWS Account-Specific Configuration

The **Services** tab in the Amazon Web Services Connect module configuration section lets you configure AWS account-specific information.

General Configuration

The **Configuration** tab in the Amazon Web Services Connect module configuration section provides more options. Most of them are similar to all other modules and therefore are not discussed in detail in this section.

Module Configuration

The following table describes the configuration options available for the Amazon Web Services module:

All of the end systems are shown in Extreme Management Center as they discovered through automatic tracking. By assigning end systems to the corresponding switches, they are assigned to the corresponding site as well.

Updating End Systems

Service-Specific Configuration	Description
Account Name	A freely configurable name for each AWS account to which you want to synchronize. The name identifies which instances belong to which accounts. This name is not part of the AWS API authorization.
Access Key ID	Used to authenticate and authorize Connect against the AWS API (see chapter above to create a key).
Access Key Secret	Used to authenticate and authorize Connect against the AWS API (see chapter above to create a key secret).
Managed Domains and VPCs	List of managed policy domains and their corresponding managed VPCs. Only policy domains configured here are used to export policies to AWS. One policy domain can be mapped to one or more VPCs. No VPC can be assigned to more than one policy domain. The managed domains and VPCs must be given in the following format: `domainName:vpcId1,vpcId2;domainName2:vpcId5,vpcId7` . Example: `Hospital:vpc-d8c5ada1`
Default Region	Used when creating new security groups. The AWS API requires a default region for this operation. **Default value:** us-east-1 **All available regions:** us-gov-west-1, us-east-1, us-east-2, us-west-1, us-west-2, eu-west-1, eu-west-2, eu-west-3, eu-central-1, ap-south-1, ap-southeast-1, ap-southeast-2, ap-northeast-1, ap-northeast-2, sa-east-1, cn-north-1, cn-northwest-1, ca-central-1

Service-Specific Configuration	Description
Regions to ignore	A list of region names that should be ignored when retrieving any data from AWS. Use semicolons to separate the region names. Tests have shown that some regions seem to have special authorization and usually produce errors when trying to query them (such as China or government). If no value is defined, ExtremeConnect tries to retrieve data from all regions. **All available regions:** us-gov-west-1, us-east-1, us-east-2, us-west-1, us-west-2, eu-west-1, eu-west-2, eu-west-3, eu-central-1, ap-south-1, ap-southeast-1, ap-southeast-2, ap-northeast-1, ap-northeast-2, sa-east-1, cn-north-1, cn-northwest-1, ca-central-1 **Default value:** us-gov-west-1;cn-north-1;cn-northwest-1

General Module Configuration	Description
Custom field to use for identification data	The number of the custom data fields for each end system to use for storing the identification data. This data is used to identify the corresponding AWS instance, network interface, and account name. It also encodes the type of cloud provider used to pull this data from (in this case: *aws*). **Important:** This value must not be the same as the configured value for **Custom field to use**. Format example: `cp=aws;iId=4253868206409840076;nwIfFp=u7wnZ-pBoYg=;accN=analytics-research-199618`
HTTP client socket timeout in milliseconds	HTTP socket timeout, in milliseconds, for all HTTP connections to the AWS API. Defines how much time is allowed for the socket towards the AWS API to be unresponsive. **Default:** 50000 (=50 seconds)
HTTP client connection timeout in milliseconds	HTTP connection timeout, in milliseconds, for all HTTP connections to the AWS API. Defines how much time is allowed for ExtremeConnect to open up a socket to the AWS API. **Default:** 10000 (=10 seconds)
Sync Policies with AWS Security Groups	When this is set to *true*, synchronizes (exports) the policies from a domain on an enforce to AWS security groups.
Sync Policies with XMC end system groups	The format of the ExtremeConnect data (such as last seen time, switch IP, switch port) that is written to the description fields of the VMs in AWS. You can customize the appearance and what information you want to include or exclude.

General Module Configuration	Description
Assign AWS security groups based on XMC end system groups	When this is set to *true*, this operation assigns EC2 instance interfaces to AWS security groups, based on the end system groups that the corresponding end system is assigned to in Extreme Management Center/EAC. The mapping between the EC2 instance interface and the Extreme Management Center end system is based on the MAC address.
Overwrite XMC end systems' Device Family with instance machine type	If enabled, uses the instance type from AWS to overwrite the device family field for imported end systems in Extreme Management Center.
Create switches in XMC for AWS Subnetworks	If enabled, imports all subnets from AWS and creates one managed device (switch) per subnet in Extreme Management Center.
Delete end systems from XMC that have been deleted from AWS	If enabled, deletes the corresponding end system from Extreme Management Center if an AWS instance has been deleted. In addition to deleting the MAC address from any group, this operation deletes the end system entry from the NAC end system list.
End system group for deleted AWS instances	If an instance or any of its network interfaces gets deleted in AWS, the corresponding end systems are pushed to this end system group.
Remove end systems from other groups on decommission	Enable this field to remove a device from all other groups when the device is moved to the Decommission group.
Regularly auto-enforce policies to AWS	When enabled, ExtremeConnect automatically verifies whether the managed policy domains are correctly synchronized to the configured VPCs. This helps to ensure that your policy configuration is kept consistent with your security groups in AWS, even if someone manually changes the managed security groups in AWS.
Regularly auto-enforce	When enabled, ExtremeConnect automatically verifies whether the managed policy domains are correctly synchronized to the configured VPCs. This helps to ensure that your policy configuration is kept consistent with your security groups in AWS, even if someone manually changes the managed security groups in AWS.

Alarm and Event Messages

This section lists all of the customer visible event messages on the Extreme Management Center **Alarms & Events** tab. This ExtremeConnect module does not generate any alarms, only events. If you want to elevate some of those events to alarms and trigger additional actions, use the Alarm Configuration feature in Extreme Management Center.

Policy Verification

There are four types of events generated when ExtremeConnect verifies policy domains with AWS security groups and Extreme Management Center end system groups.

Started Policy Verification with AWS

This event is triggered when the verification process is started. This can occur manually through a *domain verify* or *domain enforce* operation (the verification is done automatically prior to enforcing) or automatically on each module poll cycle (when the feature *Regularly auto-enforce policies to AWS* is enabled).

Started Policy Verification with Extreme Management Center End System Groups

This event is triggered when the verification process is started. This can occur manually through a *domain verify* or *domain enforce* operation (the verification is done automatically prior to enforcing) or automatically on each module poll cycle (when the feature *Regularly auto-enforce policies to XMC End-System Groups* is enabled).

Finished Policy Verification with AWS

This event is triggered when the verification process is finished. It shows the results of the verification.

Example 1: No change required

Example 2: A new policy (containing two rules) has been created on Extreme Management Center but has not yet been synchronized to AWS. This policy is missing in the configured managed AWS VPC network:

Finished Policy Verification with Extreme Management Center End System Groups

This event is triggered when the verification process is finished. It shows the results of the verification.

Example 1: No change required

Example 2: A new policy has been created on Extreme Management Center but has not yet been synchronized to an Extreme Management Center end system group:

Policy Enforcement

There are four types of events generated when ExtremeConnect enforces policy domains with AWS security groups and Extreme Management Center end system groups.

Started Policy Enforcement with AWS

This event is triggered when the enforcement process is started. This can occur manually through a domain enforce or automatically on each module poll cycle (when the feature *Regularly auto-enforce policies to AWS* is enabled).

Started Policy Enforcement with Extreme Management Center End System Groups

This event is triggered when the enforcement process is started. This can occur manually through a *domain enforce* operation or automatically on each module poll cycle (when the feature *Regularly auto-enforce policies to XMC End-System Groups* is enabled).

Finished Policy Enforcement with AWS

This event is triggered when the enforcement process is finished. It shows the results of the verification.

Example 1: No change required

Example 2: A new policy (containing two rules) has been created on Extreme Management Center. ExtremeConnect created one new security group in AWS:

Finished Policy Enforcement with Extreme Management Center End System Groups

This event is triggered when the enforcement process is finished. It shows the results of the verification.

Example: A new policy has been created on Extreme Management Center and has been enforced to an Extreme Management Center end system group. The name of that new end system group is provided in the event text:

Security Group Assignment

Whenever an Extreme Management Center end system that corresponds to an AWS instance is assigned to or removed from a managed Extreme Management Center end system group, then the corresponding instance get its assigned security groups updated (to enforce the corresponding policy). To reflect that action, the following event is logged:

Verification

This section provides information on where to find the data in Extreme Management Center that was imported from AWS.

Viewing Device Data

The devices that are automatically created for each AWS subnet will contain the following data:

- **Name:** If the subnet has a Name tag defined in AWS, that will be used. If not, the AWS subnet ID is used
- **Site:** The Extreme Management Center site location of the device (region of the subnet)
- **IP Address:** Automatically generated IP address (this is **not** the real IP of that subnet)
- **Device Type:** Always shows the AWS subnet
- **Family:** Always shows the cloud service platform
- **Location:** Zone that the subnet runs in
- **Contact:** User configured name of the AWS account that holds this subnet
- **User Data 1:** Always shows `cp=aws` (a reference that this device originates from AWS)
- **User Data 2:** AWS VPC ID

- **User Data 3:** AWS subnet ID
- **Network OS:** Always shows ExtremeConnect

To filter the list of devices per region, select **Sites** and select a region name:

Another way to filter for all devices generated based on the AWS subnets is to filter the list of devices using **by Device Type**, and select **Cloud Service Platform > AWS-Subnet**:

Viewing End System Data

To find the end system data imported from AWS in Extreme Management Center:

1. Select **Connect > Configuration > End Systems**.
2. For the imported AWS instances, look at **Custom 1** for general instance data.
3. Look at **Custom 2** for AWS-specific data.
4. On the **End Systems** tab, review the current status, IP address, hostname (public or private DNS name), device family (machine type), switch IP, switch nickname (AWS subnet) and port (zone & MAC of the instance interface). The Authentication Type is always set to *Auto-Tracking* to indicate the source of this data.

Cloud Reports

Introduced with Extreme Management Center v8.2, the AWS cloud reports are part of the Multi-Cloud dashboard. (To view the reports, select **Networks > Dashboard > Multi-Cloud**).

AWS Report

The AWS report shows:

- Statistics
- Instance Distribution by AWS
- Account Distribution of VMs per machine type (top 10)

- Distribution of VMs per zone (top 10)
- Distribution of VM interfaces per subnets (top 10)

Instance Details Report

The Instance Details report shows the list of all AWS instances with details about each VM:

Google Compute Engine

This integration provides automation and enhanced security regarding Google Compute Engine (GCE) instances and firewall rules. The main use cases are:

- Manage GCE firewall rules using policies in Extreme Management Center
- Automatically assign GCE instances to managed firewall rules
- Import GCE instances to Extreme Management Center
- Import virtual subnets as switches in the Extreme Management Center topology
- Provide reports on data retrieved from the Google Compute cloud

Goals

1. Import virtual machine (VM) instances from GCE to Extreme Management Center as end systems
2. Import the following:
    a. GCE subnets to create switches in Extreme Management Center
    b. GCE instance interfaces to create switch ports in Extreme Management Center
3. Use the data from the Extreme Management Center switches to:
    a. Update the nickname, serial number, location, and contact fields
    b. Assign the switches to Extreme Management Center sites
    c. Update the switch port name and description fields
4. Use the data on the end systems in Extreme Management Center to:
    a. Update the custom, state, authorization, device family, hostname, and IP address fields

   b. Map the data to their connected switch (=GCE subnet) and port (=instance interface on that subnet), which also maps them to their sites
5. Manage firewall rules based on Extreme Management Center policies:
   a. Import firewall rules from managed VPCs, as defined in the ExtremeConnect configuration
   b. Compare the rules to corresponding policies from managed policy domains
   c. Create and update firewall rules based on policies, services, and rules
6. Manage instance assignment to firewall rules, based on manual Extreme Management Center end system group assignments
7. Provide custom reports about networks, subnetworks, zones, and instances

Prerequisites

The following prerequisites must be met:

- Install Extreme Management Center:
  - The minimum version required is Extreme Management Center v8.2
  - The NMS-ADV advanced license must be deployed to enable this and other ExtremeConnect integrations
  - Internet access (ExtremeConnect runs on the Extreme Management Center server and requires access to the Google cloud)
- Google Compute Engine Account and Project

Integration Overview

The overall architecture is centered around the Extreme Management Center policy domain. Customers can create a dedicated policy domain with policies, service, and rules that they want to use to protect their virtual instances. The ExtremeConnect module's configuration must mention this policy domain as a managed domain and must map it to one or more projects and VPC networks.

Once this domain gets enforced, ExtremeConnect will:

- Compare the policy rules with the existing firewall rules in the configured project's network
- Convert policy rules to firewall rules, and create and update firewall rules as needed
- Create and update Extreme Management Center end system groups for each managed domain and policy.

Group names: *policyDomain__policyName*

After an administrator assigns an Extreme Management Center end system to one of the managed groups, ExtremeConnect adds the corresponding network tag to the corresponding GCE instance in the cloud to so that the corresponding firewall rules can be applied.

Multi-Account Support

The integration supports synchronization with multiple GCE projects. ExtremeConnect pulls all of the instances from all of the configured GCE projects into Extreme Management Center. It synchronizes the configured list of managed Extreme policy domains to the configured list of GCE VPC networks (configurable per project).

The following diagram shows a setup where two policy domains are created. One policy domain provides a set of standard policies that is synchronized to two GCE cloud projects. (Not all VPC networks in those two projects receive those policies.) The other policy domain provides a set of special policies that is synchronized only to a different, singular GCE project.

Managed Domains, ES Groups & Firewall Rules

The minimum configuration for this solution requires that you define at least one managed policy domain and map it to at least one project and network (in that project). A managed policy domain is a standard policy domain in Extreme Management Center that becomes managed by adding it to the ExtremeConnect module's configuration.

ExtremeConnect does not modify the policy domain; only the Extreme Management Center administrator modifies it. The managed policy domains are used by ExtremeConnect to create:

- Extreme Management Center end system groups for each policy
- GCE firewall rules for each policy rule in the list of configured VPC networks

These automatically created Extreme Management Center end system groups and GCE firewall rules are considered managed because they can be created, updated, and deleted by ExtremeConnect. **Important:** They should not be modified manually.

Regarding managed Extreme Management Center end system groups, ExtremeConnect only creates one end system group for each managed policy domain and contained

policy, no matter how many projects are being synchronized. This is because those end system groups represent exactly one policy and even if that policy is exported to multiple projects, it still represents the same policy.

Mapping Domains to VPC Networks

When configuring how to map a managed domain to a VPC network in GCE, the following rules apply:

- One managed policy domain is mapped or exported to one or more VPC networks
- No VPC network can be assigned to more than one policy domain
- Policy domains that are not configured in ExtremeConnect will not be synchronized to GCE
- VPC networks that are not configured in ExtremeConnect will not be altered (they are unmanaged VPCs)
- Customers can manually create additional firewall rules in managed VPC networks
- Changes to managed firewall rules will be overwritten on next policy enforcement operation

The image below visualizes valid and invalid configurations:

- **Valid:**
  - Map the policy domain *Custom App1* to VPC network *Custom App1*
  - Map the policy domain *Standard Apps* to two VPC networks
    - Creates the exact same firewall rules in both VPC networks
    - Can be useful for rules that you want to apply to all or most of your VPC networks because they apply some basic set of common rules
    - Avoids configuration errors, especially when the same rules have to be managed for many VPC networks
- **Not valid:** The red arrow indicates a configuration error since the destination VPC network (FinTech) is already a managed network from the Standard Apps policy domain. A VPC network cannot be managed by more than one policy domain.

VMs with Multiple NICs

Google lets you to create a VM with multiple NICs. In this case, each NIC must be connected to a different VPC. Google supports the assignment of different firewall rules on each NIC. Additionally, to support this mechanism through ExtremeConnect, it creates dedicated network tag names per VPC. Therefore, when you create an Extreme Management Center policy domain named *Cloud* and configure ExtremeConnect to synchronize this domain with GCE VPC1 and VPC2, it creates two firewall rules for each Extreme Management Center policy rule and appends the corresponding VPC name to it.

Example:

- cloud----appserver----vpc1
- cloud----appserver----vpc2

The following image shows two Extreme Management Center end systems that belong to a single GCE VM. ExtremeConnect creates an Extreme Management Center end system for each NIC on a GCE VM.

This is what was configured in the previous example and the corresponding result:

Configuration	Result
Add an Extreme Management Center end system that represents NIC0 on GCE VPC phanindervpc2 to Extreme Management Center end system group Cloud__App Server	The network tag `cloud----appserver----phanindervpc2` is added to the corresponding GCE VM
Add Extreme Management Center end system that represents NIC1 on GCE VPC default to Extreme Management Center end system group Cloud__Web Server	The network tag `cloud----webserver----default` is added to the corresponding GCE VM, which now has two network tags assigned.

In GCE, you can inspect the firewall rules that are active per NIC.

Active rules for NIC0 (only those belonging to the policy web server):

Active rules for NIC1 (only those belonging to the policy app server):

Naming Convention

When creating Extreme Management Center end system groups and GCE firewall rules, ExtremeConnect follows a specific naming convention. GCE firewall rule names and network tags must follow these naming convention rules: **only lowercase letters, numbers, and hyphens are allowed**.

To convert the various parts that are used to construct rule names and network tags, the following conversion rules are applied:

- Spaces are converted to hyphens
- Underscores are converted to hyphens
- Round brackets are converted to hyphens

Firewall Rule Name

The name of each managed firewall rule uses this syntax:

```
extremePolicy----extremePolicyRule----gceVpcNetwork
```

Example:

```
appserver----https----default
```

The four hyphens between the three rule name parts are inserted as separators to be able to clearly distinguish between them. If fewer hyphens were used (for example: three), you could not easily distinguish between the separator and a policy name (or rule name) because of the conversion rules. For example, if a policy name contains a space, a hyphen and another space (example: *Doctors - Resident*), then ExtremeConnect would convert this into three hyphens (example: *Doctors---Resident*).

The GCE network name is also encoded as part of the firewall rule name since administrators can configure ExtremeConnect to synchronize a policy domain with multiple VPC networks (within the same GCE project) and ExtremeConnect would end up trying to create multiple rules with the same name on different VPC networks. GCE does not permit that, so rule names must be unique even across network borders.

The following image shows an example of a rule name and how it is built based on the corresponding Extreme Management Center policy rule:

Firewall Rule Description Field

The description field of each managed firewall rule uses this syntax:

```
Managed by Extreme Connect;
ExtremePolicyId='extremePolicyDomain__extremePolicy__
extremePolicyService__extremePolicyRule'
```

Example:

```
Managed by Extreme Connect; ExtremePolicyId='Cloud__AppServer_
_AppAccess__HTTPS'
```

The first part is static and indicates that this rule is automatically managed by ExtremeConnect and should **not** be modified manually. The important part is the *ExtremePolicyId*, which consists of four parts separated by two underscores and encodes as follows:

- Extreme Networks policy domain name
- Extreme Networks policy name
- Extreme Networks policy service name
- Extreme Networks policy rule name

The *ExtremePolicyId* in the description field is essential for ExtremeConnect to correctly map a firewall rule to its corresponding Extreme Networks policy rule.

You can add your own comments to the description field as long as the automatically created text is not modified.

The following image shows an example of a rule description and how it is built based on the corresponding Extreme Management Center policy rule:

Firewall Target Tag

Each managed firewall rule gets a target tag applied using this syntax:

```
extremePolicyDomain----extremePolicy----googleVPC
```

Example:

```
cloud----appserver----default
```

This network tag is eventually used to apply a firewall rule to instances. When the same network tag is assigned to an instance, that firewall rule gets applied to traffic from and to that instance.

This tag is critical for the functionality of the ExtremeConnect automation. ExtremeConnect adds the same network tag to all firewall rules it creates for a specific policy and then assigns that network tag to all instances that need to be enforced with that policy.

ExtremeConnect automatically appends the name of the VPC for which this rule is created to the network tag. This allows the assignment of different tags to different network interfaces on the same VM.

The following image shows an example of a target tag and how it is built based on the corresponding Extreme Management Center policy:

Extreme End System Groups

Each managed Extreme Networks end system group name uses this syntax:

```
extremePolicyDomain----extremePolicy
```

Example:

```
Hospital__Patient
```

These end system groups represent a specific policy that you want to apply to a cloud-based instance (which is represented by an end system in Extreme Management Center). The description field lists the projects and VPC networks that this end system group is used for.

Example:

Managed by Connect for GCE projects and VPCs: VPCs for project id snappy-bucksaw-168120: [datalab-network], VPCs for project id analytics-research-199618: [kurt-vpc-1, kurt-vpc-2]

This example also shows that it is a valid configuration to synchronize one policy domain into multiple GCE projects and even multiple VPC networks in a project.

Sites

Manage Extreme Management Center Sites

Once enabled, this integration automatically creates the site location as follows:

/World/Cloud

This site node will contain all devices that are retrieved from any cloud provider (AWS, Azure, and GCP). Under the main node, the node that will hold all GCP related devices is created automatically. The path is as follows:

/World/Cloud/GCP

The following image shows what the user interface looks like when all three Cloud integration are enabled:

Assign Devices

When you select the /World/Cloud/GCP list item, the list of all retrieved GCP regions are displayed as subsites and the list of all devices is automatically filtered for those coming from GCP. Each device shows the site it belongs to.

Assign End Systems

Because the end systems are assigned to a switch and that switch belongs to a site, the end systems are assigned automatically to the corresponding sites (such as the GCP region they run in).

Topology - Extreme Management Center Devices (Switches)

ExtremeConnect creates one device (switch) in Extreme Management Center for each subnet found in GCE (from all configured projects and all regions from those projects). ExtremeConnect then creates one switch port for each instance interface that is connected to a GCE subnet. Those switches and ports are used to connect the end systems (instances) virtually, providing a sense of location for each GCE instance.

Creating Devices

The following image shows a section of Extreme Management Center devices that have been created based on GCE subnets and some of the corresponding GCE subnets.

Before creating switches, ExtremeConnect pulls the current list of switches from Extreme Management Center and tries to parse data from various fields. The following data is encoded:

- **Name:** GCP lets customers automatically create a subnet per region for all new VPC networks. If this option is used, all of those subnets are named Default automatically, which is not very helpful in identifying where they run or what they are used for. Therefore, ExtremeConnect uses the subnet name as switch nickname only if it is not named Default. If the subnet is called Default, ExtremeConnect uses the subnet's CIDR address as switch nickname.
- **Site:** The Extreme Management Center site location of the device (region of the subnet)
- **IP address:** Automatically generated IP (this is **not** the real IP of that subnet)
- **Device Type:** Always shows the GCP subnet
- **Family:** Always shows the cloud service platform
- **Location:** Region that the subnet runs in
- **Contact:** GCP project ID
- **User Data 1:** Always shows `cp=gcp` (a reference that this device originates from GCP)
- **User Data 2:** GCP VPC ID
- **User Data 3:** GCP subnet ID
- **Network OS:** Always shows ExtremeConnect

Caution

These fields should never be modified manually.

After creating the switch, ExtremeConnect creates a switch port for each instance interface that is connected to this subnet.

ExtremeConnect encodes the data in the following switch port fields:

- **Name:** Instance ID and instance name, which allows ExtremeConnect to map the end systems correctly.
- **Description:** Instance name and instance IP address.

Caution

These fields should never be modified manually.

Automatically Generate Switch IP

The IP addresses are automatically generated based off the fixed IP net 10.253.0.0. The first switch that gets created will have the IP 10.253.0.1, the second 10.253.0.2, and so on.

IP addresses are generated in this static manner because in Google the subnets' CIDR ranges are, by default, reused on each network - they use the same CIDR on different networks, resulting in duplicates.

Removing and Resynchronizing Extreme Management Center Devices

If a subnet in GCE gets deleted, the corresponding Extreme Management Center switch is deleted also.

If an Extreme Management Center device gets deleted and its corresponding GCE subnet still exists, ExtremeConnect will re-create this switch.

Updating Extreme Management Center Switch Ports

If a new instance interface is connected to a subnet in GCE, the corresponding Extreme Management Center switch will get a new switch port. If an existing instance interface is removed from a subnet in GCE, the corresponding switch port in Extreme Management Center is removed.

Extreme Management Center End Systems

Creating End Systems

This integration creates an end system entry in Extreme Management Center for each GCE instance's network interface.

The following table shows the attributes mapping from GCE instances to Extreme Management Center end systems:

GCE Instance	Extreme Management Center End System
MAC address not exposed by the API	Automatically generated MAC address, starting with the private MAC address range 02:00:00:
Network IP address	IP address

GCE Instance	Extreme Management Center End System
Name	Hostname
Machine type	Device family
Status	State: • RUNNING: ACCEPT • Everything else: DISCONNECTED
Subnet	Connected switch
Instance interface	Connected switch port. Also shows zone and instance interface name

All end systems are shown in Extreme Management Center and are discovered through the auto-tracking functionality. By assigning end systems to the corresponding switches, they are assigned to the corresponding site also.

Updating End Systems

The ExtremeConnect module holds a cache of already synchronized end systems in order to avoid having to re-create all end systems during each poll interval. Therefore, if a GCE instance is already on that cache, tests will be executed on the following end system properties before an update message is sent to the Extreme Management Center API:

- IP address (network interface IP)
- Hostname (=instance name)
- Switch IP (if you enabled the feature to synchronize GCE subnets to Extreme Management Center devices)
- Status
- Authorization

If any of these tests show that an update is required, ExtremeConnect updates the corresponding end system in Extreme Management Center.

Automatically Generate End System MAC Address

Because the GCE API does not provide a MAC address for their instance interfaces and Extreme Management Center requires a unique MAC per end system, ExtremeConnect

automatically generates one for each instance interface. All generated MACs start with the private range 02:00:00.

Updating Custom Field

The ExtremeConnect module updates two custom fields for each end system or instance imported from GCE. The data in these fields can be used to search and filter for end systems.

- One custom field contains general data about the corresponding instance. The content and syntax of this custom field can be modified through a configuration option, but modifying it will most likely make the reports unavailable. The following data and variables are available:
    - Available variables from an instance (which the interface belongs to): *instanceId*, *instanceName*, *instanceStatus*, *instanceMachineType*, *instanceDescription*, *instanceZone*, *instanceLabels*, *instanceTags*
    - Available variables from the instance interface: *mac*, *nwIfFingerprint*, *nwIfIp*, *network*, *subnetwork*, *nwIfAccessCfgType*, *nwIfAccessCfgName*, *nwIfAccessCfgNatIp*

      The default configuration for this parameter is:
      `iName=#`*`instanceName`*`#;iStatus=#`*`instanceStatus`*`#;nwIfNetwork=#`*`network`*`#;nwIfSubnet=#`*`subnetwork`*`#;iZone=#`*`instanceZone`*`#;nwIfIp=#`*`nwIfIp`*`#;iType=#`*`instanceMachineType`*`#`
- The second custom field contains data that is used to identify the GCE instance, its interface, and the project to which it belongs. **Important:** Do not manually modify the content of this custom field.

  Example:
  `cp=gce;iId=2330535448434796975;nwIfFp=4pGmMNaDfJc=;pId=analytics-research-199618`

Removing End Systems

This section describes the mechanisms available to handle end systems that have been removed, deleted, or aged from GCE and therefore do not appear in the result list that is

retrieved via the GCE API.

The following actions can be performed (all of them are configurable):

- Move deleted end systems to the deletion group. You can configure a deletion group on the ExtremeConnect module. Once an already synchronized instance has been deleted from GCE, its corresponding MAC address is deleted from any end system group in EAC and added to this end system group. Administrators can use this group to track which end systems are now outdated according to GCE.
- Delete end systems from Extreme Management Center by using its MAC. This does not remove any group memberships, but it does delete the end system from Extreme Management Center.

Extreme Management Center End System Groups

ExtremeConnect uses Extreme Management Center end system groups (MAC-based) for two purposes:

1. As a catch-all group that can be configured to put all instance MACs into a single end system group for awareness. Use this group to simplify searches, grouping, and filtering.
2. For each managed policy (from all managed domains), ExtremeConnect creates an end system group. When an end system MAC gets added to an end system group, the corresponding GCE instance gets the corresponding network tag applied. By pushing Extreme Management Center end systems to groups, firewall rules are enforced in GCE.

If the end systems get added to MAC groups that are not managed by ExtremeConnect, no change is made to the corresponding instances' network tags.

If you configure a valid (existing) MAC-based end system group for the feature *Default end system group for all instances*, be aware that if you do all three of the following items:

- Manually delete entries from this group
- Enable the feature *Assign GCE firewall rules based on XMC end-system groups*
- Enable the feature *Overwrite manual firewall assignment*

ExtremeConnect will remove any previously, manually configured network tag from the corresponding GCE instance. This can lead to communication issues with that instance. ExtremeConnect only keeps automatically assigned network tags on that instance, and if

the corresponding end system is only in that default catch-all group and is not member of any other group, ExtremeConnect removes all of the network tags from that instance, which can impact its connectivity.

Configuring GCE Authorization

After you meet the prerequisites described previously, you can configure the integration.

To authorize ExtremeConnect to pull data from GCE, you must create a service account, authorize it properly, and provide the corresponding JSON file to ExtremeConnect.

Generate the required JSON authentication file by following the directions listed at this URL:

https://cloud.google.com/iam/docs/creating-managing-service-account-keys

To summarize, for each GCE project you want to manage through ExtremeConnect, you will need one service account. To create a dedicated service account:

1. Log in to https://console.cloud.google.com.
2. From the left menu, select **IAM & Admin > Service Accounts**.
3. Select **Create Service Account** (at the top).
4. Provide a name, select the role **Compute Admin**, enable **Furnish a new private key**, and set the Key Type to **JSON.**

   This downloads a file that is required by ExtremeConnect to authenticate against your Google project. You can rename the downloaded file to make it clear what it is used for.
5. Using WinSCP, copy the downloaded file to this folder on your Extreme Management Center server: /usr/local/Extreme_Networks/NetSight/wildfly/standalone/configuration/connect

Configure ExtremeConnect

The best practice is to perform the configuration from Extreme Management Center user interface on the **Connect** tab. (If needed, you can access the configuration file directly. On an Extreme Management Center v8.1 server it is located at: /usr/local/Extreme_Networks/NetSight/wildfly/standalone/configuration/connect /GoogleComputeEngineHandler.xml.)

Google Project-Specific Configuration

The **Services** tab in the Google Compute Engine Connect module configuration section lets you configure the list of GCE project IDs to pull data from.

Example: A multi-project, multi-VPC configuration

General Configuration

The **Configuration** tab in the Google Compute Engine Connect module provides more options.

Module Configuration

The following tables describe the configuration options available for the GCE module:

Service-Specific Configuration	Description
GCE project id	This ID is located on the project's main dashboard in the Project Info widget. The project ID is a different value than the project name or the project number.
GCE authentication file name (JSON file)	The file you generated for your service account. Copy the service account file to your Extreme Management Center server using this location: **/usr/local/Extreme_ Networks/NetSight/wildfly/standalone/configuration/connect**
Mapping for Extreme policy domains to GCE VPC networks	The format for this mapping is: `PolicyDomainName:gceVpcName1,gceVpcName2,…`

General Module Configuration	Description
Custom field to use	The number of the custom data field for each end system to store the service-specific incoming data. This data is used for reporting, search, and filter functionality. The format of this custom field data can be configured using the parameter format of the incoming data, and generally should not be modified. **Default value:** 1

General Module Configuration	Description
Format of the incoming data	Format of the data that gets stored in the **Custom data field to use** field. **Default configuration and syntax example:** `iName=#`*`instanceName`*`#;iStatus=#`*`instanceStatus`*`#; nwIfNetwork=#`*`network`*`#;nwIfSubnet=#`*`subnetwork`*`#; iZone=#` *`instanceZone`* `#;nwIfIp=#`*`nwIfIp`*`#;iType=#`*`instanceMachineType`*`#` Available variables for an instance (to which the interface belongs) are: *instanceId*, *instanceName*, *instanceStatus*, *instanceMachineType*, *instanceDescription*, *instanceZone*, *instanceLabels*, *instanceTags*. Available variables from the instance interface are: *mac*, *nwIfFingerprint*, *nwIfIp*, *network*, *subnetwork*, *nwIfAccessCfgType*, *nwIfAccessCfgName*, *nwIfAccessCfgNatIp*
Custom field to use for identification data	The number of the custom data field for each end system to use for storing the identification data. This data is used to identify the corresponding GCE instance, network interface, and project ID. It also encodes the type of cloud provider used to pull this data from (in this case, *gce*). **Format example:** `CP=gce;iId=4253868206409840076;nwIfFp=u7wnZ-pBoYg=;pId=analytics-research-199618` **Important:** This value must not be the same as the configured value for **Custom field to use**. **Default value:** 2
Overwrite XMC end systems' Device Family with instance machine type	If enabled, uses the machine type from GCE to overwrite the device family field for imported end systems in Extreme Management Center.
Create switches in XMC for GCE Subnetworks	If enabled, imports all subnets from GCE and tries to create one managed device (switch) per subnet in Extreme Management Center.
Sync Policies with GCE Firewalls	When this is set to **true**, synchronizes (exports) the policies from a domain on an enforce to GCE firewall rules.
GCE max query results per poll	Maximum number of results per API query or poll. This limits the number of results (instances, subnetworks, and so on) returned from the GCE API, per request. If any resource provides more than the configured number of results, ExtremeConnect repeats the query as often as necessary to retrieve all of the available items (=paging). **Default:** 100

General Module Configuration	Description
Timeout (seconds) for all GCE API calls related to firewalls	All GCE API operations that create, update, and delete take time to finalize. ExtremeConnect checks the status of these operations every second. This parameter can be configured to define the maximum number of seconds that ExtremeConnect waits for these tasks to complete. If the configured timeout is exceeded, ExtremeConnect stops checking for the status and assumes that the task failed (although the task might still be running on the GCE cloud and will be finalized later). **Default**: 20
Assign GCE firewall rules based on XMC end system groups	When this is set to **true**, assigns instances to GCE firewall rules based on the end system groups that the corresponding end system is assigned to in Extreme Management Center/EAC. The mapping between the instance and Extreme Management Center end system is based on the MAC address.
Overwrite manual firewall assignment	When this is set to **true**, overwrites any manual firewall assignment of instance interfaces in GCE. When an end system is assigned to a group in Extreme Management Center/EAC, this parameter helps ensure that the corresponding instance is only assigned to managed firewall rules. Any other (non-managed) assigned firewall rules will be removed. Only applicable if the feature **Assign firewall based on endsystem group** is enabled.
Delete end systems from XMC that have been deleted from GCE	If enabled, deletes the corresponding end system from Extreme Management Center if a GCE instance has been deleted. This deletes the MAC address from any group and deletes the end system entry from the NAC end system list.
End system group for deleted GCE instances	If an instance or any of its network interfaces get deleted in GCE, the corresponding end systems are pushed to this end system group.
Remove end systems from other groups on decommission	Enable this parameter to remove a device from all other groups when the device is moved to the decommissioned group.
Regularly auto-enforce policies to GCE	When enabled, ExtremeConnect automatically verifies whether the managed policy domains are correctly synchronized to the configured VPCs. This operation helps to ensure that your policy configuration is kept consistent with your firewall rules in GCE, even if someone manually changes those managed firewall rules in GCE.
Regularly auto-enforce policies to XMC end system Groups	When enabled, ExtremeConnect automatically verifies whether the managed policy domains are correctly synchronized to the automatically created Extreme Management Center end system groups. This operation helps to ensure that your policy configuration is kept consistent with the Extreme Management Center end systems groups even if someone manually changes those managed groups.

Alarm and Event Messages

This section lists all of the visible event messages that can be found on the Extreme Management Center **Alarms & Event**s tab. This ExtremeConnect module does not generate any alarms, only events. If you want to elevate some of those events to alarms and trigger additional actions, use the Alarm Configuration feature in Extreme Management Center.

Policy Verification

There are four types of events generated when ExtremeConnect verifies policy domains with GCE firewall rules and Extreme Management Center end system groups.

Started Policy Verification with GCE

This event is triggered when the verification process is started. This can occur manually through a *domain verify* or *domain enforce* (the verification is done automatically prior to enforcing) or automatically on each module poll cycle (when the feature *Regularly auto-enforce policies to GCE* is enabled).

Started Policy Verification with Extreme Management Center End System Groups

This event is triggered when the verification process is started. This can occur manually through a *domain verify* or *domain enforce* (the verification is done automatically prior to enforcing) or automatically on each module poll cycle (when the feature *Regularly auto-enforce policies to XMC End-System Groups* is enabled).

Finished Policy Verification with GCE

This event is triggered when the verification process is finished. It will show the results of the verification.

Example 1: No change required

Example 2: A new policy (containing two rules) is created on Extreme Management Center but has not yet been synchronized to GCE. These policy rules are missing in both of the two managed GCE VPC networks (kurt-vpc-1 and kurt-vpc-2)

Finished Policy Verification with Extreme Management Center End System Groups

This event is triggered when the verification process is finished. It shows the results of the verification.

Example 1: No change required

Example 2: A new policy is created on Extreme Management Center but has not yet been synchronized to an Extreme Management Center end system group. These policy rules are missing in both of the two managed GCE VPC networks (kurt-vpc-1 and kurt-vpc-2)

Policy Enforcement

There are four types of events generated when ExtremeConnect enforces policy domains with GCE firewall rules and Extreme Management Center end system groups.

Started Policy Enforcement with GCE

This event is triggered when the enforcement process is started. This can occur manually through a *domain enforce* or automatically on each module poll cycle (when the feature *Regularly auto-enforce policies to GCE* is enabled).

Started Policy Enforcement with Extreme Management Center End System Groups

This event is triggered when the enforcement process is started. This can occur manually through a *domain enforce* or automatically on each module poll cycle (when the feature *Regularly auto-enforce policies to XMC End-System Groups* is enabled).

Finished Policy Enforcement with GCE

This event is triggered when the enforcement process is finished. It shows the results of the verification.

Example 1: No change required

Example 2: A new policy (containing two rules) is created on Extreme Management Center. ExtremeConnect created four new firewall rules in GCE: two rules in VPC network kurt-vpc-1 and (the same) two rules in VPC network kurt-vpc-2:

Finished Policy Enforcement with Extreme Management Center End System Groups

This event is triggered when the enforcement process is finished. It shows the results of the verification.

Example: A new policy is created on Extreme Management Center and has been enforced to an Extreme Management Center end system group. The name of that new end system group is provided in the event text:

Firewall Assignment

Whenever an Extreme Management Center end system that corresponds to a GCE instance is assigned to or removed from a managed Extreme Management Center end system group, then the corresponding instance get its network tags updated (to enforce the correct set of firewall rules). To reflect that action, the following event is logged:

Verification

Viewing Device Data

The devices that are automatically created for each GCP subnet contain the following data:

- **Name:** GCP lets customers automatically create a subnet per region for all new VPCs. If this option is used, all of those subnets are named Default automatically, which is not very helpful in identifying where they run or what they are used for. Therefore, ExtremeConnect uses the subnet name as switch nickname only if it is not named Default. If the subnet is named Default, ExtremeConnect uses the subnet's CIDR address as switch nickname instead.
- **Site:** The Extreme Management Center site location of the device (region of the subnet)
- **IP address:** Automatically generated IP address (this is not the real IP of that subnet)
- **Device Type:** Always shows the GCP subnet
- **Family:** Always shows the cloud service platform

- **Location:** Region that the subnet runs in
- **Contact:** GCP project ID
- **User Data 1:** Always shows `cp=gcp` (the reference that this device originates from GCP)
- **User Data 2:** GCP VPC ID
- **User Data 3:** GCP subnet ID
- **Network OS:** Always shows ExtremeConnect

To filter the list of devices per region, select **Sites** and select the region name you want to find:

Another way to filter for all devices generated based on GCP subnets is by selecting **by Device Type** and navigating to **Cloud Service Platform > GCP-Subnet**:

Viewing End System Data

In the end system table, you should see data on all end systems that are based on imported GCE instances.

To find the data imported from GCE in Extreme Management Center:

1. Select **Connect > Configuration > End Systems**.
2. For the imported GCE instances (which are based on the configured project IDs), look at **Custom 1** for general instance data.
3. Look at **Custom 2** for GCE-specific data.
4. On the end systems page, review the current status, IP address (public, if available; otherwise private IP), hostname (instance name), device family (machine type), switch IP (automatically generated and considered irrelevant), authorization (list of network tags assigned to the instance), switch nickname (showing the GCE subnet name) and switch port (GCE instance zone, ID, and interface name). The Authentication Type will always be set to *Auto-Tracking* to indicate the source of this data.

Cloud Reports

Introduced with Extreme Management Center v8.2, the GCE cloud reports are part of the Multi-Cloud dashboard. (To access the dashboard, select **Networks > Dashboard > Multi-Cloud**).

GCE Report

The GCE report shows:

- Statistics
- Distribution of VMs per project
- Distribution of VMs per machine type (top 10)
- Distribution of VMs per zone (top 10)
- Distribution of VM interfaces per subnets (top 10)

Instance List Report

The Instance List report shows the list of all GCE instances with details about each VM:

Citrix XenServer

The Citrix XenServer (XenServer) integration allows the provisioning of virtual machines in the network and automating the creation of virtual networks based on end system access groups. Additionally, the data in Extreme Management Center is enriched for each end system and is reciprocally made available within XenCenter. (XenCenter is the management tool for XenServer environments.)

Module Configuration

Service Configuration	Description
Username	Username used to connect to the XenServer web service. Read/Write/Execute permissions are required.
Password	Password used to connect to the XenServer web service.

Service Configuration	Description
XenCenter Webservice URL	Web service URL of the XenSever.
XenCenter Server IP	IP address of the XenServer.

General Module Configuration	Description
Poll interval in seconds	Number of seconds between connections to the XenServer.
Module log level	Verbosity of the module. Logs are stored in the Extreme Management Center server.log file.
Module enabled	Whether the module is enabled.
Push update to remote service	If set to *true*, the data from other modules will be pushed to the service.
Update local data from remote service	If set to *true*, the data from the remote service will be used to update the internal end system table.
Default end system group:	The default end system group name to use, if it is not set dynamically.
Enable Data Persistence	Enabling this option forces the module to store end system data, end system group data, and VLAN data to a file after each cycle. If this option is disabled, the module forgets all of the data after a service is restarted. However, to clean the existing data, the corresponding .dat files must be deleted.

Service-Specific Configuration	Description
Custom field to use	The custom field within ExtremeControl to update the information for end systems retrieved from XenServer. **Valid values:** 1-4.
Outgoing data format	The format of the ExtremeControl data (such as last seen time, switch IP, switch port) that is written to the description fields of the VMs in XenServer. You can customize the appearance and customize what information you want to include or exclude.
Format of the incoming data	The format of the data that is received from XenServer and written to the custom field.

Service-Specific Configuration	Description
Use global end system groups	Allows the module to use the global end system groups of the ExtremeConnect. This enables the XenServer module to use the end system groups retrieved from the ExtremeControl module and assign XenServer VMs to these end system groups.
Network deletion	If this option is enabled, networks created by end system groups are deleted if the end system group no longer exists, or if synchronization is disabled. Any connected VM is rerouted to the designated Deletion Group.
Deletion Group	If the Network Deletion feature is enabled, this setting defines the catch all network for VMs that have been connected to a Xen network after it has been deleted in Extreme Management Center. For example: If you have a Xen network, such as VM Test, that is managed by ExtremeConnect and you delete the corresponding end system group in Extreme Management Center, this feature makes sure that all VMs that are connected to the VM Test are disconnected from it, and automatically reconnected to the Xen network defined with this setting. This feature functions as a fallback network for all VMs that are connected to ExtremeConnect managed Xen networks.
Destroy NIC Bonds	If enabled, ExtremeConnect automatically destroys (removes) a bonding of 2 or more NICs on the Citrix XenServer, in case the last network that used this bond has been removed using the Extreme Management Center group configuration. Example: You create a new end system group using multiple NICs with `nic=eth0:eth1`. ExtremeConnect will create both of the following: - A bond over eth0 + eth1 with a default naming schema - A new external network connected to that bond named as your end system group. Next, you create a second end system group also using the same NIC definition `nic=eth0:eth1`. This action only creates a new external network connected to the existing bond and is called according to your end system group. If you then delete (or set `sync=false`) one of these end system groups, only the external Xen network is removed and not the bond, because the bond is in use by the other network. If you then delete the other end system group, the corresponding external network is deleted and the bond between eth0 and eth1 is destroyed.

Verification

To verify the integration:

1. Select a virtual machine.
2. On the right side of the screen, select the **General** tab.
3. At the top of the **General** tab, a description field contains the corresponding data from Extreme Management Center. If this data is correct, the integration is verified.

Citrix XenDesktop

The integration with XenDesktop is a one-way integration. Information on virtual desktops is retrieved from XenDesktop and used in NAC, but no data or configuration is sent from NAC to XenDesktop.

NOTE: The Citrix XenDesktop integration requires an adapter agent to be installed and configured before enabling the corresponding module in ExtremeConnect. The adapter file is provided by Extreme Networks.

Module Configuration

The following tables describe the configuration options available for the XenDesktop Connect module (the configuration file is XenDesktopHandler.xml).

Service Configuration	Description
Adapter IP	The IP address on which the Extreme XenDesktop adapter runs. (This IP is configured in the adapter's configuration file.) It should run on the same IP address as the XenDesktop server.
Adapter Port	The TCP port on which the Extreme XenDesktop adapter runs. (This is port configured in the adapter's configuration file).
Pre-Shared Key	The key used to encrypt traffic from and to the adapter that is running on the XenDesktop server. This key must match the configured pre-shared key from the adapter's configuration file.

General Module Configuration	Description
Poll interval in seconds	The wait time between two polls. The module contacts the XenDesktop adapter and requests the latest data on the VDI infrastructure. The module then waits for this interval to pass before polling the adapter again.
Module log level	Verbosity of the module. Logs are stored in Extreme Management Center's server.log file.
Module enabled	Whether the module is enabled.
Update local data from remote service	If this is set to *true*, the data from the remote service is used to update the internal end system table.

General Module Configuration	Description
Default end system group	The default end system group name to use, if it is not set dynamically.
Enable Data Persistence	Enabling this option forces the module to store end system data and end system group data to a file after each cycle. If this option is disabled, the module forgets all of the data after a service restarts. However, to clean the existing data, the corresponding .dat files must be deleted.

Service-Specific Configuration	Description
Custom field to use	The custom field in Extreme Management Center that is used to update the information for end systems that are retrieved from the adapter that is running on the XenDesktop server. **Valid values:** 1-4.
Format of the incoming data	The format of the data that is received from the adapter that is running on the XenDesktop server. It is also the format that is written to the custom field.

Adapter Installation

ExtremeConnect retrieves data from the XenDesktop server using an adapter. This adapter must be installed and configured before enabling the corresponding module in ExtremeConnect. The adapter consists of a Java executable file (JAR) and a configuration file.

There is no dedicated installer for the adapter. The best practice is to install the adapter manually using the following steps:

1. Install Windows .NET Framework 3.5 SP1 or above, Windows PowerShell 2.0, and the latest Java Runtime Environment (JRE) on the XenDesktop server.
2. Locate the file Datacenter Manager XenDesktop Adapter.zip on the Extreme Control server in the directory**../jboss/server/default/deploy/fusion_jboss.war/XenPlugin/** (it can also be downloaded using a browser at https://Extreme Control-IP:8443/fusion_jboss/XenPlugin/Datacenter%20Manager%20XenDesktop%20Adapter.zip).
3. Copy the executable JAR file (DCM_XENDESKTOP_ADAPTER_<version>.jar) and the configuration file (DCM_XENDESKTOP_ADAPTER.config) into a

separate directory, created under **Program Files/Extreme Networks/XenDesktop Adapter** directly on the XenDesktop server.

4. Edit the configuration file according to your environment. The configuration file contains an explanation of all of the settings. You can also find them listed below.
5. Save and close the configuration file.
6. Start the adapter manually by opening a CMD shell or PowerShell.
7. Navigate to the installation directory and use the following command: `java -jar DCM_XENDESKTOP_ADAPTER_<version>.jar`.
8. Check the log file to validate proper functionality.
9. In OneView or NAC Manager, check the custom field in the end system list to see data for the XenDesktop virtual machines that you configured in the XenDesktopHandler.xml configuration file.
10. After verifying the integration, make sure that the DCM_XENDESKTOP_ ADAPTER_1.00.jar file is starting automatically during the Windows server startup by following these steps:
    a. Stop the adapter that is currently running in the CMD or PowerShell window.
    b. Configure the auto-start for the JAR file (this depends on your Windows Server version). Restart your XenDesktop server, when appropriate, to test the auto-start of the JAR file. You should see a Java process running in the process tree.

Adapter Configuration

The following table lists the configuration options for the XenDesktop agent.

Configuration Option	Description
NETSIGHT_IP	IP address of the Extreme Management Center server.
NETSIGHT_ USERNAME	Username to authenticate against the Extreme Management Center server.
NETSIGHT_ PASSWORD	Password to authenticate against the Extreme Management Center server.
LOG_LEVEL	Set the log level of the adapter to one of the following values: ERROR, WARN or DEBUG. **Default:** WARN.
IP	IP address for the web service (=agent) to listen on.

Configuration Option	Description
PORT	TCP Port for the web service to listen on. **Warning:** This port must **not** be used by any other application on this server.
XENDESKTOP_SERVER	The host or DNS name of the XenDesktop Deliver Controller to connect to. This has only been tested with this adapter and the XD Deliver Controller running on the same server, although remote connections might work as well. **Example:** XenDesktop5 or with FQDN: XenDesktop5.test.local.
PRE_SHARED_KEY	The pre-shared key used for the communication between the adapter and ExtremeConnect. This must match the key entered when installing the ExtremeConnect XenDesktop module.
IS_PRE_SHARED_KEY_ENCRYPTED	If set to *false*, the adapter assumes that the pre-shared key configuration is not encrypted. On the first start, the adapter automatically encrypts the key and set this value to *true*. If you want to change this key at a later stage, change the PRE_SHARED_KEY value, then set this value back to *false*, then restart the adapter service.
ENABLE_PUSH_USER_TO_NETSIGHT	If set to *true*, the adapter uses web service calls to Extreme Management Center to push the username for each virtual desktop session to the corresponding end system in Extreme Management Center/NAC. If configured properly in NAC, this causes a re-authentication of the user on this virtual desktop and assigns a user-based policy.
ENABLE_PUSH_DATA_TO_NETSIGHT	If set to *true*, the adapter pushes end system data back to the corresponding module in ExtremeConnect/Extreme Management Center. This enables you to retrieve data on the virtual desktop in ExtremeConnect/Extreme Management Center and display it in the NAC Manager end system table.

Verification

To verify proper functionality, validate the data in the custom field that was configured for the XenDesktop integration in your end system list (in NAC Manager or OneView). For each virtual desktop currently in use, you should see information similar to the following graphic:

You will see the user name being set accordingly only if you enable the following option in the adapter's configuration file:

ENABLE_PUSH_USER_TO_NETSIGHT=*true*

You will see the additional information (in the custom column that you specified in your XenDesktopHandler Connect configuration file) only if you have enabled the following option in the adapter's configuration file:

ENABLE_PUSH_DATA_TO_NETSIGHT=*true*

NOTE: The user name from XenDesktop can also be used to assign a policy to each user automatically, as you could do with any 802.1X or Kerberos user name. Before enabling this feature, verify that you have configured your rule set in NAC correctly.

Microsoft Azure

This integration provides automation and enhanced security regarding Microsoft Azure (Azure) virtual machines and security groups. The main use cases are:

- Manage Azure security groups through Extreme Management Center using policies
- Automatically assign Azure virtual machines (VMs) to managed security groups
- Import Azure VMs to Extreme Management Center
- Import virtual subnets as switches in Extreme Management Center (topology)
- Provide reports on data retrieved from the Azure cloud

Goals

1. Import VMs from Azure as end systems to Extreme Management Center
2. Import:
    a. Azure subnets to create Extreme Management Center switches
    b. Azure network interfaces to create Extreme Management Center switch ports
3. Use this data on the created Extreme Management Center switches to:
    a. Update the switches' nickname, location, contact and user data
    b. Assign the switches to Extreme Management Center sites
    c. Update the switch ports' name and description
4. Use this data on the created Extreme Management Center end systems to:
    a. Update the custom fields, state, authorization, device family, hostname, IP address
    a. Map them to their connected switch (=Azure subnet) and port (=network interface on that subnet), which also maps them to sites

5. Manage security groups based on Extreme Management Center policies:
    a. Import security groups from managed resource groups (defined in ExtremeConnect configuration)
    b. Compare to corresponding policies from managed policy domains
    c. Create and update security groups based on policies, services, and rules
6. Manage virtual machine assignment to security groups, based on manual Extreme Management Center end system group assignments
7. Provide custom reports on networks, subnetworks, availability zones, and VMs

Prerequisites

The following prerequisites must be met:

- Extreme Management Center:
    - The minimum version required is Extreme Management Center version 8.2 (some features, such as assigning devices and end systems to sites, require Extreme Management Center version 8.3)
    - The NMS-ADV advanced license must be deployed to enable this and other ExtremeConnect integrations
    - Internet access (ExtremeConnect runs on the Extreme Management Center server and requires access to the Azure cloud)
- Microsoft Azure Account

Integration Overview

The overall architecture is centered around the Extreme Management Center policy domain. Customers can create a dedicated policy domain with policies, service and rules that they want to use to protect their virtual VMs. The ExtremeConnect module's configuration must mention this policy domain as a managed domain and must map it to one or more Azure accounts and resource groups.

Once this domain gets enforced, ExtremeConnect will:

- Compare the policy rules with the existing security groups in the configured account's resource group
- Convert policy rules to security group rules, and create or update security groups as needed
- Create and update Extreme Management Center end system groups for each managed domain and policy

  Group names: policyDomain__policyName

After an administrator assigns an Extreme Management Center end system to one of the managed groups, ExtremeConnect assigns the corresponding security groups to the corresponding Azure VM in the cloud to apply the corresponding security group rules.

Multi-Account Support

The integration supports synchronization with multiple Azure accounts or subscriptions. ExtremeConnect pulls all VMs from all of the configured Azure accounts into Extreme Management Center. It also synchronizes the configured list of managed Extreme policy domains to the configured list of Azure resource groups (configurable per account).

The visualization below shows a setup where two policy domains are created. One provides a set of standard policies that is synchronized to two Azure cloud accounts. (Not all resource groups in those two accounts receive those policies.) The other policy domain provides a set of special policies which is synchronized to (a different) Azure account.

Managed Domains, ES Groups & Security Groups

The minimum configuration for this solution requires the administrator to define at least one managed policy domain and map it to at least one account and resource group (within that account). A managed policy domain is simply a standard policy domain in Extreme Management Center, and it becomes a managed policy by adding it to this ExtremeConnect module's configuration.

ExtremeConnect is actually not managing (modifying) the policy domain. Only the Extreme Management Center administrator is modifying it. However, such domains are used by ExtremeConnect to:

- Create Extreme Management Center end system groups for each policy
- Create Azure security groups for each policy in the list of configured resource groups

Those automatically created Extreme Management Center end system groups and Azure security groups are considered managed because they can be created, updated, and deleted by ExtremeConnect. **Important:** They should not be modified manually.

Regarding managed Extreme Management Center end system groups, ExtremeConnect only creates one end system group for each managed policy domain and contained policy, no matter how many accounts are being synchronized. The reason is that those

end system groups represent exactly one policy and even if that policy is exported to multiple accounts, it still represents the same policy.

Mapping Domains to Resource Groups

When configuring how to map a managed domain to a resource group in Azure, the following rules apply:

- One managed policy domain is mapped and exported to one or more resource groups
- No resource group can be assigned to more than one policy domain
- Policy domains that are not configured in ExtremeConnect will not be synchronized to Azure
- Resource groups that are not configured in ExtremeConnect will not be altered (they are considered unmanaged resource groups)
- Customers can manually create additional security groups in managed resource groups
- Changes to managed security groups will be overwritten on next policy enforce

The following image visualizes valid and invalid configurations:

- **Valid:**
  - Map policy domain *Special Policies* to resource group *Special App1*
  - Map policy domain *Standard Policies* to two resource groups, which:
    - Create the exact same security groups in both resource groups
    - Is useful for rules that you want to apply to all or most of your resource groups since they apply a basic set of common rules
    - Avoids configuration errors, especially when the same rules have to be managed for many resource groups
- **Not valid:** The red arrow indicates a configuration error since the destination resource group *FinTech* is already a managed resource group from the Standard Policies policy domain. A resource group cannot be managed by more than one policy domain.

Security Groups for Multi-Regional Resource Groups

Azure allows the configuration of a resource group spanning multiple regions. If you create a resource group that contains a virtual machine in region USEAST and another VM running in region USWEST, then ExtremeConnect will have to create all managed security groups twice: one for each region. This is required because you cannot assign a virtual machine from one region to a security group from another region. The example below demonstrates this. In this example, you cannot assign the VM1 to the security groups Cloud_WebServer_USWEST nor Cloud_DbServer_USEAST.

The diagram below an example configuration:

Naming Convention

When creating Extreme Management Center end system groups and Azure security groups, ExtremeConnect follows these naming conventions.

In general, Azure requires adherence to the following naming rules for both security group and security group rule names:

- Can be up to 80 characters long
- Must begin with a word character, and it must end with a word character or with an underscore (_)
- Can contain word characters or a period (.), hyphen (-), or underscore (_)

Security Group Name & Tag

The name of each managed security group uses this syntax:

```
extremePolicyDomain__extremePolicy
```

Example:

```
Cloud__DB_Server
```

Due to the name rules in Azure, the generated name can be different from the original name of the Extreme policy domain and policy. The previous example was created based on a policy named DB Server, but ExtremeConnect has to replace the space with an underscore (_) to make the name adhere to Azure naming conventions. ExtremeConnect will replace the following characters in the policy domain and policy name if they contain an underscore (_), colon (:), comma (,), slash (/), period (.).

ExtremeConnect will also truncate the name if it is longer than 80 characters.

To allow ExtremeConnect to correctly map an Azure security group back to its Extreme domain and policy, the names are encoded in their original form with a tag that ExtremeConnect adds to each security group it creates or manages: *ExtremePolicyId*.

Caution

Do not delete or modify this tag manually. It encodes the policy domain and the policy name that it is based on (refers to).

Example: ExtremePolicyId tag:

```
Cloud__DB Server
```

This tag is used by ExtremeConnect to identify the correct security group to be applied to a virtual machine.

This visualization shows an example of a managed security group and how its name and tag is built based on the corresponding Extreme Management Center policy name.

Extreme End System Groups

Each managed Extreme end system group's name will use this syntax:

```
extremePolicyDomain----extremePolicy
```

Example:

```
Cloud__DB Server
```

These end system groups represent a specific policy you want to apply to a cloud-based virtual machine (which is represented by an end system in Extreme Management Center). The description field lists the accounts and resource groups that this end-system group is used for. Example:

Managed by ExtremeConnect for Azure account and resource groups: Resource groups for account name *DemoAccount: [ksembatest]*

Sites

Once enabled, this integration automatically creates the following site location:

/World/Cloud

This site node will contain all of the devices that are retrieved from any cloud provider (AWS, Azure, and GCP). Beneath the main node, the node that will hold all Azure related devices is created automatically:

/World/Cloud/Azure

The following image shows what the user interface looks like when all three cloud integrations are enabled:

Assign Devices

When the user clicks on the /World/Cloud/Azure list item the list of all retrieved Azure regions will be displayed as subsites and the list of all devices are filtered automatically for those coming from Azure. Each device shows the site it belongs to:

Assign End Systems

Since end systems are assigned to switches and switches belong to sites, an end system is assigned automatically to the corresponding site (the Azure region they run in).

Topology - Devices (Switches)

ExtremeConnect will create one device (switch) in Extreme Management Center for each subnet found in Azure (from all configured accounts and resource groups). ExtremeConnect then creates one switch port for each virtual machine interface that is connected to an Azure subnet. Those switches and ports are then be used to virtually connect the end systems (virtual machines) and thus provide a sense of location for each Azure virtual machine.

Creating Devices

The following image shows a section of Extreme Management Center devices that have been created based on Azure subnets and some of the corresponding Azure subnets.

Before trying to create switches, ExtremeConnect pulls the current list of switches from Extreme Management Center and tries to parse data from the nickname, serial number, location, and contact fields. The data that is encoded here is the:

- **Name:** Name of the subnet
- **Site:** The Extreme Management Center site location of the device (region of the subnet)
- **IP Address:** Automatically generated IP; this is **not** the real IP of the subnet
- **Device Type:** Always shows Azure subnet
- **Family:** Always shows cloud service platform
- **Location:** Region that the subnet runs in
- **Contact:** User configured name of the Azure account which holds this subnet
- **User Data 1:** Always shows cp=azure (a reference that this device originates from Azure)
- **User Data 2:** Azure network ID
- **User Data 3:** Azure subnet name
- **Network OS:** Always shows ExtremeConnect

Caution

These fields should never be modified manually.

After creating the switch, ExtremeConnect creates a switch port for each virtual machine interface that will connect to this subnet.

ExtremeConnect encodes data in the following switch port fields:

- **Name:** Virtual machine interface ID (shortened form)
- **Description:** Instance name

Caution

These fields should never be modified manually.

Automatically Generate Switch IP

The IP addresses are automatically generated based off the fixed IP net 10.252.0.0. Therefore, the first switch that gets created will have the IP address 10.252.0.1, the second will have 10.252.0.2, and so on.

Removing and Resynchronizing Extreme Management Center Devices

If a subnet in Azure gets deleted, the corresponding Extreme Management Center switch will be deleted as well.

For example, if an Extreme Management Center device gets deleted by accident and it corresponds to an Azure subnet that still exists, ExtremeConnect will re-create this switch.

Updating Extreme Management Center Switch Ports

If a new virtual machine interface is connected to a subnet in Azure, the corresponding Extreme Management Center switch will get a new switch port. But if an existing virtual machine interface is removed from a subnet in Azure, the corresponding switch port in Extreme Management Center is not removed. This feature requires a minimum Extreme Management Center version of 8.2.3.7.

Extreme Management Center End Systems

Creating End Systems

This integration will create an end system entry in Extreme Management Center for each Azure network interface.

The following table shows the attributes mapping from Azure virtual machines to Extreme Management Center end systems:

Azure Instance	Extreme Management Center End System
Azure only provides a MAC address if the corresponding VM is running. If it is shut down, then there is no MAC address reported by the API. ExtremeConnect assumes that the MAC addresses are dynamically assigned to the VM interfaces that could change when a VM restarts. Therefore, ExtremeConnect does not rely on the MAC addresses reported by Azure; instead, ExtremeConnect automatically generates MAC addresses that are private address spaces.	MAC address
Taken from the network interface's *primaryIPConfiguration* attribute: • Uses public IP if it is provided • Otherwise, uses private IP	IP address

Azure Instance	Extreme Management Center End System
Virtual Machine Name	Hostname
Storage Profile > OS Disk > OS Type	Device family
Power State	State: • RUNNING = ACCEPT • Everything else = DISCONNECTED
Subnet	Switch IP - The Extreme Management Center device IP is automatically generated based on the CIDR of the corresponding Azure subnet
Instance interface	Connected Switch Port - Also shows the region and the vNet
Security group attached to network interface	Authorization

All end systems are shown in Extreme Management Center as they are discovered through automatic tracking. By assigning end systems to the corresponding switches, they are assigned to the corresponding site also.

Updating End Systems

The ExtremeConnect module only updates an end system in Extreme Management Center if any of the properties change:

- IP address (network interface IP; preferred: public IP)
- Hostname (VM name)
- Switch IP (if the feature to synchronize Azure subnets to Extreme Management Center devices is enabled)
- Switch port
- State
- Authorization

In case any one of these tests show that an update is required, the ExtremeConnect module will execute the API call to Extreme Management Center containing the updated end system data.

Automatically Generate End System MAC Address

The Azure API only provides a MAC address for interfaces of virtual machines that are currently running. If you shut down a VM and retrieve data on its interfaces, no MAC addresses will be provided. When you restart that VM, the MAC addresses are provided again and, at least in our testing, they are the same as before the shutdown. However, there must be a reason why Azure does not provide MAC address information on shutdown VMs and it is possible that Azure is using a process similar to dynamic DHCP to assign MACs to interfaces at the time a VM is started. Therefore, the MAC address potentially can be different after a VM restarts. That is why ExtremeConnect ignores the MAC addresses provided by Azure and instead automatically generates one for each VM interface.

The process is as follows:

- All generated MAC addresses start with the private range 06:00:00:
- The second part (last 3 bytes) is calculated based on an auto-incremented integer:
    - Take the last integer used for generating a MAC address (starts at 0) and convert it to a hex value
    - Depending on the length of the generated hex value, fill up the hex value with the required zeros and colons. Example: if the integer used to generate the hex is 10, the hex will be “a” and the final MAC address will be: "06:00:00:00:00:0a"
    - Store the network interface fingerprint and the generated MAC address in a cache so that different MAC addresses are not being generating for the same fingerprint (they must be mapped one-to-one)

Updating Custom Field

The ExtremeConnect module updates two custom fields for each end system and VM network interface imported from Azure:

- One custom field contains general data about the corresponding VM. The content and syntax of this custom field can be modified through a configuration option but modifying it will most likely make the reports unavailable. The following data and variables are available:

- Available variables from a virtual machine (to which the interface belongs): *VMId*, *VMState*, *VMType*, *region*, *VMName*, *tags*
- Available variables from the virtual machine interface: *mac*, *interfaceId*, *interfaceStatus*, *networkId*, *networkName*, *subnetName*, *publicIpAddress*, *publicDnsName*, *privateIpAddress*, *privateDnsName*, *ipAddress*, *securityGroup*

  The default configuration for this parameter is:
  `iName=#`*`VMName`*`#;iStatus=#`*`VMState`*`#;nwIfNetwork=#`*`networkName`*`#;nwIfSubnet=#`*`subnetName`*`#;iZone=#`*`region`*`#;nwIfIp=#`*`ipAddress`*`#;iType=#`*`VMType`*`#`

- Another custom field contains data that is used to identify an Azure virtual machine, its interface, and the account name to which it belongs. **Important:** Do not manually modify the content of this custom field.

  Example content:

  ```
  cp=azure;iId=23ebd51b-779a-4a6e-ac42-47ede3e61f33/USEAZ-RG/EXTR-PKI-P-7;nwIfId=23ebd51b-779a-4a6e-ac42-47ede3e61f33/USEAZ-RG/extr-pki-p-7528;accName=ExtremeOfficial
  ```

That data can be used to search and filter for end systems.

Removing End Systems

This section describes the mechanisms available to handle end systems that have been removed, deleted, or aged from Azure and therefore do not appear in the result list retrieved via the Azure API.

The following actions can be performed (all configurable):

- **Move deleted end systems to a deletion group:** Administrators can configure a deletion group on the ExtremeConnect module. Once an already synchronized VM has been deleted from Azure, its corresponding MAC address will be deleted from any end system group in EAC and added to this end system group. You can use this group to track which end systems are now considered outdated according to Azure.

- **Delete end systems from Extreme Management Center:** Delete the end system using its MAC. This does not remove any group memberships, but it will delete the end system from Extreme Management Center.

Extreme Management Center End System Groups

ExtremeConnect uses Extreme Management Center end system groups (MAC-based) for two purposes:

- As a catch-all group that can be configured to put all VM MACs in a single end system group for awareness. Use this group to simplify searches, grouping, and filtering
- For each managed policy (from all managed domains), ExtremeConnect creates an end system group. When an end system MAC address gets added to such an end system group, the corresponding Azure VM interface gets assigned to the corresponding security group. Pushing Extreme Management Center end systems to groups enforces security groups in Azure.

This ExtremeConnect module can use the same internal interface to Extreme Management Center to add all MAC addresses that have been automatically generated based on virtual machine interfaces imported from Azure to a configurable end system group.

If those end systems get added to MAC groups that are not managed by Extreme Management Center, no change to the corresponding virtual machines' security group assignment will be performed.

Since Azure only allows the assignment of a single Network Security Group to a VM interface, an end system is not assigned to multiple groups in Extreme Management Center.

If you add an end system to managed group, the corresponding Security Group will overwrite whatever Security Group has been assigned to the VM interface.

Configuration

Make sure you meet the prerequisites, including the installation of Extreme Management Center, before proceeding with configuration.

Azure API Access

To retrieve any data from this API, the following parameters are required:

- Application ID
- Tenant ID
- Application key
- Subscription ID

You must create an Azure Active Directory Application of the type Web App / API, which will provide authentication and authorization for ExtremeConnect. Follow these Microsoft Azure instructions to create this application and retrieve the required authentication parameters from this new account:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-create-service-principal-portal#create-an-azure-active-directory-application

Configure Connect

The best practice for configuration is to do so from the Extreme Management Center **Connect** tab on the web user interface. (There is also configuration file that most customers will not use. On an Extreme Management Center v8.1 server it is located at: /usr/local/Extreme_Networks/NetSight/wildfly/standalone/configuration/connect /AzureHandler.xml)

Azure Account-Specific Configuration

The **Services** tab on the Microsoft Azure Connect module configuration page lets you configure Azure account-specific information, as follows:

Service-Specific Configuration	Description
Account Name	A freely configurable field that specifies which virtual machines belong to which account. It is not part of the Azure API authorization.ble name for each Azure account that you want to synchronize to.
Application ID	The active directory application client ID. Also known as Application ID that identifies the application that is using the token.
Tenant (domain) ID	The domain or tenant ID containing this application.
Application Key	The authentication key for the application.
Subscription ID	The Azure subscription ID.

Service-Specific Configuration	Description
Managed Policy Domains and corresponding Resource Groups	A list of managed policy domains and their corresponding managed Azure resource groups. Only policy domains configured here will be used to export policies to Azure. One policy domain can be mapped to one or more resource groups. No resource group can be assigned to more than one policy domain. The managed domains and resource groups must be given in the following format: domainName:resGroupName1\,resGroupName2;domainName2:resGroupName3\,resGroupName4

General Configuration

The **Configuration** (second) tab on the Microsoft Azure Connect module configuration page provides more options. Most of them are similar to all other modules and are explained elsewhere in this document. Some important options are:

General Configuration	Description
Custom filed to use for identification data	The number of the custom data field for each end system to store the identification data to. This data is used to identify the corresponding Azure virtual machine, network interface, and account name. It also encodes the type of cloud provider used to pull this data from (in this case, Azure). This value must not be the same as the configured value for *Custom field to use*.
Sync Policies with Azure Security Groups	When this is set to *true*, synchronizes (exports) the policies from a domain on an enforce to Azure security groups.
Sync Policies with XMC end-system groups	When this is set to *true*, synchronizes (exports) the policies from a domain on an enforce to Azure security groups.
Assign Azure security groups based on XMC end-system groups	When this is set to *true*, assigns network interfaces to Azure security groups based on the end system group that the corresponding end system is assigned to in Extreme Management Center/EAC. The mapping between the network interface and Extreme Management Center end system is based on the MAC address. An Azure NIC can only be assigned to a single security group.
Overwrite XMC end-systems' Device Family with virtual machine type	If enabled, uses the virtual machine type from Azure to overwrite the device family field for imported end systems in Extreme Management Center.

General Configuration	Description
Create switches in XMC for Azure Subnetworks	If enabled, imports all subnets from Azure and tries to create one managed device (switch) per subnet in Extreme Management Center.
Delete end-systems from XMC that have been deleted from Azure	If enabled, deletes the corresponding end system from Extreme Management Center if an Azure virtual machine has been deleted. **Note:** This actually deletes the end system entry from NAC's end system list, not just the MAC address from any group.
End-system group for deleted Azure virtual machines	If a virtual machine or any of its network interfaces get deleted in Azure, their corresponding end systems will be pushed to this end system group.
Remove end-systems from other groups on decommission	Enable this to remove a device from all other groups when it is moved to the Decommission group.
Regularly auto-enforce policies to Azure	When enabled, ExtremeConnect automatically verifies whether the managed policy domains are correctly synchronized to the configured resource groups. This helps to ensure that your policy configuration is kept consistent with your security groups in Azure, even if someone manually changes those managed security groups in Azure.
Regularly auto-enforce	When enabled, ExtremeConnect automatically verifies whether the managed policy domains are correctly synchronized to the configured resource groups. This will ensure that your policy configuration is kept consistent with your security groups within Azure, even if someone manually changes those managed security groups in Azure.
Enable DEBUG logging for Azure Rest Client	When enabled, ExtremeConnect sets the REST client (that it uses to communicate with the Azure cloud) to log in DEBUG mode (BODY_AND_HEADERS). This allows it to get more details on potential issues regarding the functionality with the cloud API. Do not enable this unless you are experienced at administration because it will generate extensive DEBUG messages in the server.log and can fill up the disk quickly.

Alarm and Event Messages

This section lists all customer visible event messages on the Extreme Management Center **Alarms & Events** tab. This ExtremeConnect module does not generate any alarms, only events. If you want to elevate some of those events to alarms and trigger additional actions, use the Alarm Configuration feature in Extreme Management Center.

Policy Verification

There are four types of events generated when ExtremeConnect verifies policy domains with Azure security groups and Extreme Management Center end system groups.

Started Policy Verification with Azure

This event is triggered when the verification process has started. This can occur manually through a *domain verify* or *domain enforce* (the verification is done automatically prior to enforcing) or automatically on each module poll cycle (when the feature *Regularly auto-enforce policies to Azure* is enabled).

Started Policy Verification with Extreme Management Center End System Groups

This event is triggered when the verification process has started. This can occur manually through a *domain verify* or *domain enforce* (the verification is done automatically prior to enforcing) or automatically on each module poll cycle (when the feature *Regularly auto-enforce policies to XMC End-System Groups* is enabled).

Finished Policy Verification with Azure

This event is triggered when the verification process is finished. It shows the results of the verification.

Example 1: No change is required.

Example 2: A new policy has been created on Extreme Management Center but has not yet been synchronized to Azure. This policy is missing in the configured managed Azure resource group.

Finished Policy Verification with Extreme Management Center End System Groups

This event is triggered when the verification process is finished. It shows the results of the verification.

Example 1: No change is required.

Example 2: A new policy has been created on Extreme Management Center but has not yet been synchronized to an Extreme Management Center end system group.

Policy Enforcement

There are four types of events generated when ExtremeConnect enforces policy domains with Azure security groups and Extreme Management Center end system groups.

Started Policy Enforcement with Azure

This event is triggered when the enforcement process has started. This can occur manually through a *domain enforce* or automatically on each module poll cycle (when the feature *Regularly auto-enforce policies to Azure* is enabled).

Started Policy Enforcement with Extreme Management Center End System Groups

This event is triggered when the enforcement process has started. This can occur manually through a *domain enforce* or automatically on each module poll cycle (when the feature *Regularly auto-enforce policies to XMC End-System Groups* is enabled).

Finished Policy Enforcement with Azure

This event is triggered when the enforcement process is finished. It shows the results of the verification.

Example 1: No change is required.

Example 2: Two new policies have been created on Extreme Management Center (ExtremeConnect created 2 new security groups in Azure).

Finished Policy Enforcement with Extreme Management Center End System Groups

This event is triggered when the enforcement process is finished. It shows the results of the verification.

Example: A new policy has been created on Extreme Management Center and has been enforced to an Extreme Management Center end system group. The name of that new end system group is provided in the event text.

Security Group Assignment

Whenever an Extreme Management Center end system that corresponds to an Azure VM is assigned to or removed from a managed Extreme Management Center end system group, the corresponding VM get its assigned security groups updated (to enforce the corresponding policy). To reflect that action, the following event is logged:

Viewing Data

This section provides information on where to find the data imported from Azure in Extreme Management Center.

Viewing Device Data

The devices that are automatically created for each Azure subnet will contain the following data:

- **Name:** Name of the subnet
- **Site:** The Extreme Management Center site location of the device (region of the subnet).
- **IP Address:** An automatically generated IP address. This is **not** the real IP of that subnet
- **Device Type:** Always shows Azure-Subnet
- **Family:** Always shows Cloud Service Platform
- **Location:** The region that the subnet runs in
- **Contact:** The user configured name of the Azure account that holds this subnet
- **User Data 1:** Always shows cp=azure (a reference that this device originates from Azure)
- **User Data 2:** Azure network ID

- **User Data 3:** Azure subnet name
- **Network OS:** Always shows Connect

To filter the list of devices per region, select **Sites > *Region Name***:

Another way to filter for all devices generated based on Azure subnets is by selecting by **Device Type > Cloud Service Platform / Azure-Subnet**:

Viewing End System Data

In the two configured custom fields in the end-system table, you can see data on all end systems that are based on (imported) Azure virtual machines (from the configured accounts). In the following images, the default Custom 1 is used for general virtual machine data and Custom 2 for identifying Azure data.

You can also see the current status, IP address, site, hostname (VM name), device family (machine type), authorization (assigned security group), switch IP, switch nickname (Azure subnet), and port (region & vNet of the virtual machine interface) in the standard table columns. The Authentication Type is always set to *Auto-Tracking* to indicate the source of this data.

Cloud Reports

Introduced with Extreme Management Center v8.2, the Azure cloud report is part of the new Multi-Cloud dashboard in Extreme Management Center Network area.

Azure Stats Report

The Azure-specific Cloud Reports shows:

- Statistics
- Instance Distribution by Azure Account
- Distribution of VMs per machine type (top 10)

- Distribution of VMs per zone (top 10)
- Distribution of VM interfaces per subnets (top 10)

Instance List Report

The report shows the list of all Azure VMs with some details about each VM:

Microsoft System Center Virtual Machine Manager (SCVMM)

The SCVMM integration allows the provisioning of virtual machines to NAC end system groups based on the virtual interfaces to which each VM is connected. Data in Extreme Management Center is enriched for each end system and is reciprocally made available in SCVMM. The VMM is a central Microsoft server that enables the management of multiple Hyper-V servers from one console.

The SCVMM server requires an adapter agent to be installed and configured before enabling the corresponding module in ExtremeConnect or before Windows Remote Management (WinRM) to be configured and accessible on the SCVMM server. In the latter case, ExtremeConnect can access SCVMM remotely and get the required information. The adapter file, if needed, is provided by Extreme Networks.

Module Configuration

The following tables describe the configuration options available for the SCVMM Connect module (the configuration file: SCVMMHandler.xml).

Service Configuration	Description
agentlessMode	A boolean value that indicates whether to use the remote WinRM management protocol (when set to *true*) or the adapter (when set to *false*).
server	The name or IP of the SCVMM server that the SCVMM adapter runs on. ExtremeConnect uses this to find the web service to retrieve SCVMM computer data.
serverPort	The TCP port on which the adapter or the WinRM service is running. You must configure the same port in the adapter's configuration file.
userDomain	The Windows domain to which the SCVMM user belongs. This value is used when agentlessMode is set to *true*.

Service Configuration	Description
userName	The SCVMM username for authentication. This username is used when agentlessMode is set to *true*.
password	The SCVMM user password for authentication. If agentlessMode is set to *false*, this value is the same as the pre-shared key that is configured in the adapter's configuration file.

Service-Specific Configuration	Description
Poll interval in seconds	The sleep time in between two synchronizations. On each synchronization, the SCVMM Connect module queries the SCVMM VM and host list from the adapter and processes it internally. Usually, it is not necessary to have the SCVMM Connect module query the SCVMM adapter for new data every few seconds because that data is not changed regularly, and each synchronization puts an extra load on both the SCVMM server and Extreme Management Center. The best practice is to set this value to a minimum of ten minutes or multiples of that (600 secs or more).
Log level	The log level for this module. Each module logs into the standard Extreme Management Center log file. The best practice is to set this to WARN or ERROR. Only use DEBUG for debugging, troubleshooting, or testing.
Enabled	Enables or disables this module.
Update local data	Always keep this set to *true*. **Important:** When set to *false*, the module will not perform the data import.
Custom field	The ExtremeControl custom field to which the SCVMM module writes its SCVMM VM and custom data. You can choose between all four available custom fields. **Important:** Ensure that you do not use the same custom field for any of the other Connect modules, otherwise they will overwrite each other continually.

Service-Specific Configuration	Description
Format of incoming VM data	Defines which parts of the imported VM data to display per NAC end system and how it is formatted. When putting one of the available VM property names within two '#' signs, the Connect module automatically replaces the variable with the corresponding content. **Available Variables:** *host name*, *vlanID*, *operatingSystem*, *virtualNetwork*, *vmNetwork*, *logicalNetwork*, *status*, *mac* **Default Config:** `Name=#name#; Host=#vmHost#; vlanID=#vlanId#; Virt. NW=#virtualNetwork#; VM NW=#vmNetwork#; Logical NW=#logicalNetwork#; Status=#status#; OS=#operatingSystem#`
Format of incoming host data	Defines which parts of the imported host data to display per NAC end system and what format to display. When putting one of the available host property names within two '#' signs, the Connect module automatically replaces the variable with the corresponding content. **Available Variables:** *name*, *hyperVState*, *vlanTags*, *operatingSystem*, *virtualNetwork*, *adapterName*, *mac* **Default Config:** `Name=#name#; vlans=#vlanTags#; Virt. NW=#virtualNetwork#; Status=#hyperVState#; OS=#operatingSystem#; Adapter=#adapterName#`
Use network name as end system group	If this is set to *true*, the name of the port group or network is used as the name for the end system group. **Note:** Only the data before the first underscore will be used.
Network name to use for naming end system group	Specifies whether to use the name of a VM network, logical network or virtual network for naming the end system group. When you select *bestMatch*, the module will try to use, in successive order, *logicalNetwork*, *vmNetwork*, and *virtualNetwork*. The name will be set to *unknown* if all three variables are returned as empty values by SCVMM.
Enable PortGroup Import	Enables the automatic creation of end system groups in Extreme Management Center based on port groups.
Automatic Enforce after import	Enables the automatic enforcement of all NAC appliances if a port group was imported.
Extended PortGroup Import	If set to *true*, creates NAC configuration and policy profiles when importing the port groups.
NAC Configuration	Name of NAC configuration that any new rules are added to. **Default value:** Default
Policy Domain	Name of the policy domain that the new policy profiles are added to. **Default value:** Default Policy Domain
Forward as Tagged	Sets the policy role VLAN to be forwarded as tagged.

Service-Specific Configuration	Description
Enable PortGroup Import Removal	If enabled, this option removes the NAC configuration when deleting port groups.
Default endsystem group	Specifies the default end system group name to use if the name is not set dynamically, or the group name to use for untagged VM and Hypervisor networks. **Default:** scvmm
Egress VLAN for untagged MACs	The egress VLAN ID to use for untagged traffic. The default is *0*, which means that none will be used, and the end system group specified by **Default endsystem group** setting will be used for these MACs. If a non-zero VLAN ID is provided, then an end system group is created using this VLAN ID and the network name selected by the **Network name to use for naming end system group** and the end system is assigned to this group. **Note:** This VLAN ID is used for all untagged MACs. If you want to use different VLAN IDs for each or a few untagged MACs, you must configure the VLAN IDs manually and then set the value for this field to *0*.
Overwrite device type	When enabled, ExtremeConnect overwrites the device type for end systems (VMs and hosts) in ExtremeControl using the imported operating system from SCVMM. **Important:** This operation overwrites any device type that is retrieved using standard ExtremeControl mechanisms, such as DHCP fingerprinting.

Adapter Installation

ExtremeConnect retrieves and sets data to or from a Virtual Machine Manager (VMM) server using an adapter. This adapter must be installed and configured before enabling the corresponding module within Connect. The adapter consists of a Java executable file (JAR) and a configuration file. There is no dedicated installer for the adapter. The best practice is to install the adapter manually following these steps:

1. Install the latest Java Runtime Environment, .NET framework, and Windows PowerShell 2.0 on the SCVMM server.
2. Acquire the file Datacenter Manager SCVMM Adapter.zip from GTAC or by contacting your local Extreme representative.
3. Copy the executable JAR file (DCM_SCVMM_ADAPTER_<version>.jar) and the configuration file (DCM_SCVMM_ADAPTER.config) into a separate directory created under **Program Files/Extreme Networks/SCVMM Adapter** directly on the SCVMM server.

4. Edit the configuration file according to your environment. The configuration file contains an explanation of all of the settings, and you can find them listed below.
5. Save and close the configuration file.
6. Start the adapter manually:
    a. Open a CMD shell or PowerShell.
    b. Navigate to the installation directory.
    c. Use the following command: `java -jar DCM_SCVMM_ADAPTER_<version>.jar`.
7. Check the log file to validate proper functionality.
8. In OneView or NAC manager, check the custom column in the end system list to see data for the SCVMM virtual machines. (You previously configured the custom column in the SCVMMHandler.xml configuration file.)
9. Verify that the DCM_ SCVMM _ADAPTER_<version>.jar file is starting automatically (during the Windows server startup) by following these steps:
    a. From the CMD or PowerShell window, stop the adapter that is currently running.
    b. Configure the auto-start for the JAR file (this depends on your Windows Server version).
    c. Restart your SCVMM server to test the auto-start of the JAR file. You should see a Java process running in the process tree.

Adapter Configuration

The following table lists the configuration options for the SCVMM agent.

Configuration Option	Description
LOG_LEVEL	Set the log level of the adapter to one of the following values: ERROR, WARN or DEBUG. **Default:** WARN
IP	IP address for the web service (=agent) to listen on.
PORT	TCP port for the web service to listen on. **Important:** This port must not be used by any other application on this server.

Configuration Option	Description
SCVMM_DLL	Location (path and filename) of Microsoft.SystemCenter.VirtualMachineManager.dll Example: C:\Program Files\Microsoft System Center Virtual Machine Manager 2008 R2\bin\Microsoft.SystemCenter.VirtualMachineManager.dll
PRE_SHARED_KEY	The pre-shared key used for the communication between the adapter and ExtremeConnect. This key must match the key entered when installing the SCVMM Connect module.
IS_PRE_SHARED_KEY_ ENCRYPTED	If this is set to *false*, the adapter assumes that the pre-shared key configured previously is not encrypted. Consequently, on the first start, the adapter will automatically encrypt the key and set this field's value to *true*. To change this key at a later stage, change the pre-shared key, then set this field's value back to *false* and restart the adapter service.
SCVMM_SERVER	The DNS name of the Virtual Machine Manager server to connect to. This has only been tested with this adapter and the VMM server running on the same server, although remote connections might work as well.

WinRM Configuration (adapter-less)

Use the command line to run this configuration:

1. Check whether WinRM is enabled on the SCVMM server by executing the following command and enabling it, if not already enabled:

   ```
   winrm quickconf
   ```

2. Dump the winrm service configuration and ensure that the highlighted values are set correctly.

   ```
   winrm get winrm/config/service
   ```

   Also, ensure that the HTTP port matches what is displayed in the following output and the ExtremeConnect service's configuration.

   The highlighted values shown in the following figure are set as follows:

   ```
   AllowUnencrypted=true
   HTTP=5985
   AllowRemoteAccess=true
   ```

Verification

From the SCVMM management console, add the **Description** field column to the overview list of all VMs. You should see network related information retrieved from Extreme Management Center/NAC in this column, and data from SCVMM in the end system list in OneView or NAC Manager.

Microsoft Hyper-V

The Hyper-V integration allows the provisioning of virtual machines to NAC end system groups based on the virtual interfaces to which each VM is connected. The data in the Extreme Management Center engine is enriched for each end system and is reciprocally made available in Hyper-V. When integrating with multiple Hyper-V servers, you can do *one* of the following options:

- Add each of those servers as a new entry in this module's configuration (a list of services or agents to connect to)
- Use the integration with System Center Virtual Machine Manager (SCVMM)

NOTE: The Hyper-V server requires an adapter agent to be installed and configured before enabling the corresponding module in ExtremeConnect. The adapter file is provided by Extreme Networks.

Module Configuration

The following tables describe the configuration options available for the Hyper-V Connect module (the configuration file is: HyperVHandler.xml).

Service Configuration	Description
Adapter IP	IP Address of the Hyper-V adapter.
Adapter Port	Port on which the Hyper-V adapter is listening.
Pre-Shared Key	The pre-shared key used to communicate with the Hyper-V adapter.

General Module Configuration	Description
Poll Interval in seconds	Number of seconds between connections to the adapter running on the Hyper-V server.
Module log level	Verbosity of the module. Logs are stored in the ExtremeControl engine server.log file.
Module Enabled	Whether the module is enabled.
Push update to remote service	If this is set to *true*, the data from other modules is pushed to the service.
Update local data from remote service	If this is set to *true*, the data from the remote service is used to update the internal end system table.
Default end system group	The default end system group name to use if it is not set dynamically.
Enable Data Persistence	Enabling this option forces the module to store end system data, end system group data, and VLAN data to a file after each cycle. If this option is disabled, the module forgets all of the data after a service restarts. However, to clean the existing data, the corresponding .dat files must be deleted.

Service-Specific Configuration	Description
Custom field to use	The custom field in ExtremeControl engine used to update the information for end systems retrieved from the adapter running on the Hyper-V server. **Valid values:** 1-4
Outgoing data format	The format of the ExtremeControl engine data (such as last seen time, switch IP, switch port) that is written to the description fields of the VMs in the Hyper-V management console. You can customize the appearance and what information you want to include or exclude.
Format of the incoming data	The format of the data that is received from the adapter running on the Hyper-V server, and the format that is written to the custom field.
Use network name as end system group	If this is set to *true*, the name of the port group or network is used as the name for the end system group (**Note:** Only the data before the first underscore (_) will be used.

Adapter Installation

ExtremeConnect retrieves and sets data from and to a Hyper-V server using an adapter. This adapter must be installed and configured before enabling the corresponding module in ExtremeConnect. The adapter consists of a Java executable file (JAR) and a

configuration file, and requires a PowerShell module for configuration. There is no dedicated installer for the adapter. The best practice is to install the adapter manually, as follows:

1. Download a PowerShell module from this location: http://pshyperv.codeplex.com/releases/view/62842#DownloadId=219013
2. Follow the instructions to install the PowerShell module from here: http://pshyperv.codeplex.com/releases/view/38769#DownloadId=101935, or follow these steps:
    a. Right-click on the zip file. Select **UNBLOCK**.
    b. Copy the zip file to the following location: C:\Windows\System32\WindowsPowerShell\v1.0\Modules
    c. Unzip and install the HyperV module using the “install.cmd” file.
    d. Open the PowerShell, and enter `Set-ExecutionPolicy Unrestricted`
    e. Run the command `Import-Module HyperV` and make sure that no errors occur. If this operation does not load the module, you can insert the folder **<*folderwhereyouunzippedthedownloadedfile*>\Hyper-V** in your PATH environment variable so that Windows knows from where to load the module.
    f. As a final test, run `get-command -module HyperV`. Check whether this operation prints the available Hyper-V commands.
3. Install the latest Java Runtime Environment (JRE).
4. Create a dedicated folder (for example, C:\Program Files\Extreme Networks\HyperV Adapter). Copy the two files (DCM_HYPERV_ADAPTER_<version>.jar and DCM_HYPERV_ADAPTER.config) to the dedicated folder.
5. Edit the configuration file DCM_HYPERV_ADAPTER.config according to your environment.
6. Start the adapter by double-clicking the file DCM_HYPERV_ADAPTER.jar or running it within a shell using `java -jar DCM_HYPERV_ADAPTER.jar`.
7. Verify that the log file was created in the same folder where the JAR file is located. The adapter automatically starts when the Windows Server starts.
8. Repeat these steps on all of the Hyper-V servers that you want to integrate with Extreme Management Center.

Adapter Configuration

The following table lists the configuration options for the Hyper-V agent.

Configuration Option	Description
LOG_LEVEL	Set the log level of the adapter to one of the following values: ERROR, WARN or DEBUG. **Default:** WARN.
IP	IP address for the web service (=agent) to listen on.
PORT	TCP port for the web service to listen on. **Important:** This port must not be used by any other application on this server.
PRE_ SHARED_ KEY	The pre-shared key used for the communication between the adapter and ExtremeConnect. This key must match the key that was entered when you installed the Hyper-V Connect module.
IS_PRE_ SHARED_ KEY_ ENCRYPTED	If this is set to *false*, the adapter assumes that the pre-shared key configured previously is not encrypted. Consequently, on the first start, the adapter will automatically encrypt the key and set this field's value to *true*. If you want to change this key later on, change the pre-shared key, set this field's value back to *false*, and restart the adapter service.

Verification

From the Hyper-V management console, select a virtual machine. You should see the corresponding data from Extreme Management Center in the **Notes** field on the bottom of the page.

VMware vSphere

The VMware vSphere integration allows the provisioning of virtual machines in the network, and the automation of creating virtual networks based on end system access groups. Additionally, the data in Extreme Management Center is enriched for each end system and is reciprocally made available in vSphere.

Module Configuration

Configuration Option	Description
Username	Username used to connect to the vSphere web service. Read/Write/Execute permissions are required.
Password	Password used to connect to the vSphere web service.
VMware Webservice URL	Web service URL of the VMware vSphere server.
Module enabled	Enables and disables the module.

Service-Specific Configuration	Description
Outgoing data format	The format of the ExtremeControl data (such as last seen time, switch IP, switch port) that is written to the description fields of the VMs within VMware or Xen. You can customize the appearance and what information you want to include or exclude. **Note:** The VMware vSphere client the annotation field is limited in size. The default outgoing format is very close to the maximum string length allowed for this field. If you want to add information to this field, consider including it with some of the existing default value.
Format of the incoming data	The format of the data that is coming from VMware or Xen, and that is written to the custom field.
Create Private VLAN Entries	If this is set to *false*, Data Center Manager does not automatically create any PVLAN entries on dvSwitches, even if you configured any. By default, this feature is disabled, and you must enable it manually if it is needed.
Create Portgroups from end system Groups	If this is set to *true*, Data Center Manager automatically creates new port groups in VMware based on the ExtremeControl engine NAC end system groups and the other configuration.
Update Portgroup VLAN IDs	This setting is useful only if the **Create Portgroups from end system groups** setting is set to *true*. Additionally, if you change the *vlan=XXXX* value in an end system group, this setting automatically changes your port group VLAN IDs accordingly.
Use Global end system Groups	If this is set to *true*, the VMware module will have access to the global end system groups that are provided by the ExtremeControl module within the main module. This is necessary if you want to create port groups automatically based on the ExtremeControl NAC end system groups.
Enable Custom Attributes	Enables or disables the creation of and updates to Custom Attributes for vCenter Servers.
Custom Attributes Data Format	Allows the configuration of Custom Attributes for vCenter Servers. ExtremeConnect creates and updates these attributes for each VM, and allows for searching and sorting of this data in vCenter. Each attribute must be configured on a single line and must follow the format: *NAME=VALUE*. *NAME* is the name of the Custom Attribute. *VALUE* is a free text value that can utilize all of the variables that are available in the **Outgoing data format** option. If a VM uses more than one network interface, the data for each variable is presented as NIC1DATA/NIC2DATA/...

Service-Specific Configuration	Description
Deletion Group	Name of the port group that a VM will be redirected to if its current end system group is deleted.
Port Group Import	Enables the automatic creation of end system groups in ExtremeControl based on port groups. The port group name is used for the end system group. **Note:** The delimiter also applies here. In the default configuration, the text after the last delimiter is truncated from the name. For example, *MyPortGroup_VLAN1_dvSwitch0* will be imported as *MyPortGroup_VLAN*1 in ExtremeControl. The VLAN IDs are updated if they change.
Automatic Enforce after import	Enables the automatic enforcement of all appliances and the policy domain (only for extended import) if a port group is imported.
Extended PortGroup Import	Creates NAC configuration and policy profiles during PortGroup Import. This also requires that you define the options for NAC Configuration, Policy Domain, and Forward as Tagged. **Note**: The truncated port group name is also used as the VLAN name and must adhere to naming limitations. In a special case, a VNI can be supplied by prefixing *VNI-#####-* (with ##### being the VNI ID) to the port group name. For example, VNI-1234-PortGroup will create a policy or control configuration with the VLAN ID set in the port group and the VLAN name specified as VNI-1234-PortGroup. An EXOS switch can then use the VNI-1234 part to set up the VxLAN mapping for that VLAN.
Add VNI to Policy Map	Adds the VNI ID from the port group name to one of the custom fields in the policy mapping configuration in ExtremeControl. This can be used to supply the VNI to a target switch using RADIUS to create a dynamic VxLAN configuration.
Enable PortGroup Import Removal	Delete the NAC configuration or end system group if the port group is deleted.
Hypervisor Import	Creates a device in Extreme Management Center network for each Hypervisor, using the pNIC, vNIC, and dvSwitch port groups to generate the device ports. LLDP data will be used, if present, to indicate neighbors on ports.
Enable Import of Management Macs	When this option is enabled, the management MAC addresses (such as the MAC addresses used for vMotion) will also be imported. These management MAC addresses should display in the end system groups corresponding to the port group they are in.
EndSystem Events	Updates the ExtremeControl end system table if RADIUS or Kerberos authentication is not available. Events will use the Hypervisor device as the connecting switch instead of the physical LAN switch that is provided through RADIUS.

Service-Specific Configuration	Description
Which Data Centers to Include or Exclude	This option can be used to limit the data being pulled to one or more data centers. If nothing is specified, data is pulled from of all the data centers. Multiple data centers can be specified by delimiting them with a semicolon. For example, the filter string `dc1;dc4` will limit data to data centers dc1 and dc4 only. The data center to exclude can be specified by prefixing it with an exclamation mark. For example, the filter string `!dc2` will pull data from all of the data centers except dc2.

Stop and restart the Extreme Management Center services (see the ExtremeConnect Installation section for instructions).

Verification

To verify the integration, follow these steps:

1. From the vSphere Client, select a virtual machine.
2. From the right pane, select the **Summary** tab. At the bottom of the tab, in the **Annotations** field, there should be corresponding data from Extreme Management Center (for example, information about the switch port and the switch IP to which this VM is physically connected).

VMware View

The integration of VMware View does not require any special tool or software to implement. The virtual desktops must be configured to use 802.1x, and for authentication purposes, users must log on to the View Client to access those desktops using PCoIP. Any Extreme switch with a reasonable amount of multi-user authentication capacity is suitable to authenticate each virtual desktop individually, and apply a policy based on the user name.

Additionally, if user authentication with 802.1x is not available, standard ExtremeConnect operations can be used to provision a NAC rule for the connected port group of each VM.

For more information regarding the setup procedure, see the VMware View VDI documentation.

Related Information

For information on related tabs:

ExtremeConnect Overview

Security Configuration

Check Point Identity Awareness

The Check Point Identity Awareness (Check Point) integration updates the Check Point gateway with the username IP mapping of end systems that connect to the ExtremeControl engines.

Module Configuration

The following table describes the configuration attributes:

Module Configuration	Description
Server	Check Point IP address.
Password	Check Point shared secret.
Ignore usernames that contain	Ignores usernames that contain the entered value. Semicolon delimited.
Ignore ExtremeControl profiles	Ignores end systems that are assigned an ExtremeControl profile. Semicolon delimited.
Session timeout	Number of hours before an API user mapping session times out.

The Check Point shared secret can be found in the Identity Web API settings:

Sample server log output:

2017-02-16 12:32:41,937 DEBUG [com.enterasys.fusion.modules.CheckPointHandler]
Sending -> https://10.224.1.252/_IA_MU_Agent/idasdk/add-identity post
{"shared-secret":"mysharedsecret","requests":[{"ip-address":"192.168.10.181","user":"doe,
john","session-timeout":3600}]}
2017-02-16 12:32:42,278 DEBUG [com.enterasys.fusion.modules.CheckPointHandler]
Response -> {
"responses" : [
{
"ipv4-address" : "192.168.10.181",
"message" : "Association sent to PDP."
}
]
}

Distributed IPS

The distributed IPS solution monitors log files for events, or opens a port on the Extreme Management server and listens for events. After an event is received, action can be taken to add the threat to an end system group or to notify Automated Security Manager (ASM) to perform a custom action.

Module Configuration

The following table describes the configuration attributes:

Configuration Option	Description
Name	Event name, which is the default threat name used in the end system group description.
Regex	Event regular expression string.
File	File, with full path, to monitor for events.
Port	Port number to open and listen for events on. Opening a port can increase vulnerability on the Extreme Management Center server.
Protocol	Port number protocol.
Sender filter	Used to process events only from specific IP addresses to prevent spoofing. This field is used in conjunction with the port and protocol.
End system group	End system group to which the threat is added.

Configuration Option	Description
End system group type	End system group type, MAC address, or IP address.
Client URL	Execute a client URL call. Supported arguments are: *-X* method name (such as GET, POST) *-u* username:password *-d* data/message *-H* header:value
MAC address regular expression	MAC address regular expression. The best practice is to avoid changing this value.
IP address regular expression	IP address regular expression. The best practice is to avoid changing this value.
Threat name regular expression	Threat name regular expression. The default regular expression matches a group of words surrounded by double quotes or a group of words without spaces. Example formats that will match the regular expression: “This is a threat 123” This_is_a_threat_123 This-is-a-threat-123 ThisIsAThreat123 This_is_a_Threat(123)

The most secure protocol for the events is HTTPS GET or POST. The events are sent to the Extreme Management Center server with basic authentication. The URL that is used for the HTTPS option is https://*ExtremeManagement:port*/connect/LogForwarding (for example, https://192.168.30.34:8443/connect/LogForwarding).

The regular expression string can be complicated. The best practice is to find keywords in the event and use those keywords as unique identifiers.

The event must contain either the MAC or IP address of the threat. When a MAC address-based end system group is used and the threat MAC address is not in the event, a lookup operation is performed to resolve the threat’s IP address, and vice-versa for an IP based end system group.

Common wildcards that will be used are:

\w = match a character

\d = match a number

\s = match a space

. = match any character

* = match 0 or more

+ = match 1 or more

Examples of Event Messages and Regular Expressions:

Example 1. Checkpoint event message

loc=4220 filename=fw.log fileid=1402093147 time= 6Jun2014 16:01:57 action=block orig=r77 i/f_dir=outbound i/f_name=eth1 has_accounting=0 product=Anti Malware web_client_type=Chrome resource=http://sc1.checkpoint.com/za/images/threatwiki/pages/TestAntiBotBlade.html src=Winsvr2012 s_port=49600 dst=23.203.225.174 service=http proto=tcp session_id=<53924865,00000002,b17361d1,c0000001> Protection name="Check Point - Testing Bot" malware_family=Check Point Confidence Level=5 severity=2 malware_action=Communication with C&C site rule_uid={AE831485-A9C8-4681-BE8F-0E2E66904BDB} Protection Type=URL reputation malware_rule_id={27CC0EC6-7CBE-F54E-AFE0-F46162CEB057} protection_id=00233CFEE refid=0 log_id=9999 proxy_src_ip=Winsvr2012 scope=Winsvr2012 __policy_id_tag=product=VPN-1 & FireWall-1[db_tag={8119E2B3-79E5-4747-80E6-6756E42EE86D};mgmt=r77;date=1402094422;policy_name=Standard] origin_sic_name=cn=cp_mgmt,o=r77..pcfxuu Suppressed logs=1 sent_bytes=0 received_bytes=0 packet_capture_unique_id=192.168.10.189_maildir_sent_new_time1402095718.mail-4230074710-508316721.localhost packet_capture_time=1402095718 packet_capture_name=src-192.168.10.189.eml UserCheck_incident_uid=80E6C145-7AB6-D2C5-1DC5-A500F1473A70 UserCheck=1 portal_message= Your computer is trying to access a malicious server. It is probably infected by malware. For more information and remediation, please contact your help desk. Click here to report an incorrect classification. Activity: Communication with C&C site URL: http://sc1.checkpoint.com/za/images/threatwiki/pages/TestAntiBotBlade.html Reference: F1473A70 UserCheck_Confirmation_Level=Application frequency=1 days

In this example, *Check Point - Testing Bot"* is the threat name and *192.168.10.189* is the threat IP address.

Regular expression:

Protection name=$threatName malware_family.* packet_capture_name=src-$threatIpAddress

The regular expression contains unique identifiers to avoid ambiguity or incorrect matches. *Protection name=* precedes the threat name and *malware_family* follows the

threat name. A wildcard (.*) is used to match against multiple characters after *malware_family*.

Simulating an event with this message generates the following log message in the Extreme Management Center server:

Regular expression match -> {$threatIpAddress=192.168.10.189, $threatName="Check Point - Testing Bot"}

Example 2. Watchguard event message

Jun 13 13:42:18 10.148.1.254 local1.info Jun 13 13:42:18 QA_LAB_FB 80BE052F336C0 http-proxy[1631]: msg_id="1AFF-0034" Deny 1-Trusted 0-External tcp 192.168.10.180 21.37.51.86 33444 80 msg="ProxyDrop: HTTP APT detected" proxy_act="HTTP-Client.Anti-X" host="fishherder.dyndns.org" path="/tmp/lastline-demo-sample.exe" md5="dd0af53fec2267757cd90d633acd549a" task_uuid="235ee8f1185e4337986a0a46eb370595" threat_level="high" (HTTP-Proxy-00)

In this example, *ProxyDrop: HTTP APT detected* is the threat name and *192.168.10.180* is the threat IP address.

Regular expression:

External tcp $threatIpAddress .* msg=$threatName proxy_act

Simulating an event with this message generates the following log message in the Extreme Management Center server:

Regular expression match -> {$threatIpAddress=192.168.10.180, $threatName="ProxyDrop: HTTP APT detected"}

Example 3. Palo Alto event message

Aug 25 15:51:28 PA-5060-1 -PaloAlto: -threatIpAddress 192.168.10.179 -threatName "Apache Wicket Unspecified XSS Vulnerability(36041)" –severity critical

In this example, *Apache Wicket Unspecified XSS Vulnerability(36041)* is the threat name and *192.168.10.180* is the threat IP address.

Regular expression:

PaloAlto: -threatIpAddress $threatIpAddress -threatName $threatName

Simulating an event with this message generates the following log message in the Extreme Management Center server:

Regular expression match -> {$threatIpAddress=192.168.10.179, $threatName="Apache Wicket Unspecified XSS Vulnerability(36041)"}

Fortinet FortiGate

The Fortinet FortiGate integration provides a single sign-on solution and network access to end systems with the use of RADIUS accounting.

Module Configuration

The following table describes the configuration attributes:

Configuration Option	Description
Server	FortiGate IP address.
Password	FortiGate RADIUS shared secret.
SSO attribute key	RADIUS attribute key. The attribute will contain the ExtremeControl profile name. The best practice is to use `profile` (without quotes) as the key.
ExtremeControl	RADIUS accounting sent to the server that matches the ExtremeControl appliances. Semicolon delimited.
RADIUS interim message interval	Set the interval to a non-zero value to enable RADIUS interim messages and keep the session active.
Ignore usernames that contain	RADIUS accounting will not be sent for end system usernames that contain this value. Semicolon delimited.
Ignore Extreme Control profiles	RADIUS accounting will not be sent for end system profiles that match this value. Semicolon delimited.
Ignore SSIDs	RADIUS accounting will not be sent for end system SSIDs that match this value. Semicolon delimited.

Foritgate Configuration

To configure the Fortigate integration:

1. Log in to the FortiGate interface.
2. Select **System > Network > Interfaces**.
3. Enable **Listen for RADIUS Accounting Messages**.
4. Select **System > Config > Features**. Enable **Endpoint Control**.
5. Select **User & Device > Authentication > RADIUS Server**.
   a. Create a new server and add the ExtremeControl server as the RADIUS server.
   b. Enter the IP address and shared secret.
   c. Select **Include in every user group**.
6. Select **Single Sign-on**. Add an RSSO_AGENT type **RADIUS SSO**.
7. Select **Authentication > Single Sign-on** and create a new agent.
8. On the **Edit Single Sign-on Server** page in the user interface, verify that the RADIUS server is configured as follows:
9. From the CLI, configure RSSO_AGENT.
   The RADIUS attributes default values that are expected by FortiGate are listed in the following table. Modify these values to be in accordance with the attributes used by the FortiGate Handler.

RSSO Information	RADIUS Attribute	CLI Field
Endpoint identifier	Calling-Station-ID	rsso-endpoint-attribute
Endpoint block attribute	Called-Station-ID	rsso-endpoint-block-attribute
user group	Class	sso-attribute

10.
11. Configure the following attributes by entering the corresponding commands:
    FGT60C3G10019088 # `config user radius`
    FGT60C3G10019088 (radius) # `edit RSSO_Agent`
12. Configure RSSO-Endpoint-attribute to User-Name:
    FGT60C3G10019088 (RSSO_Agent) # `set rsso-endpoint-attribute User-Name`
    FGT60C3G10019088 (RSSO_Agent) # `set sso-attribute-key profile`

13. Run the get command as follows:
    FGT60C3G10019088 (RSSO_Agent) # `get`
    You should receive the following response if the attributes have been configured properly:

```
name : RSSO_Agent
h3c-compatibility : disable
rsso : enable
rsso-radius-server-port: 1813
rsso-radius-response: enable
rsso-validate-request-secret: enable
rsso-secret : *
rsso-endpoint-attribute: User-Name
rsso-endpoint-block-attribute: Called-Station-Id
sso-attribute : Class
sso-attribute-key : profile
rsso-context-timeout: 28800
rsso-log-period : 0
rsso-log-flags : protocol-error profile-missing context-
missing accounting-stop-missed accounting-event endpoint-
block radiusd-other
rsso-flush-ip-session: disable
```

14. Select **User & Device > User > User Group**. Create a user group. Set the RADIUS Attribute Value to the ExtremeControl profile.

15. Select **Policy > Policy > Policy**. Create a policy with the subtype **User Identity** and add your personal filters.

iBoss Web Security

The iBoss integration provides a single sign-on solution and web content filtering capabilities based on the end system's active directory membership and network location.

Module Configuration

The following table describes the configuration attributes:

Configuration Options	Description
Server	IP addresses of the iBoss appliances. Semicolon delimited.
Port	iBoss web service port. **Default:** 8015
Password	iBoss authentication key.
Ignore usernames that contain	HTTP messages are not sent for end system usernames that contain this value. Semicolon delimited.
Ignore ExtremeControl profiles	HTTP messages will not be sent for end system profiles that match this value. Semicolon delimited.
Ignore SSIDs	HTTP messages will not be sent for end system SSIDs that match this value. Semicolon delimited.
Remove email domain from username	Removes the email domain from the username.
Remove domain from username	Removes the Windows domain from the username.
ExtremeControl rule name delimiter	Delimiter used to separate the location from the ExtremeControl rule name. The value to the right of the delimiter is the location.

This section details the steps required to install, configure, and test the integration between Active Directory, iBoss, and ExtremeControl in a hypothetical K-12 educational environment. The process for integration in other verticals is similar.

To perform these tasks, you must have a technical understanding of the ExtremeControl solution, and the skills required to implement a typical LDAP-integrated deployment.

To integrate iBoss and ExtremeControl, perform these tasks (which are described in the sections that follow):

1. Define the required user groups in Active Directory.
2. Define the various locations that require differentiated access.
3. Configure the iBoss appliance.
4. Install and configure the ExtremeConnect integration services.
5. Configure ExtremeControl.

Define Groups in Active Directory

When considering an integration project, first determine the various user populations for which you want to define access, and then place those populations into separate AD groups. For this hypothetical K-12 environment scenario, we will define access to two distinct sets of end users: staff and students. We will create two AD groups named All

Students and All Staff. These groups contain all of the student and staff AD accounts respectively.

NOTE: Creating and managing AD groups and accounts is outside the scope of this document.

Define Locations

After determining the various end user populations, and creating and populating the AD groups, the next step is to determine what locations require differentiated access for each group. For this scenario, we will provide three different iBoss filter groups for students and two different iBoss filter groups for the staff.

The following table lists the proposed user groups and locations:

AD Group	Location
All Students	Instructional Areas
All Students	Cafeteria
All Students	Gym
All Staff	Instructional Areas
All Staff	Everywhere Else

Configure the iBoss Appliance

There are three areas to configure on the iBoss appliance to integrate with Active Directory and Extreme Management Center beyond the standard configuration needed for standard iBoss operation. This document covers the integration steps, not the basic installation of the appliance.

Part A – Configure LDAP Settings

1. Open a web browser and go to https://*IP address of appliance* to access the appliance login screen. Enter the necessary credentials and select **Login**.
2. To configure the Active Directory settings, select **Home > Network Settings > LDAP Settings**.

   The **LDAP Settings** page is divided into three panes. The top pane contains global settings for the appliance. Use the default global settings.
3. From the **LDAP Server Info** pane, define the AD domain controller that iBoss will use. Specify the LDAP parameters required for communication to that domain

controller. Select **Save**.

4. Verify that the server definition you created was added to the list in the **LDAP Servers** pane. To save the changes and complete the LDAP configuration, select **Done**.

Part B – Configure the AD Plugin

To configure the Active Directory (AD) plugin:

1. Select **Home > Network Settings > AD Plugin**.
2. Navigate to the **Registered AD Servers/NAC Agents** pane at the bottom of the page and add a description of the Extreme Management Center server and its IP address. This lets the iBoss server listen to updates sent by Extreme Management Center.
3. The default settings can be used for **Default Filtering Group** and **Use Subnet For Default Filtering Group**, unless you are told differently by Support. Select **Save** (at the top of the pane).
4. From the **Global Settings** dialog, get the security key, which is used as the password in the service settings.

Part C – Configure Filters

iBoss assigns filter groups to traffic from end systems. A filter group is a set of network controls that define what website content categories, programs, QoS settings, and more, are allowed or not allowed to pass through the engine for a given connection. Filter groups are applied to end system traffic on an individual basis.

For this scenario, we will define the individual filter groups in iBoss, but will not cover how to configure the individual network controls for each filter group definition.

To configure filters:

1. To access the **Filter Group** definition page, select **Users > Groups** from the left menu. There are five pages of definitions available for defining filter groups and each page section contains five filter group definitions, for a total of 25 available filter groups.

   Note: Filter group #1 is the default filter group and should remain unchanged.

2. Configure a filter group for each AD group and location combination by specifying a name for each filter group using the format *ADGroupName@Location*. The @ symbol acts as a delimiter, so that iBoss can separate the AD group name from the location name. The specified group name must be identical to the name of AD group as specified in Active Directory, and the location must be identical to the location name as defined in ExtremeControl. Spaces are allowed in both the AD group name and the name of the location.

   For this scenario, we will configure the two staff groups that we defined previously.

3. Configure the three AD group and location combinations for students.

4. Because there are only five filter group definitions on each page, each page of definitions must be saved separately before moving on to the next page. After defining the first five filters, select **Save** at the bottom of the page to save changes.
5. To navigate to the next page of filter group definitions, select the arrow to the right of the **Filtering Groups** drop-down list at the top of the page.

6. Add the remaining student group and location definition.

7. Select **Save**.

Configuration of Extreme Management Center

The final step in configuring the integration of iBoss and Extreme Management Center is to create the location definitions, set up ExtremeControl for Active Directory access using LDAP, and configure access rules for each AD group and location combination.

NOTE: This document covers how to configure access rules, but does not cover creating LDAP profiles, roles, locations, or other ExtremeControl configuration items.

Recall our example table of groups and locations from Defining Locations:

AD Group	Location
All Students	Instructional Areas
All Students	Cafeteria
All Students	Gym
All Staff	Instructional Areas
All Staff	Everywhere Else

1. Create an LDAP user group in ExtremeControl to represent each AD group used for assigning access. For this scenario, we will create the ExtremeControl groups Students (which maps to the AD group All Students), and Staff (which maps to the AD group All Staff).
2. Create locations in ExtremeControl. For this scenario, we will create three ExtremeControl locations: Cafeteria, Gym, and Instructional Areas. We will not need a specific ExtremeControl location for everywhere else, but instead will create a general rule to assign access for those end systems.
3. Create the access rules to assign policy according to the location All Students in Instructional Areas.
   The name of the rule is significant and must be specified using this specific syntax. Name the rule by putting the AD group name this rule refers to on the left side of the @ symbol, and the location this rule applies to on the right side. Since this rule applies to All Students in the Instructional Areas location, the rule name becomes *All Students@Instructional Areas*.
   Note: Failure to name your rules in this manner prevents the integration from working properly.
4. Create the rule for All Students in the Cafeteria and All Students in the Gym using the same syntax.
   Note: In all three cases, we are assigning the same ExtremeControl profile to members of All Students. From a network perspective, these rules are for student end systems; therefore, assign the same rate limits, layer 3-4 filters, and so on, regardless of the location the end system is in. What is different about each of these rules is the location of the end system and the filter group that iBoss assigns to the end system traffic.

5. Create the rule for All Staff in Instructional Areas, using the same format as the student rules.

6. Create the final Staff rule. This rule is different in how it is named because there is no specific location information provided, so name the rule using just the name of the AD group itself.

   Recall that when we configured the filter groups in iBoss, we created a filter group with just the AD group name of All Staff. Because there is no location specified, iBoss applies that filter group to any end system registered to AD accounts that are members of All Staff that are not otherwise in a defined location. Naming the rule without the @ symbol or location name tells ExtremeConnect to omit the location when making the call to iBoss. Using this naming syntax allows filter groups to be assigned to end systems based solely on AD group membership.
   Because this rule is more general than the previous staff access rule, it must be located after the *All Staff@Instructional Areas* rule in the rules list for the ExtremeControl configuration to work correctly.

Verification

To verify the integration is working:

1. Connect to a test SSID and authenticate using two different accounts using two wireless clients.
2. Ensure each account is a member of different active directory groups.
3. Configure two iBoss filtering groups that match the AD groups that include each test account.
4. iBoss can display information about the filter groups it assigns to end systems from its web interface. Use both the Extreme Management Center and the iBoss management interface to confirm the scenario's integration configuration.
5. Locate both end systems so they connect from the Instructional Areas location. From the **Identity and Access** tab in OneView, you can see that the correct rules have been applied to each end system.

6. To see the corresponding information in iBoss, open the management interface. From the left menu, select **Users > Computers**. The information is listed in the **Detected Computers** pane.

   Note: Both Extreme Management Center and iBoss list the same end system IP address, filter set name, and AD user name for each end system. This indicates that integration is working and that the configuration is correct.

Lightspeed Rocket Web Filter

The Lightspeed integration provides a single sign-on solution and web content filtering capabilities based on the end system's active directory membership.

Module Configuration

The following table describes the configuration attributes:

Configuration Option	Description
Server	IP address of the Rocket Web Filter appliance.
Password	RADIUS shared secret.
RADIUS interim message interval	Number of minutes in which a RADIUS interim message is sent to keep the session active.
Include Calling-Station-ID	Includes the Calling-Station-ID RADIUS attribute. The calling station is set to the end system's MAC address.
Include Called-Station-ID	Includes the Called-Station-ID RADIUS attribute. The called station is set to the switch IP address.
Ignore usernames that contain	Ignores usernames that contain the entered value. Semicolon delimited.
Ignore ExtremeControl profiles	Ignores end systems that are assigned an ExtremeControl profile. Semicolon delimited.
Ignore SSIDs	RADIUS accounting is not sent for an end system SSID that match this value. Semicolon delimited.
Default domain name	Appends the username to the domain name.
Remove email domain from username	Removes the email domain from the username.
Remove domain from username	Removes the Windows domain from the username.

Configuring the Rocket Appliance

In addition to the standard configuration of the Rocket Web Filter appliance, three steps are required to integrate with Active Directory and ExtremeControl. Only the steps necessary for integration are covered in this document.

Configure LDAP Settings

To configure LDAP settings:

1. Log in to the Rocket appliance at https://*IP address of Rocket Appliance*. Enter the necessary credentials and select **Login**.
   The dashboard configuration menu opens.
2. To configure LDAP access from the Rocket Web Filter appliance to Active Directory, select **Administration** from the top right corner of the dashboard.
3. To configure the Active Directory settings, scroll down to the **Authentication Sources** pane. Select **+ Add Authentication Source**.
4. In the **Edit Authentication Source** dialog, edit the fields.
5. Select **Save**.
6. Verify that the Active Directory is listed in the **Authentication Sources** pane.
7. To verify the Active Directory configuration, select **Test**.

   The **Test Authentication Source** dialog opens.
8. Enter a known valid domain username and password, and select **Test User Login**.
   A Success message displays for a successful query.

Configure RADIUS Accounting

The RADIUS shared secret is a configurable field in the Rocket appliance. To configure the shared secret:

1. Access the **Web Filter** menu and scroll to the bottom of the page.
2. In the **Shared secret** field, enter a value to be used between the Lightspeed Systems Rocket Web Filter appliance and the ExtremeConnect Lightspeed

Systems module. Note the shared secret value for later configuration steps.

3. From **Mobile Devices**, enable **Transparent authentication**.

Configure Policy Management

The final items to configure are the rule sets in Policy Management that the Rocket Web Filter appliance assigns to end systems. Rule sets are lists of web site categories, keywords, and actions that control how users access the Internet.

Typically, customers will have predefined assignments matching the rule sets to directory objects or IP addresses, or both. For this document, the assumption is that no assignments have been created in Policy Management.

Note: A predefined rule set (Block All) is assigned to an Organizational Unit (OU=Solutions Eng,DC=testing,DC=local) that was defined in the previously added Active Directory Server.

To configure rule sets:

1. From the Rocket Appliance ribbon, select **Web Filter**. From the left menu, select **Policy Management**.

2. From the **Rule Sets** tab, verify that the Block All rule set exists in the list.

3. To assign the rule set to an object, select **Assignments > New Assignment**.

   The **New Assignee** dialog opens.
4. For **Type**, select the type of object to be used. To browse the Authentication Source, the Search feature can be used to list all of the OU's that are available on the server.

5. Verify that the Web Filter Rule in this new assignment is set to **Block All** at the bottom of the window.
6. Select **Save**.
7. Select **Web Filter > Mobile Devices**.
8. Enable **Transparent authentication**, and select the authentication source **AD** from the drop-down list.

McAfee ePO

The McAfee ePO (ePO) integration offers end system assessment and automatic anti-virus signature file updates with ePO, and the quarantine of end systems with ExtremeControl.

ePO Extension

To integrate ExtremeConnect and ePO, a vendor-specific server extension must be installed on the ePO server.

To install the extension:

1. Download the extension from the Extreme Management Center server using your browser from this link (alter the link to use your Extreme Management Center IP address or hostname): https://*XMC-IP*:8443/connect/McAfee/ExtremeNetworks-McAfee_ePO_Extension.zip
2. Log in to your McAfee ePO server as an administrator.
3. Select **Software > Extensions**. Use the button at the top of the page to add the extension you just downloaded from Extreme Management Center.
   Once installed, you should see the custom third-party extension from Extreme Networks appear on your list of extensions.

Module Configuration

The following tables describe the configuration options available for the McAfee ePO ExtremeConnect module
(the configuration file name is McAfeeEPOHandler.xml).

Service Configuration	Description
Username	Username used to connect to the ePO API.
Password	Password used to connect to the ePO API.
Server	ePO server IP address.
Port	ePO server port.

General Module Configuration	Description
Poll interval in seconds	Number of seconds between connections to the adapter running on the ePO server.

General Module Configuration	Description
Module log level	Verbosity of the module. Logs are stored in the Extreme Management Center server.log file.
Module enabled	Specifies whether the module is enabled.
Update local data from remote service	If this is set to *true*, data from the remote service is used to update the internal end system table. The best practice is to set this option to *true*. You will also need to set this to *true* if you want to populate the username and device type from McAfee in ExtremeControl (see the additional options below). **Default:** true
Default end-system group	The default end system group name to which you assign all McAfee devices in ExtremeControl. If you do not want end systems from McAfee to be assigned to this default group, configure a group name which does not exist in ExtremeControl.
Enable Data Persistence	Enabling this option forces the module to store end system data, end system group data, and VLAN data to a file after each cycle. If this option is disabled, the module forgets all of the data after a service restarts. However, to clean existing data, the corresponding .dat files must be deleted.

Service-Specific Configuration	Description
Custom field to use	The number of the custom data field for each end system to store the data retrieved from ePO. **Available values:** 1, 2, 3 or 4 **Default:** 1
Format of the incoming data	Format of the data that gets stored in the custom data field. You can use and combine any of the available variables: *ipAddress*, *macAddress*, *osType*, *osServicePackVersion*, *nodeName*, *userName*, *datVersion*, *lastUpdate*. Note that ePO might update the *lastUpdate* value for each device frequently and ExtremeConnect calls Extreme Management Center web services to refresh that value in all end systems custom fields. Depending on your poll interval, these operations can put extensive stress on the Extreme Management Center server. The best practice is to avoid using the *lastUpdate* variable here. This variable can be used only if the poll interval is very low (such as once per day) and the number of end systems is below 1,000. **Default:** NodeName=#*nodeName*#; OS=#*osType*# (#*osServicePackVersion*#); User=#*userName*#; DAT Version=#*datVersion*#

Service-Specific Configuration	Description
End-system group for decommissioned devices	The default end system group for devices that existed in ePO but have been deleted. If you want to explicitly identify those devices and even authorize them differently (since they are no longer managed by ePO, which could pose a threat) you can configure the group they should automatically be moved to here and enable the corresponding decommission feature below. Make sure you manually create this end system group in ExtremeControl.
Remove device from other groups on decommission	Enable this option to move devices that have been deleted from ePO to the ExtremeControl end system group configured by the corresponding decommission option above. If disabled, devices are not automatically moved to this group, but rather stay with their existing group membership. **Default:** false
Delete custom data in Extreme Management Center for decommissioned devices	When set to *true*, if a device is deleted in ePO, the end system's custom data field in Extreme Management Center will be cleared also. Although this will keep your data clean in Extreme Management Center, it can often be helpful to still see the old ePO data for those end systems that were previously managed by ePO. **Default:** false
Overwrite the existing username with the one acquired from McAfee ePO	If this is set to *true*, the username for devices retrieved from ePO overwrites the username that is in ExtremeControl. If no username can be retrieved from ePO for a given end system, then no change is performed in ExtremeControl. **Important:** Enabling this option can interfere with existing ExtremeControl processes if you are already retrieving and using the username through some other mechanism (such as 802.1X or Kerberos snooping) because these usernames will be overwritten. **Default:** false
Overwrite the existing device type for devices with the one acquired from McAfee ePO	If this is set to *true*, the device type (operating system) retrieved from ePO overwrites the device type that is already in ExtremeControl. If no operating system can be retrieved from ePO for a given end system, then no change is performed in ExtremeControl. **Important:** Enabling this option can interfere with existing ExtremeControl processes if you are already retrieving and using the device type through some other mechanism (such as DHCP snooping) because the device type will be overwritten. However, in most cases, enabling this feature for end systems managed by McAfee ePO should improve your current method since the quality of the information retrieved from ePO is usually good. **Default:** false

Service-Specific Configuration	Description
Max DAT version difference between ePO and client before triggering client update task	Max DAT version difference between ePO and client before triggering client update task. Example: If set to 2, and the difference between the DAT version on ePO's master catalog and the client's DAT version is at least 2, then a client update task is automatically triggered. This task is executed by ePO. If the task is executed successfully, it should update the client's DAT file. **Note:** ExtremeConnect cannot guarantee that the task will be executed successfully. Setting this value to 0 disables this feature. **Default:** 1
Max DAT version difference between ePO and client before generating a NetSight event	Creates Extreme Management Center alarms based on these events. The alarms can be configured to trigger an email or other mechanisms. Example: If set to 4, and the difference between the DAT version on ePO's master catalog and the client's DAT version is at least 4, this generates an Extreme Management Center event. The event will appear in OneView's Alarms and Events tab, with event type Console and category OneFabricConnect. To disable this feature, set the value to 0. **Default:** 4
Max DAT version difference between ePO and client before quarantining client via NAC	You can use your ExtremeControl assessment configuration to automatically push those end systems to a quarantine role if required. Example: If set to 7, and the difference between the DAT version on ePO's master catalog and the client's DAT version is at least 7, then the value for the corresponding assessment test result will be set to 10 and High. To disable this feature, set the value to 0. **Default:** 0.
Name of the ePO client task that Connect uses to trigger a DAT version update for individual devices	Use the exact name as defined in ePO to define a client task in ePO that will update a client's DAT file (and more if desired, such as the agent version). This option also finds any client tasks that include the configured name, if the name is unambiguous. **Default:** Update Agent
Time before client update task is aborted by EPO	Number of minutes after which the ePO server should abort the client update task. This value is sent to the ePO server when running the *clienttask.run* web service call as an additional parameter (*abortAfterMinutes*). To disable this feature, set the value to 0 (the parameter will not be used when making the web service call). **Default:** 10 minutes

Service-Specific Configuration	Description
Max number of client update tasks triggered per client per day	To avoid triggering too many ePO client update tasks, set this limit to a non-zero value. ePO client update tasks will not be triggered after the configured maximum number of retries has been reached for the current day. When the next day starts (the first run after midnight), the number (count) of retries per MAC address is reset to zero automatically. Client update tasks will be triggered again as long as the device is still out of date (see *dat_file_max_difference_before_trigger_update_task*) or the maximum for that day has been reached again. To disable this feature, set the value to 0. The code will trigger a client update task on each cycle as long as the device is out of date. **Default:** 1 update task per client per day
Max number of NetSight events generated per client per day	To avoid generating too many events, set this limit to a non-zero value. After the maximum number of retries has been reached for the current day, the system stops generating Extreme Management Center events . When the next day starts (the first run after midnight), the number of retries per MAC address is reset to zero automatically. Events will be generated again as long as the device is still out of date (see *dat_file_max_difference_before_generating_netsight_event*) or the maximum for that day has been reached again. To disable this feature, set the value to 0. The code will generate an event on each cycle as long as the device is out of date, no matter how many cycles or triggers per day occur. **Default:** 1 event per day
Enable Assessment	If this is set to *true*, assessment data for all devices managed by ePO are made available to the assessment adapter. Example: If McAfeeEPOHandler is configured to run every hour and the DAT version of a device is running out-of-date, it will take up to one hour to populate this data in ExtremeControl's assessment process. The data is updated on each cycle. **Default:** false
Request an immediate re-assessment of an end-system if its DEVICEOUTOFDATE value changed	If this is set to *true*, a reassessment of each end system, where its DEVICEOUTOFDATE value changed either from *true* to *false* or the other way around, will be requested from ExtremeControl. For example, if an end system has been pushed to Quarantine because its DAT file version was out-of-date, but it now has updated the DAT version, the end system will be reassessed immediately and authorized properly. If this feature is disabled, it can take hours or days for the end system to update its ExtremeControl policy or authorization, depending on the ExtremeControl assessment configuration for this end system. This request feature is only used if the assessment feature is enabled. **Default:** true

Service-Specific Configuration	Description
Use XAPI to trigger a reauth and thus also a re-assessment of an end-system	If this is set to *true*, a reassessment of an end system is not performed using a web service call, but rather executed directly on the access switch of the end system. This operation is executed using XAPI, therefore `enable web http(s)` must be configured on each ExtremeXOS switch. This executes the command `clear netlogin state mac-address` with the MAC address of the end system to immediately trigger a reauthorization. The reauthorization triggers a reassessment of the end system, which then immediately changes its authorization state from Accept to Quarantine or vice-versa. This feature is only used if the *reassess_endsystem* feature is also enabled.
Use HTTPS for XAPI calls	Enables the use of HTTPS instead of HTTP for any XAPI communication with all ExtremeXOS switches. If enabled, you must also install the SSH mod on all ExtremeXOS switches and configure `enabled web https`. This option is only used if the *reauthenticate_endsystem_using_xapi* feature is also enabled.
Username to connect to any EXOS switch if no CLI credentials are provided within Extreme Management Center	If the feature *reauthenticate_endsystem_using_xapi* is enabled, the solution will need to authenticate on all ExtremeXOS switches to perform reauthentication of end systems. It will try to retrieve the corresponding username and password from the configured CLI credentials from Extreme Management Center, but if there are not any credentials for a particular switch, then the default value is used.
Password to connect to any EXOS switch if no CLI credentials are provided within Extreme Management Center	If the feature *reauthenticate_endsystem_using_xapi* is enabled, the solution authenticates on all ExtremeXOS switches to perform reauthentication of end systems. It will try to retrieve the corresponding username and password from the configured CLI credentials from Extreme Management Center, but if there are not any credentials for a particular switch, then the default value is used.
Name of the ePO client task that Connect uses to trigger an agent wake up	Use the exact name as defined in ePO. Also, you must define a client task in ePO that will wake up a client's agent. This name is required for ExtremeConnect to wake up the agent on quarantined end systems for which a client update task has been triggered. By default, ePO agents only report their DAT version to the ePO server once per hour. As a result, ExtremeConnect only realizes that an end system has updated to the latest DAT Version after a long interval, and that end system can be quarantined for a long time. Using an agent wake up task to sending the latest DAT version to the ePO server removes end systems from the quarantine state faster.

Service-Specific Configuration	Description
Time before the agent wake up client task is triggered after a quarantine event and update task trigger	If an end system is quarantined by ExtremeControl, the code triggers an ePO client update task. The task will try to update the DAT version on the end system through the ePO agent. This process can take a few minutes. After a successful update, the ePO agent does not immediately report the current client DAT version back to the ePO server. Instead, it reports the information using its standard poll interval, which is typically set to run once per hour. To shorten the time that end systems spend in quarantine, use this parameter to trigger a client task on the ePO server. The corresponding agent wakes up *X* seconds after the client update task is triggered. To disable this feature, set this value to 0. **Default:** 0

Verification

Any data (including assessment data) is updated only during the configured update intervals. For example, if you update only once per day, do not expect any updates in ExtremeControl more than once per day. Any data retrieved from ePO and any action triggered in the direction of Extreme Management Center are handled by the ExtremeControl Handler. ExtremeControl Handler has its own update interval, and picks up any changes or updates from ePOHandler and pushes them to Extreme Management Center. Depending on the number of changes or actions during one cycle, and the number of end systems managed, you must wait awhile before you can validate the data in Extreme Management Center.

Data Import to ExtremeControl

There are multiple options to verify when data on all devices managed by ePO is imported to ExtremeControl.

You can use the OneView end system table on the **Identity and Access** tab and display the custom data field that you have configured for McAfeeEPOHandler. You will also see the username and detailed device type information retrieved from ePO, if you enabled those features.

Another option is to use the general **Search** tab to find an end system that is managed by ePO. The search displays ePO data as follows:

You can also verify whether all ePO-managed devices have been assigned to the default end system group in ExtremeControl if you configured an existing group in ExtremeControl and want to use this feature.

Assessment

If the DAT file is out-of-date and the corresponding assessment features are enabled, a healthy device will not update to the latest ePO DAT version because it is running a DAT version that is older than *X* versions configured in the ePO handler configuration file. Once ExtremeConnect recognizes the outdated DAT file, it notifies to the assessment adapter and tries to trigger the corresponding client update script on the ePO server. The update task is triggered only for end systems that are in Accept or Quarantine state, and avoids updating end systems that are disconnected, rejected, or in an error state. If ExtremeControl triggers an assessment for this end system before the device can be updated, ExtremeControl recognizes that the device is out-of-date and quarantines it.

At this stage, the device should have a policy (or VLAN) that does not allow it to harm other network devices or services, but still allows the ePO server to contact and update the device.

After ePO has successfully updated the device and the next ExtremeConnect update cycle runs, the assessment adapter receives the updated information (from ExtremeConnect) that the device is no longer out-of-date. ExtremeConnect immediately triggers a reassessment in ExtremeControl, which reauthorizes the compliant device with its VLAN policy.

End systems that contain the keyword **server** in their operating system name (retrieved from ePO) will receive a test score of 6.0 instead of 10.0 for the DEVICEOUTOFDATE test and will not be quarantined. Since most customers do not want to quarantine server systems, ePO offers a solution called MOVE, which protects virtual servers without applying a DAT file to each server (the DAT version will always be 0, although these systems are protected by ePO).

Handling Deleted ePO Devices

To test this workflow:

1. Remove or delete a device from ePO.
2. Wait for the next ExtremeConnect synchronization.
3. Verify that:
    a. The device's custom field has been emptied (if this feature has been enabled in the configuration file).
    b. The device is a member of the ExtremeControl end system group for decommissioned devices (if this feature has been enabled in the configuration file).
    c. The device does not appear in the end system list that displays at the bottom of the ExtremeConnect management web site (on the **McAfee ePO** tab). This means that the device has been deleted in the internal list as well.

Palo Alto Networks

The Palo Alto integration consists of multiple solutions. The user ID solution notifies Palo Alto of IP to username mapping.

Module Configuration

The following table describes the configuration options:

Configuration Option	Description
Username	Palo Alto username.
Password	Palo Alto password.
Server	Palo Alto IP address.
Vsys	Palo Alto vsys to update.
Extreme Control	UserID messages that are sent to server that match the ExtremeControl appliances. Semicolon delimited.
Ignore usernames that contain	UserID messages will not be sent for end system usernames that contain this value. Semicolon delimited.
Ignore ExtremeControl profiles	UserID messages will not be sent for end system profiles that match this value. Semicolon delimited.
Ignore SSIDs	UserID messages will not be sent for end system SSID that match this value. Semicolon delimited.
Default domain name	Appends the username to the domain name.

Configuration Option	Description
Append to username	Appends the string to the username.
Remove characters from username after delimiter	Removes all characters after the delimiter in the username.
Remove email domain from username	Removes the email domain from the username.
Remove domain from username	Remove the Windows domain from the username.
User-ID timeout	Palo Alto UserID timeout interval.
Multiple user queue timer	Number of seconds to wait to queue multiple userID messages before sending them,
Reuse HTTP connection	Reuses the HTTP connection to limit connections to Palo Alto.

Palo Alto Configuration

This section assumes that the userID is not currently configured on the Palo Alto NGFW. Additionally, it assumes that the onboard UserID Agent that was released with Palo Alto NGFW version 5.0 will be used. If separate UserID Agent configurations are used, see Appendix B for detailed instructions on the use of the agent.

1. Navigate to the Palo Alto NGFW that will be used. From the **Device** tab, select **User Identification**. If no other userID source will be used, make sure that that all of the check boxes are disabled on the **User ID Agent Setup** pane. Otherwise, select **Add** under the **Include/Exclude Networks** pane. To include the networks in the user identification, add the internal networks that a user will show up on.

2. To enable the user identification for the zone that will be used for the integration, select **Network > Zones**.

   The **Zones** list displays.

3. From the list, select the zone on which the users (that will be identified) reside. In the **Zone** dialog that opens, select **Enable User Identification**. In the **User Identification ACL Include List** pane, add the networks for these users. Select **OK**.

4. Verify that the **Zones** list summary reflects that the changes you made are correct, and commit the changes to the firewall.

5. On the Palo Alto NGFW, create a user account that can remotely use the XML API. Select the **Device** tab, and select **Admin Roles > Add**.

6. Define the new role as API User. From the **Web UI** tab, select each green checkmark so that it displays a red **X** instead. This action disables the Web UI access for this role.

7. From the **XML API** tab of the profile, select the red **X** on each item to grant access to the corresponding XML API feature. To save the profile, select **OK**.

8. In the **Admin Roles** list, verify that the API User role is available to assign to an administrator.

9. From the left menu, select **Administrators**. To create a new user account to use in the XML API, select **Add**.

10. In the **Administrator** dialog, create an account that can be used by the ExtremeConnect module. For **Role**, select **Role Based**. In the **Profile** drop-down list, select the API User profile that was previously created. Select **OK**.

11. Select **Interface Management > Network**. In the User-ID column, enable **User-ID** for the network.

12. To commit the changes to the Palo Alto NGFW, select **Administrators > Commit**.

Verification

To verify the userID integration:

1. Log in as a user to the network using either 802.1X or web authentication.
2. Select the Palo Alto NGFW, and select the **Monitor** tab.
3. Filter on the username that was used for the authentication. For example, if a computer was authenticated with the username *sales*, the filter would be (user.src eq sales), as shown in the following graphic:

Mobility Configuration

AirWatch

The AirWatch integration provisions mobile devices in the network based on device ownership and provides assessment data in the network access control process. Additionally, data in Extreme Management Center is enriched for each end system and offers comprehensive reporting capabilities in OneView.

Module Configuration

The following tables describe the configuration options:

Server Configuration	Description
Username	Username to contact the MDM provider. Must have access rights to the respective API.
Password	Password used to contact the MDM provider.
AirWatch Server IP	IP or hostname of the MDM server.
AirWatch Webservice URL	Base URL to connect to the API of the service.
AirWatch Tenant Code	API key provided by AirWatch to access a specific customer configuration.

General Module Configuration	Description
Poll interval in seconds	Number of seconds between connections to the MDM provider.
Module log level	Verbosity of the module. Logs are stored in the Extreme Management Center server.log file.
Module enabled	Whether the server is enabled.
Push update to remote service	If this is set to *true*, data from other modules is pushed to the service.
Update local data from remote service	If this is set to *true*, data from the remote service is used to update the internal end system table.
Default end-system group	The default end system group name to use if an end system is not approved yet.
Enable Data Persistence	Enabling this option forces the module to store end system data, end system group data, and VLAN data to a file after each cycle. If this option is disabled, the module forgets all of the data after a service restarts. However, to clean existing data, the corresponding .dat files must be deleted.

Service-Specific Configuration	Description
Custom field to use	The number of the custom data field for each end system to store the service specific incoming data.
End-system group for Managed Business Mobile Devices	The default end system group for corporate mobile devices.
End-system group for Managed Personal Mobile Devices	The default end system group for personal mobile devices.
End-system group for Decommissioned Mobile Devices	The default end system group for decommissioned mobile devices.

Service-Specific Configuration	Description
Enable Remote Wipe	When enabled, devices are wiped if they are moved to the MDM Remote Wipe end system group. **off** - Disabled **enterprise** - Always performs an enterprise wipe (only deletes corporate data) **adaptive** - Performs an enterprise wipe if the device was an employee-owned device and a full wipe if it was a company **devicefull** - Always performs a full wipe regardless of ownership
Enable Quarantine Notification	If this is set to *true*, the device is notified using the selected mode when it is quarantined.
Quarantine Notification Text	Message is included in the quarantine notification to the user.
Enable Assessment	If this is set to *true*, assessment data is made available to the assessment adapter.

Assessment Plugin Map	Description
Plugin Name	Plugin ID name.
Data Field	AirWatch data field being retrieved in this test.
Force Reassessment	Forces reassessment of the changed content.

Assessment Plugin Map	Description
Format of the incoming data	Format of the data that gets stored in the custom data field. Syntax: The end-system is currently #mdmManaged# Available variables: *id* *udid* *serialnumber* *imei* *assetnumber* *name* *locationgroupid* *locationgroupname* *username* *useremailaddress* *ownership* *platformid* *platform* *modelid* *model* *operatingsystem* *lastseen* *enrollmentstatus* *compromisedstatus* *compliancestatus* *lastcompliancecheckon* *lastcompromisedcheckon* *lastenrolledon* *macaddress* *iscompromised* *dataprotectionenabled* *blocklevelencryption* *filelevelencryption* *ispasscodepresent* *ispasscodecompliant*
Update Kerberos username for end-systems	If this is set to *true*, the username is updated for each end system and a Kerberos reauthentication is triggered.
Update custom fields for end-systems	If this is set to *true*, the custom field data is updated for each end system.

Assessment Plugin Map	Description
Update devicetype for end-systems	If this is set to *true*, the device type data is updated for each end system.

Variables available for custom field string are defined in the AirWatch API documentation.

NOTE: The look and feel of the MDM interface can vary, depending on your customization.

Create an API User

Under AirWatch user management, all users and administrators can access the web services API. The following process explains how to create a generic user with full access.

NOTE: Any user with role *API* can access the API. A new user role can be created that only grants access to the API and restricts all other access.

1. From the main dashboard, select **Menu** > **Accounts** > **Administrators**.
2. From the list of users, select **Add** > **Add User**, or edit one of the existing users.
3. For **User type**, select **Basic**, and enter user credentials.
4. Add a role. Select **Save**.
   The user and password provided in the previous screen must be provided to MDM connect in the corresponding AirWatch plugin configuration file.
5. From the AirWatch interface, select **Content** > **Settings** > **System** > **Advanced API** > **REST API**. Note the API key, which is the value that must be provided to the AirWatch module as Tenant Code. The Tenant Code (API key) is an additional parameter used for connectivity with AirWatch servers.

Creating a Compliance Profile

The basic variable provided by the Assessment Adaptor is the compliance status. This variable (TestID 100002) indicates whether the mobile device with that security profile applied is compliant with the security requirements specified by the profile.

This variable can be used as a global indicator of compliance with the security rules of the enterprise. Other variables can be considered to provide granular access control to

the network. For example, from ExtremeControl, you can use the variable PASSCODEPRESENT (TestID 100028) to verify whether a device has defined a password and quarantine devices that do not have a password during the grace period allowed by the security policy.

AirWatch differentiates between compliance profiles and device profiles. Compliance profiles define security rules that the device must comply with, such as:

- Installed applications
- Cellular use
- Encryption
- Version of OS
- Change of SIM

A device profile defines a set of configurations that the device must have to be considered compliant, such as:

- Password length
- SSID lists
- Exchange servers
- General device restrictions (such as access to SIRI, YouTube, Screen Capture, iCloud)
- Installed Certificates
- APNs

Some parameters can be configured by the MDM itself when the profile is applied. Some parameters require user intervention, and often define a grace period until they trigger a security action if a configuration change has not been performed (for example, a password change).

Device and compliance profiles are assigned by device type, location group, ownership, and so on.

Example: Define a Compliance Profile for an Application

1. Select **Add** > **Compliance Policy**.
   The **Create Device Policy** wizard opens.

2. On the **Rules** page, select application list, the desired operation (contains), and define the name of the application. If needed, select **+** to add more rules to this profile. Select **Next** when you are finished.

3. On the **Actions** page, select remediation options, such as removing or changing the device profile, notifying the user, or executing a command. Select **Next**.

4. On the **Assignment** page, select which devices will be mapped against this profile. You can choose Platform, Manager, Ownership of the device, and so on. Select **Next**.

5. On the **Summary** page, enter a name for the compliance policy and enter a description. Under the **Device Summary** pane, review how many of the currently enrolled devices will pass or fail our test.

6. To enable the policy, select **Finish And Activate**.

Integrating AirWatch MDM in the ExtremeControl Workflow

Every time a new user is created in AirWatch MDM, the user receives an email or SMS with instructions to register his device.

By following the link in the email, the user is presented with the AirWatch login page and the ability to register their device in the MDM system.

To integrate the workflows:

1. Enable registration in .ExtremeControl
2. Link to the **AirWatch MDM Registration** page from the ExtremeControl captive portal.

Once registration is enabled in ExtremeControl, you can manage the different messages that the user receives during the registration process.

1. Enable web registration in the ExtremeControl configuration, and select **Portal Options.**

2. Select **Common Page Settings**. **For Message Strings**, select the link.

   The **Message Strings Editor** opens.
3. Look for the string **registertoObtainAccess**.

   To obtain network access, you must complete the self-registration form.

   In the following example, we will change that string to contain a string similar to:

```
<h3>BYOD Self-Registration</h3>You can also register your
personal device, taping here: <form
action="https://apidev-
ds.awmdm.com/DeviceManagement/Enrollment" method="GET">
<p></p>
GroupID
<select name="AC">
<option value="SE101">SE101</option>
</select>
<p></p>
<input type="submit" name="submit "value="Register your
mobile device"></form>
<p></p>
```

   This code creates a button that will connect to the **AirWatch Registration** page. Make sure that the URL (https://apidev-ds.awmdm.com/DeviceManagement/Enrollment) is the same URL that is used in your deployment.

   This code creates the ability for the user to select the location groups to which they have been assigned when there are several locations to choose from.

   In the previous example, the option is SE101. If there is only one location group in your deployment, you can hide this content with the following code:

```
<h3>BYOD Self-Registration</h3>You can also register your
personal device, taping here: <form
action="https://apidev-
ds.awmdm.com/DeviceManagement/Enrollment" method="GET">
<p></p>
```

```
<input type=”hidden” name="AC" value="SE101">
<p></p>
<input type="submit" name="submit "value="Register your
mobile device"></form>
<p></p>
```

The look of the mobile registration page is changed to reflect this new code.

The user can enter their data in the standard ExtremeControl registration form and register as a guest to the network without control of the MDM, or they can register the mobile device by tapping **Register** and be redirected to the **AirWatch Registration** page.

When the device is successfully registered with AirWatch, the ExtremeConnect MDM plugin imports the AirWatch data to ExtremeControl. Devices classified in MDM as *Corporate owned* are placed in the end system group Mobile Devices Business. The devices classified as *Personal* are added to the group Mobile Devices Personal.

4. The ExtremeControl rule set must be adapted to reflect those groups and must act accordingly, depending on the newly registered devices.

NOTE: Devices registered by an MDM system can experience significant lag until they are added to the corresponding groups. This behavior is not a malfunction of the MDM itself or the ExtremeConnect MDM plugin. Due to the diversity of operating systems and connectivity profiles, there is no way to know in advance when a newly registered device will provide all of the data needed by the MDM software to complete the registration. It can take up to several minutes from registration to the final placement in one of the groups to obtain full access to the network.

Policy Configuration

To support the previous workflow, a device in unregistered state must be able to communicate with AirWatch servers (via HTTPS) and with Apple (via the Apple Push service). Android devices must download an agent to be registered by AirWatch, so Google Play access must be provided as well in this state.

The following policies (or more generic ones) are needed to allow AirWatch registration:

- Allow HTTPS to 12.150.127.0/24 AirWatch network
- Allow TCP 5223 to 17.0.0.0/8:TCP:5223, Apple Push service

- Allow HTTPS to 74.125.0.0/16, Google Play Downloads
- Allow TCP/UDP 5228 to 173.194.0.0/16, Google Play login

Fiberlink MaaS360

The Fiberlink MaaS360 integration requires Fiberlink authentication credentials and other account settings. This information is used in the Fiberlink MaaS360 module tab.

Module Configuration

The following tables describe the configuration options:

Configuration Option	Description
Username	MaaS360 web service username.
Password	MaaS360 web service password.
API URL	MaaS360 web service URL. Use https://services.fiberlink.com unless informed otherwise by Fiberlink.
Billing/Account ID	MaaS360 billing or account ID.
Application ID	Application ID used to contact MaaS360 web service. Use com.networks.extreme unless informed otherwise.
Application Version	Use 1.0 unless informed otherwise.
Platform ID	Use 3 unless informed otherwise.
Access Key	Do not edit this value unless informed otherwise.
Server	Set the value to the localhost.

Account Billing ID

The account billing ID is used to identify the Fiberlink MaaS360 account. To find the account billing ID, log in to the Fiberlink MaaS360 management page. In the following example, the account billing ID is 30001503:

Service Configuration	Description
Poll interval	Time period between queries to the MaaS360 web service.

Service Configuration	Description
End system group for managed business mobile devices	ExtremeControl end system group to which corporate owned devices will belong.
End system group for managed personal mobile devices	ExtremeControl end system group to which personal owned devices will belong.
Default end system group for managed mobile devices	ExtremeControl end system group to which unknown devices will belong.
Remote wipe end system group	ExtremeControl end system group that will be used to remotely wipe a mobile device.
Enable remote wipe	Enable or disable the remote wipe option.
Update Kerberos username	Enable or disable this option to update the end system username.
Update device type	Enable or disable this option to update the end system device type.
Notify user when quarantined	Enable or disable this option to notify a user when an end system is quarantined based on assessment scoring.
Enable assessment	Enable or disable this option to use the ExtremeControl assessment agent.

Verification

1. Enroll a new device with MaaS360.
2. Verify that the device is being managed by MaaS360.

3. Connect to test the SSID. Wait for the resynchronization poll to occur and verify that the end system in Extreme Management Center has device information from MaaS360.

Policy Configuration

To support the previous workflow, the device in unregistered state must be able to communicate with MaaS360 servers (via HTTPS) and with Apple (via the Apple Push service).

Some configurations require downloading an agent to be registered by MaaS360 so Google Play and Apple app store access must be provided as well in this state. If this is the case, policies must be configured to provide connectivity to the agent.

The following policies (or more generic ones) are needed to allow MaaS360 registration:

- •Allow HTTPS to MaaS360 network
- •Allow TCP 5223 to 17.0.0.0/8:TCP:5223, Apple Push service
- •Allow TCP/UDP 5228 to 173.194.0.0/16, Google Play login
- •Allow HTTPS to 74.125.0.0/16, Google Play Downloads

JAMF Casper

The JAMF Casper (Casper) integration offers provisioning of mobile devices in the network based on Casper group membership and provides assessment data in the network access control process. Additionally, the data in Extreme Management Center is enriched for each end system and provides comprehensive reporting capabilities in OneView.

Module Configuration

The following tables describe the configuration options:

Service Configuration	Description
Username	Username to contact the MDM provider. Must have access rights to the respective API.
Password	Password used to contact the MDM provider.
Server IP	IP or hostname of the MDM server.

General Module Configuration	Description
Poll interval in seconds	Number of seconds between connections to the MDM provider.
Module log level	Verbosity of the module. Logs are stored in the Extreme Management Center server.log file.
Module enabled	Whether the server is enabled.

Service-Specific Configuration	Description
Custom field to use	The number of the custom data field for each end system to store the service-specific incoming data.
Full Re-Sync Interval	The time period after which a full data resynchronization is performed. This also updates the data on devices that are already synchronized.
Incremental Re-Sync Interval	The time period after which an incremental data resynchronization is performed. This only updates the data on devices that were added to or removed from Casper since the last synchronization. Existing (already synchronized) devices are updated during an incremental synchronization.
Run full sync at specific times	Enable this option if you want full synchronizations to occur only at configured times of the day. Configure the list of those times using the option *Full Sync Times*. Verify that your configured *Poll interval in seconds* option is set to a low number (such as 60 seconds) since ExtremeConnect only performs a full synchronization if the time of the day is after one of the configured full synchronization times. If this option is disabled, ExtremeConnect runs full synchronizations regularly according to the configured *Full Re-Sync Interval* value.
Full Sync Times	List of times of day (using a 24-hour clock) at which ExtremeConnect will perform a full synchronization. Semicolon delimited. Format example: 05:00;23:00

Service-Specific Configuration	Description
Format of the incoming data for iPhones	Format of the data that gets stored in the custom data field. Syntax Example: `OS Version=#osVersion#; Last Inv. Update=#lastInventoryUpdate#; Is Managed=#isManaged#; User=#userName#; Real Name=#realName#; Email=#email#` Available Variables: *ipAddress* *mac* *osVersion* *lastInventoryUpdate* *isManaged* *modelDisplay* *userName* *realName* *email* *isSecurityDataProtection* *isSecurityBlockLevelEncryptionCapable* *isSecurityFileLevelEncryptionCapable* *isSecurityPasscodePresent* *isSecurityPasscodeCompliant* *isSecurityPasscodeCompliantWithProfile*

Service-Specific Configuration	Description

Format of the incoming data for computers	Format of the data that gets stored in the custom data field.
	
	Syntax Example:
	
	`OS=#osName# (#osVersion#);`
	`User=#userName#;`
	`Real Name=#realName#;`
	`Email=#email#;`
	`Phone=#phone#`
	
	Available Variables:
	
	macAddress
	alternateMacAddress
	osName
	osVersion
	ipAddress
	userName
	realName
	email
	phone

Default end-system group for all iPhones	The default end system group name to use if it is not set dynamically for all iPhones.
Default end-system group for all computers	The default end system group name to use if it is not set dynamically for all computers.
End-system group for decommissioned devices	The default end system group for decommissioned devices.
Overwrite the existing username for iPhones/iPads with the one acquired from CASPER	If this is set to *true*, the username for iPhones and iPads retrieved from Casper will overwrite the username that is already in ExtremeControl. If no username can be retrieved from Casper for a given end system, then no change is made in ExtremeControl. **Important:** This can conflict with existing ExtremeControl processes if you are already retrieving and using the username through some other mechanism (such as 802.1X or Kerberos snooping), and the information will be overwritten.

Service-Specific Configuration	Description
Overwrite the existing username for MACs with the one acquired from CASPER	If this is set to *true*, the username for Macs retrieved from Casper will overwrite the username that is already in ExtremeControl. If no username can be retrieved from Casper for a given end system, then no change is made in ExtremeControl. **Important:** This can conflict with existing ExtremeControl processes if you are already retrieving and using the username through some other mechanism (such as 802.1X or Kerberos snooping), and the information will be overwritten.
Overwrite the existing device type for iPhones/iPads with the one acquired from CASPER	If set to *true*, the device type (iOS) retrieved from Casper for iPhones and iPads will overwrite the device type that is already in ExtremeControl. If no operating system can be retrieved from Casper for a given end system, then no change is made in ExtremeControl. **Important:** This can conflict with existing ExtremeControl processes if you are already retrieving and using the device type through some other mechanism (such as DHCP snooping), and this information will be overwritten. This feature can improve your current method for end systems managed by Casper.
Overwrite the existing device type for MACs with the one acquired from CASPER	If this is set to *true*, the device type (iOS) retrieved from Casper for Macs will overwrite the device type that is already in ExtremeControl. If no operating system can be retrieved from Casper for a given end system, then no change is performed in ExtremeControl. **Important:** This can conflict with existing ExtremeControl processes if you are already retrieving and using the device type through some other mechanism (such as DHCP snooping), and this information will be overwritten. This feature can improve your current method for end systems managed by Casper.
Overwrite the existing device type for Advanced Search computers with the one acquired from CASPER	If this is set to *true*, the device type (operating system) retrieved from Casper for Advanced Search computers will overwrite the device type that is already in ExtremeControl. If no operating system can be retrieved from Casper for a given end system, then no change is made in ExtremeControl. **Important:** This can conflict with existing ExtremeControl processes if you are already retrieving and using the device type through some other mechanism (such as DHCP snooping), and this information will be overwritten. This feature can improve your current method for end systems managed by Casper.

Service-Specific Configuration	Description
Import data on iPhones and iPads from CASPER	If this is set to *true*, the module retrieves the data on all iPhones and iPads managed by Casper and pushes the data to ExtremeControl. You must set this option to *true* if you want the MDM assessment adapter to work, since this data is delivered to the assessment adapter via a file.
Import data on computers (MACs) from CASPER	If this is set to *true*, the module retrieves the data on all Mac computers managed by Casper and pushes the data to ExtremeControl.
Max number of days that the last inventory update for iPhones is allowed to be old	The maximum number of days after the last inventory update before an alarm is sent, if assessment is enabled. Example: If this is set to *5*, the module will send an alarm when an iPhone's last inventory update is older than 5 days.
Write assessment relevant data to an external file or not	If this is set to *true*, the assessment data for iPads and iPhones is made available to the assessment adapter.

Assessment Map Entry	Description
Plugin Name	The plugin ID name.
Data Field	The MDM data field being retrieved in this test.
Force Reassessment	Forces reassessment of changed content.

Verification

To verify proper functionality, validate the data in the custom field that was configured to be used for the Casper integration in your end system list (in NAC Manager or OneView). For each iPhone, iPad, or Mac computer, you should see information that is retrieved from Casper, as shown in the following example:

If you have enabled the feature to automatically assign Casper devices (iPhones, iPads, or Mac computers) to end system groups in ExtremeControl, based on the group name in Casper matching the end system group name in ExtremeControl, you can verify this functionality as follows:

1. From OneView, open one of the groups.
2. Verify whether the correct end systems (=MAC addresses) are listed.

As the Casper integration is a one-way integration, there is nothing to verify on the Casper server. The integration is neither pushing data to Casper nor modifying any configuration in Casper.

MobileIron

The MobileIron integration offers the provisioning of mobile devices in the network based on device ownership and provides assessment data in the network access control process. Additionally, the data in Extreme Management Center is enriched for each end system and provides comprehensive reporting capabilities in OneView.

Module Configuration

Service Configuration	Description
Username	Username to contact the MDM provider. Must have access rights to the respective API.
Password	Password used to contact the MDM provider.
MobileIron Server IP	IP or hostname of the MDM server.
MobileIron Webservice URL	Base URL to connect to the API of the service.

General Module Configuration	Description
Poll interval in seconds	Number of seconds between connections to the MDM provider.
Module log level	Verbosity of the module. Logs are stored in the Extreme Management Center server.log file.
Module enabled	Whether the server is enabled.
Push update to remote service	If this is set to *true*, data from other modules is pushed to the service.
Update local data from remote service	If this is set to *true*, data from the remote service is used to update the internal end system table.
Default end-system group	The default end system group name to use when an end system is not approved yet.
Enable Data Persistence	Enabling this option forces the module to store end system data, end system group data, and VLAN data to a file after each cycle. When this option is disabled, the module forgets all of the data after a service restarts. However, to clean existing data, the corresponding .dat files must be deleted.

Service-Specific Configuration	Description
Custom field to use	Number of the custom data field for each end system to store the service specific incoming data.
End-system group for Managed Business Mobile Devices	Default end system group for corporate mobile devices.
End-system group for Managed Personal Mobile Devices	Default end system group for personal mobile devices.
End-system group for Decommissioned Mobile Devices	Default end system group for decommissioned mobile devices.
Enable Remote Wipe	When enabled, devices are wiped if they are moved to the MDM Remote Wipe end system group. **off** - Disabled **enterprise** - Always performs an enterprise wipe (only deletes corporate data) **adaptive** - Will perform an enterprise wipe if the device was an employee-owned device and a full wipe if it was a company device **full** - Always performs a full wipe regardless of ownership
Enable Quarantine Notification	If this is set to *true*, the device is notified using the selected mode when it is quarantined
Quarantine Notification Text	Message is included in the quarantine notification to the user.
Enable Assessment	If this is set to *true*, assessment data will be made available to the assessment adapter.
Format of the incoming data	Format of the data that gets stored in the custom data field. Syntax: The end-system is currently #mdmManaged# Available Variables: See the MobileIron API Documentation for a full list of all available keywords.
Update Kerberos username for end-systems	If this is set to *true*, the username is updated for each end system and a Kerberos reauthentication is triggered.
Update custom fields for end-systems	If this is set to *true*, the custom field data is updated for each end system.

Service-Specific Configuration	Description
Update devicetype for end-systems	If this is set to *true*, the device type data is updated for each end system.

Assessment Map Entry #	Description
Plugin Name	Plugin ID name.
Data Field	MDM Data Field being retrieved in this test.
Force Reassessment	Forces reassessment of the changed content.

See MobileIron documentation for keywords available to use in custom field string.

Note: The look of the MDM interface can change depending on your customer customization.

Creating an API User

MobileIron provides a predefined user role for API access. Assigning the API role to a user automatically enables it to access the MDM API. A user with API access must be created to access the MobileIron API from the Extreme Management Center interface.

1. From the MobileIron user interface, select **User Management > Add New User**.
   Note: This step is not required if you plan to use an existing user or a user previously synchronized from a LDAP database.

2. Fill in the required fields. Note the user ID and password for later use in with the Extreme Management Center configuration.
3. Select the user you created, and select **Assign Roles**. Assign the API role, and select **Save**.

   The user is sent a registration email.

4. By following the link in the registration email, the user can access the MobileIron login screen and can register their device in the MDM system. The following is an example of the registration email:

Integrating the Workflows

To integrate this workflow with the ExtremeControl registration workflow:

1. Enable registration in ExtremeControl
2. Link to the MobileIron MDM registration page from the ExtremeControl captive portal.

In this case, preregistration in MobileIron is not needed and the user does not receive an email to register. Note that both methods are not incompatible. The user can have links to register from ExtremeControl registration pages and policies can be defined so that a user can receive an email and follow the link in it while unregistered in the Wi-Fi.

After registration is enabled in ExtremeControl, the administrator can manage the different messages that the user receives during the registration process.

To configure messages:

1. Enable web registration by selecting **Edit Default NAC Configuration > Portal Options**.

2. Select **Common Page Settings**. For **Message Strings**, select the link.

   The **Message Strings Editor** opens.
3. Look for the string **RegistertoObtainAccess**.

   To obtain network access, you must complete registration using the self-registration form.
   In the following example, we will change that string to:

```
<h3>BYOD Self-Registration</h3>You can also register your
personal device, taping here: <form
action="https://<Mobileironserver>/<customername>/ireg"
method="GET"><input type="submit" name="submit
"value="Register with MobileIron"></form>
```

   This code creates a button that connects to MobileIron's registration page. Make sure that the URL https://*Mobileironserver*/*customername*/ireg is the same that is used in your deployment.

   The new look of the mobile registration page is changed to reflect this new code.

4. The user can enter their data in the standard ExtremeControl registration form and register as a guest to the network without control of the MDM, or they can register the mobile device by selecting **Register** and being redirected to MobileIron's registration page.
5. Next, the user is prompted to install a configuration profile granting the MDM software the required permissions to manage the device.
6. To see the list of installed profiles, the user can select **Settings > General > Profiles**.

   When the device is successfully registered with MobileIron, the ExtremeConnect MDM plugin imports its data to ExtremeControl. Devices classified in MDM as *Corporate owned* are placed in the end system group Mobile Devices Business, and the devices classified as *Personal* are added to the group Mobile Devices Personal.
7. As an administrator, adapt the ExtremeControl rule set to reflect those groups and act accordingly depending on the newly registered devices in the **Edit Default NAC Configuration** dialog.

Note: Devices registered by an MDM system can experience significant lag until they are added to the corresponding groups. This behavior is not a malfunction of the MDM itself or the ExtremeConnect MDM plugin. Due to the diversity of operating systems and connectivity profiles, there is no way to know in advance when a newly registered device will provide all of the data needed by the MDM software to complete the registration. It can take up to several minutes from the registration to the final placement in one of the groups to obtain full access to the network.

Policy Configuration

To support the previous workflow, the device in an unregistered state must be able to communicate with MobileIron servers (via HTTPS) and with Apple (via the Apple Push service).

Some configurations require downloading an agent to be registered by MobileIron, so Google Play and Apple app store access must be provided also. If this is the case, policies must be configured to provide connectivity to the agent.

The following policies (or more generic ones) are required to allow MobileIron registration:

- Allow HTTPS to MobileIron network
- Allow TCP 5223 to 17.0.0.0/8:TCP:5223, Apple Push service
- Allow TCP/UDP 5228 to 173.194.0.0/16, Google Play login
- Allow HTTPS to 74.125.0.0/16, Google Play Downloads

Other Integration Options

The integration described in the previous section is one of many possible methods. The different methods will vary depending on the specific requirements of the enterprise deploying the integration.

Sophos Mobile Control

The Sophos Mobile Control (Sophos) integration requires authentication credentials and other account settings. This information is used in the Sophos MDM module tab and supports Mobile Control version 4.0.

Module Configuration

The following tables describe the configuration options:

Service Configuration	Description
Customer	Customer name.
Username	Web service username.
Password	Web service password.
Server	Hostname or IP address of the Sophos MDM server.

Service-Specific Configuration	Description
Poll interval	Time period between queries to the Sophos web service.
End system group for managed business mobile devices	ExtremeControl end system group to which corporate-owned devices will belong.
End system group for managed personal mobile devices	ExtremeControl end system group to which personal devices will belong.
Default end system group for managed mobile devices	ExtremeControl end system group to which unknown devices will belong.

Service-Specific Configuration	Description
Remote wipe end system group	ExtremeControl end system group that will be used to remotely wipe a mobile device.
Enable remote wipe	Enables or disables the remote wipe option.
Update Kerberos username	Enables or disables the option to update an end system username.
Update device type	Enables or disables the option to update an end system device type.
Notify user when quarantined	Enables or disables the option to notify a user when an end system is quarantined based on assessment scoring.
Enable assessment	Enables or disables the option to use the ExtremeControl assessment agent.

Verification

1. From the Sophos interface, select **Users**. Create the user and enroll the device.

2. Connect to test the SSID and wait for the resynchronization poll to occur.
3. Verify that ExtremeControl has device information from Sophos in the **End-Systems** list.

Policy Configuration

To support the previous workflow, the device in an unregistered state must be able to communicate with the Sophos server (via HTTPS) and with Apple (via the Apple Push service).

Some configurations require downloading an agent to be registered by Sophos, so Google Play and Apple app store access must be provided also. If this is the case, policies must be configured to provide connectivity to the agent.

The following policies (or more generic ones) are required to allow Sophos registration:

- Allow HTTPS to Sophos network
- Allow TCP 5223 to 17.0.0.0/8:TCP:5223, Apple Push service
- Allow TCP/UDP 5228 to 173.194.0.0/16, Google Play login
- Allow HTTPS to 74.125.0.0/16, Google Play Downloads

Citrix XenMobile

The Citrix XenMobile (XenMobile) integration requires authentication credentials and the XenMobile server base URL. This information is used in the XenMobile module **Services** tab.

Module Configuration

The following tables describe the configuration options:

Service Configuration	Description
Username	Web service username.
Password	Web service password.
Server	Base URL of the XenMobile server. The base URL is used to create the web service URL. Example: *base URL*/xenmobile/api/v1/device/filter.

Service-Specific Configuration	Description
Poll interval	Time period between queries to the XenMobile web service.
End system group for managed business mobile devices	ExtremeControl end system group to which corporate-owned devices will belong.
End system group for managed personal mobile devices	ExtremeControl end system group to which personal devices will belong.
Default end system group for managed mobile devices	ExtremeControl end system group to which unknown devices will belong.
Remote wipe end system group	ExtremeControl end system group that will be used to remotely wipe a mobile device.
Enable remote wipe	Enables or disables the remote wipe option.
Update Kerberos username	Enables or disables the option to update an end system username.
Update device type	Enables or disables the option to update an end system device type.

Service-Specific Configuration	Description
Notify user when quarantined	Enables or disables the option to notify a user when an end system is quarantined based on assessment scoring.
Enable assessment	Enables or disables the option to use the ExtremeControl assessment agent.
Format of the incoming message	Format of the custom data string. Available fields are: *id* *serialnumber* *imei* *username* *ownership* *devicename* *devicemodel* *devicetype* *operatingsystem* *lastseen* *enrollmentstatus* *compliancestatus* *macaddress* *jailbroken*

Verification

1. Enroll a new device with XenMobile.
2. Connect to test the SSID, and wait for the resynchronization poll to occur.
3. Verify that ExtremeControl has the device information from XenMobile in the **End-System** list.

Policy Configuration

To support the previous workflow, the device in unregistered state must be able to communicate with the XenMobile server (via HTTPS) and with Apple (via the Apple Push service).

Some configurations require downloading an agent to be registered by XenMobile, so Google Play and Apple app store access must be provided also. If this is the case, policies must be configured to provide connectivity to the agent.

The following policies (or more generic ones) are required to allow XenMobile registration:

- Allow HTTPS to XenMobile network
- Allow TCP 5223 to 17.0.0.0/8:TCP:5223, Apple Push service
- Allow TCP/UDP 5228 to 173.194.0.0/16, Google Play login
- Allow HTTPS to 74.125.0.0/16, Google Play Downloads

Microsoft Intune

The Microsoft Intune (Intune) integration requires registering a Microsoft Azure (Azure) application. The Azure application acts as a proxy to execute REST API calls on behalf of ExtremeConnect. This information is used on the Intune module tab.

Module Configuration

The following table lists the configuration options for the Intune agent:

Agent Service Configuration	Description
Client ID	Application client ID.
Password	Application client secret.
Tenant	Tenant ID to retrieve specific customer devices.
Redirect URL	URL to which the user is redirected.
Code	Generated oAuth authorization code.

Service Configuration

The table below lists the configuration options for the MS Intune server.

Service-Specific Configuration	Description
Poll interval	Time period between queries to the Intune NAC web service.
End system group for managed business mobile devices	ExtremeControl end system group to which corporate-owned devices will belong.
End system group for managed personal mobile devices	ExtremeControl end system group to which personal devices will belong.
Default end system group for managed mobile devices	ExtremeControl end system group to which unknown devices will belong.
Update Kerberos username	Enables or disables the option to update an end system username.

Service-Specific Configuration	Description
Update device type	Enables or disables the option to update an end system device type.
Notify user when quarantined	Enables or disables the option to notify a user when an end system is quarantined based on assessment scoring.
Enable assessment	Enables or disables the option to use the ExtremeControl assessment agent.

Register Azure Application

An Azure application is required to access the Intune NAC API. The application requires permission from an administrator to access device information from Intune.

1. Log in to the Azure portal at https://portal.azure.com.
2. Select **Azure services > App registrations**.
3. To create a new application, select **New registration**.
4. On the **Register an application page**, enter the application name, type, and sign-on URL. The sign-on URL is used as a redirection page after the permissions are accepted. Select **Register**.

   The registration is created and displays on the **App Registrations** page.
5. From the **App Registrations** page, in the **Connect** row, note the Application (Client) ID that was generated after the registration. This is the ID that is used in the service configuration. In the following example, the Application ID is **4c88c31c-7c8e-4cc7-8948-abd4d0106b5c**.
6. From the **Display Name** list, select **Connect**.

   The **Connect** details page opens.
7. From the left menu, select **API permissions**. On the **API permissions** page that opens, select **Add a permission**. From the **Request API permissions** dialog that opens, select **Microsoft Graph**.

8. In the **Microsoft Graph** dialog, select **Delegated Permissions > DeviceManagementManagedDevices**. Enable **DeviceManagementManagedDevices.Read.All** and select **Add Permissions**.

9. On the **Connect > API Permissions** page, verify the permissions you created:

10. To generate the secret, select **Certificates and Secrets** from the left menu. Select **New Client Secret**. Edit the fields and select **Add**.

    In the following example, the description is set to **Secret**, the duration is set to expire in **2299**, and the generated secret is **/@T=mXIEhBQG2ODMhgDnxu[wle3p7Ha0**. The generated secret used in the service configuration.
    Note: The best practice is to set the duration to a lower value, such as one or two years.

    To copy the key to the clipboard, use the clipboard icon. To delete the key, use the trash icon.

11. To generate the oAuth authorization code, create a special authentication URL with an administrator account using the following format:

    ```
    https://login.microsoftonline.com/
    tenant/oauth2/v2.0/authorize?client_id=application
    ID&response_type=code&redirect_uri=redirect URL&response_
    mode=query&scope=openid offline_access
    DeviceManagementManagedDevices.Read.All&state=random
    generated ID
    ```

    Replace *tenant* with the tenant name used in the service configuration. In this example, the tenant is extremeconnect.onmicrosoft.com.

    Replace *application ID* with the application's ID. In this example, the ID is 4c88c31c-7c8e-4cc7-8948-abd4d0106b5c.

    Replace *redirect URL* with the URL that was configured in the application. In this example, the URL is https://nms.demo.com:8443.

    Replace *random generated ID* with any random string. In this example, the state is 12345.

Using the example values, the authorization URL with the application specific fields is:

https://login.microsoftonline.com/extremeconnect.onmicrosoft.com/oauth2/v2.0/authorize?client_id=4c88c31c-7c8e-4cc7-8948-abd4d0106b5c&response_type=code&redirect_uri=https://nms.demo.com:8443&response_mode=query&scope=openid offline_access DeviceManagementManagedDevices.Read.All&state=12345

12. Open a browser, enter the URL, and accept the authorization request.

13. After the request is accepted, the authorization code displays in the browser address field. Note the authorization code, which is the value between the code and state tags. The authorization code is used in the service configuration and expires in 10 minutes.

    In the example above, the full URL is as follows, with the authentication code in Bold text:

    https://nms.demo.com:8443/?code=**OAQABAAIAAABHh4kmS_aKT5XrjzxRAtHzDDNMGhrNMMTkKyCFCY-DJ0UNkr4ATgX8pRgOEA8Lo20Q73t5KZUe2b_pWA1XZaI2yUJin53XrS_ozXlN2btRw4rbVVvAz9M5aLVXLg5VmHBYV0_86Fz2SdaKvOa017PDiN1JgvZHjXwLva6baxvBEpVj1a8e7Tw68AhOo8IEmRycDuCWN1mrLp_Z-C9XTIqqPrnrOFx9__nfSpcrb23ZF7Ak5kEPUE5Tp7J-LPTFVlQpS99p4mbTZ26atey8cw439aO7uVopemFk8n2rfk_SHFSIIIPESkbjpYH6Oz8h53T6Q2UqiQLda2AYmX1qoJGEZbnAw65PdHHstK0PNX27bDry31zUD5CPOO7X76Q6_G6R91yqrWvu_Gq_N9moBIictsdVWxyb3dhKXIv3aMoBZkkurvfT8HDbS4lNsvNtqStJ5HWfInd5iCGbitMkD4LRI2zPmbnrvH5ItCFHvUhEeLsVQB_GY-OsyyC6x264JizBI2vu9pPKT5Ch0Mc8zNsX-7fYlOOgBTjdf15AaRV7sR2zqTSvFCuaeEr9RJA-ImrnFjIfzBccEnnNWxunbT2Wo-4YKgnn2wL-LX1wPr73iJpYVB6oUyiADJNtStVmI-ERDhaXoimPDieV8k4xfZrYIAA**&state=12345&session_state=fdb2c5b8-a316-4646-99e9-c16c329aed5a

14. From ExtremeControl, select the service configuration to view the code, which will be similar to the following example:

Verification

1. Enroll the device with Microsoft Intune.
2. Connect to the test SSID and wait for the resynchronization poll to occur.
3. Verify that the end system in ExtremeControl displays the device information from Intune.

Policy Configuration

To support the previous workflow, a device in an unregistered state must be able to communicate with the Intune server (via HTTPS) and with Apple (via the Apple Push service).

Some configurations require downloading an agent to be registered by Intune, so Google Play and Apple app store access must be provided. If this is the case, policies must be configured to provide connectivity to the agent.

The following policies (or more generic ones) are required to allow Intune registration:

1. Allow HTTPS to Microsoft Intune network.
2. Allow TCP 5223 to 17.0.0.0/8:TCP:5223, Apple Push service.
3. Allow TCP/UDP 5228 to 173.194.0.0/16, Google Play login.
4. Allow HTTPS to 74.125.0.0/16, Google Play Downloads.

Google G Suite

Combining the ExtremeControl solution with Google's G Suite helps network and security administrators ensure that only registered Chrome OS devices are able to use the network and its resources. The solution also pulls extensive device data from G Suite and updates the end systems in ExtremeControl to provide network administrators with a unique view of Chrome OS data within a single management interface.

The solution currently only support Chrome OS devices.

Module Configuration

The table below lists the configuration options for the Google G Suite agent.

Agent Service Configuration	Description
Service Account ID:	Email address of the service account to use for authentication. Locate your service account ID in your Google API Manager project (https://console.developers.google.com/projectselector/apis/credentials?pli=1) where you configured or created your service account. The service ID is part if the account details. Example: gsuiteserviceaccount2@extreme-gsuite-test.iam.gserviceaccount.com
Service Account User:	Email address of a user account from your G Suite account or domain. ExtremeConnect will connect to this domain. Example: kurt@extremetest.net

Service Configuration

The table below lists the configuration options for the Google G Suite server.

Service-Specific Configuration	Description
Poll interval:	The time period (in seconds) that the module will wait after each run. For example, if you want to run the synchronization once per hour, you can configure *3600* as the value.
Default end-system group for all devices from G Suite:	The default end system group name where all of the G Suite devices are assigned to in NAC. If you do not want end systems from G Suite to be assigned to this default group, configure a group name that does not exist in NAC or disable the group assignment feature on the ExtremeControl module. **Default:** Chrome Devices

Service-Specific Configuration	Description
Format of the incoming data for devices from G Suite:	Format of the data that gets stored in the custom data field. You can choose and combine any of the available variables: *nwAdapterType*, *mac*, *annotatedAssetId*, *annotatedLocation*, *annotatedUse*, *recentUsers*, *currentUser*, *deviceId*, *etag*, *firmwareVersion*, *kind*, *lastEnrollmentTime*, *lastSync*, *model*, *notes*, *orderNumber*, *orgUnitPath*, *osVersion*, *platformVersion*, *serialNumber*, *status*, *supportEndDate*, *willAutoRenew*. **Important:** G Suite might update the *lastSync* and *lastEnrollmentTime* values for each device regularly and ExtremeConnect calls the Extreme Management Center API to refresh that value in all end systems custom fields. Depending on your poll interval, this can put a lot of stress on the Extreme Management Center server. The best practice is not to use these variables in large environments. These variables can be used only if the poll interval is low (such as a few times per day) and the number of end systems is not high (below 1000). **Default:** user=#*currentUser*#, recentUsers=#*recentUsers*#, annotatedUser=#*annotatedUser*#, adapterType=#*nwAdapterType*#; OS=#*osVersion*#, firmware=#*firmwareVersion*#
End-system group for decommissioned devices:	The default end system group for devices that existed in G Suite but have been deleted. If you want to explicitly identify those devices and even authorize them differently (since they are no longer managed by G Suite and that could pose a threat), you can configure the group that they should automatically be moved to and enable the **Remove device from other device groups** feature. You must manually create this end system group in NAC.
Remove device from other groups on decommission:	Enable this to move devices that have been deleted from G Suite to the NAC end system group configured by the **End-system group for decommissioned services** option. If disabled, devices will not be automatically move to this group, but rather stay with their existing group memberships. **Default:** false
Delete custom data in XMC for decommissioned devices:	If a device is deleted in G Suite, the end system's custom data field in Extreme Management Center is cleared also. While this will keep your data clean in NAC, it can be helpful to still see the (old) G Suite data for the end systems that were previously managed by G Suite. **Default:** false
Overwrite the existing username with the one acquired from G Suite:	If this is set to *true*, the username for devices retrieved from G Suite will overwrite the username that is already in NAC. If no username can be retrieved from G Suite for a given end system, then no change is performed in NAC. **Important:** Setting this value to *true* can interfere with existing NAC processes if you are already retrieving and using the username through some other mechanism (such as 802.1X or Kerberos snooping) and the data will be overwritten. **Default:** false

Google APIs

You must create a service account in the Google APIs management site: https://console.developers.google.com

The service account provides ExtremeConnect with credentials that enable authentication and authorization against the Google Admin SDK that is used to pull data from your G Suite domain.

1. Access the API Console Credentials page: https://console.developers.google.com/project/_/apis/credentials
2. Select your project (or create a new one) from the drop-down list.
3. On the Credentials page, select the **Create credentials** drop-down list, and select **Service account key**.
4. From the **Service account** drop-down list, select an existing service account or create a new one.
5. For **Key type**, select the **P12** key option, and select **Create**.
   The file automatically downloads to your computer.
6. Rename the downloaded credentials file to **gSuiteCredentials.p12** and copy the file to your Extreme Management Center server (for example, using WinSCP) to this location: /usr/local/Extreme_ Networks/NetSight/wildfly/standalone/configuration/connect/gSuiteCredentials.p12
7. Navigate to the details for your newly created credentials. Note the **Client-ID** (number), as this will be needed later to authorize these credentials on your G Suite domain.

Google Administration

Prerequisites:

1. If not previously done, create a Google G Suite account and connect it with your domain. For test accounts, use: https://gsuite.google.com/signup/basic/welcome.
2. Authorize the ExtremeConnect application to provide it with access to your domain and two scopes. The basic process is described at https://developers.google.com/identity/protocols/OAuth2ServiceAccount?#delegatingauthority
3. To delegate domain-wide authority to a service account, first enable domain-wide delegation for an existing service account in the Service accounts page (https://console.developers.google.com/permissions /serviceaccounts), or create a new service account

(https://developers.google.com/identity/protocols/OAuth2ServiceAccount?#creatinganaccount) with domain-wide delegation enabled.

To configure the G Suite domain:

1. As an administrator, access the G Suite domain Admin console.
2. Select **Security** from the list of controls. If you do not see Security listed, select **More controls** from the gray bar at the bottom of the page, and then select **Security** from the list of controls. If you cannot see the controls, verify that you are signed in as an administrator for the domain.
3. Select **Show more > Advanced settings**.
4. From the Authentication pane, select **Manage API client access**.
5. For **Client Name**, enter the service account's Client ID. You can find the client ID on the Service accounts page.
6. For **One or More API Scopes**, enter the list of scopes that your application should be granted access.
7. Enter these two scopes for the API client that you authorize for ExtremeConnect:

   https://www.googleapis.com/auth/admin.directory.device.chromeos
   https://www.googleapis.com/auth/admin.directory.user.readonly

   The first one allows ExtremeConnect to view and manage your Chrome OS devices' metadata, and the second one allows ExtremeConnect to view users on your domain.
8. Select **Authorize**.
9. Enable **domain-wide authority delegation** as described in the link previously.

User Privileges

Verify that the configured user is configured to have at least the privileges to manage Chrome OS devices as shown below. This privilege is needed to retrieve data on Chrome OS devices.

Verification

Verify that data from all devices managed by G Suite is imported to ExtremeControl. On the **Connect** tab, view the end system table that displays the custom data field that you configured for the G Suite module. (You might need to make the corresponding column

visible first.) If you enabled the corresponding features, you should also see the username retrieved from G Suite.

If you created and configured an end system group for all devices managed in the G Suite module, verify whether all devices managed by G Suite have been assigned to that end system group in ExtremeControl.

Deleting G Suite Devices

To test this workflow, remove the provisioning of a device from G Suite and wait for the next ExtremeConnect synchronization. Then verify the following:

1. The device's custom field has been emptied (if this feature has been enabled in the configuration file).
2. The device is now member of the NAC end system group for decommissioned devices (if this feature has been enabled).
3. The device does not display in the end system list that is located at the bottom of the ExtremeConnect management web site (**G Suite** tab). This means that the device has been deleted in the internal list as well.

Management / IT Operations Configuration

FNT Command

The FNT Command (Command) integration provides two main functions:

- Mapping the patch panel information from Command to end systems and switch ports in Extreme Management Center and ExtremeControl. Data in Extreme Management Center is enriched for each end system and provides comprehensive reporting capabilities within OneView.

- Exporting the Extreme Management Center data to FNT Command. This exports all of the switches, their modules, ports, GBICs, and connected end systems to Command's ADG database.

Module Configuration

The following tables describe the configuration options available for the FNT Command module (configuration file: FNTCommandHandler.xml).

Configuration Option	Description
Username	Username to connect to the Command Oracle DB.
Password	Password to connect to the Command Oracle DB.
Server IP	IP address of the Command Oracle DB.
Server Port	TCP port of the Command Oracle DB. **Default:** 6201
Command Service Name	The *SERVICE_NAME* to access the Oracle DB view (table) named medmgr.CTFL2D_SWITCH_2_OUTLET. Contact your Oracle DB administrator to get the service name specific to your FNT Command installation.

General Module Configuration	Description
Poll interval in seconds	The time period (in seconds) that the module waits after each run. Since the data on patch field connections or locations is relatively static, the data often does not require updating every 60 seconds. The best practice is to increase the poll interval value to 3600 seconds (once per hour), depending on the size of your infrastructure and requirements. This also decreases the processing load on the Extreme Management Center server.
Module log level	Verbosity of the module. Logs are stored in the Extreme Management Center server.log file.
Module enabled	Whether the module is enabled.
Push update to remote service	If this is set to *true*, the data from other modules is pushed to the service.
Update local data from remote service	If this is set to *true*, the data from the remote service is used to update the internal end system table.
Default end-system group	The default end system group name to use if it is not set dynamically.

General Module Configuration	Description
Enable Data Persistence	Enabling this option forces the module to store end system custom field data and group membership data in a file after each cycle. If this option is disabled, the module forgets all of the data after a service restarts. However, to clean existing data, the corresponding .dat files must be deleted. **Important:** The best practice is to enable this feature, especially in large environments, so that ExtremeConnect does not need a full resynchronization of the data every time you restart the Extreme Management Center server. **Default:** true

Service-Specific Configuration	Description
Custom field to use	Number of the custom data field for each end system to store the data retrieved from Command. **Valid values:** 1 - 4 **Default:** 1
Format of the incoming data	Format of the data that gets stored in the custom data field. Available variables: *outletId* (ID of the patch field) *outletCampus* *outletBuilding* *outletFloor* *outletRoom* **Default:** #*outletId*# / #*outletCampus*# / #*outletBuilding*# / #*outletFloor*# / #*outletRoom*#
Update NAC End-Systems with Command outlet data	If this is set to *true*, the module retrieves outlet data (such as outlet ID, room, and building) and maps it to the corresponding end systems and ports in NAC.
Command DB table name containing outlet data for NAC import	The name of the Oracle DB table that contains the Command outlet data. This is required if you enable the feature *update_nac_endsystems_with_command_outlet_data* so that ExtremeConnect knows which table to query to retrieve data about ports and their outlet data. **Default:** medmgr.CTFL2D_SWITCH_2_OUTLET

Service-Specific Configuration	Description
Push NetSight Devices to Command Auto-Discovery Gateway	If this is set to *true*, the module pushes Extreme Management Center switch data (such as IP, firmware, type, and descriptor) to Command Auto-Discovery Gateway. The module updates the corresponding database tables. Auto-Discovery Gateway manages the import of the data to Command automatically.
Push NAC End-Systems to Command Auto-Discovery Gateway	If this is set to *true*, the module pushes all NAC end systems to Command Auto-Discovery Gateway. It then tries to connect these end systems to switches and ports exported from Extreme Management Center. This option is available only if the option push_netsight_devices_to_ command_adg has been enabled also. The module updates the corresponding database tables. Auto-Discovery Gateway manages the import of the data to Command automatically.
Autodiscovery Gateway DB TCP Port	The TCP port on which the Auto-Discovery Gateway database is running. **Default:** 1521
Autodiscovery Gateway DB Username	The username to connect to the Auto-Discovery Gateway database. **Default:** command
Password	Password used to connect to the Auto-Discovery Gateway database. **Default:** command
The Map to use when exporting NetSight/NAC data to Command's ADG	Specify the map to use to export Extreme Management Center (switches) and NAC (end systems) data to ADG. The map must be configured correctly for ADG to properly map the incoming device types to existing, well-known device types. **Default:** 1
Automatically process NetSight data pushed to ADG	If this is set to *true*, the module automatically calls the AutomatedProcessomg.sh script at the end of each synchronization cycle. This triggers the ADG to immediately import the new data from Extreme Management Center. This option is supported on ADG Linux installations only.
Username to connect to the ADG server via SSH and execute automated processing script	The username to connect to the ADG server via SSH and execute the AutomatedProcessing.sh script. Make sure the user has permissions to log in remotely via SSH and has the necessary privileges to execute the script located in your Apache Tomcat folder under /webapps/command/axis/WEB-INF. This is relevant only if the option *adg_enable_automated_processing* is enabled.

Service-Specific Configuration	Description
Password to connect to the ADG server via SSH and execute automated processing script	The password to connect to the ADG server via SSH and execute the AutomatedProcessing.sh script. This is relevant only if the option *adg_enable_automated_processing* is enabled.
Username for the automated processing script (Command user)	The Command username to use as a parameter for the AutomatedProcessing.sh script. Make sure the user has the necessary privileges in Command to perform the changes that the script triggers. This is relevant only if the option *adg_enable_automated_processing* has been enabled.
Password for the automated processing script (Command user)	The Command password to use as a parameter for the AutomatedProcessing.sh script. This is relevant only if the option *adg_enable_automated_processing* has been enabled.
Tenant (=Mandant) ID for the automated processing script (Command tenant)	The Command tenant (=Mandant) to use for the user provided previously. This will be used as a parameter for the AutomatedProcessing.sh script. This is relevant only if the option *adg_enable_automated_processing* is enabled.
User group ID for the automated processing script (Command user group name)	The name of the Command user group to use for the user provided previously. This will be used as a parameter for the AutomatedProcessing.sh script. This is relevant only if the option *adg_enable_automated_processing* is enabled.
Full file path on the ADG server for the script to trigger automated processing	The full file path (path and file name) of the AutomatedProcessing.sh script. This script will be triggered on the ADG server via SSH to start the data import automatically. This is relevant only if the option *adg_enable_automated_processing* is enabled. **Default:** /usr/share/tomcat7/webapps/command/axis/WEB-INF/AutomatedProcessing.sh
Maximum number of end-systems per web service request to NetSightExtreme Control CenterExtreme Management Center	The maximum number (as an integer) of end systems that Fusion will query per request from the Extreme Management Center server. This setting lets you split large end system queries into smaller batches. Example: There are 10,000 end systems in Extreme Management Center and ExtremeControl. You set this *max_endsystem_per_request* value to 1000. Fusion will perform 10 calls to the Extreme Management Center API and retrieve 1000 end systems per call. **Default:** 1000.

Service-Specific Configuration	Description
Timeout per web service request to NetSightExtreme Control CenterExtreme Management Center	The timeout interval (in seconds) for each web service call to Extreme Management Center and ExtremeControl. Since these calls are handled by the TaskScheduleHandler, you must calculate a value as follows: Take the setting for *poll_interval_seconds* from your TaskScheduleHandler.xml config file, and add a couple of seconds for the expected time it takes for the HTTP transaction to complete. Example: 3 seconds for the poll interval for the TaskScheduleHandler plus a timeout of 7 seconds for the HTTP request to be performed equals 10 seconds for the transaction completion. **Default:** 10
The ID of the tenant to query Command outlet data for	The Command tenant ID (Mandant ID) that will be used to filter Command outlet data. This helps reduce the amount of data that ExtremeConnect must process when importing the Command outlet data and matching it to end systems in NAC. This is relevant only if the option *update_nac_endsystems_with_command_outlet_data* is enabled.
Default username for switch CLI access	The default username to connect to any switches that do not have CLI credentials stored in Extreme Management Center. This username is used only if there are no CLI credentials defined for a switch in Extreme Management Center. Otherwise, the Extreme Management Center CLI username takes priority. This is used to gather port optic information from ExtremeXOS switches using a Telnet connection.
Default password for switch CLI access	The default password to connect to any switches that do not have CLI credentials stored in Extreme Management Center. This password is used only if there are no CLI credentials defined for a switch in Extreme Management Center. Otherwise, the Extreme Management Center CLI password takes priority. This is used to gather port optic information from ExtremeXOS switches using a Telnet connection.

Verification

1. Log in to OneView.
2. Verify the incoming data from FNT Command in the custom data field in the end system table.

3. Pick a few end systems and validate that their location data in the NAC's custom field is correct according to Command data.

Glue Networks Gluware Control

The Gluware Control integration provides the option to publish policy domain configuration to Gluware. The policies are translated into ACL definitions that can be deployed to managed nodes from different manufacturers.

Module Configuration

The following tables describe the configuration options available for the Gluware Control module (configuration file: GlueNetHandler.xml)

Configuration Option	Description
Username	Username used to connect with Gluware Control.
Password	Password used to connect with Gluware Control.
Webservice URL	Webservice URL of Gluware Control.
Company	Tenant company name.
Organization	Tenant organization name.

General Module Configuration	Description
Poll interval in seconds	The time (in seconds) the module waits after each run. Since the data on patch field connections or locations is relatively static, it often does not require updating every 60 seconds. The best practice is to increase the value for the poll interval, if possible, to 3600 seconds (once per hour), depending on the size of your infrastructure and your requirements. Reducing the poll interval decreases the processing load on the Extreme Management Center server.
Module log level	Verbosity of the module. Logs are stored in the Extreme Management Center server.log file.
Module enabled	Whether the module is enabled.
Push update to remote service	If this is set to *true*, the data from other modules is pushed to the service.
Update local data from remote service	If this is set to *true*, the data from the remote service is used to update the internal end system table.

General Module Configuration	Description
Default end-system group	The default end system group name to use if it is not set dynamically.
Enable Data Persistence	Enabling this option forces the module to store end system custom field and group membership data in a file after each cycle. If this option is disabled, the module forgets all of the data after a service restarts. However, to clean existing data, the corresponding .dat files must be deleted. **Important:** The best practice is to enable this feature, especially in large environments, so that ExtremeConnect does not need a full resynchronization of the data every time you restart the Extreme Management Center server. **Default:** true

Service-Specific Configuration	Description
Naming Convention	Only policy roles matching the naming convention format will be published (.+ for all).
Provision Switches	Automatically provision (configure) switches on an enforce operation.
Switches	Name of switch nodes to provision. Semicolon delimited.

The module publishes every policy domain to Gluware Control that has a matching jboACL object name. (For example, to publish Default Policy Domain, create a new jboACL with the name Default Policy Domain).

After the data is published, the description of the ACL is changed to Created by ExtremeConnect and contains an access list for every policy role that is present in the policy domain.

NOTE: Support for policy rules depends on the underlying switch hardware. Gluware Control only supports L3-L4 IP policy rules with Accept and Deny actions, and only those will be published from the policy domain.

Cisco ACL Support in NAC Manager

To use an ACL in conjunction with a RADIUS NAC request, the RADIUS response parameters must be adjusted for use with Cisco switches. Certain switch models might require specific licenses to enable per user ACL and dynamic ACL support. For additional requirements, see the vendor documentation.

When adding a Cisco switch in NAC Manager:

1. Enable the **Gateway RADIUS Attributes to Send** option, and select **Edit RADIUS Attribute Settings** from the drop-down list.
2. To create a new profile, select **Add** and name the profile Cisco Wired Dynamic ACL & VLAN ID. Create the Attribute Definition as follows:

   This sends the ACL name and the VLAN ID to the switch upon authorization.
3. Open the Policy Mapping panel in OneView by selecting **Control** > **Identity & Access** > **I&A Configurations** > **I&AProfiles** > **Policy Mappings** > **Default**. Map the policy to the desired VLAN.
   Note: The Contain to VLAN action is not supported in IP ACLs, so VLAN assignments must be managed using RADIUS attributes in this case.
4. Continue with the regular NAC configuration steps to assign profiles using rules.

Verification

1. Log in to Gluware Control, and select **Domain Objects** > **jboAcls**.
2. Select the ACL that matches the policy domain in Extreme Management Center and verify that the access lists match with the policy roles.
3. If automatic provisioning is not enabled (which would publish the ACLs automatically), you must deploy the ACLs to the switches manually.

To verify the configuration on a switch:

1. Select **Nodes** > **lanSwitch** and connect to the desired switch.
2. To present default ACLs, Gluware creates one ACL matching the policy role in name with all rules below it. Look for the rule to verify it. The rule precedence matches with the default precedence found in ExtremeControl.

Microsoft System Center Configuration Manager

The Microsoft System Center Configuration Manager (SCCM) integration is a one-way integration that retrieves end system data from SCCM on managed devices. This data enriches each end system data set Extreme Management Center and provides comprehensive reporting capabilities in OneView.

NOTE: The SCCM server requires an adapter agent to be installed and configured before enabling the corresponding module in ExtremeConnect. The adapter file is provided by Extreme Networks.

Module Configuration

The following tables describe the configuration options available for the SCCM ExtremeConnect module (configuration file: SCCMHandler.xml).

Service Configuration	Description
Adapter IP	IP address of the SCCM adapter.
Adapter Port	Port on which the SCCM adapter is listening.
Pre-Shared Key	The pre-shared key used to communicate with the SCCM adapter.

General Module Configuration	Description
Poll interval in seconds	Number of seconds between connections to the adapter running on the SCCM server.
Module log level	Verbosity of the module. Logs are stored in the Extreme Management Center server.log file.
Module enabled	Whether the module is enabled.
Update local data from remote service	If this is set to *true*, the data from the remote service is used to update the internal end system table.
Default endsystem group	The default end system group name in NAC to assign all MAC addresses found in SCCM. Use a non-existing group name if you do not want this module to assign all SCCM MAC addresses to any NAC end system group.
Enable Data Persistence	Enabling this option forces the module to store end system data and end system group data to a file after each cycle. If this option is disabled, the module forgets all of the data after a service restarts. However, to clean existing data, the corresponding .dat files must be deleted.

Service-Specific Configuration	Description
Custom field to use	The custom field in Extreme Management Center to update the information for end systems retrieved from the adapter running on the SCCM server. **Valid values:** 1-4

Format of the incoming data	The format of the data that is received from the adapter running on the SCCM server and written to the custom field.
	
	Syntax example:
	
	`Netbios Name=#netbiosName#;`
	`User=#lastLogonUserDomain#\#lastLogonUser#;`
	`OS=#operatingSystem# (#servicePack#);`
	`Manufacturer=#computerManufacturer#`
	`Model=#computerModel#`
	
	Available Variables:
	
	path
	mac
	netbiosName
	lastLogonUserDomain
	lastLogonUser
	operatingSystem
	servicePack
	computerManufacturer
	computerModel

Overwrite the existing username with the one acquired from SCCM	If this is set to *true*, the username retrieved from SCCM overwrites the username that is already in NAC. If no username can be retrieved from SCCM for a given end system, then no change is performed in NAC. **Important:** This can interfere with existing NAC processes if you are already retrieving and using the username through some other mechanism (such as 802.1X or Kerberos snooping), and this username will be overwritten.

Service-Specific Configuration	Description
Overwrite the existing device type with the one acquired from SCCM	If this is set to *true*, the device type (Windows operating system) retrieved from SCCM overwrites the device type that is already in NAC. If no operating system can be retrieved from SCCM for a given end system, then no change is performed in NAC. **Important:** This can interfere with existing NAC processes if you are already retrieving and using the device type through some other mechanism (such as DHCP snooping) and the device type will be overwritten. However, in most cases this feature can improve your current method (at least for Windows machines managed by SCCM) since the quality of the information retrieved from SCCM is usually good.
End-system group for decommissioned devices	The default end system group for decommissioned devices.
Remove device from other groups on decommission	Enable this to remove a device from all other groups when it is moved to the decommissioned group.
Delete custom data in XMC for decommissioned devices	If a device is deleted in SCCM, the end system's custom data field in Extreme Management Center is cleared.
Enable assessment for software updates	If enabled, ExtremeConnect processes any missing software updates for each SCCM computer and adds the corresponding data to the ExtremeConnect assessment service, where it can be used by NAC to assess the end system and generate health results. **Default:** disable
Max age for Software Updates	SCCM provides a start date for each missing software update, which indicates the date and time this update was available to the computer. ExtremeConnect calculates the difference from that start date until now (as the number of days). If that difference exceeds the number configured through this option, ExtremeConnect sets a higher risk value to the associated assessment test set and sets the corresponding test set value to Not Compliant. This can be used to quarantine end systems that have not installed software updates for *X* number of days. A configured value of 0 disables this feature. **Default:** 0
Re-Assess end-systems due to changed software update status	If end systems get assessed based on their missing software updates and there is a change in compliance status (either it has been compliant before and is now non-compliant or vice versa), this feature tells NAC to immediately reauthenticate and reassess these end systems. This allows the fast quarantine of end systems that become non-compliant and gets end systems out of quarantine that previously have been non-compliant. Only applicable if the options *Enable assessment for software updates* and *Max age for Software Updates* are also enabled or configured. **Default:** disable

Service-Specific Configuration	Description
HTTP Socket Timeout	Timeout (in seconds) for the HTTP socket connection to the SCCM adapter. If you regularly see *Read timed out* error messages in your server.log, then it can be helpful to increase the default value for this option. **Default:** 30
HTTP Connect Timeout	Timeout (in seconds) for the HTTP CONNECT access to the SCCM adapter. If you regularly see *connect out* error messages in your server.log, then it can be helpful to increase the default value for this option. **Default:** 30

Adapter Installation

ExtremeConnect retrieves data from an SCCM server using an adapter. This adapter must be installed and configured before enabling the corresponding module in ExtremeConnect. The adapter consists of a Java executable file (.jar) and a configuration file. There is currently no dedicated installer for the adapter. The best practice is to follow these steps to install the adapter manually:

On the SCCM server:

1. Create a user account that the Extreme Networks adapter can use to access data on the SCCM server.
2. Provide at least the Collection Class **Read** and **Read resource** access rights to this user account:

3. Install the latest Java Runtime Environment (JRE).
4. The SCCM adapter is provided as a zip file (ConnectSccmAdapter_ v<version>.zip). Copy the file to your SCCM server and extract it to any folder. The best practice is to create and use a dedicated folder to copy the files to. Example: C:\Program Files\Extreme Networks\SCCM Adapter

   The files contained in the zip file are:

   ConnectSccmAdapter-2.0.2.jar - The actual adapter, executable jar file that runs both the data manager and the web service.

   ConnectSccmAdapter.config - The configuration file.

   log4j.properties - The log configuration file. There is no need to use this file as you will configure the log level through the main configuration file listed previously.

5. Start the adapter by double-clicking the ConnectSccmAdapter-2.0.2.jar fie or running it in a shell using java -jar ConnectSccmAdapter-2.0.2.jar.
6. Verify that the log file was created. It should be in the same folder where the .jar file is located.
7. Verify that the adapter automatically starts when the server starts up.

Adapter Configuration

The following table lists the configuration options for the SCCM agent:

Configuration Option	Description
LOG_LEVEL	Set the log level of the adapter to one of the following values: ERROR, WARN or DEBUG. **Default:** WARN
IP	IP address for the web service (=agent) to listen on.
PORT	TCP port for the web service to listen on. **Important:** This port must *not* be used by any other application on this server.
SCCM_SERVER	The DNS name of the Configuration Manager server to connect to. This has only been tested with this adapter and the SCCM server running on the same server, although remote connections might work also.
SCCM_SITE_CODE	The name of the site to connect to in Configuration Manager. Example: SCCM_SITE_CODE=*mysite*
SLEEP_INTERVAL	Set the sleep interval in seconds. The main adapter updates all of the computer data from SCCM and then sleeps for this number of seconds before running the next update to retrieve the latest data.
PRE_SHARED_KEY	The pre-shared key used for the communication between the adapter and ExtremeConnect. This must match the key entered when installing the ExtremeConnect module.
IS_PRE_SHARED_ KEY_ENCRYPTED	If this is set to *false*, the adapter assumes that the PRE_SHARED_ KEY configured previously is not encrypted, and on the first start the adapter will automatically encrypt the key and set this value to *true*. If you want to change this key at a later stage, change the pre-shared key, set this value back to *false*, and restart the adapter service.
QUERY_SMS_G_ SYSTEM_FOR_MAC_ ADDRESSES	If enabled, queries MAC addresses from the SMS_G_SYSTEM table and the SMS_G_System_NETWORK_ADAPTER table. Sometimes MAC addresses are listed in SMS_G_SYSTEM, but not in SMS_G_System_NETWORK_ADAPTER, and this feature will import those MAC addresses also (although they cannot be filtered by type, so they will be imported without further validation).

Configuration Option	Description
RETRIEVE_DEVICE_ SOFTWARE_UPDATES	If enabled, retrieves pending (available but not yet installed) software updates (patches) for each managed computer in SCCM. This data can be used by ExtremeConnect as assessment results for Extreme Management Center. It will be visible in the Health Results section, per end system, and can be used to quarantine end systems.
NR_OF_PINGS_FOR_ CONNECTIVITY_ TEST_TO_RETRIEVE_ SOFTWARE_UPDATES	When the feature to retrieve missing software updates is enabled, the adapter runs two actions (a ping test and a WMI connectivity test) before actually trying to retrieve the software update data. This configuration option lets you configure the number of pings used in the ping test. Usually, one ping is sufficient. If this is not enough for your network, you can increase this number. However, the higher the number of pings, the longer it takes for connectivity tests and the longer the overall processing time to gather missing software updates.
POWERSHELL_ TIMEOUT_ RETRIEVING_ SOFTWARE_UPDATES	The timeout (in seconds) for each Powershell command that tries to retrieve the next batch of missing software updates from all managed computers. If the configured timeout is reached, the underlying process is destroyed. **Important:** Setting this value to 0 will disable any timeout, but in customer environments the WMI query hung up the powershell process indefinitely when this option was disabled. The best practice is to configure this value properly. Note that you must increase the timeout if you increase any of the following configuration parameters, as they influence the overall processing time for the Powershell command: NR_OF_COMPUTERS_TO_PROCESS_AT_ONCE_WHEN_ RETRIEVING_SOFTWARE_UPDATES NR_OF_PINGS_FOR_CONNECTIVITY_TEST_TO_ RETRIEVE_SOFTWARE_UPDATES If you keep the number of pings for the connectivity test to the default *1* and the batch size of computers to process at once at the default *10* , a timeout of about 100 seconds will likely work.

Verification

To verify that the data on Windows-based end systems can be retrieved from SCCM:

1. Check the custom field in the NAC end system table and verify that you can see data, such as the netbios name, username, detailed operating system information, and so on.

2. If enabled, you will see a more detailed operating system information in the Device Type column.
3. If enabled, you will see the last logged on use information in the Username column.

Aruba ClearPass

Combining the Extreme Management Center solution with Aruba ClearPass (Clearpass) lets network administrators automatically import end systems from ClearPass into Extreme Management Center. This solution is mainly used for environments where customers want to deploy:

- ExtremeAnalytics and enhance it with end system data from NAC, but have already invested in ClearPass
- Extreme Management Center as their overall network management solution and pull end system data from their existing ClearPass environment

The solution pulls end system data from ClearPass and uses it to create and update end systems in Extreme Management Center. It also assigns the imported MAC addresses to end system groups in Extreme Management Center based on custom end point attributes from Clearpass.

ExtremeAnalytics can then be configured to synchronize the username and device type into its flow and application data, therefore increasing its overall value.

NOTE: Mapping end system data from ClearPass to flow data in ExtremeAnalytics requires a correctly configured IP resolution in ClearPass, since the mapping is done based on the end system's IP address.

Module Configuration

The following tables describe the configuration options available for the Aruba ClearPass module (configuration file: ArubaClearpassHandler.xml).

Service Configuration	Description
Server	IP address of the Aruba ClearPass server.
Port	Port of the Aruba ClearPass server API service – usually 443.

Service Configuration	Description
Access-Token	The HTTP authorization token, which is located after the Bearer part of the HTTP authorization header. Example: Bearer 01279b5134e633f8df3a36b145657f4f35133f16 **Note:** To generate the token, see the corresponding procedure that follows these configuration options tables.

General Module Configuration	Description
Poll interval in seconds	Number of seconds between connections to the Aruba ClearPass server.
Module log level	Verbosity of the module. Logs are stored in the Extreme Management Center server.log file.
Module enabled	Whether or not the module is enabled.
Update local data from remote service	If this is set to *true*, the data from the remote service is used to update the internal end system table.
Default endsystem group	The default end system group name in NAC to assign all MAC addresses found in ClearPass. Use a non-existing group name if you do not want this module to assign all ClearPass MAC addresses to any NAC end system group.
Enable Data Persistence	Enabling this option forces the module to store end system data and end system group data to a file after each cycle. If this option is disabled, the module forgets all of the data after a service restarts. However, to clean existing data, the corresponding .dat files must be deleted.

Service-Specific Configuration	Description
Custom field to use	The custom field in Extreme Management Center to update the information for end systems retrieved from ClearPass. **Valid values:** 1-4

Service-Specific Configuration	Description
Format of the incoming data	Format of the data that gets stored in the custom data field. Syntax: `user=#user#, domain=#domain#, online=#online#, updatedAt=#updatedAt#, roles=#roles#` Available variables from Aruba Clearpass: *ipAddress* *user* *domain* *spt* *deviceCategory* *deviceFamily* *deviceName* *online* *updatedAt* *roles*
HTTP socket timeout in seconds (Clearpass API)	The timeout interval (in seconds) for all HTTP connection sockets to the Clearpass API. Allows the HTTP client to timeout the established connection if there is no response from the ClearPass server after the configured number of seconds.
Enable device type overwrite	Enable this to use the device family or type retrieved from ClearPass to overwrite the device family or type in ExtremeControl.
End-system group for decommissioned Clearpass end-points	If an end point gets deleted from Clearpass, its corresponding end system will be pushed to this end system group.
Remove end-systems from other groups on decommission	Enable this to remove a device from all other groups when it is moved to the decommissioned group.
Delete custom data in XMC for decommissioned devices	If an end point gets deleted from Clearpass, the corresponding end system's custom data field in Extreme Management Center will be cleared.
XMC Server	Hostname or IP of the Extreme Management Center server. Required to import Clearpass end points.
XMC Port	HTTPS port of the Extreme Management Center service. **Default:** 8443

Service-Specific Configuration	Description
XMC Username	Username to connect to the Extreme Management Center server.
XMC Password	Password to connect to the Extreme Management Center server.
IP of primary NAC appliance	The Extreme Management Center API that ExtremeConnect uses to create and update end systems requires the existence of at least one NAC appliance. Although you do not have to use this NAC appliance for anything, it must still be installed and configured in Extreme Management Center. Provide this NAC appliance's IP address in this configuration parameter.
Assign the NAC end-system group based on an end-point attribute	If enabled, ExtremeConnect will not assign all end points from Clearpass to the same catch-all group in NAC. Instead, it will read the configured *Name of end-point attribute for group assignment value* and try to use that attribute's value to choose the NAC end system group to assign the MAC to in Extreme Management Center.
Names of Clearpass end-point attributes to use for NAC group assignment	List of the end point attributes (comma delimited) to use for NAC group assignment. When importing an end point, ExtremeConnect evaluates its list of attributes against this configured list and tries to find the first configured attribute name. If found, it uses the value of that attribute for the end system group assignment in NAC. If not found, tries to find the second of the configured attribute names and so on.
Regex's to parse the value of the Clearpass end-point attribute to use for NAC group assignment	Define a list of regular expressions that parse the value of the configured Clearpass end point attribute. The parsing result is used as the final name of the Extreme Management Center NAC end system group to assign the MAC address to. If an empty regex value is configured, the regex parsing is disabled and ExtremeConnect will use the full value as imported from Clearpass. This list must have exactly the same number of items (regex's) as the configured list of attribute names.
Full Sync Interval	The time period after which a full data resynchronization will be performed. This synchronization updates both the full end system objects and the group memberships.
End-System Group Sync Interval	The time period after which an end system group synchronization is performed. This only updates the end system group (MAC addresses) memberships on Extreme Management Center. It does not create or update the end system objects.

Service-Specific Configuration	Description
Run full sync at specific times	Enable this option if you want full synchronizations to occur only at configured times of the day. Configure the list of those times using the option *Full Sync Times*. Ensure your configured *Poll interval in seconds* is set to a low number (such as 60 seconds) since ExtremeConnect only performs a full synchronization if the time of the day is after one of the configured full synchronization times. If disabling this option, ExtremeConnect will run full synchronizations regularly according to the configured *Full Re-Sync Interval* value.
Full Sync Times	List of the times of day (using a 24-hour clock) at which ExtremeConnect will perform a full synchronization. Format Example: 05:00;23:00
Auto-create end-system groups in XMC	Enable this option if you want ExtremeConnect to automatically create MAC-based end system groups based on attribute values from Clearpass. This option is only relevant if the option *Assign the NAC end-system group based on an end-point attribute* is enabled. ExtremeConnect imports the end point attribute values from Clearpass and verifies whether there is an Extreme Management Center end system group for each of them. If not, it automatically creates the corresponding group.

Generate an Access Token

To generate and access token:

1. Log in to Aruba ClearPass Guest.
2. Select **Administration > API Services > API Clients**.
3. Select **Create an API Client**. Use these settings:
   Enabled: trueOperator
   Profile: Read-Only
   AdministratorGrant Type: Client Credentials
   Access Token Lifetime: Choose a high value (long lifetime). Example: 52 weeks
4. Select **Create API Client**.
   The new client configuration is shown in a list.
5. Select the list item and select **Generate Access Token**.
6. Copy the HTTP authorization token, which is located after the Bearer part of the HTTP authorization header.
   Example: Bearer 01279b5134e633f8df3a36b145657f4f35133f16

Configure NAC and ExtremeAnalytics Integration

To enable the feature that exchanges ExtremeControl data with flow data:

1. Select **Configuration > Engines > ClearPass hostname > Configuration**.
2. Select the **Enable Access Control Integration** checkbox:

Verification

The end system data from ClearPass will be visible in the Extreme Management Center end system list and the ExtremeAnalytics flow data.

In the end system table, you should see data on all ClearPass end systems in the configured custom field:

You will also see usernames and device types if they are available through ClearPass.

Additionally, as soon as the user and device type fields for ClearPass sourced end systems have been updated in Extreme Management Center, you should start seeing that information in the ExtremeAnalytics **Application Flows** tab:

Convergence Configuration

Microsoft Skype For Business

The Microsoft Skype for Business (formerly known as Microsoft Lync) integration provides dynamic call prioritization and comprehensive reporting capabilities in OneView.

Before installing and configuring the ExtremeConnect integration for Skype for Business:

1. Install the Skype for Business SDN API, which can be retrieved from Microsoft: http://www.microsoft.com/en-us/download/details.aspx?id=44274
2. Point the Skype for Business SDN management service to your Extreme

Management Center server (where ExtremeConnect is installed).

3. Read the corresponding solution guide for further details.

Module Configuration

The following tables describe the configuration options.

Service Configuration	Description
Skype for Business SDN Management Service IP	IP address of the Skype for Business SDN management service.

General Module Configuration	Description
Poll interval in seconds	The time period the module will wait during each run. **Caution:** During each run (cycle) the module performs various steps, some of which put an extra load on the Extreme Management Center server. The best practice is to avoid setting this value below 600 seconds (=10 minutes). The larger the Extreme Management Center environment (=number of NAC end systems, switches, access points, and so on) the higher this value should be. However, setting this value too high (such as 7200 seconds = 2 hours) will prevent administrators from being able to analyze call reports for up to 2 hours before those calls have ended.
Module log-level	Verbosity of the module. Logs are stored in the Extreme Management Center server.log file.
Module enabled	Whether the module is enabled.
Enable Data Persistence	Enabling this option forces the module to store end system data to a file after each cycle. If this option is disabled, the module forgets all of the data after a service restarts. However, to clean existing data, the corresponding .dat files must be deleted.

Service-Specific Configuration	Description
Custom field to use	This field is not yet used by this integration, so keep it set to the default of 1. (Valid values will be 1 - 4.)
NetSight Request Timeout	Timeout in seconds the module waits until it declares that a web service call to Extreme Management Center has timed out.

Service-Specific Configuration	Description
Time to wait for a quality update from Skype for Business	When a Skype for Business call finishes, Skype for Business sometimes sends a *QualityUpdate* request shortly after the end of the call and the call quality information from this message is retrievable. This timeout value defines the minimum number of seconds the module waits before it declares that a call has fully ended (with or without the existence of *QualityUpdate* information).
Enable audio call prioritization	Enable this to prioritize audio streams (connections or flows) for all Skype for Business calls when possible. If this is disabled, no audio streams for any Skype for Business call will be prioritized, whether via XAPI or ODL. You can still access the OneView reports, but no dynamic ACLs or QoS profiles will be created in the infrastructure for the audio flows. **Default:** true
Enable video call prioritization	Enable this to prioritize video streams (connections or flows) for all Skype for Business calls when possible. If this is disabled, no video streams for any Skype for Business call will be prioritized, whether via XAPI or ODL. You can still access the OneView reports, but no dynamic ACLs or QoS profiles will be created in the infrastructure for the video flows. **Default:** true
Enable application sharing call prioritization	Enable this to prioritize application sharing streams (connections or flows) for all Skype for Business calls when possible. If this is disabled, no application sharing streams for any Skype for Business call will be prioritized, whether via XAPI or ODL. You can still access the OneView reports, but no dynamic ACLs or QoS profiles will be created in the infrastructure for the application sharing flows. **Default:** true
QoS Profile for audio calls	The name of the QoS profile used on the ExtremeXOS access switches to prioritize audio calls. This profile must be preconfigured on each access switch manually before using it.
QoS Profile for video calls	The name of the QoS profile used on the ExtremeXOS access switches to prioritize video calls. This profile must be preconfigured on each access switch manually before using it.

Service-Specific Configuration	Description
QoS Profile for application sharing calls	The name of the QoS profile used on the ExtremeXOS access switches to prioritize application sharing calls. This profile must be preconfigured on each access switch manually before using it.
DSCP value for audio calls	The DSCP value to apply to audio call packets on access switches. This value can be picked up by all switches on the path between caller and recipient to provide end-to-end QoS for audio calls. **Default:** 46
DSCP value for video calls	The DSCP value to apply to video call packets on access switches. This value can be picked up by all switches on the path between caller and recipient to provide end-to-end QoS for video calls. **Default:** 36
DSCP value for app sharing calls	The DSCP value to apply to app sharing call packets on access switches. This value can be picked up by all switches on the path between caller and recipient to provide end-to-end QoS for app sharing calls. **Default:** 26
Default username for web access to XOS switches	The default username to connect to the HTTP(S) interface (XAPI) of ExtremeXOS switches. This username is used only if there are no CLI credentials defined for a switch in Extreme Management Center. Otherwise, the Extreme Management Center CLI username takes priority. This setting is used only if the OpenDaylight option is disabled.
Default password for web access to XOS switches	The default password to connect to the HTTP(S) interface (XAPI) of ExtremeXOS switches. This password is used only if there are no CLI credentials defined for a switch in Extreme Management Center. Otherwise, the Extreme Management Center CLI password takes priority. This setting is used only if the OpenDaylight option is disabled.

Service-Specific Configuration	Description
Hard timeout (in minutes) for Skype for Business calls	The number of minutes after which a Skype for Business call is considered having ended, even if no ended notification has been received from Skype for Business in the meantime. If the configured number of minutes have passed between the start of a call and now, this call will be considered ended. As a result, any prioritization is removed from the infrastructure, the call data is removed from the in-memory list, and reporting data is created for OneView reporting. This feature also handles cases where the Skype for Business front end or SDN management servers have been down or communication has been blocked and, as a result, ExtremeConnect did not receive the Call Ended notifications for one or more active calls. This setting is used only if the OpenDaylight option is disabled. When using an OpenDaylight controller, the corresponding flows will timeout automatically. **Default:** 360 (=6 hours).
Use Skype for Business call timestamp instead of local NetSight time	The Skype for Business front end servers typically report the call start and end timestamps in UTC time, regardless of which time zone each FE server is configured. If this option is set to *true*, these timestamps are used for OneView reporting and used for deciding when to end a call (and remove its corresponding prioritization) using the configured value for *call_hard_timeout_in_minutes*. If you enable this option, make sure that your Extreme Management Center server is also running on UTC time zone, otherwise the OneView reports will be incorrect and the hard timeout functionality for call prioritization will not work properly. The best practice is to keep this option set to *false* so that the Skype for Business timestamps will be ignored, and the local Extreme Management Center timestamp will be used when the Skype for Business notifications are received by the Extreme Management Center server. **Default:** false

Service-Specific Configuration	Description
Number of days to store call reporting data	The number of days to store data on Skype for Business calls in the Derby DB. Calls that predate the configured number of days will automatically be purged from the DB and will not appear in the OneView reports anymore. A higher value will have a negative impact on the overall performance of this module and the OneView reports. Purging is performed every night during the first run of the MS Skype for BusinessSDNHandler module after midnight. Example: If you set the interval for this module to 600 seconds, purging occurs between midnight and 00:10:00 (0:10 AM). **Default:** 30
Enable the cleanup routine for obsolete Skype for Business-related ACLs on XOS switches	Enable this to run an automated cleanup process once per night or week. It connects to all your ExtremeXOS switches via Telnet or XAPI (depending on the firmware support) and tries to identify obsolete Skype for Business-related dynamic ACLs. If obsolete ACLs are found, it removes those ACLs from all ports and deletes the ACLs from the switch afterward. Set the interval for this process using the next setting *cleanUpObsoleteACLsOnXosSwitchesInterval*. This setting is only applicable if the OpenDaylight option is disabled. When using an OpenDaylight controller, the corresponding flows will timeout automatically.
Interval for cleanup routine for obsolete Skype for Business-related ACLs on XOS switches	If the feature ExtremeXOS is enabled, use this setting to define the interval to use for the cleanup routine. **Valid values:** daily, weekly **Default:** weekly
Enable the clean-up routine for obsolete Skype for Business-related ACLs on EOS switches	Enable this option to run an automated clean-up process once per night or week. It connects to all your ExtremeXOS switches via Telnet and tries to identify obsolete Skype for Business-related policy ACLs. If obsolete policies are found, it deletes the ACLs from the switch. Set the interval for this process using the next setting *cleanUpObsoleteACLsOnEosSwitchesInterval*.
Interval for clean-up routine for obsolete Skype for Business-related ACLs on EOS switches	If the feature *cleanup_obsolete_acls_from_eos_switches* is enabled, use this setting to define the interval to use for the clean-up routine. **Valid values:** daily, weekly **Default:** weekly

Service-Specific Configuration	Description

Gateway Switches	A list of switches that are located at the edge of your network where all external Skype for Business calls pass through. If an external Skype for Business call is detected, a dynamic ACL to prioritize the call's ingress flow will be created on all switches on this list on their ANY interface. This enables QoS for external calls as they enter your network at those gateway switches. Make sure that those switches support the required number of dynamic ACLs for the ANY interface. If you do not want to enable this feature, keep an entry with 127.0.0.1 in the list. If you manually modify this list, make sure to keep the ID values for all entries consistent and unique.
	
	Example entry:
	
	`<gateway_switch_entry desc="Gateway Switch Entry" id="1" type="Entry">`
	`<info>A Gateway Switch Entry</info>`
	`<value>127.0.0.1</value>`
	`</gateway_switch_entry>`

Skype for Business Front-End Server IP addresses	A list of all Skype for Business front end server IP addresses. If you want to prioritize conference calls but you cannot (or do not want to) enable any end system tracking mechanism (such as RADIUS authentication, XOS IDM, OneController plugin) on your data center switches where your Skype for Business front end servers are connected to, provide the list of all your front end server IPs here. When calls from or to your front end servers are seen, they will be prioritized on all gateway switches in the Gateway Switches feature list. Ensure that the list of gateway switches contains all switches where your front end servers are connected. If you do not want to enable this feature, keep a single entry with IP 127.0.0.1 and ID 1 in the list. If you manually modify this list, make sure to keep the ID values for all entries consistent and unique. This setting is only applicable if the OpenDaylight option is disabled.

Service-Specific Configuration	Description
Use HTTPS for XAPI calls	Enable this option to use HTTPS instead of HTTP for any XAPI communication with all ExtremeXOS switches. If enabled, you must install the SSH mod on all ExtremeXOS switches and configure *enabled web https*. This setting is only applicable if the OpenDaylight option is disabled. **Default:** false
Use OpenDaylight controller instead of XAPI for call prioritization	Enable this to use an Open Daylight controller to locate Skype for Business call end points in the network infrastructure and prioritize audio/video calls using OpenFlow. When enabled, you will also need to configure the OpenDaylight server using various settings below. If this is disabled, it will use the Extreme Management Center API and XAPI on ExtremeXOS switches to located end points and prioritize calls. **Default:** false
IP address of the Open Daylight controller	Management IP of the Open Daylight controller. This configuration only is valid when the option *use_opendaylight* is set to *true*.
TCP/HTTP port of the Open Daylight controller	The HTTP port on which the Open Daylight REST API is provided. Only HTTP is supported. This configuration only is valid when the option *use_opendaylight* is set to *true*. **Default:** 8181
Username to connect to the Open Daylight controller API	Username for connection to the OpenDayllight Controller. The user should have administrator rights to be able to create new flows and search for a host. This configuration is valid only when the option *use_opendaylight* is set to *true*.
Password to connect to the Open Daylight controller API	The password for the user account that will connect to the Open Daylight controller API. This configuration is valid only when the option *use_opendaylight* is set to *true*.
Idle timeout for flows created via Open Daylight controller	The idle timeout in seconds for newly created flows. All flows created via the Open Daylight controller to prioritize Skype for Business calls will use this idle timeout setting. To disable this feature, set this value to *0*. **Default:** 300

Service-Specific Configuration	Description
Hard timeout for flows created via Open Daylight controller	The hard timeout in seconds for newly created flows. All flows created via the Open Daylight controller to prioritize Skype for Business calls will use this hard timeout setting. To disable this feature, set this value to *0*. **Default:** 3600
Prioritize Wi-Fi Calls	When enabled, it verifies whether the source or destination Skype for Business end point is connected through an ExtremeWireless wireless controller and access point. If that is the case, the corresponding call flow is prioritized on the switch port to which the corresponding ExtremeWireless access point (AP) is connected. This feature is available starting with Extreme Management Center 6.3 and only in Bridged@AP mode. If your Wi-Fi topology uses Bridged@Controller mode, the call flows will still be prioritized on the corresponding switch access ports, but it will not have any effect as the Wi-Fi client traffic is transparently tunneled through to the controller and the ACLs, flows, and policies configured on the access switch will never match any of those packets. Make sure that LLDP is enabled on both your access switches and all access points. Also make sure that you have enabled device statistics collection for OneView for all access switches that APs are connected to. **Default:** true
Prioritize real-time control protocol traffic	Audio and video are typically sent using RTP, which requires two UDP ports: one port for the media and one port for the control protocol (RTCP). Enable this feature to prioritize the RTCP traffic and flows also. They typically use the RTP port number reported by the Skype for Business API plus one. Example: If Skype for Business reports a UDP source port of 5000 for a specific call connection, the code prioritizes traffic on both ports 5000 and 5001. **Default:** false

Verification

To verify that the integration is properly assigning dynamic ACLs to prioritize Skype for Business calls in the infrastructure:

1. Start a call between two Skype for Business end points and keep the call active.
2. Connect to the switches where these Skype for Business end points are currently connected using Telnet or SSH. (You can use the NAC end system list to get the switches and ports of your Skype for Business end points.)
3. Perform a `show config acl` command to list all ACLs currently active on the switch and validate that you see at least one ACL with a name similar to the following syntax:

   ```
   Skype for BusinessSrcA1234567890
   ```

   The first part (Skype for Business) indicates that this ACL has been dynamically created by ExtremeConnect to prioritize a Skype for Business call.

   The Src or Dst part indicates whether this ACL is used for the source or destination end point of a call.

   The A or V indicates whether this ACL is used to prioritize the audio or video stream for the Skype for Business call.

   The rest of the name is part of the call ID retrieved from Skype for Business, which makes this ACL name unique.
4. If you see two or even four ACL names starting with `Skype for Business`, this indicates that both Skype for Business end points are connected to the same switch and/or that this is an audio or video call, so both streams get prioritized with unique ACLs.
5. Verify that those ACLs are bound to the correct ingress switch port.
6. To verify that the reporting capabilities are working as expected, log in to OneView. To launch the MS Skype for Business report, select the **Reports** tab, and select **VoIP > MS Skype for Business** from the left menu. If this report is not visible, you might be missing the required XML reporting file.
7. Verify that you see calls in the **All Calls** tab of the report and that the data seems correct.

Analytics and Reporting

ExtremeConnect provides a new set of reports focused around different generalized solution sets, such as Data Center Management and Mobile Device Management. Additionally, end system data is propagated in a dedicated custom field across all

modules. This field contains labels to identify characteristics (such as virtual or mobile) that are available to searches across the entire end system table in OneView.

Data Center Manager (DCM) System Configuration

Extreme Connect Modules for data center applications leverage Extreme Management Center end system groups to create and manage virtual port groups in 3rd party hypervisors.

DCM Fabric Manager

To leverage Extreme Management Center and ExtremeControl end system groups for ExtremeConnect, the description of a group can include multiple options that will be utilized by various integrations.

The individual configuration options are:

Configuration Options	Description
sync=true|false	If this is set to *true*, a new port group (VMware) or network (Xen) is created automatically with the same name by the Data Center Manager. Setting this value to *false* effectively hides the group from ExtremeConnect.

Configuration Options	Description
VLAN ID	To define a VLAN ID for new VMware vSwitches/dvSwitches or Xen networks (excluding the Hyper-V module), you can use the following two formats: **vlan=#static_vlan_id#**: Setting this value to *vlan=100*, for example, will create a new port group (for VMware vSwitches) or network (Xen) and assign the VLAN ID 100 to it. For proper configuration, you must then create an ExtremeControl NAC rule that binds this end system group to a policy that also assigns (using *Contain to*) the end system to VLAN 100 on the physical network. The VMware/Xen management tags the VMs in this port group or network with VLAN ID 100. **vlan=#primary_vlan_id#:#secondary_vlan_id#:isolated_or_community**: This format is exclusively used for VMware to create a new private VLAN and corresponding dvSwitch. **Important:** The primary and secondary vlan IDs used must not be the same. The third parameter can only be *isolated* or *community*. VMs connected to isolated PVLANs are not able to communicate directly with each other; all communication will traverse the physical network. VMs connected to community PVLANs can communicate directly with each other through their dvSwitch. Example: `vlan=4000:4001:isolated`
switchgroup=#name#	This is a setting exclusively used for VMware. If you have `sync=true` but do not set this switch group value, it will automatically create a new port group for this end system group on **all** vSwitches. If you have vSwitches that should, for example, only be used for management purposes, you might not want the Data Center Manager to create such port groups on all of those vSwitches. You can use the following predefined values to adjust this setting. In addition to these predefined values, you can use regular expressions to granularly define the vSwitches where you want the new port groups to be created. **vSwitchOnly**: The new port group will be created only on all vSwitches, not on distributed virtual switches. **dvSwitchOnly**: The new port group will be created only on all distributed vSwitches, not on the vSwitches. **includeAll**: The new port group will be created on all vSwitches and distributed vSwitches. **excludeAll**: No new port group will be created.

Configuration Options	Description
nic=#list of NICs#	This is a setting exclusively used for Xen. For the Data Center Manager to create a new network in Xen server, it needs to know to which physical interface to attach this network. This value must be the name of the physical interface as seen by the operating system of the Xen servers. For both examples below, remember to also use the settings `sync=true` and `vlan=XXXX`. This will create an external Xen network. Setting both the VLAN ID and the physical NIC is mandatory for external networks. Setting only one of these two values will result in the creation of an internal network that will not have a VLAN ID nor a connection to the physical network. Example 1: If you use your first interface (eth0) for management of the Xen server and you want to create a new Xen network that connects to the second physical interface, use `nic=eth1` for the corresponding end system configuration. Example 2: If you want to create a bond instead of a simple network, you must provide a list of NICs that should be attached to this bond. You can use the following syntax: `nic=eth1,eth2`

Verification

If synchronization is not enabled for a group, ExtremeConnect acts as if that group does not exist when creating external port groups and networks.

End System Groups

After initial installation the following groups should be present in ExtremeControl:

End-system group for Disconnected Devices	Fusion Disconnected Systems

These are the default names for each group. These names can be changed during installation or on the configuration page.

These groups provide the ability to configure access rules for end systems that qualify for any of these. The approval pending group contains end systems that are connected to a port group with the `approval=true` flag being set, before they are approved by an administrator.

The disconnected devices group creates a port group on the hypervisor when an end system group is deleted, if the port group/network deletion feature is enabled and the to-be-deleted port group/network still has VMs attached. These VMs will be moved to the

Disconnected Systems port group and consequently show up in the end system group of the same name.

Private VLANs

Private VLANs (PVLANs) currently only exist in VMware. In a standard VMware setup, all VMs connected to the same distributed vSwitch (dvSwitch) can talk to each other. With PVLANs, it is possible to isolate VMs connected to the same dvSwitch from each other so that they cannot directly communicate with each other. Any communication between those isolated VMs must be carried out outside of the VMware environment over the physical network. The best practice is to control traffic and applications used by these VMs (using Extreme Management Center policies) and, if needed, screen that traffic using Netflow technology.

Requirements

You must have the following items to meet the minimum requirements for using this functionality:

- A VMware vCenter license that can use distributed vSwitches
- At least one distributed virtual switch (dvSwitch)

Useful Information about PVLANs

The vCenter Server can manage multiple ESX hosts. A dvSwitch is a virtual Switch on which exists on all your ESX servers managed by a vCenter Server and is unique to all of them. You cannot use PVLANs on normal vSwitches.

NOTE: The following section is intended to be informational only, as the described tasks are automated via Data Center Manager.

To create PVLANs:

1. Create a new dvSwitch and navigate to its settings windows.
2. Choose the **Private VLAN** tab.
3. Create primary and secondary private VLANs. Every primary private VLAN ID must have one secondary VLAN ID with the same ID in promiscuous mode, and then they can have multiple other secondary VLAN IDs. The secondary VLANs can either be of type *isolated* or *community*. In isolated mode, the VMs connected to these secondary VLANs will not be able to communicate with other VMs on the same dvSwitch without being routed through the physical network. The community mode allows direct VM communication in the virtual network environment

(dvSwitch). No secondary VLAN ID or static VLAN ID can be the same as any existing primary VLAN ID.

4. When these VMs communicate on the physical network, you will see the secondary private VLAN ID, not the primary one. For additional information, see the corresponding knowledge base article from VMware: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1010691

Promiscuous PVLANs have the same VLAN ID both for primary and secondary VLAN.

Community and isolated PVLANs traffic travels tagged as the associated secondary PVLAN.

Traffic inside PVLANs is not encapsulated (there is no secondary PVLAN encapsulated inside a primary PVLAN packet).

Traffic between virtual machines on the same PVLAN but on different ESX hosts go through the physical switch. Therefore, the physical switch must be PVLAN aware and configured appropriately to allow the secondary PVLANs to reach their destination.

Switches discover MAC addresses per VLAN. This can be a problem for PVLANs because each virtual machine appears to the physical switch to be in more than one VLAN, or at least, it appears that there is no reply to the request because the reply travels back in a different VLAN. For this reason, it is a requirement that each physical switch, where ESX with PVLANs are connected, must be PVLAN aware.

To use these private VLANs, you must create a port group in the dvSwitch. In the settings section of this port group, you can configure the VLAN. Select **Private VLAN** as the type, and then select from those private VLANs that you configured previously.

NOTE: If you configure a secondary private VLAN 201 and at the same time add the following string to an end system group's description field in ExtremeControl NAC manager (`vlan=200:201:isolated`), Data Center Manager will recognize this and create the appropriate configuration, and then add all VMs in this end system group to that private VLAN dvSwitch.

Setup Reference

This reference topic shows an example of how to deploy a PVLAN configuration. The goal of this setup is to create two VMs that are connected to the same dvSwitch in the same secondary isolated PVLAN, which can only communicate with each other traversing the physical network. This has been extended to also traverse a routing instance. This way, you can create the same setup where the VMs are distributed over two physical ESX servers that are located in different routing networks.

The following diagram provides an overview of the general system setup and some configuration hints:

Policy Domain Configuration

This section describes the setup of the different policy domains used for the different switching/routing layers. The following information is an overview of the scenario:

1. Dynamic role at the S-series in layer 2 mode (switching) assigns all traffic based on the source MAC of the VMs to the following VLANs:
    a. All traffic to the router (VRRP) MAC address is contained into VLAN 4000.
    b. All ARP traffic is contained into VLAN 4001.
    c. Additional rules can be added.
2. VLAN to policy map at the S-series in layer 3 mode (routing) for PVLAN L3:
    a. Is assigned to all traffic tagged with VLAN ID 4001. There is no dynamic policy assignment based on the MAC addresses of the VMs.
    b. Contains all ARP traffic to VLAN 4000 (all other traffic is already contained to 4000).
    c. The router interface in this VLAN 4000 is replying to the ARP requests with its own MAC address (local proxy ARP) and sends the reply in VLAN 4000.
3. The VLAN 4000 and 4001 must be statically configured on the uplinks/trunk in between the physical switches.

Policy Domain Layer 2 – Role VM PVLAN Access

All traffic coming from the VM is tagged with VLAN ID 4001 (the secondary PVLAN ID for the dvSwitch where this VM is connected to). The following role configuration has been implemented:

- **Role level**: VLAN 4000 tagged egress. Dynamically assigns this VLAN to this port VLAN egress list so that on the way back from the physical network to the VM, the traffic will be tagged with VLAN 4000.
- **Role level**: TCI overwrite enabled.
- **Role level**: Deny All traffic by default.
- **Rule**: Contain packets to the backbone router's MAC address (00:00:5e:00:01:01) to VLAN 4000. This avoids inter-VM communication via broadcast and multicast.

- **Rule**: Value 0x806 (ARP) contain to VLAN 4001. Only ARP traffic is kept in VLAN 4001 to make sure it is only broadcast to the upstream of the layer 2 switch where the router is connected (this router replies to the ARP broadcasts).

Policy Domain Core – Policy VM PVLAN L3

The core router is S-series switch configured as a router. It receives the IP traffic on VLAN 4000 and the ARP broadcasts on VLAN 4001 from the VMs. This router has *local proxy ARP* enabled to reply with its own MAC address when it receives any ARP broadcast for any VMs (even residing on the same local subnet), since all traffic from the secondary PVLAN 4001 should be routed through this router and not travel directly between the VMs. The following configuration has been implemented:

- **Role level**: VLAN 4000 tagged egress. Assigns VLAN 4000 tagged egress for IP traffic back to the VMs.
- **Role level**: TCI override enabled.
- **Role level**: Role mapping of VLAN ID 4001 to policy VM PVLAN L3.
- **Rule**: Value 0x806 (ARP) contain to VLAN 4000. This is where the ARP traffic is remapped from 4001 to 4000, to have this router's interface in VLAN 4000 reply to the ARP broadcast with its own MAC address (local proxy ARP). After this re-mapping is done, there is no more traffic on VLAN 4001.

Packet Flow Example for Reference Setup

The following diagram shows the packet flow for the first ARP request sent by VM1 before it starts communicating with VM2. It also shows how its attributes are changed while traversing the virtual and physical network.

The following diagram shows the first ping from VM1 to VM2 after the successful ARP resolution (as shown in the previous diagram), and shows the packet flow for all IP traffic between these two VMs.

Mobile Device Management (MDM) System Configuration

To be used by Extreme Networks MDM Connector plugin, the MDM software must be configured to provide the data that is imported by ExtremeControl as assessment information or end system data.

End System Groups

After the initial installation, the following groups should be present in ExtremeControl:

Group for Managed Business Mobile Devices	Managed Mobile Devices Business
Group for Managed Personal Mobile Devices	Managed Mobile Devices Personal
Group for Decommissioned Mobile Devices	Managed Mobile Devices Decommissioned
End-system group for Managed Devices Wipe	Managed Mobile Devices Wipe

These are the default names for each group, which can be changed during installation or on the configuration page.

The Managed Mobile Devices Wipe group provides the wipe functionality.

These groups contain the inventory information coming from the MDM provider. End systems are classified in each group depending on the ownership information from the MDM provider.

The Decommissioned group is a placeholder for devices that have been un-enrolled in the MDM provider. Typically, its treatment should be the same as unregistered users.

The Wipe group is an exception to this rule; the group is only used to trigger a wipe notification to the MDM provider. The wipe signal resets the configuration of the end system to its factory settings. This option is disabled by default.

Related Information

For information on related tabs:

Extreme Management Center ExtremeConnect Overview

ExtremeConnect Assessment Configuration

The ExtremeConnect Assessment Configuration includes assessment map entries and the assessment adapter, which provide you with health tests and results for your Connect modules.

Assessment MAP Entries

All modules, except McAfee EMM, currently use the assessment adapter to report health results to Extreme Management Center. (McAfee EMM has its own plugin.) The assessment adapter creates 30 new assessment tests or plugin IDs to use by NAC. Each test is reported to NAC by a plugin ID created as follows:

- base value = 100.000
- plugin id = base value + ENUM ID (i.e. OWNERSHIP -> 100.000 + 22 = 100.022)

The following is the complete list of tests and IDs:

- EXISTS(1)
- COMPLIANT(2)
- JAILBROKEN(3)
- AUTHORIZED(4)
- WIPED(5)
- UNINSTALLED(6)
- COMPROMISED(7)
- OSOUTOFDATE(8)
- POLICYOUTOFDATE(9)
- DEVICEOUTOFDATE(10)
- BLOCKED(11)
- INFECTED(12)
- LOST(13)
- RETIRED(14)
- UDID(15)

- SERIALNUMBER(16)
- IMEI(17)
- ASSETNUMBER(18)
- NAME(19)
- LOCATION(20)
- USER(21)
- OWNERSHIP(22)
- PLATFORM(23)
- MODEL(24)
- OSVERSION(25)
- PHONENUMBER(26)
- LASTSEEN(27)
- PASSCODEPRESENT(28)
- PASSCODECOMPLIANT(29)
- DATAENCRYPTION(30)

You can map each test to different variables in each MDM connector.

In the JAMF Casper module default configuration, the test EXISTS (pluginID 100001) is mapped to the value of the variable *managed* in the JAMF Casper database.

NAC Manager can assign risk values and scores to each test using their plugin ID. This is needed in order to quarantine devices based on their risk level.

Assessment Adapter

The assessment adapter infrastructure reports health results from ExtremeConnect modules to NAC, if available. The assessment adapter must be manually configured for automatic start-up for most MDM assessment integrations.

The assessment adapter scripts are located in the following directories:

- **Linux:**

  Extreme Management CenterRootdir/jboss/server/default/deploy/fusion_jboss.war/assessment/launchAS.sh

- **Windows:**

  Extreme Management CenterRootdir\jboss\server\default\deploy\fusion_jboss.war\assessment\launchAS.cmd

To configure the assessment adapter:

1. To make the script executable, set the executable bit on that script in a Linux environment as follows:

   ```
   cd /usr/local/Extreme_
   Networks/NetSight/wildfly/standalone/deployments/Connect.w
   ar/assessment/


   chmod +x launchAS.sh
   ```

2. To verify that the script works, enter:

   ```
   ./launchAS.sh
   ```

   If it worked, you will see a long line of text showing the startup of the Java Virtual Machine, including all its Java libraries.

3. To stop the script, enter `CTR-C`.

4. To properly start the script as a daemon process running in the background at all times, edit the /etc/rc.local file and add the following two lines just before the last line (exit 0):

   ```
   cd /usr/local/Extreme_
   Networks/NetSight/wildfly/standalone/deployments/Connect.w
   ar/assessment/

   nohup ./launchAS.sh > /usr/local/Extreme_
   Networks/NetSight/wildfly/standalone/deployments/Connect.w
   ar/assessment/launchAS-startup.log 2>&1 &
   ```

   The first line changes to the correct directory where the launchAS.sh script is located. The second line executes that script using the *nohup* signal, which tells Linux to disconnect the process that started the script from the process running it (sending it to background). It also redirects any start-up output to the following file (which can be verified later to ensure proper start-up):

   /usr/local/Extreme_
   Networks/NetSight/wildfly/standalone/deployments/Connect.war/assessment/launchAS-startup.log

5. Manually start the script using the following command:

   ```
   service rc.local start
   ```

6. To verify that the script was started and is running, perform the following steps:
    a. Run the following command and make sure there is exactly one process that runs this script:

    ```
    ps ax | grep launchAS.sh
    ```

    Ignore output lines such as *grep --color=auto launchAS.sh*
    b. Run the following command and make sure there is exactly one process that runs the JVM:

    ```
    ps ax | grep 8448
    ```

    The Java Virtual Machine will start the service on port 8448 by default and you should see a very long text output.
    c. Run the following command and make sure that it shows exactly one line for port 8448:

    ```
    netstat -an | grep 8448
    ```

    d. Check the start-up log file for any errors (see the filename in step 4).
    e. Check the assessment adapter log file for any warnings or errors: /usr/local/Extreme_ Networks/NetSight/wildfly/standalone/deployments/Connect.war/assessment /logs/assessment.log
7. If starting the adapter was successful, reboot the Extreme Management Center server and verify that the service has been started automatically (using the same verification steps used in step 6).

McAfee EMM Assessment Plugin

McAfee EMM uses a separate assessment plugin to gather data from the server and report it as health results to the Extreme Management Center server. The MDMAdapter.jar files are located in the following directory:

Extreme Management CenterRootdir/jboss/server/default/deploy/fusion_ jboss.war/assessment/launchAS.sh

Before the assessment adapter can be used in NAC Manager, you must create a valid assessment server by following these steps:

1. From the **Assessment Configuration** page, select **Assessment Servers > Add**.

2. In the **Edit Assessment Server** dialog, edit the fields:
   Assessment Server IP - IP address of the ExtremeControl server.
   Assessment Server Name - A name for easily identify our server.
   Assessment Server Port - If launched with the launchAS commands, the agent runs on server 8448.
   Assessment Server Type - FusionAssessmentAgent
   Max Concurrent Scans - Leave empty. This can be used afterward to increase the capacity of the server. By default, the server allows 10 concurrent scans.

   To use this server for assessment purposes, the server must be in an assessment pool and the assessment pool must be used by an assessment configuration.
3. From assessment configuration, select **New Test Set**. In the **Edit Other Test Set** dialog, configure a new test set that uses the new server pool and the FusionAssessmentAgent type:
4. Create a scoring override for one or more of these test cases to quarantine end systems in case they match a certain result string in their description field. From the **Health Results Details** tab, select **Configure > Add Scoring Override > To Apply Score**. The following example shows how to do this for the OSVERSION test case.
5. In the **Add Scoring Override** dialog, edit the fields. If you want to quarantine all iPads with an iOS version of 5.x, an Override Score value of *7.0* would (if the risk level configuration has not been altered from the default value) ensure that this device will be marked with a high risk level and will be quarantined.
6. Make sure you have enabled **Use Quarantine Policy** in the corresponding NAC profile and that the corresponding policy on the WLAN controller has a redirect configured in that policy that points to the NAC captive portal.
7. To display the NAC remediation (self-help) page, from the NAC **Advanced Configuration** dialog, enable **Assessment Remediation**.
8. Customize your remediation portal if needed. For example, you can add a

remediation link that allows users to register their devices on the MDM portal:

9. Another customization best practice is to define the **Custom Remediation Actions** to improve the user experience with the help texts on the remediation page.

Troubleshooting and FAQs

Installation and General Configuration

I'm getting a java error while trying to start the installer. What can I do?

Usually this happens when using an older Java Runtime Environment (JRE) to execute the installer. The best practice is to use the JRE in the Extreme Management Center Java directory.

What ports does Extreme Connect use?

Upcoming ExtremeConnect modules can use additional or different ports. The following ports are used by all modules:

- 443 (HTTPS)
- 80 (HTTP)
- 8443 (HTTPS)
- Any port configured by the various adapters

How do I reset module passwords using the CLI?

ExtremeConnect stores passwords in an encrypted format for security purposes. To reset a password:

1. Open the configuration file in the CLI.
2. Change the password.
3. Set the *crypt* attribute to **false**.
   During the next run cycle, the password is encrypted automatically, and the *crypt* attribute is reset to **true**.

How do I start the installer in CLI mode?

Add `-console` at the end of the `java -jar …` command.

Does ExtremeConnect use a database?

ExtremeConnect does not store any data persistently, except for configuration data. All information is kept in memory, and then cleared when Extreme Management Center (or the JBoss service) is restarted.

Which files are modified by ExtremeConnect upon installation?

The following files are backed up and then modified in the Extreme Management Center directory:

- ../jboss/server/default/deploy/fusion_jboss.war/*
- ../jboss/server/default/conf/fusion/*
- ../jboss/server/default/conf/log4j.xml
- ../appdata/NSJboss.properties
- ../appdata/System/Shared/ThirdPartyMenu.xml

How do I find and change the configuration on the CLI?

The configuration files for all modules are stored in ../jboss/server/default/conf/fusion/.

All files use an XML format and must comply with the internal data model.

NOTE: Faulty settings can force the module to shut down or can cause other unpredictable problems. It is safer, and the best practice, to use the configuration web page where all data is stored according to the data model.

I changed the configuration of a module. Do I need to restart the Extreme Management Center service before the changes will apply?

No. The modules constantly check if the configuration files were modified and will reload them at the next run cycle.

Is it possible to switch to another language on the configuration page?

No, however, you can manually translate all of the text information. The web page is dynamically created from the configuration files. The best practice is to translate the *<info>* sections in the configuration file to the desired language.

How do the adapters for SCVMM, Hyper-V, and XenDesktop work?

These adapters are written in Java, and use Windows Powershell commands to retrieve data on virtual machines (SCVMM) and virtual desktops (XenDesktop). These act as a server in a client-server relationship with the corresponding ExtremeConnect module. During each interval configuration, the corresponding module acts as a web service client and calls the web service server (=the adapter) to get information from that adapter. The communication uses the configured IP address, port, and pre-shared key. The adapter gathers the requested data using Powershell commands, encrypts the data, and then returns that data to the corresponding module. The ExtremeConnect module then populates Extreme Management Center/NAC with the data.

General Issues

The Connect tab is missing when I access ExtremeConnect.

If the **Connect** tab is not visible in the user interface, the ExtremeConnect plugin was not installed or an Advanced License is not present.

To fix this issue:

1. Install or reinstall the ExtremeConnect plugin.
2. Update the Extreme Management License to **Advanced**.
3. Restart the services.

Extreme Management Center is not responding.

Restart ExtremeConnect:

1. Restart the Extreme Management Center service.
2. Change the directory as follows:
   `cd /usr/local/Extreme_Networks/Extreme Management Center/scripts`
3. Stop the Extreme Management Center service by typing:
   `./stopserver.sh`

4. Wait for the prompt, and then start the Extreme Management Center service by typing:
   `./startserver.sh`

How do I restart or reset ExtremeConnect?

ExtremeConnect runs within the JBoss context. The service can be restarted by restarting the JBoss service (or Extreme Control).

If the ExtremeConnect cache needs to be reset, do the following:

1. Shut down the Extreme Management Center service.
2. Delete the *.dat files under ../jboss/server/default/conf/udcp/ of the Extreme Management Center installation directory.

Is there a log file and where do I find it?

ExtremeConnect creates logs within the JBoss context of the Extreme Management Center server. Do one of the following actions to access the log file:

- Look for the server.log file in the in the ../appdata/logs/ folder
- Open the server log from any Extreme Management Center client.

What log levels are available and how do I change them?

Every module of ExtremeConnect, including the main application itself, has individual log level settings in its respective configuration file. The default level is ERROR. The best practice is to keep it at this default level, except for when you are troubleshooting issues. The log levels are (from least to most talkative):

- ERROR
- WARN
- INFO
- DEBUG

I am getting a lot of errors and would like to turn logging completely off for a specific module.

In addition to the four log levels used by all modules, Log4J also supports the FATAL log level, which is currently not used by any module without ExtremeConnect. To set a module to use this log level, the configuration file must be edited manually. To prevent shutting down the logging operation accidentally, the FATAL option is not provided on the web page.

Some modules stopped working and the log file reports show that many errors occurred.

Each module is monitored by the main ExtremeConnect process regarding errors that happen during each run cycle (such as authentication errors). If a module produces more than 10 failures in a row, the module is disabled to prevent further errors. To restart a module:

1. Try to identify the problem source (for example, a remote server is not responding).
2. Fix the issue.
3. Update the module configuration file.
   When the timestamp of the configuration file is changed, the configuration is reloaded and the failure counter is reset to zero until further failures happen. The counter will also be reset, if at least one successful cycle was completed in the meantime.

The logs notate local or remote data storage. What are these?

ExtremeConnect logs are always written from the ExtremeConnect perspective. *Local* means the ExtremeConnect service, and *remote* relates to another contacted service (such as ExtremeControl or VMware). Each module has its own data store to track changes, and update local or remote data. Therefore, if information for an end system is missing from a specific module, the best practice is to start by looking at the data store and log for that particular module.

What happens to a module if an error occurs?

The error is logged. Depending on the severity of the error, the run cycle for the module will continue or end. If an error crashes a module, a full stack trace is logged and the module is terminated until the JBoss service restarts. All other modules will not be affected by this and will continue to run, even if they do not receive further updates from other modules.

After JBoss starts, I do not see any data updates for several minutes. Is something wrong?

No, this happens by design. ExtremeConnect starts all of the modules and waits a short time to verify that everything is running correctly. After that, the modules enter their run cycles and start retrieving data from various sources. It can take several minutes to see the data, depending on the time it takes to retrieve the data and the interval time for each module.

Extreme Management Center

How does ExtremeConnect communicate with Extreme Management Center?

ExtremeConnect only uses Extreme Management Center web service calls to retrieve or alter data. There is no direct access from the module to the Extreme Management Center database, even though both applications usually run on the same server.

Is it possible to use one instance of ExtremeConnect with multiple Extreme Management Center servers?

No.

ExtremeConnect is supposed to update a custom field in the Extreme Management Center NAC Manager for each end system, but I do not see such a field. How can I make the custom fields visible?

From the Extreme Management Center NAC Manager, right-click on any of the end system table headers. Change the view properties to display the custom fields.

Where is the configuration page located for ExtremeConnect?

The direct access URL is https://Extreme Management Center-IP:8443/fusion_jboss/, or access the page from the **Connect** tab in ExtremeConnect.

There is an Axis error in the logs about an unknown HTML method error. What does the error mean?

The server responded to a request with a simple HTML page. This error is most likely due to wrong user or password information, to which the server responds by displaying a login error. However, the application is unable to handle this type of output from the server and logs the error as an unknown HTML method instead.

Check the account information for spelling errors.

VMware vSphere Configuration

Do I have to create a dedicated user for ExtremeConnect to access the vSphere webservice?

No, but the best practice is to create a dedicated user. This lets you filter events and tasks more easily in the VMware client.

What are the minimum permission requirements for the web service user?

At minimum, the account must have permissions to:

- Register the Extreme Management Center Plugin Extension
- Write data to VM annotation fields
- Read data from VM configurations (MAC, Network)

Although ExtremeConnect seems to be running fine, I only see n/a in the annotation fields and no records associated with the ExtremeConnect plugin. Why is that?

Most likely, none of the MAC addresses for the VM are listed in the end system table of the NAC Manager.

1. Verify that authentication (at least MAC Auth) is set up properly on the physical switch.
2. Verify that the VM is sending traffic.

How often does ExtremeConnect update the information (such as annotations and switches) in vSphere?

ExtremeConnect checks whether the current remote data differs from its local. If so, it updates all of the data that is different on the remote service. This is especially true for the annotation field. The best practice is to avoid using variables like *LastSeenTime* in the annotation text because the data changes often, resulting in frequent updates.

Is there any way to delete the event or task logs for every update that ExtremeConnect performs within vSphere?

No. This functionality is handled by vSphere, and ExtremeConnect cannot stop it. vSphere offers a filtering mechanism that can be used to limit the information shown and help to find specific data more efficiently.

How does ExtremeConnect determine the name of the end system group that a VM MAC address should be added to?

ExtremeConnect retrieves the name of the virtual network or port group from its default configuration, and uses the part before the first underscore as the end system group name. This method corresponds to the naming convention used when ExtremeConnect is configured to automatically create port groups from end system groups. The format used is:

```
endSystemGroup_virtualSwitchName
```

This naming method is due to the vSphere requirement that two port groups on the same host cannot share the same name. Therefore, the (d)vSwitch name is appended to the end system group name with an underscore. This helps to ensure that vMotion is possible for VMs on two hosts, which also requires that both port groups on those hosts have the same name.

Is it possible to let ExtremeConnect create port groups automatically while letting the VM administrator handle the VLAN configurations?

Yes, there is a configuration option to turn off VLAN create and update operations.

What happens if VLAN updates are enabled and a VM administrator changes the settings of a port group?

ExtremeConnect will update the settings using the local configuration data. It will not delete and re-create the port group; it only updates the existing configuration.

What happens if an end system group is deleted and the port group deletion option is enabled?

ExtremeConnect moves all virtual machines that are attached to that port group or network to the VM Disconnected Systems group, and deletes the original port group or network.

If a port group has been deleted by ExtremeConnect, can another port group with the same name be created manually within vSphere after the deletion

Using its local data store, ExtremeConnect puts the name of the end system group onto a special deletion stack. During each run cycle, every module checks the stack and removes all port groups that use the same name, until the deletion interval timer runs out. The default value is 2 minutes. After the interval has passed, a VM administrator can safely create a port group using the same name without the new group being deleted.

Although port group deletion is enabled, groups are not getting deleted by ExtremeConnect. What is the reason for that?

ExtremeConnect deletes all of the groups if the groups are on the deletion stack and the entry has not timed out. By default, the deletion timer interval is 2 minutes. If more time is required for each run through, try increasing the deletion interval timer so that the module has a better chance of completing the operation.

Citrix XenServer Configuration

Do I have to create a dedicated user for ExtremeConnect to access the Xen Server web service?

No, you can use the root account on the Xen Server.

What are the minimum permission requirements for the web service user?

The minimum permissions an account must have are as follows:

- Write data to VM description fields
- Read data from VM configurations (MAC, Network)

Although ExtremeConnect seems to be running fine, I only see *n/a* in the annotation fields and no records via the ExtremeConnect plugin. Why is that?

Most likely, none of the MAC addresses for the VM are listed in the end system table of the NAC Manager.

1. Make sure that authentication (at least MAC Auth) is set up properly on the physical switch.
2. Verify that the VM is sending traffic.

How often does ExtremeConnect update the information (such as descriptions and networks) in XenCenter ?

ExtremeConnect checks whether the remote data differs from the local data. If it differs, ExtremeConnect updates all of the data that is different on the remote service. This is especially true for the description field. The best practice is to avoid using variables like *LastSeenTime* in the annotation text, because the data changes often, resulting in frequent updates.

How does ExtremeConnect determine the name of the end system group that a VM MAC address should be added to?

ExtremeConnect creates Xen networks with the same name as the corresponding Extreme Management Center end system group. ExtremeConnect checks all of the managed Xen networks and the VMs that are assigned to them. The MAC addresses of these VMs are then added to the corresponding end system group in Extreme Management Center.

Is it possible to let ExtremeConnect create networks automatically, and let the VM administrator handle VLAN configuration?

No, this feature is supported only for VMware, not for Xen.

What happens if a Xen administrator changes the settings of a network (such as VLAN ID or NIC)?

ExtremeConnect updates the settings using the local configuration data. To perform an update, all of the VMs connected to the network are temporarily disconnected from the network. Then the network is reconfigured, and the previously connected VMs are reconnected.

What happens if an end system group is deleted and the network deletion option is enabled?

ExtremeConnect moves all of the VMs attached to that network to the VM Disconnected Systems network, and deletes the original network.

If a network has been deleted by ExtremeConnect, can another network with the same name be created manually in XenCenter after the deletion?

Using its local data store, ExtremeConnect puts the name of the end system group in a special deletion stack. During each run cycle, every module checks the stack and removes all of the networks that use the same name until the deletion interval timer runs out. By default, this value is 2 minutes. After the interval passes, a Xen administrator can safely create a network of the same name without the new network being deleted.

Although network deletion is enabled, networks are not getting deleted by ExtremeConnect. What is the reason for that?

ExtremeConnect deletes all of the networks (groups) that are in the deletion stack if the entry has not timed out. By default, the interval is 2 minutes. If more time is required for each run through, try increasing the deletion interval timer so that the module has a better chance of completing the operation.

I have set the description of an end system group to `sync=true vlan=100`. However, in Xen, only an internal network is being created, not an external network with the corresponding VLAN ID. Why is this happening?

To create an external network, ExtremeConnect requires two settings to be configured in Xen, as follows:

- VLAN ID
- A physical NIC to connect with the external network

I have set the description for an end system group to `sync=true nic=eth1`. However, in Xen, only an internal network is being created, not an external network attached to nic eth1 without a VLAN ID. Why is this happening?

To create an external network, ExtremeConnect requires two settings to be configured in Xen, as follows:

- VLAN ID
- A physical NIC to connect with the external network

It is not possible to create an external Xen network without assigning a VLAN ID (all external Xen networks are tagged).

Adapters for XenDesktop, Hyper-V, SCVMM and SCCM Configuration

What does the adapter do and how does it work?

The adapter creates a web service that is bound to the IP and port that are configured in the configuration file. ExtremeConnect makes web service calls to this adapter to retrieve data on managed end systems (such as VMs and Windows devices) .

Depending on which integration is used, ExtremeConnect also updates the data on the remote server (such as description fields for VMs).

What ports are required for communication between ExtremeConnect and the adapter?

Only one port is required. The port is configured in the adapter configuration file.

Is the communication secure?

All of the data that is sent to and retrieved from the adapter is encrypted using the pre-shared key. The administrator defines the pre-shared key when setting up the adapter and installing ExtremeConnect. The key gets encrypted automatically.

Information is not synchronized. What should I check?

Check the adapter's log file, which shows when the adapter has been called by ExtremeConnect, what Powershell commands it tried to execute, and what the return values of these commands were.

To view and print the adapter's log file:

1. Set the log level to DEBUG.
2. Restart the adapter to print detailed logging information.

How can I check whether the adapter's web service is working and reachable?

Use a Linux tool like wget to request one of the following web URLs. Select the URL that relates to the adapter you are trying to troubleshoot:

- **XenDesktop**: http://<IPofAdapter>:<PortOfAdapter>/DCM_XENDESKTOP_ADAPTER
- **Hyper-V:** http://<IPofAdapter>:<PortOfAdapter>/DCM_HYPERV_ADAPTER
- **SCVMM:** http://<IPofAdapter>:<PortOfAdapter>/DCM_SCVMM_ADAPTER
- **SCCM:** http://<IPofAdapter>:<PortOfAdapter>/FUSION_SCCM_ADAPTER

If you get a browser error stating that it cannot connect or the page does not exist, you either have an issue with a firewall along the communication path or the adapter's web service did not start properly on the configured IP and port.

Citrix XenDesktop Configuration

Why do the user names in Extreme Management Center NAC Manager appear as Kerberos user names?

The XenDesktop adapter uses the same web service call as the Kerberos snooping process. For the system's functionality, this makes no difference. You can create user groups, rules, and profiles based on these user names.

Sometimes the user names are deleted or disappear in NAC Manager. Why does this happen?

This issue is caused by one of the following situations:

- The corresponding XenDesktop session has ended. In this case, the adapter resets the user name on the corresponding end system VM, which also triggers any existing rule / NAC profile changes.
- The Kerberos aging timer was triggered. In NAC Manager, you can configure an interval after which the Kerberos user names will automatically age out. If you do not want this timer to interfere with the XenDesktop adapter functionality, set a very high value for the interval or disable this feature.

Although some users have disconnected from their XenDesktop session, the user names are still active within NAC Manager. Why does this happen?

XenDesktop distinguishes between a closed (non-existent) session and a disconnected one. A session is first active, then disconnected, and finally closed. As long as the session is in the Disconnected state, the adapter does not reset the user name in Extreme Management Center. If the user re-activates their session, there is no need for the adapter to set the user name, and the corresponding user profile is already active in NAC.

Microsoft Hyper-V and Virtual Machine Manager Configuration

How often does ExtremeConnect update the information in the Notes field?

ExtremeConnect checks whether the remote data differs from its local data. If it differs, it updates all of the data that is different on the remote service. This is especially true for the Notes field. The best practice is to avoid using variables like *LastSeenTime* in the Notes text because the data changes often, resulting in frequent updates.

How does ExtremeConnect determine the name of the end system group that a VM MAC address should be added to?

ExtremeConnect reads the virtual networks (virtual switches) that each VM belongs to, and puts its MAC address into the corresponding end system group in Extreme Management Center. For this feature to work, both of the following items must be configured:

- End system groups with the exact same name as the virtual networks from Hyper-V must exist in Extreme Management Center
- The description field must contain `sync=true`.

Connect Diagnostics

The **Diagnostics** tab lets you explore the current data per ExtremeConnect module and analyze performance statistics per module.

The **Diagnostics** tab contains three subtabs:

- **End-Systems** – Displays all of the end-system data that ExtremeConnect has for each module. The columns in the list show all of the properties that ExtremeConnect could potentially update per end-system.
- **End-System Groups** – Displays all of the end-system groups used by ExtremeConnect that end-systems can be assigned to.
- **Statistics** – Displays operational statistics and the average duration in milliseconds for each enabled module.

Related Information

For information on related tabs:

- ExtremeConnect Overview
- ExtremeConnect Configuration

Services API

The ExtremeConnect **Services API** tab lets you execute a client/server application, known as a web service.

NOTE: The web services documentation is located at http://*Extreme Management Center IP*/connect/rest/openapi.json

The available web services are organized based on the type of function they perform:

- **Control** – Perform Extreme Management Center Control operations such as retrieving or sending end-system or end-system group data to or from Extreme Management Center.
- **Device** – Perform ExtremeControl device configuration operations.
- **Label** – Retrieve and modify labels for end-system and MAC addresses.
- **Module** – Retrieve and modify general module services.
- **nbi** – Perform mutate and query operations for NBI.
- **Policy** – Perform Policy Manager operations.
- **Services** – Retrieve statistics and delete end-systems by MAC address.

Related Information

For information on related tabs:

- ExtremeConnect Overview
- ExtremeConnectConfiguration

Web Service Error Codes

Error Code	Description
0	Operation was successful
1	The requested object does not exist
2	Object already exists
3	Parameter value is incorrect
4	Error parsing an input
5	Result would be an Invalid configuration
6	Remote connection error
7	Unexpected error condition
8	End system group does not exist
9	CSV operation error