Managing a Lost or Stolen Device

Revised: July 11, 2014

What’s New: Added a note about how ACL behavior has changed in version 7.5+ of the Wireless LAN Controller.

When a previously provisioned device is reported lost or stolen, the device must be denied access to prevent unauthorized access to the network.

A first level of defense to protect against a lost or stolen device is to enforce the use of a PIN lock, a passcode required to access the device that may lock the device automatically after a short period of inactivity (typically five to ten minutes). This can also be enhanced by erasing all data on the mobile device after a number of failed passcode attempts or performing a selective wipe. This and other rules may be enforced by the integration of Cisco ISE with a Mobile Device Manager.

The Cisco ISE offers different ways to prevent a lost or stolen device from connecting to the network. The My Devices Portal allows the employee to mark a device as lost and prevent others from gaining unauthorized access with that device. In addition, if the device is connected to the network when the device is marked as lost, the ISE may issue a Change of Authorization (CoA) to force the endpoint off the network.

The administrator is also able to blacklist a device and force the endpoint off the network. In addition, the administrator is able to use Endpoint Protection Services (EPS) to quarantine an endpoint from the network.

Employees and administrators have different capabilities to block lost or stolen devices:

Employees:
From the My Devices Portal:
- Report devices as lost.
- Enforce a PIN lock through the MDM.
- Initiate a remote device wipe through the MDM.
- Reinstate a device to regain access without having to register the device again.

Note: Devices that have been fully wiped cannot be restored by ISE and will need to re-register to recover the certificate and WiFi profile.
Blacklist Identity Group

The Blacklist identity group is system generated and maintained by ISE to prevent access to lost or stolen devices. In this design guide, two authorization profiles are used to enforce the permissions for wireless and wired devices within the Blacklist:

- Blackhole WiFi Access
- Blackhole Wired Access

The Blacklist Identity Group is displayed by clicking Administration > Identity Management > Groups > Endpoint Identity Groups. Figure 22-1 shows an empty Blacklist identity group containing one endpoint.

Figure 22-1  Blacklist Identity Group

Devices that have been blacklisted are assigned to the Blacklist identity group. Both wired and wireless devices can be placed into the Blacklist identity group. An authorization profile is used to define the access granted to the blacklisted devices. Blacklisted device connection requests are redirected to a web page that informs the user that the device is blacklisted.

Administrators:

- Add the endpoint to the Blacklist Identity Group.
- If the endpoint is connected, force it off the network using the Show Live Sessions screen.
- Enforce a PIN lock through the Endpoints screen in ISE.
- Initiate a remote device wipe through the Endpoints screen in ISE.
- Quarantine the endpoint using the ISE’s Endpoint Protection Services feature (employees are not able to reinstate endpoints quarantined by the administrator).
- Revoke the device’s digital certificate.
- Disable the RSA SecurID token.
Blacklisting Wireless Devices

To enforce the blacklist permissions, an authorization rule is defined under **Policy > Authorization**. **Figure 22-2** shows the Wireless Black List Default rule enforcing the Blackhole WiFi Access permissions.

**Figure 22-2  Wireless Black List Default Authorization Rule**

The Blackhole WiFi Access authorization profile is configured under **Policy > Policy > Elements > Results > Authorization Profiles**, as shown in **Figure 22-3**. The Access Type is defined as **ACCESS_ACCEPT** and the following cisco-av-pairs are defined:

- **cisco-av-pair: url-redirect=https://ip:port/blackhole/blackhole.jsp.** The user gets redirected to this page when a device is in the Blacklist identity group.

- **cisco-av-pair: url-redirect-acl=ACL_BLACKHOLE_Redirect.** The Wireless LAN Controller must have an ACL named ACL_BLACKHOLE_Redirect configured for the redirection to work at the campus and a FlexConnect ACL at the branch with the same name.

This authorization profile only allows access to the ISE “Unauthorized Network Access” page to inform the user that access to the network has been denied for that device.
The behavior of the two ACLs in the authorization profile is slightly different between CUWN wireless controllers, such as the CT5508 and Flex 7500, and IOS XE based controllers such as the CT5760 and Catalyst 3850. For CUWN wireless controllers, ACL_BLACKHOLE_Redirect functions as both the ACL which controls web redirection, as well as the ACL which controls what the wireless client is allowed to access on the network.

Figure 22-4 shows how the ACL_BLACKHOLE_Redirect access list is defined in a CUWN WLC to only allow access to the ISE and DNS server. By granting access to DNS and ISE, the endpoint is able to reach the blackhole.jsp web page hosted at the ISE.
The ACL specifies the following access:

- Allow IP access to and from the DNS server (10.230.1.45).
- Allow IP access to and from the ISE Server (10.225.49.15).
- Deny access to and from all other addresses.

**Note**

ACL_BLACKHOLE serves simply as an extra security configuration. CUWN wireless controllers do not make use of this ACL when URL redirection is specified. For CUWN wireless controllers the ACL_BLACKHOLE ACL can be the same as the ACL_BLACKHOLE_Redirect ACL.

**Note**

The ACL behavior has changed in version 7.5+ of the Wireless LAN Controller. The presence of an Airespace ACL Name in the authorization profile affects the webauth redirect functionality for access points operating in FlexConnect mode. For FlexConnect deployments, the ACL_Provisioning Airespace ACL must be removed from the configuration. This implies that there needs to be two independent authorization profiles for provisioning: one for FlexConnect and CUWN wireless controllers and another one for Converged Access wireless controllers. Refer to Appendix E, “Airespace ACLs in WLC 7.5+” for sample configurations.

For endpoints connecting to the branch, a similar FlexConnect ACL is defined and applied to the FlexConnect Group. **Figure 22-5** shows the ACL_BLACKHOLE_Redirect FlexConnect ACL. This ACL is similar to the one used for campus devices, shown above, but defined under Security > Access Control Lists > FlexConnect ACLs.
Figure 22-5  ACL_BLACKHOLE_Redirect FlexConnect ACL

To apply this FlexConnect from the branch, select the appropriate FlexConnect Group and click the Policies tab. Add the ACL_BLACKHOLE_Redirect ACL, as shown in Figure 22-6.

Figure 22-6  Policies for Branch1

On converged access products, namely the CT5760 wireless controller or Catalyst 3850 Series switches, both the BLACKHOLE_ACL_Redirect and BLACKHOLE_ACL ACLs must be configured. An example of the BLACKHOLE_ACL_Redirect ACL is shown below.

```
!  ip access-list extended ACL_BLACKHOLE_Redirect/ Blacklisting REDIRECTION ACL
deny  udp any eq bootpc any eq bootps
deny  udp any host 10.230.1.45 eq domain
deny  ip any host 10.225.49.15
permit ip any any
```

The above ACL specifies the following access:
- Deny DHCP access (bootpc and bootps).
- Deny IP access to and from the DNS server (10.230.1.45).
- Deny IP access to and from the ISE server (10.225.49.15).
Blacklist Identity Group

- Allow (redirect) all other IP access.

The ACL above causes any web traffic (HTTP or HTTPS) from any source to any destination to be redirected to the blacklisted devices web page within the Cisco ISE.

The authorization profile also applies a second, RADIUS specified local ACL (BLACKHOLE_ACL) across the WLAN for network access. The CT5760 and Catalyst 3850 Design use named ACLs. The name of the ACL is sent from the ISE to the Catalyst 3850 Series switch or the CT5760 wireless controller via the RADIUS Airespace-ACL-Name attribute-value pair within the Airespace dictionary. The specific form for the example is as follows:

Airespace-ACL-Name = ACL_BLACKHOLE

The WLAN access-control ACL (ACL_BLACKHOLE) determines what traffic is allowed on the WLAN by the Catalyst 3850 series switch or the CT5760 wireless LAN controller. An example of the BLACKHOLE_ACL ACL is shown below.

```!
ip access-list extended ACL_BLACKHOLE Blacklisting Access Control ACL
   permit udp any eq bootpc any eq bootps
   permit udp any host 10.230.1.45 eq domain
   permit ip any host 10.225.49.15
!
```

The above access-list specifies the following access:

- Allow DHCP access (bootpc and bootps).
- Allow IP access to and from the DNS server (10.230.1.45).
- Allow IP access to and from the ISE server (10.225.49.15).
- Implicitly deny all other IP access.

The ACL above allows traffic from any source to the blacklisted devices webpage within the Cisco ISE.

Once a device is in the Blacklist identity group, future attempts to connect to the network are denied. When a user opens a web browser on a blacklisted device, the session is redirected to the page shown in Figure 22-7.

**Figure 22-7 Unauthorized Network Access**

This device has been identified as lost and does not have network access.
Figure 22-8 shows how a device in the Blacklist attempts to connect to the network and how the Blackhole WiFi Access authorization profile is applied.

Figure 22-8  Device in Blacklist Identity Group

Blacklisting Wired Devices

The user experience when a wired device is blacklisted is similar to a wireless device that has been blacklisted. The ISE authorization policy rule for blacklisting of on-boarded wired devices will be the same for devices connected via Converged Access products and other Catalyst switches for BYOD. When a device is blacklisted and the user attempts to access any web page, the device is re-directed to the portal that lets the user know that the device has been identified as lost. The following steps show how to implement this behavior:

Step 1  Create an ACL_BLACKHOLE downloadable DACL that only allows access to the ISE.

Step 2  Create a URL Redirect ACL called ACL_BLACKHOLE_Redirect on the access layer switch that matches any HTTP or HTTPS traffic.

Step 3  Create a Blackhole Wired Access authorization profile that pushes the DACL and redirect-link to the switch.

Step 4  Define a new rule in the Authorization policy that matches on the blacklisted devices and assigns the authorization profile Blackhole Wired Access.

Creating a Downloadable ACL on ISE

The ACL_BLACKHOLE DACL is created under Policy > Policy Elements > Results > Downloadable ACLs, as shown in Figure 22-9.
The ACL above allows traffic from any source to the blacklisted devices webpage within the Cisco ISE.

Creating the URL REDIRECT ACL on the Switch

The configuration of the URL redirect ACL is the same, regardless of whether the switch is a Converged Access Catalyst 3850 Series switch, or a Catalyst 3750-X series switch. An example of the configuration for the ACL_BLACKHOLE_Redirect ACL on the wired switch is shown below.

```plaintext
!  ip access-list extended ACL_BLACKHOLE_Redirect  / Blacklisting Redirection ACL
  udp any eq bootpc any eq bootps
  udp any host 10.230.1.45 eq domain
  ip any host 10.225.49.15
  permit ip any any
```

Note that this is the same URL redirect ACL used for blacklisted wireless devices for the Catalyst 3850 Series switch, discussed above. Bear in mind that the ACL is only required on the Catalyst 3850 and not on the CT5760 wireless controller because only the Catalyst 3850 supports direct connection of wired clients through its switch ports.

Configuring the Authorization Profile

Define an authorization profile called Blackhole Wired Access under Policy > Policy Elements > Results > Authorization Profiles, as shown in Figure 22-10.
The following cisco-av-pairs are defined:

- cisco-av-pair: url-redirect=https://ip:port/mydevices/blackhole.jsp. The user gets redirected to this page when a device is in the Blacklist identity group.
- cisco-av-pair: url-redirect-acl=ACL_BLACKHOLE_Redirect. The access layer switch must have an ACL named ACL_BLACKHOLE_Redirect configured for the redirection to work.

Creating a Rule in the Authorization Policy

The last configuration step is to create a new rule in the authorization policy that uses the Blackhole Wired Access authorization profile created above when it matches a dot1x wired device which is blacklisted. Figure 22-11 displays the rule.
Once the rules are defined, a blacklisted wired device will be denied access to the network.

**Employees’ My Devices Portal**

Using the My Devices Portal, employees are able to mark any of their devices as Lost to prevent further network access. The portal requires user authentication and displays the devices that have been added or registered by the employee. The My Devices Portal may be accessed from the following URL:

https://<ISE_IP_Address>:8443/mydevices/

In addition to being able to report a device lost or stolen, the portal is used to enforce MDM Actions, such as PIN lock and device wipes through MDM integrations. Figure 22-12 shows the My Devices Portal page.
The portal displays devices assigned to the employee or previously registered using the self-registration portal.

**Reporting a Device as Lost**

The employee is able to edit the device’s description and report a device as lost, as shown in Figure 22-13.

**Figure 22-13  Lost Device**

Before blacklisting a device, ISE displays the warning shown in Figure 22-14.

**Figure 22-14  Blacklist Warning**

Once the device is marked as lost, the device is added to the Blacklist Identity Group. If the device is connected to the network at that time, ISE issues a Change of Authorization (CoA) and forces the device off the network. To verify that the device has been added to the Blacklist Identity group, click Administration > Identity Management > Groups > Endpoint Identity Groups and review the Blacklist. Figure 22-15 shows the MAC address added to the Blacklist.
Reinstating a Device

The My Devices Portal also gives the user the option to reinstate a blacklisted device, allowing the device to regain access to the network. Figure 22-16 shows the Reinstate option.

Before reinstating a device, ISE displays the warning shown in Figure 22-17.
PIN Lock and Device Wipes

The integration with an MDM provides additional device control to the user. With the My Devices Portal, the employee is able to:

- Initiate a Corporate Wipe—Remove settings and applications configured in the MDM policies.
- Initiate a Full Wipe—Remove all information from the device (factory reset).
- Enforce a PIN lock—Lock the device.

Figure 22-18 shows the MDM actions available from the My Devices Portal:

Administrators—Blacklisting a Device

Administrators are able to blacklist a device by adding it manually to the BlackList Identity Group. Click Administration > Groups > Endpoint Identity Groups > Blacklist and add the MAC address of the device to be blacklisted. Figure 22-19 shows the MAC address added to the identity group.
Note that by adding the device to the Blacklist Identity Group, ISE prevents future attempts to connect to the network, but if the user is currently connected to the network, an additional step is required to force the endpoint off the network.

To force a device off the network, click **Operations > Authentications > Show Live Sessions**, as shown in Figure 22-20.

To terminate the endpoint’s session, select Session termination from the CoA Action menu, as shown in Figure 22-21.
Administrators—Blacklisting a Device

The employee has the option to reinstate a device that was blacklisted by the administrator using the My Devices Portal.

**MDM Actions**

The administrator also has the option to initiate MDM actions on the endpoints. To perform an action, click on Administration > Identities > Endpoints and select the appropriate device, as shown in Figure 22-22.

**Figure 22-22 MDM Actions**
Endpoint Protection Services (EPS)

Endpoint Protection Services is a service provided by the ISE to extend the monitoring and controlling capabilities of endpoints. EPS also monitors and changes the authorization state of endpoints. EPS can be used to change the authorization state of an endpoint without having to modify the overall authorization policy. EPS allows the administrator to quarantine or limit access to a device and unquarantine a device or allow full access to the network to reverse the quarantine status.

Note

EPS requires an ISE Advanced license.

To enable EPS, click Administration > System > Settings > Endpoint Protection Services and select Enabled, as shown in Figure 22-23.

Figure 22-23 Enable EPS

Create an authorization profile to define the permissions to specified network services. Click Policy > Policy Elements > Results > Authorization > Authorization Profiles and define a new authorization profile, as shown in Figure 22-24.
Create an EPS Exception policy and rule to be processed before the standard policies are processed. Click Policy > Authorization > Exceptions > Create a New Rule, as shown in Figure 22-25.
Enter a Rule Name and under Conditions create a new condition (**Advanced Option**). Under Expression click **Select Attribute** and select **EPSStatus Equals Quarantine**, as shown in Figure 22-26.

**Figure 22-26   EPS Exception Policy**

Under Permissions, select the previously defined **EPS_Quarantine** Authorization Profile. Figure 22-27 shows the complete Exception policy.

**Figure 22-27   EPS Quarantine Permissions**

To quarantine a device, click **Operations > Endpoint Protection Service** and enter the endpoint’s MAC Address to be quarantined. Under Operation select **Quarantine**, as shown in Figure 22-28.

**Figure 22-28   EPS**

As soon as the administrator clicks **Submit**, the device is forced off the network and future attempts to connect are rejected.
Figure 22-29 shows the EPS_Quarantine authorization profile being applied and how a device is denied access.

**Figure 22-29  Quarantined Endpoints**

EPS provides an extra layer of control to monitor and change the authorization state of endpoints.

Since EPS has higher precedence over blacklisted devices, employees do not have the option to reinstate devices that have been quarantined by the administrator.

To unquarantine a device, enter the device’s MAC address and select **Unquarantine** from the operation pull down menu, as shown in Figure 22-30.

**Figure 22-30  Unquarantine a Device**

The EPS activities are logged by ISE and can be reviewed by clicking **Operations > Reports > Endpoints and Users > Endpoint Session History**. Figure 22-31 shows one of the reports that includes endpoint information.
Administrators—Blacklisting a Device

Chapter 22  Managing a Lost or Stolen Device

Figure 22-31  EPS Logs

Revocation of Digital Certificate

Administrators also have the option of revoking an employee’s digital certificate from the CA server to prevent further use by unauthorized devices. The CA server periodically publishes the Certificate Revocation List (CRL). ISE is configured to validate the certificate presented by the clients against the CRL list. If there is a match, the ISE rejects the digital certificate presented by the client.

The first step is to revoke the digital certificate from the CA server. Figure 22-32 shows how to revoke the digital certificate for username “toby”.

Figure 22-32  Revoking the Digital Certificate on the CA Server

Once the above process is complete, the certificate serial number is added to the Certificate Revocation List (CRL). Figure 22-33 displays the CRL information.
Administrators—Blacklisting a Device

Figure 22-33 Certificate Revocation List

This information is periodically published by the CA server. Figure 22-34 shows the location of the CRL where the ISE can download the list.

Figure 22-34 CRL Distribution Point

The next step is for ISE to be configured with CRL distribution location so that it can periodically download the list and compare it with the certificates presented by the clients. Click Administration > Certificates > Certificate Authority Certificates and configure the CRL values, as shown in Figure 22-35.
Figure 22-35  CRL Location Information on the ISE

Disable the RSA SecurID Token

When a device that has been previously provisioned is reported lost or stolen, the device must be denied access to prevent unauthorized access to the network. In addition, the remote user’s RSA SecurID token must be disabled at the RSA Server so that the remote user cannot use the network. Figure 22-36 shows how to disable the RSA SecurID token at the RSA server.