Call Control Discovery

The call control discovery feature leverages the Service Advertisement Framework (SAF) network service, a proprietary Cisco service, to facilitate dynamic provisioning of inter-call agent information. By adopting the SAF network service, the call control discovery feature allows Cisco Unified Communications Manager to advertise itself along with other key attributes, such as directory number patterns that are configured in Cisco Unified Communications Manager Administration, so other call control entities that also use SAF network can use the advertised information to dynamically configure and adapt their routing behaviors; likewise, all entities that use SAF advertise the directory number patterns that they own along with other key information, so other remote call-control entities can learn the information and adapt the routing behavior of the call.

This chapter contains the following topics:

- Configuration Checklist for Call Control Discovery, page 3-2
- Introducing Call Control Discovery for Cisco Unified Communications Manager, page 3-5
  - Overview of Call Control Discovery, page 3-5
  - Components for the Call Control Discovery Feature, page 3-6
- System Requirements for Call Control Discovery, page 3-16
- Interactions and Restrictions, page 3-16
- Installing and Activating Call Control Discovery, page 3-18
- Configuring Call Control Discovery, page 3-18
  - Considerations for Call Control Discovery Configuration, page 3-19
  - Call Control Discovery Feature Parameters, page 3-23
  - SAF Security Profile Configuration Settings, page 3-25
  - SAF Forwarder Configuration Settings, page 3-26
  - Hosted DN Group Configuration Settings, page 3-31
  - Hosted DN Pattern Configuration Settings, page 3-32
  - CCD Advertising Service Configuration Settings, page 3-34
  - Partition Configuration Settings for Call Control Discovery, page 3-36
  - CCD Requesting Service Configuration Settings, page 3-37
  - Blocked Learned Pattern Configuration Settings, page 3-40
  - Finding Configuration Records for Call Control Discovery, page 3-42
  - Configuring Call Control Discovery (Procedure), page 3-44
Configuration Checklist for Call Control Discovery

The call control discovery feature leverages the Service Advertisement Framework (SAF) network service, a proprietary Cisco service, to facilitate dynamic provisioning of inter-call agent information. By adopting the SAF network service, the call control discovery feature allows Cisco Unified Communications Manager to advertise itself along with other key attributes, such as directory number patterns that are configured in Cisco Unified Communications Manager Administration, so other call control entities that also use SAF network can use the advertised information to dynamically configure and adapt their routing behaviors; likewise, all entities that use SAF advertise the directory number patterns that they own along with other key information, so other remote call-control entities can learn the information and adapt the routing behavior of the call. Table 3-1 provides a checklist for configuring the call control discovery feature in your network. Use Table 3-1 in conjunction with the “Related Topics” section on page 3-47.

### Table 3-1 Call Control Discovery Configuration Checklist

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;Configure the Cisco IOS router as the SAF forwarder.</td>
<td>See the documentation that supports your Cisco IOS router; for example, see the Cisco IOS Service Advertisement Framework Configuration Guide or the Cisco IOS Service Advertisement Framework Command Reference. Cisco Feature Navigator allows you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <a href="http://www.cisco.com/go/cfn">http://www.cisco.com/go/cfn</a>.</td>
</tr>
</tbody>
</table>
| Step 2<br>Configure the SAF security profile for the SAF forwarder (Advanced Features > SAF > SAF Security Profile). You can configure more than one SAF security profile in Cisco Unified Communications Manager Administration. A SAF forwarder, which is a Cisco IOS router that you configured for SAF, handles the publishing requests for the local Cisco Unified Communications Manager cluster and the service advertisements from remote call-control entities. | - SAF Forwarders, page 3-13  
- SAF Security Profile Configuration Settings, page 3-25  
- Considerations for Call Control Discovery Configuration, page 3-19 |
Table 3-1  Call Control Discovery Configuration Checklist (continued)

<table>
<thead>
<tr>
<th>Configuration Steps</th>
<th>Related Procedures and Topics</th>
</tr>
</thead>
</table>
| Step 3              | • SAF Forwarders, page 3-13  
                     | • SAF Forwarder Configuration Settings, page 3-26  
                     | • Considerations for Call Control Discovery Configuration, page 3-19 |
| Configure the SAF forwarders in Cisco Unified Communications Manager Administration (Advanced Features > SAF > SAF Forwarder). Cisco recommends that you configure a primary and backup SAF forwarder for failover support. |
| Step 4              | • Hosted DN Patterns and the CCD Advertising Service, page 3-9  
                     | • Learned Patterns and the CCD Requesting Service, page 3-10  
                     | • Configuring a SAF-Enabled Trunk, page 3-45  
                     | • Considerations for Call Control Discovery Configuration, page 3-19 |
| Configure SAF-enabled SIP and/or H.323 intercluster (non-gatekeeper controlled) trunks (Device > Trunk). The local Cisco Unified Communications Manager cluster uses SAF-enabled trunks that are assigned to the CCD requesting service to route outbound calls to remote call-control entities that use the SAF network. The Cisco Unified Communications Manager cluster advertises the SAF-enabled trunks that are assigned to the CCD advertising service along with the range of hosted DNs; therefore, when a user from a remote call-control entity makes an inbound call to a learned pattern on this Cisco Unified Communications Manager, this Cisco Unified Communications Manager receives the inbound call from this SAF-enabled trunk and routes the call to the correct DN. |
| Step 5              | • Hosted DN Patterns and the CCD Advertising Service, page 3-9  
                     | • Hosted DN Group Configuration Settings, page 3-31  
                     | • Identifying Which Hosted DN Patterns Belong to a Hosted DN Group, page 3-46  
                     | • Considerations for Call Control Discovery Configuration, page 3-19 |
| Configure the Hosted DN groups. Cisco recommends that you group the hosted DN patterns by location; for example, hosted DN patterns that represent different zip codes for a city may get grouped together. (Call Routing > Call Control Discovery > Hosted DN Group) Hosted DN groups are a collection of hosted DN patterns that you group together in Cisco Unified Communications Manager Administration. You assign a hosted DN group to a CCD advertising service in Cisco Unified Communications Manager Administration, and the CCD advertising service publishes all the hosted DN patterns that are a part of the hosted DN group. You can only assign one Hosted DN group to one call control discovery advertising service. |
| Step 6              | • Hosted DN Patterns and the CCD Advertising Service, page 3-9  
                     | • Hosted DN Pattern Configuration Settings, page 3-32  
                     | • Considerations for Call Control Discovery Configuration, page 3-19 |
| Configure the Hosted DN patterns. (Call Routing > Call Control Discovery > Hosted DN Pattern) Hosted directory number (DN) patterns are patterns that represent directory numbers that belong to a call-control entity; for example, hosted DN patterns that you configure in Cisco Unified Communications Manager Administration are a range of directory numbers that belong to the local Cisco Unified Communications Manager cluster that you want to advertise to remote call-control entities. The CCD advertising service publishes the hosted DN patterns to the active SAF forwarder. |
To publish the hosted DNs for the local Cisco Unified Communications Manager cluster, configure the Call Control Discovery Advertising service. (Call Routing > Call Control Discovery > Advertising Service) You can configure as many CCD advertising services as you want.

The call control discovery advertising service, which resides in Cisco Unified Communications Manager, allows the local Cisco Unified Communications Manager cluster to advertise its hosted DNs and the PSTN failover configuration to the remote call-control entities that use the SAF network.

Configure a partition that is used specifically for call control discovery. (Call Routing > Call Control Discovery > Partition) This route partition gets used exclusively by the CCD requesting service to ensure that all learned patterns get placed in digit analysis under the route partition.

You assign the partition to the CCD Requesting Service in Cisco Unified Communications Manager Administration.

Tip The partition that you assign to the CCD requesting service must belong to a calling search space that the devices can use for calling the learned patterns, so assign the partition to the calling search space that you want the devices to use. If you do not assign a calling search space that contains the partition to the device, the device cannot call the learned patterns.

To ensure that the local Cisco Unified Communications Manager cluster can listen for advertisements from the SAF network, configure one call control discovery requesting service. (Call Routing > Call Control Discovery > Requesting Service) You can only configure one CCD requesting service.

The call control discovery requesting service, which resides in the local Cisco Unified Communications Manager, allows the local Cisco Unified Communications Manager to listen for hosted DN advertisements from remote call-control entities that use the SAF network.

If you have not already done so, configure your remote call-control entity to use the SAF network; for example, configure Cisco Unified Communications Manager Express or other Cisco Unified Communications Manager clusters for the SAF network.

See the documentation that supports your remote call-control entity; for example, the Cisco Unified Communications Manager Express documentation.

After you configure call control discovery, you may block learned patterns that remote call-control entities send to the local Cisco Unified Communications Manager. (Call Routing > Call Control Discovery > Blocked Learned Patterns)
Introducing Call Control Discovery for Cisco Unified Communications Manager

This section contains information on the following topics:

- Overview of Call Control Discovery, page 3-5
- Components for the Call Control Discovery Feature, page 3-6

Overview of Call Control Discovery

The call control discovery feature leverages the Service Advertisement Framework (SAF) network service, a proprietary Cisco service, to facilitate dynamic provisioning of inter-call agent information. By adopting the SAF network service, the call control discovery feature allows the local Cisco Unified Communications Manager to advertise itself along with other key attributes, such as directory number patterns that are configured in Cisco Unified Communications Manager Administration, so other call control entities that also use SAF network can use the advertised information to dynamically configure and adapt their routing behaviors; likewise, all entities that use SAF advertise the directory number patterns that they own along with other key information, so other remote call-control entities can learn the information and adapt the routing behavior of the call. Additionally, the call control discovery feature enables the network to facilitate communication between SAF-supported entities, instead of relying on additional servers to enable intercall agent communications.

Tip

The call control discovery feature eliminates the need for redundant SIP proxies or complex gatekeeper configurations, which provide dial plan resolution and reachability status of remote call-control entities in the network.

With the call control discovery feature, each local Cisco Unified Communications Manager cluster can perform the following tasks:

- Establish an authenticated connection with the SAF network
- Advertise the cluster to the SAF network by providing the IPv4 address or hostname of the server, the signaling protocol and port numbers that the SAF network uses to contact the cluster, and the directory number patterns that are configured in Cisco Unified Communications Manager Administration for the cluster
- Register with the SAF network to listen for requests that are coming from other remote call-control entities that also use the SAF-related network
- Use the information that is learned from the advertisements to dynamically add patterns to its master routing table, which allows Cisco Unified Communications Manager to route and set up calls to these destinations by using the associated IP address and signaling protocol information
- When connectivity to a remote call-control entity gets lost, the SAF network notifies Cisco Unified Communications Manager to mark the learned information as IP unreachable. The call then goes through the PSTN.
- Provide redundancy to advertise and listen for information, so if a server loses connectivity to its primary SAF forwarder for any reason, another backup SAF router can be selected to advertise and listen for information.
Components for the Call Control Discovery Feature

This section contains detailed information on the following topics:

- Call Control Discovery Terminology, page 3-6
- Call Control Discovery Advertising Service, page 3-8
  - The CCD Advertising Service and SAF-enabled Trunks, page 3-8
  - Hosted DN Patterns and the CCD Advertising Service, page 3-9
- Call Control Discovery Requesting Service, page 3-10
  - Learned Patterns and the CCD Requesting Service, page 3-10
  - The CCD Requesting Service and SAF-Enabled Trunks, page 3-11
  - Network Withdrawal Support, page 3-13
- SAF Forwarders, page 3-13

Tip: All components for the call control discovery feature work together, so review all sections to understand how the feature works.

Call Control Discovery Terminology

Table 3-2 provides a brief overview of terminology that is associated with the call control discovery feature. For detailed information on each concept, click the links in the Description column in the table.

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Description</th>
</tr>
</thead>
</table>
| Call control discovery (CCD) advertising service                            | • Resides in Cisco Unified Communications Manager  
  • Advertises the PSTN failover configuration and hosted DN patterns along with the SAF trunk access information for the local Cisco Unified Communications Manager cluster to the remote call-control entities that use the SAF network.  
  • Configured under Call Routing > Call Control Discovery > Advertising Service in Cisco Unified Communications Manager Administration  
  • For More Information—Call Control Discovery Advertising Service, page 3-8 |
## Call Control Discovery Terminology (continued)

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Description</th>
</tr>
</thead>
</table>
| Call control discovery (CCD)       | - Resides in Cisco Unified Communications Manager  
| requesting service                 | - Allows the local Cisco Unified Communications Manager to listen for advertisements from remote call-control entities that use the SAF network.  
|                                   | - Ensures that learned patterns (hosted DN patterns from remote call-control entities) get inserted into digit analysis on the local Cisco Unified Communications Manager  
|                                   | - Performs load balancing for calls to learned patterns  
|                                   | - Handles withdrawals for Cisco Unified Communications Manager from the SAF network  
|                                   | - Configured under Call Routing > Call Control Discovery > Requesting Service in Cisco Unified Communications Manager Administration.  
|                                   | - For More Information—Call Control Discovery Requesting Service, page 3-10                                                                                                                                |
| Hosted DN patterns                 | - Directory number patterns that belong to the local call-control entity  
|                                   | Tip For example, hosted DN patterns that you configure in Cisco Unified Communications Manager Administration under Call Routing > Call Control Discovery > Hosted DN Pattern are directory numbers pattern ranges for the local Cisco Unified Communications Manager cluster that you want to advertise to remote call-control entities.  
|                                   | - For the local Cisco Unified Communications Manager, published by the CCD advertising service to the SAF forwarder.  
|                                   | - For More Information—Hosted DN Patterns and the CCD Advertising Service, page 3-9                                                                                                                       |
| Learned patterns                   | - Patterns that are inserted into digit analysis by the CCD requesting service  
|                                   | - Can be manually purged or blocked on the local Cisco Unified Communications Manager  
|                                   | - Viewed in RTMT  
|                                   | - For More Information—Learned Patterns and the CCD Requesting Service, page 3-10                                                                                                                      |
| SAF forwarder                      | - Cisco IOS router  
|                                   | - Notifies the local Cisco Unified Communications Manager when remote call-control entities advertise their hosted DNs patterns.  
|                                   | - Receives publish requests from the local Cisco Unified Communications Manager cluster so that Cisco Unified Communications Manager can advertise the hosted DN patterns for the cluster.  
|                                   | - For More Information—SAF Forwarders, page 3-13                                                                                                                                                    |
Introducing Call Control Discovery for Cisco Unified Communications Manager

Chapter 3      Call Control Discovery

Table 3-2  Call Control Discovery Terminology (continued)

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAF-enabled trunks</td>
<td>• SAF-enabled trunks that are assigned to the CCD advertising service handle inbound calls from remote call-control entities that use the SAF network</td>
</tr>
<tr>
<td></td>
<td>• SAF-enabled trunks that are assigned to the CCD requesting service handle outgoing calls to learned patterns</td>
</tr>
<tr>
<td></td>
<td>• For More Information—The CCD Advertising Service and SAF-enabled Trunks, page 3-8 and Learned Patterns and the CCD Requesting Service, page 3-10</td>
</tr>
</tbody>
</table>

Call Control Discovery Advertising Service

The call control discovery advertising service, which resides in Cisco Unified Communications Manager, allows the local Cisco Unified Communications Manager cluster to advertise the PSTN failover configuration, the hosted DN patterns, and the SAF-enabled trunk access information for its cluster to the remote call-control entities that use the SAF network. In Cisco Unified Communications Manager Administration under Call Routing > Call Control Discovery > Advertising Service, you can configure as many CCD advertising services as you want.

This section contains information on the following topics:

- The CCD Advertising Service and SAF-enabled Trunks, page 3-8
- Hosted DN Patterns and the CCD Advertising Service, page 3-9

The CCD Advertising Service and SAF-enabled Trunks

Consider the following information, which relates to how SAF-enabled trunks work with the CCD advertising service.

- After you configure SAF-enabled trunks in Cisco Unified Communications Manager Administration, you can choose one SIP trunk and one H.323 (non-gatekeeper controlled) trunk to associate with the CCD advertising service in the CCD Advertising Service window. The CCD advertising service advertises the hosted DN patterns, the PSTN failover configuration for the hosted DN patterns, the IP address for the node, the dynamic port number for the H.323 trunk, the QSIG configuration for the H.323 trunk, standard port 5060 for the SIP trunk, and the SIP route header information. It advertises the information for each trunk that is assigned to the CCD advertising service.

- SAF-enabled trunks do not have preconfigured destinations. For inbound calls from remote call-control entities, the local Cisco Unified Communications Manager uses the advertised dynamic trunk port number and/or SIP route header to find the proper dynamic trunk to process the call.

- The CCD advertising service, which runs on the same nodes as its assigned/selected trunks, advertises the same set of hosted DN pattern ranges for each type of trunk.

- For inbound calls from remote call-control entities to the local Cisco Unified Communications Manager, the call gets routed to the appropriate SAF-enabled trunk that is advertised by the CCD advertising service. For H.323 trunks, the incoming called party prefixes get applied to the called party number before the call gets routed.
• H.323 trunks support different features than SIP trunks; for example, H.323 supports QSIG, and SIP supports presence. If your feature support requires that you assign both a H.323 and SIP trunk to the CCD advertising service, assign both trunk types. If your feature support allows you to assign one trunk type, Cisco recommends that you assign one trunk to the CCD advertising service that best serves the cluster.

• If you assigned both a SAF-enabled SIP trunk and SAF-enabled H.323 (non-gatekeeper controlled) intercluster trunk to the CCD advertising service, load sharing of inbound calls occurs for the two trunks.

• The QSIG Variant and ASN.1 ROSE OID Encoding settings in the H.323 Configuration window get advertised by the CCD advertising service. These settings impact decoding of QSIG messages for inbound tunneled calls; for call control discovery, they do not impact outgoing calls.

Hosted DN Patterns and the CCD Advertising Service
Hosted directory numbers (DNs) patterns are a range of directory number patterns that belong to the call-control entity; for example, hosted DN patterns that you configure in Cisco Unified Communications Manager Administration under Call Routing > Call Control Discovery > Hosted DNs Pattern are directory numbers patterns for the local Cisco Unified Communications Manager that you want to advertise to remote call-control entities. The CCD advertising service publishes the hosted DN patterns for the local cluster to the active SAF forwarder.

• The CCD advertising service on the local Cisco Unified Communications Manager sends an advertising publish request on behalf of the hosted DN service in Cisco Unified Communications Manager to the primary SAF forwarder.

• Each hosted DN pattern belongs to a hosted DN group, which you assign to the CCD advertising service. Placing hosted DN patterns into a hosted DN group ensures that a CCD advertising service can advertise multiple patterns.

• When you update configured hosted DN patterns in the Hosted DN Patterns window in Cisco Unified Communications Manager Administration, the CCD advertising service resends a publishing request with the updated patterns to the active SAF forwarder. A publishing request gets sent for each trunk that is assigned to the CCD advertising service.

• If a Hosted DN pattern gets added or deleted in Cisco Unified Communications Manager Administration, the CCD advertising service sends a new publish request with a higher service version number to the SAF network.

• If you change the hosted DN group that is assigned to the CCD advertising service, the CCD advertising service publishes the patterns from the newly-updated hosted DN group along with a higher version number for each assigned SAF-enabled trunk.

• The CCD advertising service attempts to send many hosted DN patterns in a single publishing request. If there are more hosted DN patterns than can be sent in a single request, the local Cisco Unified Communications Manager sends multiple requests, each with a unique service identifier.

• For some clusters, the same hosted DN pattern may be published multiple times based on the SAF-trunk selection in the CCD advertising service configuration window. For example, hosted DN pattern 8902XXXX gets published twice for each node and each SAF-enabled trunk if the CCD advertising service configuration contains both a SAF-enabled SIP and H.323 (non-gatekeeper controlled) trunk. If the Cisco Unified Communications Manager group for the trunk contains two nodes, four publishing requests for 8902XXX get sent. This approach ensures that the receiving entity performs load sharing.

• When you choose a different hosted DN group in the CCD Advertising Service window in Cisco Unified Communications Manager Administration, the service sends a request to the SAF forwarder to unpublish the hosted DN group and then publishes the updated configuration.
Introducing Call Control Discovery for Cisco Unified Communications Manager

If a hosted DN group association changes, a SAF trunk association changes, a SAF trunk is reset in Cisco Unified Communications Manager Administration, or the CCD advertising service is reset, the CCD advertising service will unpublish the previous request and publish it again with a new service ID; in addition, other clusters receive a withdrawal service notification from the SAF network, followed by a new notification from the SAF network.

For More Information
Related Topics, page 3-47

Call Control Discovery Requesting Service

The call control discovery requesting service which resides in Cisco Unified Communications Manager, allows the local Cisco Unified Communications Manager to listen for advertisements from remote call-control entities that use the SAF network. The CCD requesting service is also responsible for inserting learned patterns from the remote call-control entities into digit analysis and the local cache. In Cisco Unified Communications Manager Administration under Call Routing > Call Control Discovery > Requesting Service, you can configure only one CCD requesting service.

After the SAF forwarder notifies the local Cisco Unified Communications Manager that remote call-control entities are advertising information, the CCD requesting service inserts the learned patterns along with a configured partition into digit analysis on the local Cisco Unified Communications Manager, and locally caches the learned patterns and the associated PSTN failover configuration from the remote call-control entity.

This section contains information on the following topics:

- Learned Patterns and the CCD Requesting Service, page 3-10
- The CCD Requesting Service and SAF-Enabled Trunks, page 3-11
- Network Withdrawal Support, page 3-13

Learned Patterns and the CCD Requesting Service

Remote call-control entities, such as other Cisco Unified Communications Manager clusters or Cisco Unified Communications Manager Express, request that their hosted DN patterns get advertised to other remote call-control entities. For Cisco Unified Communications Manager, after the CCD requesting service inserts the advertised DN patterns into digit analysis on the local Cisco Unified Communications Manager, Cisco Unified Communications Manager considers the pattern to be a learned pattern.

Consider the following information about learned patterns and the CCD requesting service:

- The CCD requesting service on the local Cisco Unified Communications Manager subscribes its primary SAF forwarder to the hosted DN service in order to learn about the hosted DN patterns that are advertised by the remote call-control entities. For the CCD requesting service to subscribe to the hosted DN service, you must assign a SAF-enabled trunk to the service and you must activate the service in the CCD Requesting Service Configuration window.
- If the local Cisco Unified Communications Manager receives overlapping DN patterns from remote call-control entities in single or multiple advertisements, Cisco Unified Communications Manager performs a best match for routing the call. For example, Cisco Unified Communications Manager receives patterns 813XXXX and 8135XXX. If a user dials 8135233, Cisco Unified Communications Manager routes the call to the trunk that is associated with pattern 8135XXX.
When a learned pattern from a remote call-control entity such as Cisco Unified Communications Manager Express is the same as a locally configured static pattern, the local Cisco Unified Communications Manager uses the calling search space configuration for the calling device to determine whether to route the call to the local or learned pattern.

The CCD requesting service can identify duplicate learned patterns from remote call-control entities, such as other Cisco Unified Communications Manager clusters or Cisco Unified Communications Manager Express. How the CCD requesting service handles the patterns depends on your feature parameter configuration for call control discovery in Cisco Unified Communications Manager Administration. If the Issue Alarm for Duplicate Learned Pattern feature parameter is set to True, the CCD requesting service issues an alarm and stores the duplicate learned patterns; calls that use those patterns get load balanced among different call-control entities.

If a call to a learned pattern cannot go over IP, the CCD requesting service routes the call via the PSTN. Be aware that the CCD requesting service redirects a call to the DID number based on the PSTN failover configuration for the learned pattern. If configured, the AAR calling search space for the calling device gets used to redirect the call during PSTN failover.

If the CCD requesting service receives a learned pattern that is advertised by its own cluster, Cisco Unified Communications Manager ignores the patterns; for example, if a node in the same cluster as the requesting service advertises the learned patterns, Cisco Unified Communications Manager discards the patterns.

The CCD requesting service performs regular expression checking for all learned patterns and converts lowercase wildcards to uppercase wildcards.

If you want to do so, you can purge learned patterns that you no longer want to use, and you can block the learned patterns so that the local Cisco Unified Communications Manager ignores the patterns when they are advertised by remote call-control entities. For example, if you want to block a learned pattern with prefix 235 from a remote call-control entity with IP address of 111.11.11.11, you can block the pattern specifically for this call-control entity by entering the relevant information in the Block Learned Patterns window; in this example, after you save the configuration, the CCD requesting service searches the local cache and purges the learned patterns with 235 prefix from the remote call-control entity with IP address of 111.11.11.11. Any subsequent notifications with this information gets blocked and ignored by the local Cisco Unified Communications Manager. Be aware that blocking and purging of patterns is based on exact match; for example, configuring 235XX blocks 235XX, not any subsets of that pattern. Be aware that if you do not specify a remote call-control entity or remote IP address, Cisco Unified Communications Manager purges and blocks the pattern for all remote call-control entities that advertise the pattern.

You can view purged and blocked learned patterns in the Find and List Blocked Learned Patterns window in Cisco Unified Communications Manager Administration. These purged or blocked patterns do not display in RTMT. If you delete a blocked pattern from Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager can relearn those patterns if they are still available in the SAF network (and if the maximum number of learned patterns has not been reached for the cluster).

The CCD Requesting Service and SAF-Enabled Trunks

When you configure the CCD requesting service, you assign a SAF-enabled trunk to the service. Consider the following information on how the CCD requesting service works with SAF-enabled trunks:

- Cisco Unified Communications Manager routes outbound calls over SAF-enabled SIP or H.323 intercluster (non-gatekeeper controlled) trunks to remote call-control entities that use the SAF network; that is, the SAF-enabled trunks that you assign to the CCD requesting service manage outgoing calls to the learned DN patterns from the remote call-control entities.
Chapter 3 Call Control Discovery

Introducing Call Control Discovery for Cisco Unified Communications Manager

- If the SAF-enabled trunk uses a Cisco Unified Communications Manager group with two Cisco Unified Communications Manager nodes, the CCD requesting service runs on each node after the SAF-enabled trunk registers with the Cisco Unified Communications Manager.

- When the device pool for a SAF-enabled trunk on a remote Cisco Unified Communications Manager contains three Cisco Unified Communications Manager nodes, the trunk runs on all three nodes and advertises the hosted DN service with the same DN patterns. The local Cisco Unified Communications Manager that subscribes to the Hosted DN service receives three advertisements with identical DN patterns but with different IP addresses for the 3 nodes. The CCD requesting service adds the DN patterns into its local cache and associates the patterns with the IP addresses of the three nodes. For an outbound call to a remote Cisco Unified Communications Manager, the CCD requesting service provides the dialed pattern and list of Cisco Unified Communications Managers that are associated with the DN to a SAF-enabled trunk that is assigned to the CCD requesting service. Load balancing occurs, as indicated in Table 3-3 on page 3-12. The trunk establishes the call in the order that is available to the trunk, and it goes to the next node in the list when a node is not available.

- The CCD requesting service provides the IP address and port number for the remote call-control entity to the SAF-enabled trunk.

- SAF-enabled trunks do not have preconfigured destinations. For outgoing calls to learned patterns, call control discovery provides the destination IP addresses to a dynamic trunk on a per call basis.

- The remote call-control entity determines whether QSIG tunneling is required for outgoing calls over H.323 trunks. If the remote call-control entity advertises that QSIG tunneling is required, the QSIG message is tunneled in the message of the outgoing call, even if the H.323 Configuration window in Cisco Unified Communications Manager Administration indicates that QSIG support is not required.

- The CCD requesting service performs round-robin load balancing for calls to learned patterns by considering learned pattern protocols, its local trunks, and IP addresses of the remote call-control entity that advertised the patterns. Table 3-3 on page 3-12 shows how the CCD requesting service load balances calls to learned patterns by using SAF-enabled SIP and H.323 intercluster trunks.

Table 3-3  Round-Robin Load Balancing for Calls to Learned Patterns

<table>
<thead>
<tr>
<th>Call</th>
<th>How it works</th>
</tr>
</thead>
<tbody>
<tr>
<td>For the first call to 8408XXXX</td>
<td>The CCD requesting service selects the SIP trunk, and the call gets routed to the SIP trunk with the learned SIP trunk IP addresses of 10.1.1.1/5060, 10.1.1.2/5060.</td>
</tr>
<tr>
<td>For the second call to 8408XXXX</td>
<td>The CCD requesting service selects the H323 intercluster trunk with learned H323 trunk IP addresses of 10.1.1.1/3456, 10.1.1.2/7890.</td>
</tr>
<tr>
<td>For the third call to 8408XXXX</td>
<td>The CCD requesting service selects the SIP trunk, and the call gets routed to the SIP trunk with the learned SIP trunk IP addresses of 10.1.1.2/5060, 10.1.1.1/5060.</td>
</tr>
<tr>
<td>For the fourth call to 8408XXXX</td>
<td>The CCD requesting service selects the H.323 intercluster trunk with the learned H.323 trunk IP addresses of 10.1.1.2/7890, 10.1.1.1/3456.</td>
</tr>
</tbody>
</table>
Network Withdrawal Support

The CCD requesting service handles withdrawals from the SAF network, as described in the following bullets:

- When the remote call-control entity unpublishes specific learned patterns, the CCD requesting service purges those learned patterns from the local cache and digit analysis when it receives a source withdrawal request from the SAF network; in this case, no calls can occur to those learned patterns.

- When the SAF forwarder loses network connection with its call-control entity, the SAF forwarder withdraws those learned patterns that were published by the call control entity. In this case, CCD requesting service marks those learned patterns as unreachable via IP, and the calls gets routed through the PSTN gateway.

  When a broken connection cannot be restored and if no new notification requests come in before the PSTN failover timer times out, the CCD requesting service unregisters all unreachable learned patterns from digit analysis and purges them from its local cache. In this case, no calls to these learned patterns occur.

- When the local Cisco Unified Communications Manager loses the TCP connection to both the primary and secondary SAF forwarder, the CCD requesting service marks all learned patterns as IP unreachable after the timer for the CCD Learned Pattern IP Reachable Duration feature parameter expires; in this case, all calls to learned patterns get routed through the PSTN gateway. If a connection to the SAF network does not get restored before the timer for the CCD PSTN Failover Duration parameter expires, the CCD requesting service unregisters all unreachable learned patterns from digit analysis and purges them from its local cache. Calls to the purged learned patterns fail.

- When the local Cisco Unified Communications Manager loses the TCP connection to the SAF forwarder, that SAF forwarder contacts all other SAF forwarders. In this case, the other SAF forwarders notify their call control entities, and the call control entities mark their patterns as unreachable via IP after their unreachable pattern duration timer expires (for Cisco Unified Communications Manager, this is the CCD Learned Pattern IP Reachable Duration feature parameter). For Cisco Unified Communications Manager, if a connection to the SAF network does not get restored before the timer for the CCD PSTN Failover Duration parameter expires, the CCD requesting service unregisters all unreachable learned patterns from digit analysis and purges them from its local cache. Calls to the purged learned patterns fail.

For More Information
Related Topics, page 3-47

SAF Forwarders

A SAF forwarder, which is a Cisco IOS router configured for SAF, notifies the local Cisco Unified Communications Manager cluster when remote call-control entities advertise their hosted DNs patterns. In addition, the SAF forwarder receives publishing requests from the local Cisco Unified Communications Manager cluster for each configured and registered trunk that is configured in the CCD Advertising Service window; the publishing request contains the Hosted DN patterns for the Cisco Unified Communications Manager, the PSTN failover configuration, the listening port for the trunk, and, for SIP trunks, the SIP route header field, which contains a URI for the trunk.
Table 3-4 describes the SAF deployment models that Cisco Unified Communications Manager supports.

**Table 3-4 SAF Deployment Models**

<table>
<thead>
<tr>
<th>Deployment Models</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clusterwide</td>
<td>All nodes in the cluster can connect to all SAF forwarders.</td>
<td>The clusterwide deployment model can support primary and backup SAF forwarders.</td>
</tr>
<tr>
<td>Node-specific</td>
<td>Particular nodes in the cluster are assigned to the SAF forwarders, and those nodes prioritize these SAF forwarders over other configured SAF forwarders in the network; this means that the particular nodes always contact the assigned SAF forwarders first over other configured SAF forwarders.</td>
<td>The node-specific deployment model can support primary and backup SAF forwarders. This deployment model is recommended for cluster over WAN deployments where each node in the cluster is separated geographically and you route local traffic through local nodes; for COW deployments, you can configure multiple sets of primary and backup SAF forwarders to support different geophysical locations. You can assign up to two SAF forwarders to a particular node.</td>
</tr>
</tbody>
</table>

You can configure a single SAF forwarder, which provides no failover support, or you configure a primary and backup SAF forwarder to provide failover support. With primary and backup SAF forwarders, the Cisco Unified Communications Manager advertises to and subscribes to the backup SAF forwarder when the primary SAF forwarder is unavailable.

The SAF forwarder contains the IPv4 address and port that Cisco Unified Communications Manager uses to communicate with the SAF network. At start-up time, the SAF client control, which is a nonconfigurable, inherent component of Cisco Unified Communications Manager, marks the first SAF forwarder that registers with Cisco Unified Communications Manager as the primary SAF forwarder. Be aware that the primary SAF forwarder subscribes to the hosted DN services; the backup does not perform this task. The backup SAF forwarder immediately gets promoted to the primary SAF forwarder if/when the primary SAF forwarder becomes unavailable for any reason.

The SAF client control component in Cisco Unified Communications Manager maintains the connection to the SAF forwarder by sending keepalive messages to the SAF forwarder at regular intervals. The SAF client control component experiences keepalive response timeouts with network errors, TCP connection failures, or SAF forwarder failures. When the primary SAF forwarder becomes unreachable, the backup SAF forwarder automatically becomes the primary SAF forwarder, and the SAF client component in Cisco Unified Communications Manager tries to establish a connection with the failed SAF forwarder. When the connection is successfully established, the SAF forwarder gets designated again as the backup SAF forwarder. Under these circumstances, the SAF client control component uses the newly (currently) promoted primary SAF forwarder and notifies the CCD advertising and requesting services that the current primary SAF forwarder is being used. The CCD services send all publishing and subscription requests to the current primary SAF forwarder, and the current primary SAF forwarder sends notifications for all the Hosted DNs service advertisements that it receives to the SAF client control component, which forwards the advertisements to the CCD requesting service. The CCD requesting service compares the notifications that it received from the backup SAF forwarder with its cached information and updates, deletes or adds new information, as appropriate. The SAF client control
component attempts to reconnect to the failed SAF forwarder at regular intervals. When the connection attempt is successful, the SAF client control component registers again with the previously failed SAF forwarder and redesignates the other SAF forwarder as the backup.

Tip
Cisco Unified Communications Manager always advertises to and subscribes to the primary SAF forwarder, even when you have more than 2 SAF forwarders configured in the database. If the primary SAF forwarder gets deleted from the database, then the backup SAF forwarder automatically becomes the primary SAF forwarder, and Cisco Unified Communications Manager promotes another configured SAF forwarder to the backup SAF forwarder.

For clusterwide deployments, you cannot designate the primary and backup SAF forwarders. The Cisco Unified Communications Manager database sends an ordered list of SAF forwarders to the Cisco Unified Communications Manager.

If one or both of the SAF forwarders do not work, Cisco Unified Communications Manager does not attempt to connect to a third SAF forwarder, even if a third SAF forwarder is configured. If the connection is lost for the primary and backup SAF forwarder, the Cisco Unified Communications Manager does not connect to the third SAF forwarder, even if a third SAF forwarder is configured.

If the CCD advertising or requesting service loses connection with SAF network, the SAF forwarder informs all other call control discovery services about the service interruption. The client continually attempts to register to the SAF forwarder. After the CCD service reconnects with the SAF network, the SAF forwarder immediately informs all CCD services about the service restoration.

When the SAF forwarder detects a TCP connection failure with other SAF forwarders or one of its external clients, such as Cisco Unified Communications Manager or Cisco Unified Communications Manager Express, Cisco Unified Communications Manager marks learned patterns as unreachable after it receives a network withdrawal notification from the SAF forwarder. All subsequent calls to these learned patterns get routed over the PSTN by using the PSTN failover configuration for the unreachable learned patterns. The timer for the CCD PSTN Failover Duration feature parameter starts as soon as the network withdrawal notification is received. If Cisco Unified Communications Manager receives another network withdrawal notification when the timer is going, Cisco Unified Communications Manager restarts the timer.

Tip
Cisco Unified Communications Manager uses digest authentication (SHA1) to communicate with the SAF forwarder. You configure a SAF Forwarder security profile, which includes the username and password in requests that Cisco Unified Communications Manager sends to the SAF forwarder; the requests must include the MESSAGE INTEGRITY attribute to include the username and password.

When a connection loss occurs between the SAF forwarder and the Cisco Unified Communications Manager, for example, a cable for the server or router gets unplugged, the registration status may look correct, even when it is not. In this case, patterns may appear to be reachable until the SAF keepalive timer (on the SAF forwarder) or the TCP timer expires. After the timer for the TCP timer expires, the patterns are marked as unreachable.

For More Information
- Related Topics, page 3-47
- Cisco IOS Service Advertisement Framework Configuration Guide
- Cisco IOS Service Advertisement Framework Command Reference
System Requirements for Call Control Discovery

The following system requirements exist for Cisco Unified Communications Manager:

- Local Cisco Unified Communications Manager 8.0(2) (or higher) cluster
- SAF-enabled SIP or H.323 intercluster (non-gatekeeper controlled) trunks
- Remote call-control entities that support and use the SAF network; for example, other Cisco Unified Communications Manager 8.0(2) (or higher) clusters or Cisco Unified Communications Manager Express servers
- Cisco IOS router(s) that are configured as SAF forwarders

**Tip**
Cisco Feature Navigator allows you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to [http://www.cisco.com/go/cfn](http://www.cisco.com/go/cfn).

Interactions and Restrictions

**Autonomous System**

All Cisco Unified Communications Manager clusters are limited to advertised or learned routes within the same autonomous system (AS).

**BLF Subscriptions**

If a user wants to subscribe BLF status of a SAF learned pattern, Cisco Unified Communications Manager sends a SIP subscribe message over a SIP trunk to the remote cluster.

This functionality is supported with SAF-enabled SIP trunks only (not with SAF-enabled H.323 trunks).

**Bulk Administration Tool**

In the Bulk Administration Tool, you can import and export the configuration for SAF security profiles, SAF forwarder, CCD advertising service, CCD requesting service, hosted DN groups, and hosted DN patterns, and so on. For information on how to import and export the configuration, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

**Call Detail Records**

Cisco Unified Communications Manager supports redirecting onBehalfOf as SAFCCDRequestingService with a redirection reason as SS_RFR_SAF_CCD_PSTNFAILOVER, which indicates that the call is redirected to a PSTN failover number.

For more information on call detail records, see the *Cisco Unified Communications Manager Call Detail Records Administration Guide*.

**Incoming Called Party Settings**

The H.323 protocol does not support the international escape character +. To ensure that the correct DN patterns get used with SAF/call control discovery for inbound calls over H.323 gateways/trunks, you must configure the incoming called party settings in the service parameter, device pool, H.323 gateway, or H.323 trunk windows; that is, configuring the incoming called party settings ensures that when a
inbound call comes from a H.323 gateway or trunk, Cisco Unified Communications Manager transforms the called party number back to the value that was originally sent over the trunk/gateway. See the following example for more information.

- For example, a caller places a call to +19721230000 to Cisco Unified Communications Manager A.
- Cisco Unified Communications Manager A receives +19721230000 and transforms the number to 55519721230000 before sending the call to the H.323 trunk. In this case, your configuration indicates that the international escape character + should be stripped and 555 should be prepended for calls of International type.
- For this inbound call from the trunk, Cisco Unified Communications Manager B receives 55519721230000 and transforms the number back to +19721230000 so that digit analysis can use the value as it was sent by the caller. In this case, your configuration for the incoming called party settings indicates that you want 555 to be stripped and +1 to be prepended to called party numbers of International type.

Cisco Unified Serviceability
Cisco Unified Serviceability provides alarms to support the call control discovery feature. For information on how to configure alarms, see the Cisco Unified Serviceability Administration Guide. For alarm definitions that are associated with the call control discovery feature, see the “Troubleshooting Call Control Discovery” section on page 3-47.

Dialed Number Analyzer
Dialed Number Analyzer allows you to add learned patterns so that you can analyze them for your dialing plan. For more information on how to perform this task, see the Cisco Unified Communications Manager Dialed Number Analyzer Guide.

Security (Digest Authentication)
Cisco Unified Communications Manager uses digest authentication (without TLS) to authenticate to the SAF forwarder. When Cisco Unified Communications Manager sends a message to the SAF forwarder, Cisco Unified Communications Manager computes the SHA1 checksum and includes it in the MESSAGE-INTEGRITY field in the message.

You must configure a SAF security profile. For more information, see the “SAF Security Profile Configuration Settings” section on page 3-25.

QSIG
The QSIG Variant and ASN.1 ROSE OID Encoding settings in the H.323 Configuration window get advertised by the CCD advertising service. These settings impact decoding of QSIG messages for inbound tunneled calls; for call control discovery, they do not impact outgoing calls.

The remote call-control entity determines whether QSIG tunneling is required for outgoing calls over H.323 trunks. If the remote call-control entity advertises that QSIG tunneling is required, the QSIG message is tunneled in the message of the outgoing call, even if the H.323 Configuration window in Cisco Unified Communications Manager Administration indicates that QSIG support is not required.

Real Time Monitoring Tool
The Real Time Monitoring Tool displays perfmon counters that support the call control discovery features. For information on these perfmon counters, see the Cisco Unified Real Time Monitoring Tool Administration Guide.

The Real Time Monitoring Tool allows you to view reports for learned patterns and SAF forwarders.
Learned Pattern reports include such information as learned pattern name, time stamp, reachability status for the pattern, remote call-control entity that hosts the pattern, the PSTN failover configuration, and the destination IP address and port. RTMT allows you to search based on different criteria; for example, if you specify a search for the remote call-control entity, all the learned patterns display for the remote call-control entity.

SAF Forwarder reports display information such as authentication status, registration status of SAF forwarders, and so on.

For more information on these reports, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

**SAF Network Issues**

When the Cisco Unified Communications Manager cannot connect to the SAF forwarder, Cisco recommends that you do not update the configuration for the CCD requesting service or CCD advertising service, unless these services are inactive; that is, the Activated Feature check box is unchecked in Cisco Unified Communications Manager Administration. If you update the services when Cisco Unified Communications Manager cannot connect to the SAF network and these services are active, problems may occur; for example, patterns may not be classified correctly as unreachable or reachable, duplicate or stale patterns may exist, and so on.

In addition, Cisco recommends that you do not update the SAF forwarder configuration when the Cisco Unified Communications Manager cannot connect to the SAF forwarder.

**Installing and Activating Call Control Discovery**

After you install Cisco Unified Communications Manager, your network can support the call control discovery feature if you perform the necessary configuration tasks. For information on configuration tasks that you must perform, see the “Configuration Checklist for Call Control Discovery” section on page 3-2.

**Configuring Call Control Discovery**

Before you configure the call control discovery feature, review the “Configuration Checklist for Call Control Discovery” section on page 3-2.

This section contains information on the following topics:

- Considerations for Call Control Discovery Configuration, page 3-19
- Call Control Discovery Feature Parameters, page 3-23
- SAF Security Profile Configuration Settings, page 3-25
- SAF Forwarder Configuration Settings, page 3-26
- Hosted DN Group Configuration Settings, page 3-31
- Hosted DN Pattern Configuration Settings, page 3-32
- CCD Advertising Service Configuration Settings, page 3-34
- Partition Configuration Settings for Call Control Discovery, page 3-36
- CCD Requesting Service Configuration Settings, page 3-37
Review the following considerations before you configure the call control discovery feature:

- SAF Forwarders, page 3-19
- Hosted DN Patterns and Hosted DN Groups, page 3-19
- CCD Advertising and Requesting Services, page 3-20
- SAF-Enabled Trunks, page 3-21

This section does not describe all configuration considerations. This section provides high-level considerations that you should review before you configure the CCD configuration settings. Use this section in conjunction with the sections that are highlighted under the “Configuring Call Control Discovery” section on page 3-18.

**SAF Forwarders**

- Cisco recommends that you configure a primary and backup SAF forwarder for redundancy.
- When you configure a SAF forwarder or SAF security profile, some configuration in Cisco Unified Communications Manager Administration must match the configuration that you entered on the Cisco IOS router.
- Cisco Unified Communications Manager supports the following deployment models for SAF forwarders: clusterwide or node-specific. Before you configure SAF forwarders, review Table 3-4 on page 3-14, which describes these deployment models.
- You can only configure IPv4 for SAF forwarders.
- Each SAF forwarder must have a unique IP address.
- Cisco recommends that you do not update the SAF forwarder configuration when the Cisco Unified Communications Manager cannot connect to the SAF forwarder.
- For information on SAF forwarder field descriptions, see the “SAF Security Profile Configuration Settings” section on page 3-25 and the “SAF Forwarder Configuration Settings” section on page 3-26.

**Hosted DN Patterns and Hosted DN Groups**

- Be aware that the PSTN Failover Strip Digits, PSTN Failover Prepend Digits, and Use HostedDN as PSTN Failover settings display in both the Hosted DN Group and Hosted DN Patterns Configuration windows. If you do not configure these settings in the Hosted DN Patterns Configuration window, the Hosted DN Group configuration applies to the hosted DN patterns.
Each hosted DN group covers one geophysical location advertising DN range.

In the Find and List window for Hosted DN Patterns, you can download a .csv file so that you can add or update multiple hosted DN patterns for the call control discovery feature at the same time. Then, you can upload the patterns in the same window. (You can also add or update multiple hosted DN patterns in BAT.)

If you choose to replace the patterns when you upload the patterns, you lose all hosted DN patterns. If invalid or bad data exists in the .csv file, the data gets ignored by Cisco Unified Communications Manager.

Cisco Unified Communications Manager allows you to configure up to 2,000 hosted DN patterns per cluster.

Each hosted DN pattern must be unique. Each hosted DN pattern can only exist in one hosted DN group.

The Find and List Hosted DN Patterns window allows you to identify which hosted DN patterns belong to a Hosted DN group. For more information on how to perform this task, see the “Identifying Which Hosted DN Patterns Belong to a Hosted DN Group” section on page 3-46.

For information on field descriptions for hosted DN groups and hosted DN patterns, see the “Hosted DN Group Configuration Settings” section on page 3-31 and “Hosted DN Pattern Configuration Settings” section on page 3-32.

**CCD Advertising and Requesting Services**

- You cannot name any CCD advertising service and the CCD requesting service the same name in Cisco Unified Communications Manager Administration.

- You must enable SAF on the trunk in Cisco Unified Communications Manager Administration and assign SAF-enabled trunks to the CCD advertising and requesting services in Cisco Unified Communications Manager Administration. Be aware that SAF-enabled SIP trunks only support UDP or TCP. If you want to do so, you can use the same SAF-enabled trunks for the CCD advertising service and CCD requesting service. For information on enabling SAF on the trunks, see the “Configuring a SAF-Enabled Trunk” section on page 3-45.

- You can configure one CCD requesting service. You can configure as many CCD advertising services as you want.

- Only one hosted DN group can be associated with one CCD advertising service.

- The call control discovery feature relies on a route partition, which you configure in the CCD Partition window (Call Routing > Call Control Discovery > Partition). This route partition gets used exclusively by the call control discovery to ensure that all learned patterns get placed in digit analysis under the route partition. You assign this partition to the CCD requesting service. Be aware that the CCD partition does not display under Call Routing > Class of Control > Partition in Cisco Unified Communications Manager Administration.

For field descriptions for the CCD partition, see the “Partition Configuration Settings for Call Control Discovery” section on page 3-36.

**Tip**

Updating the Learned Pattern Prefix field or Route Partition field in the CCD Requesting Service Configuration window may impact system performance because the digit-analysis master routing table automatically gets updated when these fields are changed. To avoid system performance issues, Cisco recommends that you update these fields during off-peak hours.
After you make changes to the configuration for the CCD advertising and requesting services, click **Save**. You do not need to click the Reset button in these windows unless you want the following events to occur:

- For the CCD Advertising Service—The Reset button in the CCD Advertising Service Configuration window triggers the call control discovery advertising service to withdraw existing publishing requests and to publish all the related information again.
- For the CCD Requesting Service—The Reset button in the CCD Requesting Service Configuration window causes the requesting service to remove the learned patterns from the local cache and for the requesting service to subscribe to the SAF network again. By clicking the Reset button in the CCD Requesting Service Configuration window, Cisco Unified Communications Manager can learn patterns again.

To minimize the impact to your network, Cisco recommends that you click the Reset button in the CCD Advertising Configuration window or the CCD Requesting Configuration window during off-peak hours.

Be aware that clicking Reset in the CCD Advertising and Requesting Service Configuration windows does not reset the trunk. You reset the trunk in the Trunk Configuration window.

- When you delete a CCD advertising service, all hosted DN patterns that are advertised with each assigned trunk get unpublished.
- When you delete the CCD requesting service, all learned patterns get unregistered from the local cache and digit analysis.
- If you want a user to make outbound calls to learned patterns that are advertised by remote call-control entities, ensure that the calling search space that you assign to the device contains the route partition that is assigned to the CCD requesting service.
- When the Cisco Unified Communications Manager cannot connect to the SAF forwarder, Cisco recommends that you do not update the configuration for the CCD requesting service or CCD advertising service, unless these services are inactive; that is, the Activated Feature check box is unchecked in Cisco Unified Communications Manager Administration. If you update the services when Cisco Unified Communications Manager cannot connect to the SAF network and these services are active, problems may occur; for example, patterns may not be classified correctly as unreachable or reachable, duplicate or stale patterns may exist, and so on.
- Make sure that the call-control entities do not advertise the same hosted DN patterns.

If the call-control entities advertise the same hosted DN patterns, problems may occur; for example, a call routing loop may occur between advertising clusters when these clusters make calls to learned patterns by using a calling search space where the learned pattern partition is in front of the locally configured static partition.

- For information on field descriptions for the CCD advertising service and for the CCD requesting service, see the “CCD Advertising Service Configuration Settings” section on page 3-34 and the “CCD Requesting Service Configuration Settings” section on page 3-37.

**SAF-Enabled Trunks**

- One configured SAF-enabled H.323 trunk and one configured SAF-enabled SIP trunk can serve all SIP and H.323 calls to learned patterns for one cluster.
- Make sure that you apply the configuration to the SAF-enabled trunk before you assign the trunk to the CCD advertising or requesting service. You apply the configuration in the Trunk Configuration window.
- If you do not select/assign a SAF-enabled trunk when you configure the CCD requesting service, the CCD requesting service does not get created and patterns do not get learned.
• If you assign both a H.323 and a SIP SAF-enabled trunk to the CCD requesting service, make sure that the same Cisco Unified Communications Manager group exists in the device pool that is assigned to the trunk.

• To support clustering over WAN deployments, configure different Cisco Unified Communications Manager groups to associate with sets of SAF-enabled trunks.

• To ensure redundancy and reduce call-processing traffic, Cisco recommends that no more than two nodes exist in the Cisco Unified Communications Manager group for the device pool that you assign to the SAF-enabled trunk.

• If a trunk is assigned to a route group or associated with a route pattern, you cannot enable SAF on the trunk. Likewise, if you enable SAF on the trunk, you cannot assign the trunk to a route group or associate the trunk with a route pattern.

• Verify that the SIP trunk has a security profile of Nonsecure before you enable SAF on the trunk. You cannot enable SAF on SIP trunks that use authenticated or encrypted security profiles.

• Resetting a SAF-enabled trunk that is assigned to the CCD advertising service causes the CCD advertising service to unpublish the hosted DN patterns and republish with a different service ID for that trunk.

• If different SAF-enabled trunks are configured to use different Cisco Unified Communications Manager groups, the inbound and outbound SAF-related call traffic gets distributed among different Cisco Unified Communications Manager nodes.

• If a Cisco Unified Communications Manager group changes for the SAF-enabled trunk, the CCD advertising service sends unpublish requests to the SAF network; in addition, the CCD requesting service removes the learned patterns from the local cache and digit analysis because no trunk runs on this Cisco Unified Communications Manager node. After the CCD advertising service and/or requesting service start on the new nodes, the advertising service sends a publish request to the SAF network, and the requesting service sends a subscribe request to the SAF network.

• If you change the device pool of the SAF-enabled trunk, the CCD advertising service sends unpublish requests to the SAF network; in addition, the CCD requesting service removes the learned patterns from the local cache and digit analysis because no trunk runs on this Cisco Unified Communications Manager node. After the CCD advertising service and/or requesting service start on the new nodes, the advertising service sends a publish request to the SAF network, and the requesting service sends a subscribe request to the SAF network.

• If you want to delete a SAF-enabled trunk from Cisco Unified Communications Manager Administration, you must unassign the trunk from the CCD advertising service and/or CCD requesting service before you delete it from the Trunk Configuration window.

• Be aware that resetting a SAF-enabled trunk or changing the Cisco Unified Communications Manager group for the trunk impacts the CCD advertising and requesting services. For example, if you reset a trunk and the CCD requesting service cannot access the trunk after 10 seconds have passed, all learned patterns get purged from digit analysis and from the local cache, and the requesting process stops.

Miscellaneous Considerations

• To ensure PSTN failover, configure a route pattern and assign the route pattern to the gateway.

• If your cluster does not support E.164, you must configure translation patterns so that your users can dial E.164 numbers.
Chapter 3  Call Control Discovery

Configuring Call Control Discovery

- You can view purged and blocked learned patterns in the Find and List Blocked Learned Patterns window in Cisco Unified Communications Manager Administration. If you delete a blocked pattern from Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager can relearn those patterns if they are still available in the SAF network (and if the maximum number of learned patterns has not been reached for the cluster).
- Learned patterns are viewed in RTMT.

Call Control Discovery Feature Parameters

To access the feature parameters that support the call control discovery feature, choose Call Routing > Call Control Discovery > Feature Configuration. Table 3-5 describes the feature parameters for the call control discovery feature. For additional information, you can click the question mark help in the Feature Configuration window.

<table>
<thead>
<tr>
<th>Feature Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCD Maximum Number of Learned Patterns</td>
<td>This parameter specifies the number of patterns that this Cisco Unified Communications Manager cluster can learn from the SAF network. The higher the number of allowed learned patterns, the more memory and CPU processing power is required for your server. When Cisco Unified Communications Manager attempts to learn more patterns than is specified in the parameter configuration, the alarm, CCDLearnedPatternLimitReached, gets issued. You can enter a number from 1 to 20000, which is the default.</td>
</tr>
<tr>
<td>CCD Learned Pattern IP Reachable Duration</td>
<td>This parameter specifies the number of seconds that learned patterns stay active (reachable) before Cisco Unified Communications Manager marks those patterns as unreachable. For example, you configure 20 seconds for this parameter; when Cisco Unified Communications Manager cannot communicate with the SAF forwarder after 20 seconds, all calls to learned patterns fail over to the PSTN until IP connectivity to the SAF forwarder gets restored. During the PSTN failover, Cisco Unified Communications Manager cannot learn new patterns. After the time that you specified for this parameter elapses, Cisco Unified Communications Manager marks the learned patterns as unreachable. Use this parameter with the CCD PSTN Failover Duration parameter, which allows patterns that have been marked as unreachable to be reached through PSTN failover. You can enter a number (seconds) from 0 to 300; the default equals 60 seconds.</td>
</tr>
</tbody>
</table>
### Table 3-5  Call Control Discovery Feature Parameters (continued)

<table>
<thead>
<tr>
<th>Feature Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCD PSTN Failover Duration</td>
<td>This parameter specifies the number of minutes that calls to unreachable/inactive learned patterns are routed through the PSTN gateway and then purged from the system. The configuration for this parameter does not take effect until after the timer expires for the CCD Learned Pattern IP Reachable Duration parameter. The expiration of the CCD Learned Pattern IP Reachable Duration parameter indicates that IP connectivity fails between the SAF forwarder and Cisco Unified Communications Manager, and all learned patterns get marked as unreachable. Then, when the duration expires for CCD PSTN Failover Duration parameter, all learned patterns get purged from the system and calls to purged patterns are rejected (caller hears reorder tone or “number is unavailable” announcement). Setting this parameter to 0 means that PSTN failover cannot occur; that is, if the SAF forwarder cannot be reached for the number of seconds that you defined in the CCD Learned Pattern IP Reachable Duration parameter, no failover option is provided over the PSTN, and calls to learned patterns immediately fail. Setting this parameter to 525600 means that PSTN failover never expires and learned patterns never get purged because of IP connectivity issues. You can enter a number (minutes) from 0 to 525600; the default equals 2880.</td>
</tr>
<tr>
<td>Issue Alarm for Duplicate Learned Patterns</td>
<td>This parameter determines whether Cisco Unified Communications Manager issues the alarm, DuplicateLearnedPattern, when it learns duplicate patterns from different remote call-control entities on the SAF network. The default equals False.</td>
</tr>
</tbody>
</table>
### SAF Security Profile Configuration Settings

**Configuration Path**—Advanced Features > SAF > SAF Security Profile

In the SAF Security Profile Configuration window, you configure a SAF security profile so that a secure connection occurs between the SAF forwarder and the Cisco Unified Communications Manager. When you configure a SAF forwarder in the SAF Forwarder Configuration window, you must choose a SAF security profile to apply to the SAF forwarder.

The call control discovery feature leverages the Service Advertisement Framework (SAF) network service, a proprietary Cisco service, to facilitate dynamic provisioning of inter-call agent information. For more information on the call control discovery feature, see the “Call Control Discovery” section on page 3-1.

Cisco Unified Communications Manager uses digest authentication (SHA1) to communicate with the SAF forwarder.

**Before You Begin**

Be aware that some of the information that you configure in this window must also be configured on the SAF forwarder.

Before you configure the SAF security profile, see the “Configuration Checklist for Call Control Discovery” section on page 3-2 and “Considerations for Call Control Discovery Configuration” section on page 3-19.

---

**Table 3-5 Call Control Discovery Feature Parameters (continued)**

<table>
<thead>
<tr>
<th>Feature Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCD Stop Routing On Unallocated Unassigned Number</td>
<td>This parameter determines whether Cisco Unified Communications Manager continues to route calls to a remote call-control entity, such as a Cisco Unified Communications Manager cluster or Cisco Unified Communications Manager Express, when the remote call-control entity rejects the call with the cause code for Unallocated/Unassigned Number. Be aware that an unallocated number represents a hosted DN that does not exist in the current call control entity. The default equals True. If the parameter is set to True, the call is released as soon as Cisco Unified Communications Manager receives the cause code from the remote call-control entity. If the parameter is set to False, when Cisco Unified Communications Manager extends the call to the learned pattern and the remote call-control entity sends the unallocated number cause value, Cisco Unified Communications Manager attempts to find another reachable IP address for the remote cluster for this learned pattern. If any reachable remote destination is available, Cisco Unified Communications Manager tries to extend the call to the IP address of the available reachable remote cluster.</td>
</tr>
</tbody>
</table>
Table 3-6  SAF Security Profile Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the SAF security profile. The name that you enter displays in the Find and List SAF Security Profile window and in the SAF Security Profile drop-down list box in the SAF Forwarder Configuration window. Valid entries include alphanumeric characters, hyphen, period, underscore, and blank spaces. You can configure up to 50 characters.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the SAF security profile. You can enter all characters except for , &quot;, &lt; &gt;, &amp; , and %. You can configure up to 128 characters.</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter a value that you want Cisco Unified Communications Manager to include in requests when it contacts the SAF forwarder.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> To ensure that the Cisco Unified Communications Manager can register with the SAF forwarder, enter the same user name that you entered on the router (SAF forwarder). The user name is case sensitive, so enter the user name exactly as you entered it on the SAF forwarder.</td>
</tr>
<tr>
<td>User Password</td>
<td>Enter a value that you want Cisco Unified Communications Manager to include in requests when it contacts the SAF forwarder.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> To ensure that the Cisco Unified Communications Manager can register with the SAF forwarder, enter the same password that you entered on the router (SAF forwarder). The password is case sensitive, so enter the password exactly as you entered it on the SAF forwarder.</td>
</tr>
</tbody>
</table>

**SAF Forwarder Configuration Settings**

Configuration Path—Advanced Features > SAF > SAF Forwarder
A SAF forwarder, a Cisco router that you configure for call control discovery/SAF, handles the publishing requests from Cisco Unified Communications Manager for the call control discovery feature. In addition, the SAF forwarder handles advertising requests from remote call-control entities for the call control discovery feature. For information on call control discovery, see the “Call Control Discovery” section on page 3-1.

Before You Begin
Before you configure the SAF forwarder, make sure that you have configured at least one SAF security profile.
Be aware that some of the information that you configure in this window must also be configured on the SAF forwarder.
Before you configure the SAF forwarder, see the “Configuration Checklist for Call Control Discovery” section on page 3-2 and “Considerations for Call Control Discovery Configuration” section on page 3-19.

Table 3-7 SAF Forwarder Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the SAF forwarder. Valid entries include alphanumeric characters, hyphen, period, and underscore. You can enter up to 50 characters. The value that you enter in this field gets used to classify SAF forwarder records in the database. The value that you enter displays in the Find and List SAF Forwarder window when you perform a search.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the SAF forwarder. You can enter all characters except for , &quot;, &lt;, &gt;, &amp; and %. You can enter up to 128 characters.</td>
</tr>
</tbody>
</table>
Table 3-7  SAF Forwarder Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Label</td>
<td>The client label allows the SAF forwarder to identify the Cisco Unified Communications Manager node. Valid entries include alphanumeric characters, underscore, and @. You can enter up to 50 characters. Each Cisco Unified Communications Manager node that you select to interact with this SAF forwarder includes its unique client label in the registration message that it sends to the SAF forwarder. When the SAF forwarder receives the registration message, it verifies whether you configured the client label on the SAF forwarder. When you configure a single SAF forwarder for the entire cluster, all nodes in the cluster use the same SAF forwarder configuration and register to the same SAF forwarder. To create a unique client label for the nodes in the cluster, you can append @ to the client label value, which ensures that the registration message includes the basename followed by @&lt;nodeid&gt;. For example, you enter abcde_ny@ for the client label for a two-node cluster that connects to one SAF forwarder, so the registration message includes abcde_ny@1 for node 1 or abcde_ny@2 for node 2. If you do not append the @ to the client label value, you do not need to configure the basename parameter for the client label on the router, but you do need to configure the client label on the router. If you append the @ to the client label value, you must configure the basename parameter with the client label on the router.</td>
</tr>
</tbody>
</table>

Tip     | If more than one Cisco Unified Communications Manager node displays in the Selected Cisco Unified Communications Managers pane under the Showed Advanced section, append @ to the client label value; otherwise, errors may occur because each node uses the same client label to register with the SAF forwarder. |
### Table 3-7 SAF Forwarder Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAF Security Profile</td>
<td>Choose the SAF security profile that you want to apply to this SAF forwarder. The username and password from the security profile get sent to the SAF forwarder, so choose a security profile that contains a username and password that the SAF forwarder will accept. (The SAF forwarder must be configured to use the same username and password.)</td>
</tr>
<tr>
<td>SAF Forwarder Address</td>
<td>Enter the IPv4 address of the SAF forwarder.</td>
</tr>
<tr>
<td>SAF Forwarder Port</td>
<td>Enter the port number that Cisco Unified Communications Manager uses to establish a connection with the SAF forwarder. The default setting is 5050. The port that you enter must match the port number that you configure on the SAF forwarder. The port range on the SAF forwarder is 1024 to 65535.</td>
</tr>
<tr>
<td>Enable TCP Keep Alive</td>
<td>Check the Enable TCP Keep Alive check box to ensure that Cisco Unified Communications Manager gets notified if the TCP connection between the SAF forwarder and Cisco Unified Communications Manager fails. If this check box is unchecked, the Cisco Unified Communications Manager does not get notified that the TCP connection fails until the SAF forwarder keepalive timer expires (configured on the SAF forwarder). Cisco recommends that this check box remains checked.</td>
</tr>
</tbody>
</table>

#### Show/Hide Advanced

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAF Reconnect Interval</td>
<td>Enter the time (in seconds) that Cisco Unified Communications Manager allows to pass before it attempts to reconnect to the SAF forwarder after a connection failure. Enter a value between 0 and 500. The default value is 20.</td>
</tr>
<tr>
<td>SAF Notifications Window Size</td>
<td>Enter the number of outstanding Notify requests that the SAF forwarder can maintain at the same time to the Cisco Unified Communications Manager. The default value is 7. You can enter a number between 0 to 255. If you enter 0 in this field, the SAF forwarder does not send any notification to this Cisco Unified Communications Manager, but the Cisco Unified Communications Manager can still publish hosted DNs to the SAF network if the CCD advertising service is configured and active.</td>
</tr>
</tbody>
</table>
### Table 3-7 SAF Forwarder Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Cisco Unified Communications</td>
<td>This setting works with the Selected Cisco Unified Communications Managers pane. Every node in the Available Cisco Unified Communications Managers pane can connect to the SAF forwarder that you configure in the SAF Forwarder Configuration window. If you want to do so, you can assign a particular node to this SAF forwarder so that the node prioritizes this SAF forwarder over other configured SAF forwarders. You assign the node to the SAF forwarder by moving the node to the Selected Cisco Unified Communications Managers pane. To move a node to or from the Available Cisco Unified Communications Managers pane, highlight the node and click the up or down arrow. If you have assigned a node to two SAF forwarders, the assigned node does not display in the pane because you can only assign a node to two SAF forwarders. For example, three SAF forwarders exist—forwarder1, forwarder2, and forwarder3. You assign node_2 to forwarder1 and forwarder3, which means that node_2 does not display in the Available Cisco Unified Communications Managers pane for forwarder2.</td>
</tr>
<tr>
<td>Managers</td>
<td></td>
</tr>
<tr>
<td>Selected Cisco Unified Communications</td>
<td>Use this pane for cluster over WAN (COW) configurations. This pane displays the nodes that prioritize this SAF forwarder over other configured SAF forwarders. For example, if node_1 and node_2 display in this pane for forwarder1, then node_1 and node_2 always choose forwarder1 first, even though you may have configured other SAF forwarders. To move a node to or from the Selected Cisco Unified Communications Managers pane, highlight the node and click the up or down arrow below the Available Cisco Unified Communications Managers pane. To order the nodes in the pane, highlight the node and click the up or down arrow to the right of the pane.</td>
</tr>
<tr>
<td>Managers</td>
<td></td>
</tr>
</tbody>
</table>
Hosted DN Group Configuration Settings

Configuration Path—Call Routing > Call Control Discovery > Hosted DN Group

Supported with the call control discovery feature, hosted DN groups are a collection of hosted DN patterns that you group together in Cisco Unified Communications Manager Administration. After you assign a hosted DN group to the CCD advertising service in Cisco Unified Communications Manager Administration, the CCD advertising service advertises all the hosted DN patterns that are a part of the hosted DN group. You can assign only one hosted DN group per CCD Advertising Service.

For more information on the call control discovery feature, see the “Call Control Discovery” section on page 3-1.

Before You Begin

Before you configure the hosted DN groups, see the “Configuration Checklist for Call Control Discovery” section on page 3-2 and “Considerations for Call Control Discovery Configuration” section on page 3-19.

Table 3-8 Hosted DN Group Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the hosted DN group. Valid entries include alphanumeric characters, hyphen, period, underscore, and blank space. You can enter up to 50 characters. The value that you enter displays in the Find and List Hosted DN Group window, the Hosted DN Group Configuration window, the Hosted DN Pattern Configuration window, and the CCD Advertising Service Configuration window,</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the hosted DN group. You can enter all characters except for , &quot;, &lt; &gt;, &amp;, and %. You can enter up to 128 characters.</td>
</tr>
<tr>
<td>PSTN Failover Strip Digits</td>
<td>Enter the number of digits that you want stripped from the hosted DN if the call fails over to the PSTN. You can enter a value between 0 and 16.</td>
</tr>
<tr>
<td>PSTN Failover Prepend Digits</td>
<td>Enter the international escape character, +, or digits (0-9) that you want to add to the beginning of the directory number if the call fails over to the PSTN. You can enter up to 16 characters. For example, enter an access or area code.</td>
</tr>
</tbody>
</table>
Table 3-8 Hosted DN Group Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use HostedDN as PSTN Failover</td>
<td>If you check this check box, Cisco Unified Communications Manager ignores the configuration that you entered in the PSTN Failover Strip Digits or PSTN Failover Prepend Digits. If you do not need to strip digits from or prepend digits to the hosted DN when the call fails over to the PSTN, check the Use Hosted DN as PSTN Failover check box. When you check the check box, the PSTN Failover Strip Digits or PSTN Failover Prepend Digits fields display as disabled. If you check the check box, the entity that makes the outbound call uses the original hosted DN range for PSTN failover.</td>
</tr>
</tbody>
</table>

Hosted DN Pattern Configuration Settings

Configuration Path—Call Routing > Call Control Discovery > Hosted DN Patterns

Hosted DN Pattern Configuration window supports the call control discovery feature, which allows Cisco Unified Communications Manager to use the SAF network to learn information, such as directory number patterns, from other remote call-control entities that also advertise SAF.

Hosted DN patterns are directory number patterns that belong to Cisco Unified Communications Manager; the CCD advertising service advertises these patterns to other remote call-control entities that use the SAF network. You associate these patterns with Hosted DN groups, which allow you to easily associate multiple patterns to a CCD advertising service.

Table 3-9 describes the configuration settings that display in the Hosted DN Pattern Configuration window; these same settings display in the .csv file where you can add or modify hosted DN patterns and then upload them into the Cisco Unified Communications Manager database.

Before You Begin

Before you configure the hosted DN patterns, see the “Configuration Checklist for Call Control Discovery” section on page 3-2 and “Considerations for Call Control Discovery Configuration” section on page 3-19.

For more information on call control discovery, see the “Call Control Discovery” section on page 3-1.
### Table 3-9  Hosted DN Pattern Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosted Pattern</td>
<td>Enter the value for the hosted DN pattern, which can contain a maximum of 50 characters. The value that you enter in this field gets advertised by the CCD advertising service to remote call-control entities. You can enter the international escape character + followed by pattern or dialable digits (0-9A-Da-d), pattern ([6-9]), wildcard character (X), or (^) with optional % or ! at the end of the entry.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the hosted DN pattern. You can enter all characters except for , “, &lt;, &gt;, &amp;, and %. You can enter up to 128 characters.</td>
</tr>
<tr>
<td>Hosted DN Group</td>
<td>Choose the Hosted DN group that you want to associate with this hosted DN pattern. If both of the following conditions are met, Cisco Unified Communications Manager applies the PSTN failover configuration for the hosted DN group to the hosted DN pattern: • In the Hosted DN Patterns window, you do not configure the PSTN Failover Strip Digits or PSTN Failover Prepend Digits fields (or you use the defaults). • In the Hosted DN Patterns window, you uncheck the Use HostedDN as PSTN Failover check box.</td>
</tr>
<tr>
<td>PSTN Failover Strip Digits</td>
<td>Enter the number of digits that you want to strip from the beginning of the directory number when an IP connection is not available and the call fails over to the PSTN. You can enter a value between 0 and 16. When all of the following conditions are met, the hosted DN group configuration applies: • When you enter 0 in this field (or leave it blank) • When you leave the PSTN Failover Prepend Digits field blank • When the Use Hosted DN as PSTN Failover check box is unchecked If the value that you enter in this field is longer than the hosted DN pattern, all digits in the pattern get stripped before any digits are prepended.</td>
</tr>
</tbody>
</table>
Configuring Call Control Discovery

Table 3-9 Hosted DN Pattern Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| PSTN Failover Prepend Digits | Enter the international escape character, +, or the digits that you want to add to the beginning of the directory number if the call fails over to the PSTN. You can enter up to 16 characters. When all of the following conditions are met, the hosted DN group configuration applies:  
  • When you enter 0 in this field (or leave it blank)  
  • When you leave the PSTN Failover Strip Digits field blank  
  • When the Use Hosted DN or PSTN Failover check box is unchecked |
| Use HostedDN as PSTN Failover | If you do not need to strip digits from or prepend digits to the hosted DN when the call fails over to the PSTN, check the Use Hosted DN as PSTN Failover check box. When you check the check box, the PSTN Failover Strip Digits or PSTN Failover Prepend Digits fields display as disabled. If you check the check box, the entity that makes the outbound call uses the original hosted DN range for PSTN failover.  
  If you are modifying the .csv file for hosted DN patterns, enter TRUE, which indicates that you want to use the Hosted DN exactly as is during PSTN failover, or FALSE, which indicates that you plan to strip digits from and prepend digits to the directory number during PSTN failover. |

CCD Advertising Service Configuration Settings

Configuration Path—Call Routing > Call Control Discovery > Advertising Service

The call control discovery advertising service, which supports the call control discovery feature, allows Cisco Unified Communications Manager to advertise the hosted DNs for the cluster and the PSTN failover configuration to remote call-control entities that use the SAF network. Table 3-10 describes the CCD Advertising Service configurations settings.

Before You Begin

Before you configure the CCD advertising service, see the “Configuration Checklist for Call Control Discovery” section on page 3-2 and “Considerations for Call Control Discovery Configuration” section on page 3-19.
### Table 3-10   CCD Advertising Service Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the CCD advertising service. Valid entries include alphanumeric characters, hyphen, period, underscore, and blank space. You can enter up to 50 characters. You cannot name any CCD advertising service and the CCD requesting service the same name in Cisco Unified Communications Manager Administration, so ensure that the name is unique.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the CCD advertising service. You can enter all characters except for , &quot;, &lt; &gt;, &amp;, and %. You can enter up to 128 characters.</td>
</tr>
<tr>
<td>SAF SIP Trunk</td>
<td>Choose the SIP trunk that you want to use with this CCD advertising service. For inbound calls to the Cisco Unified Communications Manager, the call gets routed to the appropriate trunk that is advertised by the CCD advertising service. If a trunk does not display in the drop-down list box, you did not choose Call Control Discovery from the Trunk Service Type drop-down list box when you first configured the trunk.</td>
</tr>
<tr>
<td>SAF H323 Trunk</td>
<td>Choose the H.323 trunk that you want to use with the CCD advertising service. For inbound calls to the Cisco Unified Communications Manager, the call gets routed to the appropriate trunk that is advertised by the CCD advertising service. If a trunk does not display in the drop-down list box, verify that you checked the Enable SAF check box in the Trunk Configuration window for H.323 (non-gatekeeper controlled) trunks.</td>
</tr>
<tr>
<td>HostedDN Group</td>
<td>Choose the Hosted DN group that you want to associate with this CCD advertising service. The CCD advertising service advertises the hosted DN patterns that are a part of the hosted DN group. You can only assign the hosted DN group to one CCD advertising service, so only unassigned hosted DN groups display in this drop-down list box.</td>
</tr>
<tr>
<td>Activated Feature</td>
<td>Ensure the Activated Feature check box is checked. If the Activated Feature check box is not checked, the CCD advertising service does not work.</td>
</tr>
</tbody>
</table>

**Additional Information**

See the “Related Topics” section on page 3-47.
Partition Configuration Settings for Call Control Discovery

Configuration Path—Call Routing > Call Control Discovery > Partition

The CCD requesting service, which supports the call control discovery feature, allows Cisco Unified Communications Manager to listen for hosted DN advertisements from remote call-control entities that use the SAF network. In addition, the CCD requesting service ensures that learned patterns get inserted into the digit analysis master routing table.

The partition under Call Routing > Call Control Discovery > Partition only supports the call control discovery feature; that is, all learned patterns automatically belong to the CCD partition that you assign to the CCD requesting service. The call control discovery partition ensures that the learned patterns get inserted into digit analysis under this partition for call control discovery.

Be aware that the CCD partition does not display under Call Routing > Class of Control > Partition in Cisco Unified Communications Manager Administration.

Before You Begin

Before you configure the CCD partition, see the “Configuration Checklist for Call Control Discovery” section on page 3-2 and “Considerations for Call Control Discovery Configuration” section on page 3-19.

Next Steps

Assign the partition to the CCD requesting service.

The partition that you assign to the CCD requesting service must belong to a calling search space that the devices can use for calling the learned patterns, so assign the partition to the calling search space that you want the devices to use. If you do not assign a calling search space that contains the partition to the device, the device cannot call the learned patterns.

Table 3-11 Partition Configuration Settings for Call Control Discovery

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the partition that you plan to assign to the CCD requesting service. You can enter alphanumeric characters, underscore (_), hyphen (-), or space. You can enter up to 50 characters.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the partition. You can enter all characters except for , “, &lt;, &gt;, &amp;, and %. You can enter up to 128 characters.</td>
</tr>
</tbody>
</table>
Configuring Call Control Discovery

CCD Requesting Service Configuration Settings

Configuration Path—Call Routing > Call Control Discovery > Requesting Service

The CCD requesting service, which supports the call control discovery feature, allows Cisco Unified Communications Manager to listen for advertisements from remote call-control entities that use the SAF network. In addition, the CCD requesting service ensures that learned patterns get inserted into the digit analysis.

In Cisco Unified Communications Manager Administration, you can configure only one call control discovery requesting service.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Schedule</td>
<td>From the drop-down list box, choose a time schedule to associate with this CCD partition. The associated time schedule specifies when the partition is available to make outgoing calls to learned patterns for this cluster. The default value specifies None, which implies that time-of-day routing is not in effect and the partition remains active at all times. In combination with the Time Zone value in the following field, association of a partition with a time schedule configures the partition for time-of-day routing. The system checks outgoing calls to learned patterns under this partition against the specified time schedule.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Choose one of the following options to associate a CCD partition with a time zone: Operations Device—If you choose this option, the system checks the partition against the associated time schedule with the time zone of the calling device. Specific Time Zone—If you choose this option, choose a time zone from the drop-down list box. The system checks the partition against the associated time schedule at the time that is specified in this time zone. When an outgoing call to a CCD learned pattern occurs, the current time on the Cisco Unified Communications Manager gets converted into the specific time zone set when one option is chosen. The system validates this specific time against the value in the Time Schedule field.</td>
</tr>
</tbody>
</table>
Before You Begin

Before you configure the CCD requesting service, see the “Configuration Checklist for Call Control Discovery” section on page 3-2 and “Considerations for Call Control Discovery Configuration” section on page 3-19.

Table 3-12 CCD Requesting Service Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the CCD requesting service. Valid entries include alphanumeric characters, hyphen, period, underscore, and blank space. You can enter up to 50 characters. You cannot name any CCD advertising service and the CCD requesting service the same name in Cisco Unified Communications Manager Administration, so ensure that the name is unique.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the CCD requesting service. You can enter all characters except for , “, &lt; &gt;, &amp;, and %. You can enter up to 128 characters.</td>
</tr>
<tr>
<td>Route Partition</td>
<td>From the drop-down list box, choose the partition where you want the learned patterns to belong. The Route Partition field only supports the call control discovery feature; that is, all learned patterns automatically belong to the partition that you choose. This route partition gets used exclusively by the CCD requesting service to ensure that all learned patterns get placed in digit analysis under the route partition. If you choose a partition besides None from the drop-down list box, the partition that you choose must belong to a calling search space that the devices can use for calling the learned patterns. In this case, if you do not assign a calling search space that contains the partition to the device, the device cannot call the learned patterns.</td>
</tr>
<tr>
<td>Tip</td>
<td>Cisco strongly recommends that you configure a unique partition and assign it to the CCD requesting service. If you choose None from the Route Partition drop-down list box, all devices can call the learned patterns.</td>
</tr>
<tr>
<td>Tip</td>
<td>Updating the Learned Pattern Prefix field or Route Partition field may impact system performance because the digit-analysis master routing table automatically gets updated when these fields are changed. To avoid system performance issues, Cisco recommends that you update these fields during off-peak hours.</td>
</tr>
</tbody>
</table>
 Learned Pattern Prefix  

The learned pattern prefix gets applied to the hosted DN pattern before the CCD requesting service registers with digit analysis. For outgoing calls to learned patterns, the learned pattern prefix gets stripped. Enter the prefix that you want to apply to the hosted DN pattern before the hosted DN pattern registers with digit analysis.

To make calls to the learned patterns, the phone user must dial the prefix followed by the learned pattern.

You can enter numbers, *, #, or +. You can enter up to 24 characters.

Tip

Updating the Learned Pattern Prefix field or Route Partition field may impact system performance because the digit-analysis master routing table automatically gets updated when these fields are changed. To avoid system performance issues, Cisco recommends that you update these fields during off-peak hours.

PSTN Prefix

Enter the digits that will get prepended to the learned patterns when PSTN failover occurs. You can enter numbers, *, #, or +. You can enter up to 24 characters.

When calls to learned patterns fail over to the PSTN, the PSTN prefix gets added to the learned pattern after the PSTN failover settings that are advertised by the remote call-control entity for that learned pattern get applied.

Available SAF Trunks

A list of SAF-enabled trunks that are not assigned to the CCD requesting service display in the Available SAF Trunks pane. To assign the trunk to the CCD requesting service, highlight the service and click the down arrow to move the trunk to the Selected SAF Trunks pane.

Selected SAF Trunks

Cisco Unified Communications Manager routes outbound calls over SAF-enabled SIP or H.323 intercluster (non-gatekeeper controlled) trunks to remote call-control entities that use the SAF network; that is, the SAF-enabled trunks that you assign to the CCD requesting service manage outgoing calls to the learned DN patterns.

A list of SAF-enabled trunks that are assigned to the CCD requesting service display in the Selected SAF Trunks pane. You can assign as many SAF-enabled trunks as you want. Outbound calls get managed in a round-robin fashion; that is, if the learned pattern supports both SIP and H.323 protocol, then outbound calls alternate between the trunk types.

To unassign the trunk from the CCD requesting service, highlight the service and click the up arrow to move the trunk to the Available SAF Trunks pane. To order the trunks in the pane, highlight the trunk and click the up and down arrows to the right of the pane.

Tip

At least one SAF-enabled trunk must exist in the Selected SAF Trunks pane; otherwise, the CCD requesting service does not get started for the local cluster, and patterns do not get learned.
Chapter 3      Call Control Discovery

Configuring Call Control Discovery

Blocked Learned Pattern Configuration Settings

Configuration Path—Call Routing > Call Control Discovery > Blocked Learned Patterns

The Blocked Learned Pattern Configuration window supports the call control discovery feature by allowing you to purge and block learned patterns, for example, learned patterns that you no longer want to use.

If you want to do so, you can purge learned patterns that you no longer want to use, and you can block the learned patterns so that Cisco Unified Communications Manager ignores the patterns when they are advertised by remote call-control entities. For example, if you want to block a learned pattern with prefix 235 from remote call-control entity, xyz with IP address of 111.11.11.11, you can block the pattern specifically for this call-control entity by entering the relevant information in the Block Learned Patterns window; in this example, after you save the configuration, the CCD requesting service searches the local cache and purges the learned patterns with 235 prefix from remote call-control entity xyz with IP address of 111.11.11.11. Any subsequent notifications with this information gets blocked and ignored by Cisco Unified Communications Manager. Be aware that blocking and purging of patterns is based on exact match; for example, configuring 235XX blocks 235XX, not any subsets of that pattern. Be aware that if you do not specify a remote call-control entity and IP address for the entity, Cisco Unified Communications Manager purges and blocks the pattern for all remote call-control entities that use it.

You can view purged and blocked learned patterns in the Find and List Blocked Learned Patterns window in Cisco Unified Communications Manager Administration. These purged or blocked patterns do not display in RTMT. If you delete a blocked pattern from Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager can relearn those patterns if they are still available in the SAF network and if the maximum number of learned patterns has not been reached for the cluster. For a pattern to be relearned by Cisco Unified Communications Manager, you must delete the entire record for the blocked learned pattern from Cisco Unified Communications Manager Administration; that is, Cisco Unified Communications Manager does not relearn a pattern when you only delete part of the blocked learned pattern configuration; for example, if you only delete the Remote Call Control Identity or Remote IP configuration for the record.

For Cisco Unified Communications Manager to block or purge a pattern, the learned pattern must match all data that you configure in the Blocked Learned Patterns window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activated Feature</td>
<td>Ensure the Activated Feature check box is checked. If the Activated Feature check box is not checked, the CCD requesting service does not work.</td>
</tr>
</tbody>
</table>

Tip

You can view purged and blocked learned patterns in the Find and List Blocked Learned Patterns window in Cisco Unified Communications Manager Administration. These purged or blocked patterns do not display in RTMT. If you delete a blocked pattern from Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager can relearn those patterns if they are still available in the SAF network and if the maximum number of learned patterns has not been reached for the cluster. For a pattern to be relearned by Cisco Unified Communications Manager, you must delete the entire record for the blocked learned pattern from Cisco Unified Communications Manager Administration; that is, Cisco Unified Communications Manager does not relearn a pattern when you only delete part of the blocked learned pattern configuration; for example, if you only delete the Remote Call Control Identity or Remote IP configuration for the record.

For Cisco Unified Communications Manager to block or purge a pattern, the learned pattern must match all data that you configure in the Blocked Learned Patterns window.
Table 3-13 describes the blocked learned patterns configuration settings that display in the Blocked Learned Pattern Configuration window.

Table 3-13  Blocked Learned Pattern Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Learned Pattern        | **Tip** If you want Cisco Unified Communications Manager to block all patterns based on a prefix that gets prepended to the directory number, do not configure this field; instead, configure the Learned Pattern Prefix field.  
**Tip** If you want to block all learned patterns from a particular remote call-control entity, do not configure this field; instead, configure the Remote Call Control Identity field or the Remote IP field.  
For this field, enter the exact learned pattern that you want to block. Cisco Unified Communications Manager blocks a pattern based on exact match, so you must enter the exact pattern that you want Cisco Unified Communications Manager to block. For example, if you enter 235XX, Cisco Unified Communications Manager blocks 235XX patterns. |
| Learned Pattern Prefix  | **Tip** If you configured the Learned Pattern field, do not configure the Learned Pattern Prefix field.  
If you want to block a learned pattern based on the prefix that is prepended to the pattern, enter the prefix in this field. For example, if you want to block learned patterns that use +1, enter +1 in this field.  
If you configure the Remote Call Control Identity or Remote IP fields, Cisco Unified Communications Manager blocks the learned patterns that use the particular prefix from the remote call-control entity that you configure (not from all remote call-control entities that advertise patterns with the prefix). If you do not enter a remote call-control entity or remote IP address, then all patterns that use the prefix get blocked. |
| Remote Call Control Identity | Enter the name of the remote call-control entity that advertises the pattern that you want to block. For example, you may enter the name of a cluster or a site.  
If you leave this field and the Remote IP field blank, Cisco Unified Communications Manager blocks the learned pattern for all remote call-control entities that advertise the pattern. |
| Remote IP               | Enter the IP address for the remote call-control entity where you want to block the learned pattern.  
If you want to block a particular learned pattern from all remote call-control entities, you do not need to configure this field. Configure this field when you want to block a particular learned pattern from a specific remote call-control entity. |
Finding Configuration Records for Call Control Discovery

The call control discovery feature leverages the Service Advertisement Framework (SAF) network service, a proprietary Cisco service, to facilitate dynamic provisioning of inter-call agent information. By adopting the SAF network service, the call control discovery feature allows Cisco Unified Communications Manager to advertise itself along with other key attributes, such as directory number patterns that are configured in Cisco Unified Communications Manager Administration, so other call control entities that also use SAF network server can use the advertised information to dynamically configure and adapt their routing behaviors; likewise, all entities that use SAF advertise the directory number patterns that they own along with other key information, so other remote call-control entities can learn the information and adapt the routing behavior of the call.

After you configure call control discovery, you can search for the configuration records in the related Find and List windows in Cisco Unified Communications Manager Administration. The Find and List windows allow you to search for records based on specific criteria.

Procedure

Step 1 To locate one of the Find and List windows for the call control discovery feature in Cisco Unified Communications Manager Administration, perform one of the following tasks:

- Choose Advanced Features > SAF > SAF Security Profile.
- Choose Advanced Features > SAF > SAF Forwarder.
- Choose Call Routing > Call Control Discovery > Hosted DN Group.
- Choose Call Routing > Call Control Discovery > Hosted DN Patterns.
- Choose Call Routing > Call Control Discovery > Advertising Service.
- Choose Call Routing > Call Control Discovery > Partition.
- Choose Call Routing > Call Control Discovery > Blocked Learned Pattern.

Tip No Find and List window displays for the CCD requesting service because you can configure only one CCD requesting service in Cisco Unified Communications Manager Administration. When you choose Call Routing > Call Control Discovery > Requesting Service, the record, if configured, displays.

In the Find and List window for Hosted DN Patterns, you can download a .cvs file so that you can add or update multiple hosted DN patterns for the call control discovery feature at the same time. To download a .csv file, click Download in the window. To upload a modified .csv file in the Find and List window for Hosted DN Patterns, click Upload File; browse to the file that you
want to upload, check the Replace Existing Patterns check box if you want to overwrite the existing patterns, and then click Upload File.

The Find and List Hosted DN Patterns window allows you to identify which hosted DN patterns belong to a Hosted DN group. For more information, see the “Identifying Which Hosted DN Patterns Belong to a Hosted DN Group” section on page 3-46.

The Find and List window displays. Records from an active (prior) query may also display in the window.

**Step 2**
To find all records in the database, ensure the dialog box is empty; go to Step 3.
To filter or search records
• From the first drop-down list box, select a search parameter.
• From the second drop-down list box, select a search pattern.
• Specify the appropriate search text, if applicable.

To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

If you search by the search parameter, Activated Feature, in the Find and List CCD Advertising Service window, you must enter t or f to indicate true or false if you specify search text. Do not enter true or false when you specify the search text.

**Step 3**
Click Find.
All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking Delete Selected. You can delete all configured records for this selection by clicking Select All and then clicking Delete Selected.

**Step 4**
From the list of records that display, click the link for the record that you want to view.

To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

**Additional Information**
See the “Related Topics” section on page 3-47.
Configuring Call Control Discovery (Procedure)

The call control discovery feature leverages the Service Advertisement Framework (SAF) network service, a proprietary Cisco service, to facilitate dynamic provisioning of inter-call agent information. By adopting the SAF network service, the call control discovery feature allows Cisco Unified Communications Manager to advertise itself along with other key attributes, such as directory number patterns that are configured in Cisco Unified Communications Manager Administration, so other call control entities that also use SAF network server can use the advertised information to dynamically configure and adapt their routing behaviors; likewise, all entities that use SAF advertise the directory number patterns that they own along with other key information, so other remote call-control entities can learn the information and adapt the routing behavior of the call.

This section describes how to add, copy, or update configuration for call control discovery in the Cisco Unified Communications Manager database. For call control discovery, you configure a SAF security profile, SAF forwarders, hosted DN groups and patterns, CCD advertising services, and the CCD requesting service. Before you configure call control discovery, see the “Configuration Checklist for Call Control Discovery” section on page 3-2.

Tip
This section does not describe how to enable trunks for SAF. For information on how to enable a trunk for SAF, see the “Hosted DN Group Configuration Settings” section on page 3-31.

To identify which hosted DN patterns belong to a hosted DN group, see the “Identifying Which Hosted DN Patterns Belong to a Hosted DN Group” section on page 3-46.

This section does not display how to access the CCD Feature Configuration window, which displays feature parameters for call control discovery. For more information on feature parameters, see the “Call Control Discovery Feature Parameters” section on page 3-23.

Procedure

Step 1 Perform one of the following tasks:

- If you are configuring the CCD requesting service, choose Call Routing > Call Control Discovery > Requesting Service. The CCD Requesting Service Configuration window displays; go to Step 3.
- Choose Advanced Features > SAF > SAF Security Profile.
- Choose Advanced Features > SAF > SAF Forwarder.
- Choose Call Routing > Call Control Discovery> Hosted DN Group.
- Choose Call Routing > Call Control Discovery> Hosted DN Patterns.
- Choose Call Routing > Call Control Discovery> Advertising Service.
- Choose Call Routing > Call Control Discovery> Blocked Learned Pattern.

The Find and List window displays for the SAF Security Profile, SAF Forwarder, Hosted DN Group, Hosted DN Patterns, Partition, and CCD Advertising Service windows.

Step 2 From the Find and List window, perform one of the following tasks:

- To copy an existing record related to call control discovery, locate the record as described in the “SAF Security Profile Configuration Settings” section on page 3-25, click the Copy button next to the record that you want to copy, and continue with Step 3.
- To add a new record related to call control discovery, click the Add New button and continue with Step 3.
• To update an existing record, locate the appropriate record as described in the “SAF Security Profile Configuration Settings” section on page 3-25 and continue with Step 3.

• In the Find and List window for Hosted DN Patterns, you can download a .csv file so that you can add or update multiple patterns for the call control discovery feature at the same time. To download a .csv file, click **Download** in the window.

**Step 3** Configure the appropriate fields as described in the following sections:

- SAF Security Profile Configuration Settings, page 3-25
- SAF Forwarder Configuration Settings, page 3-26
- Hosted DN Group Configuration Settings, page 3-31
- Hosted DN Pattern Configuration Settings, page 3-32
- Partition Configuration Settings for Call Control Discovery, page 3-36
- CCD Advertising Service Configuration Settings, page 3-34
- CCD Requesting Service Configuration Settings, page 3-37
- Blocked Learned Pattern Configuration Settings, page 3-40

**Step 4** To upload a modified .csv file in the Find and List window for Hosted DN Patterns, click **Upload File**; browse to the file that you want to upload, check the Replace Existing Patterns check box if you want to overwrite the existing patterns, and then click **Upload File**.

**Step 5** To save the configuration information to the database, click **Save**.

**Tip**

The Reset button in the CCD Advertising Service Configuration window triggers the call control discovery advertising service to withdraw existing publishing requests and to publish all the related information again. The Reset button in the CCD Requesting Service Configuration window triggers the requesting service to remove the learned patterns from the local cache, resubscribe to the SAF network, and to learn patterns again. To ensure that your network is not impacted, Cisco recommends that you click the Reset button during off-peak hours.

**Additional Information**

See the “Related Topics” section on page 3-47.

### Configuring a SAF-Enabled Trunk

You can configure a SIP or H.323 (non-gatekeeper controlled) trunk so that it supports SAF. For SIP trunks, you choose **Call Control Discovery** from the Trunk Service Type drop-down list box, which displays in the same window where you assign the trunk type and trunk protocol. Be aware that you cannot change the trunk service type after you choose it from the drop-down list box.

For H.323 (non-gatekeeper controlled) trunks, you check the **Enable SAF** check box in the Trunk Configuration window when you configure the trunk (after you choose the trunk type and trunk protocol). If you want to disable SAF on the H.323 trunk after you enable it, uncheck the Enable SAF check box.

For trunk configuration considerations, see the “Considerations for Call Control Discovery Configuration” section on page 3-19.
Identifying Which Hosted DN Patterns Belong to a Hosted DN Group

The Find and List Hosted DN Patterns window allows you to identify which hosted DN patterns belong to a Hosted DN group. In the Find and List Hosted DN Patterns window, you can perform one of the following tasks:

- You can search for all hosted DN patterns, which displays the hosted DN group in the Hosted DN Group when the results display. (The GUI groups the hosted DN groups together in the results.)
- You can search specifically for a particular hosted DN group by choosing Hosted DN Group from the Find drop-down list box and then entering a hosted DN group in the search criteria.

Deleting Configuration Records for Call Control Discovery

This section describes how to delete a configured call control discovery record in Cisco Unified Communications Manager Administration.

Before You Begin

If you delete a blocked pattern from Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager can relearn those patterns if they are still available in the SAF network (and if the maximum number of learned patterns has not been reached for the cluster).

When you delete a CCD advertising service, all hosted DN patterns that are advertised with each assigned trunk get unpublished.

When you delete the CCD requesting service, all learned patterns get unregistered from the local cache and digit analysis.

Note

You can delete multiple records from the Find and List window by checking the check boxes next to the appropriate records and clicking Delete Selected. You can delete all records in the window by clicking Select All and then clicking Delete Selected.

Procedure

Step 1

If you want to delete the record from the Find and List window, perform the following tasks:

a. Find the record that you want to delete by using the procedure in the “Finding Configuration Records for Call Control Discovery” section on page 3-42.

b. Click the record that you want to delete.

c. Click Delete Selected.

You receive a message that asks you to confirm the deletion.

d. Click OK.

The window refreshes, and the record gets deleted from the database.

Step 2

If you want to delete the record from the configuration window, perform the following tasks:

a. Find the record that you want to delete by using the procedure in the “Finding Configuration Records for Call Control Discovery” section on page 3-42.

b. Access the configuration window; click Delete in the configuration window.

You receive a message that asks you to confirm the deletion.
Providing Information to End Users

The call control discovery feature does not impact end users; for example, it does not impact phone users.

Troubleshooting Call Control Discovery

For information on troubleshooting call control discovery, see the Troubleshooting Guide for Cisco Unified Communications Manager.

Related Topics

- Configuration Checklist for Call Control Discovery, page 3-2
- Introducing Call Control Discovery for Cisco Unified Communications Manager, page 3-5
  - Overview of Call Control Discovery, page 3-5
  - Components for the Call Control Discovery Feature, page 3-6
- System Requirements for Call Control Discovery, page 3-16
- Interactions and Restrictions, page 3-16
- Installing and Activating Call Control Discovery, page 3-18
- Configuring Call Control Discovery, page 3-18
  - Considerations for Call Control Discovery Configuration, page 3-19
  - Call Control Discovery Feature Parameters, page 3-23
  - SAF Security Profile Configuration Settings, page 3-25
  - SAF Forwarder Configuration Settings, page 3-26
  - Hosted DN Group Configuration Settings, page 3-31
  - Hosted DN Pattern Configuration Settings, page 3-32
  - CCD Advertising Service Configuration Settings, page 3-34
  - Partition Configuration Settings for Call Control Discovery, page 3-36
  - CCD Requesting Service Configuration Settings, page 3-37
  - Blocked Learned Pattern Configuration Settings, page 3-40
  - Finding Configuration Records for Call Control Discovery, page 3-42
  - SAF Security Profile Configuration Settings, page 3-25
– Configuring a SAF-Enabled Trunk, page 3-45
– Identifying Which Hosted DN Patterns Belong to a Hosted DN Group, page 3-46
– Deleting Configuration Records for Call Control Discovery, page 3-46

• Providing Information to End Users, page 3-47
• Troubleshooting Call Control Discovery, page 3-47
• *Cisco IOS Service Advertisement Framework Configuration Guide*
• *Cisco IOS Service Advertisement Framework Command Reference*