BeyondTrust

Privilege Management for Windows & Mac

iC3 Administration Guide 2.2.35697.0 GA

Powered by Avecto

TC:4/30/2019

Table of Contents

Introduction

iC3 is a management platform for Privilege Management that allows you to manage your Windows and Mac endpoints from one central location.

This Administration Guide details the features and functionality of iC3. Detailed instructions for configuring the MMC and iC3 can be found in the iC3 Installation and Configuration Guide.

Sign in to iC3

> ***Note:*** *You must have cookies enabled in your browser to use iC3. If you don't enable cookies you will get a blank page when you try and navigate to iC3.*

To log in to iC3:

1. Navigate to your iC3 instance and click **Sign in**.
2. Enter your iC3 username and password and click **Sign in**.
3. When you first sign in you are prompted to confirm the date and time format. You can choose the date format from:

```
dd/mm/yyyy 24hr
```

```
mm/dd/yyyy 12hr
```

4. Select your time zone from the drop-down menu and click **Confirm**. These settings are specific to you.

Automatic Logout

You will be logged out of the iC3 portal after 15 minutes of inactivity.

iC3 Search

You can search across "Computers" on page 25, "Policies" on page 22, "Groups" on page 19 and "Users" on page 31 using the search box on the top right of iC3. The icon adjacent to the search term indicates if it's a Computer, Policy, Group or User respectively.

iC3 QuickStart

This section details the most likely tasks you need to perform to get started with iC3, including automatically authorizing and assigning computers to groups in iC3.

Once you have deployed iC3 you can manage policy, create groups and assign policy, and use scripts to authorize and assign computers to these groups.

Manage Policy

There are various approaches you can take to iC3. For example, if you are new to iC3 you may want to create a group, assign it as the Default Group, add all your computers to that group, and then assign the Privilege Management QuickStart policy to that group.

If you are migrating to iC3, you may want to replicate your existing groups and assign the same policy to them, before authorizing and placing your computers in those groups. See "Manage iC3 Policy" on page 12 for more information.

Once you have your policy, you can create groups in iC3 and assign policies to those groups, see "Create Groups and Assign Policy" on page 7

Create Groups and Assign Policy

Creating Groups

1. Navigate to the **Groups** tile or select **Systems** > **Groups** from the top menu.
2. Select **Actions** > **Create Group** or right-click on the grid and click **Create Group**.
3. Enter a Group Name. The Description and Annotations fields are optional.
4. Click **Submit**. Your group is created and appears in the grid list below.

Once the group has been created you can set it as the Default Group. If set, the Default Group is always the group that's selected by default when you add one or more computers to a group. To set the group as the Default Group, right-click on it and select **Set Default**.

Assigning Policy

1. Navigate to the **Groups** tile or select **Systems** > **Groups** from the top menu.
2. Select **Actions** > **Assign Policy** or right-click on the grid and click **Assign Policy**. The row will briefly flash green to indicate that iC3 has processed your request.
3. Select the policy you want to assign from the drop-down and the associated revision. By default the revision is the most recent.
4. The text at the bottom tells you how big the policy is and how many computers it will be assigned to. Click **Assign** to assign the policy to your group.

See "Policy Deployment Settings" on page 33 for details on how you can control the deployment of your policy.

Installing the Privilege Management Client

You need to install the Privilege Management client for the target operating system as well as the iC3 adapter.

For Windows endpoints, the Privilege Management installation packages differ based on your operating system:

For 32-bit (x86) systems run:

```
DefendpointClient_x86.exe
```

For 64-bit (x64) systems run:

```
DefendpointClient_x64.exe
```

You need to install the Privilege Management Windows client in silent mode with the iC3 switch enabled:

```
Msiexec.exe /i DefendpointClient_x.xxx.x.msi IC3MODE=1 /qn /norestart
```

This will install the Windows client in silent mode with the iC3 switch enabled.

For Mac endpoints run:

```
Defendpoint_x.x.xxxxx.x.pkg
```

Install the Windows Adapter

The iC3 client adapter installers can be found in the 'AdapterInstallers' folder of the iC3 deployment. You need to use the Windows Command Prompt to install the Windows iC3 Adapter.

***Note:** The adapters poll every 60 minutes by default. An additional delay is applied based on the CPU load of the node that the adapter is connected to. The minimum supported adapter poll time is 5 minutes.*

You must install the Privilege Management adapters for Windows and Mac using this process. You can optionally choose to automatically assign endpoints to groups and authorize them in one step using the `GroupID` parameter for the Windows and Mac adapters. This is detailed in the following sections.

When Privilege Management agents are managed by iC3, the iC3 adapter is responsible for delivering policies and events between the endpoint and iC3 servers

If you are not using the `GroupID` to automatically assign and authorize computers groups, you can assign and authorize endpoints in iC3, see "Authorizing and Assigning Computers to a Group" on page 26 for more information.

You can install and automatically authorize Windows machines to connect to iC3 using the command line.

There are five parameters for the iC3 Adapter:

- `TenantID` for your chosen method of authentication. This was recorded when iC3 was installed.
- `InstallationID`. You get this from iC3. Click **Administration** > **Agent Installation**. Copy the Installation ID for this script.
- `InstallationKey`. You get this from iC3. Click **Administration** > **Agent Installation**. Copy the Installation Key for this script.
- `ServerURL`, this is the URL for your iC3 portal.
  Please note that there is no port number or slash character on the end of this URL.

- `GroupID` (Optional), if supplied, this will auto-authorize the endpoint and assign it to the specified group. If that group doesn't exist the computer will remain in the pending state. You get this from iC3. Click the Group you want to use. The **Group ID** is shown in the **Details** page for the script. Copy the **Group ID** for this script.

To install adapters:

> ***Note:*** *Include the GroupID to automatically group and authorize the endpoint.*

1. Navigate to the location of the Adapter installer. By default this is the **AdapterInstallers** folder.
2. Enter the command line with the required attributes and press enter. The Adapter installer launches. Proceed through the installation wizard as required.

Example command line

The line breaks must be removed before you run the script.

```
msiexec.exe /i "AvectoIC3Adapter_x64_x.x.xxxx.x.msi"
TENANTID="<TenantID_GUID>"
INSTALLATIONID="<InstallationID>"
INSTALLATIONKEY="<InstallationKey>"
SERVICEURI="<ic3 URL>"
GROUPID="<iC3 GroupID GUID>"
```

Add the following argument if you don't want the Adapter service to start automatically. This option is useful when Privilege Management and the iC3 adapter are being installed to an image that will be reused to create many individual computers. If the adapter is not disabled in this scenario, the iC3 adapter will immediately join the iC3 instance indicated.

```
SERVICE_STARTUP_TYPE=Disabled
```

You can start the 'IC3Adapter' service manually later in the Services.

Example

```
msiexec.exe /i "AvectoIC3Adapter_x64_x.x.xxxxx.0.msi" TENANTID="6b75f647-d3y7-4391-9278-
002af221cc3f" INSTALLATIONID="08A1CD8F-FAE4-479F-81B4-00751A55EEB8"
INSTALLATIONKEY="ABCDEFGHIJKLMNO" SERVICEURI="https://test.ic3.avecto.com" GROUPID="e531374a-55b9-
4516-g156-68f5s32f5e57"
SERVICE_STARTUP_TYPE=Disabled
```

Configure the Windows iC3 Adapter

When the iC3 Adapter communicates with the iC3 Portal it uses HTTPS. If there is a proxy in place that this communication goes through, it must be configured for the iC3 Adapter user which is separate to the logged on user account.

The endpoint needs to be configured to use proxy settings for the whole machine rather than the individual user. The following registry key needs to be edited to make this change:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings]
```

The Data value must read '0'. This specifies the whole machine ('1' specifies per user).

Name	Type	Data
ProxySettingsPerUser	REG_DWORD	0

Ensure the iC3Adapter User has the "User Can Log on as a Service" right

When you install the iC3 Adapter it creates a user called **iC3Adapter** as part of the installation process. The **iC3Adapter** user is granted the rights to "Log on as a Service" by the installation process. If you have a Group Policy in place that revokes this permission you need to ensure the **iC3Adapter** user is excluded as it needs the "Log on as a Service" right. For details of how to do this, see the Microsoft Knowledgebase article https://technet.microsoft.com/en-gb/library/cc794944(v=ws.10).aspx.

Example

```
msiexec.exe /i "AvectoIC3Adapter_x64_x.x.xxxxx.0.msi" TENANTID="6b75f647-d3y7-4391-9278-
002af221cc3f" INSTALLATIONID="08A1CD8F-FAE4-479F-81B4-00751A55EEB8"
INSTALLATIONKEY="ABCDEFGHIJKLMNO" SERVICEURI="https://test.ic3.avecto.com" GROUPID="e531374a-55b9-
4516-g156-68f5s32f5e57"
SERVICE_STARTUP_TYPE=Disabled
```

Install the Mac Adapter

The iC3 client adapter installers can be found in the 'AdapterInstallers' folder of the iC3 deployment. You need to use the Terminal to install the Mac iC3 Adapter.

> ***Note:*** *The adapters poll every 60 minutes by default. An additional delay is applied based on the CPU load of the node that the adapter is connected to. The minimum supported adapter poll time is 5 minutes.*

You must install the Privilege Management adapters for Windows and Mac using this process. You can optionally choose to automatically assign endpoints to groups and authorize them in one step using the `GroupID` parameter for the Windows and Mac adapters. This is detailed in the following sections.

When Privilege Management agents are managed by iC3, the iC3 adapter is responsible for delivering policies and events between the endpoint and iC3 servers

If you are not using the `GroupID` to automatically assign and authorize computers groups, you can assign and authorize endpoints in iC3, see "Authorizing and Assigning Computers to a Group" on page 26 for more information.

You can install and automatically authorize Mac machines to connect to iC3 using the command line.

There are six parameters for the iC3 Adapter:

- **TenantID** for your chosen method of authentication. This was recorded when iC3 was installed.
- `InstallationID`. You get this from iC3. Click **Administration** > **Agent Installation**. Copy the Installation ID for this script.
- `InstallationKey`. You get this from iC3. Click **Administration** > **Agent Installation**. Copy the Installation Key for this script.
- `ServerURL`, this is the URL for your iC3 portal.
  Please note that there is no port number or slash on the end of this URL.
- `GroupID` (Optional), if supplied, this will auto authorize the endpoint and assign it to the specified group. If that group doesn't exist the computer will remain in the pending state. You obtain this from iC3.
- `Cacertificateid` (Optional) is the thumbprint of your SSL certificate. If you are using an SSL certificate that is trusted by a global provider you do not need to add this parameter. If it's not, the SSL certificate must be added to the **System** keychain (not Login). The SSL certificate must also be set to 'Trusted' in the **System** keychain.

To install the private key of the SSL Certificate:

> ***Note:*** *You only need to do these steps if your SSL certificate is not issued by a trusted global provider that is pre-installed on the macOS.*

1. Obtain the pfx portion of your SSL certificate.
2. Double click the pfx file to install it into the **Keychain** application on the Mac. You'll need to enter the password for the SSL certificate. By default the certificate will be placed in the **login** keychain folder.
3. Move the root certificate from the **login** keychain folder to the **System** folder keychain.
4. Set the root certificate to **Always Trust**.
5. Extract the thumbprint of your SSL certificate from the certificate as you need this to install the Mac Adapter.

To install adapters:

> ***Note:*** *Include the GroupID to automatically group and authorize the endpoint.*

> ***Note:*** *Include the Cacertificateid if your SSL certificate is not issued by a trusted global provider.*

1. Navigate to the location of the Adapter installer. By default this is the **AdapterInstallers** folder.
2. Mount the DMG and place the iC3 adapter onto the desktop. Run the following command line from the Terminal. Once the Adapter installer launches, proceed through the installation wizard as required.

Example command line

The line breaks must be removed before you run the script.

```
sudo /Avecto_ic3_Adapter_x_x_x/install.sh tenantid="750e85d1-c851-4d56-8c76-b9566250cf1d"
installationid="95a10760-2b96-4a0e-ab65-ed7a5e8f1649"
installationkey="VGhpcyBzZWNyZXQgaTYzIGJlZW4gQmFzZTY0IGVuY29kZWQ="
serviceuri="https://test.ic3.avecto.com" groupid="fcc4022e-12fa-4246-87w8-0de9a1483a68"
cacertificateid="b36b7345ff30aa7fb15fcd985fe2989c3e11aba7"
```

Manage iC3 Policy

You manage policy in iC3 using the Privilege Management MMC snap-in for iC3. The set up and configuration for this is detailed in the iC3 Installation and Configuration Guide.

iC3 policies can be viewed, created, drafts saved, checked in to iC3 and checked in from iC3 using the Privilege Management snap-in for the MMC.

In addition, iC3 gives you the ability to manually move XML policy files around by downloading them, uploading them, or uploading policy revisions.

Policy Management in iC3

iC3 allows you to upload and download policy files as well as override a policy check out if you have the appropriate user permissions. The editing, checking in and checking out of policies is managed in the Privilege Management MMC snap-in, see "Policy Management in the MMC" on page 13 for more information.

Upload File to Create Policy

You can upload an XML policy to iC3. If the policy doesn't exist it will become revision one. If the policy does exist it will be a new revision, see "Upload Revision" on page 12 for more details.

1. Navigate to the **Policies** tile or click **Policies** from the top menu.
2. Right-click anywhere on the grid and click **Upload File to Create Policy** or select **Actions** > **Upload File to Create Policy**.
3. Either drag the XML file into the upload area or click the upload icon to browse to the XML file and click **Open**. The XML file is then uploaded to the portal.

Upload Revision

You can upload a new revision of an existing policy to iC3. Policies that are downloaded from iC3, modified and then re-uploaded are recognized as a new revision based on a unique identifier in the XML.

To upload a new revision of an existing policy:

1. Navigate to the **Policies** tile or click **Policies** from the top menu.
2. Right-click on the policy you want to upload a new revision of and click **Upload Revision** or select **Actions** > **Upload Revision**.
3. Either drag the XML file into the upload area or click the upload icon to browse to the XML file and click **Open**. The XML file is then uploaded to the portal.
4. The new revision is uploaded providing the XML validation passes. If the XML policy doesn't pass validation, the row is highlighted in red and the policy isn't uploaded.

Each time the same policy is checked in from the MMC, the revision of the policy is incremented. New revisions of the same policy need to be manually assigned to the group, this is not done automatically, see "Assign a Policy to a Group" on page 23 for details.

Discard Draft and Undo Check Out

If the policy has been checked out using the Privilege Management MMC snap-in, you can force iC3 to discard the changes and undo the check out providing you are an Administrator or Policy Administrator.

To discard draft & undo check out of a policy:

1. Navigate to the **Policies** tile or click **Policies** from the top menu.
2. Right-click on the policy that has been checked out to the Privilege Management MMC snap-in and click **Discard Draft & Undo Check Out**.
3. You are prompted to check that you do want to perform this action. Click **Continue Anyway** to discard the draft and undo the check out, otherwise click **Cancel**.

Download

You can download a policy from iC3 as an XML file. This is useful if you need to share the policy with other people in your organization.

To download a policy XML file:

1. Navigate to the **Policies** tile or click **Policies** from the top menu.
2. Right-click on the policy and click **Download**. The policy is downloaded to your downloaded files location.

Policy Management in the MMC

The Privilege Management MMC snap-in allows you to create, edit, check in, and check out policies to the iC3 portal. See the 'Windows Administration Guide' or 'Mac Administration Guide' for details on editing workstyle policy for Windows and Mac endpoints respectively.

Policy Workflow

Policies are managed on a per revision basis in iC3. When you create or import an iC3 policy in the Privilege Management MMC snap-in, you can save one or more local drafts before you check it in to iC3. Revisions are not created when you're working with local drafts and iC3 does not have visibility of them.

Each time you check a policy back in to iC3 from the MMC a new revision is created. This allows you to revert to an older revision, if required. If you check a policy out and make changes but then change your mind, you can discard your changes and the associated check out to cancel your original check out and any changes.

You can check policies in and out from the Privilege Management MMC snap-in as well as create new ones.

There are six user roles for policies:

- Abort
- Create
- Delete
- Modify
- Query
- View

Only users in the Administrators or Policy Administrators group have all of the user roles. See "User Roles" on page 56 for more details.

Agent and Group Locks

When a policy is applied to an endpoint or group, this will lock it, which results in locked rows in the Computers or Groups grids, respectively. Once all commands have been applied, the endpoint or group will unlock. Once the endpoint or group is unlocked, you can interact with the computer or group. Subsequent commands are queued by iC3 as required.

Create a Policy

If you are creating a policy from new you can do so using the functionality in the Privilege Management MMC snap-in.

To create a new policy:

1. Click **Create** in the Privilege Management MMC snap-in.
2. Enter a name for your policy and click **OK**. This creates the policy so you can now start editing it. At this stage the policy is in draft, iC3 does not have visibility of it. iC3 can only see policies that you have checked in.
3. See the 'Windows Administration Guide' or 'Mac Administration Guide' for details on editing policy on Windows or Mac endpoints respectively.

View Policies

You can view a list of policies that are both local to the Privilege Management MMC snap-in, and in iC3 can see the state of them.

To view policies:

1. In the Privilege Management MMC snap-in, if you have a policy checked out and you'd like to view all policies, click **iC3 Policies** within the Start section on the left. If you don't have a policy checked out you can click **Browse all iC3 policies** in the iC3 Policy section.
2. You can perform additional actions such as **Save Draft**, **Check in Changes**, **Discard Draft** and **View** from this list depending on your user role and the state of the policy.

Check in a Policy

Once you have created or imported a policy you can check it in to iC3. This will create the first revision of the policy if it's new to iC3, otherwise it will increment the revision of the policy.

To check in a policy:

1. In the Privilege Management MMC snap-in, click **Check in your changes** in the iC3 Policy section.
2. Add a description of your changes and click **OK**. Your policy is now checked into iC3 and is visible in the iC3 portal.

Each time the same policy is checked in or uploaded to the Privilege Management MMC snap-in, the revision of the policy is incremented. New revisions of the same policy need to be manually assigned to the group, this is not done automatically, see "Assign a Policy to a Group" on page 23 for details.

Check out a Policy

Policies that have been checked in to iC3 must be checked out to be edited.

To check out a policy:

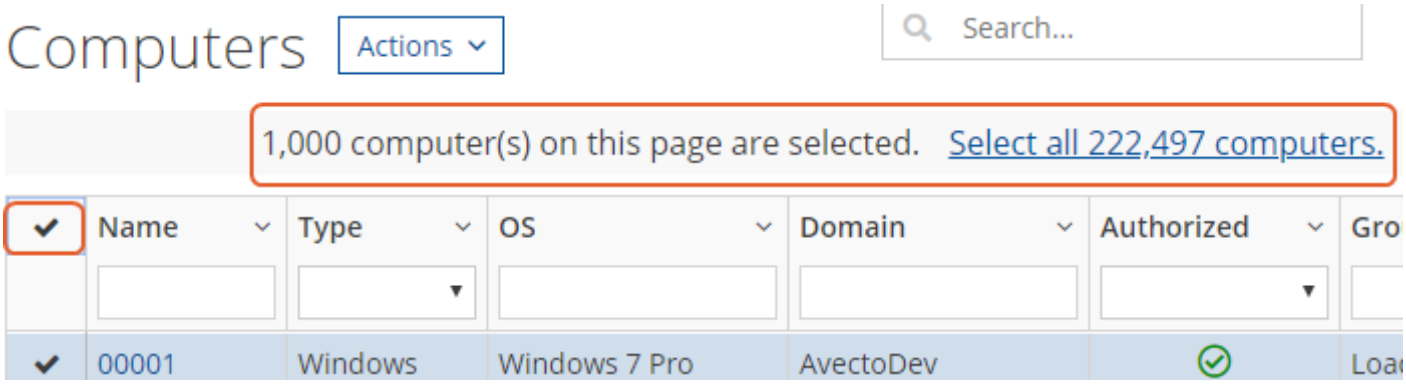
1. In the Privilege Management MMC snap-in, click **Browse all iC3 policies** in the iC3 policy section.
2. Select your policy from the list and click **Check Out**. You can now edit the policy in the Privilege Management MMC snap-in.

Grid Behavior

There are several grids in iC3 that have similar behavior. The Computers grid supports the standard Windows behavior for selecting multiple rows as you can interact with multiple computers in one action.

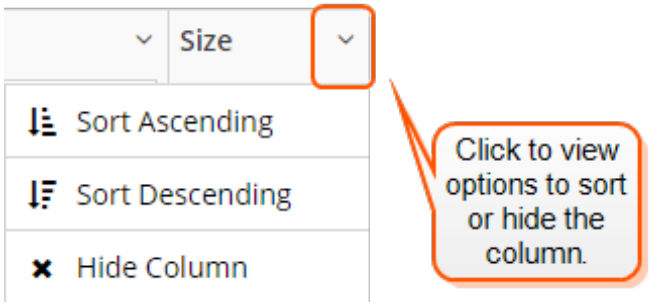
Select All

To select the first 1,000 rows, select the check mark in the top-left hand corner. If you want to select all rows in the grid, first select the first 1,000 rows using the check mark, and then click the link that is displayed. For example:

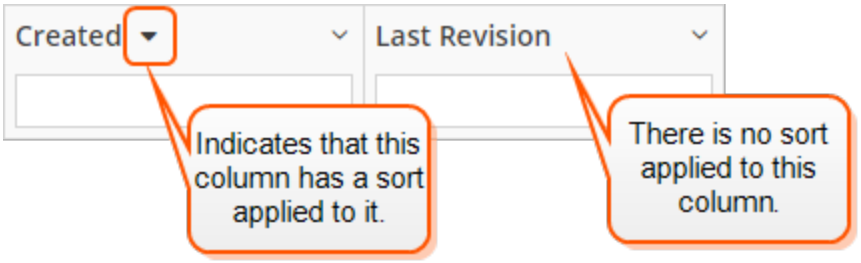


Sort Columns

By default, the grid is ordered by the Name, however you can sort by any of the other columns using the arrow at adjacent to the column name. Click the down arrow to choose how you want to sort the columns. You can also hide columns using this functionality.

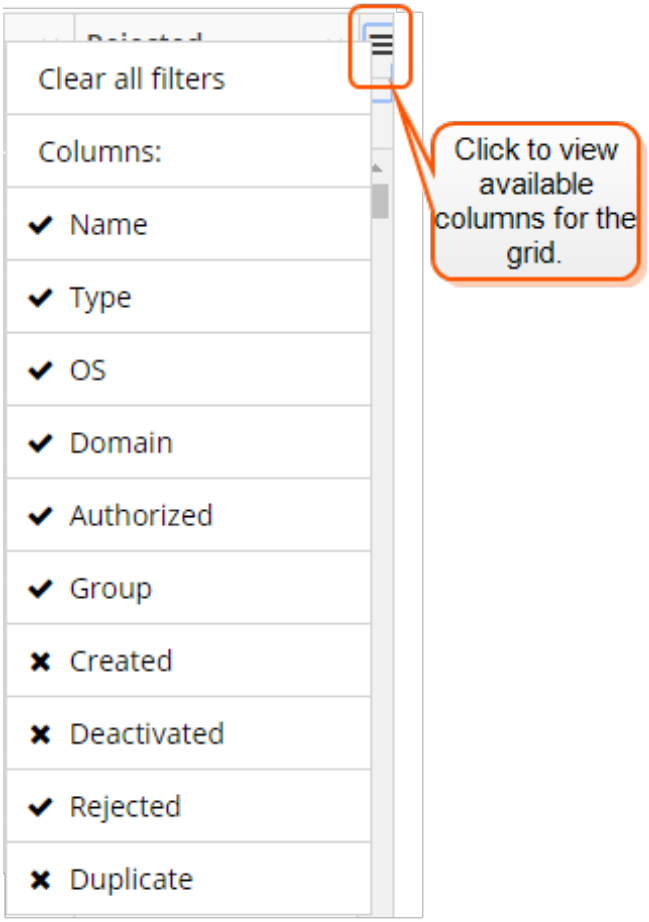


A column that has a sort applied to it is indicated by a solid triangle adjacent to the name. Clicking this solid triangle will clear the sort from the column.



Add or Remove Columns

You can configure the columns on pages with grids by clicking the hamburger icon on the right-hand side and selecting or clearing the tick adjacent to the column you want to see or hide respectively.



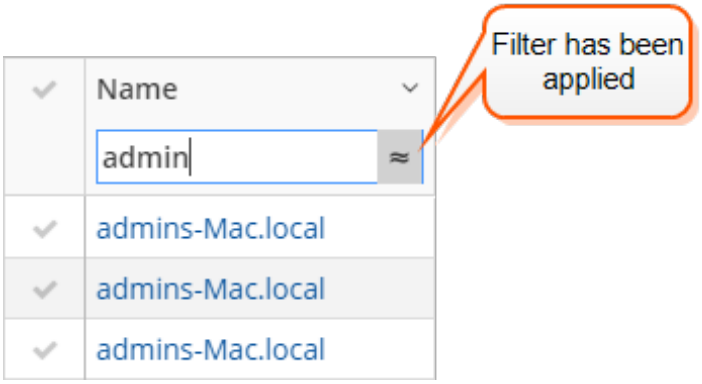
Filter

You can filter in the grids by using the empty fields at the top of each column. If you type text into these fields the results in the grid filter below automatically update to the records that contain that string.

The icon to the right of the field turns gray to indicate that a filter is applied.

The following grids support filtering:

- Computers
- Policies
- Groups
- Users



You can click the filter icon to negate the filter criteria. It will then read "does not contain".

Data Refresh

When there is new data available for iC3 you will see a blue notification on the bottom right of the screen stating that new data is available. Click the refresh link in this notification to see the updated data.

Progress and Change Indicators

When iC3 is busy performing an action you see a spinner on the grid to indicate that it's processing.

Where actions affect one or more rows you see the row briefly flash green to indicate that iC3 has processed your request.

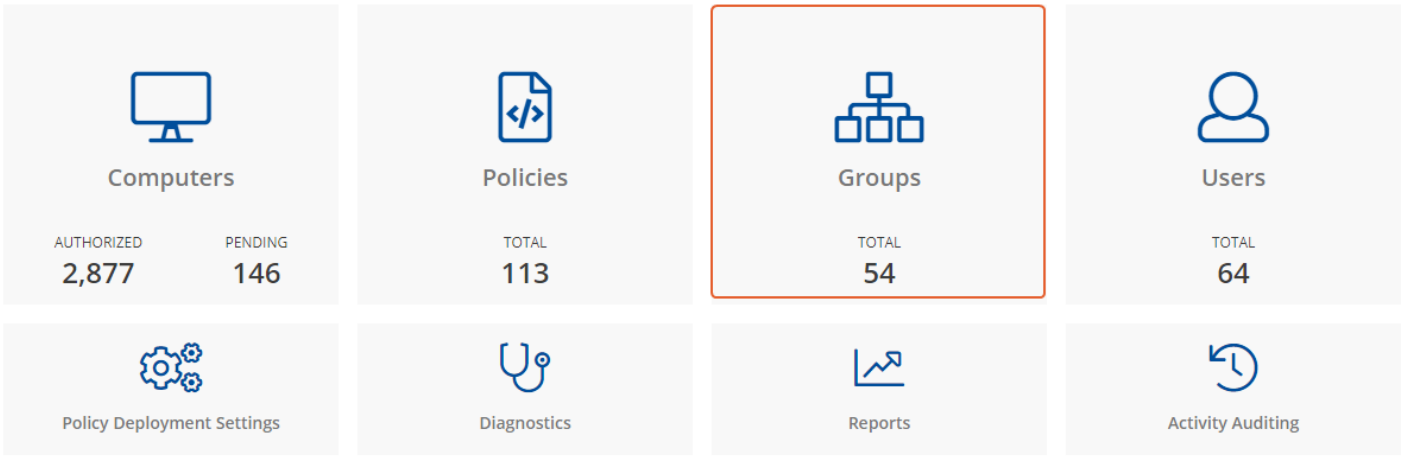
Error Notifications

If iC3 cannot complete an action successfully it doesn't make any changes and you get a notification on the top right next to the search field. iC3 does not process a task that it can't action successfully. The error notification tells you that the action wasn't successful. You can clear the errors as required from the page that generated the error.

Groups

Groups contain one or more computer. A policy is assigned to a group.

You can perform the following tasks in the Groups tile:



Create a Group

A group is a collection of computers to which a policy can be assigned.

1. Navigate to the **Groups** tile or select **Systems** > **Groups** from the top menu.
2. Select **Actions** > **Create Group** or right-click on the grid and click **Create Group**.
3. Enter a Group Name. The Description and Annotations fields are optional.
4. Click **Submit**. Your group is created and appears in the grid list below.

Once the group has been created you can set it as the Default Group. If set, the Default Group is always the group that's selected by default when you add one or more computers to a group. To set the group as the Default Group, right-click on it and select **Set Default**.

View the Details of a Group

1. Navigate to the **Groups** tile or select **Systems** > **Groups** from the top menu.
2. Right-click the group you want to view the details for and click **Details** from the menu.

3. These tabs allow you to see additional information for the group and what policy is currently applied to it, if any. You can click **Edit** to change these details, see "Edit Properties of a User" on page 32.

Edit Properties of a Group

1. Navigate to the **Groups** tile or select **Systems** > **Groups** from the top menu.
2. Right-click the group you want to edit the details for and click **Edit Properties** from the menu.
3. Change the Group Name, Description and Annotations as required and click **Submit**.

Changing the details of a group, including the name, does not affect the computers that are added to the group, or the policy delivered to those computers.

Set a Default Group

The Default Group, when set, appears first in the **Group** down-down list in iC3.

1. Navigate to the **Groups** tile or select **Systems** > **Groups** from the top menu.
2. Right-click the group you want to make the default group and click **Set Default** from the menu. The row will briefly flash green to indicate that iC3 has processed your request and the Default column will contain a green tick to indicate that it is the default group.

Computers being added to the system do not join the default group if no group is specified at install time, see "Create Groups and Assign Policy" on page 7.

Assign a Policy to a Group

Assigning a policy to a group will allow you to manage computers in that group with the policy.

1. Navigate to the **Groups** tile or select **Systems** > **Groups** from the top menu.
2. Right-click the group you want to assign a policy to and click **Assign Policy** from the menu.
3. Choose the policy you want to be assigned to the group from the menu and which revision of that policy.
4. Click **Assign** to assign that policy to the group. The row will briefly flash green to indicate that iC3 has processed your request.

Clear a Policy from a Group

Computers in the group will have the policy removed when you clear a policy from a group.

1. Navigate to the **Groups** tile or select **Systems** > **Groups** from the top menu.
2. Right-click the group you want to clear the policy from and click **Clear Policy** from the menu.
3. You are notified how many computers will be affected by the change. Click **Continue Anyway** to clear the policy, otherwise click **Cancel**.

Delete a Group

You can only delete groups that do not have any computers assigned to them. Groups can be deleted if they have a policy assigned to them.

1. Navigate to the **Groups** tile or select **Systems** > **Groups** from the top menu.
2. Right-click the group you want to delete and click **Delete** from the menu.

3. Click **Delete** to continue deleting this group, otherwise click **Cancel**.

Policies

The Policies tile allows you to see and interact with the policies being deployed by iC3.

You can perform the following tasks in the Policies tile:

Upload a File to Create Policy

You can upload an XML policy to iC3. If the policy doesn't exist it will become revision one. If the policy does exist it will be a new revision, see "Upload Revision" on page 12 for more details.

1. Navigate to the **Policies** tile or click **Policies** from the top menu.
2. Right-click anywhere on the grid and click **Upload File to Create Policy** or select **Actions** > **Upload File to Create Policy**.
3. Either drag the XML file into the upload area or click the upload icon to browse to the XML file and click **Open**. The XML file is then uploaded to the portal.

Upload Policy Revision

1. Navigate to the **Policies** tile or click **Policies** from the top menu.
2. Right-click on the policy you want to upload a new revision of and click **Upload Revision** or select **Actions** > **Upload Revision**.
3. Either drag the XML file into the upload area or click the upload icon to browse to the XML file and click **Open**. The XML file is then uploaded to the portal.

4. The new revision is uploaded providing the XML validation passes. If the XML policy doesn't pass validation, the row is highlighted in red and the policy isn't uploaded.

Each time the same policy is checked in from the MMC, the revision of the policy is incremented. New revisions of the same policy need to be manually assigned to the group, this is not done automatically, see "Assign a Policy to a Group" on page 23 for details.

View Policy Details

For a single policy you can view additional details.

1. Navigate to the **Policies** tile or select **Policies** from the top menu.
2. Right-click the policy you want to view the details of and click **Details** from the menu. The Policy details screen includes additional information about the policy. You can also download the policy from this area.

Download Policy

You can download a policy from iC3 in XML form if required.

1. Navigate to the **Policies** tile or click **Policies** from the top menu.
2. Right-click on the policy and click **Download**. The policy is downloaded to your downloaded files location.

Edit Properties of Policy

You can edit the details for a single policy.

1. Navigate to the **Policies** tile or select **Policies** from the top menu.
2. Right-click the policy you want to view the details of and select **Edit Properties** from the menu.
3. You can edit the Policy Name, Description and Annotations here. Click **Submit** to save your changes.

Assign a Policy to a Group

A policy can be assigned to one or more groups.

1. Navigate to the **Policies** tile or select **Policies** from the top menu.
2. Right-click the policy you want to assign to a group and click **Assign Policy to Group**.
3. Select the group you want to assign the policy to from the drop-down and click **Assign**.
4. The text at the bottom tells you how big the policy is and how many computers it will be assigned to. Click **Assign** to assign your group to the policy. The row will briefly flash green to indicate that iC3 has processed your request.

See "Policy Deployment Settings" on page 33 for details on how you can control the deployment of your policy.

Discard Policy Draft and Undo Check Out

If the policy has been checked out using the Privilege Management MMC snap-in, you can force iC3 to discard the changes and undo the check out providing you are an Administrator or Policy Administrator.

To discard draft & undo check out of a policy:

1. Navigate to the **Policies** tile or click **Policies** from the top menu.
2. Right-click on the policy that has been checked out to the Privilege Management MMC snap-in and click **Discard Draft & Undo Check Out**.
3. You are prompted to check that you do want to perform this action. Click **Continue Anyway** to discard the draft and undo the check out, otherwise click **Cancel**.

Delete a Policy

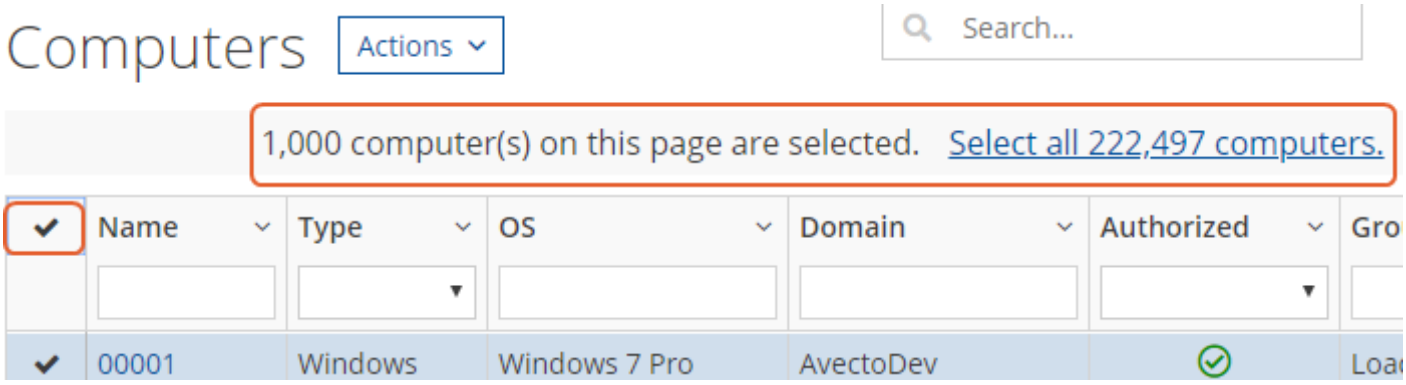
You can only delete policies if they're not assigned to any group.

1. Navigate to the **Policies** tile or click **Policies** from the top menu.
2. Right-click on the policy that you want to delete and click **Delete**.
3. You are prompted to check that you do want to perform this action. Click **Delete Anyway** to discard the draft and undo the check out otherwise click **Cancel**.

Computers

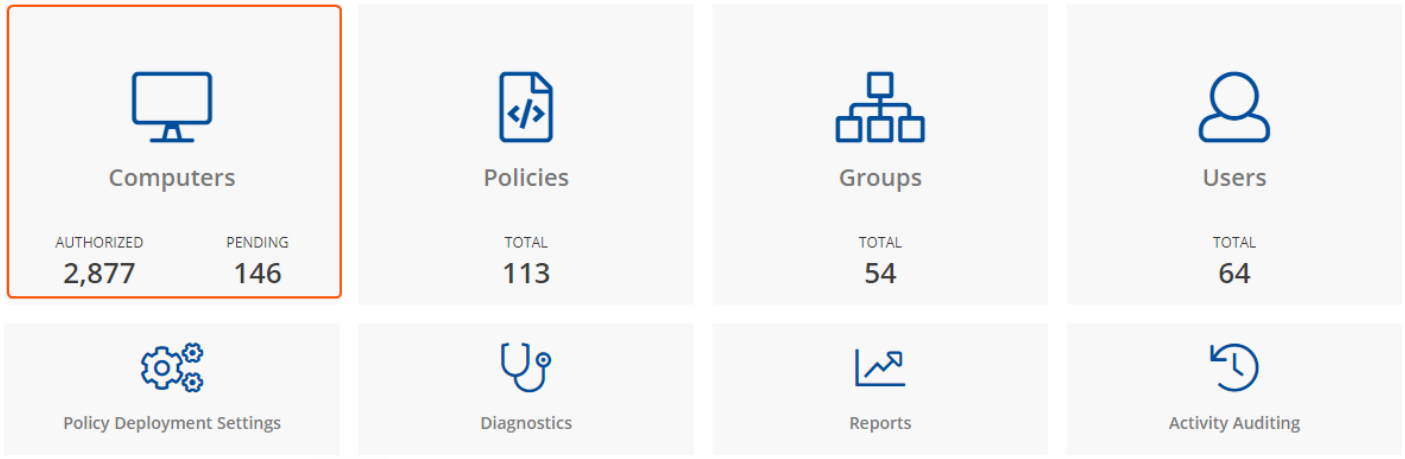
The Computers tile allows you to see and interact with the endpoints being managed by iC3.

To select the first 1,000 rows, select the check mark in the top-left hand corner. If you want to select all rows in the grid, first select the first 1,000 rows using the check mark, and then click the link that is displayed. For example:



You can perform the following tasks in the Computers tile:

- "Authorizing and Assigning Computers to a Group" on page 26
- "Reject Computers" on page 26
- "Details" on page 26
- "Edit Properties" on page 27
- "Assign Computers to a Group" on page 27
- "Clear a Computer from a Group" on page 27
- "Deactivate Computers" on page 28
- "View Duplicate Computers" on page 28
- "Update Policy on All" on page 29
- "Update Policy on Selected" on page 30



Authorizing and Assigning Computers to a Group

You can authorize and assign computers to a group in one step providing the computers haven't previously been authorized. If they have previously been authorized then follow "Assign Computers to a Group" on page 27 instead.

You can see which endpoints have not been authorized by selecting **Pending** from the top of the **Authorized** column. See "Grid Behavior" on page 16 for more detailed information on the grids and filtering.

1. Navigate to the **Computers** tile or select **Systems** > **Computers** from the top menu.
2. Right-click the computer(s) you want to place in a group and authorize in one step, and select **Authorize and Assign Group** from the menu.

> ***Note:*** *You can select multiple rows using the standard Windows functionality.*

3. Select the group you want to assign it to from the drop-down group and click **Assign**. If you haven't created any groups yet you will only see 'No Group' in the drop-down. See "Create a Group" on page 19 for instructions on creating a group in iC3.
4. If you have a Default Group it will be selected by default, otherwise you can select the group you want to use from the drop-down menu. Click **Assign**. The rows that you have selected will briefly flash green to indicate that iC3 has processed your request.

Reject Computers

You can reject endpoints that have not yet been authorized with iC3. If the computer has already been authorized, see "Deactivate Computers" on page 28 for more information on manual deactivation, or you can use iC3 to manage deactivation's automatically, see "Auto Deactivate Settings" on page 57 for more information.

Rejected computers are disconnected from iC3 and will no longer be able to communicate with iC3. This action can't be reversed unless you re-install the software on the client computer.

1. Navigate to the **Computers** tile or select **Systems** > **Computers** from the top menu.
2. Right-click the computer(s) you want to reject and click **Reject** from the menu. You are prompted to check you want to continue with the rejection of the computer(s). Click **Reject Anyway** to proceed, otherwise click **Cancel**.

Details

For a single computer you can view additional details.

1. Navigate to the **Computers** tile or select **Systems** > **Computers** from the top menu.
2. Right-click the computer you want to view the details of and click **Details** from the menu.

The Computer details screen includes additional information about the endpoint including its Authorization Status, Deactivation Type, Computer Deactivated and Computer Authorized timestamps where applicable.

You can also view information about the endpoint, the name of the policy and the version that is applied.

Update

You can force this page to refresh by clicking **Update** on the right-hand side of the pane. This action gets the latest information from the endpoint.

Force Policy Update

If you need to force a policy update on a specific computer you can do so here.

1. Click **Actions** > **Force Policy Update**. The policy update for that computer will now be performed by iC3. This command is then queued up so there may be a small wait for the policy to be updated on the computer.

Computer Logs

1. In the Computer Details screen, click **Computer Logs**. This shows you a list of logs that have previously been requested. To get a new set of logs from the computer, click **Request Logs**.
2. iC3 will request the logs from the computer and you can view them when this request is returned. This action can take up to two hours to complete.

Command Log

1. In the Computer Details screen, click **Command Log**. This shows you a list of commands that have been communicated between iC3 and the computer.

Edit Properties

1. Navigate to the **Computers** tile or select **Systems** > **Computers** from the top menu.
2. Right-click the computer you want to edit the properties for and click **Edit Properties**.
3. Click the plus sign next to **Annotations** to add an annotation to this computer.
4. Click **OK** to save your annotation and **Submit** to save it in iC3.

Assign Computers to a Group

1. Navigate to the **Computers** tile or select **Systems** > **Computers** from the top menu.
2. Right-click the computer(s) you want to place in a group and click **Assign Group** from the menu.

Note: *You can select multiple rows using the standard Windows functionality.*

3. Select the group you want to assign it to from the drop-down group and click **Assign**. If you haven't created any groups yet you will only see 'No Group' in the drop-down, see "Create a Group" on page 19 for instructions on creating a group in iC3.
4. If you have a Default Group it will be selected by default, otherwise you can select the group you want to use from the drop-down menu. Click **Assign**. The rows that you have selected will briefly flash green to indicate that iC3 has processed your request.

Clear a Computer from a Group

1. Navigate to the **Computers** tile or select **Systems** > **Computers** from the top menu.
2. Right-click the computer(s) you want to clear the group from and click **Clear Group** from the menu. You are prompted to check you want to continue with clearing the group from the computer(s). Click **Continue Anyway** to proceed, otherwise click **Cancel**.

Since policies are assigned to groups rather than individual computers, if you clear a computer from a group, the policy on that computer is also cleared. The policy assignment to the wider group is not affected.

View Duplicate Computers

iC3 detects duplicate computers automatically. The task to check for duplicate computers runs every day at 02:00 server time on the node where the job service is running. The service checks for computers with the same name. If iC3 finds one or more computers with the same name it adds the 'Duplicate' flag to all of them except the most recently created one.

Duplicate computers are hidden by default in the Computers grid. You can filter on duplicate computers using the grid filter and adding the column called 'Duplicate'. iC3 does not do any additional processing to computers that are flagged as duplicates and they continue to receive policy from iC3. All computers that do not contact iC3 for the number of days specified in the "Auto Deactivate Settings" on page 57 are deactivated if you have chosen to automatically deactivate inactive computers.

Deactivate Computers

Computers can be automatically deactivated by iC3 if you choose to enable the functionality, see "Auto Deactivate Settings" on page 57 for more information. You can also manually deactivate a computer that has previously been authorized by iC3 . If the computer hasn't been authorized, see "Reject Computers" on page 26 for more information.

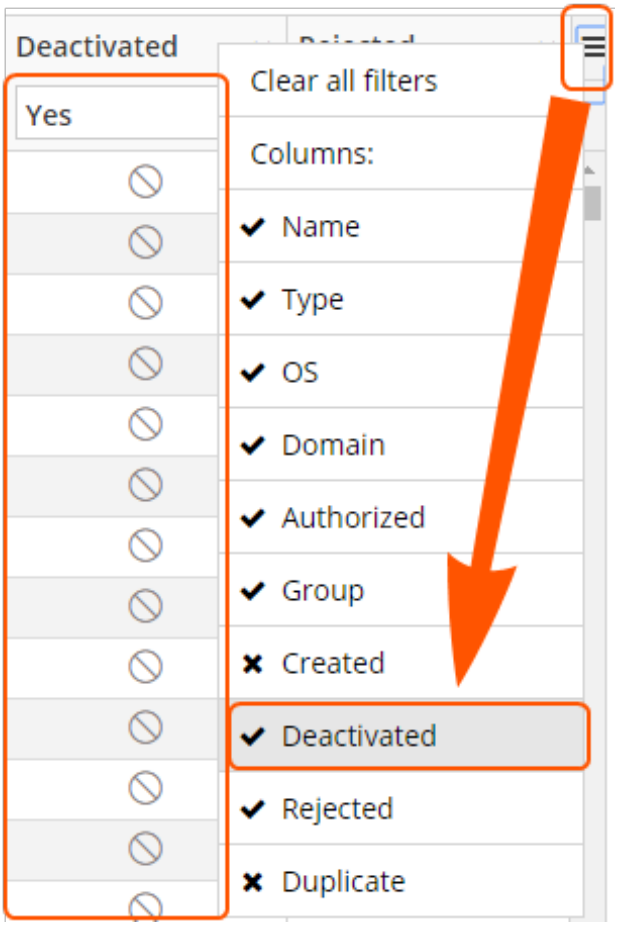
Deactivated computers are disconnected from iC3 and will no longer be able to communicate with iC3. This action can't be reversed unless you re-install the software on the client computer.

1. Navigate to the **Computers** tile or select **Systems** > **Computers** from the top menu.
2. Right-click the computer(s) you want to deactivate and click **Deactivate** from the menu. You are prompted to check you want to continue with the deactivation of the computer(s). Click **Deactivate Anyway** to proceed, otherwise click **Cancel**.

Filter to Deactivated Computers

To see which computers have been deactivated:

1. In the **Computers** grid, scroll to the right and select the filter drop down.
2. Click **Deactivated** so it has a tick next to it:



3. The Deactivated column is displayed. Select **Yes** from the filter at the top of the **Deactivated** column to see computers that have been deactivated. This is indicated by a circular icon with a slash through it.

Update Policy on All

This option is only available if you have manual deployment set in the "Policy Deployment Settings" on page 33. This allows you to manually deploy the policy to all computers. The deployment will be spread across the number of minutes you define in the "Policy Deployment Settings" on page 33.

1. Navigate to the **Computers** tile or select **Systems** > **Computers** from the top menu.
2. Right-click anywhere in the grid click **Update Policy on All** from the menu. You are prompted to check you want to continue with updating the policy on all computer(s). Click **Update Policy on All** to proceed, otherwise click **Cancel**.

Update Policy on Selected

This option is only available if you have manual deployment set in the "Policy Deployment Settings" on page 33. This allows you to manually deploy the to the selected computers. The deployment will be spread across the number of minutes you define in the "Policy Deployment Settings" on page 33.

1. Navigate to the **Computers** tile or select **Systems** > **Computers** from the top menu.
2. Right-click the computer(s) you want to update the policy on and click **Update Policy on Selected** from the menu. You are prompted to check you want to continue with updating the policy. Click **Update Policy Anyway** to proceed, otherwise click **Cancel**.

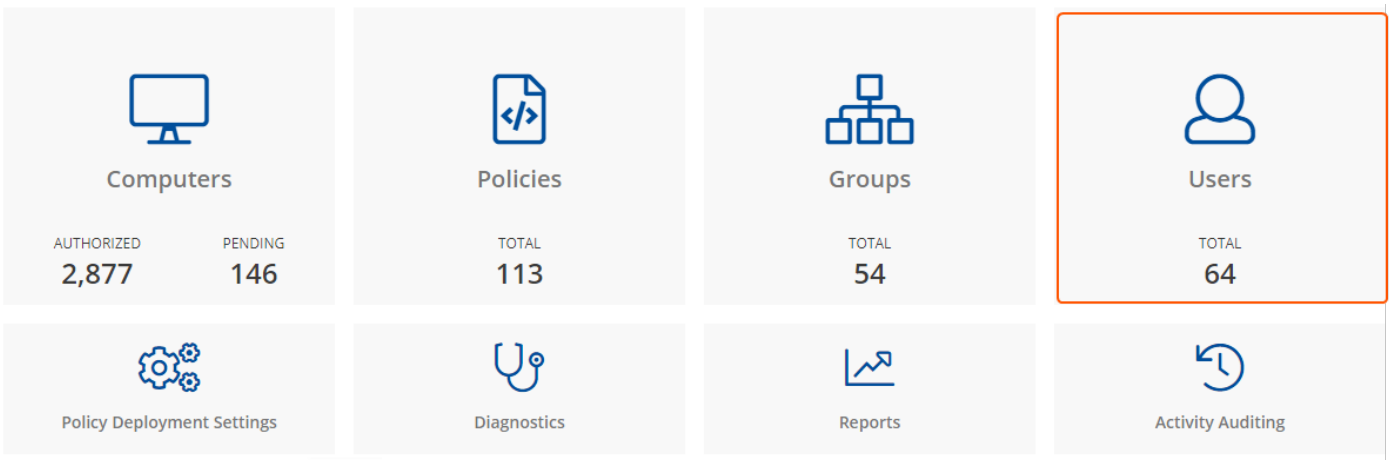
Note: *You can select multiple rows using the standard Windows functionality.*

Users

Each user in iC3 must exist in your authentication provider. Each user is assigned a role which determines what actions they are allowed to perform in the iC3 portal and Privilege Management MMC snap-in.

You can perform the following tasks in the Users tile:

- "Create a User" on page 31
- "View Details of a User" on page 32
- "Edit Properties of a User" on page 32
- "Assign Roles to a User" on page 32
- "Disable a User" on page 32
- "Enable a User" on page 32



Create a User

The user needs to exist in your authorization provider before you add that user in to iC3.

1. Navigate to the **Users** tile or select **Administration** > **Users** from the top menu.
2. Right-click anywhere on the grid and click **Create User** or select **Actions** > **Create User** from the top menu.
3. Enter the Account Name. For AD FS this must take the form:

```
<username>@<AD  FS Domain>.com
```

4. For Azure AD this must take the form:

```
<username>@<tenantname>.onmicrosoft.com
```

5. Enter the user's email address and select a Role. User roles are detailed in the "User Roles" on page 56 section.
6. Click **Submit** to create your User.

View Details of a User

1. Navigate to the **Users** tile or select **Administration** > **Users** from the top menu.
2. Right-click on the User you want to view the Details for and click **Details** or select **Actions** > **Details** from the top menu. This section shows you the details for the User. You can add annotations if required. You can also edit the details of the user here, see "Edit Properties of a User" on page 32 for more information.

Edit Properties of a User

1. Navigate to the **Users** tile or select **Administration** > **Users** from the top menu.
2. Right-click on the User you want to view the Details for and click **Edit Properties** or select **Actions** > **Edit Properties** from the top menu. This section allows you to edit the details for the User. You can edit details such as the account name, email address, the time & date format as well as the time zone here.
3. Click **Submit** to save your changes.

Assign Roles to a User

1. Navigate to the **Users** tile or select **Administration** > **Users** from the top menu.
2. Right-click on the User you want to assign a new role to and click **Assign Role** or select **Actions** > **Assign Role** from the top menu. This section allows you to change the role that is assigned to the user. User Roles are detailed in the "User Roles" on page 56 section.
3. Click **Submit** to save your changes.

Disable a User

1. Navigate to the **Users** tile or select **Administration** > **Users** from the top menu.
2. Right-click on the User you want to disable from Details for and click **Disable** or select **Actions** > **Disable** from the top menu.
3. You are prompted to check you really want to disable the user. Click **Disable Anyway** to disable the user, otherwise click **Cancel**. You can enable the user again later if required, see "Enable a User" on page 32 for more information. The row will flash green to indicate that iC3 has processed your request and the user will be removed from the grid if you are using the default view.

Users that are disabled are not shown by default. To view users that are disabled, click the hamburger icon on the top right of the grid and click **Disabled** to show the Disabled column. You can now change the filter for the Disabled column to show those users who have been disabled.

Enable a User

Disabled users are not shown by default. To view users that are disabled, click the hamburger icon on the top right of the grid and click **Disabled** to show the Disabled column. You can now change the filter for the Disabled column to show those users who are disabled.

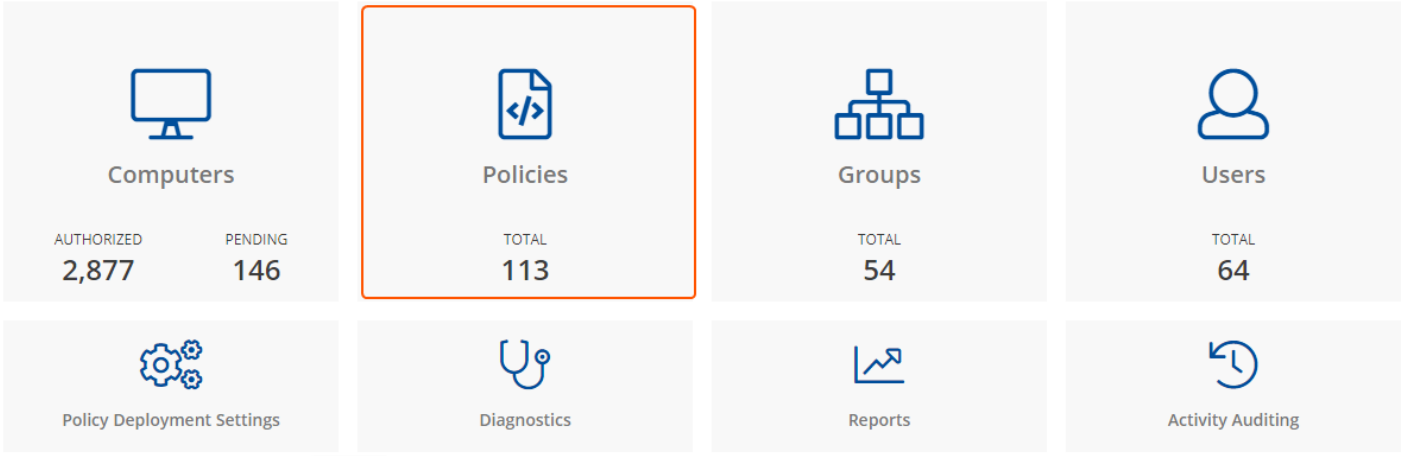
1. Navigate to the **Users** tile or select **Administration** > **Users** from the top menu.
2. Right-click on the User you want to enable for and click **Enable** or select **Actions** > **Enable** from the top menu.
3. The row will briefly flash green to indicate that iC3 has processed your request and the user is now enabled.

Policy Deployment Settings

The Policy Deployment Settings tile allows you change the settings related to policy deployment.

You can perform the following tasks in the Policy Deployment Settings tile:

- "Manage Policy Deployment Settings" on page 33



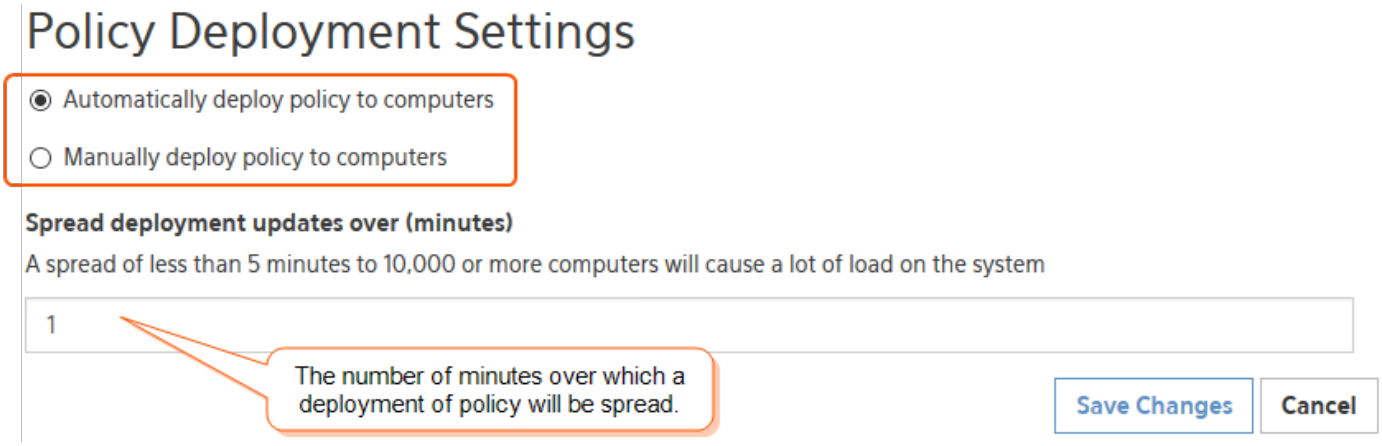
Manage Policy Deployment Settings

In the Policy Deployment Settings page you can choose to deploy the policy automatically or manually to your computers.

If you select automatic deployment, you do not need to do anything else to deploy a policy that is assigned to a group containing computers.

If you select manual deployment there are two additional options when you right-click one or more computers in the Computers grid. These settings allow you to deploy to the selected computers or all computers.

You also choose how many minutes to spread the deployment across your endpoints for both automatic and manual deployment.

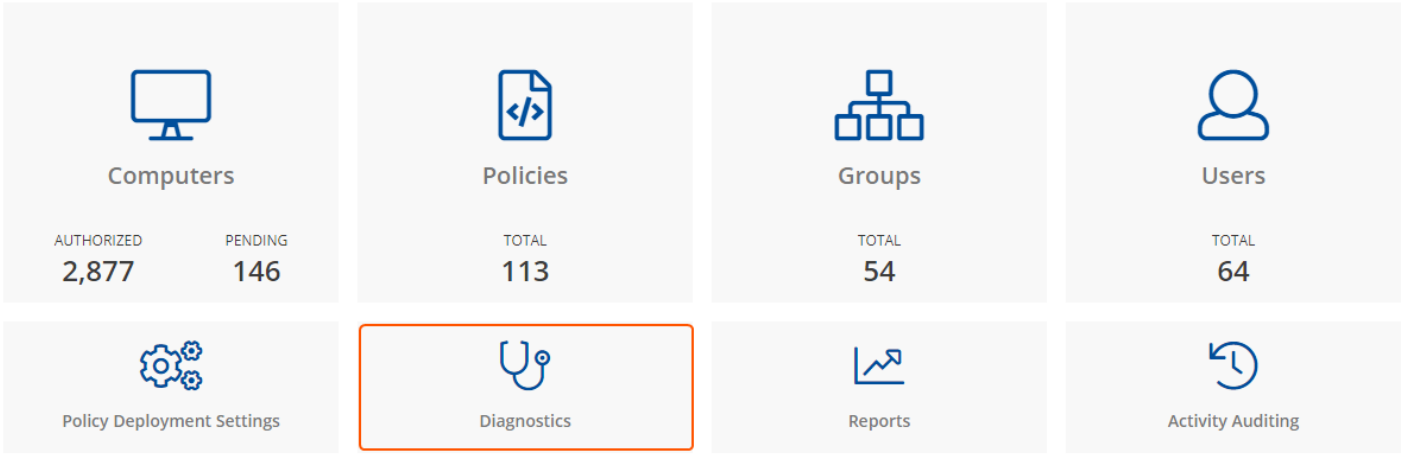


Diagnostics

The Diagnostics tile allows you view various diagnostics for iC3 including:

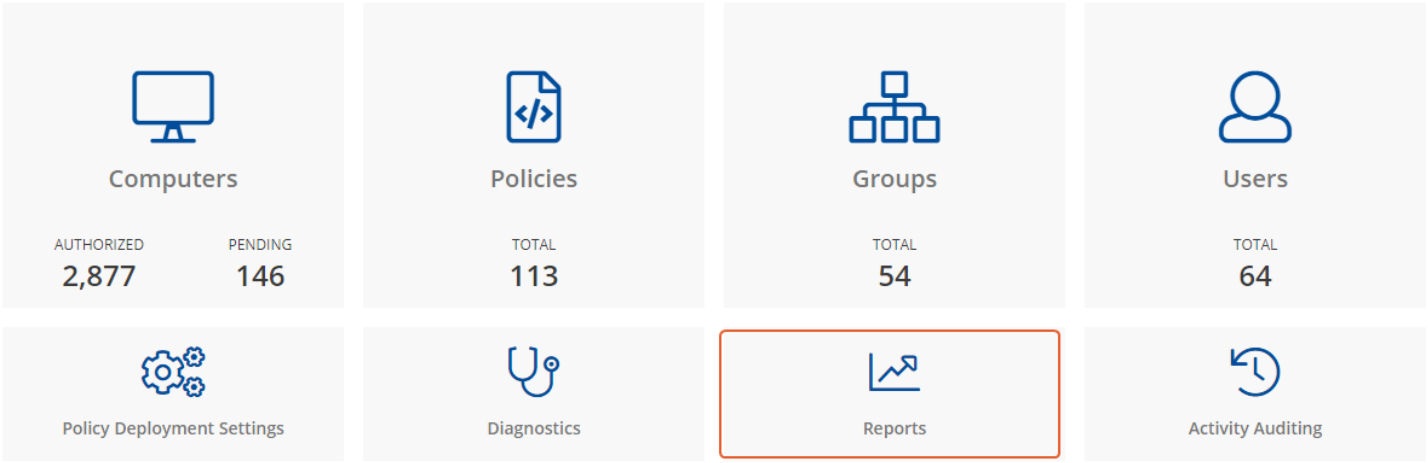
- Version
- Deployment Id
- Source
- Role
- Instance
- Api Connection
- User
- Tenant Id
- ER Database Version

The User Claims are also listed here. This information may be required by BeyondTrust Support.



Reports

The Reports tile allows you to view Enterprise Reporting within iC3.



Summary

The **Summary** dashboard summarizes the most important activity that has occurred in the time period defined by the quick filter. You can use this information to inform workstyle development or to show anomalous user behavior in your organization.

The Summary Dashboard includes the following charts:

Chart	Description
<number> Applications Discovered	The total number of newly discovered **Applications** split by the type of user rights required: • Admin rights required • Standard rights required
<number> Admin Logins by <number> users on <number> endpoints	Summarizes the number of admin logons, how many users carried them out and how many endpoints were used. Clicking the number of Admin Logons, Users or Endpoints shows you additional information about the Administrator logins.
<number> Applications run from external sources	The number of applications that were run from external sources. Clicking this tile takes you to the Target Types > All report with the Source filter applied.
<number> TAP incidents affecting <number> users	The number of Trusted Application incidents, how many users, and how many endpoints were affected. Clicking the TAP Incidents tile takes you to the Process Detail report with the Trusted Application Name filter applied. Clicking the Users tile takes you to a list of users that were affected by the TAP incident.
<number> attempts to modify privileged groups	The number of blocked attempts to modify privileged groups. Clicking this tile takes you to the Privileged Account Management report.
<number> UAC Matches	The number of applications that triggered User Account Control (UAC). Clicking this tile takes you to the Target Types > All report with the UAC Triggered filter applied.
<number> Applications used on demand	The number of applications that were launched using on-demand privileges. Clicking this tile takes you to the Target Types > All report with the Shell or Auto filter applied.
<number> Hosts Audited	The number of computers that were audited. Clicking this tile takes you to a list of hosts that have been audited.
<number> Activities Blocked	The number of applications that were blocked. Clicking this tile takes you to the Target Types > All report with the Action filter applied.
<number> Events audited	The number of events that were audited. Clicking this tile takes you to the Events > All report.

Discovery

This report displays information about applications that have been discovered by the reporting database for the first time. An application is first discovered when an event is received by the Enterprise Reporting database.

This dashboard displays the following charts:

Chart	Information
Applications first reported over the last x months (number)	Grouped by: • Admin Rights Detected • Admin Rights Not Detected
Types of newly discovered applications	Grouped by: • Admin Rights Detected • Admin Rights Not Detected
New applications with admin rights detected (top 10 of <number>)	Clicking the 'View All' link takes you to the Discovery > All report with the Admin Rights filter applied. Clicking an application takes you to the Discovery > All report with the Matched, Application Description and Publisher filters applied.
New applications with admin rights not detected (top 10 of <number>)	Clicking the 'View All' link takes you to the Discovery > All report with the Admin Rights filter applied. Clicking an application takes you to the Discovery > All report with the Matched, Application Description and Publisher filters applied.
New applications with admin rights detected (by type)	Clicking the 'View All' link takes you to the Discovery > All report with the Admin Rights filter applied. Clicking an application takes you to the Discovery > All report with the Admin Rights and Application Type filters applied.
New applications with admin rights not detected (by type)	Clicking the 'View All' link takes you to the Discovery > All report with the Admin Rights filter applied. Clicking an application takes you to the Discovery > All report with the Admin Rights and Application Type filters applied.

Discovery by Type

Discovery Requiring Elevation

Discovery from External Sources

This table displays all applications that have originated from an external source such as the Internet or an external drive.

You can click on the link in the Description column to see more detailed information on the application including the actions over the last 30 days split by the type of token, the top 10 users, the top 10 hosts, the run method and the portion of those discoveries where admin rights was detected.

The following columns are available for the Windows and OS X Discovery By Publisher table:

- **Description** – The description of a specific application.
- **Publisher** – The publisher of the applications.
- **Name** – The product name of a specific application.
- **Type** – The Type of application.
- **Source** - The source of the application.
- **Version** – The version number of a specific application.
- **# Users** – The number of users.
- **Median # processes / user** – The median number of processes per user.
- **# Hosts** – The number of hosts.
- **# Processes** – The number of processes.
- **Date first reported** – The date when the application was first entered into the database.
- **Date first executed** – The first known date that the application was executed.

New applications from external sources first reported over the last <time period>

This table groups the applications by type. You can click the plus icon to expand the path to show each individual application. You can view additional information about the application, their type, version, and the number of users using them. You can click the description to see in depth information about the application.

Discovery All

This table lists all applications discovered in the time period, grouped by the application description. If multiple versions of the same application exist, they are grouped on the same line. These can be expanded by clicking on the '+' symbol in the **Version** column.

The following columns are available for the Windows and OS X Discovery By Publisher table:

- **Description** – The description of a specific application.
- **Publisher** – The publisher of the applications.
- **Name** – The product name of a specific application.
- **Type** – The Type of application.
- **Version** – The version number of a specific application.
- **# Users** – The number of users.
- **Median # processes / user** – The median number of processes per user.
- **# Hosts** – The number of hosts.
- **# Processes** – The number of processes.
- **Date first reported** – The date when the application was first entered into the database.
- **Date first executed** – The first known date that the application was executed.

You can click on the link in the Description column to see more detailed information on the application including the actions over the last 30 days split by the type of token, the top 10 users, the top 10 hosts, the run method and the portion of those discoveries where admin rights was detected.

Actions

The following reports are available for Actions:

- **Actions Elevated** detailed on page 1
- **Actions Blocked** detailed on page 1
- **Actions Passive** detailed on page 1
- **Actions Canceled** detailed on page 1
- **Actions Custom** detailed on page 1
- **Actions Drop Admin Rights** detailed on page 1

Actions Elevated

The **Actions Elevated** report breaks down the elevated application activity by target type.

This dashboard displays the following charts:

Chart	Information
Elevated activity over the last <time period>	The number of targets that were elevated for each time segment split by the type of action. Clicking on the chart takes you to the Target Types > All report with the Action, Target Type, Range Start Time and Range End Time filters applied.
Distinct elevated target count by target type	The number of targets that were elevated for the complete time period split by the type of action. Clicking on the chart takes you to the Target Types > All report with the Action and Target Type filters applied.
Top 10 elevated targets	The top ten targets that were elevated for the time period. Clicking on the chart takes you to the Events > All report with the Action, Ignore Admin Required Events and Target Description filters applied.

Actions Blocked

The **Actions Blocked** dashboard breaks down the blocked application activity by target type.

This dashboard displays the following charts:

Chart	Information
Blocked activity action over the last <time period>	The number of targets that were blocked for each time segment split by the type of action. Clicking on the chart takes you to the **Target Types** > **All** report with the **Action**, **Target Type**, **Range Start Time**, and **Range End Time** filters applied.
Distinct blocked action target count by target type	The number of targets that were blocked for the complete time period split by the type of action. Clicking on the chart takes you to the **Target Types** > **All** report with the **Action** and **Target Type** filters applied.
Top 10 blocked action targets	The top ten targets that were blocked for the time period. Clicking on the chart takes you to the **Events >** All report with the **Action**, **Ignore Admin Required Events**, and **Target Description** filters applied.

Actions Passive

The **Actions Passive** dashboard breaks down the passive application activity by target type.

This dashboard displays the following charts:

Chart	Information
Passive action activity over the last <time period>	The number of targets where a passive token was used for each time segment split by the type of action. Clicking on the chart takes you to the Target Types > All report with the Action, Target Type, Range Start Time and Range End Time filters applied.
Distinct passive activity action target count by target type	The number of targets where a passive token was used for the complete time period split by the type of action. Clicking on the chart takes you to the Target Types > All report with the Action and Target Type filters applied.
Top 10 passive action targets	The top ten targets where a passive token was used for the time period. Clicking on the chart takes you to the Events > All report with the Action, Ignore Admin Required Events and Target Description filters applied.

Actions Canceled

The **Actions Canceled** dashboard breaks down the canceled application activity by target type.

This dashboard displays the following charts:

Chart	Information
Canceled activity action over the last <time period>	The number of targets that were canceled for each time segment split by the type of action. Clicking on the chart takes you to the **Target Types** > **All** report with the **Action**, **Target Type**, **Range Start Time**, and **Range End Time** filters applied.
Distinct canceled action target count by target type	The number of targets that were canceled for the complete time period split by the type of action. Clicking on the chart takes you to the **Target Types** > **All** report with the **Action** and **Target Type** filters applied.
Top 10 canceled action targets	The top ten targets that were canceled for the time period. Clicking on the chart takes you to the **Events** > **All** report with the **Action**, **Ignore Admin Required Events**, and **Target Description** filters applied.

Actions Custom

The **Actions Custom** report breaks down the custom application activity by the type of action.

This dashboard displays the following charts:

Chart	Information
Custom action activity over the last <time period>	The number of targets where a custom token was used for each time segment split by the type of action. Clicking on the chart takes you to the Target Types > All report with the Action, Target Type, Range Start Time and Range End Time filters applied.
Distinct custom action target count by target type	The number of targets where a custom token was used for the complete time period split by the type of action. Clicking on the chart takes you to the Target Types > All report with the Action and Target Type filters applied.
Top 10 custom action targets	The top ten targets where a custom token was used for the time period. Clicking on the chart takes you to the Events > All report with the Action, Ignore Admin Required Events and Target Description filters applied.

Actions Drop Admin Rights

The **Actions Drop Admin Rights** dashboard breaks down the drop admin application activity by target type.

This dashboard displays the following charts:

Chart	Information
Drop admin rights action activity over the last <time period>	The number of targets where a drop admin rights token was used for each time segment split by the type of action. Clicking on the chart takes you to the Target Types > All report with the Action, Target Type, Range Start Time and Range End Time filters applied.
Distinct drop admin rights action target count by target type	The number of targets where a drop admin rights token was used for the complete time period split by the type of action. Clicking on the chart takes you to the Target Types > All report with the Action and Target Type filters applied.
Top 10 targets drop admin rights action targets	The top ten targets where a drop admin rights token was used for the time period. Clicking on the chart takes you to the Events > All report with the Action, Ignore Admin Required Events and Target Description filters applied.

Target Types All

This table lists all applications active in the time period, grouped by the application description ordered by user count descending.

The following columns are available for the Windows and OS X Discovery All table:

- **Description** – The description of a specific application.
- **Platform** – The platform that the events came from.
- **Publisher** – The publisher of a specific application.
- **Product Name** – The product name of a specific application.
- **Application Type** – The type of application.
- **Product Version** – The version number of a specific application.
- **# Process Count** – The number of processes.
- **# User Count** – The number of users.
- **# Host Count** – The number of hosts.

You can click the Description to can view additional information about the target, its actions over the time period, the top 10 users, top 10 hosts, the type of run method and if admin rights were detected.

Trusted Application Protection

This report shows information about TAP incidents. A TAP incident is a child process of a Trusted Application being blocked due to a Trusted Application policy, or, a DLL being blocked from being loaded by a Trusted Application because it doesn't have a trusted owner or trusted publisher.

> ***Note:*** *There are no advanced filters for the Trusted Application Protection dashboard.*

Chart	Description
All Trusted Application Protection incidents over the time period.	A stacked bar chart showing the number of the different incidents broken down by the trusted application.
Trusted Application Protection incidents, by application	A table listing each trusted application, the number of TAP incidents, the number of Targets, the number of Users, and the number of Hosts affected.
Top 10 targets	The top 10 targets for TAP incidents. Clicking the Target name shows you more information about the target including its actions over the time period. Clicking on the Users shows you more information about the host. Clicking on the Host shows you more information about the host. Clicking on the Incidents takes you to the **Process Detail** detailed on page 1 report with the Distinct App ID filter applied.

Users

There are two reports for Users:

Users Privileged Logons

The **Privileged Logon** report shows you how many accounts with 'Standard' rights, 'Power User' rights and 'Administrator' rights have generated logon events broken down over the specified time frame.

This dashboard displays the following charts:

Chart	Information
Privileged logons over the last <time period>	A chart and table showing the number of logons by the different account types over time. Clicking the chart shows you more information about each privileged logon with the Range Start Time, Range End Time, Show Administrator Logons, and Show Standard User Logons filters applied.
Administrators, Power Users and Standard Users table	This table shows you the number of logon events made by Administrators, Power Users and Standard Users and how many users logged in.
Logons by account privileged	A chart showing the total number of logons broken down by logon privilege. Clicking the chart takes you to more information about the user logons for the time period with the Show Administrator Logons, Show Standard User Logons, and Show PowerUser Logons filters applied.
Logons by account type	A chart showing the total number of logons broken down by Domain Accounts and Local Accounts. Clicking the chart takes you to more information about the user logons for the time period with the Account Authority, Show Administrator Logons and Show Standard, Logons, and Show PowerUser Logons filters applied.
Top 10 logons by chassis type	A chart showing the total number of logons broken down by the top 10 Chassis types. Clicking the chart takes you to more information about the user logons for the time period with the Show Administrator Logons, Show Standard User Logons, and Show PowerUser Logons filters applied.
Top 10 logons by operating system	A chart showing the total number of logons broken down the top 10 host operating systems. Clicking the chart takes you to more information about the user logons for the time period with the Show AdministratorLogons, Show Standard User Logons, OS and Show PowerUser Logons filters applied.

Chart	Information
Top 10 accounts with admin rights	A chart showing the top 10 accounts with Admin rights that have logged into the most host machines. Clicking the chart takes you to more information about the user logons for the time period with the Show AdministratorLogons, Show Standard User Logons, User Name and Show PowerUser Logons filters applied.
Top 10 hosts with admin rights	A chart showing the top 10 host machines that have been logged on to by the most users with Admin Rights. Clicking the chart takes you to more information about the user logons for the time period with the Host Name, Show Administrator Logons, Show Standard User Logons, and Show PowerUser Logons filters applied.

Users Privileged Account Management

The **Privileged Account Management** report shows any blocked attempts to modify Privileged Accounts over the specified time interval.

Chart	Description
Privileged Account Management over the last <time period>	A chart breaking down the privileged account managements events and the number of events.
Activity table	A table showing the number of Users blocked, Hosts blocked, Applications blocked and the Total number of block events within the specified time frame.
By Privileged Group	The same data grouped by type of account. Clicking the account type takes you to detailed information about the account and hosts with the Group Name filter applied.
By application	A chart showing the privileged account modification activity that was blocked broken down by the description of the application used. Clicking the chart takes you to a more detailed view of that privileged account management activity for that application with the Application Description filter applied.
Top 10 users attempting account modifications	A chart showing the top 10 users who attempted modifications. Clicking the chart takes you to a more detailed view of that privileged account management account modifications with the Application User Name filter applied.
Top 10 hosts attempting account modifications	A chart showing the top 10 Hosts attempting privileged account modifications. Clicking the chart takes you to a more detailed view of that privileged account management account modifications with the Host Name filter applied.

Events

This report shows information about the different types of events that have been raised over the specified time period. It also shows the time elapsed since a host raised an event.

Chart	Description
Events over the last <time period>	A column chart showing the number of the different Event Types broken down by the time period. Clicking the chart takes you to the Events > All report with the Event Category, Range Start Time and Range End Time filters applied.
Event Types	A chart showing how many events have been received broken down by the Event Type. Clicking the chart takes you to the Events > All report with the Event Number filter applied.
By Category	A chart breaking down the events received split by Category. Clicking the chart takes you to the Events > All report with the Event Category filter applied.
Time since last endpoint event	A chart showing the number of endpoints in each time group since the last event category. Clicking the chart takes you to more detailed information about the host.

Events All

The following columns are available for the Windows and OS X **Events** > **All** table:

- **Event Time** – The time of the event.
- **Platform** – The platform that the event came from.
- **Description** – The description of the event.
- **User Name** – The user name of the user who triggered the event.
- **Host Name** – The host name where the event was triggered.
- **Event Type** – The type of event.
- **Workstyle** – The workstyle containing the rule that triggered the event.
- **Event Category** – The category of the event.
- **Elevation Method** – The method of elevation.

You can click some of the column data to review additional information on that event.

Process Detail

This report gives details about a specific process control event. Only processes that match rules in Workstyles are displayed.

There is an **Advanced** view available with this report which is available from the **Filters** drop-down. The Advanced view shows you the full set of columns available in the database.

- **Start Time** - The start time of the event.
- **Platform** - The platform that the events came from.
- **Description** - The description of a specific application.
- **Publisher** - The publisher of a specific application.
- **Application Type** - The type of application.
- **File Name** - The name of the file where applicable.
- **Command Line** - The command line path of the file if applicable.
- **Product Name** - The product name where applicable.
- **Trusted Application Name** - The name of the trusted application.
- **Trusted Application Version** - The version of the trusted application.
- **Product Version** - The version of the product of applicable.
- **Group Policy Object** - The group policy object, if applicable.
- **Workstyle** - The workstyle containing the rule that triggered the event.
- **Message** - Any message associated with the event.
- **Action** - Any action associated with the event.
- **Application Group** - The Application Group that the application that triggered the event belongs to.
- **PID** - The operating system process identifier.
- **Parent PID** - The operating system process identifier of the parent process.
- **Parent Process File Name** - The name of the parent process.
- **Shell / Auto** - Whether the process was launched using the shell 'Run with Defendpoint' option or by normal means (opening an application).
- **UAC Triggered** - Whether or not Windows UAC was triggered.
- **Admin Rights Detected** - Whether or not admin rights was detected.
- **User Name** - The user name that triggered the event.
- **Host Name** - The host name where the event was triggered.
- **User Reason** - The reason given by the user if applicable.
- **COM Display Name** - The display name of the COM if applicable.
- **Source URL** - The source URL if applicable.

Filters

Filters and advanced filters are available from the **Filters** drop-down.

The reports retrieve data and sort it using Javascript. If the volume of data exceeds the row limit, you may get misleading results due to this restriction.

Name	Description
Action	This filter allows you to filter by a type of action.
	• All • Elevated • Blocked • Passive • Sandboxed • Custom • Drop Admin Rights • Enforce Default Rights • Canceled • Allowed
Activity ID	Each Activity Type in Privilege Management has a unique ID. This is generated in the database as required.
Admin Required	This allows you to filter on if Admin Rights were required, not required or both.
	Filter options: • All • True • False
Authorization Required	This allows you to filter on if Authorization was required, not required or both.
	Filter options: • All • True • False
Admin Rights	Allows you to filter by the admin rights token.
	Filter options: • All • Detected • Not Detected
Application Description	A text field that allows you to filter on the application description.
Application Group	A text field that allows you to filter on the application group. You can obtain the application group from the policy editor.

Name	Description
Application Hash	This field is used by Enterprise Reporting. You do not need to edit it.
Application Type	A text field that allows you to filter on the application type. You can obtain the application type from the policy editor.
Authorizing User Name	The name of the user that authorized the message.
Browse Destination URL	The destination URL of the sandbox.
Challenge / Response	Allows you to filter by challenge / response events. For example, you can filter the application that required elevation on those applications that were launched following a completed challenge / response message.
	Filter options: • All • Only C/R
Client IPV4	This field is used by Enterprise Reporting. You do not need to edit it.
Client Name	This field is used by Enterprise Reporting. You do not need to edit it.
COM Application ID	This field is used by Enterprise Reporting. You do not need to edit it.
COM Display Name	This field is used by Enterprise Reporting. You do not need to edit it.
COM CLSID	This field is used by Enterprise Reporting. You do not need to edit it.
Command Line	A text field that allows you to filter on the command line.
Date Field	This allows you to filter by the time the event was generated, the application was first discovered or the time the application was first executed.

	Filter options:
	• Time Generated
	  ◦ This is the time that the event was generated. One application can have multiple events. Each event has a Time Generated attribute.
	• Time App First Discovered
	  ◦ This is the time that the first event for a single application was entered into the database. This can be delayed if the user is working offline.
	• Time App First Executed
	  ◦ This is the first known execution time of events for that application.

Name	Description
Device Type	The type of device that the application file was stored on.
	Filter options: • Any • Removeable Media • USB Drive • Fixed Drive • Network Drive • CDROM Drive • RAM Drive • eSATA Drive • Any Removeable Drive or Media
Distinct Application ID	This field is used by Enterprise Reporting. You do not need to edit it.
Elevate Method	Allows you to filter by the elevation method used.
	Filter options: • All • Admin account used • Auto-elevated • On-demand
Event Category	This filter allows you to filter by the category of the event.
	Filter options: • All • Process • Content • DLL Control • URL Control • Privileged Account Protection • Agent Start • User Logon • Services
Event Number	This field is used by Enterprise Reporting. You do not need to edit it. The number assigned to the event type.
File Owner	The owner of the file.
File Version	You can filter on the file version in the Advanced View of the Process Detail report.
GPO Name	You can filter on the Group Policy Object (GPO) name in some of the advanced reports such as Process Detail.
Host Name	This field allows you to filter by the name of the endpoint the event came from.

Name	Description
Ignore Admin Required Events	This field is used by Enterprise Reporting. You do not need to edit it.
Just Discovery Events	This field is used by Enterprise Reporting. You do not need to edit it.
Matched	Allows you to filter on the type of matching.
	Filter options: • All • Matched as child • Matched directly
Message Name	The name of the message that was used.
Message Type	The type of message that was used:
	Filter options: • Any • Prompt • Notification • None
Ownership	Allows you to group by the type of owner.
	Filter options: • All • Trusted owner • Untrusted owner
Parent PID	The operating system process identifier of the parent process.
Parent Process File Name	The file name of the parent process.
Path	Allows you to filter by the path. For example, to filter on applications that were launched from the System path.
	Filter options: • All • System • Program Files • User Profiles
PID	The operating system process identifier.

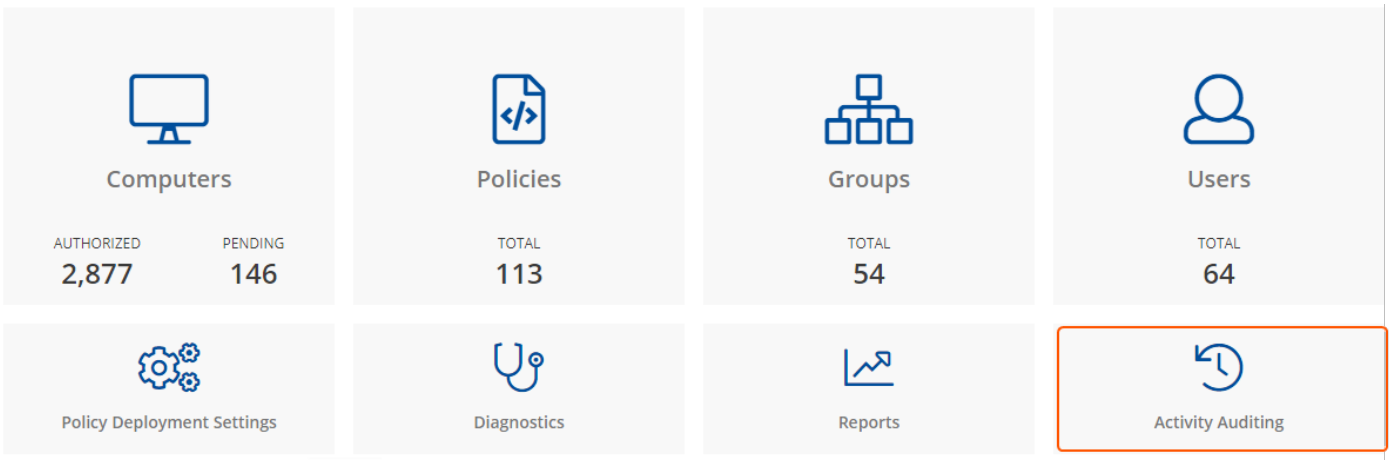
Name	Description
Platform	Filters by the type of operating system.
	Windows • Filters by endpoints running a Windows operating system. OS X • Filters by endpoints running a Mac operating system.
Process Unique ID	The unique identification of the process.
Product Code	This field is used by Enterprise Reporting. You do not need to edit it.
Product Name	The product name of the application.
Product Version	The product version of the application.
Program Files Path	Sets the Program Files path used by the **Discovery** > **By Path** report.
Publisher	The publisher of the application.
Range End Time	The end time of the range being displayed.
Range Start Time	The start time of the range being displayed.
Row Limit	The maximum number of rows to be retrieved from the database.
Rule Match Type	Rule Match Type: • Any • Direct match • Matched on parent
Sandbox	The sandboxed setting.
	Filter options: • Not Set • Any Sandbox • Not Sandboxed
Shell or Auto	Whether the process was launched using the shell 'Run with Defendpoint' option or by normal means (opening an application):
	Filter options: • Any • Shell • Auto
Show Discovery Events	Whether or not you want to show Discovery events. An event is a Discovery event if it's been inserted into the database in the filtered time period.

Name	Description
Source	The media source of the application. For example, was the application downloaded from the Internet or removable media.
	Filter options: • All • Downloaded over the internet • Removeable media • Any external source
System Path	Sets the system path.
Target Description	This field allows you to filter by the target description.
Target Type	This filter allows you to filter by a type of target. For example, you can filter to the applications that have been canceled across your time range in the Actions > Canceled report.
	Filter options: • All • Applications • Services • COM • Remote PowerShell • ActiveX • URL • DLL • Content
Time First Executed	This is the time range over which the application was first executed.
	Filter options: • 24 Hours • 7 Days • 30 Days • 6 Months • 12 Months
Time First Reported	This is the time range filtered by the date the application was first entered into the database.
	Filter optons: • 24 Hours • 7 Days • 30 Days • 6 Months • 12 Months

Name	Description
Time Range	This is the time range that the actions are displayed over.
	Filter options: • 24 Hours • 7 Days • 30 Days • 6 Months • 12 Months
Token Type	The type of Privilege Management token that was applied to the trusted application protection event.
	Filter options: • All • Blocked • Passive • Canceled
Trusted Application Name	The trusted application that triggered the event.
Trusted Application Version	The trusted application version number.
Trusted File Owner	Whether the file owner of the target file is considered trusted. To be a trusted owner the user must be in one of the following Windows groups; TrustedInstaller, System, Administrator.
UAC Triggered	Whether or not Windows UAC was triggered.
	Filter option: • Not Set • Triggered UAC • Did not trigger UAC
Uninstall Action	The type of uninstall action.
	Filter options: • Any • Change / Modify • Repair • Uninstall
Upgrade Code	This field is used by Enterprise Reporting. You do not need to edit it.
User Name	The user name of the user who triggered the event.
User Profiles Path	Sets the 'User Profiles' path.
Workstyle	A drop-down of workstyles in use.
Workstyle Name	The name of the workstyle that contained the rule that matched the application.
Zone Identifier	The Avecto Zone Identifier. This tag will persist to allow you to filter on it even if the ADS tag applied by the browser is removed.

Activity Auditing

The Activity Auditing tile allows you to view audit activity for iC3 administration activity if you have a user role that allows it. Rows that indicate an error are shown in red. You can also filter for those using the **Error** column.



Administration

The Administration menu contains the following areas:

- The "Users" on page 31 tile
- "User Roles" on page 56
- "Settings" on page 56
- "Agent Installation" on page 58
- The "Activity Auditing" on page 55 tile
- The "Diagnostics" on page 34 tile

User Roles

Each user in iC3 has an associated user role. You can view the roles by going to **Administration** > **User Roles**.

There are five user roles:

- Administrator
- Agent administrator
- Policy administrator
- Policy editor
- Standard user

Each user role has various permissions across 11 areas:

- Agent
- Dashboard
- Enterprise reports
- Group
- Policy
- Policy draft
- Remote access settings
- Role
- Settings
- Task
- User

iC3 displays which user roles have which permissions.

Settings

This menu has two options:

- "Auto Deactivate Settings" on page 57
- The "Policy Deployment Settings" on page 33 tile

- "Remote Access Settings" on page 57

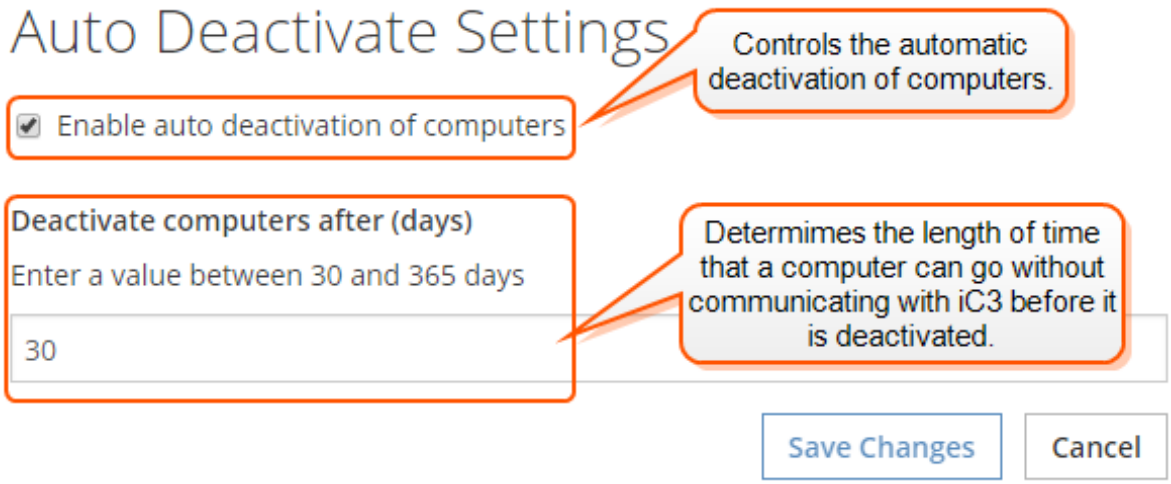
Auto Deactivate Settings

This page allows you to choose whether you want to deactivate computers that have not contacted iC3 for a number of days that you define when you enable the functionality. For example, a computer might not have contacted iC3 if it's a duplicate, see "View Duplicate Computers" on page 28.

The task to deactivate computers runs every day at 02:30 server time on the node where the job service is running. The deactivation job is audited in the Activity Log. You can filter on deactivated computers in the Computers grid, see "Deactivate Computers" on page 28 for more information.

To enable the automatic deactivation of computers select the **Enable auto deactivation of computers** check box. When this check box is selected, you can enter a value between 30 and 365 days. This determines the duration since the computer last contacted iC3 before it is automatically deactivated.

Deactivated computers are disconnected from iC3 and will no longer be able to communicate with iC3. This action can't be reversed unless you re-install the software on the client computer.



You can also manually deactivate Computers, see "Deactivate Computers" on page 28 for more information.

Remote Access Settings

This contains the remote access settings that are used to communicate with the Privilege Management MMC snap-in.

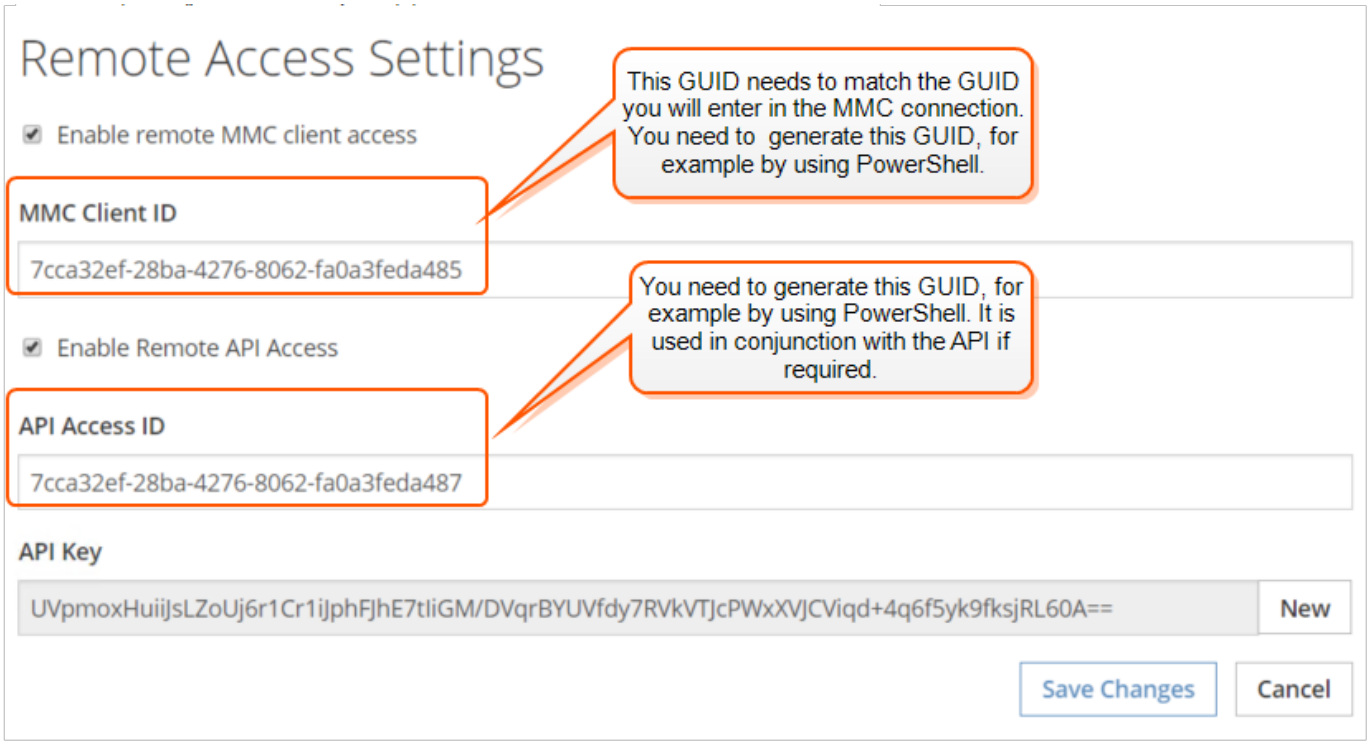
You need to configure iC3 to allow the Privilege Management MMC snap-in to communicate with the iC3 services.

1. Click **Administration** > **Settings** > **Remote Access Settings** from the top menu.
2. Select the **Enable remote MMC client access** check box. You need to generate a new GUID and enter it here. You need to use the same GUID when you configure the MMC. This is the **MMC Client ID** in the MMC.

There are many ways to generate a GUID, for example you can use a PowerShell cmdlet:

```
new-guid
```


3. Select the **Enable API key access** check box. This can be any GUID because the Application ID is required. This GUID is required if you want to use the PowerShell API. Once again you need to generate this GUID.
4. You can optionally click the drop-down and click **New** to generate an API key click. This GUID is required if you want to use the PowerShell API.



Agent Installation

This page contains the Installation ID and Installation Key GUIDs that are required to connect computers to iC3. You can create new Installation IDs and Installation Keys here and delete them if required. Once you revoke an Installation Key you don't need to re-install adapters that have been authorized, only pending ones.

See "Install the Windows Adapter" on page 8 and "Install the Mac Adapter" on page 10 for more information on how these fields are used.

